MREM 58 SferON

APS mini Plus reader module for SFERA panels

User's guide

techfass®

(Date of release: 2015/06/03, valid for FW version 5.12)

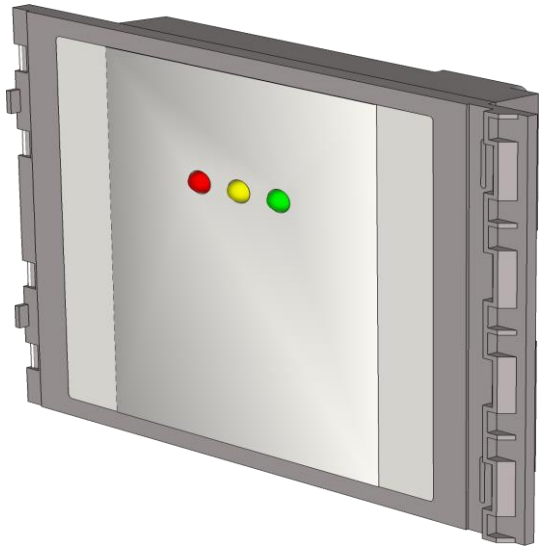
1 Content

2 Product description

The *MREM 58 SrefON* [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. 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 modules (*pic. 1*) are designed for installation in *SFERA* entry panels (models: All metal, All white, All street and Robur) of audio and video systems of *Bticino* company, which is a part of *Legrand* group. The reader modules are integrated in the bottom part of the Namespace module (part n. 352200), and occupy space of one standard module in the panel. The module has to be covered with a top part of the Namespace module in appropriate design (352201 – All metal; 352202 – All white; 352203 – All street; 352205 – Robur).

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



Pic. 1: MREM 58 SferON

techfass®

3 Technical parameters

3.1 Product version

Product version	Product designation	Catalogue number	Module design for entry panel	Module features [2]	
				TF	EM
	MREM 58 SferON – TF	53458600	SFERA New	✓	✘
	MREM 58 SferON – EM	53458601	SFERA New	✓	✓

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		9 ÷ 32 VDC
	Current demand	Typical	27 mA (27 V); 50 mA (12 V)
		Maximal	140 mA (9 V)
	Version with keypad		N/A
	ID technology, typical reading range	EM Marin	4 cm (with ISO card)
	Real-time clock		Yes, with self-backup for min. 24 hours
	Memory	Cards	2,000 ID, 2 programming cards
		Events	3,400
		Time schedules	64
	Inputs	1st input	Logical potential-free contact
		2nd input	Voltage input for connecting SFERA door lock output (+ 9 ÷ + 32 VDC)
	Output	Door lock	Relay NC/NO, 2A/24V
		Alarm	Relay NC/NO, 2A/24V
	I/O Port	External device	Ext. tamper / ext. reader buzzer control / module disable function / reading synchronization MASTER/SLAVE modes
	Signalization		3x LED 1x PIEZO
	Tamper protection	Against disassembly	Reed contact
	Communication interface		RS 485
	Alternative data 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* relay output module can be used for increasing the security of door control. The relay module is controlled by the *WIEGAND* interface of the reader module; *WIO 22* is located in the secure area and used for physical connection of the door lock contacts.

The *WIO 22* module control is active when the reader module operates in the standard operating mode. The relay module must be paired with the reader module before use (see http://techfass.cz/products-en/wio-22.html).

The WIO 22 can be used only with reader modules with FW version 4.12 or higher.

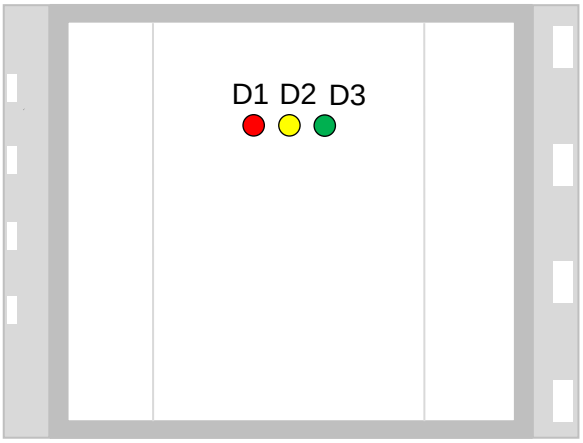
3.5 Mechanical design

Mechanical	Weight	0.114 kg
	Operating Temperature	-25 ÷ 60 °C
	Humidity	Max 95%, non-condensing
	Housing	IP 54, IK08 (built in entry panel)
	Pigtail	2x 0.5 m
	Dimensions (Height x Width x Depth)	115 x 91 x 27 mm

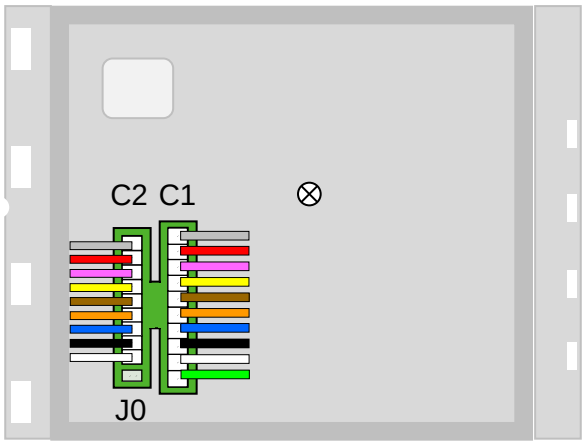
Table 4: Mechanical design

4 Installation

4.1 Connectors, jumpers and indicators description



Pic. 1: Front side of the MREM 58 SferON reader module



Pic. 2: Rear side of the MREM 58 SferON reader module

Described elements	Element	Purpose
	C1	Connector for C1 cable connection (10-wire cable)
	C2	Connector for C2 cable connection (9-wire cable)
	J0	Configuration jumper for RS 485 line termination
	D1	Red-green LED, operating mode and ID reading indication
	D2	Yellow LED, programming mode indication, door lock status indication
	D3	Green LED, door lock status indication

Table 5: Connectors, jumpers and indicators description

4.2 C1 a C2 cables wiring description

Wiring description	C1 cable		
	#	Color	Purpose
	1	Grey	GND (0 V)
	2	Red	+9 ÷ +32 VDC
	3	Pink	NO relay – lock
	4	Yellow	NC relay – lock
	5	Brown	C relay – lock
	6	Orange	Input 2 (1st contact)
	7	Blue	Input 2 (2nd contact)
	8	Black	RS 485 – A cable
	9	White	RS 485 – B cable
	10	Green	Input 1

C2 cable		
#	Color	Purpose
1	Grey	GND (0 V)
2	Red	+9 ÷ +32 VDC
3	Pink	NO relay – alarm
4	Yellow	NC relay – alarm
5	Brown	C relay – alarm
6	Orange	Input / output 3
7	Blue	GND (0 V)
8	Black	Wiegand data 0
9	White	Wiegand data 1

Table 6: Wiring description

4.3 LED Indicators

LED indicators				
	D1	Red-green	Continuously lit (red)	Online operating mode
			Flashing with 4 s period (red)	Offline operating mode
			Fast switching (red / green)	Address setting mode; RS 485 BUS testing mode
			Single flash (green)	ID media reading
	D2	Yellow	Continuously lit / flashing	Programming mode
			Short flashing with 1s per.	Indicating door lock release (configurable)
	D3	Green		Indicating door lock release

Table 7: LED indicators

4.4 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 when voltage 9 ÷ 32 VDC between input contacts (disregards polarity)
	Output 1 (relay)	Door lock control
	Output 2 (relay)	Active on any alarm condition
	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 8: 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. 9* is used when the door status contact is not installed and no Forced Door and Door Ajar alarms are triggered.

4.5 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 perform 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.

4.6 Mounting and removal the module

Reader module assembly and disassembly is performed the same way as other functional modules of the *SFERA* panel. Relevant mounting procedures can be found in the user's guide to the *SFERA* entry panel.

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 / external tamper / tamper / disabling function	REX button
	Third input / output port		Tamper / ext. buzzer signal / 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 after 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 9: 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.

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

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 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

ID with Alarm flag alarm occurs when an ID with the Alarm flag is read.

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. 6*) 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. 6*) is used as an input for monitoring an external device tamper status.

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

Table 10: 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 11*.

Wiegand	Input 1	Beeper control (0 V active)
	Input 2	Yellow LED control (+9 ÷ + 32 VDC active)
	Output 1 (relay)	Tamper signaling; it follows the alarm state of tamper sensors (tamper signal = relay switched on) [3)]

Table 11: Signal function in WIEGAND 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.

6.6.3 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. 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.

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

6.7 Programming mode

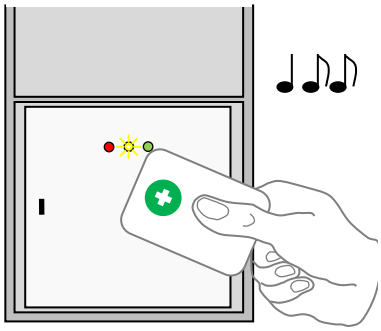
The module enters programming mode by reading one of the two *programming cards* (cards "+" and "-"). The programming mode cannot be entered while the module is in hardware address setting mode (for modules with HW address setting via the communication line). The module's functionality in programming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

6.7.1 Inserting cards into the reader's memory

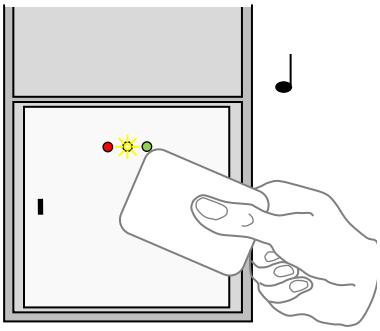
Follow these steps for inserting cards into the reader module's memory:

Step 1



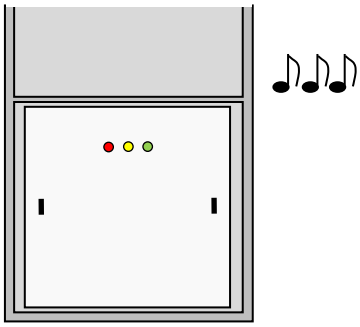
Read the programming card for *inserting*: the reader goes into *programming mode*.

Step 2



One by one, read the cards which are to be granted access.

Step 3



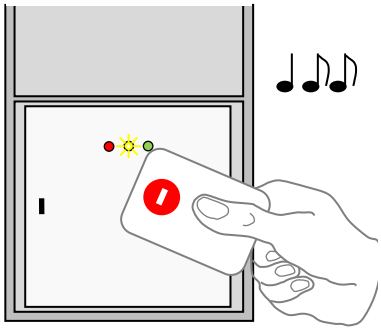
About 15 seconds after inserting the last card the reader module goes back into *standard operating mode*.

Pic.4 a): Inserting cards

6.7.2 Deleting cards from the reader's memory

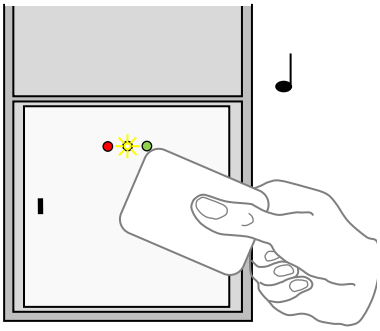
For deleting the cards from the reader module's memory use following steps:

Step 1



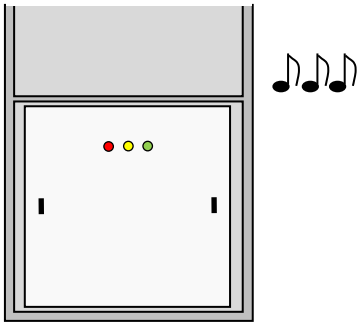
Read the programming card for *deleting*: the reader goes into *programming mode*.

Step 2



One by one, read the cards which are to have their access revoked.

Step 3



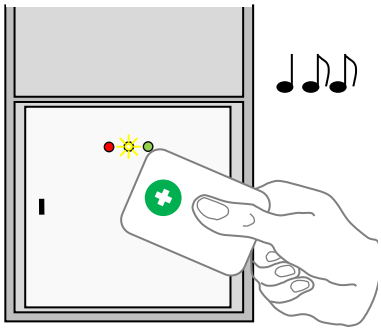
About 15 seconds after deleting the last card the reader module goes back into *standard operating mode*.

Pic.4 b): Deleting cards

6.7.3 Deleting cards „above or below“

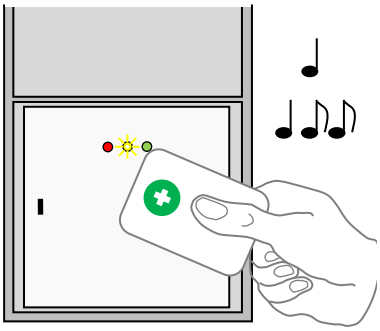
If a user loses his ID medium, it is usually impossible to delete the ID from the memory with the procedure described in the previous chapter, since the medium is no longer available (with an exception of entering the code at the keypad). Following procedure can be used for deleting such ID. The procedure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

Step 1



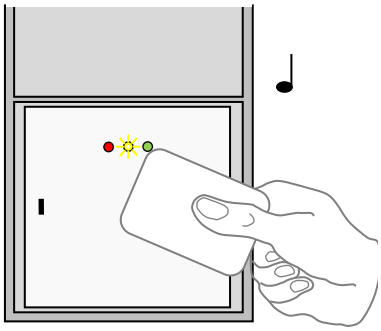
Read the programming card for *inserting*: the reader goes into *programming mode*, which is indicated by slow flashing of yellow LED.

Step 2



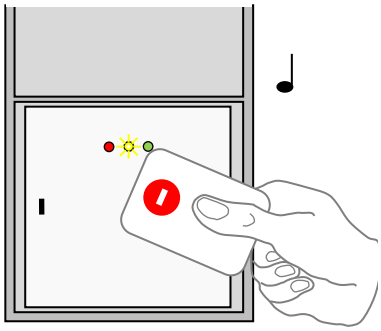
Read the programming card for inserting 5 times in a row; the reader will go into *Deleting cards “above or below”* mode indicated by fast flashing of yellow LED.

Step 3



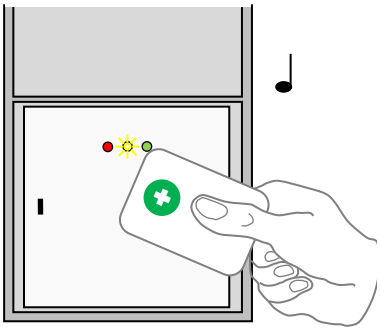
Read a card, which is located in the module’s memory *right before or right after* the card you wish to delete. After this step the module quickly flashes with yellow LED.

Step *4 - A*



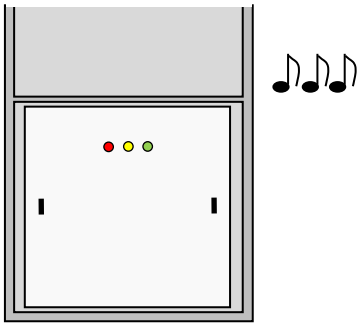
For deleting an ID located *right before* the ID used in precious step, read the programming card for *deleting*.

Step *4 - B*



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

Step 5

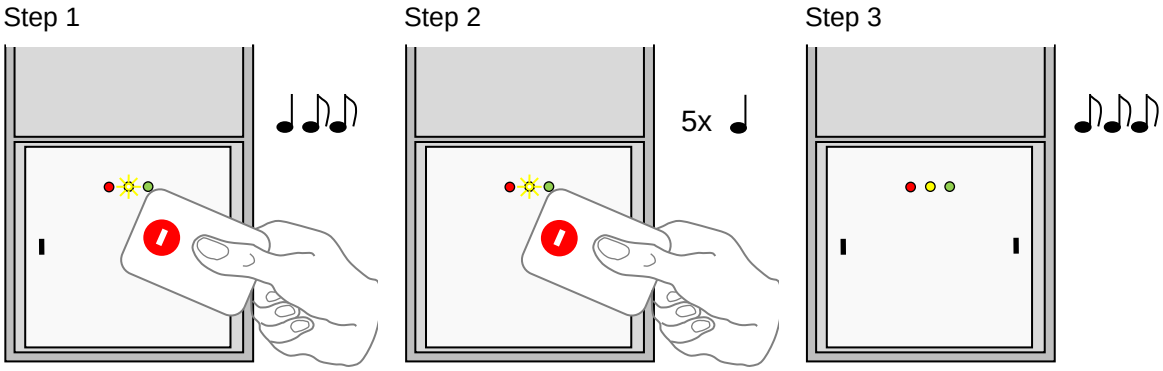


The reader module goes back into *standard operating mode*.

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

6.7.4 Deleting all cards from the reader's memory

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



Read the programming card for *deleting*: the reader goes into *programming mode*.

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

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

Pic.4 d): Deleting all cards

6.7.5 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 6.7.1* – 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 6.7.3* – 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

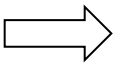
⇨

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 6.7.3* – 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 6.7.1* 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 6.7.4*, it is necessary to create a new filing table.

6.8 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.

6.9 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).

6.10 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).

6.10.1 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.

6.10.2 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.

techfass®

6.11 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.

6.12 Reading synchronization

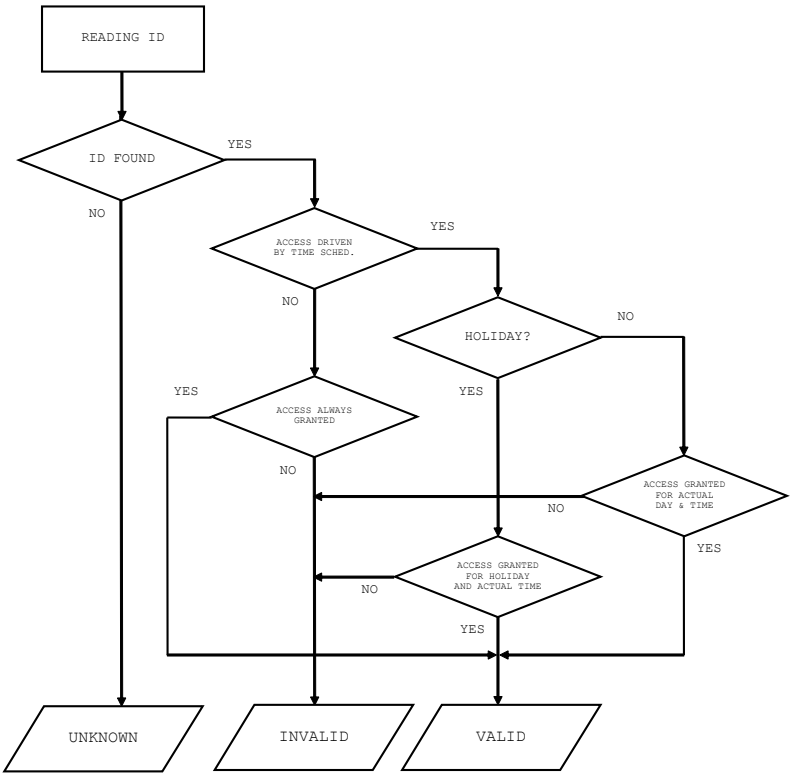
Since the *FW version 5.09* the reading synchronization of a *couple of TECHFASS readers* is implemented, enabling to *cancel the mutual disturbance* of the modules. The reader module offers to use the *IO synchronization* in both *MASTER* and *SLAVE* mode. The *input/output port 3* is used as the *synchronization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

6.13 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

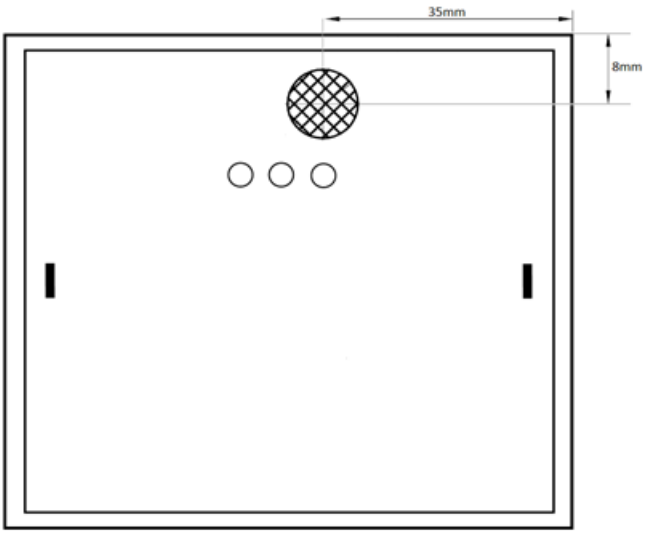
The model of access rights contains time schedules and a table of holidays. A block diagram for access right evaluation can be seen in *pic.5*.



Pic. 5: Simplified access rights evaluation

8 Magnet placement for tamper alarm indication

Magnet for tamper alarm indication should be attached to the front side of used installation box. The *picture 6* shows the position of the magnet relative to the MREM 58 SferON reader module position displayed from the front. The magnet position in the installation box is given by projecting the drawing at the front side of the installation box.



Pic. 6: Magnet placement

9 Useful links

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