

MWGD 46XT

*APS mini Plus dual WIEGAND door controllers
supporting 4 APERIO wireless locks control*

User's guide



techfass®

1 Content

1	Content.....	2
2	Product description.....	3
2.1	MWGD 46XT door module.....	3
2.2	MWGD 46XT.IP door module.....	3
3	Technical parameters.....	4
3.1	Product version.....	4
3.2	Technical features.....	4
3.3	Mechanical design.....	5
4	Installation.....	5
4.1	Terminals and jumpers.....	5
4.2	Standard connection.....	6
4.3	LED Indicators.....	7
4.4	Installation instructions.....	7
5	Setting parameters of the door module.....	8
5.1	Configurable parameters.....	8
5.2	Door module parameters setting.....	8
5.3	Configuration of the connected reader keypad.....	9
5.4	HW address setting.....	9
5.5	TCP/IP parameters setting ⁵⁾	10
6	Door modules functioning.....	11
6.1	“Door Open” function description.....	11
6.2	Function permanent door lock release according to a time schedule.....	12
6.3	Alarm states.....	12
6.4	Standard operating modes.....	13
6.5	WIEGAND input data interpretation.....	13
6.6	Programming mode.....	14
6.7	Using the module with the APERIO wireless locks.....	14
6.8	ID expiration function.....	14
6.9	ID with Alarm flag function.....	14
6.10	Duress PIN.....	15
6.11	Disabling function.....	15
7	Useful links.....	15

2 Product description

The **MWGD 46XT**¹⁾ modules are designed for connection of *up to 4 APERIO* wireless locks and/or one or two readers, biometric sensors and similar devices with a **WIEGAND output** to the RS 485 bus of the **APS mini Plus** access control system, or for standalone operation. It is possible to connect up to 8 MWGD 46XT door modules to a single communication line of the APS mini Plus system, each occupying 4 successive addresses. These modules may be combined with other **APS mini Plus** reader modules on the communication line, however the total number of addresses on the line cannot exceed 32. In effect the number of lines is not limited.

The modules are designed for control of *up to 4 APERIO* wireless locks.

The modules are delivered inside a cover for DIN rail mounting.

2.1 MWGD 46XT door module

A module for general use (*Pic.1*). It is designed for control of up to **4 APERIO** wireless locks and/or for connection of one or two standard readers with Wiegand interface independent of the identification technology. So, various reader technologies (HID Proximity, iCLASS, Mifare, Mifare DesFire, Indala etc.) according to the needs of customers can be used in **APS mini Plus** access control system.



Pic. 1: MWGD 46XT

2.2 MWGD 46XT.IP door module

This module is functionally compatible with the previous one but in addition it is set by Ethernet interface for a direct connection to LAN using **TCP/IP protocol** (*Pic.2*). This door module can substitute the combination of MWGD 46XT and RS 485 / TCP/IP converter with price and installation benefit.



Pic. 2: MWGD 46XT.IP

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⁾	
			Attachable devices	IP
	MWGD 46XT	53446A00	4x APERIO wireless lock 2x reader with a standard WIEGAND output	✗
	MWGD 46XT.IP	53446B00		✓

Table 1: Product version

²⁾ IP – IP version of the module with an Ethernet interface

3.2 Technical features

Technical features	Supply voltage		8 ÷ 18 VDC
	Current demand	Typical	70 mA (140 mA – IP version)
Maximal		150 mA (230 mA – IP version)	
Real-time clock			Yes, with self backup for 12 hrs.
Memory	Cards		4x 748 ID, (2 programming cards) ³⁾
	Events		4x 1,440
	Time schedules		64
Inputs	Door status		4x Logical potential-free contact
	2 nd input		2x Logical potential-free contact
Outputs	Door lock		2x Relay NC/NO, 2A/24V
	Alarm		2x Relay NC/NO, 2A/24V
Indicators			LED indicators for communication and input/output status signaling on the PCB
Tamper protection			Terminals for external NC contact
APERIO locks interface			1x RS 485 for APERIO BUS
Reader interface			2x Wiegand, 2x LED, 2x PIEZO, 2x power supply terminals
Communication interface			1x RS 485 for system BUS 1x Ethernet (IP version only)

Table 2 Technical features

³⁾ The programming cards are not included, they must be ordered separately.

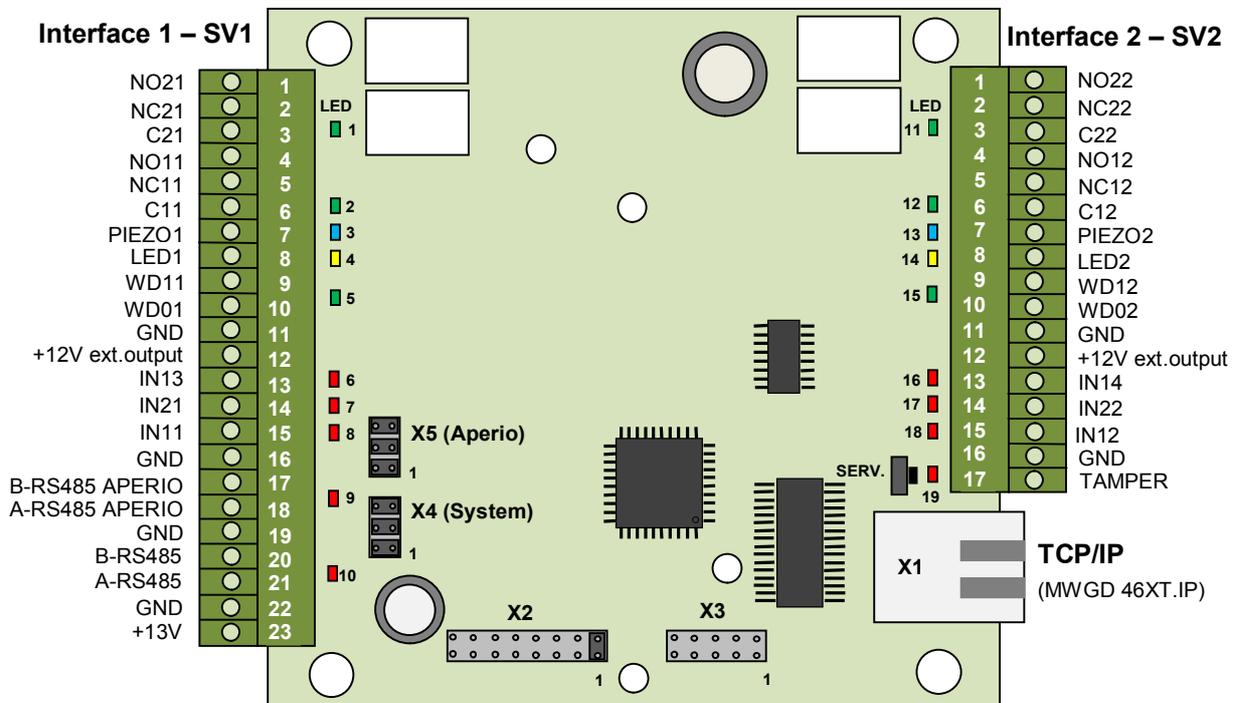
3.3 Mechanical design

Design	Weight	MWGD 46XT	0,218 kg
		MWGD 46XT.IP	0,225 kg
	Operating temperature		-10°C ÷ +40°C
	Humidity		Max. 75%, non-condensing
	Environment		Indoor
	Dimensions		6 DIN units, low profile

Table 3: Mechanical design

4 Installation

4.1 Terminals and jumpers



Pic. 3 Terminals and jumpers

Addr. X2	X2.1 ÷ 5	HW address (A0 ÷ A4)
	X2.6 ÷ 8	Reserved

Table 4: Address jumpers X2

X3	X3.1 ÷ 5	Factory use
-----------	----------	-------------

Table 5: Factory use connector X3

RS 485 X4, X5	X4(5).1	Idle state definition (B)
	X4(5).2	Idle state definition (A)
	X4(5).3	Line terminator

Table 6: Setting the RS 485 lines X4, X5

Terminal block SV1	1	Ad 1 - Relay2 NO	LED 1
	2	Ad 1 - Relay2 NC	
	3	Ad 1 - Relay2 C	
	4	Ad 1 - Relay1 NO	LED 2
	5	Ad 1 - Relay1 NC	
	6	Ad 1 - Relay1 C	
	7	Ad 1 - Beeper (reader)	LED 3
	8	Ad 1 - LED (reader)	LED 4
	9	Ad 1 - Wiegand DATA 1	LED 5
	10	Ad 1 - Wiegand DATA 0	
	11	0 V output	
	12	+8 ÷ 18 VDC external output	
	13	Ad 3 - Input 1	LED 6
	14	Ad 1 - Input 2	LED 7
	15	Ad 1 - Input 1	LED 8
	16	0 V	
	17	B wire – APERIO BUS	LED 9
	18	A wire – APERIO BUS	
	19	0 V	
	20	B wire RS 485	LED 10
	21	A wire RS 485	
	22	0 V power supply	
	23	+8 ÷ 18 VDC power supply	

Tab. 7: Terminal block SV1 and LEDs

Terminal block SV2	1	Ad 2 - Relay2 NO	LED 11
	2	Ad 2 - Relay2 NC	
	3	Ad 2 - Relay2 C	
	4	Ad 2 - Relay1 NO	LED 12
	5	Ad 2 - Relay1 NC	
	6	Ad 2 - Relay1 C	
	7	Ad 2 - Beeper (reader)	LED 13
	8	Ad 2 - LED (reader)	LED 14
	9	Ad 2 - Wiegand DATA 1	LED 15
	10	Ad 2 - Wiegand DATA 0	
	11	0 V output	
	12	+8 ÷ 18 VDC external output	
	13	Ad 4 - Input 1	LED 16
	14	Ad 2 - Input 2	LED 17
	15	Ad 2 - Input 1	LED 18
	16	0 V	
	17	TAMPER	

Tab. 8: Terminal block SV2 and LEDs

Service	1 short click	Address change (X2) confirmation	LED 19
	Press and hold >5 s	Reset of IP address to default	

Table 9: Service button

4.2 Standard connection

Std. connection	Address 1, 2	Input 1	Door contact, active when door closed
		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	Alarm status signaling (relay2)
	Address 3, 4	Input 1	Door contact, active when door closed

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 LED 19	Continuously lit	Online communication with a PC
		Flashing with 4s period	Offline operating mode
	Yellow LED 4 (14)	Continuously lit	Programming mode, PIN changing mode
		Flashing	Door lock relay release indication
	Red LED 10		RS 485 system bus communication
	Red LED 9		APERIO RS 485 bus communication
	Green LED 5 (15)		ID media reading from external reader or APERIO lock sensor
	Red LED 6,7,8 (16,17,18)		Activated inputs
	Green LED 1,2 (11,12)		Relays switched on
	Blue LED 3 (13)		Activated beepers (PIEZO1,2 outputs)

Table 11: LED indicators

Note: Yellow LED (4, 14) is intended optical signalization at connected reader.

4.4 Installation instructions

The door module is intended for DIN rail mounting into a switchboard or directly on the wall using the DIN rail enclosed.

5 Setting parameters of the door module

5.1 Configurable parameters

Configurable parameters	Parameter	Possible range	Default setting	
	Door lock release time ⁴⁾	0 ÷ 255 s	7 s	
	Door lock control setting ⁴⁾	Direct / reverse	Direct	
	Door lock relay function setting ⁴⁾	Standard / toggle	Standard	
	Permanent door lock release according to a time schedule ⁴⁾	Never / Schedule index	Never	
	Door lock status indication ⁴⁾	YES / NO	NO	
	Acoustic signal of door lock release ⁴⁾	YES / NO	YES	
	Door ajar time	0 ÷ 255 s	20 s	
	Second input configuration ⁴⁾	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	
	Automatic summer time adjustment ⁵⁾	YES / NO	YES	
	Saving events in the module's archive	Door opened	Enabled / Disabled	Enabled
		Door closed	Enabled / Disabled	Enabled
Input 2 On ⁴⁾		Enabled / Disabled	Enabled	
Input 2 Off ⁴⁾		Enabled / Disabled	Enabled	
Strike released ⁴⁾		Enabled / Disabled	Enabled	
	Strike closed ⁴⁾	Enabled / Disabled	Enabled	

Table 12: Configurable parameters

Stated settings do not affect timings of connected APERIO locks.

⁴⁾ These settings are meaningful only for first two addresses of the module.

⁵⁾ This setting is applied to all 4 addresses of the module.

5.2 Door module parameters setting

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

5.3 Configuration of the connected reader keypad

The door controller can accommodate either reader without keypad or keypad readers, the keypad type can be set by the configuration software. When a key press evaluation is required by the door controller, the keypad data transmission has to be configured as follows:

- One key buffering.
- Message length 4 bits.
- No parity.

The keypad setting determines interpretation of keys pressed at the reader. In the Reason keypad configuration a key is used for entering as a reason code; in the PIN keypad configuration keys are used for entering a PIN code; in the Code keypad configuration a valid identification can be performed by entering a valid access code.

The keyboard setting is meaningful only for first two addresses of the module.

5.4 HW address setting

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

When configuring the address jumpers it is necessary to keep in mind that the module occupies four successive addresses on system bus and X2 jumpers define the lower one. E.g., it is not possible to set the following module address to the value of the previous one + 1 - 3; the address conflict appears on system bus in this case.

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)

Confirmation of any address setting by clicking the service button on the PCB is required. If not the address change will be taken into account after the nearest disconnecting and connecting of the module supply voltage.

5.5 TCP/IP parameters setting ⁵⁾

⁵⁾ TCP/IP settings are meaningful in IP versions of MWGD 46XT only.

5.5.1 Factory defaults

Default factory parameters of TCP/IP interface are:

- IP address: *192.168.1.253*
- IP port: *10001*
- password: *1234*

These parameters can be set by depressing the *RESET* button for *5 seconds period* or more. The exceeding of this period is signaled with a fast flashing of a LED. A shorter depression of the *RESET* button restarts the converter and keeps its settings.

5.5.2 Changing converter parameters

The *MWGD46XT.IP* communication parameters setting can be realized via *TELNET terminal* with a following procedure:

- Connect the *MWGD 46XT.IP* 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 module 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 module 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.

5.5.3 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.

5.5.4 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.

5.5.5 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 converter to its factory defaults.

5.5.6 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*.

6 Door 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 (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. 12*.

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

Reading a programming card during door lock release will not cause the reader to enter the programming mode.
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 (disconnecting the external switch connected between TAMPER and GND terminals)
- 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 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 (TAMPER and GND terminals) the "Tamper" state is activated at all four addresses of the module.

The Tamper alarm contact 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 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 signalinging “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 input data interpretation

The WIEGAND input setting is meaningful only for first two addresses of the module.

6.5.1 Standard configuration

The module accepts the *WIEGAND* formats mentioned in the *table 14*. If the read signal is formatted otherwise, the data are not considered as valid and thus ignored. If another format of data is required to be considered as valid, it is necessary to set up the *User configuration* of the data read at the WIEGAND input. The table also shows the process used for individual width of read data.

Accepted formats	Read data width	Process	Resulting code width
	26 bits	Parity bits cut off (in front and at the back)	24 bits
	32 bits	Data bytes reversed	32 bits
	34 bits	Parity bits cut off (in front and at the back)	32 bits
	37 bits	Parity bits cut off (in front and at the back)	35 bits
	42 bits	Parity bits cut off (in front and at the back)	40 bits
	44 bits	Last 4 bits cut off	40 bits
	56 bits	Data bytes reversed	56 bits

Table 14: Accepted formats of read WIEGAND data– standard configuration

6.5.2 User configuration

The module offers an option to use the *user configuration of WIEGAND input interpretation*. By default the user configuration is not used. To enable user configuration, refer the *APS Reader* manual at http://www.techfass.cz/files/m_aps_miniplus_reader_en.pdf.

Note: User configuration *WIEGAND input* requires a deeper knowledge of the issue; we recommend leaving the setting to an installation company.

6.6 Programming mode

The module enters programming mode by reading one of the two *programming cards* (cards “+” and “-“) when the cards are enclosed (it concerns the kits supplied together with readers). The modules standardly come without programming cards, programming of the modules is performed with appropriate software, see

http://www.techfass.cz/aps_miniplus_sw_en.html.

Basic programming mode with programming cards is supported only.

6.7 Using the module with the APERIO wireless locks

The module enables connection of up to 4 *APERIO* wireless locks to the *RS 485 BUS* reserved for the APERIO communication. The locks are identified by their HW addresses at the APERIO BUS, the *MWGD 46XT* module expects locks with *addresses 1 - 4*. Since such lock is connected to the BUS, the controller opens communication with it immediately. The resources of the controller (access rights, events archive, etc.) are used for the lock with relevant address – the lowest address of the controller is linked with the APERIO lock with HW address 1, the highest address of the controller is linked with the APERIO lock with HW address 4.

Since the *APERIO* wireless lock is powered from a battery, it is “waked up” from a power saving mode (in which it standardly operates) only after an ID is read at its sensor, otherwise it saves battery and is not able to respond to the controller commands. Therefore the *APERIO* lock release can be performed only after a valid card is read at its sensor. The *remote door open function*, *permanent door lock release according to a time schedule function*, *door lock toggle function*, or the *module advanced function cannot be used with the APERIO lock* (the functions are bound to the controller lock relays only – only usable for 1 and 2 addresses of the controller)!

Reading a valid card at the *APERIO* lock sensor causes the release of the *APERIO* lock and furthermore the standard “*Door open*” function (according to the configuration) of the controller is performed at the relevant address. Reading an unknown or invalid card does not cause the lock release, the controller reaction is similar as when an unknown or invalid card is read at a connected WIEGAND reader.

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 is no longer valid. 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 Duress PIN

This function is implemented since the FW version 5.2.

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

6.11 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.

7 Useful links

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