MREP 78

APS mini Plus reader modules for wall-mounting, for BPT Xolid panels nad for OEM use in own applications

User's guide

(Date of release: 2014/5/15, valid for FW version 5.11)

1 Content

2 Product description

The *MREP 78* [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 can be used for a simple IDS control.

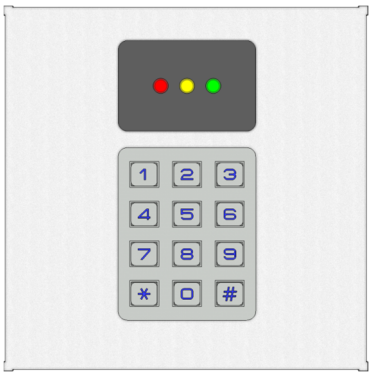
2.1 MREP 78 module

The reader module (*pic. 1*a) is intended for wall-mounting in both indoor and outdoor environment.

Pic. 1a: MREP 78

2.2 MREP 78X module

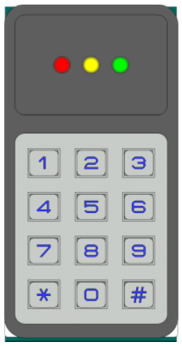
The reader module (*pic. 1b*) is designed for installation in Xolid entry panels of BPT audio and video system, where it occupies space of a single module.



Pic. 1b: MREP 78X

2.3 MREP 78E module

The reader module (pic. 1c) is designed for OEM applications, supplied as PCB. The module is designated for customers' own installation boxes.



Pic. 1c: MREP 78E

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

techfass®

3 Technical parameters

3.1 Product version

Product version	Product designation	Mechanical design	Catalogue number	Module features [2)]		
				TF	EM	HID
	MREP 78 – TF	*Wall-mounted*	53478400	✓	✘	✓
	MREP 78X – TF	*Xolid panel*	53478410	✓	✘	✓
	MREP 78E – TF	*OEM solution*	53478420	✓	✘	✓
	MREP 78 – EM	*Wall-mounted*	53478401	✓	✓	✓
	MREP 78X – EM	*Xolid panel*	53478411	✓	✓	✓
	MREP 78E – EM	*OEM solution*	53478421	✓	✓	✓

Table 1: Product version

[2)] *TF* – TECHFASS factory ID media reading; *EM* – EM Marin ID media reading; *HID* – HID Proximity ID media reading

3.2 Technical features

Technical features			
Supply voltage			8 ÷ 18 VDC
Current demand		Typical	70 mA
		Maximal	120 mA
Keypad layout			Numeric keypad, 12 keys
ID technology, typical reading range		EM Marin	5 cm (with ISO card)
		HID Proximity	2 cm (with ISO card)
Real-time clock			Yes, with self backup for 12 hrs.
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	Relay NC/NO, 2A/24V
I/O Port		External device	Ext. tamper / ext. reader buzzer control / input for IDS status monitoring / module disable function / reading synchronization MASTER/SLAVE modes
Indicators			3x LED 1x PIEZO
Tamper protection		Opening the cover Against tearing-off	Opto-electronic
Communication interface			RS 485
Alternative data input/output			WIEGAND (configurable)

Table 2: Technical features

3.3 Special accessories

Accessories		
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.

The *WIO 22* module is always required when the reader module is used for *IDS control*.

techfass®

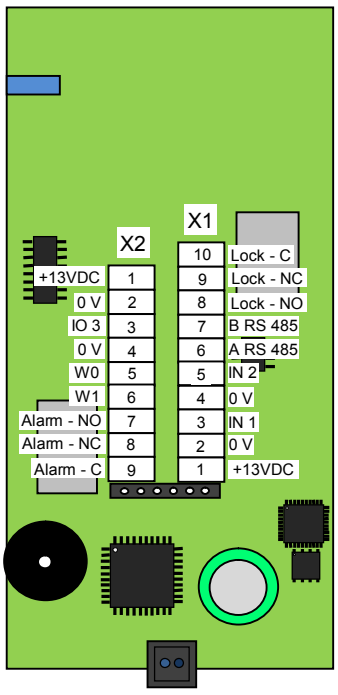
3.5 Mechanical design

Mechanical design	Weight	MREP 78	0.420 kg
		MREP 78X	0.306 kg
		MREP 78E	0.129 kg
	Operating temperature		-25 ÷ 60 °C
	Humidity		Max 95%, non-condensing
	Housing		IP 54
	Pigtail (MREP 78)		2 m
	Environment		Indoor and outdoor
	Dimensions	MREP 78	115 x 62 x 35 mm
		MREP 78X	120 x 120 x 33 mm
		MREP 78E	104 x 52 x 35 mm

Table 4: Mechanical design

4 Installation

4.1 Terminals and wiring description



Pic. 2: MREP 78X/E

Terminal description X1	#	Color	Function
	1	Red	+13 V pow. supply
	2	Blue	0 V pow. supply
	3	Yellow	Input 1
	4	Grey brown	0 V
	5	Grey	Input 2
	6	Black	A – RS 485
	7	White	B – RS 485
	8	Violet	NO lock relay
	9	Grey pink	NC lock relay
	10	Brown	C lock relay

Table 5: Terminal description X1

Terminal description X2	#	Color	Function
	1	Red blue	+13 V
	2	Green	0 V
	3	Pink	IO Port 3
	4	N / A	0 V
	5	Green white	Wiegand data 0
	6	Green brown	Wiegand data 1
	7	White grey	NO alarm relay
	8	White yellow	NC alarm relay
	9	Yellow brown	C alarm relay

Table 6: Terminal description X2

4.2 LED indicators description

Pic. 3: LED indicators description

LED indicators	D1	Communication status, ID media reading
	D2	Door lock status, programming mode
	D3	IDS monitoring

Table 7: LED indicators

LED indicators description	D1	Continuously lit – RED	Online operating mode
		Flashing with 4 s period – RED	Offline operating mode
		Fast switching – RED / GREEN	Address setting mode; RS 485 testing
		Single flash – GREEN	ID media reading
	D2	Lit - GREEN	Indicating door lock release
		Flashing / lit – YELLOW	Programming mode, PIN changing mode
		Short flashing with 1s p.– YELLOW	Indicating door lock release (optional)
	D3	Continuously lit – GREEN	Indicating IDS disarmed status
		Continuously lit – RED	Indicating IDS armed status
		Continuously lit – YELLOW	Indicating IDS arming / disarming status

Table 8: LED indicators description

4.3 Standard connection

Standard 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	Door lock control (relay)
	Output 2	Alarm status signaling (relay)
	I/O Port	External tamper (Standard operating mode) External reader buzzer control (op. mode with entry reader) Input for IDS status monitoring (op. mode standard with IDS control) Disabling function Reading synchronization: MASTER / SLAVE mode

Table 9: 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. 10* is used when the door status contact is not installed and no Forced Door and Door Ajar alarms are triggered.

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.

5 Setting parameters of the reader module

5.1 Configurable parameters

Configurable parameters				
	Parameter		Possible range	Default setting
	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 6.11*	Disabled
	Automatic summer time adjustment		YES / NO	YES
	Release lock with REX button when 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 10: 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.

techfass®

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.
- IDS control in the relevant operating mode using the WIO 22 relay module

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

- Reading a valid ID medium (card, key fob, etc. – for the standard reader module and the reader module with a reason keypad), reading a valid ID medium and entering a PIN code (for the reader module with a PIN keypad), or entering a valid code (reader module with a code keypad).
- Pressing the exit button (according to configuration).
- 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 module (optoelectronic sensor) 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. 10*, 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).

6.5.2 HID Proximity ID media format

When working with *HID Proximity* technology ID media, the module operates with a code in a recognized 26 or 32 bit format, in other cases it uses all 45 bits of a media (45bit raw format). If a specific format of the *HID Proximity* IDs is required, it can be performed by setting up the user's configuration of read 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 (operating mode)

6.6.1 Standard operating mode

In the *Standard operating mode* the interface can be used for remote control of the *WIO 22 relay module*. The *WIO 22* module outputs copy the status of the reader module door lock control and alarm outputs.

When the reader module operates in the standard operating mode, the I/O Port (*tab. 6*) is used as an input for monitoring an external device tamper status.

6.6.2 Wiegand input (entry reader)

When using the standard operating mode, the module can be configured for controlling the door from both sides (*entry reader mode*).

In the *entry reader mode* an identification event raised 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 (or the key code pressed when the reader keypad configuration is used).

When the reader module operates in the entry reader operating mode, the I/O Port (*tab. 6* 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.

6.6.3 Standard operating mode with IDS control

The *MREP 78* modules can be configured to the *Standard with IDS control* operating mode. In this mode the *WIEGAND interface* is used for controlling a *WIO 22 module, which is used for control of the IDS*. The first relay of the WIO 22 module is copying the status of the reader module door lock relay status, while the second relay is used for the IDS control.

When the reader module operates in the IDS control operating mode, the I/O Port (*tab. 6*) is used for monitoring the IDS status. The interpretation of its status is: I/O Port active status (= 0V signal from the IDS at the I/O Port) = IDS armed.

The IDS can be controlled with one of the following modes:

- *Status control* – the IDS is controlled by the status of the WIO 22 second relay, the status is defined: output active = IDS disarmed / output inactive = IDS armed
- *Pulse control* – the IDS status (armed / disarmed) is switched by a pulse of the WIO 22 second relay, the width of the pulse can be defined in the range of 0 ÷ 25500 ms with a 100 ms step

When using the Pulse control mode, the proper connection of the I/O Port for the IDS status monitoring is required!

Detailed description of the IDS control function is described in *chapter 8*.

6.6.4 Wiegand output operating mode

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 6.6*), after that they are sent in the output format. The *HID Proximity* ID media are sent in the same format as set for the standard operating mode.

When the reader module operates in this operating mode, the I/O Port (*tab. 11*) 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
	HID Proximity	Automatically recognized format / 45bit raw data
		User configuration

Table 11: 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 12*.

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 12: Signal function in WIEGAND operating mode

Key codes sent in *WIEGAND output* operating mode are described in *table 13*.

Key codes	Key pressed	Keypad configuration	
		PIN / ID keypad	Key code keypad
	1 ÷ 9 (digits)	Codes 1 ÷ 9	
	# (hash)	Code 11	
	0	Code 0	Code 10
	∗ (star)	Code 10	Code 0

Table 13: Key codes sent in WIEGAND output operating 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.

6.7 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 14 defines the interpretation of keys pressed at the keypad of *MREP 78 reader modules* according to the program configuration of the keypad function.

Pressed key interpretation	Key pressed	Keypad configuration	
		PIN / ID keypad	Key code keypad
	Keys 1 ÷ 9 (digits)	Digits 1 ÷ 9	Reason 1 ÷ 9
	Key 0	Digit 0	Reason 10
	Key ✳ (star)	Digits input cancel	Reason 0
	Key # (hash)	Input submit (enter)	Reason 11

Table 14: Pressed key interpretation

Note: When the operating mode "*Standard with IDS control*" is set, the press of *# (hash)* 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 4 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.

techfass®

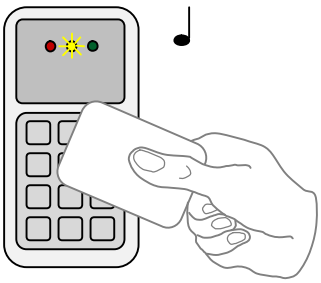
6.8.1 Inserting cards (codes) into the reader's memory

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

Step 1

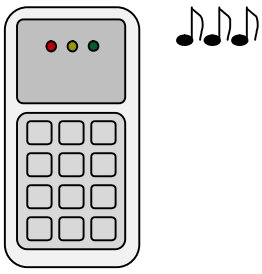
Read the programming card (or enter the programming code) for *inserting*: the reader goes into *programming mode*.

Step 2



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

Step 3



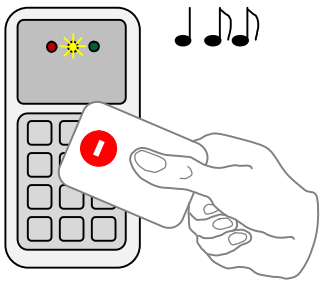
About 15 seconds after inserting the last card (code) the reader module goes back into *standard operating mode*.

Pic.4 a): Inserting cards (codes)

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

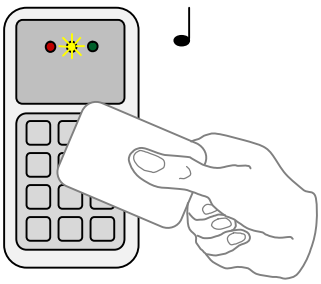
For deleting the cards from the reader module's memory use following steps:

Step 1



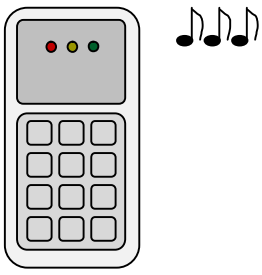
Read the programming card (or enter the programming code) for *deleting*: the reader goes into *programming mode*.

Step 2



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

Step 3



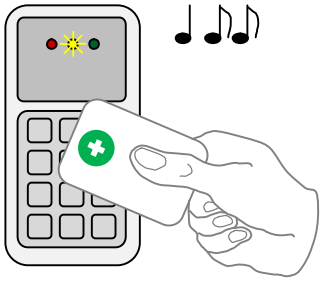
About 15 seconds after deleting the last card (code) the reader module goes back into *standard operating mode*.

Pic.4 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

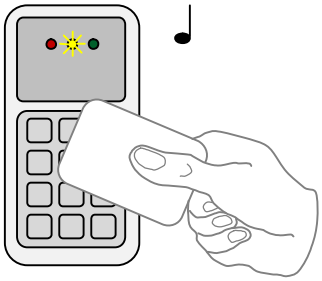


Read the programming card (or enter the programming code) for *inserting*: the reader goes into *programming mode*, which is indicated by slow flashing of yellow LED.

Step 2

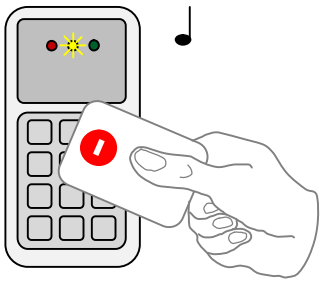
Read the programming card for inserting 5 times in a row (or enter the programming code); the reader will go into *Deleting cards “above or below”* mode indicated by fast flashing of yellow LED.

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*

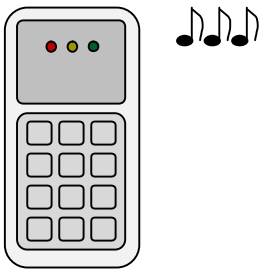


For deleting an ID located *right before* the ID used in precious step, read the programming card for *deleting* (or enter the programming code).

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



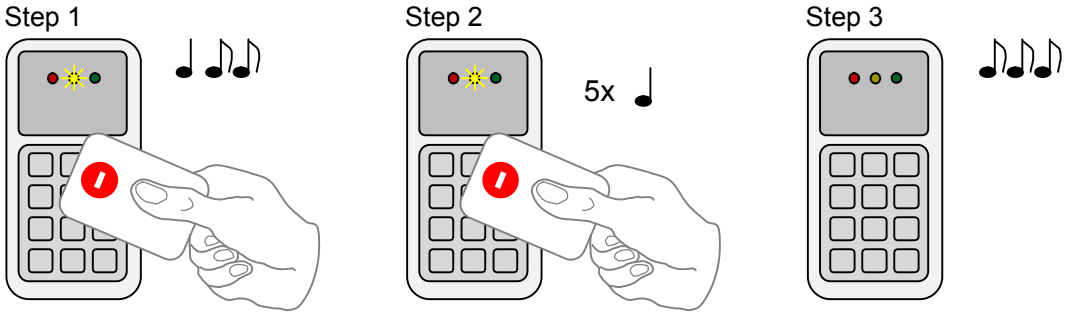
The reader module goes back into *standard operating mode*.

Pic.4 c): Deleting cards (codes) “above or below”

techfass®

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:



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

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.

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

Pic.4 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.4 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

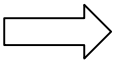
⇒

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

Pic.4 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.4 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. 4 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.
- *Clear opposite APB flag* – if the option is enabled, passing at the reader module causes a reset of the APB timer flag at the opposite side (entry reader) of the module.

In case of using the operating mode Standard with Entry reader the time APB function is evaluated at the entry reader only.

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.
- *Set opposite APB flag after APB alarm* – if the Zone APB alarm is raised, the Zone APB alarm flag is set for both directions (entry reader and the module itself) of the module.
- *Clear opposite APB flag* – if the option is enabled, passing at the reader module causes a reset of the Zone APB alarm flag at the opposite direction.

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

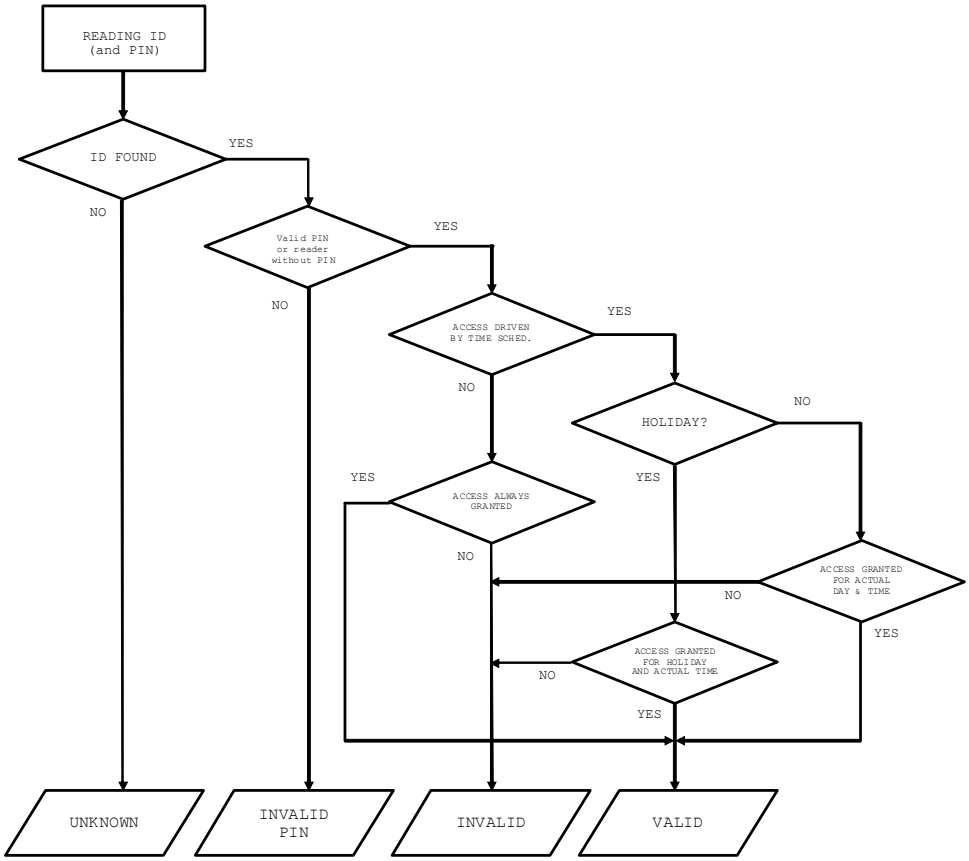
Since the *FW version 5.09* the reading synchronization of a *couple of TECHFASS readers* is implemented, enabling to *cancel the mutual disturbance* of the modules. The reader module offers to use the *IO synchronization* in both *MASTER* and *SLAVE* mode. The *input/output port 3* is used as the *synchronization 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. 5.*



Pic. 5: Simplified access rights evaluation

8 IDS control function

The special function of the reader is a *simple IDS control* with a use of a *WIO 22 relay module*. The function description follows.

8.1 IDS connection

The *IDS control function* is performed by the *second relay* of the *WIO 22 relay module*, which is connected to the reader module using the *WIEGAND interface* (the first relay of the WIO 22 module still copies the status of the reader module door lock relay).

The IDS can be controlled either by the *status* of the IDS control relay, or by an *impulse* of the IDS control relay. The width of the impulse is configurable (see *chapter 6.7.3*). The function of the IDS control relay is described in *table 15*.

Relay	Status control	Relay active	Disarm IDS
		Relay inactive	Arm IDS
	Impulse control	Relay active impulse	Switch IDS status (armed / disarmed)

Table 15: IDS control relay function

The IDS status is indicated by the third LED of the MREP 78 reader module (located on the right). In the status control mode the indication is based only on the control relay status, in the impulse control mode it is given by the I/O Port status. The meaning of the LED color and the logic of IDS signal at the I/O Port are described in *tables 16 and 17*:

LED	D3	Green	Indicating IDS disarmed status
		Red	Indicating IDS armed status
		Yellow	Indicating IDS arming / disarming status

Table 16: IDS status indicated at the reader module

I/O Port	0 V (GND) signal from the IDS connected to the I/O Port	IDS armed
	Other signal (or I/O Port not used) from IDS	IDS disarmed

Table 17: Logic of the IDS signal at the I/O Port

Proper connection of the reader module I/O Port with the IDS status signal is required for the correct function in the impulse control mode!

8.2 IDS operation

8.2.1 IDS disarmed

If the *IDS is disarmed* (indicated by the LED indicator – *green color*), a standard door open function is performed after a valid identification. *To arm the IDS*, the # (hash) key must be pressed *before identification*. The action of the reader and connected WIO 22 relay module depends on the IDS control mode:

- *Status control mode* – the control relay is switched off to arm the IDS and the IDS status LED indicator turns red.

- *Impulse control mode* – the control relay is activated for the defined time (impulse width), the LED indicator turns yellow, the reader starts to indicate arming process with short beeping and awaits the IDS to change its status (signal at the I/O Port). If the status is changed, the LED indicator turns red and the IDS is armed. If the status is not changed within 10 s, the LED indicator turns green and an event is saved to the reader's memory: Failed to arm the IDS.

8.2.2 IDS armed

If the *IDS is armed* (indicated by the LED indicator – *red color*), the standard door open function is not performed after a valid identification without entering a PIN code. To disarm the IDS, PIN code entering is standardly required. Since the *FW version 5.4* the PIN code entering for disarm operation can *be suppressed according to a time schedule*. After a valid identification the disarm operation is performed. The action of the reader and connected WIO 22 relay module depends on the IDS control mode:

- *Status control mode* – the control relay is switched on to disarm the IDS and the IDS status LED indicator turns yellow and the reader starts to indicate disarming process with short beeping for 5 s. After that the LED indicator turns green and a standard door open function is performed.
- *Impulse control mode* – the control relay is activated for the defined time (impulse width), the LED indicator turns yellow, the reader starts to indicate disarming process with short beeping and awaits the IDS to change its status (signal at the I/O Port). If the status is changed, the LED indicator turns green, the IDS is disarmed and a standard door open function is performed. If the status is not changed within 10 s, the LED indicator turns red and an event is saved to the reader's memory: Failed to disarm the IDS.

If the disarming process fails (impulse control mode), a user can use the emergency door open function – this will perform the standard door open function even when the IDS is armed. The emergency door open function is activated when a user attempts to disarm the IDS within 25 s after an unsuccessful attempt to disarm the IDS.

8.3 IDS general notes

When using the IDS control mode, be aware of following facts:

- IDS arming operation can be performed by any known user (even if his access permission is defined by a currently invalid time schedule or his Antipassback flag is currently set).
- IDS disarming operation can be performed only by a user with valid access rights.
- Arming operation cannot be performed if the door is open – such attempt is stored in the events archive.
- Remote door open function cannot be performed when the IDS is armed – such attempt is stored in the events archive.
- Permanent door lock release according to a time schedule function is performed only when the IDS is disarmed.

9 Useful links

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