MDEM 31

T&A terminal for APS mini Plus system

User's guide

techfass®

(Date of release: 2019/06/03, valid for FW version 5.10)

1 Content

2 Product description

The *MDEM 31* [1)] (T&A terminal with a 4'' display, an integrated 125 kHz RFID reader and a single door controller) is designed for to the RS 485 bus of the *APS mini Plus* access control system, or for standalone operation. Up to 32 MDEM 31 terminals can be connected to a single line of the APS mini Plus system. Number of lines is not limited.

The terminal is intended for mounting in the indoor environment.

Pic. 1: MDEM 31 terminal

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

3 Technical parameters

3.1 Product version

Product version	Product designation	Catalogue number	Module features [2)]		
			IP	TF	EM
	MDEM 31 – TF	53431000	✘	✓	✘
	MDEM 31 – EM	53431001	✘	✓	✓
	MDEM 31.IP – TF	53431100	✓	✓	✘
	MDEM 31.IP – EM	53431101	✓	✓	✓

Table 1: Product version

[2)] *IP* – IP version of the terminal with an Ethernet interface; *TF* –TECHFASS factory 125 kHz ID media reading; *EM* – 125 kHz ID media reading;

techfass®

3.2 Technical features

Functional properties	Supply voltage		8 ÷ 18 VDC
	Current demand	Typical	200 mA
		Maximal	350 mA
	Display		4'' LCD touch screen, 320x240 pixels, black & white
	ID technology, typical reading range	EM Marin	8 cm (with an ISO card)
	Real-time clock		Yes, with a min. 24 hrs backup
	Memory	Configuration card	Micro SD card
		IDs count	2.000 IDs
		Events	2.150
		Time schedules	64
	Inputs	1st input	Logical potential-free contact
		2nd input	Logical potential-free contact
	Outputs	Door lock	Relay NC/NO, 2A/24V
		Alarm	Transistor output 5V/5mA
		Output 3	OC for external reader buzzer control Reading synchronization – MASTER mode
	Signalization		2x LED 1x PIEZO
	Tamper protection	Ag. opening cover	Integrated micro-switch
	Communication interface		1x RS 485 – APS mini Plus BUS 1x RS 485 – AUX for future use 1x Ethernet (IP version only)
	Alternative data input/output		WIEGAND (configurable)

Table 2: Functional properties

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.

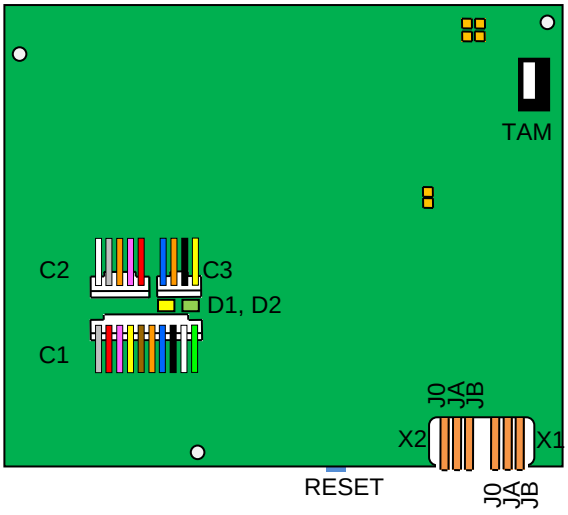
3.5 Mechanical design

Mechanical design	Weight	0,210 kg
	Operating temperature	-10 ÷ + 40 °C
	Humidity	Max 75%, non-condensing
	Cover	Plastic
	Environment	Indoor
	Color	Dark grey
	Dimensions	115x93x27 mm

Table 4: Mechanical design

4 Installation

4.1 Connectors and jumpers



Pic. 2: Rear part of the MDEM 31 terminal

Connectors and jumpers	C1	Connector C1 (10-core)
	C2	Connector C2 (5-core)
	C3	Ethernet connector (4-core)
	D1	Ethernet communication
	D2	Ethernet connection
	X1	RS 485 BUS jumpers
	X2	AUX jumpers (reserved)
	TAM	Tamper contact
	RESET	Reset button

Tab. 5: Connectors and jumpers

techfass®

4.1.1 Wiring and jumpers description

C1 cable wiring description		
	Grey	0 V
	Red	+8 ÷ +18 VDC power s.
	Pink	NO relay contact
	Yellow	NC relay contact
	Brown	IN 1
	Orange	IN 2
	Blue	C relay contact
	Black	RS 485 – A cable
	White	RS 485 – B cable
	Green	Output 3

Table 6: C1 cable wiring description

C2 cable		
	Grey	Aux RS 485 – A cable
	White	Aux RS 485 – B cable
	Orange	Alarm output
	Pink	WIEGAND data 0
	Red	WIEGAND data 1

Table 7: C2 cable wiring description

X1 jumpers		
	J0	Line terminator
	JA	Idle state definition (A)
	JB	Idle state definition (B)

Table 8: RS 485 BUS jumpers

X2 jumpers		
	J0	Reserved
	JA	Reserved
	JB	Reserved

Table 9: Auxiliary BUS jumpers

RESET		
	Short press	Module restart
	Press > 5 s	IP address reset

Table 10: RESET button function

4.2 Standard connection

Connection		
	Input 1	Door contact, active when door closed; REX button
	Input 2	Request to exit button or handle contact, active when button or handle pressed; Tamper; Disabling function
	Output 1	Door lock control (relay1)
	Alarm output	Low power transistor output (+5 V in any alarm state)

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. 8* is used when the door status contact is not installed and no Forced Door and Door Ajar alarms are triggered.

4.3 Installation instructions

The terminal 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.

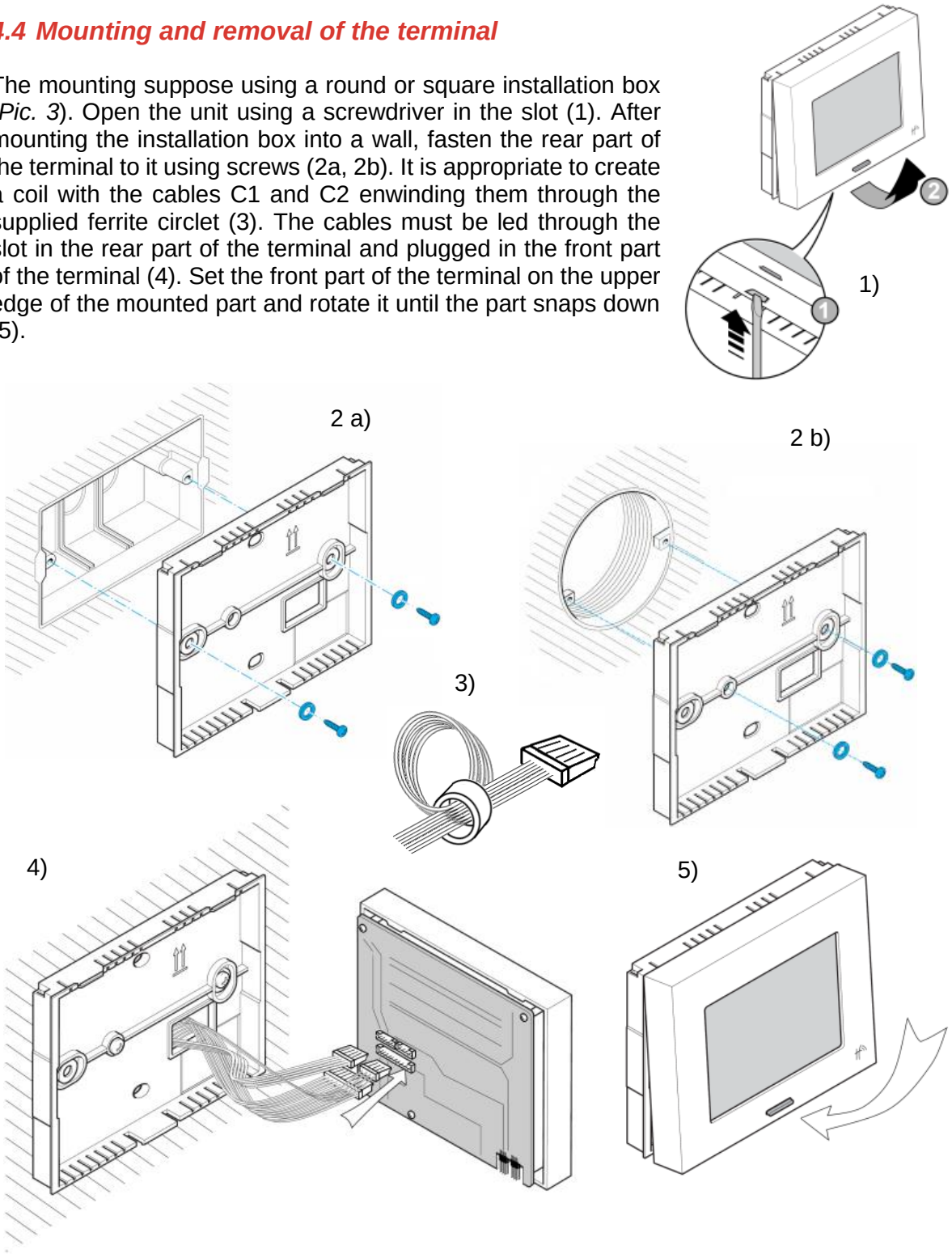
Radiated noise is transmitted through the air. It can be caused by computer monitors or other electrical equipment generating electromagnetic fields.

Consequently, a short distance between the reader modules or terminals themselves can cause reading malfunctions – for correct operation it is necessary to keep a minimum distance of 50 cm. Various metallic constructions may have 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.

4.4 Mounting and removal of the terminal

The mounting suppose using a round or square installation box (*Pic. 3*). Open the unit using a screwdriver in the slot (1). After mounting the installation box into a wall, fasten the rear part of the terminal to it using screws (2a, 2b). It is appropriate to create a coil with the cables C1 and C2 enwinding them through the supplied ferrite circlet (3). The cables must be led through the slot in the rear part of the terminal and plugged in the front part of the terminal (4). Set the front part of the terminal on the upper edge of the mounted part and rotate it until the part snaps down (5).



Pic. 3: Terminal mounting

The dismounting of the terminal is performed similarly. Open the unit using a screwdriver in the slot (1). Continue with an opposite procedure than performed when mounting the terminal.

5 Terminal functional properties and settings

5.1 Terminal control

Pic. 4: MDEM 31 terminal control

5.1.1 Display description

Display description	#	Symbol	Meaning
	1	–	No ID read
		?	Read ID is unknown
		⊗	Read ID is invalid
		↑	Read ID is valid
	2		less than 5 % of events buffer filled
			5 ÷ 30 % of events buffer filled
			30 ÷ 60 % of events buffer filled
			60 ÷ 90 % of events buffer filled
		blinking	over 90 % of events buffer filled, when the buffer is full the terminal deletes the oldest events in order to store the new ones
	3		Communication lost
	4	⚠ ? ⚠	Alarm status (according to its description)
	5		Door lock / input 2 (WIEGAND operating mode) status indication
	6	Day in a week in preset format	
	7	Date in preset format	
	8	Selected reason	
	9	Text description of the preset reason	
	10	Time in preset format	
	11	Arrows allowing movement among the reason icons	
	12	Area for entering configuration menu	
	BUT	Terminal functional button with LED signalization	

Table 12: Display description

5.1.2 BUT – functional button description

BUT button		
	Signalization	Red LED
		Green LED
	Press	Toggle help screen display

Table 13: BUT – functional button description

5.1.3 LED indicators

LEDs			
	Red	Continuous lit	Online operating mode via RS 485
		Blinking with 4 s period	Offline operating mode
		Fast switching with green	Address setting mode
	Green		ID media reading

Table 14: LED indicators description

techfass®

5.2 Factory defaults

Default factory parameters of TCP/IP interface are:

- IP address: *192.168.1.253*
- IP port: *10001*
- Password: *1234*
- Subnet mask: *255.255.255.0* *)
- Gateway IP address: *192.168.1.1* *)

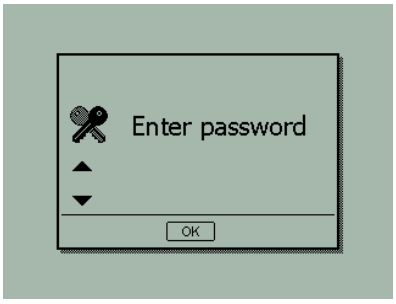
*) These settings are available only when configuring the device via telnet terminal.

These parameters can be set by pressing the *RESET* (*tab. 10*) button for *5 seconds period* or more. The exceeding of this period is signalized with a fast flashing of a LED. A shorter depression of the *RESET* button restarts the terminal and keeps its settings.

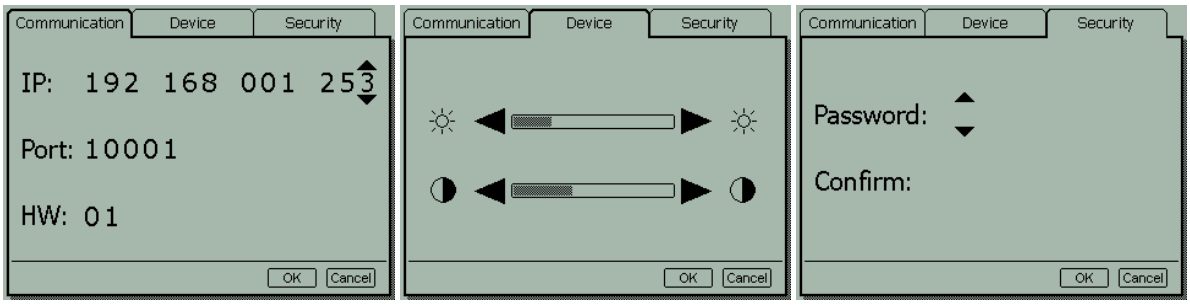
5.3 Configuring terminal from the configuration screen

To enter the *configuration screen* touch the terminal screen in *area 12* (see *pic. 4*) 5 times in a row. A *login dialog* will appear (*pic. 5*). Use the arrows to enter the password (for next character touch the empty space just next to the first character) and then press the *OK* button.

After entering the configuration screen you can change terminal communication, screen and security settings (*pic. 6a, b, c*).



Pic. 5: Configuration screen login



Pic. 6a, b, c: Communication, device and security settings from the configuration screen

5.3.1 Communication screen [3)]

[3)] TCP/IP settings are meaningful in *IP* versions of *MDEM 31* only.

At this tab of the configuration screen you can change the *IP address*, *IP port* and the *HW* address of the terminal. Use arrows to set desired values. After setting up all parameters, use the *OK* button to save the settings or the *Cancel* button to cancel all changes.

5.3.2 Device screen

At this tab of the configuration screen you can change *brightness* and *contrast* of the display. Use arrows to set desired intensity. After setting up all parameters, use the *OK* button to save the settings or the *Cancel* button to cancel all changes.

5.3.3 Security screen

At this tab of the configuration screen you can set up a *new configuration password*. Use arrows to set the password in the password and confirmation fields. After setting up the password, use the *OK* button to save the settings or the *Cancel* button to cancel all changes.

5.4 TCP/IP parameters setting via TELNET terminal [3)]

5.4.1 Changing terminal parameters

The *MDEM 31.IP* communication parameters setting can be also realized via *TELNET terminal* with a following procedure:

- Connect the *MDEM 31* to a *LAN* and connect a *power supply*.
- Run the command line with *cmd* command.
- Run the command *telnet IP_Address 9999* to access the *Converter setting* in a telnet terminal.
- Enter the *password* and press *Enter*.

For entering the device configuration menu you can also use one of the *APS mini Plus* programs. For detailed instruction, read the appropriate user's guide.

After a successful entering of the password, MAC address of the device and a settings menu will be displayed.

If you do not know the *IP address* of the termianl and you cannot use the *reset button* to set the default parameters, the *IP address* can be temporarily set for a single connection with this procedure:

- Insert a record into the *ARP table* with the command *arp –s IP_Address MAC Address*. *IP_Address* must be in the same subnet as your network interface, *MAC_Address* is printed in the module accessories.
- Run the command *telnet IP_Address 1* to insert the desired IP address into *ARP table* of the module (Telnet shows an error message after a while). This assignment is only temporary; you must set the *IP Address again* in next steps.

You can continue now with the procedure described above.

5.4.2 Changing IP address

You can change the *IP address* by selecting *1 Set IP*. A new address is entered by single bytes separated by the *Enter* key. If the entered value is out of allowed range, the byte is not changed. After inserting all of the address bytes the *final IP address* is displayed and you are returned back to the main menu.

5.4.3 Changing IP port

Changing an *IP port* is available after choosing the option *2 Set port*. If the entered value is out of allowed range, IP port is not changed. After a successful insertion the *IP port* is displayed and you are returned back to the main menu.

5.4.4 Changing the password

A change of the *password* is available after choosing the option *3 Set password*. You can use any alphanumerical string as a password, it can contain up to 9 characters. A blank password is not allowed. The password is saved by pressing the *Enter* key.

If a password is lost, the only solution to enable accessing the settings menu is resetting the terminal to its factory defaults.

5.4.5 Changing subnet mask

You can change the *subnet mask* by selecting *4 Set IP subnet mask*. A new subnet mask is entered by single bytes separated by the *Enter* key. If the entered value is not allowed, the subnet mask is not changed. After inserting all of the address bytes the *final subnet mask*is displayed and you are returned back to the main menu.

5.4.6 Changing gateway IP address

You can change the *gateway IP adress* by selecting *5 Set gateway IP*. A new address is entered by single bytes separated by the *Enter* key. If the entered value is out of allowed range, the byte is not changed. After inserting all of the address bytes the *final IP address* is displayed and you are returned back to the main menu.

5.4.7 Saving the settings

To *save the settings* choose the option *9 Save & Exit*. If you *do not want to save* the parameters, exit the settings menu by choosing *8 Exit without saving*.

5.5 Setting parameters of the terminal

5.5.1 Operational parameters

Operational 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 / external / 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
	Automatic summer time adjustment		YES / NO	YES
	Module advanced function		YES / NO	NO
	Release lock with REX button while tamper alarm active		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 15: Operational parameters

5.5.2 Operational parameters setting

Detailed instructions for setting terminal operational 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.

5.5.3 Display parameters setting

Detailed instructions for setting the display parameters are described in the individual configuration program *MDEM 31 Configuration Tool* user's guide available at the address http://www.techfass.cz/files/m_aps_miniplus_mdem31cfg_en.pdf.

techfass®

6 Terminal functioning

The terminal supports the following functions:

- Standard “Door Open” function.
- Door status monitoring.
- Exit-devices contact monitoring.
- Alarm output activated when any alarm condition occurs.
- Storing a code of pressed button with the read ID in events memory.

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).
- 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. 15*.

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. 15*. The door lock relay status remains unchanged until another “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 3 alarm states:

- Tamper alarm (against tearing-off the wall and opening a cover)
- Forced door alarm
- Door ajar alarm

Alarm state reporting is performed as follows:

- Via communication line.
- By acoustic signal (beeper).
- Activating the alarm output (AUX).

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

Two ways of acoustic signaling can be carried out:

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

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

If any *used* alarm state *(with setting of the acoustic alarm timer > 0)* occurs, the alarm output is activated. It can drive a low-input transistor relay which contact 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 opening the cover) the “Tamper” state is activated [4)].

[4)] The Tamper alarm contact and sensor are operational after their first change of status since switching on the module. There is no need to configure the module when the additional magnet is not installed.

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. 8*, the “Door Ajar“ alarm is activated.

6.3.4 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 terminal's memory when the terminal goes online.

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, 40 or 44 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 Terminal operating modes

6.6.1 Wiegand output

The terminal 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.

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

Table 16: 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 17*.

Wiegand	Input 1	Beeper control (0 V active)
	Input 2	Control of icon 4 at the display (see *tab. 4*, 0 V active)
	Output 1 (relay)	Tamper signaling; it follows the alarm state of tamper sensors (tamper signal = relay switched on) [3)]

Table 17: 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.

6.6.2 Wiegand input (external reader)

The terminal can be configured into a mode of controlling the door from both sides (*entry reader mode*) or into a mode, where the reading of IDs is provided by an external reader only (*external reader mode*).

In the *entry reader mode* an identification at an external reader connected via the *WIEGAND interface* acquires a *reason code 255*, the terminal own reader operates standardly, the reason codes are acquired according to a reason icon selected at the display.

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.

In the *external reader mode* the terminal own reader is disabled. The ID media reading is provided by an external reader, which is connected to the terminal with the *WIEGAND interface*. The code of the reason selected at the terminal display is assigned directly to the identification event raised at the external reader.

The acoustic signalization of the events raised at the external reader is announced directly at the external device itself – the signal for the beeper control is present at the cable 1 (see *tab. 6*).

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

6.7 Module advanced function

If the advanced function is selected, the door lock release is caused only when an ID medium is read at the entry reader. Reading an ID medium at the terminal embedded reader saves an event in the memory, but does not release the door lock.

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.

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.

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

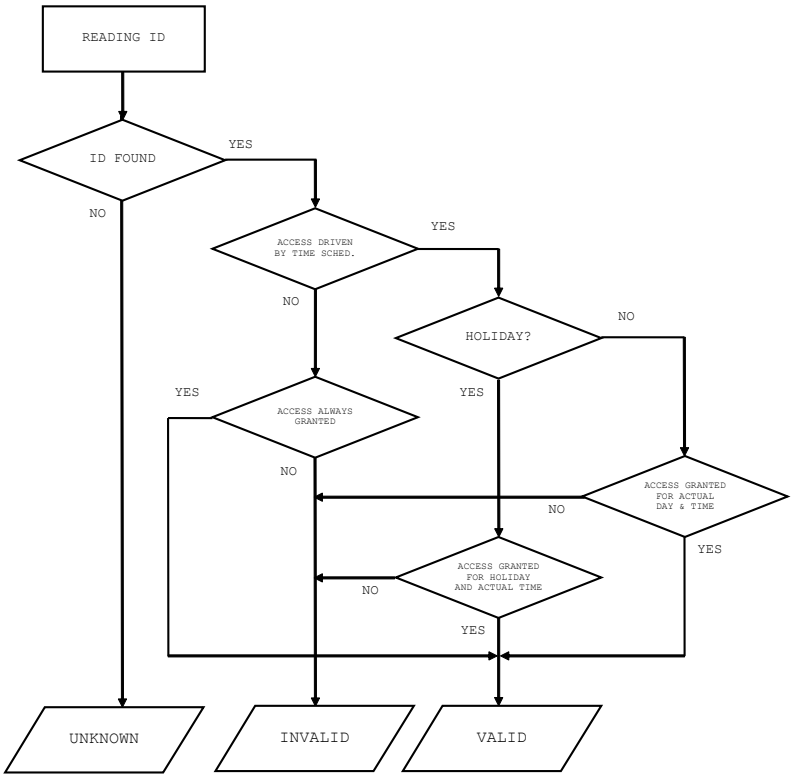
The disabling status changes and disabled actions are logged in the events archive.

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 *MASTER* mode. The *output 3* is used as the *synchronization signal*.

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.7*.



Pic. 7: 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