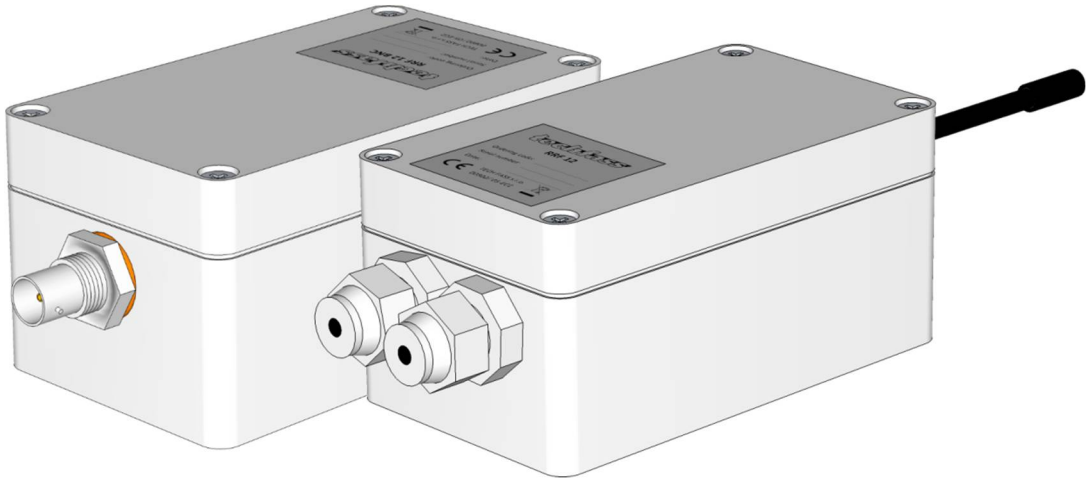
APS mini

MRRF 12

APS mini Plus long range 433 MHz reader modules

User's guide



techfass®

(Date of release: 2015/09/10, valid for FW version 5.11)

1 Content

2 Product description

The *MRRF 12* [1)] long range reader modules (433,92 MHz reader 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.

Active transmitters *Tx Key*, *Tx Cross* or *Tx Auto* are required for proper operation.

The modules are intended for surface mounting in outdoor environment. They are suitable for vehicle door control and wherever a long reading range is required, e.g. gates, garages, bars etc.

2.1 MRRF 12

The MRRF 12 module (*pic. 1a*) is equipped with an integrated antenna supporting typical reading range about 10 m.

Pic. 1a: MRRF 12

2.2 MRRF 12 BNC

The MRRF 12 BNC module (*pic. 1b*) is equipped with a BNC connector for connecting a 433 MHz antenna. Offered antenna type can be found in the product accessories list.

Pic. 1b: MRRF 12 BNC

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

techfass®

3 Technical parameters

3.1 Product version

Product version	Product designation	Catalogue number	Antenna	Identification media
	MRRF 12 – TF	53412000	Integrated	433 Mhz TF media
	MRRF 12 BNC – TF	53412800	External	433 Mhz TF media

Table 1: Product version

3.2 Technical features

Technical features			
	Supply voltage		8 ÷ 15 VDC
	Current demand	Typical	70 mA
		Maximal	130 mA
	Operating frequency		433.92 MHz
	Typical reading range	MRRF 12	10 m
		MRRF 12 BNC	Depends on used antenna type
	Real-time clock		Yes, with self backup for 12 hrs..
	Memory	Transmitters	2.000 ID, (1 master transmitter)
		Events	400F
		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
	Indicators		3x LED 1x terminals for external beeper
	Tamper protection		Integrated NC contact
	Communication interface		RS 485
	Alternative data output		WIEGAND (configurable)

Table 2: Technical features

3.3 Mechanical design

Design	Weight	0,214 kg
	Operating temperature	-25°C ÷ +60°C
	Humidity	Max. 95%, non-condensing
	Housing	IP 65
	Dimensions	65x115x55 mm

Table 3: Mechanical design

3.4 Special accessories

Special accessories	GP 433	51901400	Omnidirectional external antenna for MRRF 12 BNC
			
	Tx Key	51590200	Miniature pocket transmitter 433 MHz with 2 buttons, rolling code
	Tx Key/50	51590201	Miniature pocket transmitter 433 MHz with 2 buttons, rolling code (50 pc.)
			
	Tx Cross	51590300	Miniature pocket transmitter 433 MHz with 4 buttons, rolling code
	Tx Cross/50	51590301	Miniature pocket transmitter 433 MHz with 4 buttons, rolling code (50 pc.)
			
	Tx Auto	51590400	Car transmitter 433 MHz for fixed assembly, rolling code
	Tx Auto/100	51590401	Car transmitter 433 MHz for fixed assembly, rolling code (100 pc.)
			
	WIO 22	51901200	Remote control module, 2x relay
			

Table 4: Special accessories

3.5 Transmitters description

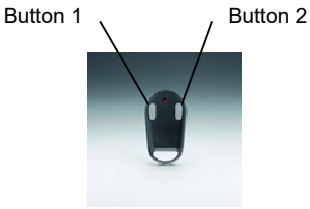
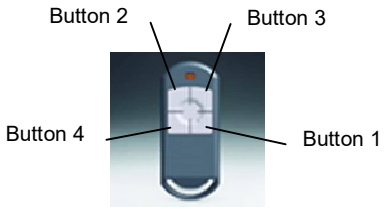
Transmitters description	Tx Key	Tx Cross	Tx Auto
			Button 1 – 1x click Button 2 – 2x click Button 3 – 3x click Button 4 – 4x click *Refer the Tx Auto manual please*

Table 5: Transmitters description

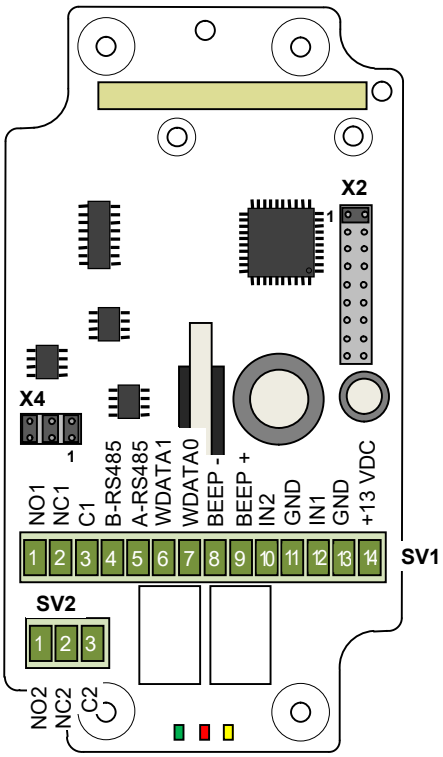
3.6 Using WIO 22 module for remote output control

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

4 Installation

4.1 Terminals and jumpers



Pic. 2 Terminals and jumpers

Jumpers X2	X2.1 ÷ 5	HW address (A0 ÷ A4)
	X2.6, 9	Reserved
	X2.7, 8	Setting of operational button

Table 6: Address jumpers X2

RS 485 X4	X4.1	Idle state definition (B)
	X4.2	Idle state definition (A)
	X4.3	Line terminator

Table 7: Setting the RS 485 line X4

Terminal block SV1	1	Relay1 NO
	2	Relay1 NC
	3	Relay1 C
	4	B - RS 485
	5	A - RS 485
	6	Wiegand DATA 1
	7	Wiegand DATA 0
	8	Beeper -
	9	Beeper +5 V
	10	Input 2
	11	0 V
	12	Input 1
	13	Supply voltage 0V
	14	Supply voltage +13,8 V

Table 8: Terminal block SV1

Relay2 SV2	1	Relay2 NO
	2	Relay2 NC
	3	Relay2 C

Table 9: Terminal block SV2

techfass®

4.2 Standard connection

Std. connection	Input 1	Door contact, active when door closed; REX button
	Input 2	Request to exit button or handle contact; Tamper; Disabling function; 0 VDC active
	Output 1	Door lock control (relay1)
	Alarm output	Alarm status signaling (relay2)

Table 10: 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. 12* 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	Red	Continuously lit	Online operating mode via RS 485
		Flashing with 4 s period	Offline operating mode
	Green		ID media reading
	Red/Green switching		RS 485 bus testing mode
	Yellow	Lit / flashing	Programming mode
		Short flashing with 1s per.	Door lock release indication (configurable)

Table 11: LED indicators

The indicating LEDs are situated directly on the PCB, so they can be seen when the cover is open only.

4.4 Installation instructions

Fasten the module directly on the wall in outdoor or indoor environment. Keep the module away from large metal parts to prevent decrease of reading range.

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	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
	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 6.9*	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 12: 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®

5.3 HW address setting

HW address setting is defined by the configuration of address jumpers X2.1 ÷ 5, see *Tab.6 and Tab.13.*

Keep in mind that every module on the line must be set to a unique address. When any address is duplicated, the address conflict appears on system bus and the system cannot work properly.

Address jumpers X2																
	Address	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
	X2.1	●	○	●	○	●	○	●	○	●	○	●	○	●	○	●	○
	X2.2	○	●	●	○	○	●	●	○	○	●	●	○	○	●	●	○
	X2.3	○	○	○	●	●	●	●	○	○	○	○	●	●	●	●	○
	X2.4	○	○	○	○	○	○	○	●	●	●	●	●	●	●	●	○
	X2.5	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	●
	Address	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32
	X2.1	●	○	●	○	●	○	●	○	●	○	●	○	●	○	●	○
	X2.2	○	●	●	○	○	●	●	○	○	●	●	○	○	●	●	○
	X2.3	○	○	○	●	●	●	●	○	○	○	○	●	●	●	●	○
	X2.4	○	○	○	○	○	○	○	●	●	●	●	●	●	●	●	○
	X2.5	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	○

Table 13: Address jumpers X2

Legend: ● *… set (ON)* ○ *… removed (OFF)*

5.4 Selecting the operational button

With respect to possibility of installing the modules close each other (for a control of multiple gates, bars etc.) without causing interference, different operational button can be set on every transmitter for controlling 2 or up to 4 devices [3)]. The selection of particular button is provided by setting of the X2.7 and X2.8 jumpers (*Tab. 6*) as follows:

Button select. X2	Jumpers		Operational button	Usable transmitters [3)]
	X2.7	X2.8		
	●	○	1	Tx Key, Tx Cross, Tx Auto
	○	●	2	Tx Key, Tx Cross, Tx Auto
	●	●	3	Tx Cross, Tx Auto
	○	○	4	Tx Cross, Tx Auto

Table 14: Selecting the operational button

Reader module's reset is required after any change of address or operational button setting, disconnect and connect the supply voltage again.
[3)] It is necessary to use Tx Cross or Tx Auto transmitters when the operational button is set to 3 or 4.

6 Reader modules functioning

The reader module supports the following functions:

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

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

- Reading a valid ID (Tx Key, Tx Cross, Tx Auto transmitter).
- 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 *Tab. 8*.

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 *Tab. 8*. The door lock relay status remains unchanged until another “Door Open” function is activated.

Reading a programming transmitter during door lock release will not cause the reader to enter the programming mode. Reading a valid transmitter 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.

6.3 Alarm statuses

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

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 (relay) (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 removing the cover or changing the status of input 2 in proper configuration) the “Tamper” state is activated [4)].

[4)] The Tamper switch is operational after its first change of status since switching on the module.

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 Wiegand operating mode

The reader module can be configured into a standard reader with a standard 26, 32, 42 or 44 bits *WIEGAND output*.

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* operating mode is described in *table 15*.

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) [4)]

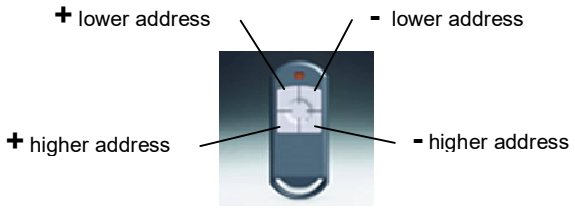
Table 15: Signal function in WIEGAND operating mode

6.6 Programming mode

The module enters programming mode by reading one of the two *programming buttons pressed on the master transmitter* ("+" or "-" button). The programming mode cannot be entered while the "Door Open" function is being performed (reading a programming transmitter is ignored). Alarm states are not triggered in programming mode. The module's functionality in programming mode can be seen in *Pic. 3*.

It is not possible to use the time schedules when inserting transmitters in the programming mode, therefore the transmitters inserted are always valid.

Since the FW version 5.05 there is the *Advanced function* of the module at disposal. If it is active, the module *gains 2 addresses*; each of them has a single lock relay and door lock status input assigned. The *pair of buttons located on top* at the master transmitter is used for programming mode control at the lower address, while the *pair of buttons located at the bottom* at the master transmitter is used for programming mode control at the *higher address*.



Pic. 3: Master transmitter

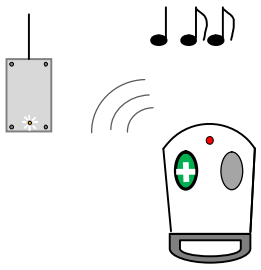
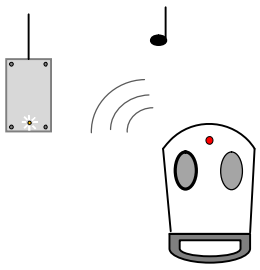
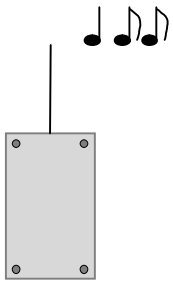
If the *Advanced function is not used*, it is necessary to use the *pair of buttons located on top* of the master transmitter.

Detailed description of the Advanced function can be found in chapter *6.10*.

Following pictures demonstrate the module behavior when using the master transmitter. For simplification the drawing shows only the horizontal location of the buttons (+/-), but in real you must always use only the button for relevant address!

6.6.1 Inserting transmitters in the reader's memory

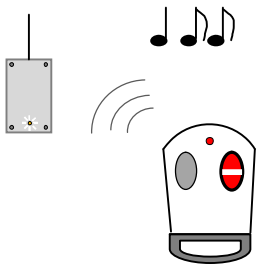
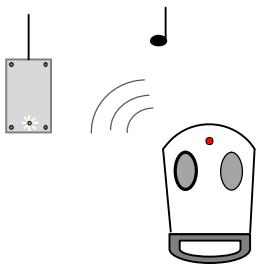
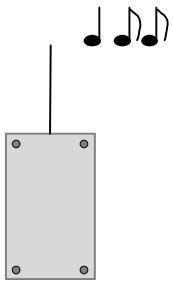
For inserting the transmitters in the reader module's memory use following steps:

Step 1	Step 2	Step 3
		
Press the left button of the programming transmitter for *inserting*: The reader goes into *programming mode*.	One by one press the relevant (*see Tab.12*) button of the transmitters which are to be granted access.	About 15 seconds after pressing the last button the reader module goes back into *standard operating mode*.

Pic. 3 a): Inserting transmitters in the memory

6.6.2 Deleting transmitters from the reader's memory

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

Step 1	Step 2	Step 3
		
Press the right button of the programming transmitter for *deleting*: The reader goes into *programming mode*.	One by one press the relevant (*see Tab.12*) button of the transmitters which are to be denied access.	About 15 seconds after pressing the last button the reader module goes back into *standard operating mode*.

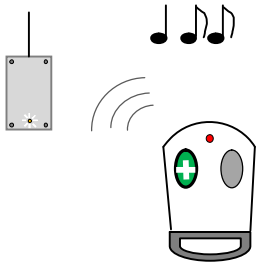
Pic. 3 b): Deleting transmitters from the memory

techfass®

6.6.3 Deleting transmitters „above or below“

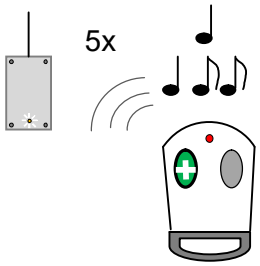
If a user loses his transmitter, it is impossible to delete it from the memory with the procedure described in the previous chapter, since the medium is no longer available. Following procedure can be used for deleting such transmitter. The procedure *requires using a transmitter*, which was inserted *right before or right after the transmitter*, which is meant to be deleted.

Step 1



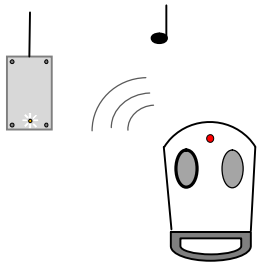
Press the left button of the programming transmitter for *inserting*: The reader goes into *programming mode*.

Step 2



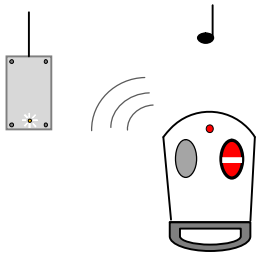
Press the left button of the programming transmitter for *inserting 5 more times*: the reader will go into *Deleting transmitters “above or below”* mode.

Step 3



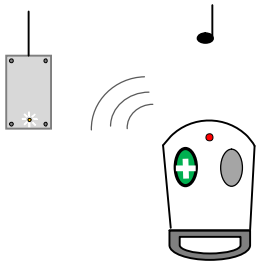
Press the relevant (*see Tab.12*) button of the transmitter, which is located in the module’s memory *right before or right after* the transmitter you wish to delete.

Step *4 - A*



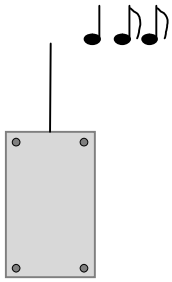
For deleting the transmitter located *right before* the transmitter used in previous step, press the right button of the programming transmitter for *deleting*.

Step *4 - B*



For deleting the transmitter located *right after* the transmitter used in previous step, press the right button of the programming transmitter for *instering*.

Step 5



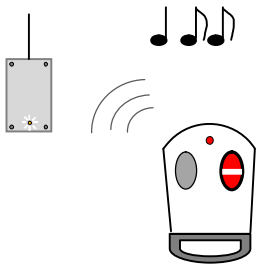
The reader module goes back into *standard operating mode*.

Pic.3 c): Deleting transmitters “above or below”

6.6.4 Deleting all transmitters from the reader's memory

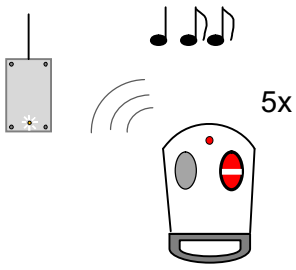
For deleting all transmitters from the reader module's memory use following steps:

Step 1



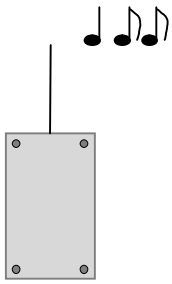
Press the right button of the programming transmitter for *deleting*: The reader goes into *programming mode*

Step 2



Press the *right button* of the programming transmitter for deleting *5 times in a row*. The reader will erase all transmitters from its memory.

Step 3



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

Pic. 3 c): Deleting all transmitters

6.6.5 Recommended method for access rights management (using master transmitter)

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

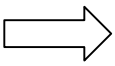
- Inserting *5 new transmitters* using the procedure from *chapter 6.5.1* – Press *left (inserting) button of the master transmitter*, press proper buttons at transmitters 1-5, after 15 s the programming mode is exited, *create a table*.

position	transmitter
1	transmitter 1
2	transmitter 2
3	transmitter 3
4	transmitter 4
5	transmitter 5

Pic.3 e): Table after inserting 5 transmitters

- *Transmitter 3 gets lost* – Delete it *using the transmitter 4*, which is available, and using the procedure from *chapter 6.5.3* – press the *left button (inserting) of the programming transmitter*, then *5x left button again*, then proper button of *transmitter 4*, and finally *right button (deleting) of the programming transmitter*. *Register the change in your table*.

position	transmitter
1	transmitter 1
2	transmitter 2
3	transmitter 3 (lost)
4	transmit. 4 (available)
5	transmitter 5

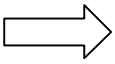


position	transmitter
1	transmitter 1
2	transmitter 2
~~3~~	~~transmitter 3~~
4	transmitter 4
5	transmitter 5

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

- *Transmitter 4 gets lost* – Delete it *using the transmitter 2*, which is available, and using the procedure from *chapter 6.5.3* – press the *left button (inserting) of the programming transmitter*, then *5x left button again*, then proper button of *transmitter 2*, and finally *left button (inserting) of the programming transmitter*. *Register the change in your table*.

position	transmitter
1	transmitter 1
2	transmit. 2 (available)
~~3~~	~~transmitter 3~~
4	transmitter 4 (lost)
5	transmitter 5



position	transmitter
1	transmitter 1
2	transmitter 2
~~3~~	~~transmitter 3~~
~~4~~	~~transmitter 4~~
5	transmitter 5

Pic.3 g): Deleting transmitter 4 using the transmitter 2, table after deleting transmitter 4

- It is necessary to *add another transmitter* (transmitter 6). We proceed with the procedure from *chapter 6.5.1* again. Press *left (inserting) button of the master transmitter*, press proper buttons at transmitter 6, after 15 s the programming mode is exited, *create a table*.

position	transmitter
1	transmitter 1
2	transmitter 2
~~3~~	~~transmitter 3~~
~~4~~	~~transmitter 4~~
5	transmitter 5
6	transmitter 6

Pic. 3 h): Table after inserting transmitter 6

A new transmitter is always inserted at the position after the last inserted transmitter. In case of deleting all transmitters using the procedure described in *chapter 6.5.4*, it is necessary to create a new filing table.

6.7 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.

6.8 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).

6.9 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).

6.9.1 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 relevant address. 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 relevant address. 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 relevant address causes a reset of the APB timer flag at the opposite side of the module.

6.9.2 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 relevant address. 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 sides of the module.
- *(*) Clear opposite APB flag* – if the option is enabled, passing at the relevant address causes a reset of the Zone APB alarm flag at the opposite side of the module.

(*) – only when using the *Advanced function*

6.10 Advanced function description

Since the *FW version 5.05* there is the *Advanced function* of the module at disposal.

This function enables to realize *application with control of 2 devices* (locks, gate motors, etc.) with a single module.

When the *Advanced function is active*, the module *gains two addresses*. *Each address* has a *single lock relay* and single *door contact input* assigned. The first address is defined by the configuration of address jumpers (*tab. 13*); the second is higher by 1.

The inputs and outputs purpose when using the Advanced function is described in *table 16*.

Advanced function	Physical description	Logical purpose (Advanced function)		Standard connection
	Input 1 (IN1)	Input 1	Lower address	Door (gate) contact 1
	Relay 1	Output 1 (Relay)		Lock control 1 (relay)
	Input 2 (IN2)	Input 1	Higher address	Door (gate) contact 2
	Relay 2	Output 1 (Relay)		Lock control 2 (relay)

Table 16: Standard connection of the module in the Advanced function mode

For identification at individual module address it is always necessary to *press the relevant button* (send relevant signal) at the transmitter.

Due to the fact that the modules are often located nearby and control multiple gates, bards, etc., it might be necessary to alter the setting of the functional buttons to avoid disturbance. The *functional buttons configuration* for individual modules is set by the *configuration of X2.7 and X2.8 jumpers* (*tab. 6*) like this (*tab. 17*, buttons descriptions: *tab. 5*):

Functional buttons	Jumpers		Address	Tx Key	Tx Cross	Tx Auto
	X2.7	X2.8				
	●	○	Lower	Button 1	Button 1	1x impulse
			Higher	Button 2	Button 2	2x impulse
	○	●	Lower	N / A	Button 2	2x impulse
			Higher	Button 1	Button 3	3x impulse
	●	●	Lower	N / A	Button 3	3x impulse
			Higher	N / A	Button 4	4x impulse
	○	○	Lower	Button 2	Button 4	4x impulse
			Higher	N / A	Button 1	1x impulse

Table 17: Configuration of functional buttons in Advanced function mode

Module must be restarted to use the new configuration of the functional buttons setting.

6.11 Disabling function

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

The *module disabling function* can be set at the second. The logic of the function is configurable. 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.

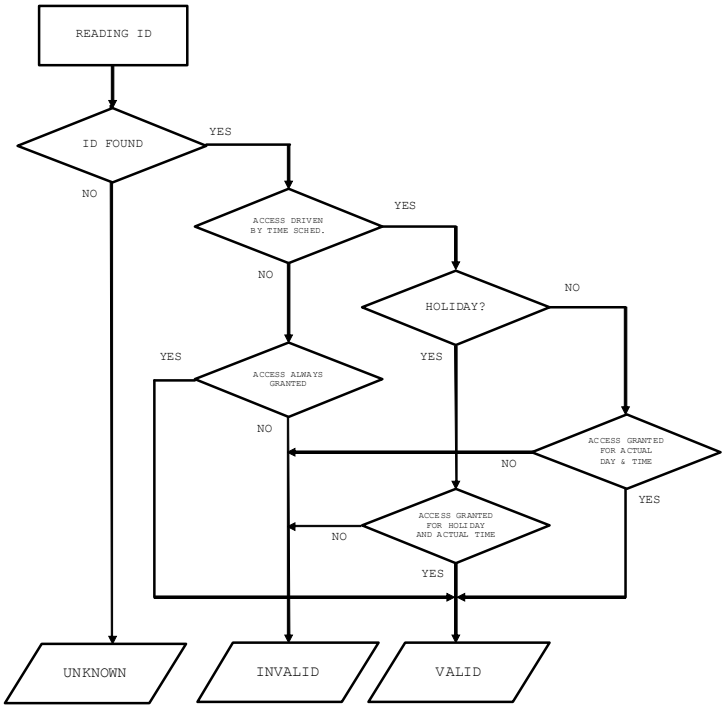
When using the module advanced function the module does not have an Input 2; therefore the disabling function is not usable in this configuration.

6.12 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. 4*.



Pic. 4: Simplified access rights evaluation

8 Useful links

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