XM3

Master Manual *XM3*
Advanced / Stand-alone

V2.0

May 2002

Important Notice

This manual is for use of authorized Cross Point OEM's only. It is intended to serve as an example user manual and as a guide to the functions of the *XM3*. Authorized Cross Point OEM clients may freely copy and edit the text and graphics contained in this document for including in their own documentation.

This manual describes all available procedures for the *XM3*. For specific markets, where the OEM client may not need all available options, it is recommended that those parts of the text which deal with unneeded options or operations be omitted, provided they are not made accessible to the end user or installer.

References to the "user" should be interpreted as "the user of the OEM's end product". Where reference is made to the *XM3*, the OEM should insert the product name under which the end product is marketed. Other *XM3* specific names like I/O1, I/O2, I/O3 and I/O4 may be changed to the names or numbers of the input and output ports used in the OEM's end product.

In the interest of improvement, specifications of the *XM3* may vary slightly due to updates being made. Detailed specifications of updates will be made available, to be incorporated in the OEM's manuals when necessary.

This document is subject to changes without prior notice. Cross Point cannot be held liable for the use of the provided information. In case of doubt please contact your supplier.

1   INTRODUCTION

THE STRUCTURE OF THIS DOCUMENT:

This document contains the following parts:

- Introduction.
- Getting started
- Remote programmer section
- Master card section (only for Stand-alone configuration)

1.1   Introduction

This manual is for use of authorized Cross Point OEM's only. It describes the full functionality of the stand-alone reader and the advanced reader. On-line basic is described in the *XM3* Quick Guide.

The two versions contain the following features:

XM3 Feature description	Software Configuration	
	Advanced	**Stand-Alone**
RS-485 Network Support	√	√
Dynamic Switching	√	√
Wiegand Interface	√	√
Magstripe Interface	√	√
Event Logging	√	√
Keypad options (PIN code, Access code, Alarm code)	√	√
User names (max 24 characters per name)	√	√
Time Zones	√	√
Anti passback	√	√
Support for remote programmers	√	√
Support for master cards		√
Printer support		√

Table 1. Overview of features.

On-line advanced:

- This is an on-line reader that has dynamic switch mode. So if the network is down the XM3 will switch to stand-alone mode and continue to operate.
- When the network is on again the XM3 will switch to network mode.
- The data that was picked up during network down can be read from the XM3 when on-line again.
- It is recommended to connect the power of the XM3 on a different power supply than the Computer or controller. This to prevent the XM3 from powering down when the network is down.
- When network is down the XM3 can be operated with a Remote programmer.

Stand-alone:

- This is a stand-alone reader which has the possibility for Event logging and Event printing
- The stand-alone XM3 can also be used in combination with a PIN keypad using PIN codes and other keypad options.
- The stand-alone XM3 can be switched to an on-line reader or an advanced reader.

The XM3 provides the basis for as well Stand-alone use as On-line use. Although technologically sophisticated, it is compact, quick and simple to use and flexible in operation. The XM3 applies proximity detection techniques to sense the presence of a unique RFID tag, as authorization to allow automatic opening or unlocking of a door, gate or other access.

Proximity detection has the advantage of not requiring physical contact between ID reader and ID-carrier. The tag functions without use of a battery. The ID Reader scans the ID-carrier by means of a Long Wave radio frequency transmission. If within range, the tag is activated and powered by this signal and in return transmits its specific ID number. This technique ensures easy to use, highly reliable, vandal proof access control.

The standard tags are available as cards, conforming to the ISO standard, or as small key tags which can be attached to key rings. The ISO card can optionally be equipped with a magnetic strip for dual ID applications. The tags used with the *XM3* have a laser-engraved number on the outside. Allowing up to billions of combinations, this ID number is unique for each tag.

When the *XM3* is installed, it first needs to be programmed. This is done at installer level. The anti-tamper led at the front is then disabled and all specific settings can be done. At user level the anti-tamper is active. The (end) user can decide to 'protect' the installation against unauthorized access by installer.

All tags must have their ID numbers *added* to the *XM3* meaning that they are read, and inserted into internal memory of the *XM3* before they can be used. Once added, the tag number will be held in memory until it is *voided* (erased). Memory management of tag numbers may be performed by means of so-called *Masters* (standard tags that have been "promoted" to perform certain management functions) or by using a *Remote Programmer* (a separate self-contained programming device with a built-in tag, capable of more advanced management functions).
Also a PC application (XM3 Manage) can be used for maintenance and configuration.

The internal memory of the *XM3* can hold up to 5000 tag numbers in its most simple configuration. In this manual referred to as MAX. MAX is dependent on the chosen file system configuration. This total must include at least three Masters and/or two Remote Programmers (typical one Program Master, One Add Master and one Void Master, and possibly one or two Remote Programmer for advanced functions. There is no maximum to the number of Masters and/or Remote Programmers, other than the MAX capacity.

1.2 Remote Programmer

A Remote Programmer allows a wider range of programming steps to be performed on an *XM3* than Master tags do. The general technique for using the Remote Programmer is similar to Program Masters, in that way too they are recognized by the *XM3* when held within reading range.

In fact, a Remote Programmer may be regarded as a Master that has a more extensive repertoire and is equipped with a numeric keyboard. When presented to the *XM3*, a unique code (also engraved as a number on the outside) is transmitted, in a similar fashion as with normal tags or Master tags. If the code is unknown to the *XM3*, the Remote Programmer is ignored. This offers security against unauthorized attempts to obtain access or to perform memory management operations. When a valid programmer is presented to the *XM3*, it will switch itself to Program mode. All LED's will turn off, except for LED number 7, the 'Program' LED.

1.3 XM3 version and card types

The XM3 card types are available in four versions. Within these versions there are 9 and 13 digits tag sorts available. In the following table an overview is given of this.

XM3 versions	13 digits	9 digits
EM only	EM 4001 and EM 4102	Cross Point
EM + HID	EM 4001 and EM 4102 HID Standard 26 Bit (H10302) HID Standard 34 Bit (H10306) HID Standard 37 Bit (H10302/H10304) HID corporate 1000	Cross Point
EM + Microchip	EM 4001 and EM 4102 Microchip MCRF 355/360	Cross Point
EM + Mifare	EM 4001 and EM 4102 Mifare standard	Cross Point

2   XM3 MANAGE

2.1   Introduction

Cross Point supports three ways of installing and programming the XM3. Users can use either Master cards, Remote Programmers or XM3 Manage, a MS-Windows based application. This section describes the configuration of the XM3 using XM3 Manage.

Amongst others, XM3 Manage offers you the possibility to:

- Maintain all system settings of an XM3
- Maintain the user database in the XM3
- Read the event log
- Save the user database and event log in extensible markup language files (.xml)
- Upload new software into the XM3

The XM3 is also able to interface with third party Access Control software. For this purpose, the Windows API-description is published in the XM3 Manage API manual. To interface directly with the XM3 without using the Windows API, a RS485 Protocol manual is available describing the API of the XM3 itself.

2.2   Connections

Pin	Color	Standalone	Magstripe (ABA)	Wiegand
1	Brown	Extra Ground		
2	Violet	Relay out [1]		
3	Black	Ground		
4	Red	Power +12V DC [2]		
5	Yellow	RS-485-B		
6	Blue	RS-485-B		
7	White	RS-485A		
8	Pink	RS-485A		
9	Grey	IO-1 Door-contact input [3]	\ RDP output	DATA 0
10	Green	IO-2 Ext. Night lock / Rex input [3]	\ RCP output	DATA 1
11	Grey / Pink	IO-3 Forced entry output [3]	\ CLS output	STROBE
12	Red / Blue	IO-4 Night lock enabled output [3]	\ Access input	\Access

Cable
- 12 wire E111235 AWM STYLE 2560 60°C 30V low voltage computer cable

[1] Solid state relay output is 1A/30VDC, open collector.
[2] Current is 40mA.
[3] Logically true, corresponds with 0V.
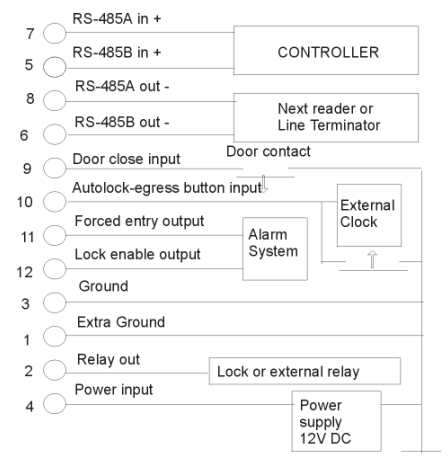
2.3   System requirements and Installation

XM3 Manage supports the following operating systems: Windows 98 2nd Edition, Windows ME, Windows NT 4.0, Windows 2000 and Windows XP Professional. The minimal hardware requirements are Pentium processor, minimal 32 MB RAM and 1 COM-port available.

XM3 Manage can be used to maintain a single XM3 or a RS485-network of XM3's. In a network, it is recommended to use twisted pair cable AWG-26 for the RS485 bus. The value of the resistors (R) to open and terminate the bus is 120 Ohm.

Up to 32 XM3 stand-alone units can be placed in a RS485 network. The XM3 Manage software can do maintenance on the XM3 units. All settings can be done and the user database can be downloaded from the connected PC.

Connector XM3	Name	Color
7	RS-485A in	White
8	RS-485A' out	Pink
5	RS-485B in	Yellow
6	RS-485B' out	Blue

Length = max. 1000m

n = max 32 stand-alone units
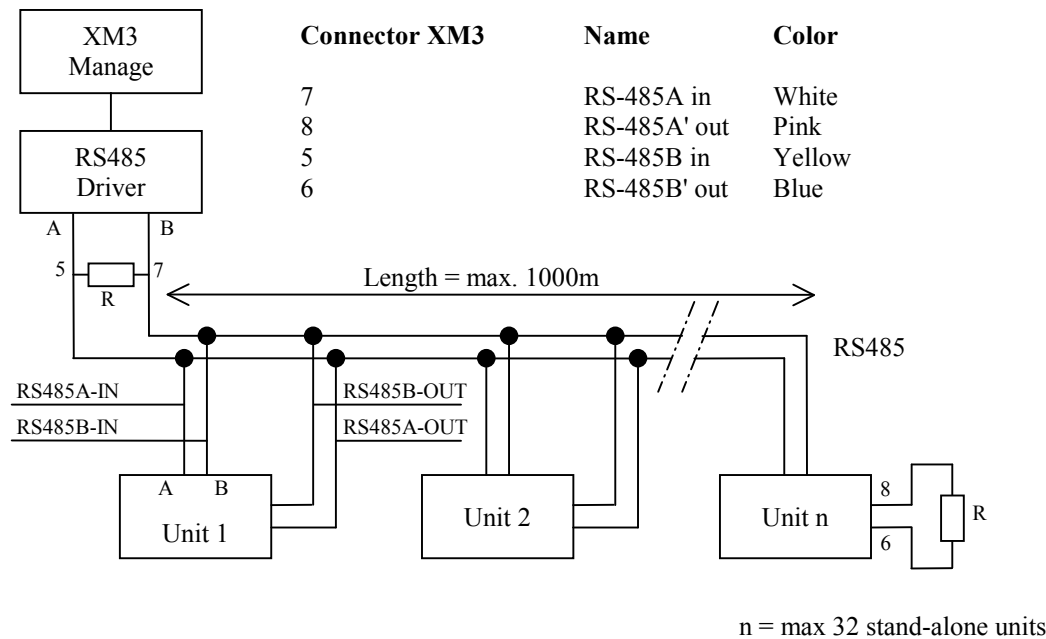
To connect the PC to the XM3 or network you need a RS484 to RS232 converter as supplied by Cross Point. The RS232-connector must be plugged into an available COM-port of the PC. Please note that you can either connect a PC to the network or a printer, but not at the same time.

To install XM3 Manage on the PC:
- Run setup.exe
- Select the language you want from the Choose Language dialogue.
- Follow the instructions on the screen to complete the installation.

If you want another language than the one you installed, it is necessary to remove XM3 Manage and install it again.

To start XM3 Manage navigate to the Cross Point entry in the start-menu and click XM3 Manage to start the program. Please note that for security reasons, XM3 Manage will automatically stop after a (configurable) period.

2.4   Getting started

When starting XM3 Manage, you first have to specify which communication port you have used to connect the XM3. If you plan to use this port, in future sessions check the checkbox. If checked, this dialog will not appear the next time you log in.
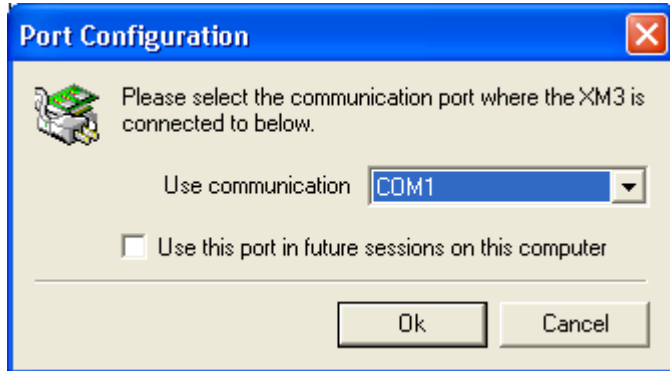
XM3 Manage continues to identify the XM3's connected to the specified COM-port. This may take a while. When all XM3's are identified you need to log in to the application.

You can log in as either installer or as end-user. Based on the type of user, different functionality will be enabled: for instance, an installer will be able to upload new software into an XM3 while this is not possible for an end-user. Also the XM3 configuration (on line basic, on-line advanced or stand-alone) will enable or disable functionality in XM3 Manage. Please note that this chapter will describe all functionality while not all functionality might be enabled. This depends on the log in level.

To log in, the following information must be provided:
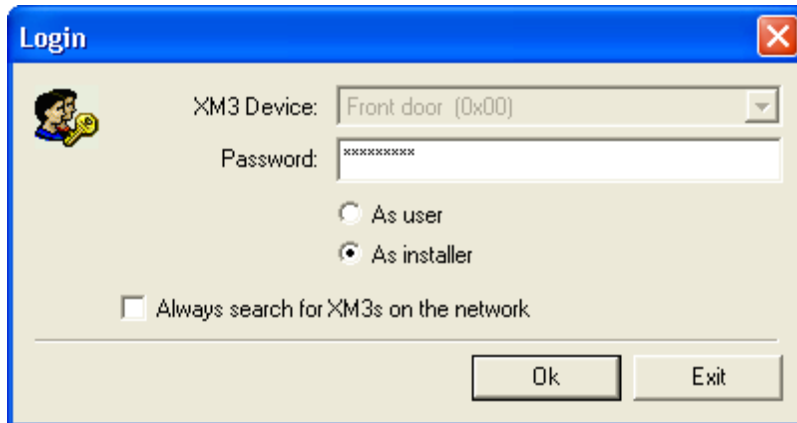
- XM3 Device: In case you have established a RS485-network of stand-alone XM3's, select the XM3 you want to log in to. You can only connect to one XM3 at a time.

- Password: Enter your password. The default passwords for both the installer and user are: 123456789. The password can be changed on the parameters-tab later on.

- Check the checkbox 'Always search for XM3's on the network' if you regularly connect new XM3's to the network.

When logged in, XM3 Manage presents 5 tabs with information. Each tab has a log off button. Use this button to switch between XM3's in your network. In the next sections each tab will be described.

2.5 Users

The users tab enables you to maintain the user database in the XM3. User databases can also be saved to or loaded from a file.
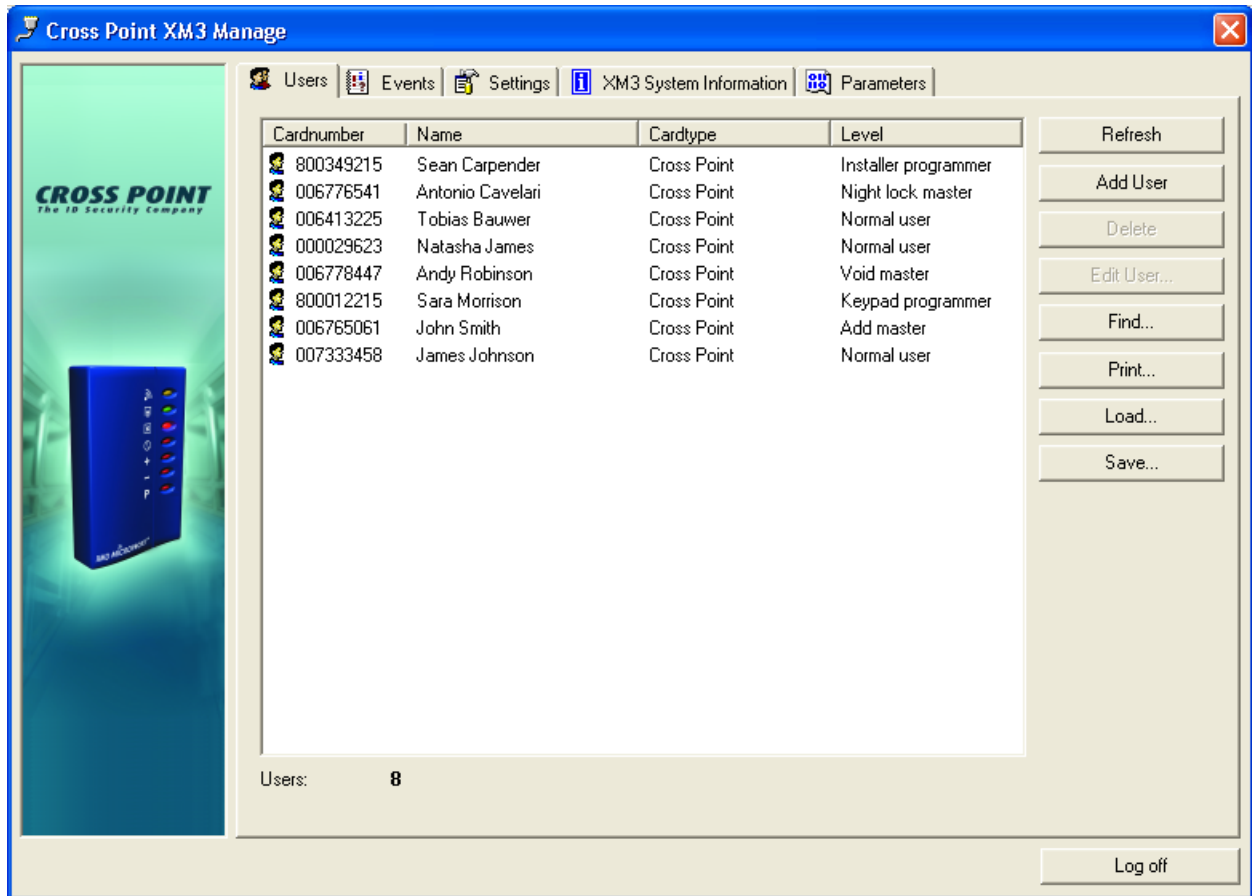
2.5.1 Refresh

To display an actual list of the users, click on the button Refresh.

2.5.2 Add User

To add a user, perform the following steps:
- Click the Add User button
- Enter the Tag ID
- Enter the Name
- Choose the level of the tag that has to be added. Levels are used to assign a tag specific functionality. Choose the functionality level of the card that has to be created.
- Choose the Card type. The Card type is the tag technology used. Note that the XM3 hardware must support the Card type you choose.

2.5.3 Delete User

To delete a user, select the user and click the Delete button. To delete more than one user at the same time, select all users that have to be deleted and click the Delete button.

2.5.4 Edit User

To edit a user, select the user and click the Edit User button. Alternatively double-click on the user. If a pincode is forgotten or the card is given to another user, the pincode can be reset by clicking the <Reset pincode> button. Now the user can define a new pincode.

2.5.5 Find

Use the Find button to find specific entries in the list.

2.5.6 Print

To receive an overview from the users in the users database, click on the button Print.

2.5.7 Load

Existing User databases stored in .xml files can also be loaded into the XM3. Click the Load button and choose the file to be loaded. Click Open to load the file and new users will be added to the XM3 user database.

2.5.8 Save

To save the user database click the Save button and choose the location where you want to store your file. User databases are stored in extensible markup language (.xml) file format. Any (ASCII) text editor or spreadsheet can read this file type.

2.6   Events

The Events tab displays all events logged in the XM3. Note that the XM3 must have Event logging enabled. Events can be saved to a .xml file using the Save button. The figure shows an event indicating that an unauthorized card was presented to the XM3.

Tip: Events can also be used to efficiently enter a large number of users. Use the following procedure:
- Present the cards to the XM3
- An event is generated for the unknown card, as displayed in the figure
- Double click the event. Using the arrow buttons, you can now navigate through the events.
- Click the Add user button to enter the user.

To prevent re-ordering of events during this procedure you might want to disable the parameter 'Event polling mode'.

Note that when event logging is configured as destructive read (see Event log options in the parameters tab), all events will be deleted after clicking the refresh button.
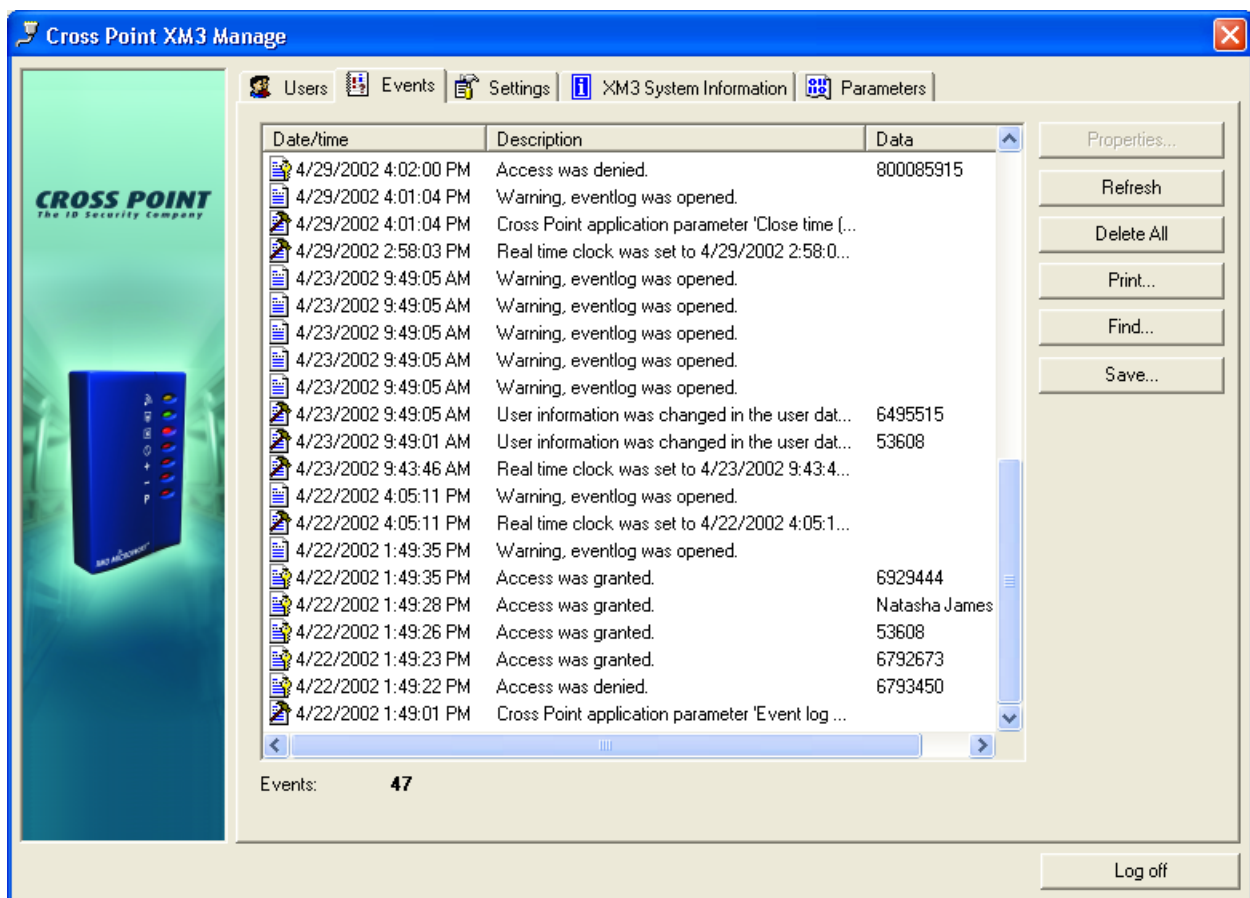
2.7   Settings

The settings tab provides general, hardware, network and file system information. Four buttons enable you to change the settings.

2.7.1   Synchronize date/time

The synchronize date/time button updates the XM3 date/time with the current date/time of the PC. Click the button to synchronize.

2.7.2 Change file system

Warning: changing the file system will result in the loss of all current information in the user and event databases of the XM3!

The file system determines how the internal memory in the XM3 is partitioned. You can configure the maximum number of users, PIN codes, names and events. By default, file system 11 is active. This allows the XM3 to store 1000 users, 1000 PIN codes, 1000 names and 500 events.

To change the file system:
- Select the new file system
- Click the Ok button
- Confirm the confirmation dialogue to make the change effective

2.7.3 Switch configuration

The XM3 supports an on-line, on line advanced and a stand-alone configuration. To switch between the different configurations you need a unique and XM3 specific switch key. Get into contact with Cross Point to obtain a switch key (See Appendix1).

2.7.4 Change address

To change the (network) address of an XM3 use the Change Address button. Except for the host address, any address between 0 and 255 can be selected.
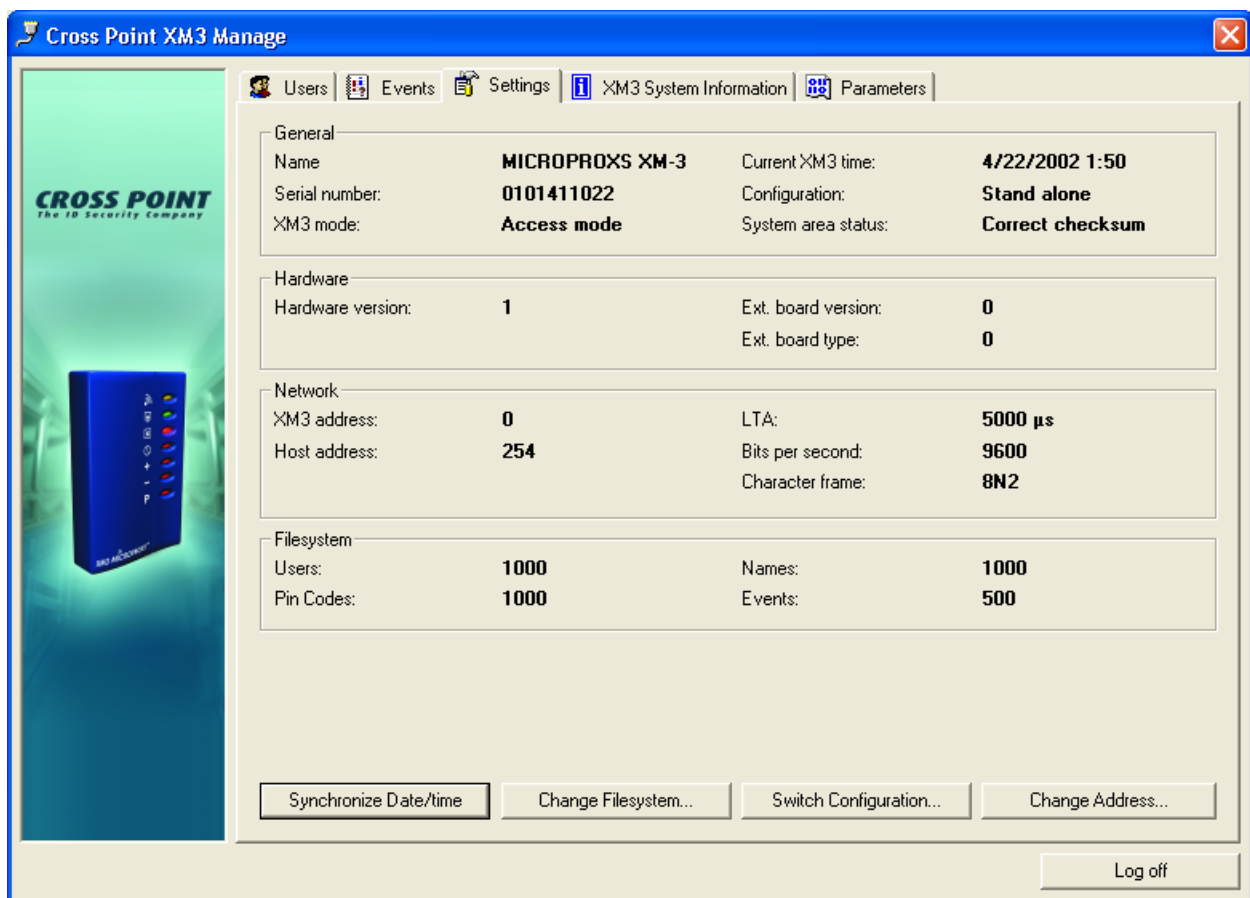
2.8   XM3 System Information

The XM3 system information tab provides details about the software versions loaded into the XM3. The software in the XM3 contains 3 layers: a bootloader, an operating system and an application. It is at any time possible to load other or newer operating systems or application software versions into the XM3. This functionality is only enabled when logged on as installer.

2.8.1   Upload new Operating System or Application

To upload a new Operating System (OS) or Application, you need a XM3<version>.os file and a XM3<version>.cpa file. These files are supplied by Cross Point. For convenience reasons it is recommended to store both files in the same directory. To upload a new Application, click on the <upload new CPA> button. The dialog 'Select CPA' is displayed. Navigate to the directory where the files have been stored and select the XM3<version>.cpa file. Click on the <open> button and follow the instructions on the screen. The CPA will be loaded into the XM3. After uploading the new software, the system is reset. Follow the same procedure to upload a new Operating System if necessary.
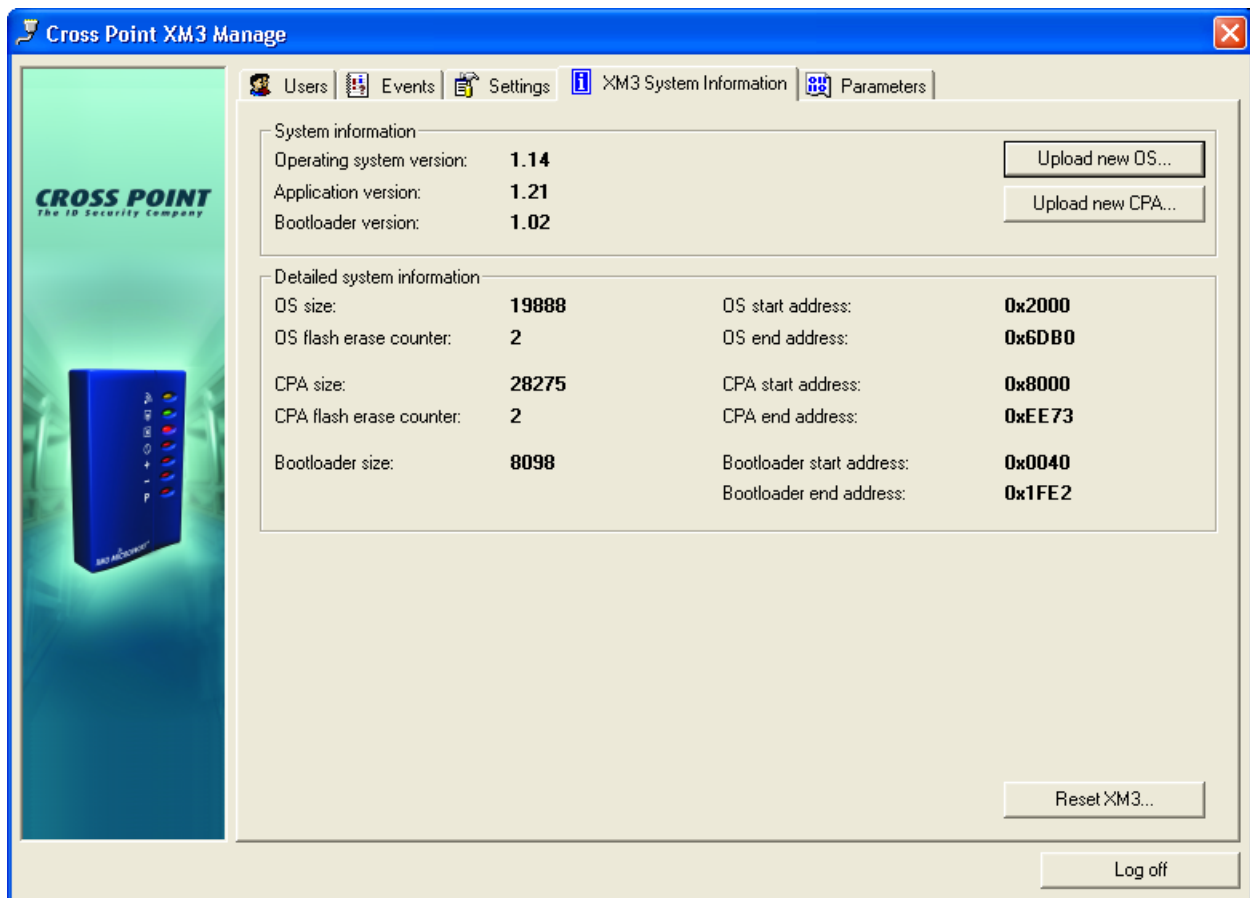
2.8.2   Reset XM3

This button resets the **XM3**. A reset is necessary if you have not performed a reset directly after uploading new software.

2.9 Parameters

The parameter tab allows you to maintain all parameter settings of a XM3. The parameters are called non-volatile parameter (NVP) because they reside in memory after a power reset of the XM3. Most parameters correspond to (*) commands as explained in the remote programmer section of this manual.
For this purpose after each parameter the (*) command is shown. For details on the behaviour of each parameter please refer to the corresponding section where the (*) command is described. Please note that the number of parameters will be different for an installer and a normal user. Also the software configuration (on-line basic, on-line advanced or stand-alone) influences the number of parameters.

All parameters are grouped as shown in the figure. Each parameter has a name and a value. To change a parameter:
- Navigate to the parameter.
- Click on the value. Dependent of the type of value, a select box appears or the value can be changed through editing the field. Change the value.
- Change any other values if applicable.
- To make the changes effective in the XM3 click the Apply button.

At any time, you can restore the default settings by clicking on the <default> button. Please note that the parameter Installer – Operational Mode is described in the corresponding section in the master manual 'Select XM3 operational mode'.

A few parameters do not correspond with (*) commands, but are settings of the XM3 Manage application. These parameters are grouped in XM3 Manage options. The parameters have the following functionality:
- User polling mode: the frequency used by XM3 Manage to update the list of users on the PC screen with the actual list of users in the XM3.
- Event polling mode: the frequency used by XM3 Manage to update the list of events on the PC screen with the actual list of events in the XM3.
- Auto log off: this setting prevents unauthorised use of XM3 Manage by closing down the XM3 manage application after the configured time of inactivity has expired.
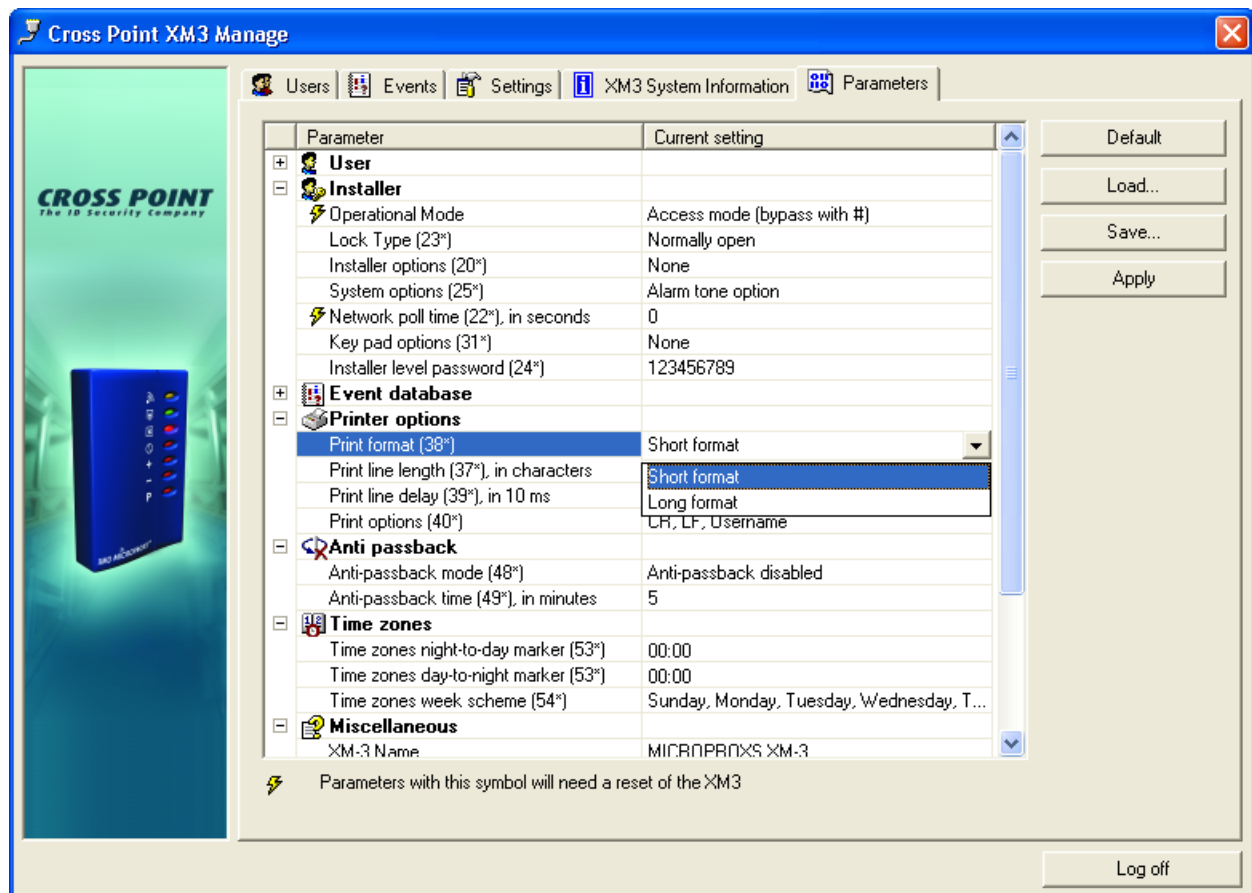
2.9.1   Example: Configuring time-zones

Using time zones, you can configure different access permissions based on the time of the day. Usually this feature is used as a daytime zone for most users and a night time zone for only some users. Time zones make use of the internal real-time clock of the XM3. All settings can be saved to a .xml file and be reloaded later. The settings can be reloaded to another XM3 as well.

- To configure time zones open the 'Time zones' group by clicking on the (+) sign.
- Click on the value field of the night-to-day marker
- Change the value in 08:00h
- Click on the value field of the day-to-night marker
- Change the value in 17:00h
- Now click on the time zones week scheme to specify for which days the time zones are valid. Deselect the days Sunday and Saturday.
- Click the Apply button to make the changes effective.

The daytime users now have access from 08:00h until 17:00h every weekday. On Saturday and Sunday, the XM3 stays in the last time zone, which is the night time zone.

Note: Night lock master cards can overrule time zones.
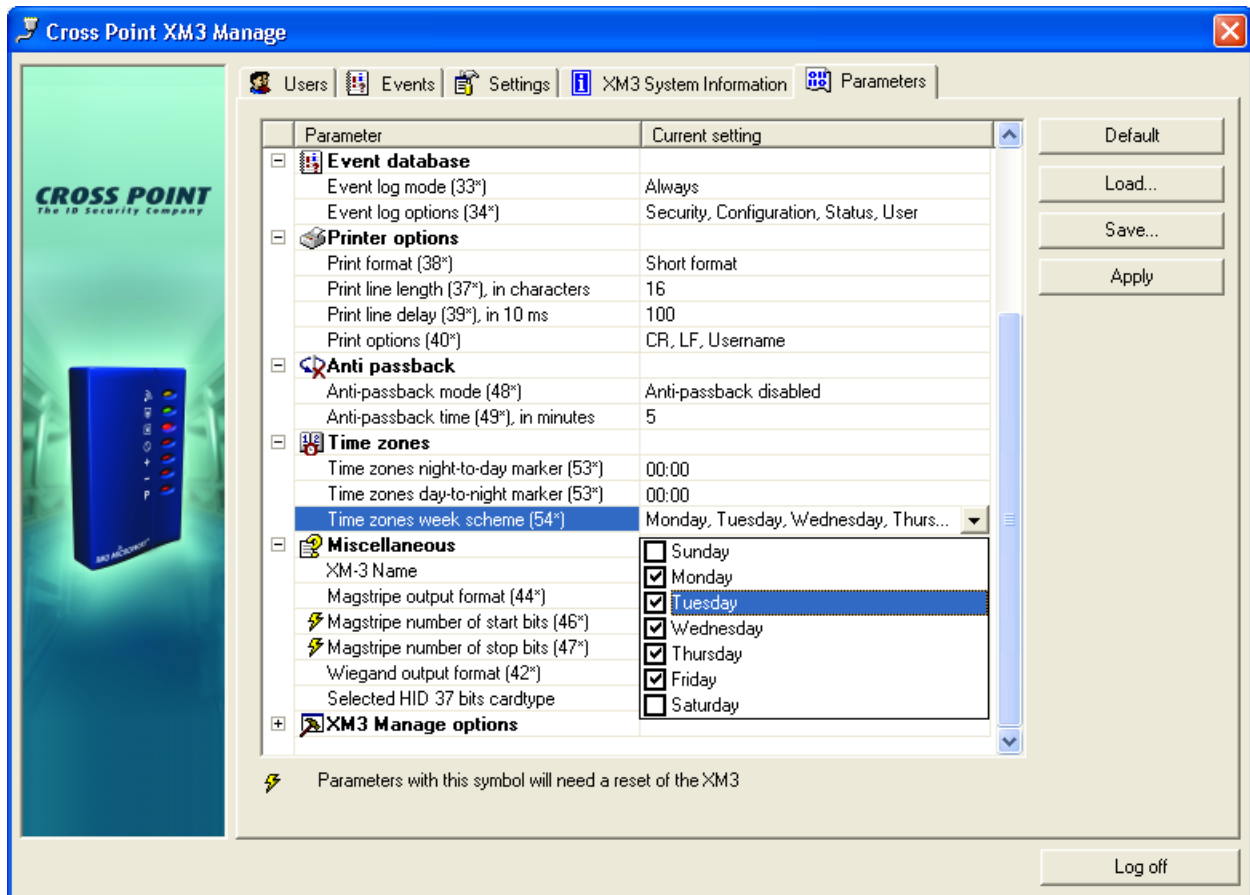
XM3

Remote Programmer Section

3   REMOTE PROGRAMMER FUNCTIONS

3.1   General

3.1.1   Operating

The Remote Programmer is operated within reading range of the **XM3**, by typing one or two digit numbers on the Remote Programmer keyboard, using the Enter key (*) for punctuation, and the Backspace key (#) for correcting typing errors. With option 10*4* on, LED 1 (yellow) is used to indicate that the Remote Programmer is within reading range as is the case with a normal tag.

The Remote Programmer should be presented and held in a stable position, where all LED's on the **XM3** are visible, for example next to the reader.

Enter key   Backspace key
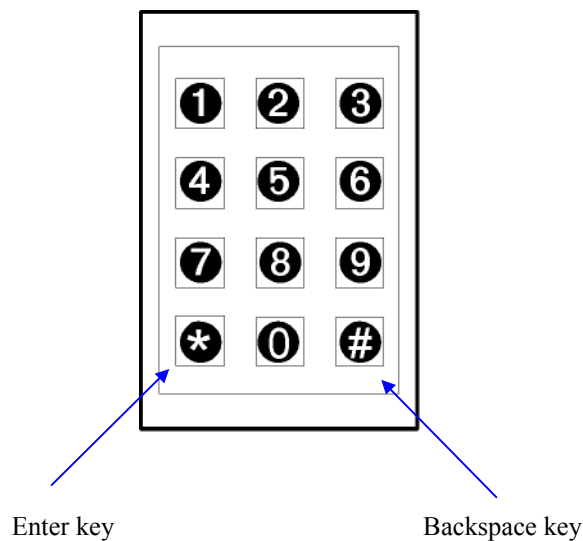
While the **XM3** is in Program mode, it will sound a short beep at each numeric key press. Pressing the Enter (*) key will cause the **XM3** to execute the chosen function, as determined by preceding numeric key presses, and to display the resulting status with its LED's.
In some cases where operation or programming caused an error, the system can be bypassed, i.e. power off the system, hold the programmer (known or unknown) in the field while powering on. The **XM3** will go in Program mode. Make sure that when doing this the tamper contact at the back of the **XM3** is not covered.

A complete remote programming step is for example:

1. Set Program mode, keeping the Remote Programmer in reading range

2. Type the program number on the keyboard. Possible leading zeros (white keys) can be omitted.

3. LED(s) light up to show the chosen function

The chosen program is executed.

Once a Remote Programmer function is completed, the *XM3* usually returns to normal operation.
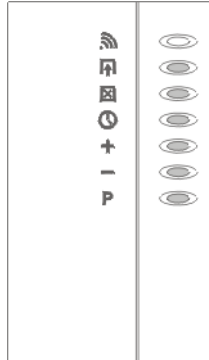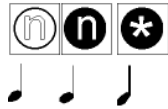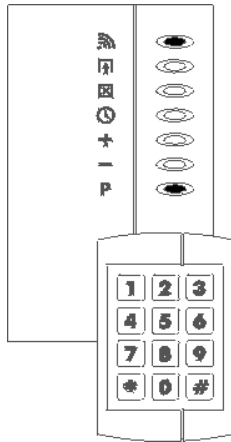
A program may involve several steps, each with key presses, LED readouts, and/or presenting of tags.
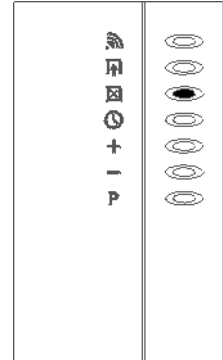
Outputs: inactive
Inputs: inactive

If several different functions must be performed consecutively, the user can leave the Remote Programmer within range and switch the *XM3* back to Program mode by pressing (*) or (#). Alternatively, the Remote Programmer can be moved out of reading range and then back into reading range to return to Program mode.

Remarks:
- When a number has to be entered starting with one or more zeros, the leading zeros can be omitted.

3.1.2   Different Operating Modes overview

For security reasons the XM3 has two operating modes. These are **Installer level** and **User level** operating modes.
Table 1 gives for every command the actions that are allowed for each operation mode. Refer to the table of contents to find the page where the codes are explained.

Code	Description	Installer programmer		User Programmer
		Installer level	**User level**	**User level**
1*	Access with remote programmer	Yes	No	Yes
2*	Add tags with remote programmer	Yes	No	Yes
3*	Toggle the night lock mode	Yes	Yes	Yes
4*	Add tags by presenting tags	Yes	No	Yes
5*	Void tags by presenting tags	Yes	Yes	Yes
6*	Set clock time and date	Yes	No	Yes
7*	Add special user tags	Yes	No	Yes
8*	Add night lock tags only	Yes	No	Yes
9*	Void tags with remote programmer	Yes	Yes	Yes
10*1*	Set protection option	Yes	Yes	Yes
10*4*	Set read indication option	Yes	Yes	Yes
10*5*	Set read and protect option	Yes	Yes	Yes
10*n*	Combination of user options	Yes	Yes	Yes
11*	Set open time	Yes	Yes	Yes
12*	Set close time	Yes	Yes	Yes
13*	Add night lock	Yes	No	Yes

14*	Add Add master	Yes	No	Yes
15*	Add void master	Yes	Yes	Yes
16*	Copy remote programmer	Yes	Yes	Yes
17*	Set inactivity time out	Yes	Yes	Yes
18*0*	Set PIN code change code	Yes	Yes	Yes
18*1*	Set general access code	Yes	Yes	Yes
18*2*	Set general alarm code	Yes	Yes	Yes
18*n*	Combination of Keypad options	Yes	Yes	Yes
19*	Set password to access XM3 via RS-485 at user level	Yes	No	Yes
20*1*	Set private Option	Yes	Yes	No
20*2*	Set public option	Yes	Yes	No
20*4*	Enable egress button	Yes	Yes	No
20*n*	Combination of options	Yes	Yes	No
22*	Set RS-485 polling time	Yes	Yes	No
23*0*	Set lock normally open	Yes	Yes	No
23*1*	Set lock normally closed	Yes	Yes	No
23*2*	Set lock coded signal	Yes	Yes	No
24*	Set password to access XM3 via RS-485 at installer level	Yes	Yes	No
25*1*	Override open time with night lock master	Yes	Yes	No
25*4*	Change alarm tone	Yes	Yes	No
25*8*	Redirect tamper alarm output to night lock enabled output	Yes	Yes	No
25*16*	Tamper off option	Yes	Yes	No
25*32*	Fixed frequency	Yes	Yes	No
25*n*	Combination of installer options	Yes	Yes	No
26*	Set file system configuration	Yes	Yes	No
27*	Switch to RS-485 network mode or stand-alone mode	Yes	Yes	No
28*	Set XM3 network address	Yes	Yes	No
29*	Display SNR of reception signal	Yes	Yes	No
30*	Add a keypad (XRP-2K)	Yes	Yes	No
31*1*	Enable keypad sabotage signal	Yes	Yes	No
31*2*	Enable PIN code option	Yes	Yes	No
31*4*	Use keypad as user remote prog.	Yes	Yes	No
31*8*	Set PIN code ' at night only	Yes	Yes	No
31*nn*	Combination of PIN keypad options	Yes	Yes	No
33*	Set event log mode	Yes	Yes	No
34*	Set events to be logged	Yes	Yes	No
35*	Erase all events in event log	Yes	Yes	No
37*	Set print line length	Yes	Yes	No
38*	Set print format	Yes	Yes	No
39*	Set print delay	Yes	Yes	No
40*	Set print options	Yes	Yes	No
42*0*	HID standard 26 bit	Yes	No	No
42*1*	HID standard 34 bit	Yes	No	No
42*2*	HID standard 37 bit	Yes	No	No
42*3*	HID corporate 1000 35 bit	Yes	No	No
42*4*	Cross Point 42 bit	Yes	No	No
42*5*	Cross Point 46 bit	Yes	No	No
44*0*	Standard 9 digit format	Yes	No	No
44*1*	Cross Point 13 digit format	Yes	No	No
44*2*	Cross Point 14 digit format	Yes	No	No
45*	HID card type 37 bits	Yes	No	No
46*X*	Start bits (max 8)	Yes	No	No
47*Y*	Stop bits (max 8)	Yes	No	No

48*M*	Set anti-passback mode	Yes	Yes	No
49*T*	Set anti-passback	Yes	Yes	No
50*	Set print mode	Yes	Yes	Yes
51*	Set user name	Yes	Yes	Yes
53*TZ*TM*	Set day-night time	Yes	Yes	Yes
54*(N*N*N*)9*	Change time for a weekday	Yes	Yes	Yes
58*	Re-enable users	No	No	Yes
93*	Show operation level	Yes	Yes	Yes
94*	Show programmer level	Yes	Yes	Yes
95*	Display application version	Yes	Yes	Yes
98*	Perform self test	Yes	Yes	Yes
99*nn*	Erase all tags from level 'nn' downwards	Yes	Yes	Yes

Table 1.

3.2   XM3 LED Indicators

The *XM3* is provided with seven LED's which serve as status indicators.

Led 1 (yellow) Read indicator
Led 2 (Green) Access
Led 3 (Red)   Closed
Led 4 (Red)   Night Lock
Led 5 (Red)   Add
Led 6 (Red)   Void
Led 7 (Red)   Program
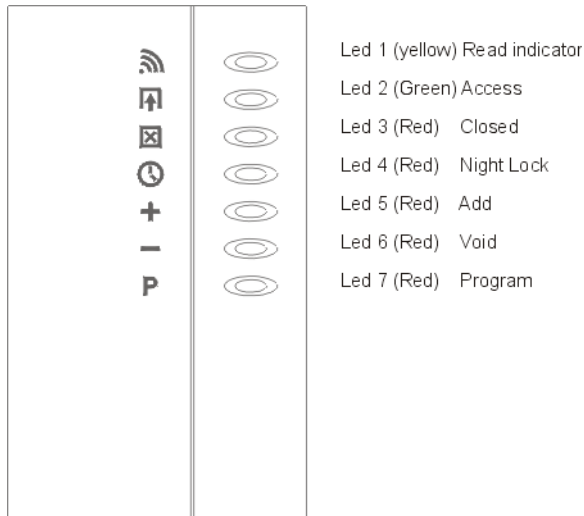
This manual describes the *XM3* procedures step by step, showing the LED readout after each step. The status of each LED can be either on, off, blinking, or unknown (on or off, depending on the situation), as follows:

Off   On   Unknown

The order of LED indicators is as follows:

LED1	Read	On when a tag or Programmer is within reading range, and being identified
LED2	Open	On when door or gate is unlocked
LED3	Closed	Indicates Access mode. On when door or gate is locked
LED4	Night Lock	Night Lock mode
LED5	Add	Add mode
LED6	Void	Void mode
LED7	Program	Program mode: when a Program Master or Remote Programmer is presented

Sound:

In addition to the LED display, the *XM3* provides feedback by means off sounds:

A short beep (for example when a tag is read),

A long beep (to indicate recognition of a Master tag).

Or a few short beeps (in case of error)

Alarm beep (tamper alarm)

3.3   Wake-up

When powering up the *XM3* from Sleep mode, a Remote Programmer must be presented. This Programmer will be added at the level at which the *XM3* was put to sleep mode.

At Wake-up all LED's of the *XM3* are on, except for one LED which indicates the specific level it was set to. Below the possible level display of LED 1-7 on Wake-up are shown:

Sleep mode	Led 1-7	Sleep mode	Led 1-7
Level 1: Designate Installer Programmer		Level 0: Designate User Programmer	

Wake-up operation:

1. Power on

2. Designate Remote Programmer at specific level

3. Access mode
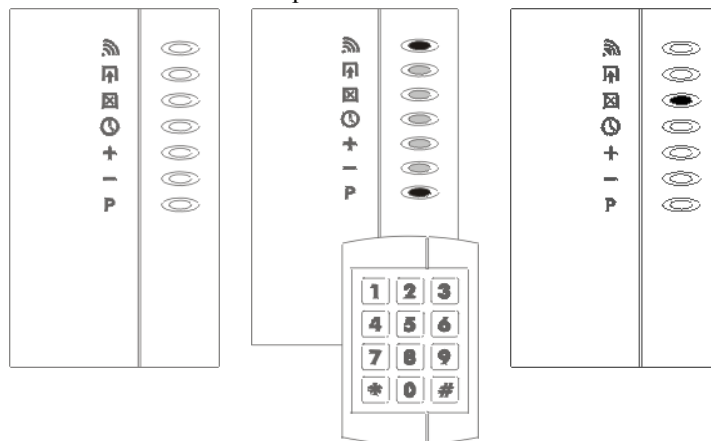
Remarks:
- Any new Remote Programmer will be accepted. Its unique code will be memorized.
- Remote Programmers, that are already present in memory, are accepted only if they have been set at the same level.
- In case of a mistake in the level setting, the Wake-up mode can be bypassed by presenting any added Remote Programmer during power up. After that the *XM3* will immediately enter Program mode.
- If the wrong Remote Programmer is presented, memorizing the correct Remote Programmer and using this to void the unwanted one can change it.
- Where several *XM3* units are in use for easier management and better security, one and the same Remote Programmer can be employed on all installations, as long as they are on the same level.
- Label the Remote Programmer with its level to avoid mistakes.
- Record the number of the Remote Programmer and its level. In case of loss the Remote Programmer can be voided from memory by number, by using another Remote Programmer.
- When waking up from installer level, only a Remote Programmer is accepted (no proximity cards).
- When waking op from user level, both a Remote Programmer and a Proximity Card are accepted. The card will become a Program Master.

Possible errors:

- A Remote Programmer is not added to memory; after the error tone the *XM3* returns to Wake-up mode. The Programmer number is present in memory, but at a different level. Apply another Remote Programmer. If a mistake was made when setting Sleep mode, a bypass of this mode can be performed by re-powering the *XM3* while presenting the Remote Programmer. Note: the tamper at the back of the *XM3* must be uncovered. As mentioned above, special attention must be taken when doing so, since the bypass cannot be undone.

- If the *XM3* indicates Access or Night Lock mode from the start, and returns errors on presentation of tags or Programmers, the unit was not set to Sleep mode on power-up. Most likely a Remote Programmer was already added. Check whether any Remote Programmer was supplied with the *XM3*. If not, no memory management is possible; please contact your supplier.

NOTE:

For waking up with the use of a master card see chapter 'Master cards'.

3.4   Tag level overview

In table 2 the different tag levels are shown:

Nn	Tag levels	
11	Installer Programmer	
10	User Programmer, Program Master	
9	Void Master	
8	Add Master	
7	Night lock Master	
6	PIN keypad	
3-5	Undefined	
2	Status III tags	Night lock only
1	Status II tags	Normal and Night lock ('Special' users)
0	Status I tags	Normal users

Table 2.

Levels are used to assign a tag specific functionality.

4   SOFTWARE CONFIGURATION SWITCHING

The XM3 is available in 3 different configurations.

- **Basic**: On-line configuration with limited functionality (Network mode only, EM technology)
- **Advanced**: On-line configuration with full functionality (Network mode + Dynamic switching)
- **Stand-alone**: Configuration in which *XM3* has local access rights (Stand-alone operation + Optional printer)

It is possible to switch the *XM3* configuration from Basic to either Advanced or Stand-alone or from Advanced to Stand-alone. Switching from Stand-alone to either advanced or basic is considered not to be done, because the stand-alone version contains full functionality and can be set online and advanced.

To switch to a different configuration a switch key is necessary. To receive such a key the '*XM3* Configuration Switch Form', see paragraph 17.1, must be filled in and send to Cross Point.

The required information for this form is:

- XM3 unique serial number.
- XM3 hardware version.
- Extension board type (if present).
- Extension board version (if present).
- Bootloader version.
- Operating system version.
- Cross Point application version (in some cases custom version).
- Current software configuration.
- Wanted software configuration.
- Description of XM3 usage.

This information can be retrieved from XM Manage under the tabs 'settings' and 'information'.

The information can also be retrieved from the XM3 with a remote programmer. The programmer can be at Installer level or User level. See the next chapters for retrieving the information using a remote programmer.

4.1   Retrieve system info

This function retrieves the system info. The info is also displayed in XM3 Manage.

Retrieve system info:

1. Program mode
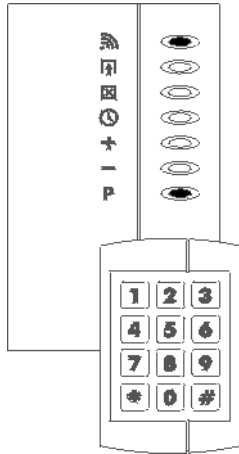
2. Retrieve system info:

3. LED's show system info:
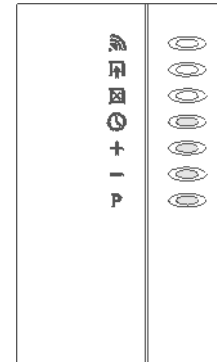
4. Show next digit:

5. Resume normal operation:
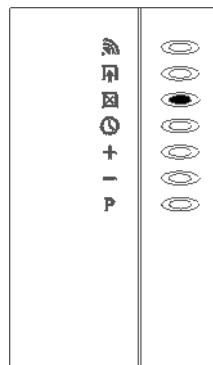
N= number of item for which information must be displayed.

0 = Serial number (10 digits)
1 = Hardware version (3 digits)
2 = Extension board type (3 digits)
3 = Extension board version (3 digits)
4 = Bootloader version (5 digits)
5 = OS version (5 digits)
6 = CPA version (5 digits)
7 = Current software configuration (3 digits)

All items are displayed in binary code (BCD) format on the lowest 4 LED's of the XM3. Numbers are displayed using one BCD digit at the time. The XM3 will show one digit at a time. The (*) key on the remote programmer can be used to force displaying the next digit. With each digit the green LED will toggle (on/off) and a short beep will be generated. Pressing the (*) key after the last digit is shown the XM3 will return to its normal mode.

Table 1 shows the LED value in BCD format and the conversion to decimal numbers.

Table 1: BCD converted into Decimal.

EXAMPLE

This is Number: 0301361004

Remarks:
- This option can be executed from both levels and both Remote programmers.

With this information Cross Point can determine whether the requested configuration switch is possible with the current software in the *XM3*.

When all information is correct, Cross Point will give a 'key' which has to be used to change the software configuration.

The key for the new software configuration is a 10-digit decimal number.

After the reset is completed the user can verify the new software configuration with the (95*7*) option.

Remarks:
- Both a software configuration identifier and a key are required.
- For security reasons the software configuration feature will be disabled after 3 consecutive invalid keys. The *XM3* will have to be powered down before software configuration can be switched again.

The software configuration can also be done using *XM3* Manage. For the procedure see the *XM3* Manage manual.

5 OPERATIONAL FUNCTIONS

To provide for using a single Master or Remote Programmer at the same level on different *XM3* units, the *XM3* must be specially prepared before shipment. When such a unit is powered up, the first tag or Programmer presented will be set to the level the *XM3* was set to before shipment, obtaining a superior status to tags and Programmers that are added later.

5.1 Set operation level; set to sleep mode (0*)

Show and/or set operation level:

1. Program mode   2.   3. Show current level
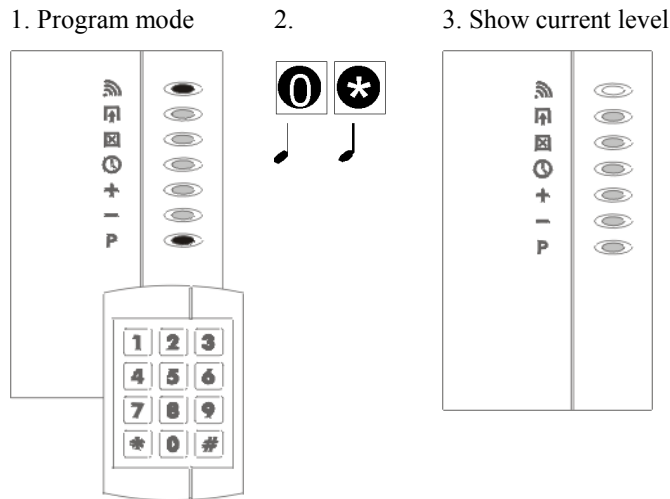
To set a new level prior to entering Sleep mode:

4. Set new level '0' or '1'   5. Level shown   6. Go to sleep mode
                                                       < Power off>

User level

OR

Installer level
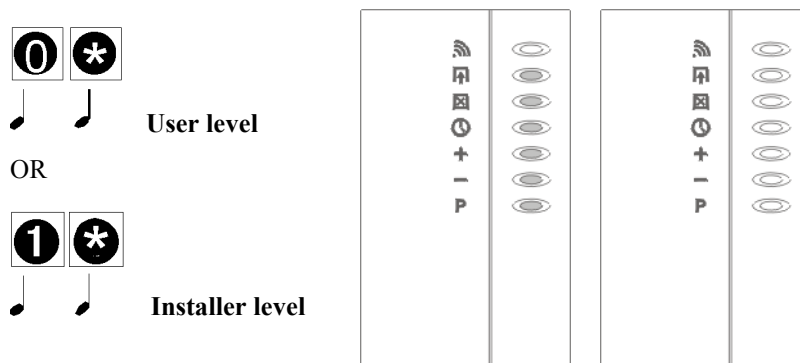
Remarks:
- Step 6 <Power off> must be executed.

To resume operations without changing level:

4.   5. Resume normal operation
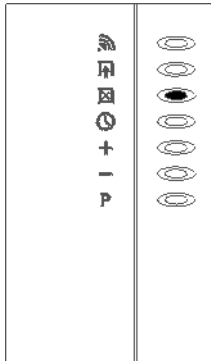
Outputs: Inactive
Inputs: inactive

Remarks:
- Setting a higher level than the level of the Programmer itself is not allowed.

Possible errors:
- The *XM3* does not enter Program mode, instead an alarm is generated. The Programmer is not present in memory: present another Programmer.
- When setting the level, error tone sounds, after which the *XM3* resumes normal operation; the level ('n'), which was entered, is higher than the level of the presented Programmer. The level that is being set must be lower than or equal to the level of the Programmer itself.

5.2   Access (1*)

Any valid Remote Programmer can obtain access; there is no need for a separate user tag.

Access:
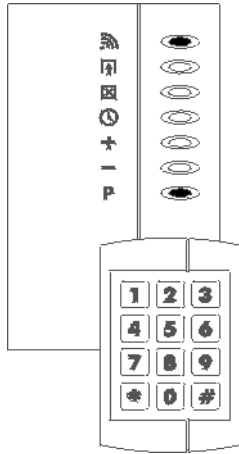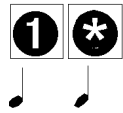
1. Program mode	2.	3. Access mode I or II, depending on settings	4. Open Time	5. Resume normal operation
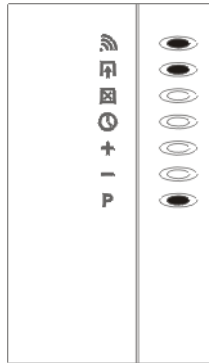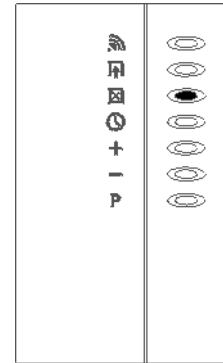
Outputs: Relay activated   Relay deactivated
Inputs: Inactive

Remarks:
- For purposes of test and maintenance, higher level programmers will only be allowed access when the XM3 is set at a higher level than 0.
- After a certain period of no operation the *XM3* will generate an error tone, after which it will resume normal operation. This period known as Overall Time-out is by default set to 30 seconds.

Possible errors:
- When presenting the programmer an error tone sounds: the Programmer is not present in the memory of the *XM3*, or the 'Protect' option was set.
- When selecting the step indicated after pressing the Enter key, an error tone sounds: the Programmer is not a User Programmer, while the *XM3* is set at level 0.

5.3   Add tags by number (2*)

In standard Access mode, the *XM3* will not grant access to a tag unless its ID number is present in memory. A tag can be added to memory by a Master or a Remote Programmer, provided the tag is available for presentation. If the tag is not available, e.g. because the person carrying it is not present, it can still be added by entering its *Add level* and number with a legitimate Remote Programmer, as described below.

Add tags by number:

1. Program mode

2. Enter Add mode

3. Add mode

4. Set the Tag level

5. Set Tag type.

6. Enter facility code

7. Enter tag number (**repeat for each new tag** at this Add level)

8. Exit Add mode

9. Resume normal operation

nn	Tag levels	nn	Tag type
11	Installer Programmer	0	Cross Point H4201 (no facility code)
10	User Programmer, Program master	1	HID Standard 26 bit (H10302)
9	Void Master	2	HID Standard 34 bit (H10306)
8	Add Master	3	HID Corporate 1000 (no facility code)
7	Night Lock Master	4	HID Standard 37 bit (H10302)
6	PIN Keypad	5	HID Standard 37 bit (H10304)
3-5	Undefined	6	Microchip MCRF 355/360 (no facility code)
2	Status III tags. Night lock only	7	-reserved-
1	Status II tags. Always access	8	Mifare Standard (no facility code)
0	Status I tags. Normal users	9	EM Marin H4201/H4001 (no facility code)

Levels are used to assign a tag specific functionality. Choose the functionality level of the card that has to be created.

Remarks:
- When Cross Point cards are used, the card ID will consist of 9 digits. All other sorts of cards have a card ID consisting of 13 digits.
- The EN text facility code has to be entered only when a HID card is used with the facility code.
- Any tag can be added, unless it is already present in memory.
- The number of ID's that the *XM3* memory can hold depends on the configuration that has been chosen (including at least 3 Masters and/or Remote Programmers).
- Leading zeroes of the ID number (step 5) need not be entered, e.g. for ID number (0042062) entering (42062 *) is sufficient.
- It is not permitted to add at higher levels than the presented tag or Programmer is authorized for (see above diagram).
- After a certain period of no operation the *XM3* will generate an error tone, after which it will resume normal operation. This period known as Overall Time-out is by default set to 30 seconds.
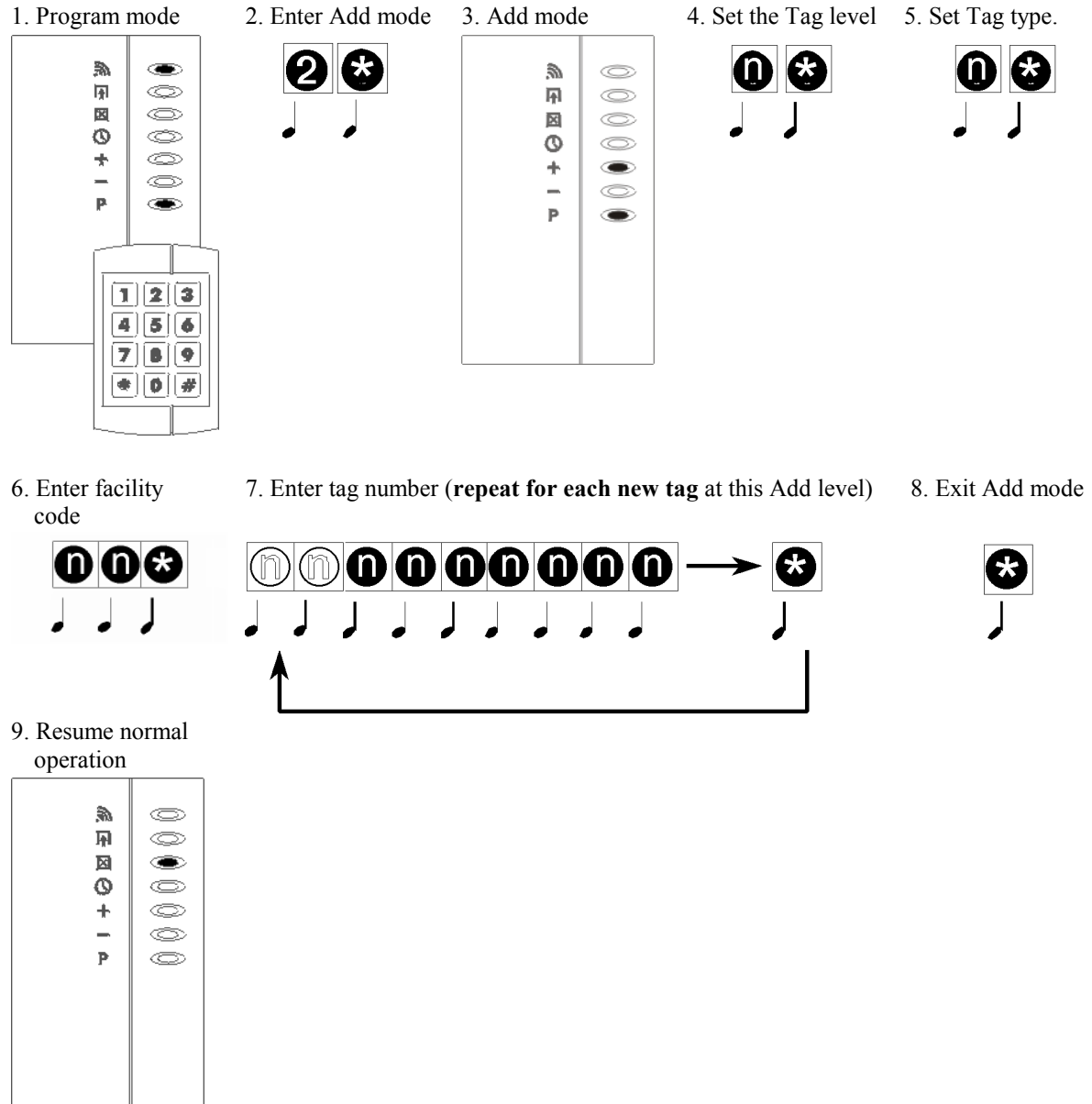- Keep records of the ID numbers and functionality of all tags and Programmers, and of their users. In case of loss, tags can be voided from memory by number, using Remote Programmer function 9*.
- In user mode an Installer Programmer cannot be used to add tags.
- Dependant on the Tag type, the facility code can be minimal 3 characters and maximal 5 characters.

Possible errors:
- When presenting the Programmer, an error tone sounds: the Programmer is not present in the *XM3* memory, or the 'Protect' option was set.
- After the Add level is entered, an error tone sounds, and normal operation resumes; the presented Programmer is not allowed to add at the entered level (see above diagram); check the Programmer's level.
- After entering a new tag number, an error tone sounds: the memory is full or the tag number is already present in memory. In the latter case, a wrong number may have been entered; if not, the records should be checked to determine holder and status of the tag.
- After the ID number has been entered, it is difficult to correct typing errors.
- Access is denied to a newly entered tag. Most likely a typing error has been made while entering the new tag number. It is not possible to locate such a faulty number. Type the number again.

5.4   Set Night Lock mode (3*)

The Night Lock mode is a special mode in which the normal tags are denied access.

The Night Lock triggers output I/O4, intended for external control, e.g. to switch on an external alarm system or to control the mains for lighting or for other electrical devices. Night Lock mode can be switched on and off by a Remote Programmer, and/or via an external control. In Night Lock mode, a User level Remote Programmer can be used to obtain access, while switching the *XM3* to Access mode (level 0), just like a Night Lock Master.

Set Night Lock mode:

| 1. | 2. Program mode | 3. Night Lock on | 4. Night Lock mode |
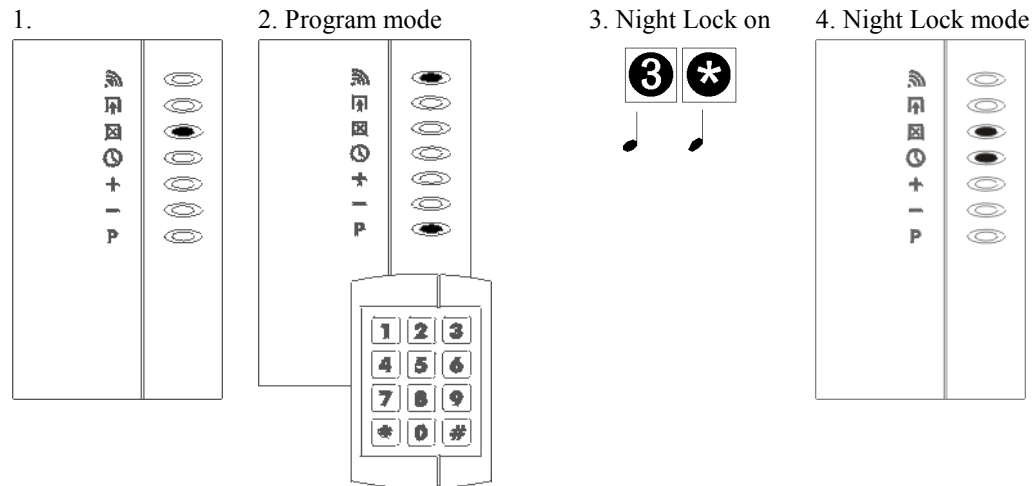
Outputs: Inactive   I/O4 activated

Inputs: Inactive

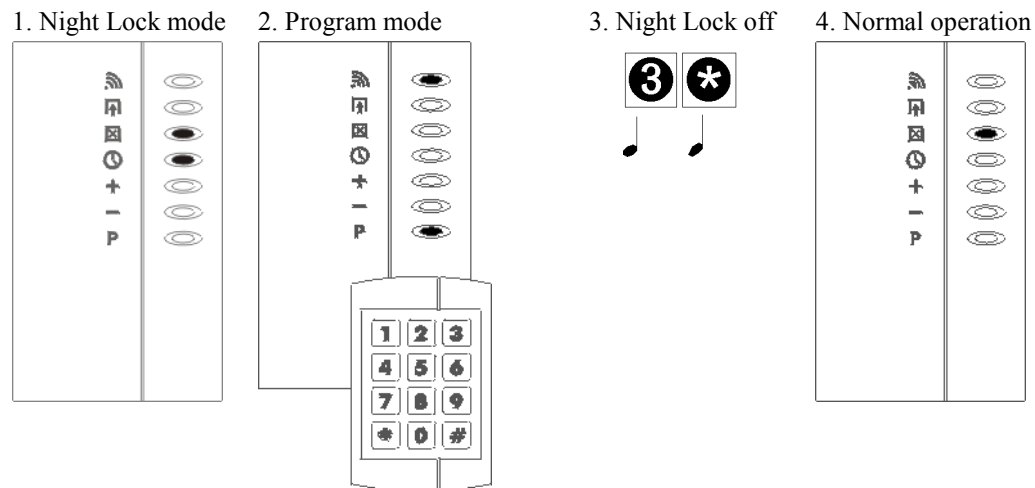**Switch Night Lock mode off (if in User mode and Installer programmer):**

| 1. Night Lock mode | 2. Program mode | 3. Night Lock off | 4. Normal operation |

Outputs: I/O4 active   I/O4 deactivated

Inputs: Inactive

Switch Night Lock mode off (if in User mode and User Programmer, or at higher level and higher Programmer):
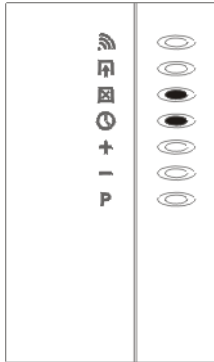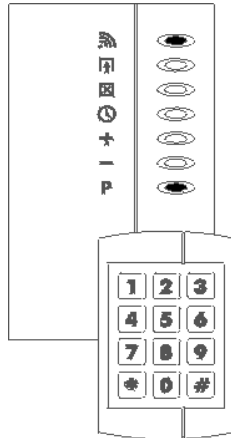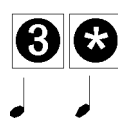
1. Night Lock mode   2. Program mode   3. Night Lock off   4. Access
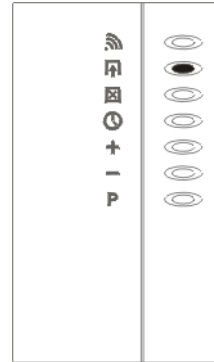
Outputs: I/O4 active   I/O4 deactivated,
                                                        Relay activated

Inputs: Inactive

Remarks:
- Any Programmer at any level is allowed to perform this operation except when the 'Protect' option was set, in which case only a User Programmer will be valid.
- Switching off Night Lock mode is similar to presenting a Night Lock Master in that access will be granted, however, this will be effective only with a User Programmer set at operation level 0 or with any other Programmer set at a higher level.
- After a certain period of no operation the *XM3* will generate an error tone, after which it will resume normal operation. This period known as Overall Time-out is by default set to 30 seconds.
- When presenting the programmer an error tone is generated; the programmer is unknown to the *XM3* or the 'protect' option was set.
- Night Lock set/reset is being performed but no access was granted; the Programmer is not regarded as valid for obtaining access at the current operation level. Check whether the Programmer is a User Programmer at level 0, or if not, whether the operation level was set to zero.

5.5   Add tags – status I (4*)

To be granted access by the *XM3*, tags have to be added first. With the Remote Programmer new tags can be added when they are presented. After this step the new User tags will be granted access in Access mode, i.e. when only the Closed LED is on. This is referred to as Status I.

Add new User tags (status I):

1. Program mode	2. Enter Add mode	3. Add new User tags (present each new tag)	4. Add mode off	5. Resume normal operation
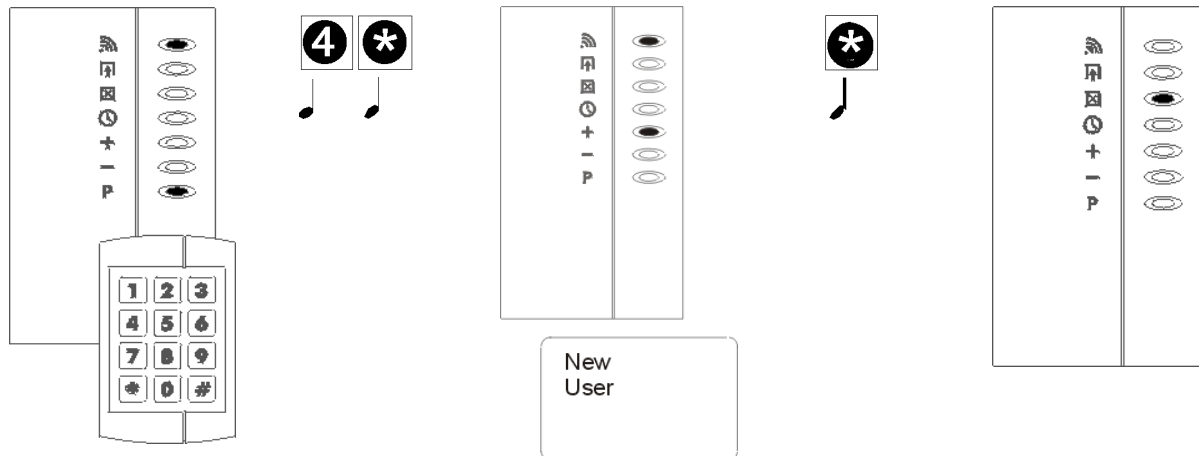
Outputs: Inactive
Inputs: Inactive

Remarks:
- Any tag can be added, except Master Cards and cards that are already present in memory.
- With a Remote Programmer, tags can be added even in Night Lock mode; with an Add Master this is not possible.
- Write down the number of the tag and the name of the user. When a tag is lost, it can be voided from memory by entering its number using a Remote Programmer.
- Up to MAX minus the number of Master tags and/or programmers (minimal 3) can be added.
- After a certain period of no operation the *XM3* will generate an error tone, after which it will resume normal operation. This period known as Overall Time-out is by default set to 30 seconds.

Possible errors:
- When presenting the Programmer an error tone sounds; the Programmer is unknown to the *XM3* or the 'protect' option was set.
- When entering programming step (4 *), an error tone sounds, and the *XM3* resumes normal operation: the Programmer is present in memory, but is not regarded as valid to add tags to memory. Check the operation level that was set by using (93 *). When set to 0, only a User Programmer is regarded as valid. The level of the Programmer can be checked with (94 *).
- While presenting new tags an error tone sounds, resuming normal operation; the tag was already present in memory: check its function by presenting it.
- The memory is full: check the number of free positions with (92 *).

5.6   Void tags (5*)

To deny old tags or programmers access, they must be voided from memory. After this step, which clears the memory space they occupied, they will be regarded as unknown by the *XM3*.

Void tags:

1. Program mode	2. Enter Void mode	3. Void old tags & Programmers (present each old one)	4. Void mode off	5. Resume normal operation

Outputs: Inactive
Inputs: Inactive

Remarks:
- Any tag or Programmer in memory can be voided, except for Programmers that have a higher level than the presented Programmer.
- After a certain period of no operation the *XM3* will generate an error tone, after which it will resume normal operation. This period known as Overall Time-out is by default set to 30 seconds.
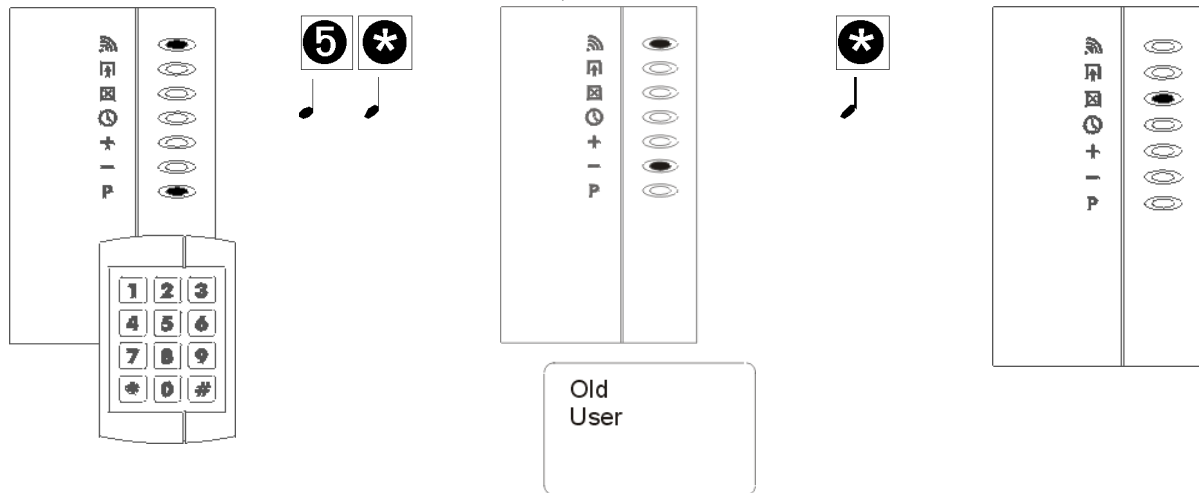- Keep records of the ID numbers and functions of all tags, and of the names of their users. When tags are lost, they can be voided from memory by entering their number using a Remote Programmer.

Possible errors:
- When presenting the Programmer an error tone sounds; the Programmer is unknown to the *XM3* or the 'protect' option was set.
- While presenting tags or Programmers that have to be voided an error tone is generated, resuming normal operation;
- The tag presented as an old tag or Programmer was unknown in memory; confirm this, if necessary, by checking its function in normal mode: when unknown, an error tone should be heard. In case a Programmer was presented it is also possible that it is already present in memory, but has a higher level. Check the Programmer level(s) with (94 *).

5.7   Set internal real time clock (6*)

The *XM3* is supporting the option to set the date and time value for its internal real time clock using a remote programmer.

For the internal real time clock the Gregorian calendar notation is used. The time must be entered as 4-digit decimal numbers representing a 24 hour time stamp in the 'hhmm' format, e.g. 2359 = 23:59.

To set the time and date program the following values:

yyyy	=	Year A.D.	(2000.2099)
mm	=	Month of the year	(1…12)
dd	=	Day of the month	(1…31)
hh	=	Hour since midnight	(0…59)
nn	=	Minute after hour	(0…59)
ss	=	Seconds after the minute	(0…59)

Set time and date:

1. Program mode
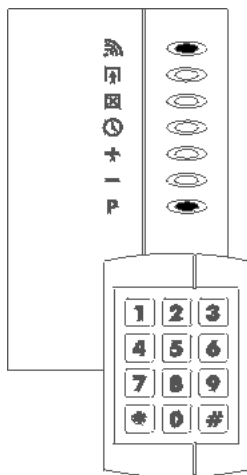
2. Activate 'set clock mode'

3. Set clock mode
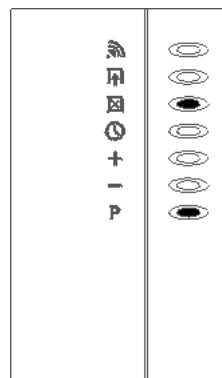
4. Enter time and date.
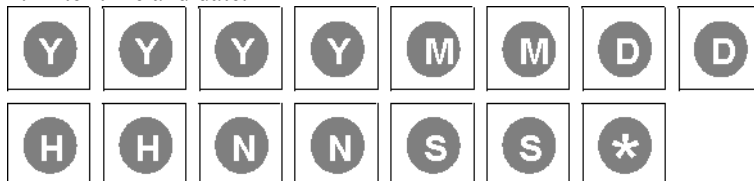
5. Resume normal operation.
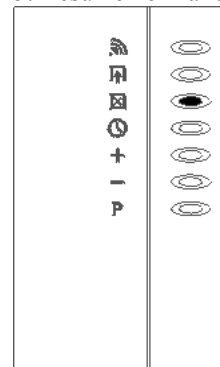
Remarks:
- The *XM3* real-time clock has no battery back-up so date and time are reset to 01-01-2000 00:00:00 after a power reset of the *XM3*.
- The network interface should normally be used to periodically update the real-time-clock of the *XM3*. However, there are situations conceivable in which this is not possible, e.g. stand-alone mode configuration or log printer is attached to RS-485 interface.
- When the *XM3* is using a configuration in which event logging is used the real-time clock will be automatically set to the date and time stamp of the youngest event in the event log after powering up or reset.

Notes:
- This requirement applies only if an event log is included in the file system configuration.
- This results in a new event and will always be younger than the oldest stored event and therewith avoids invalid or illogical order of events in event log.
- After a certain period of no operation the *XM3* will generate an error tone, after which it will resume normal operation. This period known as Overall Time-out is by default set to 30 seconds.

5.8   Add special User tags – status II (7*)

The *XM3* provides the possibility of adding specific tags, referred to as Special User tags, which are granted access both in Access mode and in Night Lock mode. These Special User tags can be added directly without setting Night Lock mode first.
After this step the new Special User tags will be granted access at any time, regardless of the status of the Night Lock LED.

Add new Special User tags (status II):

1. Program mode	2. Enter Add mode	3. Add new Special User tags	4. Add mode off	5. Resume normal operation

New
Special user
Only

Outputs: Inactive
Inputs: Inactive

Remarks:
- Tags that can be added are: unknown tags and tags with a lower level (these will be upgraded).
- Up to MAX minus the number of master tags and/or programmers (minimal 3) can be added.
- After a certain period of no operation the *XM3* will generate an error tone, after which it will resume normal operation. This period known as Overall Time-out is by default set to 30 seconds.
- Keep records of the ID numbers and functions of all tags and of the names of their users. When tags are lost, they can be voided from memory by entering their number using a Remote Programmer.

Possible errors:
- When presenting the programmer an error tone sounds; the Programmer is unknown to the *XM3* or the 'protect' option was set.
- When entering the programming step (7 *) an error tone sounds, resuming normal operation; the Programmer is present in memory, but is not regarded as authorized to add tags to memory. Check the operation level that was set by (93 *): when set to 0, only a User Programmer is regarded as authorized. The level of the Programmer can be checked with (94 *).
- While presenting new tags an error tone is generated, resuming normal operation; the tag was already present in memory. Check its function by presenting it.
- The memory is full: check the number of free positions with (92 *).

5.9   Add Night Lock only tags (8*)

Sometimes it may be necessary to grant a group of users access at times when another group is to be denied access and vice versa. For example, security personnel or cleaning staff may have access only outside normal office hours and during holidays when the *XM3* would be set to Night Lock mode. In such cases, the Night Lock status functions as a discriminative (time) zoning system.

Add new Night Lock Only tags (status III):

1. Program mode	2. Enter Add mode for status III	3. Add new Night Lock Only tags (present each new tag)	4. Add mode off	5. Resume normal operation

Outputs: Inactive
Inputs: Inactive

Remarks:
- Tags that can be added are: unknown tags and tags with a lower level (these will be upgraded).
- Up to MAX minus the number of Master tags and/or Programmers (minimal 3) can be added.
- After a certain period of no operation the *XM3* will generate an error tone, after which it will resume normal operation. This period known as Overall Time-out is by default set to 30 seconds.
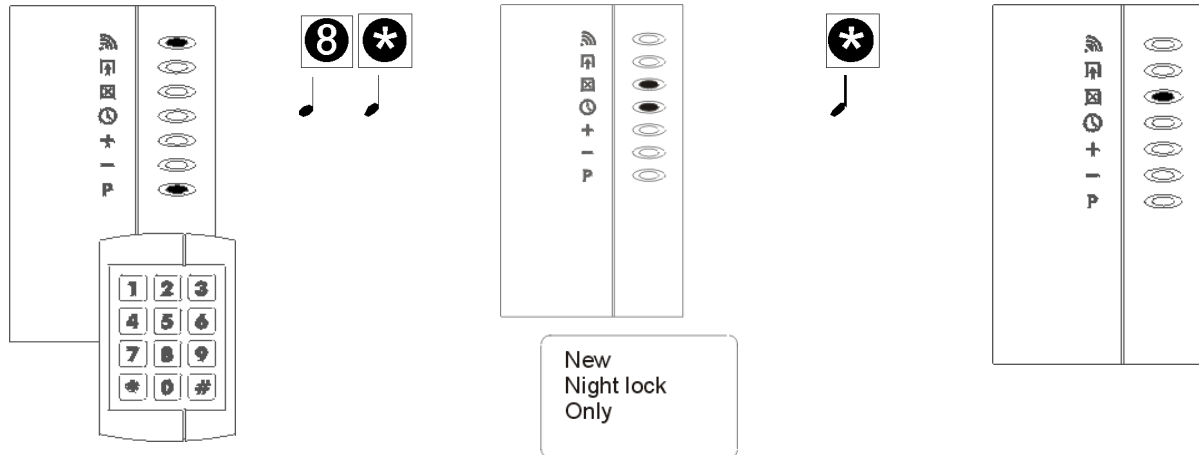
Possible errors:
- When presenting the programmer an error tone sounds; the Programmer is unknown to the *XM3* or the 'protect' option was set.
- When entering the programming step (8 *) an error tone is generated, resuming normal operation; the Programmer is present in memory, but is not regarded as being authorized to add tags to memory. Check the operation level that was set by (93 *): when set to 0, only a User Programmer is regarded as authorized. The level of the Programmer can be checked with (94 *).
- While presenting new tags an error tone sounds, resuming normal operation; the tag was already present in memory: Check its function by presenting it.
- The memory is full: Check the number of free positions with (92 *).

5.10 Voiding tags by number (9*)

To use the Remote Programmer to void tags or Programmers because they are for instance lost, stolen or so severely damaged that they cannot be used, the specific ID number must be known. For this reason it is important to keep records of all added tags, Masters and Remote Programmers.

Void tags by number:

1. Program mode   2. Enter Void mode   3. Void mode   4. Enter tags sort   5. Enter Facility code
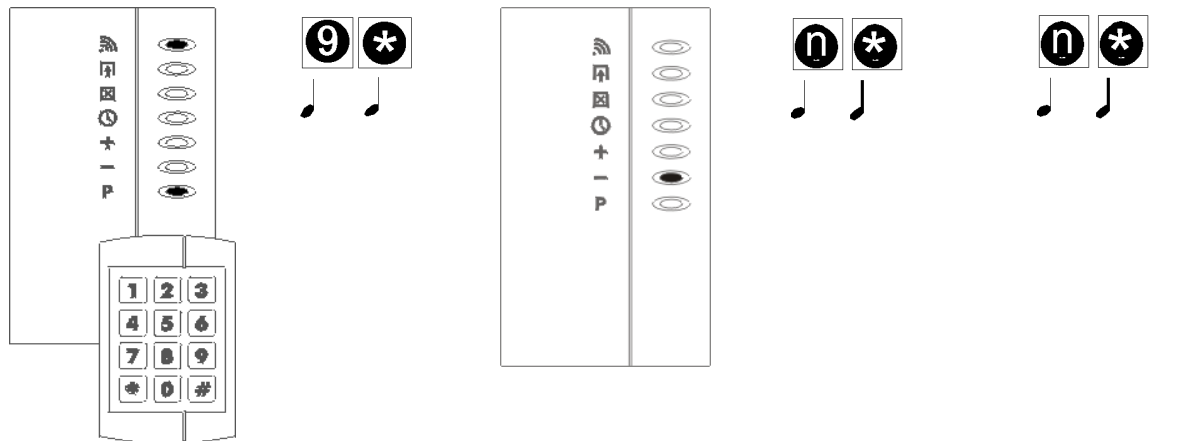
6. Enter tag number (**repeat for each old tag**)   7. Exit Void mode   8. Resume normal operation
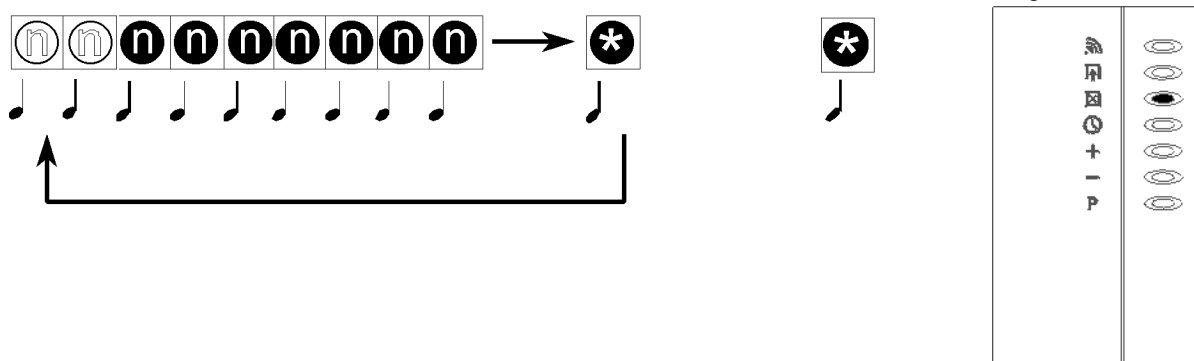
Outputs: Inactive
Inputs: Inactive

nn	Tag type
0	Cross Point H4201 (no facility code)
1	HID Standard 26 bit (H10302)
2	HID Standard 34 bit (H10306)
3	HID Corporate 1000 (no facility code)
4	HID Standard 37 bit (H10302)
5	HID Standard 37 bit (H10304)
6	Microchip MCRF 355/360 (no facility code)
7	-reserved-
8	Mifare Standard (no facility code)
9	EM Marin H4201/H4001 (no facility code)

Remarks:

- When Cross Point cards are used, the card ID will consist of 9 digits. All other sorts of cards have a card ID consisting of 13 digits.
- The EN text facility code has to be entered only when a HID card is used with the facility code.
- Leading zeroes of the ID number n_1 to n_9 need not be entered, e.g. for ID number (004290672) entering (4290672 *) would be sufficient.
- If the User Programmer is missing or badly damaged, the user should request the installer or supplier, who should have a programmer for backup/maintenance purposes, to perform this operation. Also, a new User Programmer should be added as soon as possible.
- Any tag or Programmer in memory can be voided, except for those Programmers that have a higher level than the Programmer used to void by number.
- After a certain period of no operation the *XM3* will generate an error tone, after which it will resume normal operation. This period known as Overall Time-out is by default set to 30 seconds.
- It is not permitted to use a Programmer to void itself.
- Keep records of the ID numbers and functions of all tags and of the names of their users. When tags are lost, they can be voided from memory by entering their number using a Remote Programmer.
- Dependant on the Tag type, the facility code can be minimal 3 characters and maximal 5 characters.

Possible errors:

- When presenting the programmer an error tone sounds; the Programmer is unknown to the *XM3* or the 'protect' option was set.
- After entering the number of the tag or Programmer to be voided an error tone is generated, and normal operation resumes: the number entered was not present in memory. Check to make sure that the number is correct. If the ID number belongs to a Programmer, it is also possible that it is in memory at a higher level than the applied Programmer: check the Programmer level.

6 USER FUNCTIONS

Programming steps (0*-19*) and (50*-99*) are intended for users possessing a User Programmer, as well as for installers and dealers. Steps (20*-49*) are reserved for dealers and installers.

6.1 User Options mode (10*)

Display/set User Options:

1. Program mode   2. Enter User Option mode   3. Display current User Option settings
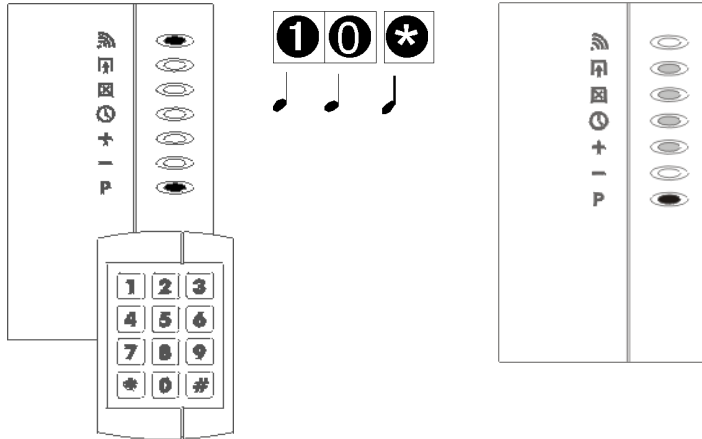
Outputs: Inactive
Inputs: Inactive

To set new User Options:

4. Type the sum of the Options numbers   5. Display new User Option settings   6. Wait one second   6. Resume normal operation
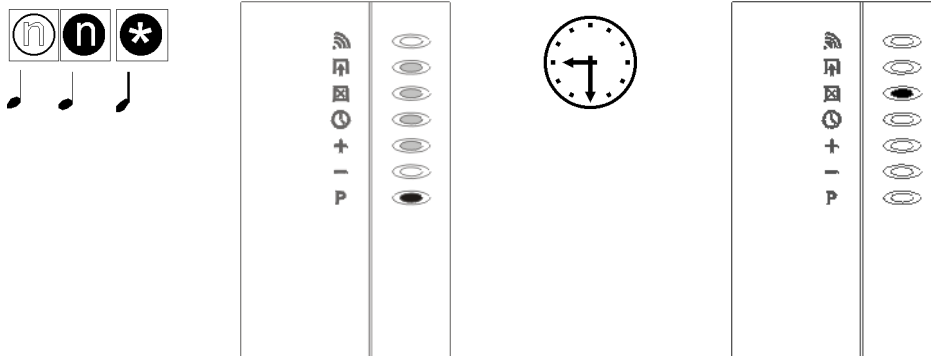
Outputs: Inactive
Inputs: Inactive

To resume normal operations without setting new Installer Options:

4.   5. Resume normal
                               operation

Outputs: Inactive
Inputs: Inactive

6.1.1   Protect option (10*1*)

The 'Protect' option limits Program mode to the User Programmer. Any other Programmers in memory, even if they have higher levels, are prevented from entering Program mode. By default the Protect option is off. 'Protect' can be bypassed only when the Programmer is presented in the RF-field while re-powering the system. Programmers added at higher levels are intended for backup and maintenance purposes only, and will not be able to obtain access. The User Programmer cannot erase these higher-level Programmers from memory.
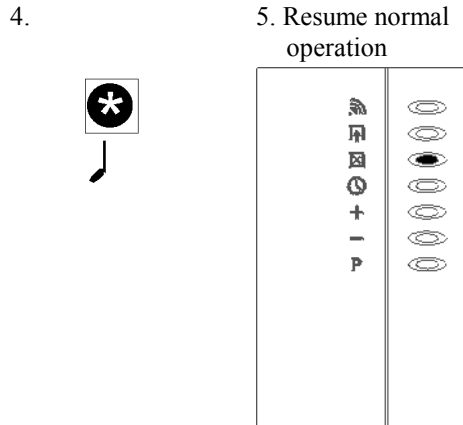
6.1.2   Read indication option (10*4*)

If this option is on, LED 1 will go on when a tag or Programmer is read or identified. Default is: read indication on.

The User options can be used in any combination. Individual 'on' values of the options are: '1' for Protect and '4' for Read indication. When the options are to be combined, the individual values must be added. For example, when setting both Protect and Read indication, enter **5**, (1 + 4).

Display of option		Add values of 'n'
Off: Protect option off	On: Protect option on	0 when off, 1 when on
Off: Reserved for future option		0 when off, 2 when on
Off: No Read indication	On: Read indication with LED 1	0 when off, 4 when on
		+
		Total is 'nn'

Remarks:
- 'Protect' does not disable tags and Programmers added at level 0, even if this was done prior to installation. For this reason, in cases where the *XM3* has been newly installed with a User Programmer (level 0), **the user is strongly recommended to erase memory first** at level 0 with (99* 10*), **before performing any other operation**, unless otherwise agreed with the *XM3* supplier. This operation will disable access by any unknown and unauthorized tags and Programmers that were added at level 0 before installation.
- After a certain period of no operation the *XM3* will generate an error tone, after which it will resume normal operation. This period known as Overall Time-out is by default set to 30 seconds.

Possible errors:
- When presenting the Remote Programmer an error tone is generated; the Programmer is unknown to the *XM3* or the 'protect' option was set. Bypass it during Power on to restore the situation.

6.2   Setting the Open Time-out (11*)

Whenever access is granted, the Relay and I/O3 output of the *XM3* can be activated during a certain number of seconds, called the Open Time-out.

This time period is adjustable from 1 to 255 seconds. The Open Time-out default is 2 seconds. For testing purposes 4 seconds for a normal door and 20 seconds for a gate are recommended.

The Open Time-out is independent from the Close Time-out. In special user mode (Access mode II) the Relay and
I/O3 are switched off, i.e. inactive when the door or gate is closed even before the Open time has elapsed.

Program Open Time-out:
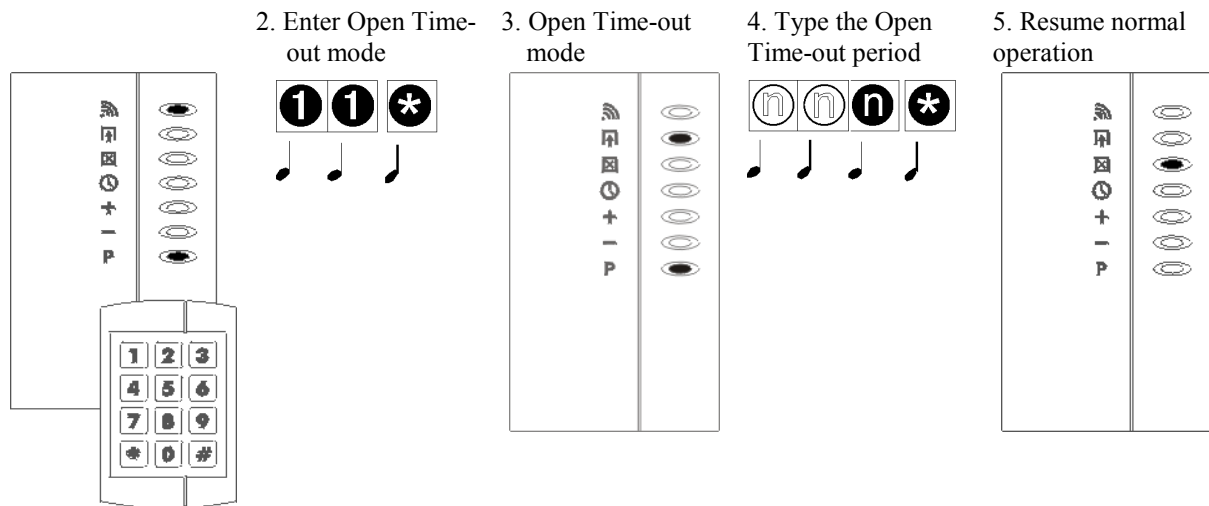
Remarks:
- The value of 'n₁, n₂ and n₃' must be within a range of 1 to 255.
- Any Programmer at any level is allowed to perform this operation, except when the 'Protect' option is set, in which case only a User Programmer will be valid.
- After a certain period of no operation the *XM3* will generate an error tone, after which it will resume normal operation. This period known as Overall Time-out is by default set to 30 seconds.

Possible errors:
- When presenting the Programmer an error tone sounds; the Programmer is unknown to the *XM3* or the 'protect' option was set.
- After Open time was entered an alarm tone sounds; check whether the correct mode and value were entered. Enter once more the correct mode and value.

6.3 Setting the Close Time-out (12*)

The *XM3* has a special timer that is intended to check whether the gate or door has been closed within a specific time period, adjustable from 0 up to 255 seconds. A period of 4 seconds for a normal door, and 20 seconds for a gate are recommended. The Close Time-out default is 0 (inactive, Access mode I). Any other value will activate the option (Access mode II). I/O1 should be connected to a ground when using this option.

Program Close Time-out:

1. Enter Program Mode	2. Enter Close Time-out mode	3. Close Time-out mode	4. Type the Close Time-out period	5. Resume normal operation

Outputs: Inactive
Inputs: Inactive

Remarks:

- The value of 'n_1, n_2 and n_3' must be within a range of 0 to 255, (0) meaning that the Close Time-out and Door Contact Checking are disabled.
- Any programmer at any level is allowed to perform this operation, except when the 'protect' option was set, in which case only a user programmer will be valid.
- After a certain period of no operation the *XM3* will generate an error tone, after which it will resume normal operation. This period known as Overall Time-out is by default set to 30 seconds.
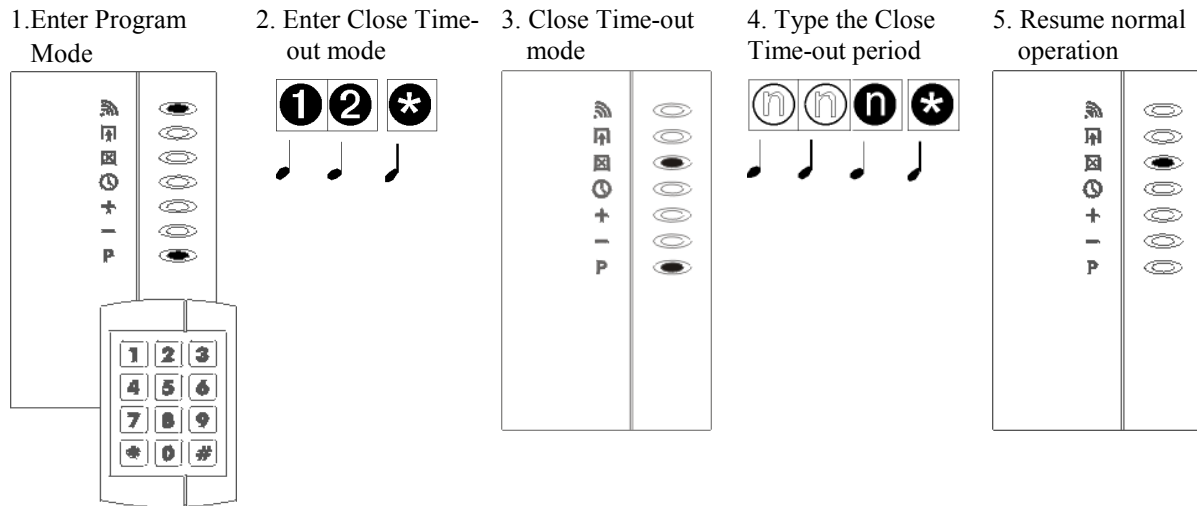
Possible errors:

- When presenting the Programmer an error tone is generated; the Programmer is unknown to the *XM3* or the 'protect' option was set.
- After the Close time was entered a continuous alarm is generated; the Open led is flashing indicating a door open situation. Check whether the door contact is connected and closed when connected properly, I/O1 should be connected to ground. In case of a defective door contact or cable, the continuous alarm can be disabled by bypassing this mode, during presenting a Programmer during power reset of the *XM3*. Once in Program mode, set the Close Time-out time to (0).
- After the Close Time was entered, an alarm tone is generated and normal operations resumes: check whether the correct mode and value was entered. Repeat the operation.

6.4   Adding the Night Lock Master (13*)

The *XM3* has a special mode in which normal tags cannot obtain access, called the Night Lock mode. This mode can be switched on and off by a Night Lock Master, or alternatively with a Remote Programmer by entering (3 *).

Add new Night Lock Master:

1. Program mode	2. Enter Night Lock Master Add mode	3. Night Lock Master Add mode	4. Add New Night Lock Master, resume normal operation
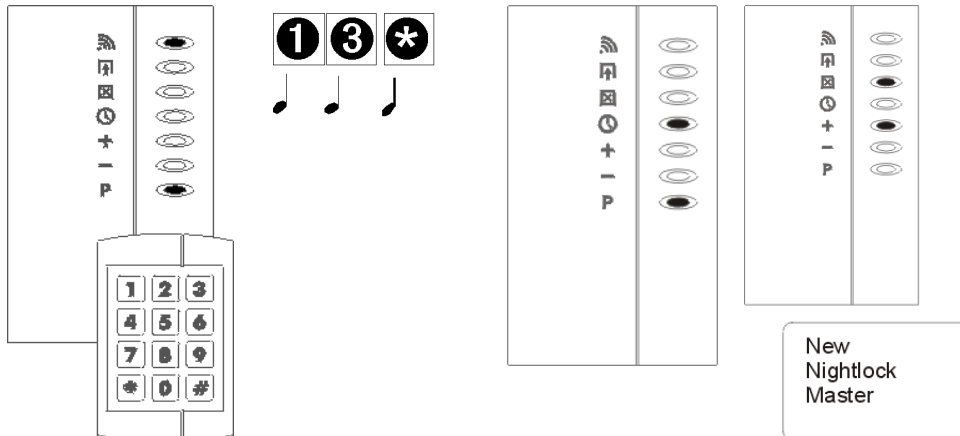
Outputs: Inactive
Inputs: Inactive

Remarks:
- At operation level 0, non-User Programmers are not allowed to program any Masters.
- Any tag can be made a Master, even if it is already present in memory when designated.
- When using more than one *XM3*, it is advisable, for easy management, to use the same Night Lock Master for all Readers.
- Write down the number of the Night Lock Master tag. When a tag is lost, it can be voided from memory by entering its number using a Remote Programmer.
- To ensure access at all times, after a certain time of inactivity while in program mode (set to 30 seconds as default time-out), the *XM3* sounds an error tone, and resumes normal operation.
- Keep records of the ID numbers and functions of all tags, and of the names of their users. When tags are lost, they can be voided from memory by entering their number, using a Remote Programmer.
- After a certain period of no operation the *XM3* will generate an error tone, after which it will resume normal operation. This period known as Overall Time-out is by default set to 30 seconds.

Possible errors:
- When presenting the Programmer an error tone is generated; the Programmer is unknown to the *XM3* or the 'protect' option was set.
- When entering programming step (13 *) an error tone is generated; the presented Programmer is not a User Programmer, the operation level however is set to user (0): use another Programmer or change the level with (0 * n *).
- When presenting the tag an error tone is generated; memory is full. Check the number of free positions.

6.5 Program Add Master (14*)

The *XM3* allows user tags to be added after presentation of an Add Master.

This can also be achieved with a Remote Programmer by entering (4 *).

It can be useful to have more than one tag privileged to perform this function. For instance, a particular person, or a specific group of persons, authorized to work in certain rooms or areas where *XM3* units are applied might carry a separate Master, which is not valid within other rooms or areas.

Add new Add Master:

1. Program mode	2. Enter Add Master Add mode	3. Add Master Add mode	4. Add New Add Master, resume normal operation
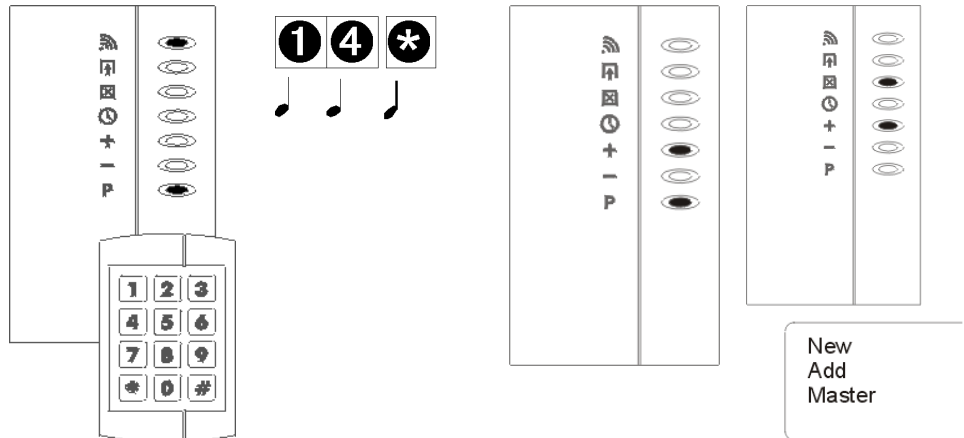
Outputs: Inactive
Inputs: Inactive

Remarks:
- At normal operation level (level 0), non-user programmers are not allowed to program any masters.
- Any tag, known or unknown can be programmed as master.
- When using more than one *XM3*, it is advised for ease of management, to use the same Add master for these functions on other readers.
- Attach a label to the Add Master mentioning its function to avoid mistakes.
- To ensure access at all times after a certain time of inactivity while in program mode (set to 30 seconds as default time-out), the *XM3* generates an error tone and resumes normal operation.
- Keep records of the ID numbers and functionality of all tag, and of the names of their users. When tags are lost, they can be voided from memory by entering their number using a Remote Programmer.
- After a certain period of no operation the *XM3* will generate an error tone, after which it will resume normal operation. This period known as Overall Time-out is by default set to 30 seconds.

Possible errors:
- When presenting the Programmer an error tone is generated; the Programmer is unknown to the *XM3* or the 'protect' option was set.
- When entering the programming step (14 *) an error tone is generated; the Programmer being applied is not a User Programmer, the operation level however is set to user (0): change programmer or change the level with (0 * n *).
- When presenting the tag an error tone is generated; memory is full. Check the number of free positions by using option (92 *).
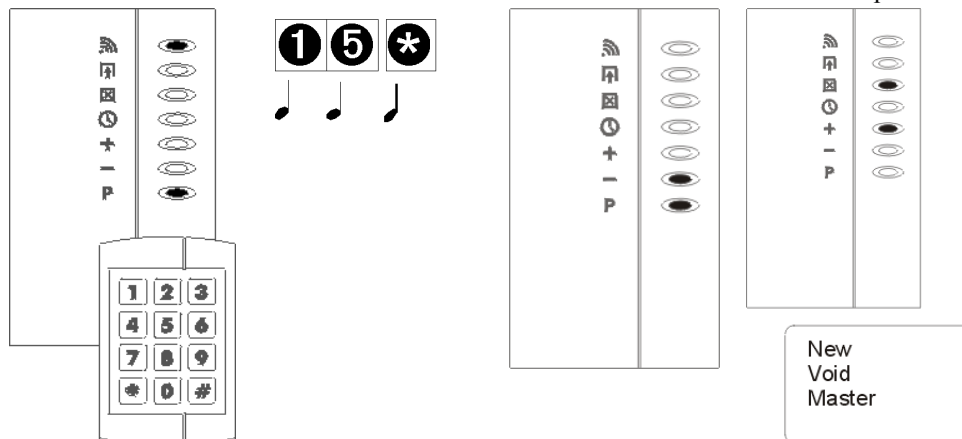
6.6   Program Void Master (15*)

The *XM3* allows user tags to be voided from memory by applying a Void Master.

The same can be achieved with a Remote Programmer by entering (5 *).

It can be useful to have more than one tag privileged to perform this function. For instance, a particular person, or a specific group of persons, authorized to work in certain rooms or areas where *XM3* units are applied might carry a separate Master, which is not valid within other rooms or areas.

Add new Void Master:

1. Program mode   2. Enter Void Master   3. Void Master Add   4. Add New Void
                     Add mode   mode   Master, resume
                                                                 normal operation

Outputs: Inactive
Inputs: Inactive

Remarks:
- Any tag, known or unknown can be programmed as master.
- When using more than one *XM3*, it is advised for ease of management, to use the same Void Master for these functions on other readers.
- Attach a label to the Void Master mentioning its function to avoid mistakes.
- To ensure access at all times after a certain time of inactivity while in program mode (set to 30 seconds as default time-out), the *XM3* generates an error tone and resumes normal operation.
- Keep records of the ID numbers and functionality of all tags, and of the names of their users. When tags are lost, they can be voided from memory by entering their number, using a Remote Programmer.
- After a certain period of no operation the *XM3* will generate an error tone, after which it will resume normal operation. This period known as Overall Time-out is by default set to 30 seconds.
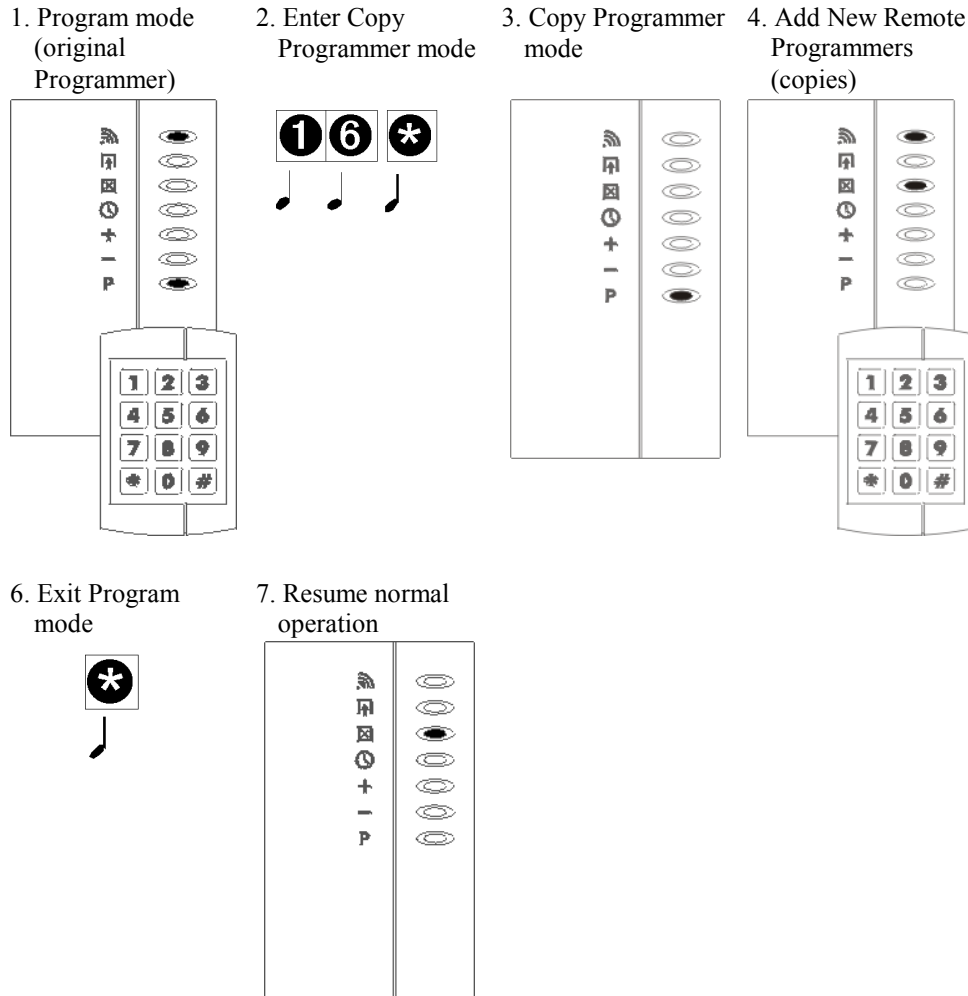
Possible errors:
- When presenting the Programmer an error tone sounds; the Programmer is unknown to the *XM3* or the 'protect' option was set.
- When presenting the tag an error tone sounds; memory is full. Check the number of free positions by using option (92 *).

6.7   Copy Remote Programmer (16*)

Copy Remote Programmer allows a new Programmer to be added to memory at the same level as the original programmer.

Copy Remote Programmer:

1. Program mode (original Programmer)

2. Enter Copy Programmer mode

3. Copy Programmer mode

4. Add New Remote Programmers (copies)

6. Exit Program mode

7. Resume normal operation

Outputs: Inactive
Inputs: Inactive

Remarks:
- Any Programmer can be added to memory, provided it was not present in memory with a higher level than the original one, 'downgrading' by a lower level tag is regarded as an illegal operation. Attach a label to the programmer, mentioning its function/level to avoid mistakes.
- Keep records of the ID numbers and functionality of all tags and Programmers, and of their users. When tags are lost, they can be voided from memory by entering their number, using Remote Programmer function (9*).
- After a certain period of no operation the *XM3* will generate an error tone, after which it will resume normal operation. This period known as Overall Time-out is by default set to 30 seconds.
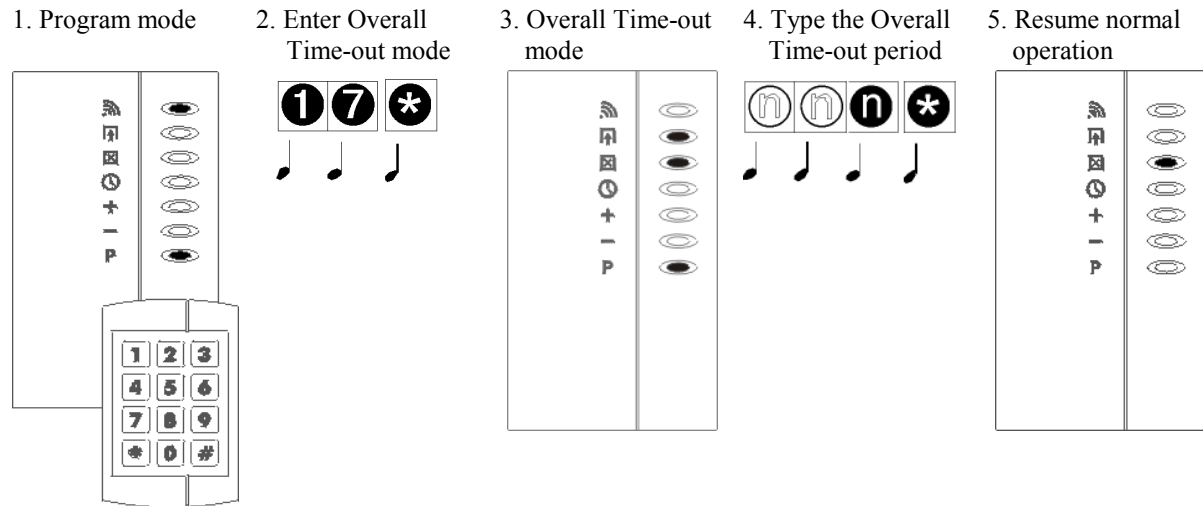
Possible errors:
- When presenting the (original) Programmer an error tone is generated; the Programmer is unknown to the *XM3* or the 'protect' option was set.
- When presenting the new Programmer an error tone is generated; the Programmer might already be in memory at a higher level; it is not allowed to override this level.
- The memory is full: check the number of free positions. This can be checked with (92 *).

6.8   Program Overall Time-out (17*)

The *XM3* has a timer which in Program mode operations, i.e. Adding, Voiding, etc. and is used to count the number of seconds since the latest key-press on the Remote Programmer. If the count exceeds a pre-set value, the *XM3* generates an alarm and resumes normal operation. This period of time is known as the Overall Time-out and is adjustable from 5 up to 255 seconds. The default Overall Time-out is 30 seconds.

Program Overall Time-out:

1. Program mode	2. Enter Overall Time-out mode	3. Overall Time-out mode	4. Type the Overall Time-out period	5. Resume normal operation

Outputs: Inactive
Inputs: Inactive

Remarks:
- The value of 'n_1, n_2 and n_3' must be within a range of 5 to 255.
- Any programmer at any level is allowed to perform this operation except when the 'protect' option was set, in which case only a User Programmer will be valid.
- After a certain period of no operation the *XM3* will generate an error tone, after which it will resume normal operation. This period known as Overall Time-out is by default set to 30 seconds.

Possible errors:
- When presenting the Programmer an error tone is generated; the Programmer is unknown to the *XM3* or the 'protect' option was set.
- After the Overall time has been entered, an alarm tone is generated and normal operation is resumed. Check whether the correct mode and value have been entered. If not, type the correct mode and value.

6.9   Set codes (18*)

6.9.1   Set the PIN code change code (18*0*)

The user can change his personal PIN code by using the PIN code change code.

Set PIN code change code:

1. Program mode   2. Set PIN code change code   3. Change code

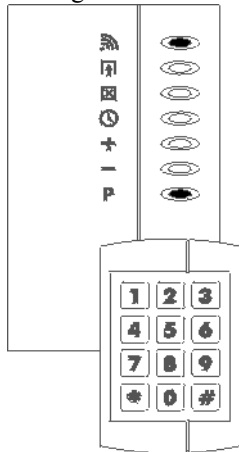4. Normal operation
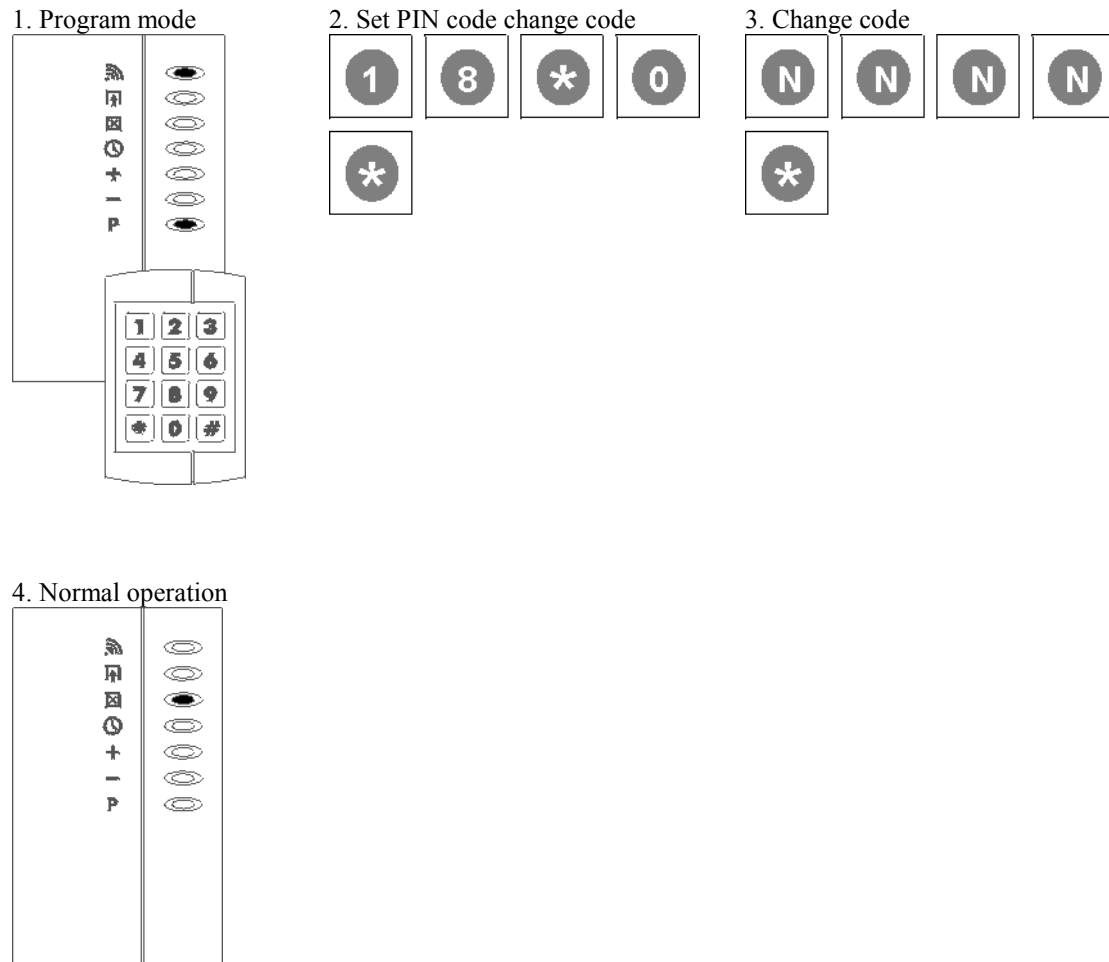
Remarks:
- The PIN code change code can be only activated when the PIN code option is active.
- The PIN code change code must be programmed with a remote programmer.
- The PIN code change code can be activated by programming a 4-digit code that is not 0000.
- The PIN code change code can be deactivated by programming 0000.
- When the PIN code change code is deactivated no more PIN codes can be changed.
- The PIN code change code can't be the same as the alarm code. However, when an attempt is made to do this, the *XM3* will generate a failure.
- After a certain period of no operation, the *XM3* will generate an error tone, after which it will resume normal operation. This period known as Overall Time-out is by default set to 30 seconds.

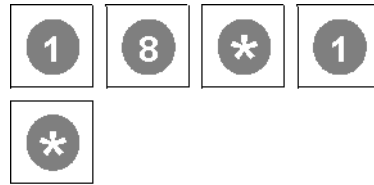### 6.9.2 Set the access code (18*1*)

A special code can be programmed to grant user access without using a tag.
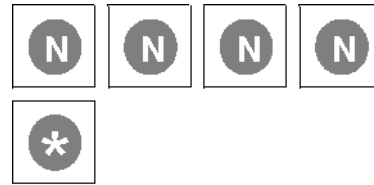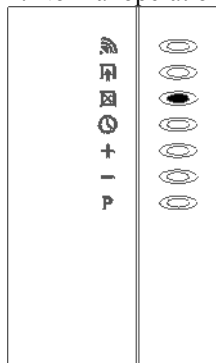
Set the access code:

1. Program mode.

2. Set access code
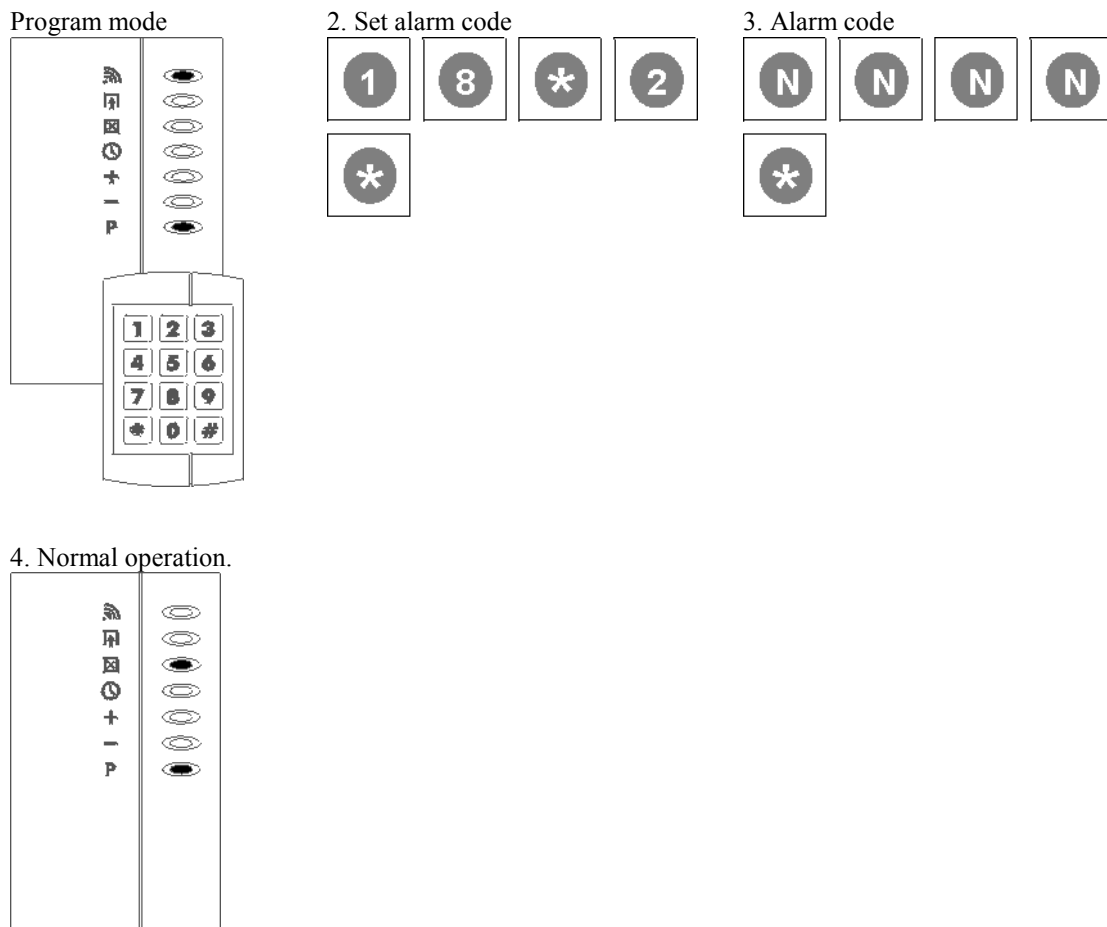
3. Access code

4. Normal operation

Remarks:
- The access code can only be activated when the PIN code option is active
- The access code is an identical code for all users. This means that all users that know the access code have access.
- The access code must be programmed with a remote programmer.
- The access code can be activated by programming a 4-digit code that is not 0000.
- The access code can be deactivated by programming 0000.
- After a certain period of no operation the **XM3** will generate an error tone, after which it will resume normal operation. This period known as Overall Time-out is by default set to 30 seconds.

6.9.3 Set the alarm code (18*2*)

A special alarm code can be programmed that enables a user to activate a silent alarm.

Set the alarm code:

Program mode

2. Set alarm code

1 8 * 2
*

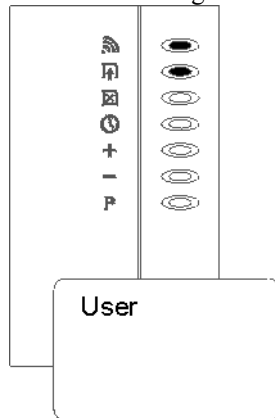3. Alarm code

N N N N
*

4. Normal operation.

Remarks:
- The alarm code can only be activated when the PIN code option is active.
- Because the PIN code option and the alarm code option are related to each other, it is possible to trace the person who activated the alarm. The alarm cannot be activated anonymous.
- An external alarm panel can be activated through I/O3.
- The alarm code must be programmed with a remote programmer.
- The alarm code is an identical code for all users. This means that all users knowing this code can activate the silent alarm.
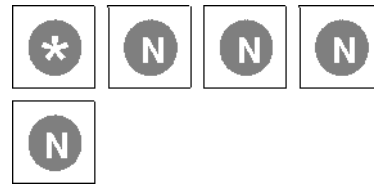
The silent alarm can be activated by presenting any valid user tag and then typing the Alarm code.
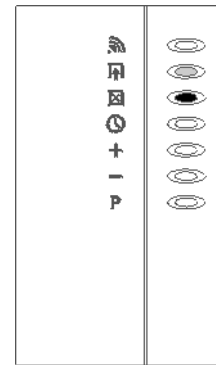
Activating the silent alarm:

1. Present user tag   2. Enter Alarm code   3. Silent alarm

I/O3 Active

4. Wait inactivity time.   5. Normal operation.
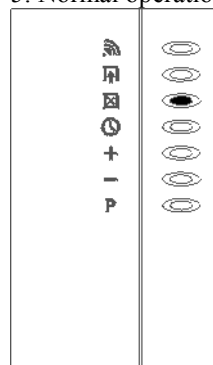
I/O3 Active

I/O3 Active

Remarks:
- After the Alarm code is entered, an error tone will be generated if a wrong PIN code is entered.
- The green led will keep flashing, and I/O3 will remain active.
- There will not be any audio or visual signals after the alarm is triggered.
- Access will not be granted when the Alarm code is entered.
- After the inactivity time-out is reached the *XM3* will go into normal operation except I/O3, which will remain active.

Deactivate the silent alarm:

1. Present user tag.
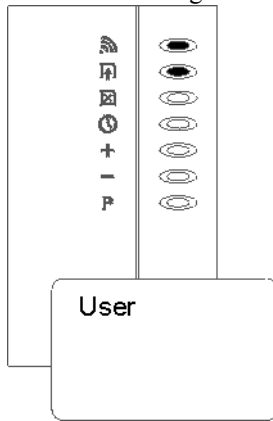
User

I/O3 Active

2. Enter alarm code.
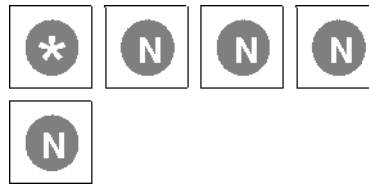
I/O3 Active

3. Normal operation.
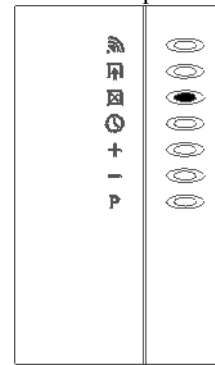
I/O3 Deactivated

Remarks:
- The silent alarm can be deactivated by using any valid user tag.
- Access will be granted now as in any normal situation.
- After a certain period of no operation the *XM3* will generate an error tone, after which it will resume normal operation. This period known as Overall Time-out is by default set to 30 seconds.

6.10 Set password to access *XM3* at user level via RS485 (19*)

To log in to the XM3 via RS485 at user level a password needs to be specified by using a user programmer.

Set user password:

1. Program mode
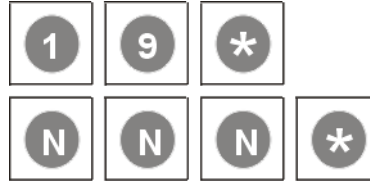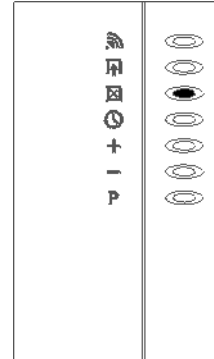
2. Set password

3. Normal operation

Remarks:
- A password (NNN) can consist of 10 digits.
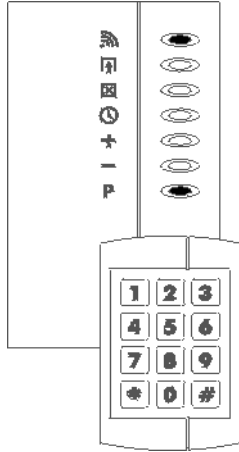- The password is implemented for security purposes.
- Automatic log off is performed if no XM3 operations are executed for a period of NN seconds. This period of time can be set with (17*), the Overall time-out.
- If no password has been defined for user level logon will fail for this level.
- Setting the password to (0) functional disables access to the *XM3* operations at the corresponding level.
- The log in feature will be disabled after 3 false attempts to log in. The *XM3* must be powered down before another attempt to log in can be made.
- After a certain period of no operation the *XM3* will generate an error tone, after which it will resume normal operation. This period known as Overall Time-out is by default set to 30 seconds.

7   INSTALLER FUNCTIONS

The following programming steps, (20*-49*), are intended for installers and/or dealers. The *XM3* should be at installer level (level 1) to successfully perform these steps.

7.1   Program installer options (20*)

Display/set Program Installer Options:
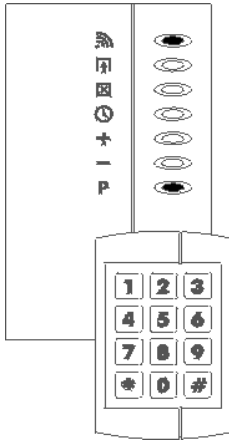
1. Program mode   2. Enter Installer   3. Display current
                        Option mode   Options settings
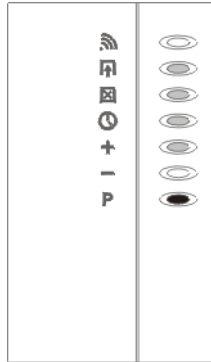
To set new Installer Options:

4. Type the sum of   5. Display new   6. Wait one second   6. Resume normal
   the Options   Option settings   operation
   numbers
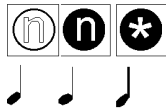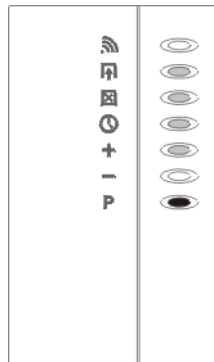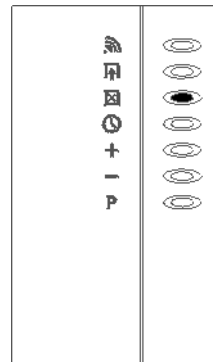
To resume normal operations without setting new Installer Options:

4. Resume   5. Normal operation
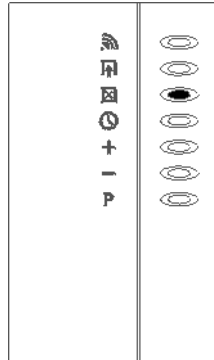
Outputs: Inactive
Inputs: Inactive

At level 1 (Installer), three options are available to change the normal mode of operation of the *XM3*:

7.1.1   Private (20*1*)

Switches the *XM3* into a special operation mode in which it will grant access to only one user tag at a time after which it will go into 'Lock' status. Until the 'Lock'' status is switched off, no other the tags are accepted. Lock status is similar to Night Lock mode and uses the same LED; I/O4 is also activated. However, the Lock status is not memorized in EPROM, so after a power failure or a deliberate power-off the *XM3* always resets to the latest status. By connecting I/O4 to an external relay circuit, an external device can be activated: for instance a light indicating 'Lock' status.

The Lock can be switched off as follows:
            a) Push the egress button (see 7.1.3)
            b) Present the same user tag again.

For safety reasons, and in case of emergency, access can still be obtained as follows:
            a) Present a Night Lock Master.
            b) Turn the power off and on and present any user tag.

Applications: Small (safe) deposits, mailboxes, lavatories, showers, rooms in hospitals or clinics, control switches or computer equipment etc.

7.1.2   Public (20*2*)

Disables the validity check for the presence in *XM3* memory of the numbers of the presented user tags, thus allowing any tag access, regardless whether it is in memory or not. The functionality of Remote Programmers and Master Tags will remain unchanged.
The Public function can only be used during access mode: not in Night lock mode.

Applications:
Large (safe) deposits, parking lots and front doors of large hotels, public institutions or companies etc.

7.1.3 Egress (20*4*)

Allows the connection of a push button mounted inside a separate room. This push button can be used to grant passage when exiting. When set, this option will disable the external Night Lock control which uses the same I/O2 input. The method of access is controlled in a similar way as normal access i.e. using Open Time-out- and Close Time-out, starting from the moment when the button was pushed.
Regress is low active i.e. access is granted when I/O2 is connected to ground potential for a short while.

The Installer options can be used in combination. Especially when the egress button is combined with one of the other options, they are suited for use in applications like public save deposits, money dispensers, showers, lavatories etc.

The individual values of the options are: (1) for private, (2) for Public and (4) for Egress. When the options are to be combined, the individual values must be added. For example, when setting both Public and Egress, type **6**, (2 + 4); when activating all options, type **7** (1 + 2 + 4).
When option 20*1* and 20*2* are combined option 20*1* is overruled.

Led	Display of option led 2-6		Add values of 'n'
2	Off: Private option off	On: Private option on	0 when off, 1 when on
3	Off: Public option off	On: Public option on	0 when off, 2 when on
4	Off: Egress option off	On: Egress option on	0 when off, 4 when on
			+
			Total is 'nn'

Remarks:
- The value of 'n' must be within a range of 0 to 15.
- Only an Installer Programmer can set these options and only when the *XM3* is at Installer Level. When the 'protect' option was set, first reset this option or bypass it during power on, since 'protect' will only accept the user programmer(s).
- After a certain period of no operation the *XM3* will generate an error tone, after which it will resume normal operation. This period known as Overall Time-out is by default set to 30 seconds.

Possible errors:
- When presenting the Programmer an error tone is generated; the Programmer is unknown to the *XM3* or the 'protect' option was set.
- After program step (20 *) was entered the *XM3* generates an alarm tone and resumes normal operation. Check whether the operation level of the *XM3* is not set at (0) with (93 *), and with (94 *) that the Programmer is not a User Programmer.
- After typing the option value (n) an alarm is generated and normal operation is resumed; re-type the correct value.

7.2 Set RS485 network poll time-out (22*)

In network mode the XM3 is connected to a central host computer using a RS485 half-duplex poll/select protocol. In this configuration the host computer is the master and the XM3 is the slave.

In dynamic mode the poll time-out can be set. The XM3 is now able to switch between stand-alone and network mode. The XM3 automatically will switch to stand-alone mode when connection with the host is broken, e.g. network down or power down.

Set poll time-out:

1. Program mode   2. Set polling time   3. Normal operations
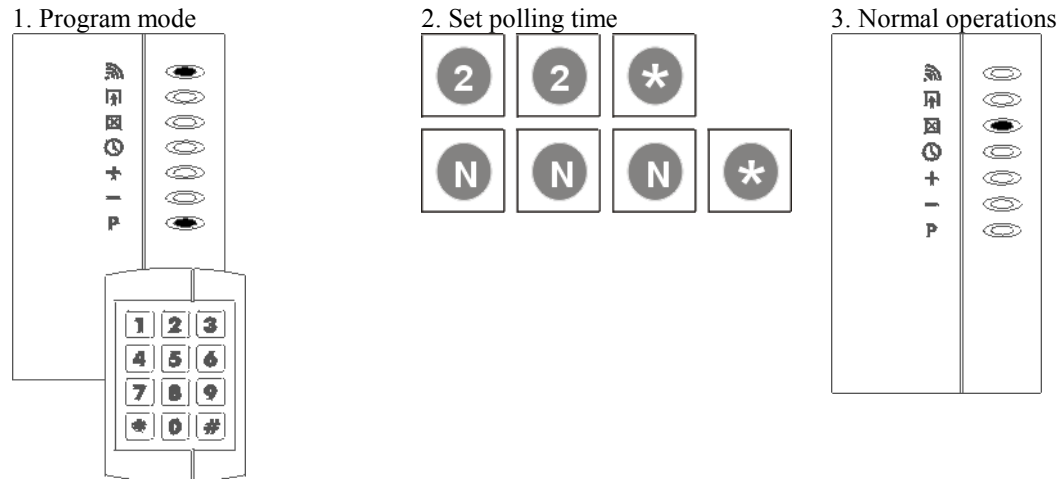
To activate this option, a power reset must be performed.

Remarks:
- When poll time equals 0 the poll time is disabled.
- Poll time can be set to any value within a range of 0-255.
- After a network failure is detected the XM3 will assume that the network is operational again as soon as it receives a valid message from the central host computer.
- In a typical RS485 network the XM3 is polled for about 5 to 15 times per second. This depends on the communication load of the RS485 network.
- It is the responsibility of the central host computer to restart/resume communication with the XM3 after a network failure. The XM3 will not resend the last send message upon a response timeout.
- Events that have taken place during the time the network was down can be downloaded by using event log dump printer (event log must be activated).
- After a certain period of no operation the *XM3* will generate an error tone, after which it will resume normal operation. This period known as Overall Time-out is by default set to 30 seconds.

7.3   Set lock type (23*)

The XM3 lock output can be set in three different ways:

- Normally open
- Normally closed
- Coded signal

These settings can only be programmed with an installer programmer at installer level. The settings normally open and normally closed are used when a lock is directly connected to the XM3. The coded signal is used to trigger an external relay (Cross Point article: XMER-1). The external relay offers higher security.

The lock type can be set by using the following codes:

7.3.1   Set lock type to normally open (23*0*)

Set lock type **normally open**:

- Press (23*0*)

7.3.2   Set lock type to normally closed (23*1*)

Set lock type **normally closed**:

- Press (23*1*)

7.3.3   Set lock type to coded signal (23*2*)

Set lock type **coded signal**:

- Press (23*2*)

Remarks:
- With lock type normally open en normally closed **only DC locks** can be used.
- After a certain period of no operation the *XM3* will generate an error tone, after which it will resume normal operation. This period known as Overall Time-out is by default set to 30 seconds.

7.4   Set password to access *XM3* at installer level via RS485 (24*)

To log in to the XM3 via RS485 on installer level a password needs to be specified by using an installer programmer.

Set the installer password:
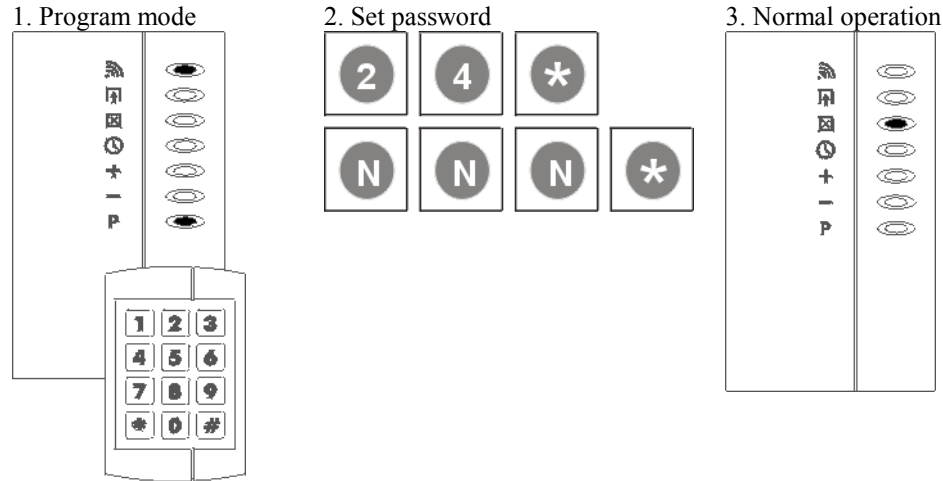
1. Program mode   2. Set password   3. Normal operation

Remarks:
- A password (NNN) can consist of 10 digits.
- The password is implemented for security purposes.
- Automatic log off is performed if no *XM3* operations are executed for a period of NN seconds. This period of time can be set with (17*), the inactivity time.
- If no password has been defined for installer level, log in will fail for this level.
- Setting the password to (0) disables access to the *XM3* operations at the corresponding level.
- The log in feature will be disabled after 3 false attempts to logon. The *XM3* must be powered down before another attempt can be made.
- After a certain period of no operation the ***XM3*** will generate an error tone, after which it will resume normal operation. This period known as Overall Time-out is by default set to 30 seconds.

7.5   Special system settings (25*)

At Installer level (level 1) four optional system settings are available:

7.5.1   Unlock status option (25*1*)

This option can be set in situations where persons need more time than the programmed open-time to enter a room. By presenting the Lock master (equivalent to the Night lock Master) the door or gate will be continuously open. As soon as the (Night) Lockmaster is presented again the unit switches back to normal operation.

Note: the Night lock mode option is not available when this option is set.

7.5.2   Change alarm tone (25*4*)

The alarm tone can be set to continuous (default) or pulsing.

7.5.3   Tamper alarm output select (25*8*)

This option can be used to separate the tamper alarm and the forced entry alarm.
Default they are both available on the Forced entry output. With this option set (25*8*) the tamper alarm is redirected to Night lock enable output.

7.5.4   Tamper off option (25*16*)

When the tamper contact is not used, this option makes it possible to switch the tamper off.

7.5.5   Fixed frequency (25*32*)

In some cases a fixed frequency of 125 kHz is needed. Using this option makes it possible to fix the frequency to this value. If this option is not used, the tolerance of the frequency is +/- 3Hz.

Options above can be combined by typing the sum of the various options. For example to set Unlock (25*1*) mode and change alarm output (25*8*) type: (25* 9*), 1+8.

Led 1-7	Led | Display of option	Led | Display of option	Add values of 'n'
*	Off: No tag	On: Tag read indication	
*	Off: Unlock/Lock option off	On: Unlock/Lock option on	0 when off, 1 when on
*	Off: Alarm tone option off	On: Alarm tone option on	0 when off, 4 when on
*	Off: Tamper alarm output option	On: Tamper alarm output option on	0 when off, 8 when on
*	Off: Tamper on	On: Tamper off	0 when on, 16 when of
*	Off: Fixed frequency off	On: Fixed frequency on	0 when on, 32 when off
*			

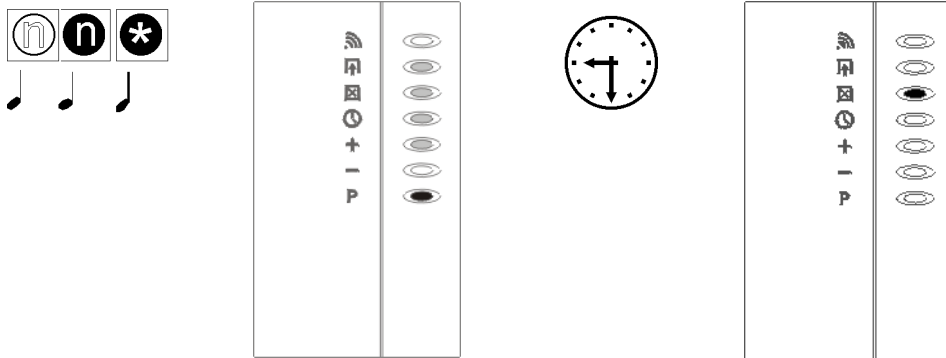<div align="right">+</div>

Total is 'nn'

To display current settings:

1. Program mode

2. Enter set mode

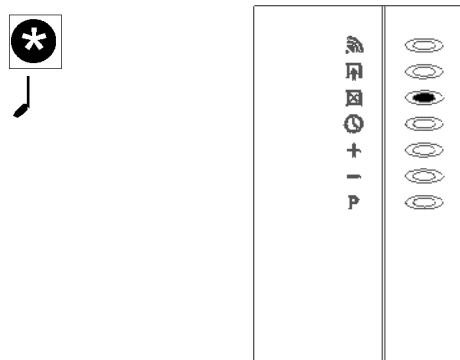3. Display current 'Options' settings
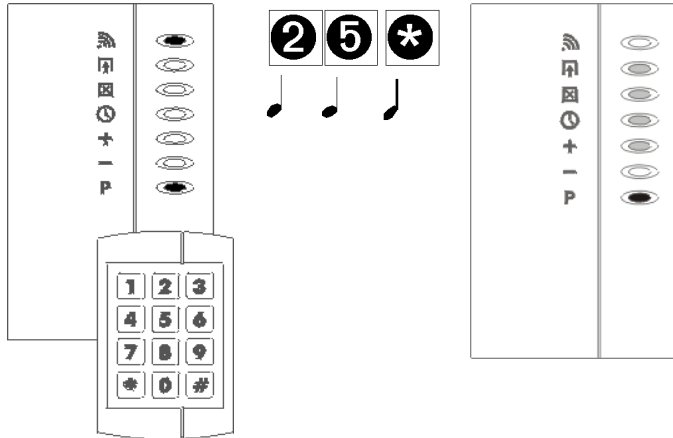
To set new system Options:

4. Type the sum of the 'Options' numbers

5. Display new Option settings

6. Wait one second

7. Normal operation

To resume normal operations without setting new system Options:

4. Resume

5. Normal operation

Remarks:
- The value of 'n' must be within a range of 0 to 61.
- Only the installer programmer at level 1 is allowed to perform this operation. When the 'protect' option was set, first reset this option or bypass it during power on, since 'protect' will only accept the user programmer(s).
- To reset all system settings to default type (25*0*).
- After a certain period of no operation the *XM3* will generate an error tone, after which it will resume normal operation. This period known as Overall Time-out is by default set to 30 seconds.
- If 25*0* is used all option are disabled.

Possible errors:
- When presenting the Programmer an error tone is generated; the Programmer is unknown to the *XM3* or the 'protect' option was set.
- After program step (25 *) was entered, the *XM3* generates an alarm tone, and resumes normal operation. Check that the operation level of the *XM3* is not set at (0) with (93 *), and with (94 *) that the Programmer is not a User Programmer.
- After typing the option value 'n', an error tone is generated and normal operation is resumed; retype the correct value.

7.6   Set file system configuration (26*)

The *XM3* offers the possibility to choose from 16 different file configurations. This makes it possible for the installer to set-up a configuration according to the customers wish. For every *XM3* option there is a file in the file system.

|	
1. NVP file	Contains all *XM3* option adjustments like 'open time', 'close time, etc
2. ID database	Contains ID codes of all valid tags, programmers, keypads
3. PIN code file	Contains PIN code information for all valid tags
4. Event log file	Contains data of all access control events from the past
5. Names file	Contains names/initials of all valid tags

For configuration set-up codes a code can be chosen from table 1.

Configuration code	Amount of Users	Amount of PIN codes	Amount of Names	Amount of Events
0	5000	0	0	0
1	3700	3700	0	0
2	3200	0	0	1000
3	2400	2400	0	1000
4	1300	0	1300	0
5	1200	1200	1200	0
6	850	0	850	1000
7	800	800	800	1000
8	1000	0	0	2300
9	1000	1000	0	2100
10	1000	0	1000	200
11	1000	1000	1000	500
12	250	0	0	2800
13	250	250	0	2750
14	250	0	250	2350
15	250	250	250	2300

Table 1.

Set file system configuration:

1. Program mode.
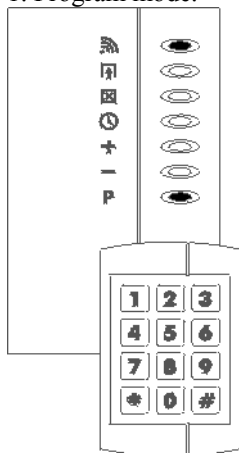
2. Set configuration.

3. Normal configuration
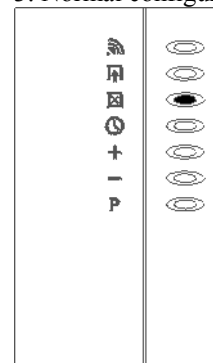
Remarks:
- The file system configuration can only be set using an installer programmer at installer level.
- Every time the file system configuration is changed all data in the *XM3* memory will be lost.
- After changing the system configuration the *XM3* will switch to installer sleep mode.
- In order to activate the *XM3* a power supply reset must be performed.

7.7   Select *XM3* operation mode

The *XM3* can be set to six different operation modes by using the remote programmer.

These operation modes are:

- RS-485 Network mode
- Access mode
- Program mode
- Magstripe mode
- Wiegand mode

In paragraph 7.7.1 up and including 7.7.5 is described how these modes can be activated.

7.7.1   RS-485 network mode

Make sure that the tamper contact of the *XM3* is uncovered (remove the cover). Hold the remote programmer in the field of the *XM3* and push the (2) button while powering up the *XM3*. The RS-485 network mode is now active.

7.7.2   Access mode

Make sure that the tamper contact of the *XM3* is uncovered (remove the cover). Hold the remote programmer in the field of the *XM3* and push the (#) button while powering up the *XM3*. The Access mode is now active.

7.7.3   Program mode

Make sure that the tamper contact is uncovered. Hold the remote programmer in the field of the *XM3* while powering up the *XM3*. The program mode is now active.

Remarks:
- The *XM3* can be set to the default settings by using the bypass option. This option is similar to the access mode as described above.

7.7.4   Wiegand mode

Make sure that the tamper contact of the *XM3* is uncovered (remove the cover). Hold the remote programmer in the field of the *XM3* and push the (1) button while powering up the *XM3*. The Wiegand mode is now active.

*7.7.4.1   Set Wiegand format (42*N*)*

The Wiegand format can be activated by 42*N*, where N is 0-5 for one of the formats in the table below. The default value is 42*0*, being the HID standard 26 bits.

The table below shows the Wiegand formats which are supported by the *XM3*.

Format	RPG command	Number of XM3 Id output bits	Number of parity bits	Remarks
HID Standard 26 bits	42*0*	24	2	XM-2 compatible. Data is ID in BCD format; the most significant digit is send first. From a 44-bit XM-3 ID only the least significant 32 bits are send. No output about the card type.
HID Standard 34 bits	42*1*	32	2	No output about the card type.
HID Standard 37 bits	42*2*	35	2	No output about the card type.
HID Corporate 1000 35 bits	42*3*	32	3	No output about the card type
Cross Point 42 bits	42*4*	40	2	No output about the card type.
Cross Point 46 bits	42*5*	44	2	Output about the card type. Most significant 4 bits indicate the card type.

Remarks:
- Default setting is N = 0; HID Standard 26 bits.
- This function is only accessible on Installer level, using an Installer programmer.
- All HID, EM and Microchip ID carriers will, when presented to the *XM3*, create an output according to the selected Wiegand format.

7.7.5   Magstripe mode

Make sure that the tamper contact of the *XM3* is uncovered (remove the cover). Hold the remote programmer in the field of the *XM3* and push the (*) button while powering up the *XM3*. The Magstripe mode is now active.

7.7.5.1   Set Magstripe format (44*N*)

The Magstripe format can be activated by 44*N*, where N is 0-2 for one of the formats in the table below. The default value is 44*0*, being the Standard 9 digits.

The table below shows the Wiegand formats which are supported by the *XM3*.

Format	RPG command	Number of XM3 ID output bits	Remarks
Standard 9 digits	44*0*	32	XM-2 compatible. Data is ID in BCD format. Most significant digit is send first. From a 44 bits XM-3 ID only the least significant 32 bits are send. No output about the card type.
Cross Point 13 digits	44*1*	40	No output about card type.
Cross Point 14 digits	44*2*	44	Output about card type. Most significant 4 bits of these 44 bits indicate the card type.

Remarks:
- Default setting is N = 0; standard 9 digits.
- This function is only accessible on Installer level, using an Installer programmer.
- All HID, EM and Microchip ID carriers will, when presented to the *XM3*, create an output according to the selected Magstripe format.

7.7.5.2   Set number of start bits (leading zeros) (46*X*)

This function enables controlling the number of start bits (leading zeros) which precede the Magstripe frame.

X must be within a range of 1-255.

7.7.5.3   Set number of stop bits (trailing zeros) (47*Y*)

This function enables controlling the number of stop bits (trailing zeros) which follow the Magstripe frame.
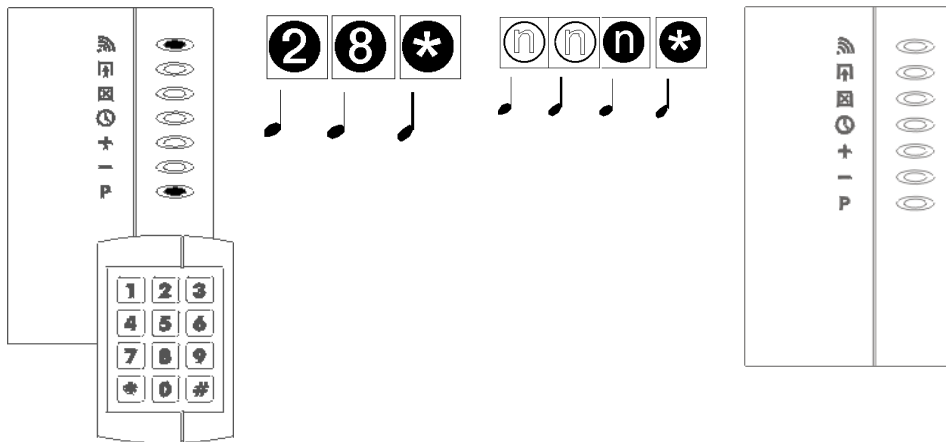
Y must be within a range of 1-255.

Remarks:
- These functions are only accessible on Installer level, using an Installer programmer.

7.8   Set RS485 address (28*)

This function can be used to set the address of the *XM3* (default: 0) when connected in a network. When the address is set, the *XM3* will switch to RS485 mode. To switch the *XM3* back to stand-alone mode, use the procedure described at the previous chapter under access mode.

Set RS485 address:

1. Program mode	2. Change address mode	3. Type new address (1-255)	4. RS-485 reader With address nnn

3. Resume	4. Normal operation
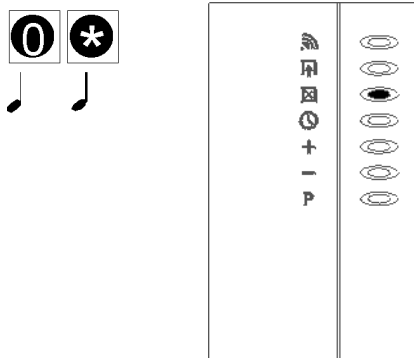
Remarks:
- The value of 'n₁, n₂ and n₃' must be within a range of 1 to 255.
- When a tag is presented while in RS485 mode only the read indication led lights up.
- After a certain period of no operation the *XM3* will generate an error tone, after which it will resume normal operation. This period known as Overall Time-out is by default set to 30 seconds.
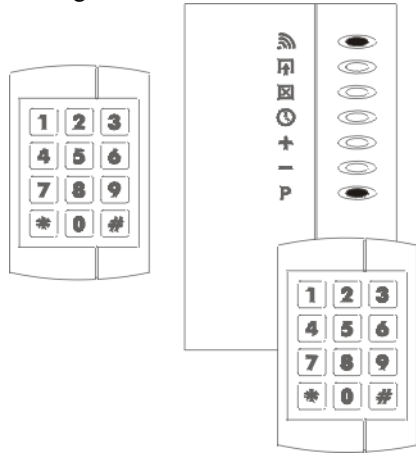
Possible errors:
None listed.

7.9   Add a Keypad (30*)

A keypad can be added to the *XM3* for use with PIN code option.
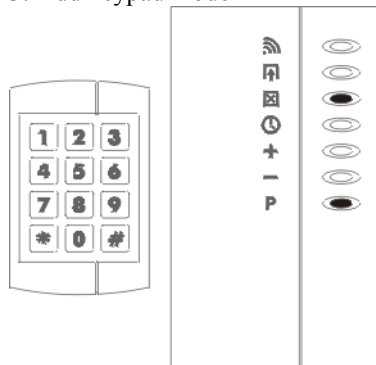
Add keypad:
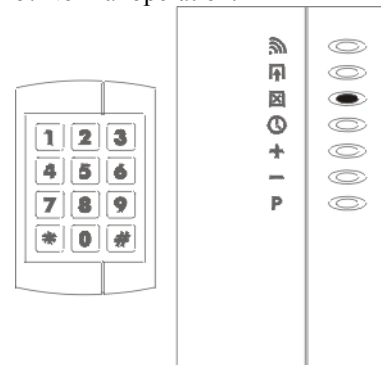
1. Program mode

2. Add keypad

3. Add keypad mode

4. Confirm keypad.

5. Normal operation.

Push on keypad.

Remarks:
- The installation of the keypad is an installer affair so an installer remote programmer is necessary.
- The keypad must be mounted in the field of the *XM3*.
- The keypad must be read into the *XM3*.
- The keypad will only work in stand-alone mode.
- The keypad options will only work for tags with the classification 'Normal user tags', 'Special user tags', 'Night lock only tags'.
- The keypad options will only work in access mode
- After a certain period of no operation the *XM3* will generate an error tone, after which it will resume normal operation. This period known as Overall Time-out is by default set to 30 seconds.

The keypad number can also be added to the *XM3* memory by using the (2*) option.
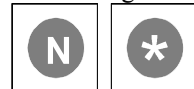
Add keypad:

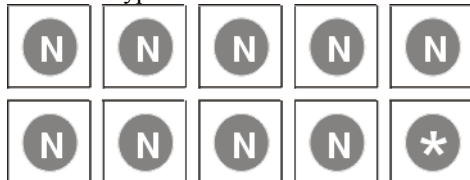1. Program mode.
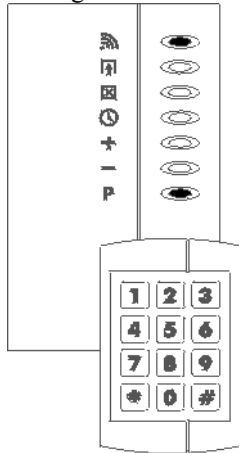
2. Enter add mode

3. Enter keypad level.

4. Enter tags sort.

4. Enter keypad number.

5. Exit add level.

6. Normal operation.
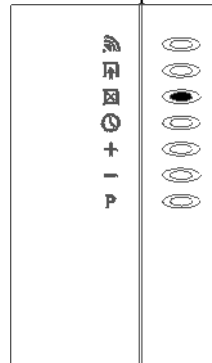
Remarks:
- Leading zeros of the keypad number do not have to be entered e.g. for keypad number (0042062) entering (42062*) is sufficient.
- Keep record of the keypad number. In case off a defect the keypad can be voided from memory by its number using remote programmer option (9*).
- After a certain period of no operation the *XM3* will generate an error tone, after which it will resume normal operation. This period known as Overall Time-out is by default set to 30 seconds.

7.10   XRP-2k PIN Keypad options (31*)

For the XM3 using a PIN keypad there are a few options.

7.10.1 Set XRP-2K alarm notification mode (31*1*)

1. Program mode
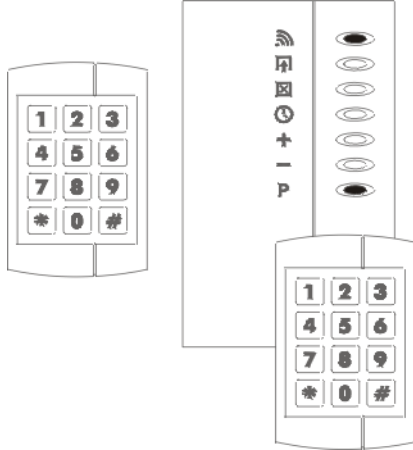
2. Enter keypad option mode

3. Enter alarm option

4. Normal operation

Remarks:

- The XRP-2K will send an intermittent ID to the *XM3*. This ID is unique and is send every 5 seconds.
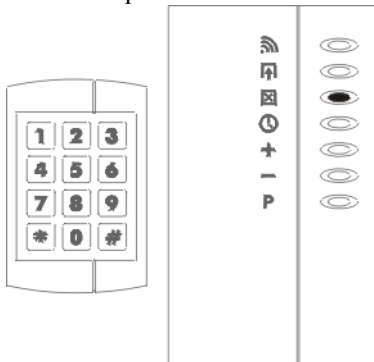- When The XRP-2K is taken out of reading distance from the *XM3* for more than 15 seconds and the intermittent ID is not seen by the *XM3* an alarm will go off and I/O3 will be activated. It is meant that an alarm device is connected to I/O3. When the XRP-2K is put back in the field of the *XM3* the alarm will stop and I/O3 will be deactivated.
- I/O3 is also the contact that is activated when the tamper switch is activated or when the door contact is molested.
- If there is a tamper alarm and a XRP-2K alarm, I/O3 will not be deactivated until both alarms are disabled.
- XRP-2K alarm option is only working on 'user Level'.
- When the (25*8*) option is enabled the alarm will go through I/O4 and not through I/O3.
- XRP-2K alarm option can be disabled with (30*0*).
- After a certain period of no operation the *XM3* will generate an error tone, after which it will resume normal operation. This period known as Overall Time-out is by default set to 30 seconds.
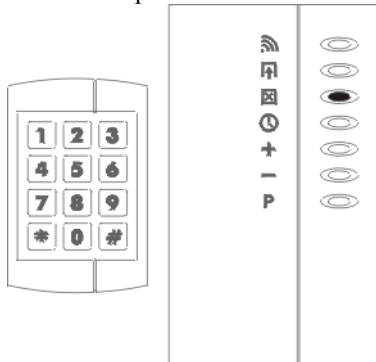
7.10.2 PIN code option (31*2*)

1. Program mode
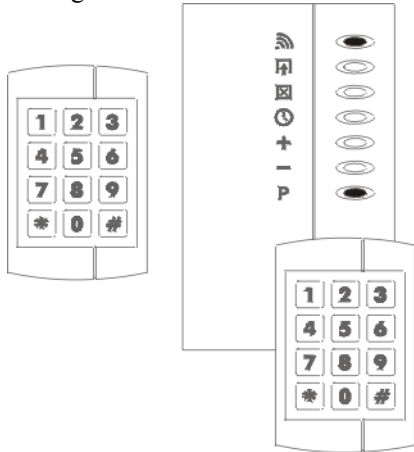
2. Enter keypad option mode

3. Enter PIN code mode

4. Normal operation.

Remarks:
- For every tag a random PIN code can be defined. Two tags can have the same PIN code.
- The only code that not can be used is the alarm code (see alarm code option).
- When a tag is voided the PIN code must be voided as well.
- The user has three attempts to gain access.
- When a PIN code is not entered correctly three times in a row, the tag will be blocked.
- The blocked tag can be made valid again by voiding the tag and then add it.
- When the PIN code option is disabled the blocked tags will not be valid.
- The PIN code will be seen as not complete if the time between presenting the tag and the first number of the PIN code is longer than the inactivity time (17*).
- The PIN code will be seen as not complete if during the process of identifying the PIN code another tag or programmer is presented to the XM3
- A PIN code that is not complete will not be seen as a wrong PIN code.
- The PIN code option can be disabled with (30*0*).
- After a certain period of no operation the *XM3* will generate an error tone, after which it will resume normal operation. This period known as Overall Time-out is by default set to 30 seconds.

7.10.3 Defining a PIN code (31*NNNN*)
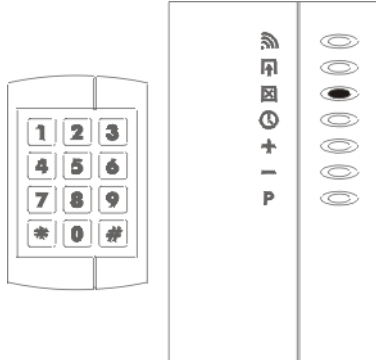
1. Normal mode 2. Present User Tag 3. Define PIN code.

User Tag
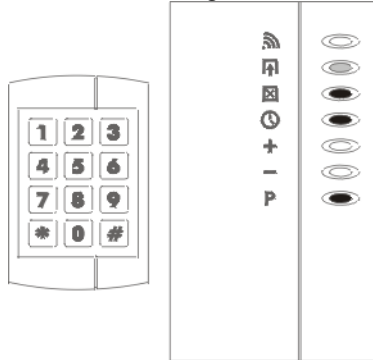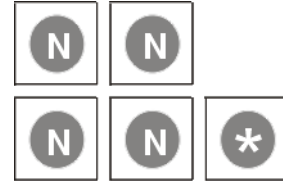
4. Verification mode. 5. Verification. 6. Normal operation.
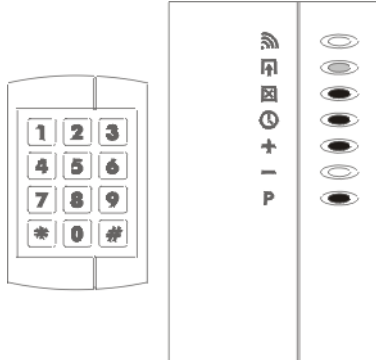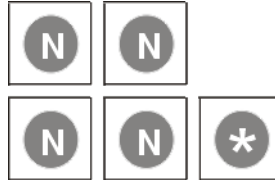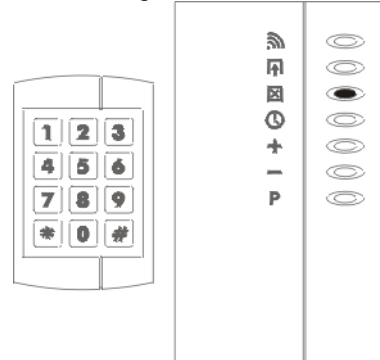
Remarks:
- Only the user of the tag can define the PIN code. It is not possible to enter a PIN code with a remote programmer.
- The PIN code must be defined the first time that the user presents the tag.
- When the PIN code mode is activated after tags have been added to the *XM3*, the users of those tags have to define a PIN code the first time they present their tag.
- After a certain period of no operation the *XM3* will generate an error tone, after which it will resume normal operation. This period known as Overall Time-out is by default set to 30 seconds.

7.10.4 Change PIN code option

A programmed PIN code can be changed by making use of the PIN code change code (see paragraph 18*).

Change PIN code:

1. Present user Tag.

User
Tag
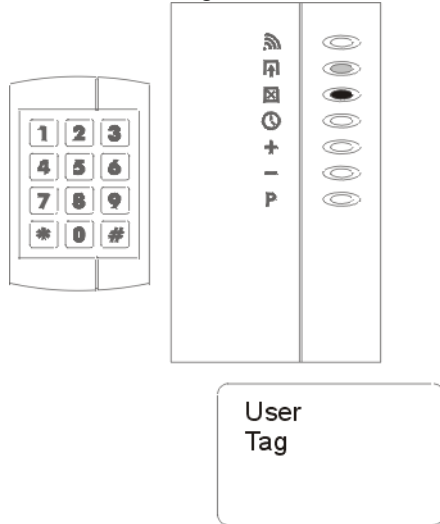
2. Enter PIN code change code

3. Enter old PIN code
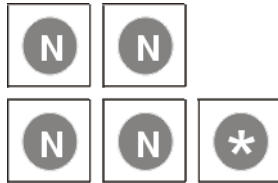
4. PIN code change mode.
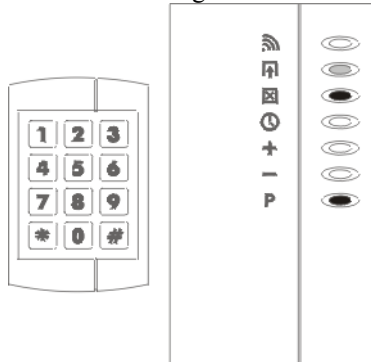
5. Enter new PIN code.
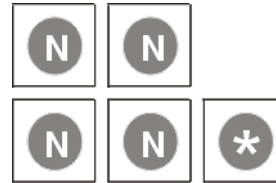
6. New PIN code mode
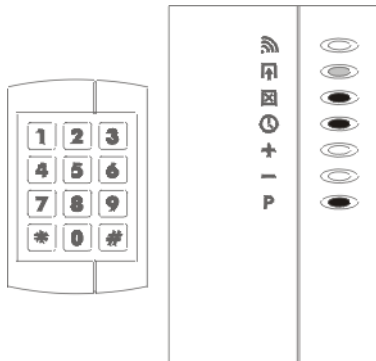
7. Confirm new PIN code.
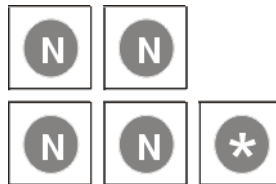
8. Confirm new PIN code mode.
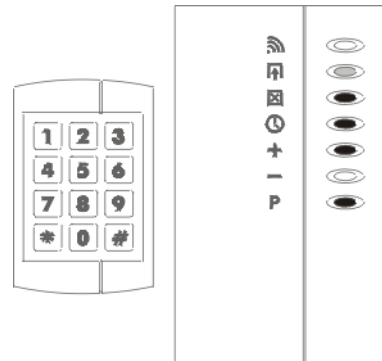
Resume normal operation.

Remarks:
- When in step 3 the wrong PIN code is entered, the *XM3* will resume to normal operation.

7.10.5 XRP-2K as user programmer (31*4*)

The keypad can be used as user programmer. In this mode all programs for users can be executed.

Set XRP-2K as User programmer:
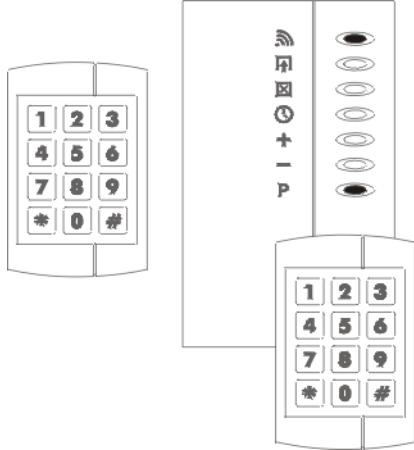
1. Program mode.   2. Set user programmer mode.   3. Normal operation.
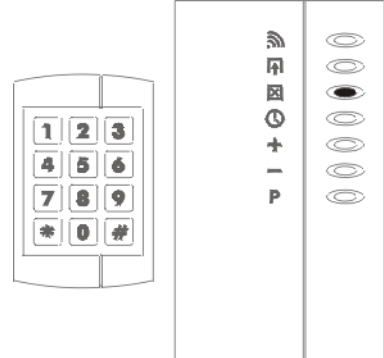
Remarks:
- By presenting a program master the user programmer mode will be activated.
- If a program master is presented more than one time to the XM3 and a button is pushed on the keypad, a failure will occur and the XM3 will resume normal operation.
- All user programmer codes can be used.
- After every used option the XM3 will return to access mode. For every new option the program master must be presented.
- Contrary to the real user programmer the keypad cannot be used to enter program mode.
- Program mode can be disabled with (30*0*).
- After a certain period of no operation the **XM3** will generate an error tone, after which it will resume normal operation. This period known as Overall Time-out is by default set to 30 seconds.

XRP-2K options can be combined by typing the sum of the various options:

Add values of 'n"

Set alarm notification mode	n = 0 when off	n = 1 when on.
Set PIN code option	n = 0 when off	n = 2 when on.
Use XRP-2K as user programmer	n = 0 when off	n = 4 when on.
Night time zone	n = 0 when off	n = 8 when on.
+		
		total = n

Example:

When the PIN code option and the alarm notification is used (31*3*) must be entered.

Remarks:
- The PIN keypad options can be disabled with (31*0*).

7.10.6 Time zones and PIN code option

The XM3 supports an option that makes it possible to have access with ID-carrier and PIN code only during the night time zone. This is built in as an extra security during the Night-time zone.
This function can be used to set the 'at-night-only' option for the PIN code option. The (31*8*) option is a toggle option, just like the other (31*n*) keypad options. See previous page.

Set PIN code option 'At night only':
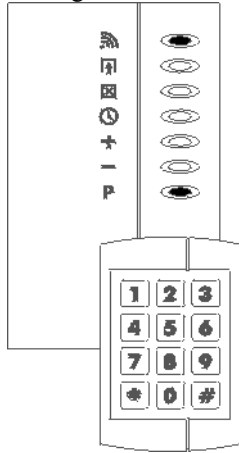
1. Program mode: 2. Change time zones for a weekday: 3. Normal operation:
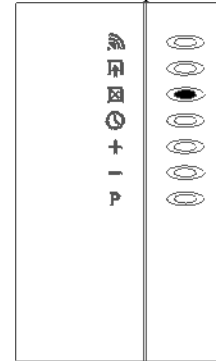
If set, the PIN code option is active in night lock mode only.
If not set, the PIN code option is active in both access mode and night lock mode.

Remarks:
- This option is only active when the PIN code option is enabled with (31*2*). If the PIN code option is disabled, the XM3 will never ask a user for its PIN code, regardless of the setting of the (31*8*) option.
- By default the PIN code is active in both access mode and night lock mode.
- This option can only be executed with an installer programmer on installer level.

8 EVENT LOGGING (33*)

The *XM3* supports three kinds of event logging modes that are specified in table 1.

Mode	Description
0	Event logging is disabled (default).
1	Always log events.
2	Log events only when in dynamic switch mode (22*) option and while the network is offline.

Table 1: Event logging modes

8.1 Set Event Log Mode (33*NN*)

1. Program mode:

2. Set event log mode:

Choose mode from table 1.

3. Normal operation:
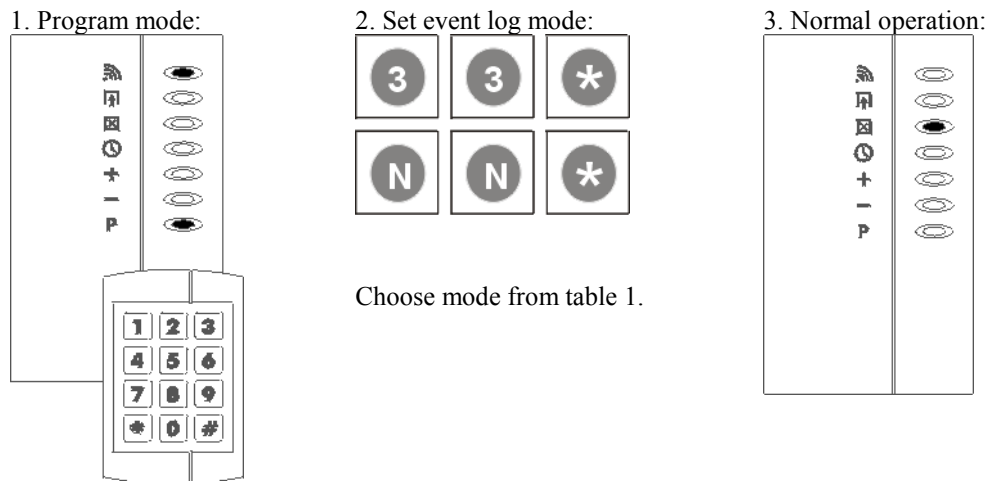
There are four event classes. For specification see table 2. These classes can be used separately or all together.

Security	Security related events. Examples: - Access to a specific ID was granted/denied - Tamper alarm was activated/deactivated - User was blocked after 3 attempts to enter the correct PIN code failed - Network interface was blocked after 3 attempts to enter correct user or installer password. - A user logged in via the network interface
Configuration	Configuration related events. A change to *XM3* configuration was made. (Change with non-volatile characteristic, i.e. change that remains effective even after powering of the *XM3*) Examples: - A system area parameter was changed - A CPA parameter was changed - A user was added to/voided from the user database - A user defined/changed its PIN code
Status	Status related events. Generated when a specific system status, error or exceptional situation was detected by the *XM3* firmware. Examples: - System startup (opening of event log) - An error was detected by the *XM3* firmware. The error was not fatal for continued normal operation of *XM3*. - A fatal error was detected by the*XM3* firmware. The *XM3* cannot continue its normal operation. Service/user intervention is required.
User	User defined events. Reserved for user extension.

Table 2.

8.2   Set Event Class (34*NN*)

Set event class:

1. Program mode:
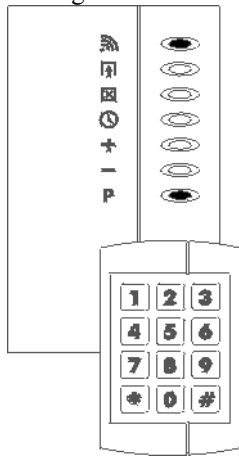
2. Set class:

Choose class or classes from table 3.

3. Normal operational
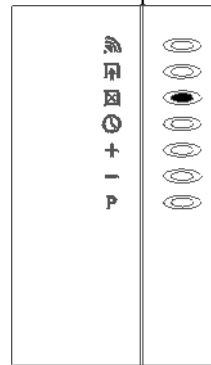
Event	Value
Enable logging of security events.	nn = 1
Enable logging of configuration events.	nn = 2
Enable logging of status events.	nn = 4
Enable logging of user events.	nn = 8
Read option, for reading event over network interface:	
Erase event record after reading.	nn = 16

Table 3.

By default logging of event classes is enabled.

The event logging classes can be used in any combination. When the options are to be combined, the individual values (nn) must be added.
For example, when security events and status events are used, the value must be 5 (1 + 4).

The **XM3** supports logging events as specified in table 4.

Event ID	Event data	Event class	Description
0	User ID	Security	Access was granted to user presenting ID carrier.
1	User ID	Security	Access was denied to user presenting unknown ID carrier
2		Security	Access was granted to user entering correct access code
3	User ID	Security	Access was denied to user entering incorrect access code
4	User ID	Security	Access was granted to user executing 1* menu option on remote programmer
5	User ID	Security	User entered invalid PIN code.
6	User ID	Security	User was blocked after 3 attempts to enter correct PIN code failed
7		Security	Network interface was blocked after 3 attempts to enter correctly
8			User or installer password failed
9		Security	Tamper alarm was activated
10		Security	Forced entry alarm was activated
11		Security	User entered alarm code on keypad
12		Security	Tamper alarm was deactivated
64		Security	Forced entry alarm was deactivated
65	Parameter ID	Configuration	System area parameter setting was changed
66	Parameter ID	Configuration	CPA parameter setting was changed
67	User ID	Configuration	User defined its code (first time)
68	User ID	Configuration	User changed its PIN code
69	User ID	Configuration	An user was added to user database
71	User ID	Configuration	An user was voided from user database
128	Level	Configuration	Users were voided from user database by level
144	Warning status specific information	Status	Warning events. Status events are not an error but just report a specific system situation. Logging of these events may be valuable for XM3 troubleshooting. The status specific information contains additional information about the occurrence of the situation, e.g. location in firmware where situation was detected, specific parameters etc.
160	Error status specific information	Status	Error events. The status specific information contains additional information about the occurrence of the error, e.g. location in firmware where error was detected, specific parameters etc.
161	Fatal error location	Status	Fatal error events. The status specific information contains additional information about the occurrence of the fatal error (location in firmware where fatal error was detected)

Table 4.

Remarks:
- Note that security related events will only be generated when the **XM3** is in access or night lock mode.

8.3   Erase event log (35*)

Erase event log:

1. Program mode: 2. Erase events: 3. Normal operation:

All events are being erased
from XM3
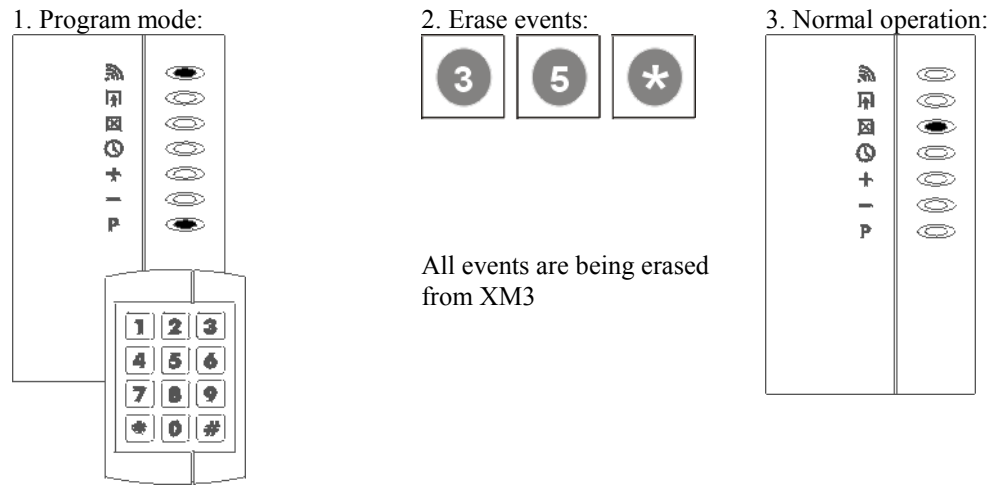
Event log access by an external host computer can be made through the RS-485 network interface with the functions as specified in table 5.

Function	Description
Get event log information	Returns information about the structure of the event log. The information includes: - Size of event log (total number of record entries in event log) - Structure of one event record. - Number of events currently in the event log
Read next event	Returns information about the next event in the event log. Includes option to clear the event log entry after transmission of event data, so that event is read only once
Erase event log	Erases all events in event log

Table 5: Network interface event log functions.

The information record that is logged in the event log for an event is fixed in size and shall be formatted as specified in table 6.

Field	Size	Description.
Time stamp	32 bit	Real-time clock stamp for time and date at which the event occurred
Event ID	8 bit	Event ID: identifies an event from Table 4. Most significant 2 bits will be used to indicate the event class of the event. So per class there is a maximum of 64 events.
Event data	48 bit	Event specific data, depends on event ID, see also Table 4

Table 6: Event log record format.

Remarks:
- The remote control programmer functions for event logging are all in the range of (20*-39*) and therefore can only be executed with a remote programmer on installer level.
- If the event log is full and a new event occurs that should be registered, the oldest registry is overwritten by the newest. This feature assures that the events in the event log are up to date, even in case of an event log overflow.
- After a certain period of no operation, the *XM3* will generate an error tone, after which it will resume normal operation. This period known as Overall Time-out is by default set to 30 seconds.

9   EVENT LOG DUMP PRINT

9.1   General

The *XM3* enables printing of all events that are logged. Therefore a serial printer must be connected to the *XM3*. For connections see Table 1.

XM3 pin settings	Signal name	Description
5,6	RS-485A	RS-485 Data – signal
7,8	RS-485B	RS-485 Data + signal
10,12	Ground	Signal ground

Table 1.

The XM3 uses the communication set up for the RS-485 interface as specified in Table 2.

Parameter	Value
Transmit/receive mode	Fixed to transmit mode.
Communication mode	Asynchronous
Baud rate	9600 baud
Character frame	8 data bits, no parity, 2 stop bits
Flow control	-None-

Table 2.

Remarks:
- The only external available *XM3* interface is the serial RS-485 interface. There are not enough I/O lines available for a parallel interface.
- In case of printers with a RS-232C interface a RS-232 to RS-485 converter must be used between the printer and the *XM3*.
- As the *XM3* has only one serial RS-485 interface, the other functions for this interface will have to be disabled for the period of time during which the printer is attached.
- In case of a printer requiring additional hardware (handshake) signals, e.g. CTS for a RS-232 interface, these hardware signals have to be realized directly on the printer, e.g. using discrete hardware. The *XM3* can not provide these signals.
- Some printers report errors (e.g. paper jam) or status (e.g. printer ready) information through dedicated hardware signals. As these signals cannot be connected to the *XM3*, the *XM3* will not be able to report such information to the user or interpret those signals itself (e.g. stop sending print data when a printer error occurs). Problems with the printer will therefore have to be detected and solved by the user itself.
- This serial communication setup is the default setup for most printers with a serial interface.
- This serial communication setup is fixed and cannot be changed.
- Fixing the RS-485 interface to transmit mode means that the RS-485 interface hardware will be setup for transmission of data mode for as long as event log dump printing is enabled with (50*1*) No switching between transmit and receive mode avoids line-turn-around time overhead. In other words: the interface is immediately ready for transmission of the next character.
- See chapter 'General remarks' for important remarks.

9.2 Set print line length (37*)

The print line length determines the number of characters that will be printed on one line.

Set print line length:

1. Program mode:
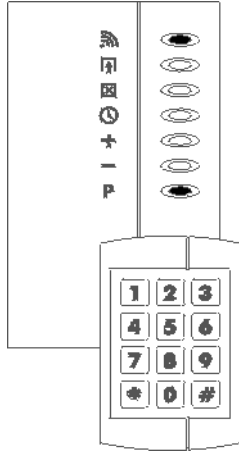
2. Enter print line length

3. Normal operation:
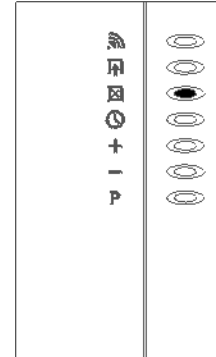
Table 1 shows the typical values that can be entered for the print line length.
Default setting is 16 characters.

Print line length	Value
Default	nn = 16
Other typical values:	nn = 24
	nn = 32
	nn = 40
	nn = 42

Table 1.

Remarks:
- See chapter 'General remarks' for important remarks.

9.3   Set print format (38*)

The print format determines the lay-out of the event information.

Set print format:
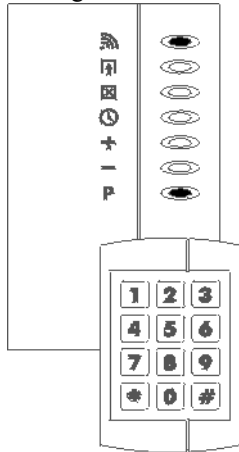
1. Program mode: 2. Enter print format choice   3. Normal operation:
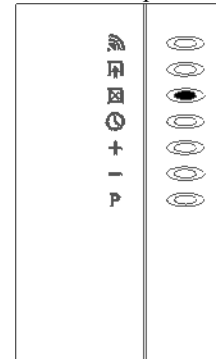
Table 1 shows the typical values that can be entered for the print format.
Default setting is short format.

Print format	Value
Short format	nn = 0
Long format (readable)	nn = 1

Table 1.

Remarks:
* See chapter 'General remarks' for important remarks.

9.3.1   Printout examples

Format description	Format layout is specified by…
Short format (default)	Figure 1
Long format	Figure 2

Table 2: Supported print formats

```
www dd-mmm-yyyy
hh:mm:ss eee nnnnnnnnnnnnnnnnnnnnnnnnnnnn
hh:mm:ss eee nnnnnnnnnnnnnnnnnnnnnnnn
hh:mm:ss eee nnnnnnnnnnnnnnnnnnnnnnnnnnnn
www dd-mmm-yyyy
hh:mm:ss eee nnnnnnnnnnnnn
```

Figure 1: Short print format

```
www dd-mmm-yyyy hh:mm:ss tttttttttttttttttttt nnnnnnnnnnnnnnnnnnnnnnnnnnnn
www dd-mmm-yyyy hh:mm:ss tttttttttttttttttttt nnnnnnnnnnnnnnnnnnnnnnnnnnnn
www dd-mmm-yyyy hh:mm:ss tttttttttt
www dd-mmm-yyyy hh:mm:ss tttttttttttttttttttttt nnnnnnnnnnnnnnnnnnnnnn
```

Figure 2: Long print format

Field	Size (chars)	Format	Range	Description
www	3	Text	*'Sun', 'Mon', 'Tue', 'Wed', 'Thu', 'Fri', 'Sat'*	Weekday
dd	2	Decimal number, with leading zero(s) if required.	*'01'.. '31'*	Day of month
mmm	3	Text	*'Jan', 'Feb', 'Mar', 'Apr', 'May', 'Jun', 'Jul', 'Aug', 'Sep, 'Oct', 'Nov', 'Dec'*	Month of year
yyyy	4	Decimal number, with leading zero(s) if required.	*'2000'.. '2136'*	Year
Hh	2	Decimal number, with leading zero(s) if required.	*'00'.. '23'*	Hours since midnight
Mm	2	Decimal number, with leading zero(s) if required.	*'00'.. '59'*	Minutes after the hour
Ss	2	Decimal number, with leading zero(s) if required.	*'00'.. '59'*	Seconds after the minute
eee	3	Decimal number, with leading zero(s) if required.	*'000'.. '255'*	Event number, refer to [SRD-EVENT] for more details.
tttttt	0.. 20	Text describing event.	-	Text is event specific.
nnnnn	0. 24	Format is event specific, see Table 2.	-	Event number, refer to [SRD-EVENT] for more details.

Table 1: Explanation of format fields

| Event data type	Size (chars)	Format	Range	Description
User ID	13	Decimal number, with leading zero(s) if required.	*'0000000000000'. '999999999999'*	13-digit decimal ID number as engraved on XM3 ID-carrier.
User ID	9	Decimal number, with leading zero(s) if required.	*'000000000'. '999999999'*	9-digitdecimal ID number as engraved on XM-2 ID-carrier.
User ID	0..24	Text	-	Name of user is found in user database
System parameter number	3	Decimal number, with leading zero(s) if required.	*'000'.. '255'*	Number of system area parameter
CPA parameter number	3	Decimal number, with leading zero(s) if required.	*'000'.. '255'*	Number of Cross Point Application parameter that was changed.
Level	2	Decimal number, with leading zero(s) if required.	*'00'.. '11'*	Hierarchical level as used for records in user database
RTC value	2	Date and time string, same format as in Table 1.	*dd-mmm-yyyy hh:mm:ss*	New date and time value for XM3 real-time clock.
Self-test number	3	Decimal number, with leading zero(s) if required.		Number of self-tests that failed.
Fatal error location	2	Decimal number, with leading zero(s) if required.	*'00'.. '99'*	Number indicating location in CPA software where fatal error was detected.

Table 2: Format for event data field

Remarks:

- Printing for each event is started on a new line and may extend more then one line. This is not shown in the figures above.
- Printout examples can be found in chapter H7.9.
- The short print format is intended for low-cost small paper width printers. It uses codes for indicating the events that occurred.
- The long format is more readable as it uses English texts for indicating events, not event codes.
- Gregorian calendar notation is used for time & date calculations and representations.
- Language for 'weekday' and 'month' fields is fixed to English language.
- With the short format the date is printed only in 2 situations:
  - When printing is first enabled with the (50*1*) command.
  - When the date of the next event to be printed is different from the date already printed before.
- All print formats can be used with all line lengths. If the length for a print line exceeds the installed line length (37*), the XM3 firmware will automatically insert a Carriage Return/Line Feed (CR/LF) pair forcing the printer to continue printing on the next line. (Not displayed in figures above).
- The format field notations used in the figures above are specified in Table 1 on the previous page.

9.4   Set print delay (39*)

The print delay specifies the length of the period of time the XM3 will wait after it has completed sending event information to the printer before it will send the next event information. This delay allows the printer to process and print the event information.

Set print delay:
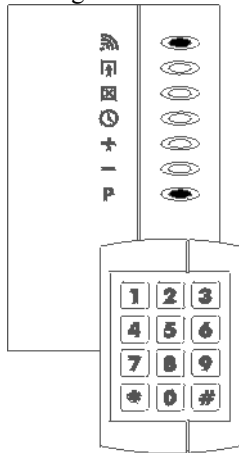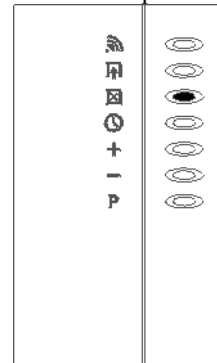
1. Program mode: 2. Enter delay time   3. Normal operation:

NNN = duration of delay in units of 10 mS (value must be within a range of 0-255).
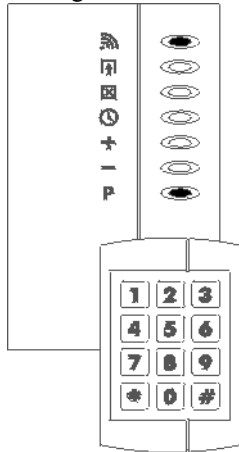Default value = 100, where the delay time is 1 second.

Remarks:
• See chapter 'General remarks' for important remarks.

9.5   Set event log dump printer options (40*)

This option enables various event log dump printer options (see table 1).

Set event log dump printer options:

1. Program mode: 2. Set event log dump printer options   3. Normal operation:
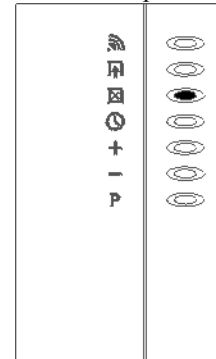
Table 1 shows the various event log dump printer options.

Event log dump printer options	Value
Printing of CR/LF characters at the end of each line	nn = 0; Print no CR/LF
	nn = 1; Print CR at the end of each line
	nn = 2; Print LF at the end of each line
Printing of user ID/user name in event data	nn = 4; Print user name (if defined)

Table 1.

Remarks:
- See chapter 'General remarks' for important remarks.

9.6   Set event print mode (50*)

This procedure specifies the mode for event printing.

Set event print mode:
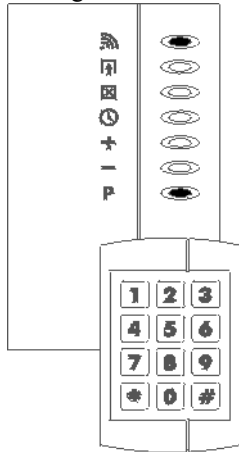
1. Program mode: 2. Set event print mode: 3. Normal operation:
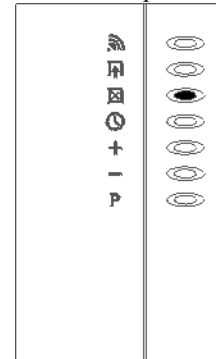
Table 1 shows the various event printing modes.

Event print mode	Value
Printing disabled	nn = 0
Printing events from the event log	nn = 1
Printing events from the event cache	nn = 2

Table 1.

Remarks:
- See chapter 'General remarks' for important remarks.

9.7   Define user name (51*)

9.7.1   Define a user name

This procedure defines a user name. The 13-digit ID number will be substituted by the user name on an event log dump print. This enables the user to add names per user in situations where this cannot be done using a temporary network connection, e.g. using laptop computer.

Define user name:

1. Program mode:
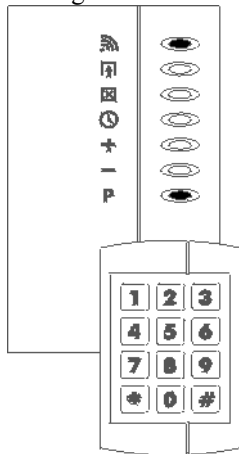
2. Enter user name:
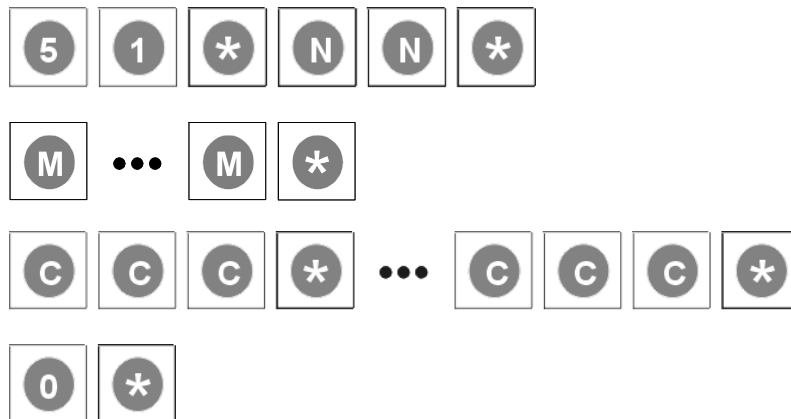
3. Normal operation:
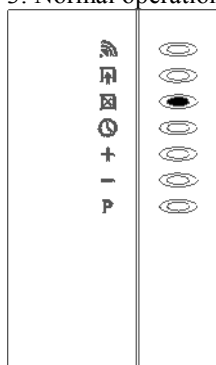
Value	Description
nn	Card type, see paragraph 5.3.
MM	ID- number (minimal 9, maximum 13 numbers).
ccc	Decimal value of the (ASCII) printable characters. Leading zeros are allowed.

Remarks:
- See chapter 'General remarks' for important remarks.
- Not supported for cards with facility codes (HID)

9.7.2 Delete a user name

This procedure deletes a user name from the event log.

Delete a user name:

1. Program mode: 2. Enter user ID to delete: 3. Enter tags sort.   4. Enter tags number

| **5** | **1** | ***** | | **N** | ***** | | **N** | **N** | **N** | ***** |

5. Confirm   6. Normal operation:

| **0** | ***** |
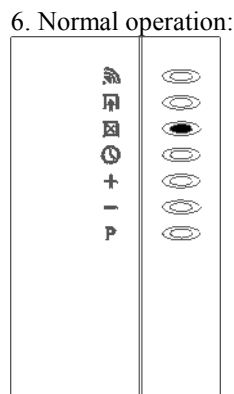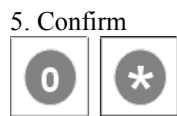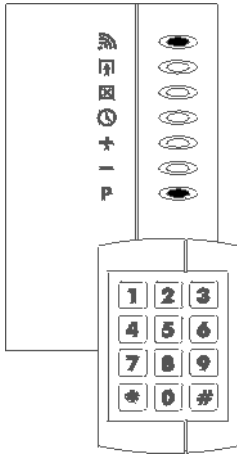
Value	Description
nn	9 or 13-digit ID of the user to delete.

Remarks:
- Because the Remote Programmer has no alphabetical keys this option is rather cumbersome. Option for adding/editing names via network connection is much user-friendlier, even for stand-alone mode configurations, and should be preferred.
- See chapter 'General remarks' for important remarks.

9.8   Important remarks

Remarks:
- All parameters are non-volatile, i.e. their value is maintained after (power on) reset.
- The (50*) option is accessible with user programmer. As no option entries are free in range (0* – 19*) and options in range (20* – 49*) are installer options that are accessible with installer programmer only, a new range of 'user options' is allocated. (Range = 50* - 59*)
- As long as the printing is not disabled with the (50*0*) command the XM3 will continue to print events until all events in the event log have been printed.
- By default printing of events from the event log is disabled. This is compatible with XM-2, which does not support the event log dump print functionality.
- Event printing mode 2 (50*2*) can be used to print events even if a file configuration is configured with the (26*) option that contains no event log. In case of event printing mode 2 events will be directly printed from the event cache.
- If event log dump printing in network mode is wanted, the bypass feature must be used first to switch to access mode. Additionally, before the (50*0*) option can be used to enable event log dump printing, the RS-485 network containing the host computer must be physically disconnected before the printer can be attached. This is required, because the printer will not support the Cross Point RS-485 communication protocol that is used by the host computer and/or the other XM3 unit(s) on the network. If the XM3 were not disconnected, transmission by the host computer and the other XM3 units would result in 'scrambled' character strings being printed on the printer.
- If the read option for the event log feature (34*) is not set to 'Erase event record after reading', the events will not be erased from the event log after printing. This means that after a (power on) reset of the XM3 the same events may be printed again if (50*1*) command is used to start event log dump printing.
- The print delay is intended for avoiding an overflow of the receive data buffer at the printer side. Such an overflow may otherwise occur as the XM3 does not support any software and/or hardware based handshaking mechanism for communications with the printer. Due to the relatively slow mechanical characteristics of the printhead of the printer the processing of data received from the XM3 will in most cases be significantly slower than the speed at which the XM3 is able to send new data.
- It is assumed that the receive buffer of the printer is large enough to hold at least the print data for one event.
- The XM3 does not implement an inter-character delay for transmissions of the print data through its RS-485 interface.
- All events in the event log will be printed. If printing of a specific class of events is not wanted, logging of events belonging to that class should be disabled with the (34*) command.
  Printing of events that are received in the event log is done on a first in first out base.
- The ASCII character set specification includes only characters in the range of 0x00 – 0x7F.
- All characters not mentioned in the table on the next page are considered printer-specific control characters, which may not be supported by all printers and will therefore not be generated by the XM3 firmware.
- Characters in the range of 0x80-0xFF can only originate from user specified name fields. For other fields printed by XM3 only characters in the range of 0x20-0x7F are generated.
- This means that all printed characters have the same character cell dimensions being width and height.
- If a non-proportional font is not the default printer font, the font will have to be selected manually at the time of installation. The XM3 firmware provides no features for selecting a specific printer font.
- The user ID event data field can be printed in 3 formats:
  - The 13-digit decimal number as engraved on an XM3 ID-carrier.
  - The 9-digit decimal number as engraved on an old XM-2 ID-carrier.
  - The name of the user.
  The name of the user will only be printed if all of the following conditions are met:
  - If the selected file system configuration includes the name file (26*).
  - If a name was defined for the user.
  - If printing of the user name is enabled (40*).
  In all other situations the user ID event data will be printed as a decimal number (see Table 1).
- Only the English language is supported for event texts.

Event ID (dec/hex value)	Text printed in long print format
0 / 0x00	'Access granted:'
1 / 0x01	'Access denied:'
2 / 0x02	'Access granted (access code):'
3 / 0x03	'Access denied (incorrect access code):'
4 / 0x04	'Access granted:'
5 / 0x05	'Incorrect PIN code:'
6 / 0x06	'User blocked:'
7 / 0x07	'Network interface blocked:'
8 / 0x08	'Tamper alarm activated:'
9 / 0x09	'Forced entry alarm activated:'
10 / 0x0A	'Alarm code entered:'
11 / 0x0B	'Tamper alarm deactivated:'
12 / 0x0C	'Forced entry alarm deactivated:'
64 / 0x40	'SA parameter changed:'
65 / 0x41	'CPA parameter changed:'
66 / 0x42	'PIN code defined:'
67 / 0x43	'PIN code changed:'
68 / 0x44	'User added:'
69 / 0x45	'User voided:'
70 / 0x46	'Users voided by level:'
71 / 0x47	'Real-time-clock set:'
128 / 0x80	'Event log opened:'
144 / 0x90	'Self-test failed:'
160 / 0xA0	'Invalid operational mode:'
161 / 0xA1	'Internal software error:'
162 / 0xA2	'Adding HRT failed:'

Table 1: Event texts for long print format

Manufacturer	Type/model	Remarks
Axiom	DP1014	Version with RS-232 interface.
Star	SP200-2	Version with RS-232 interface.

Table 2: Tested and approved printers

9.9 Printout examples

Following figures show some printout examples with various line lengths and print formats used.
A non-proportional printer font is used in the examples.

```
1234567890123456

Sat 01-jan-2000
22:02:03 000 Rob
ert Hulsebos
22:53:27 000 Ric
k Tjepkema
22:54:59 008
23:59:04 068 006
4433234235
Sun 02-jan-2000
08:29:17 000 Rob
ert Hulsebos
08:31:27 000 006
4433123499
```

Figure 1: Example printout; line length = 16, print format = short format

```
123456789012345678901234

Sat 01-jan-2000
22:02:03 000 Robert Huls
ebos
22:53:27 000 Rick Tjepke
ma
22:54:59 008
23:59:04 068 00644332342
35
Sun 02-jan-2000
08:29:17 000 Robert Huls
ebos
08:31:27 000 00644331234
99
```

Figure 2: Example printout; line length = 24, print format = short format

```
12345678901234567890123456789012

Sat 01-jan-2000
22:02:03 000 Robert Hulsebos
22:53:27 000 Rick Tjepkema
22:54:59 008
23:59:04 068 0064433234235
Sun 02-jan-2000
08:29:17 000 Robert Hulsebos
08:31:27 000 0064433123499
```

Figure 3: Example printout; line length = 32, print format = short format

```
1234567890123456789012345678901234567890

Sat 01-jan-2000 22:02:03 Access granted:
Robert Hulsebos
Sat 01-jan-2000 22:53:27 Access granted:
Rick Tjepkema
Sat 01-jan-2000 22:54:59 Tamper alarm
Sat 01-jan-2000 23:59:04 User added: 006
4433234235
Sun 02-jan-2000 08:29:17 Access granted:
Robert Hulsebos
Sun 02-jan-2000 08:31:27 Access granted:
0064433123499
```

Figure 4: Example printout; line length = 40, print format = long format
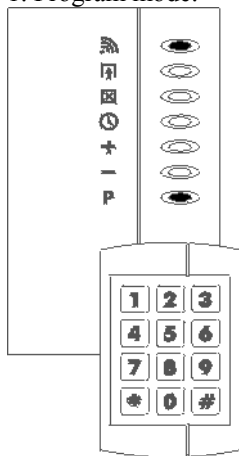
10 ANTI-PASSBACK (48*)

The anti-passback feature provides a build in extra safety. When a user obtained access the XM3 will temporarily disable the users tag for a certain time. This makes it impossible for the user to gain access obtain during this time. So the user cannot pass back his tag to another person to get also access. When this time is elapsed the user has the possibility to present his tag again to obtain access.

10.1 Set anti-passback mode (48*M*)

When the anti-passback mode is disabled, the user with a valid ID-carrier can have access at any time without restrictions. When the anti-passback mode is enabled after access is granted, a user's ID-carrier will be disabled for a fixed period of time.

Set anti-passback mode:

1. Program mode:
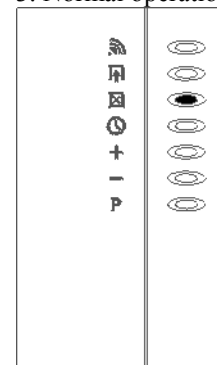

2. Set anti-passback mode:

Anti-passback mode disabled; M = 0
Anti-passback mode enabled; M = 1
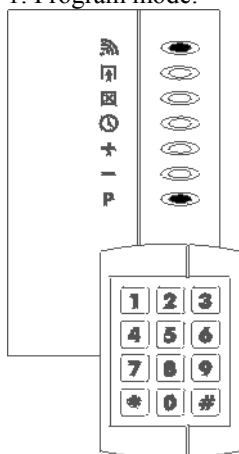
3. Normal operation:

10.2 Set anti-passback time (49*T*)

This function can be used to set the fixed time period an ID-carrier is disabled with anti-passback mode 1.

Set anti-passback time:
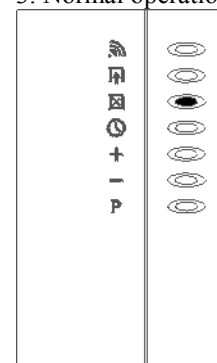
1. Program mode:

2. Set anti-passback time:

T = 1-254 minutes

3. Normal operation:

Remarks:
- The anti-passback time is fixed and is the same for all ID-carriers and starts at the moment when access was granted for the first time.
- The anti-passback time is accurate up to 1 minute and shall be at least the total number of configured minutes.
- The anti-passback feature is only applicable for tags with the hierarchical level 'Normal users', 'Special users' and 'Night lock only'. For all other Master tags and remote programmers the anti-passback feature will have no effect.
- The anti-passback feature applies only when in (stand-alone) access mode.
- The default anti-passback mode is 0 (disabled).
- The default anti-passback time is set to 5 minutes.
- The anti-passback options mentioned in table 1 can only be executed with an installer remote programmer on installer level.

10.3 Re-enable Users (58*)

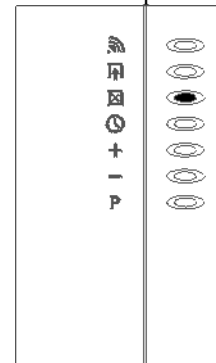This function enables all users that are currently disabled as a result of the anti-passback feature.

1. Program mode:
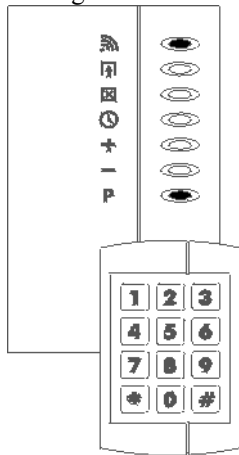
2. Re-enable users

3. Normal operation:

Remarks:
- This option does not disable the anti-passback feature. The anti-passback feature will still disable the next user that presents its ID-carrier.
- This option can be enabled with a user programmer at user level and an installer remote programmer at installer level.

10.4   Anti-passback in on-line configurations

In network mode the central host computer uses the RS-485 communication protocol for polling the *XM3* for the presence of an ID-carrier in the proximity field and for enabling/disabling the door lock. The *XM3* does not authorize users or grant access to users as is the case in stand alone access mode. The implementation of anti-passback in network mode therefore is a matter of software on the central host computer. The central host computer must implement a database including all users for all attached *XM3* units. It must also implement a timing mechanism for accounting anti-passback time for each user that is reported by one of the attached *XM3* units. In network mode the real-time clock of the *XM3* is not used for disabling and re-enabling ID-carriers. The time based enabling/disabling mechanism for anti-passback in network mode is implemented solely by the central host computer sending the applicable protocol messages for enabling/disabling the door lock for a specific user.

A special option is the dynamic switching option, where the *XM3* automatically switches from network mode to (stand-alone) access mode when a network failure is detected:

If anti-passback and dynamic switching are both enabled the *XM3* will automatically enable (local) anti-passback when a network failure is detected.

Remarks:
- In network configurations with more than one *XM3* units this means that all units will enable the anti-passback feature when the network goes down. As the central host computer in this situation can not coordinate anti-passback and the units cannot communicate with each other this implicitly means that the anti-passback is now really 'a local affair'. With each individual *XM3* unit access is limited to the anti-passback time installed for that *XM3* unit. However, a user can get multiple accesses within anti-passback time by presenting his ID to another *XM3* unit that is attached to the same troubling network. This would not be possible if the network were online.
- When the network is restored the *XM3* switches automatically back to network mode and the (local) *XM3* anti-passback feature is disabled again.

10.5   Enable anti-passback using *XM3* Manage

The anti-passback feature can also be activated using *XM3* Manage. In order to do so, the installer should go to the tab Parameters and then to 'anti-passback'. The feature can be enabled by setting the value to (1) and disabled by setting the value to (0).
The default time is 5 minutes, but can be changed in 'anti-passback time'. The value that can be chosen must be within the range of 1-254 minutes.

After the parameters are set push the apply button to save the new settings to the *XM3*.

11 TIME ZONES

The **XM3** Microproxs supports 2 time zones, called day-time and night-time, to enable time based access control schemes to groups of zero or more users. The time zones can be set in time frames of 24 hours. Each time zone has an active period, during which access shall be granted to a group of users, and an inactive period in which no access will be granted to the same group of users. The time zones cannot have an overlap in time.
When the time zones are set, they can be used every day of the week. This can be set for every day separately. When the day-night scheme for a weekday is disabled, **XM3** will remain in the night-time zone for the 24 hours of that day.
For instance: When the time zones are disabled for Saturday and Sunday. The **XM3** will go into night time zone on Friday night and will go into daytime zone on Monday morning.

The **XM3** will switch to night lock mode when the real-time-clock reaches the day-to-night-time marker. When the **XM3** real-time-clock reaches the night-to-day-time marker it will switch to access mode.

On the **XM3** can be seen in what time zone the **XM3** is. When LED 4 is off the **XM3** is in access mode. When LED 4 is on the **XM3** is in night lock mode.

The Night lock master can be used to overrule the **XM3** time zone that was activated by the time markers. When the night lock master is used to overrule the active time zone, the **XM3** will return to its normal time zone scheme when the real time clock reaches the next time marker.
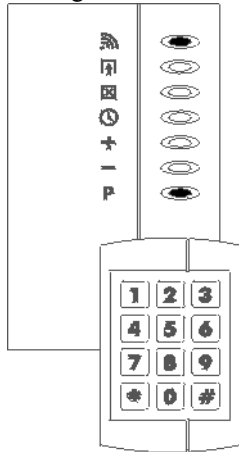
The time zone Options only apply for tags with hierarchical level 'Normal user', 'Special user' and 'Night lock only user'. For all other (master) tags and remote programmers the time zones will have no effect.
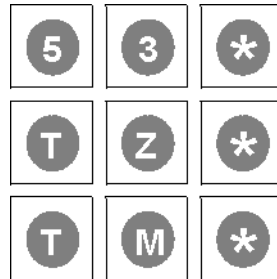
11.1 Set day-night scheme (53*)

This function can be used to set day-night scheme for real time clock based time zone switching.
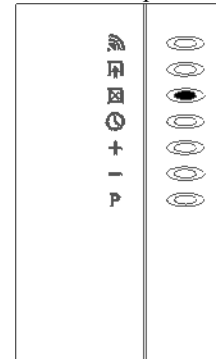
Set day-night scheme:

1. Program mode:

2. Set day-night scheme:

3. Normal operation:

TZ = Selected time zone
0 = Night-to-day time
1 = Day-to-night time

TM = Time marker for time zone that was selected with TZ

Time markers must be entered as 4-digit decimal numbers representing a 24 hour time stamp in the 'hhmm' format, e.g. 2359 = 23:59
The time markers indicate the first minute during which access in the respective time zone is possible. Setting day-night-time to 0800 and the night-day-time to 1700 means that day-time access is possible from 08:00 AM to 16:59 PM. Night access from 17:00 PM until 07:59 AM.

Remarks:
- Setting both time markers to 00:00 disables the real time clock based time zone switching. So one of the time markers must be unequal to 00:00 to enable the real time clock based time zones.
- Default value for both time markers is 00:00. This means that the real time clock based time zones are disabled.
- This option can only be executed with an installer programmer on installer level.
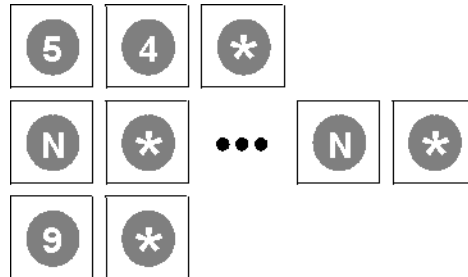
11.2 Change time zones for a weekday (54*)

This function can be used to enable/disable the day-night scheme that was set with the (53*) option for each of the seven days of a week.

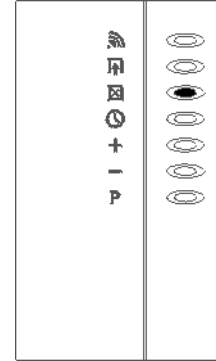**Change time zones for a weekday:**
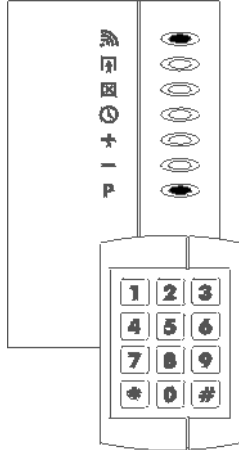
1. Program mode: 2. Change time zones for a weekday: 3. Normal operation:

N = Number of weekday for which day-night scheme is to be enabled/disabled in the weekday scheme.

The following numbers can be used:

- 0 = Enable/disable day-night scheme for Sunday.
- 1 = Enable/disable day-night scheme for Monday.
- 2 = Enable/disable day-night scheme for Tuesday.
- 3 = Enable/disable day-night scheme for Wednesday.
- 4 = Enable/disable day-night scheme for Thursday.
- 5 = Enable/disable day-night scheme for Friday.
- 6 = Enable/disable day-night scheme for Saturday.

Remarks:
- Enabling/disabling the day-night scheme for a weekday is a toggle option. E.g. Use (0*) to enable the day-night scheme if it is currently disabled. If (0*) is used again, the day-night scheme is disabled again, etc.
- The terminating (9*) command is used to indicate the end of scheme programming and will cause an exit from program mode.
- After entering (54*) on the remote programmer the current scheme for all weekdays is indicated on the LED's of the XM3. The uppermost LED indicates Sunday, the lowermost LED indicates Saturday. If a LED is on, the day-night scheme is enabled for the weekday. If a LED is off, the day-night scheme is disabled for the weekday.
- By default the day-night scheme is enabled for all weekdays.
- This option can only be executed with an installer programmer on installer level.

11.3 Time zones and PIN code option (31*8*)

The XM3 supports an option that makes it possible to have access with ID-carrier and PIN code only at the night time zone. This is built in as an extra security during the Night-time zone.
This function can be used to set the 'at-night-only' option for the PIN code option. The (31*8*) option is a toggle option, just as the other (31*n*) keypad options.

Set PIN code option 'At night only':
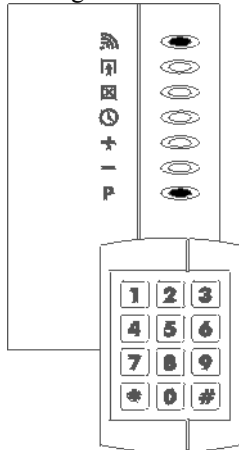
1. Program mode: 2. Change time zones for a weekday: 3. Normal operation:
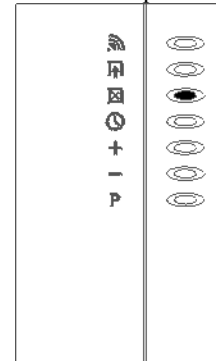
When the Pin code option is set, it is only active in night lock mode.
If not set, the PIN code option is active in both access mode and night lock mode.

Remarks:
- This option is only active when the PIN code option is enabled with (31*2*). If the PIN code option is disabled, the XM3 will never ask a user for its PIN code, regardless of the setting of the (31*8*) option.
- By default the PIN code is active in both access mode and night lock mode.
- This option can only be executed with an installer programmer on installer level.

12 TIME ZONES AND NETWORK MODE

In network mode the *XM3* is connected to a host computer. The on -line *XM3* will only function as a device that passes on the information of the user ID-carrier. The function 'Time zones' will not work when the *XM3* is in network mode. If the time zone option has to be used, the software in the host computer must be used to establish that. A special case is the dynamic switching option (when *XM3* Advanced is used) where the *XM3* automatically switches from network mode to (stand-alone) access mode when a network failure is detected.

Remarks:
- If Time zones and dynamic switching are both enabled, the *XM3* will automatically enable local real time clock based time zone functionality when a network failure is detected.
- When the network is restored the *XM3* switches automatically back to network mode and the time zone feature is disabled again.

12.1 TIME ZONES in *XM3* Manage

Time zones can also be activated by using *XM3* Manage at installer level.
Go to the tab Parameters and click on time zones. In this field the three different parameters can be set.
Firstset the day -to-night time parameter, e.g. 17:00. Then set the night-today time parameter, e.g. 08:00.
Finally set the days that should work with the time zone option.
These parameters can be activated by clicking the Apply button.

13 MISCELLANEOUS FUNCTIONS

The following programming steps, starting with (9), are intended for installation, diagnostics and testing purposes.

13.1 Show operation level (93*)

The Show Operation Level function is useful to determine whether the right level was set, specifically after installation when the level should be set to (0).

Show Operation level:

1. Program mode	2. Enter Show Option level mode	3. One of LED 2-6 displays current Operations level	4. Wait 1 second	5. Resume normal operation
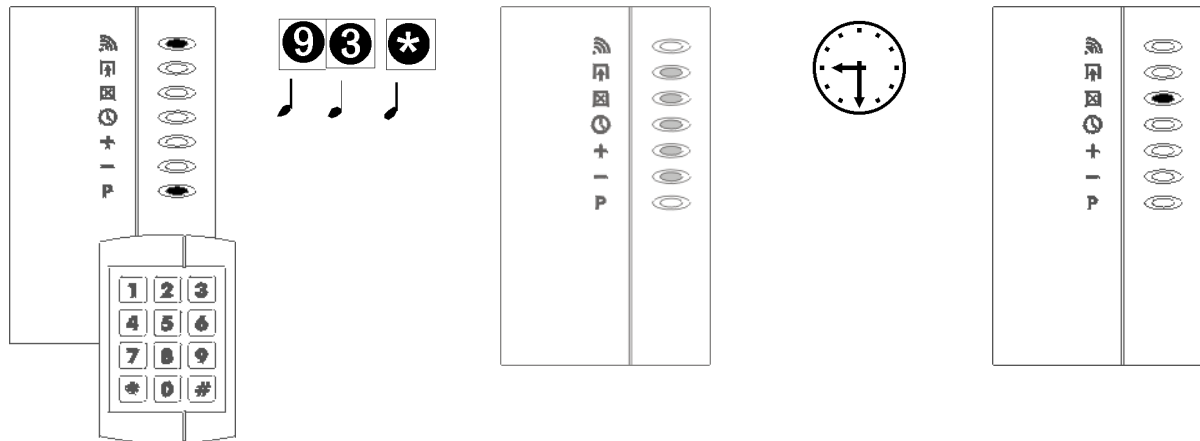
Outputs: Inactive
Inputs: Inactive

LED	Display of level
2	On: User level (level 0)
3	On: Installer level (level 1)

Remarks:
- After its installation, check whether the *XM3* has been set at level (0). If not, Remote Programmers intended for maintenance/backup might obtain illegal access.
- After a certain period of no operation the *XM3* will generate an error tone, after which it will resume normal operation. This period known as Overall Time-out is by default set to 30 seconds.

Possible errors:
- When presenting the Programmer an error tone sounds; the Programmer is unknown to the *XM3* or the 'protect' option was set.
- The *XM3* has been installed but doesn't read level (0); consult with your installer/dealer, since access through backup programmers might be obtained when not installed at level (0).

13.2 Show programmer level (94*)

The Show Programmer Level function reads the level at which the programmer in question was added to memory.
When more than one Programmer, and one or more *XM3's* are in use, it is recommended to use the Programmer at one and the same level. Also, a label indicating the function ('user', 'installer', etc.) and other pertinent information should be attached.
The Read Programmer operation can be used to reconfirm its level.

Show Programmer level:

1. Program mode	2. Enter Show Programmer level mode	3. One of LED 2-6 displays current Programmer level	4. Wait 1 second	5. Resume normal operation
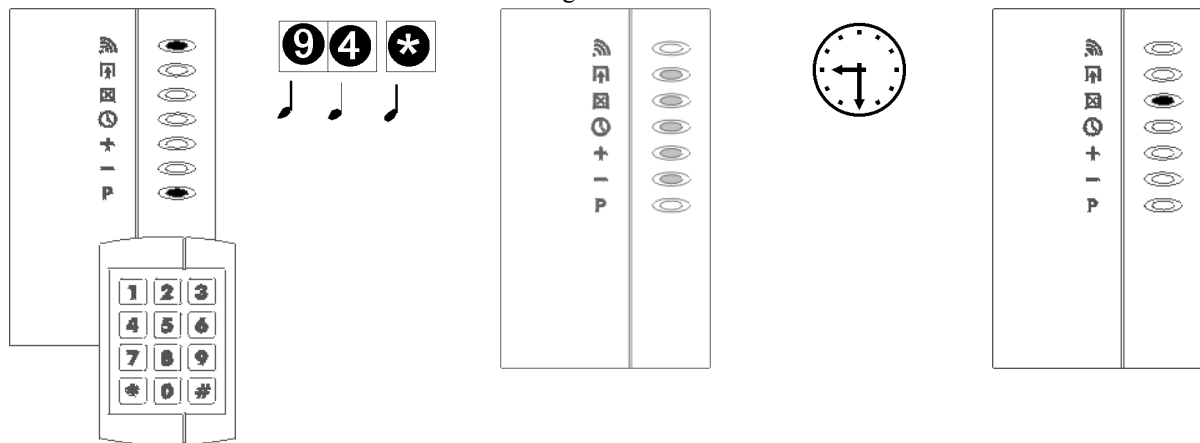
Outputs: Inactive
Inputs: Inactive

LED	Display of level
2	On: User programmer
3	On: Installer programmer

Remarks:
- After installation, check whether the programmer has been installed at level (0). If not, no access-related matters can be managed once the *XM3* is installed at level (0).
- After a certain period of no operation the *XM3* will generate an error tone, after which it will resume normal operation. This period known as Overall Time-out is by default set to 30 seconds.

Possible errors:
- When presenting the Programmer an error tone sounds; the Programmer is unknown to the *XM3* or the 'protect' option was set.
- The supplied Programmer should be at user level but does not read level (0); consult with your installer/dealer since no access related matters can be managed once the *XM3* is installed at level (0).

13.3 Retrieve system info (95*)

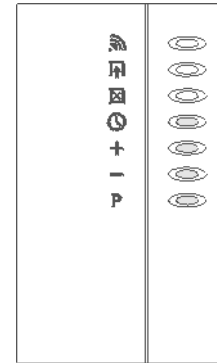This function retrieves the system info.

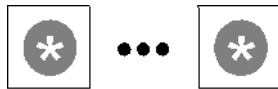**Retrieve system info:**

1. Program mode
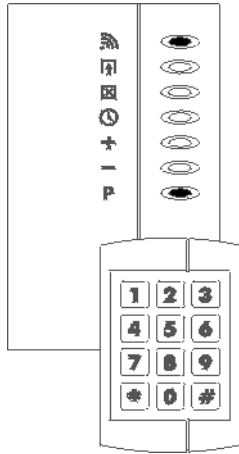
2. Retrieve system info:

3. LEDs show first digit of system info:

4. Show next digit:

5. Resume normal operation:
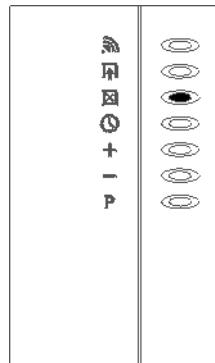
N= number of items for which information must be displayed.

0 = Serial number (10 digits)
1 = Hardware version (3 digits)
2 = Extension board type (3 digits)
3 = Extension board version (3 digits)
4 = Bootloader version (5 digits)
5 = OS version (5 digits)
6 = CPA version (5 digits)
7 = Current software configuration (3 digits)

All items are displayed in BCD format on the lowest 4 LED's of the XM3. Numbers are displayed using one BCD digit at the time. The XM3 will show one digit at the time. The (*) key on the remote programmer can be used to force displaying the next digit. With each digit the green LED will toggle (on/off) and a short beep will be generated. Pressing the (*) key after the last digit is shown the XM3 will return to its normal mode.

Table 1 shows the LED value in BCD format and the conversion to decimal numbers.

0	1	2	3	4	5	6	7	8	9

Table 1: BCD converted into Decimal.
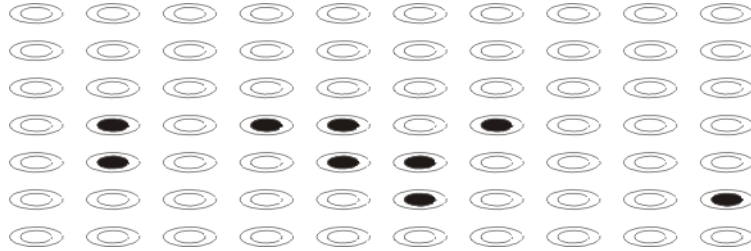
EXAMPLE

This is Number: 0301361004

Remarks:
- This option can be executed from both levels and both Remote programmers.

With this information Cross Point can determine whether the asked configuration switch is possible.

13.4 Diagnostics (98*)

A complete self-test to check on possible defects or faulty installation of the in/external functions of the *XM3* is initiated by Diagnostics.

Operation:

1. Program mode

Outputs: Inactive
Inputs: Inactive
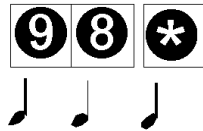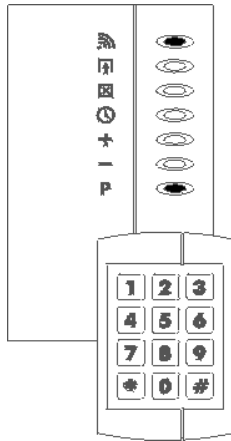
2. Enter Diagnostics mode

3. Relay test: only if not normal operation level

If Operation level > 0, trigger the relay **4x** for ¼ second at ¼ second intervals

Relay active (when not level '0')

4. LED test 2x. (Visual check; lights each LED (2-7) in sequence)

5. EPROM test 2x. Caution: do not switch off power in this step!
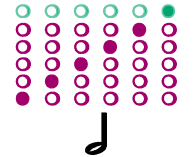
Alarm when error

6. I/O test (no display): only if not normal operation level

LED 2-7

If Operation level > 0: Output first logical 0 (off) then 1 (on)
- On I/O4 pin, test return values
- On I/O3 pin, test return values
- On I/O2 pin, test return values
- On I/O1 pin, test return values

Alarm when error

7. Read test start

8. Tag read test (use any tag)

Any tag

9. Remote Programmer Read Test
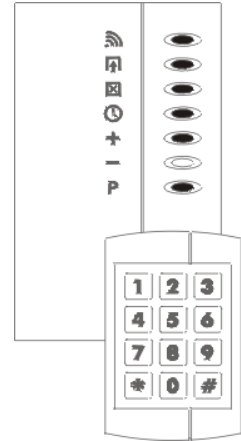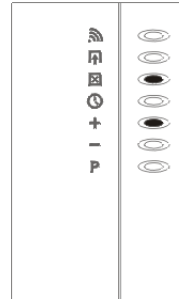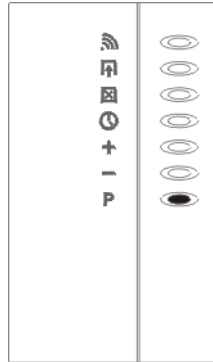
Outputs: I/O1 to I/O4 active in sequence
Inputs: I/O1 to I/O4 active in sequence
(when not at Operation level '0')

Outputs: inactive
Inputs: inactive

10. Keyboard input test
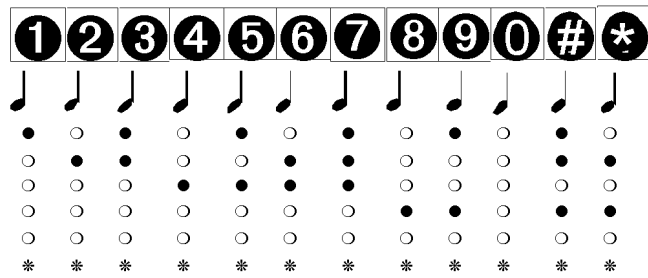
11. Resume normal operation

❶②③④⑤⑥⑦⑧⑨⓪#✱   ✱

♩	♩	♩	♩	♩	♩	♩	♩	♩	♩	♩	♩
●	○	●	○	●	○	●	○	●	○	●	○
○	●	●	○	○	●	●	○	○	○	●	●
○	○	○	●	●	●	●	○	○	○	○	○
○	○	○	○	○	○	○	●	●	○	●	●
○	○	○	○	○	○	○	○	○	○	○	○
✳	✳	✳	✳	✳	✳	✳	✳	✳	✳	✳	✳
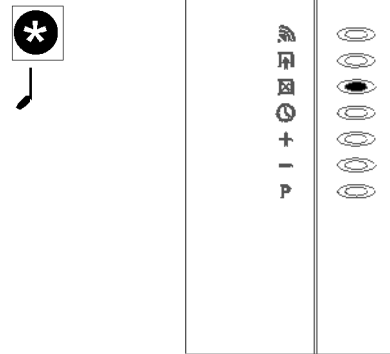
Outputs: inactive
Inputs: inactive

Remarks:
- If the XM3 is installed at level 0, the I/O test will be skipped as I/O conflicts may damage internal or external circuits. Caution: **never** connect external 'hard' potentials without pull-up or pull-down resistors.
- The relay test occurs only if a User Programmer is applied after installation to prevent unauthorized access.
- After a certain period of no operation the *XM3* will generate an error tone, after which it will resume normal operation. This period known as Overall Time-out is by default set to 30 seconds.

Possible errors:
- When presenting the Programmer an error tone sounds; the Programmer is unknown to the *XM3* or the 'protect' option was set (see Chapter 4).
- During a test an error tone sounds and normal operation resumes: the test failed. This can be in the EPROM test or the I/O test; the other tests provide audio/visual feedback. Check whether I/O1 and I/O2 are open (not connected).
- Test stops because anti-tamper was not covered.

13.5 Erase memory (99*)

The Erase memory function makes it possible to void entire groups of tags and Programmers from the *XM3* memory. To determine which group(s) must be erased, a so-called Erase level must be entered. All tags and Programmers at or below this level will be erased.

Erase memory:

1. Program mode   2. Enter Erase mode   3. Erase mode
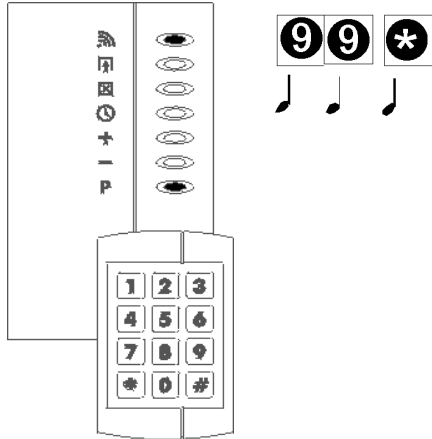
To proceed with erase:

4. Type the Erase level   5. Erasing (short beep for each erasure)   6. Resume normal operation
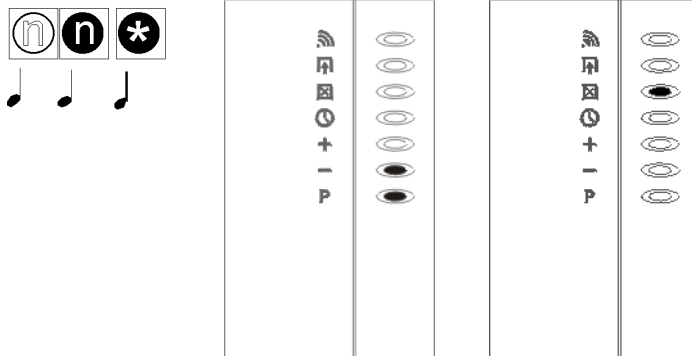
n_1 n_2	Programmer level, Erase level
11	Installer Programmer
10	User Programmer, Program Master
9	Void Master
8	Add Master
7	Night Lock Master
6	PIN keypad
3-5	Undefined
2	Status III Night lock tags
1	Status II special user tags
0	Status I, user tags

To cancel erase:

4.   5. Resume normal operation
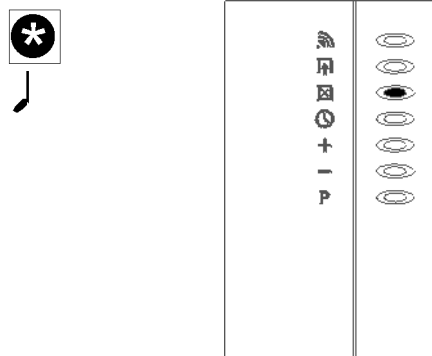
Outputs: Inactive
Inputs: Inactive

Remarks:
- It is not permitted to enter higher Erase levels than the Programmer is authorized for (see diagram).
- All tags and Programmers below the entered Erase level value will be voided from memory.
- After a certain period of no operation the *XM3* will generate an error tone, after which it will resume normal operation. This period known as Overall Time-out is by default set to 30 seconds.

Possible errors:
- When presenting the Programmer, an error tone sounds: the Programmer is not present in the *XM3* memory, or the 'Protect' option was set.
- After the Erase level is entered, an error tone sounds, and normal operations resumes; the presented Programmer is not allowed to erase at the entered level. See above diagram; check the Programmer's level.

XM3

MasterCard Section

14 MASTERCARD FUNCTIONS

14.1 *XM3* LED Indicators

The *XM3* has a row of (usually) seven LED's, which serve as status indicators. The first LED is yellow: this is the Read indicator and is always in use (except when disabled through user options). The second LED is green: this is the Access indicator. The other LED's indicators (3-7) are red.

Led 1 (yellow)	Read indicator
Led 2 (Green)	Access
Led 3 (Red)	Closed
Led 4 (Red)	Night Lock
Led 5 (Red)	Add
Led 6 (Red)	Void
Led 7 (Red)	Program
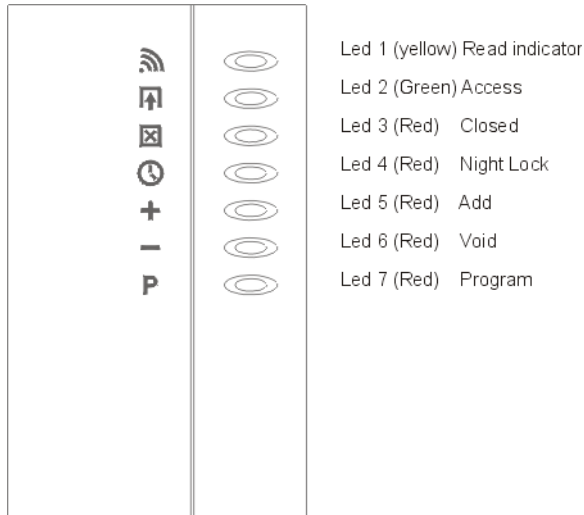
This manual describes the *XM3* procedure step by step, showing the LED readout after each step. The status of each LED can be either on, off, blinking, or unknown (on or off, depending on the situation), as follows:

Off   On   Unknown

The order of LED indicators is as follows:

LED1	Read	On when a tag or Programmer is within reading range, and being identified.
LED2	Open	On when door or gate is unlocked.
LED3	Closed	Indicates Access mode. On when door or gate is locked.
LED4	Night Lock	Night Lock mode.
LED5	Add	Add mode.
LED6	Void	Void mode.
LED7	Program	Program mode: when a Program Master or Remote Programmer is presented.

Sound:

In addition to the LED display, the *XM3* provides feedback by means off sounds:

A short beep (for example when a tag is read),

A long beep (to indicate recognition of a Master tag).

A few short beeps (in case of error)

Alarm beep (tamper alarm)

14.2 Contacts

The *XM3* offers two input and two output contacts, which can be used for interaction with external devices. By default the input contacts are set to inactive.

I/O1   Door Contact input
I/O2   External Night Lock control / Egress button input (normally open by default)
I/O3   Forced Entry output
I/O4   Night Lock Enabled output

Note: Refer to the Quick Guide for more details about the connection to external devices.

14.3 *XM3* operating and program modes

The *XM3* can be set to various modes of operation. In case of power failure, the current mode is memorized in EPROM.

- Access mode I   Basic access mode; allows access of normal user tags, with inactive Door Open contact.
- Access mode II   Basic access mode, with active Door Open contact.
- Night Lock mode   Access for Special User and Night Lock Only tags. No access for normal user tags.
- Sleep mode   The mode in which the *XM3* is shipped.

In addition a number of special modes and Program modes exist which can be activated with Master tags or Remote Programmers.

Basically two (non-exclusive) ways exist to operate the *XM3*:

1. Using tags only: in this case various Master Tags are used to control a limited set of options and maintenance functions.
2. Using a Remote Programmer: in this case one or more Remote Programmers are used to control the full *XM3* range of options and functions.

14.4 Master tag types

The *XM3* can be switched to various operating modes, by presenting Master tags or Remote Programmers. The following types of Master tags are recognized:

- Program Master
- Void Master
- Add Master
- Night Lock Master

- Remote Programmer

14.5 Presenting the tags

The best way to present the tag or the programmer to the *XM3* is shown in the pictures below.
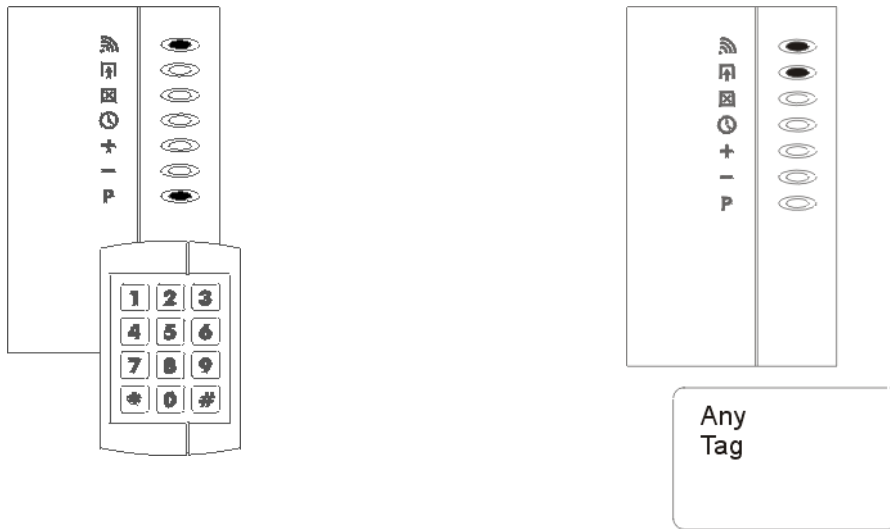
14.6 User tag status

User tags can have a status, related to the *XM3* operating mode (see Modes):

Status I - tags can be used in Access mode only
(Daytime user tag);

Status II - 'Special User' tags can be used both in Access mode and in Night Lock mode
(All time user tag);

Status III - 'Night Lock Only' tags can be used in Night Lock mode only
(Night time user tag).

14.7 Defaults

The **XM3** is normally shipped with a number of pre-set *defaults*. These default settings are:

Mode	:	Installer Sleep mode (level 1)
Door Close time-out	:	0 seconds (disabled)
Door Open Contact check	:	disabled
Open Time	:	2 seconds
Overall Time-out	:	30 seconds
Night Lock mode by external control	:	enabled
Operation mode	:	Access mode I (Private, Public and Regress switched off)
LED 1	:	Read indication enabled

15 MASTERCARD BASIC PROCEDURES

15.1 Wake up: declaring the Program Master

The supplier ships the *XM3* in Sleep mode. Sleep mode is shown by all LED's being lit, except for one that indicates the level at which the *XM3* was set to sleep mode.

If a User Remote Programmer is supplied refer to the Remote Programmer manual for the wake-up procedure. When powering up a *XM3* Reader for the first time at user level (5 red LED's on) the new *Program Master* has to be designated.
The Program Master may be regarded as a kind of master of Masters; it will be instrumental in enabling all other Masters and tags.

Subordinate to the Program Master are:
- Void Masters, used to delete (void) existing tag numbers from the *XM3* internal memory;
- Add Masters, used to add tag numbers into the *XM3* internal memory;
- Night Lock Masters, used to distinguish between access time zones.

This division of functions allows the implementation of complex security schemes, e.g. by dividing various Masters among different authorized persons.
This chapter deals with basic Master functions only to provide for a quick start-up. All other functions of the Program Master will be explained in the next chapter.

Wake-up operation:
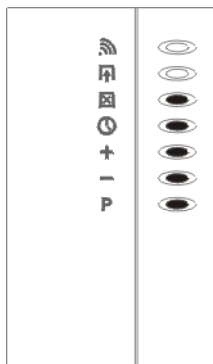
1. Power on   2. New Program Master   3. Access mode

New
Program
Master

Outputs: Inactive
Inputs: Inactive

Remarks:

- Any new tag can be chosen to serve as the Program Master
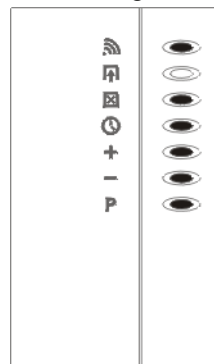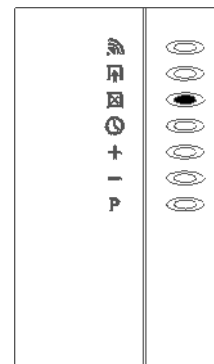- In case a mistake is made, the designated Program Master can be changed into another Program Master, e.g. one that is to be used on another *XM3.*
- For ease of management and security, the same Program Master can be used for all ID Readers when using more than one *XM3.*
- Clearly label the Master tags to avoid mistakes. The Program Master in particular can be regarded as the 'master key' to the whole security system, so be very careful with it, and store it in a secure place.
- Record the ID number of the Program Master. If it is lost, it can be voided from memory by its number using a remote Programmer. A new one can be added.
- If a Remote Programmer must be added while only Master tags are available, all memory must first be cleared at level 0.

Possible errors:

- The Program Master presented at Wake-up is not accepted; the *XM3* sounds an error tone and returns to the Wake-up mode: the Remote Programmer is not in memory. Note: in operational mode a Program Master can only be added by using the other Program Master that is already present in memory.
- If the *XM3* indicates Access mode or Night Lock mode from the start, the unit was not set to sleep mode. In this case the Masters may already have been added. Check whether any Masters are present by presenting any of the Masters to the XM3. If not, no memory management is possible; please contact your supplier.
- If a Program Master was designated previously and the XM3 was set to sleep mode by accident with a Remote Programmer the user can present the original Program Master to bypass the Wake-up mode.
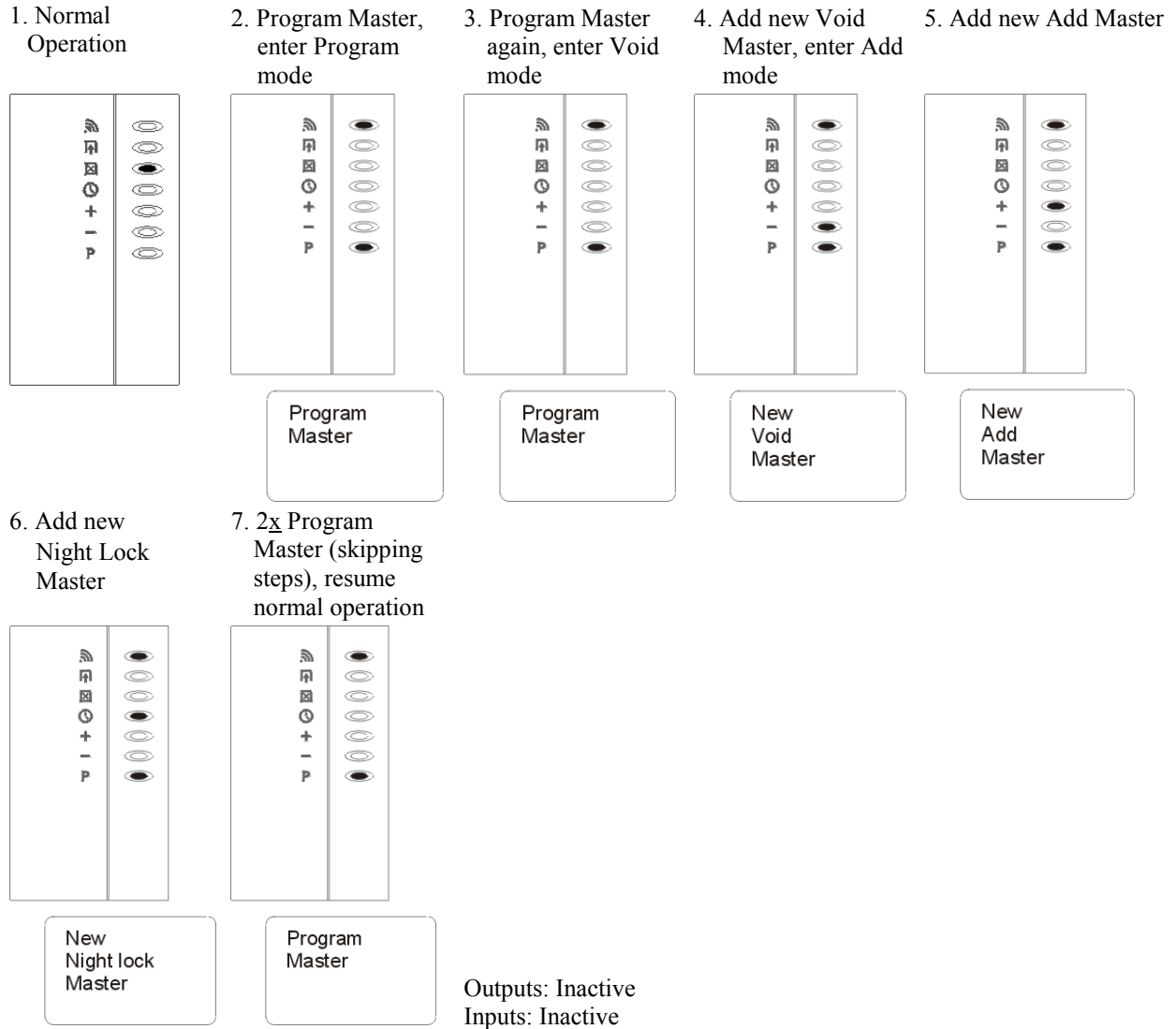
15.2 Program: adding the Void, Add and Night Lock Master

To enable access, user-tags must be added/entered into the internal memory of the *XM3*. Adding tags is initiated by means of an Add Master. The opposite: voiding (removing) numbers from memory is initiated by a Void Master. For the programming of the Night Lock mode a Night Lock Master is programmed. The procedure below describes the designation of the Void Master, Add Master and Night Lock Master.

<u>Caution:</u> **if the presented Masters are already present in memory, this procedure will void them.**

With the *XM3* in Program mode, the Program Master can be used to designate the Add and Void masters. Other functions of the Program mode are explained in Chapters 2 and 3.

Adding the Void, Add and Night Lock Master:

1. Normal Operation

2. Program Master, enter Program mode

   Program Master

3. Program Master again, enter Void mode

   Program Master

4. Add new Void Master, enter Add mode

   New Void Master

5. Add new Add Master

   New Add Master

6. Add new Night Lock Master

   New Night lock Master

7. 2<u>x</u> Program Master (skipping steps), resume normal operation

   Program Master

   Outputs: Inactive
   Inputs: Inactive

2 x

Remarks:

- Any tag which has not been designated as a Master can be added in this way.
- When using more than one **XM3**, for ease of management and best security, the user is advised to employ one and the same Program Master for these functions on all ID readers.
- Label the Add and Void Masters with their function to avoid mistakes.
- Keep records of the ID numbers and functions of all tags, and of the names of their users. In case of loss, tags can be voided from memory by their number, using a Remote Programmer.
- After a certain period of no operation the **XM3** will generate an error tone, after which it will resume normal operation. This period known as Overall Time-out is by default set to 30 seconds.

Possible errors:

- The tags presented, as Void, Add or Night Lock Master was already present in memory as such. In this case they will be voided. Repeat this procedure with the same tags.
- The **XM3** internal memory is full: Check the number of free positions. This can be checked by a Remote Programmer.
- After a certain period of no operation the **XM3** will generate an error tone, after which it will resume normal operation. This period known as Overall Time-out is by default set to 30 seconds.

15.3 Add mode: Adding new user tags

To enable recognition of the tags which are to be granted access by the *XM3* must first be entered into its memory.

The Add Master allows new tags to be added. After undergoing this procedure, the newly entered tags will be granted access by the *XM3* access mode, that is: when only the Closed LED is on.

Add new User tags operation:

| 1. Normal | 2. Enter Add mode | 3. Add new User tags (present each new tag) | 4. Add mode off, resume normal operation |
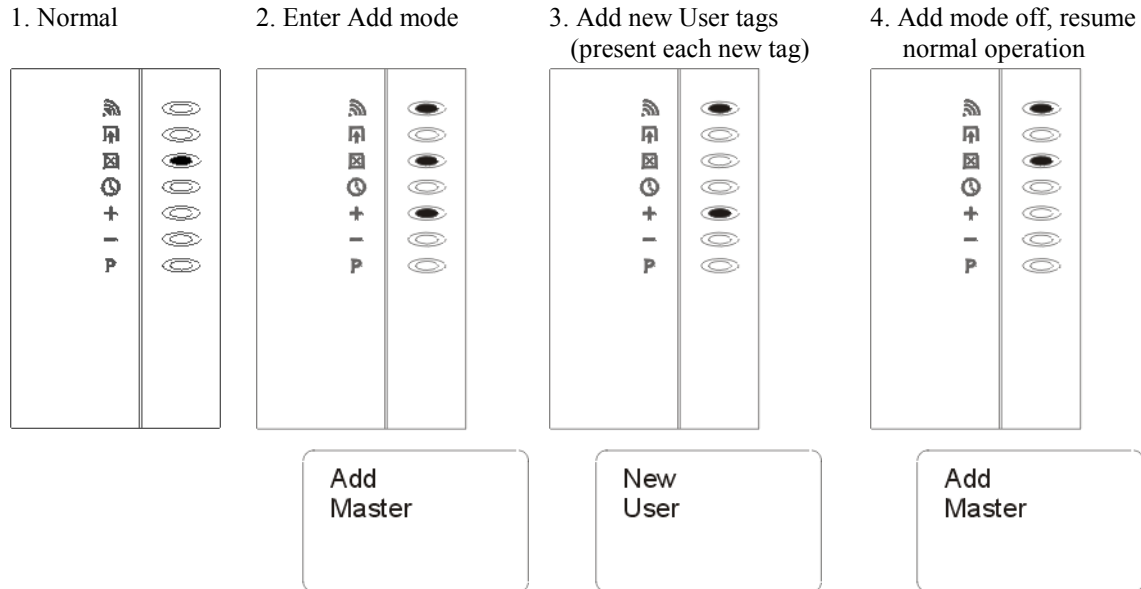
Outputs: Inactive
Inputs: Inactive

Remarks:
- Any tag can be added, except those that are already present in memory.
- The number of tags that can be added is MAX minus the number of Masters and/or Remote Programmers (3 minimum).
- Keep records of the ID numbers and functions of all tags and Programmers, and of their users. In case of loss, tags can be voided from memory by their number using Remote Programmer function (9*).
- After a certain period of no operation the *XM3* will generate an error tone, after which it will resume normal operation. This period known as Overall Time-out is by default set to 30 seconds.

Possible errors:
- The newly presented tag was already present in memory. Check the functionality of the tag. If necessary start again using another tag.
- The *XM3* internal memory is full. Check the number of free positions. This can be checked using a Remote Programmer.

15.4   Access mode I

Access mode I is the simplest mode of access.
In this mode the Door Open Contact check is inactive. This is default for the *XM3.*

Access 1 operation:

1. Normal	2. Access	3. Open Time	4. Resume normal operation

User
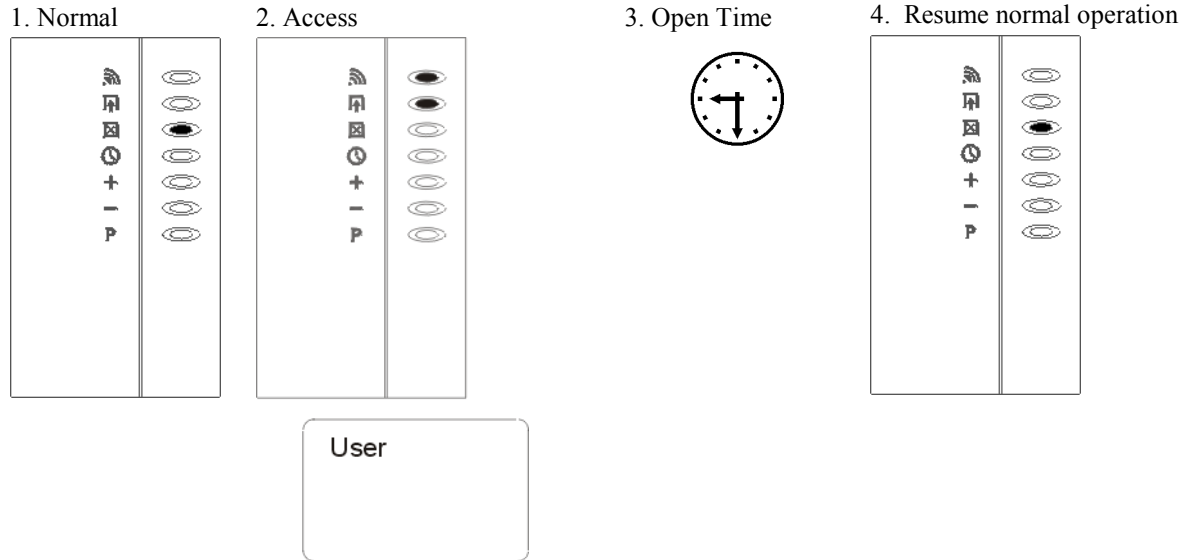
Outputs: Relay activated   Relay deactivated
Inputs: Inactive

Remarks:

- The Open Time is variable, and can be set with the Program Master (see Chapter 3.5).
- Besides Access Mode I and II, some other modes of operation are available such as private mode and/or public mode; refer to Installer Options.
- After a certain period of no operation the *XM3* will generate an error tone, after which it will resume normal operation. This period known as Overall Time-out is by default set to 30 seconds.
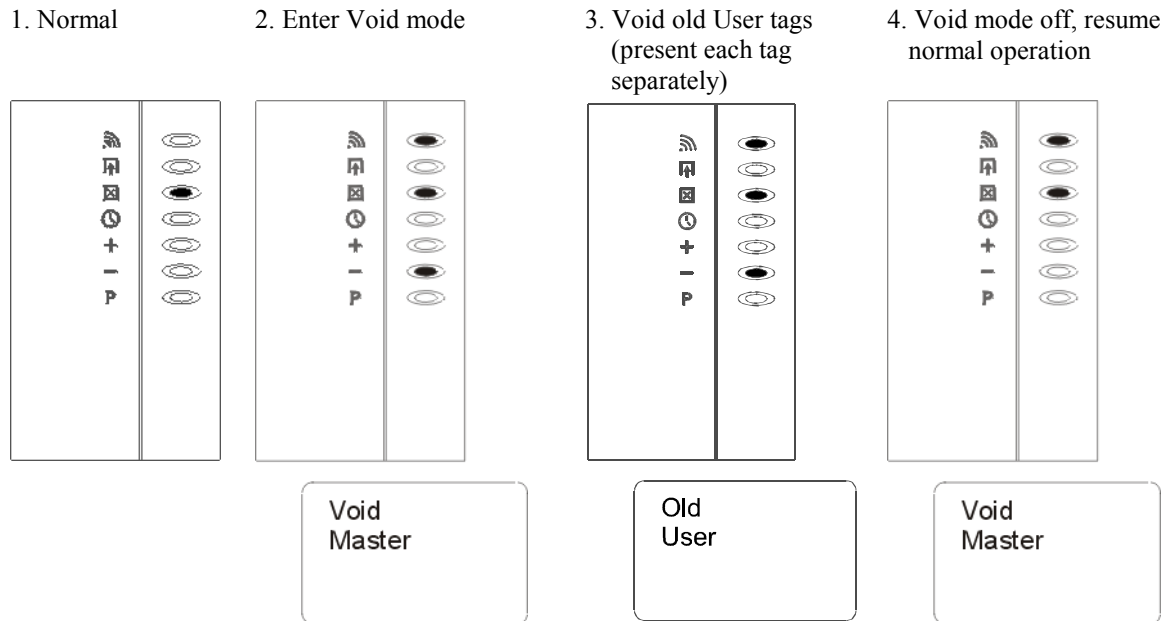
Possible errors:

- After presenting a tag, no access is granted, and an error tone sounds. Check whether the tag is present in memory. If so, check whether the *XM3* was set in the Night Lock mode. This is indicated by the Night Lock indicator (the fourth LED) being on. If not, the ID number is not present in memory as a tag number. Check for any restrictions made for the specific area; see also the Special User Tags section.

15.5 Void tags from memory

For the *XM3* to deny access to old, invalidated tags, they must be voided from memory. The Void Master is used to remove old tags from memory, and thus clearing the memory space they occupied. The cleared memory space can be used for other tags. After this procedure the old, voided tags will no longer be granted access.

Void tags operation:

1. Normal	2. Enter Void mode	3. Void old User tags (present each tag separately)	4. Void mode off, resume normal operation

Void Master

Old User

Void Master

Outputs: Inactive
Inputs: Inactive

Remarks:
- Any tag number in memory can be voided this way, except those that were designated as Master (to avoid mistakes).
- Record the number of the voided tag and the name of the user.
- After a certain period of no operation the *XM3* will generate an error tone, after which it will resume normal operation. This period known as Overall Time-out is by default set to 30 seconds.

Possible errors:
- The presented tag number was not present in memory. Confirm this, if necessary, by checking its function in normal mode: if unknown, an error tone will be heard.
- The presented tag was already present in memory as a Master; confirm this, if necessary, by checking its function in normal mode. If such a Master tag is presented, the Closed LED, together with the Night Lock, Add, Void or Program LED should light up, indicating that the *XM3* has been switched to the corresponding mode. This can be undone by presenting the Master tag again.
- To ensure access at all times, after a certain time of inactivity while in Void mode (set to 30 seconds as default time-out), the *XM3* sounds an error tone, and resumes normal operation.

16 MASTERCARD ADVANCED PROCEDURES

16.1 General

The *XM3* has built in advanced functions, which can also be activated by presenting Master Cards. This chapter describes the advanced Master tag procedures for user access and memory management.

Each Programming function is described here separately. However, during programming with a Program Master, any sequence of the following programming functions can be executed without leaving Program mode:
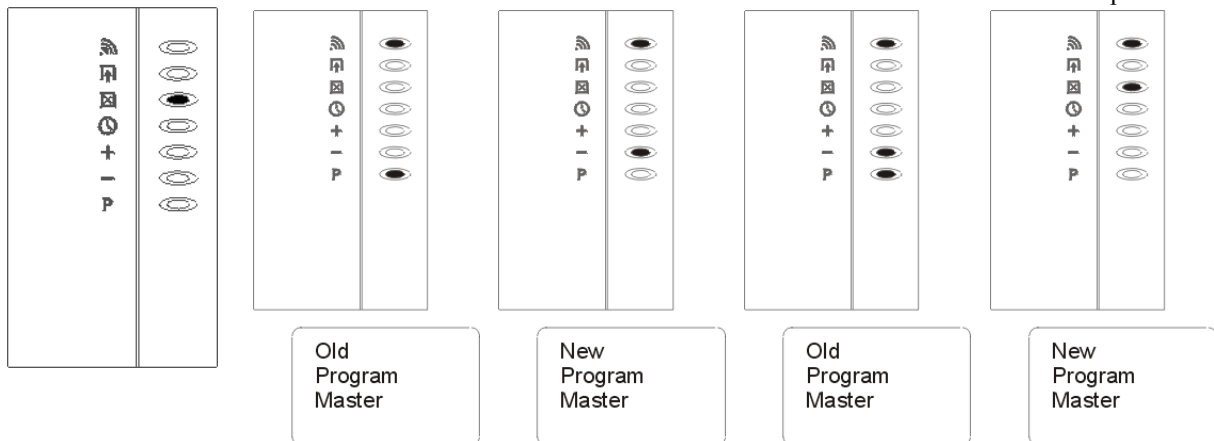
- Change Program Master
- Night Lock mode
- Add an Add Master, Void Master or Night Lock Master
- Void an Add Master, Void Master or Night Lock Master
- Set Close Time-out
- Set Open Time-out

16.2 Change Program Master

It is possible to transfer the function of the current Program Master to another tag. The old Program Master is thereby voided from the *XM3* memory, and the new tag is designated as Program Master instead. This can be done when another Program Master than the desired one was added to memory during Wake-up.

Change Program Master operation:

1. Normal	2. **'Old'** Program Master, enter Program mode	3. **'New'** Program Master, added	4. **'Old'** Program Master voided	5. **'New'** Program Master **5x** (skip steps), resume normal operation

Outputs: Inactive
Inputs: Inactive

Remarks:
- Any tag can be designated as a new Program Master, except Master tags that are already in the memory of the *XM3.*
- If the new Program Master is already known as Program Master, the old Program Master is not voided.
- When using more than one *XM3* for ease of management, use the same Program Master on all readers.
- If the wrong tag was designated as new Program Master, finish the procedure as indicated and then repeat the procedure with the correct tag.
- Clearly label the new Program Master to avoid mistakes.
- Keep records of the ID numbers and functions of all tags and of the names of their users. In case of loss, tags can be voided from memory by their number, using a Remote Programmer.
- After a certain period of no operation the *XM3* will generate an error tone, after which it will resume normal operation. This period known as Overall Time-out is by default set to 30 seconds.

Possible errors:
- The tag presented as the new Program Master was already present in memory as another Master. Check the functionality of the Master. You may have to use a different tag.
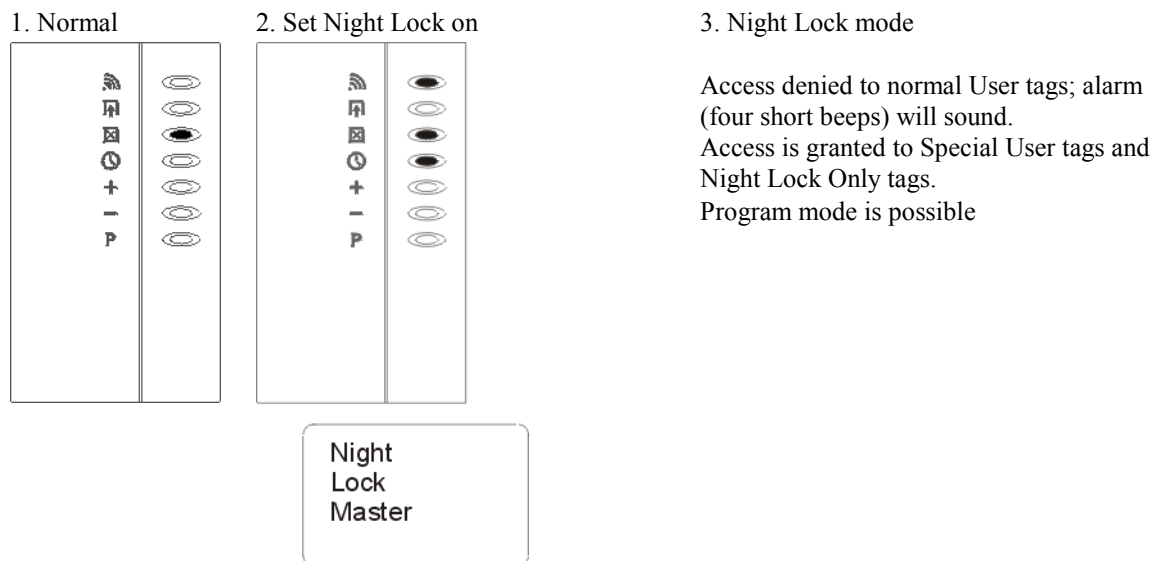
16.3   Night Lock mode

The *XM3* has a special Night Lock mode in which the normal tags are denied access. In this mode access is granted to Special User tags and Night Lock Only, but not to normal User tags. This mode can be used to distinguish time zones, for example office hours and non-office hours.

When a tag is presented while the Night Lock mode is active the *XM3* triggers an output contact (assigned as I/O4). This output contact is intended for external control, for example to switch on an external alarm system or to control the mains for switching on lighting or other electrical devices.

16.3.1 Set Night Lock mode

Night Lock mode can be switched on and off by a Night Lock Master or by an external timer. Once the Night Lock mode is set, a Night Lock Master can be used to obtain access while resetting to Access mode.

Set Night Lock on operation:

1. Normal   2. Set Night Lock on   3. Night Lock mode

Access denied to normal User tags; alarm (four short beeps) will sound.
Access is granted to Special User tags and Night Lock Only tags.
Program mode is possible

Night Lock Master

Outputs: I/O4 activated   I/O4 active
Inputs: Inactive.

Remarks:
- In case of power failure or surge, the *XM3* will memorize the current status of the Night Lock.
- Tags that are added while the *XM3* is in the Night Lock mode are entered in memory as Special User tags, to be permitted access both in Night Lock mode and in normal access mode.
- Tags that are added by means of a Remote Programmer, as Night Lock Only tags, are allowed access in Night Lock mode, but denied access in normal access mode.
- After a certain period of no operation the *XM3* will generate an error tone, after which it will resume normal operation. This period known as Overall Time-out is by default set to 30 seconds.

Possible errors:
None listed.

16.3.2 Switch off Night Lock mode

The Night Lock Master can be used to switch off Night Lock mode and obtain access at the same time. Because it combines these functions its bearer does not need to carry two separate tags.

The Night Lock Master is intended for convenient use by person(s) who are authorized to enable access for others, for example to unlock an office building in the morning, so personnel with a user tag can enter.

The Night Lock triggers an output contact intended for control of external devices, e.g. to switch off an external alarm system or to control the mains for lighting or other electrical appliances.

Night Lock mode can also be switched on and off by an external timer.

Switch off Night Lock operation in user mode:
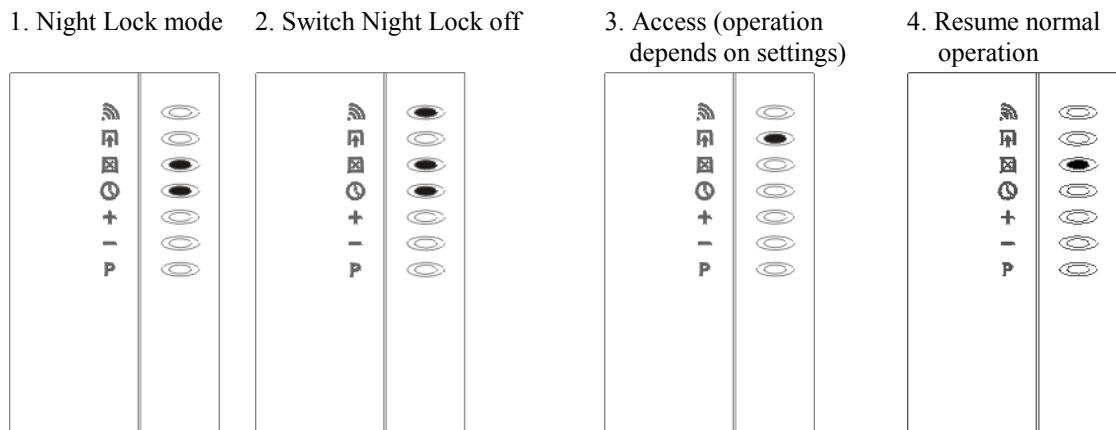
1. Night Lock mode   2. Switch Night Lock off   3. Access (operation depends on settings)   4. Resume normal operation

Night
Lock
Master

Outputs: I/O4 active   I/O4 deactivated
Inputs: Inactive.

Remarks:
- In case of power failure or power surge the *XM3* will memorize the latest status of the Night Lock.
- After a certain period of no operation the *XM3* will generate an error tone after which it will resume normal operation. This period known as Overall Time-out is by default set to 30 seconds.

Possible errors:
None listed.

16.3.3 Set Night Lock mode by external control

The Night Lock Master can be used to control normal operation and Night Lock manually. However, external (automatic) control has been provided for as well. This can be useful in situations where control of the Night Lock by a Master is not practical, or where use of the Night Lock Master is not permitted. The external control can be a simple timer device, switch or remote control device.

Set Night Lock by external control operation:
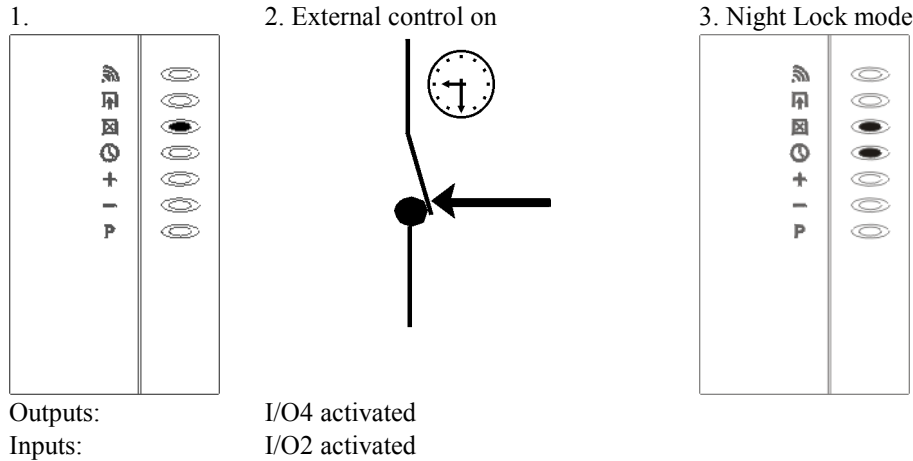
1.	2. External control on	3. Night Lock mode

Outputs:	I/O4 activated
Inputs:	I/O2 activated

Remarks:
- When an external control is employed for the Night Lock mode, the Night Lock Master can still be used at any time to resolve or override the external control. It is still allowed to switch the Night Lock Mode on using the Night Lock Master, even when the external contact is still inactive (open). A subsequent status change of the external control, 'contact closed', will then be ignored, since the *XM3* has already been set to Night Lock.
- In case of power failure or surge, the *XM3* will memorize the latest status of the Night Lock, regardless of the external contact status.
- The Night Lock mode works only when the *XM3* is in access mode.
- After a certain period of no operation the *XM3* will generate an error tone, after which it will resume normal operation. This period known as Overall Time-out is by default set to 30 seconds.
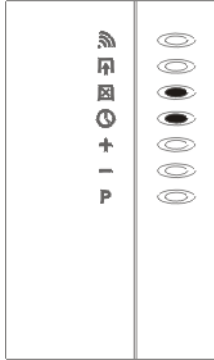
Errors:
None listed.

16.3.4 Switch off Night Lock mode by external control

Switching off Night Lock mode externally differs from using a Night Lock Master in that it will not trigger access mode (i.e. the door solenoid is not activated).
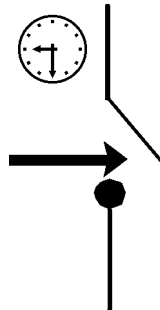
Switching off Night Lock mode by external control operation:
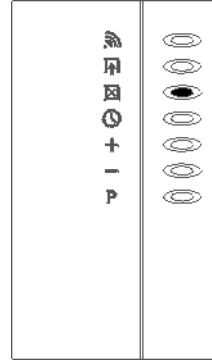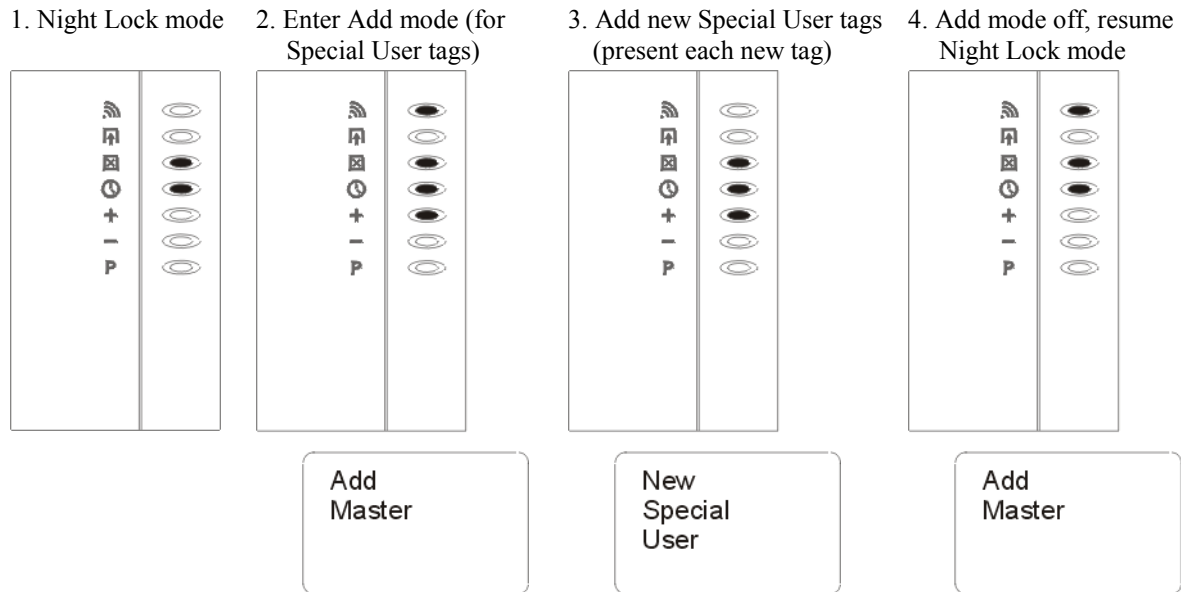
1. Night Lock mode	2. External control off	3. Resume normal operation

Outputs: I/O4 active
Inputs: I/O2 active

I/O4 deactivated
I/O2 deactivated

Remarks:
- When an external control is employed for the Night Lock mode, the Night Lock Master can be used at any time to resolve or override the status controlled externally. It is still allowed to switch the Night Lock Mode off using the Night Lock Master, even when the external contact is still active (closed). A subsequent status change of the external control, 'contact open, will be ignored since the *XM3* has already been set to normal operation.
- In case of power failure or surge, the *XM3* will memorize the latest status of the Night Lock, regardless of the external contact status.
- The Night Lock mode is only working when the *XM3* is in access mode.
- After a certain period of no operation the *XM3* will generate an error tone, after which it will resume normal operation. This period known as Overall Time-out is by default set to 30 seconds.

Errors:
None listed.

16.3.5 Adding Special User tags

The *XM3* provides the possibility of granting specific tags access at any time, both while in Access mode and in Night Lock mode ignoring the status indicated by the Night Lock LED. To prepare these Special User tags they must be added while the *XM3* is in Night Lock mode. Unlike the Night Lock Master which allows one-way access while switching Night Lock off, use of these Special User tags will not affect the Night Lock mode itself.

Add Special User tag operation:

1. Night Lock mode	2. Enter Add mode (for Special User tags)	3. Add new Special User tags (present each new tag)	4. Add mode off, resume Night Lock mode
	Add Master	New Special User	Add Master

Outputs: Inactive
Inputs: Inactive

Remarks:
- Any tag can be added, except tags which are already present in memory as Special User tags or Master tag.
- Special User tags can be voided in the same way as normal tags (in Void mode, independent of the Night Lock status.
- Up to MAX tags can be added minus the number of master tags and/or programmers (minimal 3).
- Keep records of the ID numbers and functions of all tags and of the names of their users. In case of loss, tags can be voided from memory by their number, using a Remote Programmer.
- After a certain period of no operation the *XM3* will generate an error tone after which it will resume normal operation. This period known as Overall Time-out is by default set to 30 seconds.

Possible errors:
- The presented tag was already present in memory as a Special User tag or as a Master. Check the functionality of the tag. If necessary start again using another tag or void the one already present.
- The *XM3* memory is full: Check the number of free positions. This can be checked with a Remote Programmer.

16.3.6 Access in Night Lock mode

Only Special User tags and Night Lock Only tags will be granted access while the *XM3* is in Night Lock mode. Normal user tags will not be admitted.

Access in Night Lock mode operation:

1. Night Lock mode	2. Access	3. Open Time	4. Resume Night Lock mode
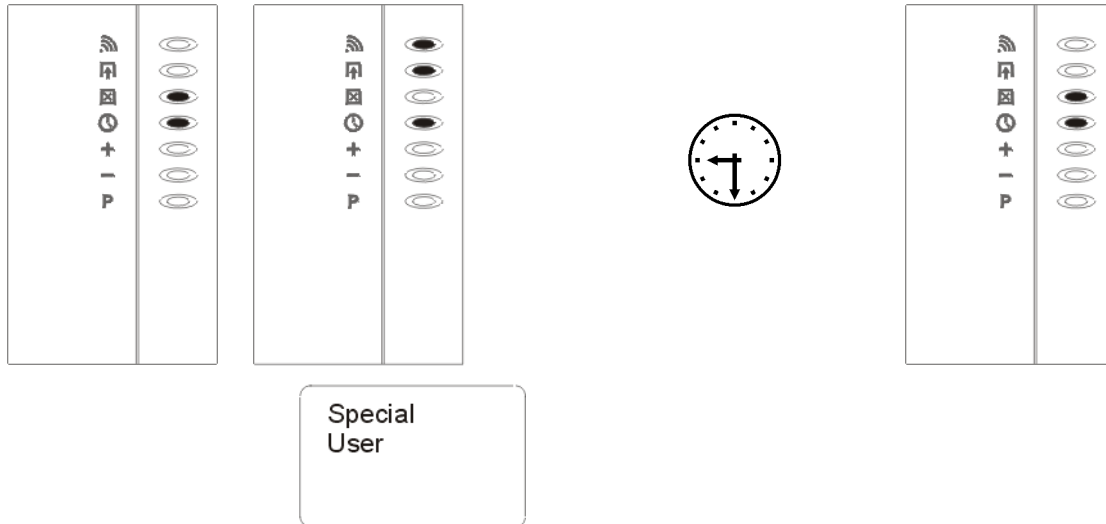
Outputs: I/O4 active   I/O4 active

                                         Relay activated   Relay deactivated

Inputs: Inactive

Remarks:
- Special User tags are granted access while *XM3* is in normal operation as well as in Night Lock mode.
- The normal access mode parameters are applicable for Night Lock Mode as well.
- Checking of the door contact is by default disabled.

Possible errors:
- When presenting a Special User tag no access is granted and an error tone generated: the tag number is not present in memory or is not present as a Special User tag. Check for any restrictions made for the specific access served by this *XM3*.

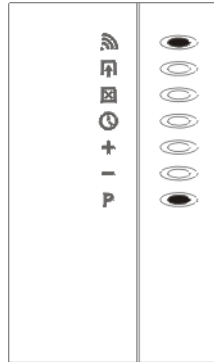### 16.3.7 Voiding the Night Lock Master

When the Night Lock mode is not used, the Night Lock Master can be voided. The operation described below voids the Night Lock Master from the *XM3* memory.
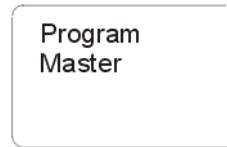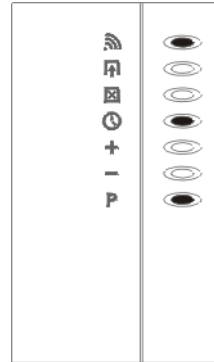
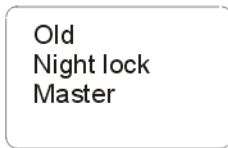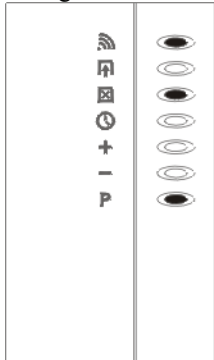**Voiding Night Lock Master operation:**
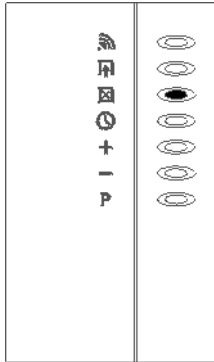
1.Normal status | 2. Program Master, enter Program mode | 3. Program Master, **3x** (skipping steps)
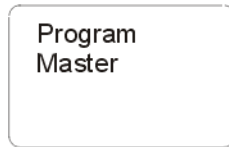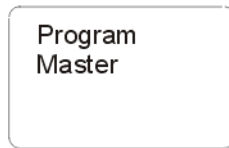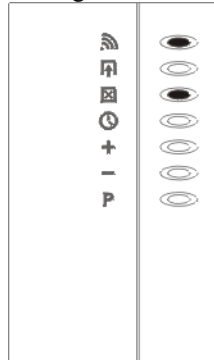
Program Master

Program Master

4. Night lock master voided | 5. Program master **2x** (skip steps) | 6. Resume normal operation

Old Night lock Master
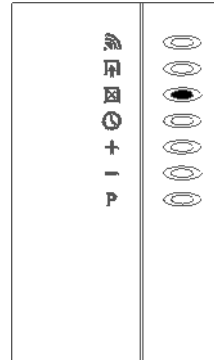
Program Master

Outputs: Inactive
Inputs: Inactive

Remarks:
- In case of loss Master tags can be voided from memory by their number, using a Remote Programmer (9*).
- The tag which had to be a new Night Lock Master was already in memory as a different type of Master tag. Check the functionality of the tag. Try once more with another tag.
- The Night Lock Master tag that was to be voided was not in memory. It will be added as a Night Lock Master. To void the tag, repeat the operation.
- After a certain period of no operation the *XM3* will generate an error tone after which it will resume normal operation. This period known as Overall Time-out is by default set to 30 seconds.
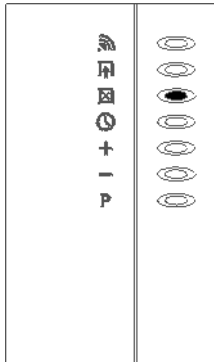
16.4 Open Time-out

The Relay and I/O3 output of the *XM3* can be set to activate during a variable period of time while access is in progress. This period of time can be adjusted from 1 up to 255 seconds. As default the Open Time-out has been set to 2 seconds. For testing purposes at installation, a period of 4 seconds for a door, or up to 20 seconds for a gate is recommended.
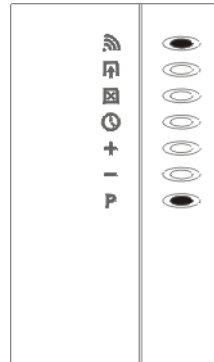
The Open Time-out operates independent from the Close Time-out. In Access mode II, the relay and I/O3 are switched off, i.e. made inactive as soon as the door or gate is closed even if this occurs before the Open Time has elapsed. Refer to Access mode II, Case 1.

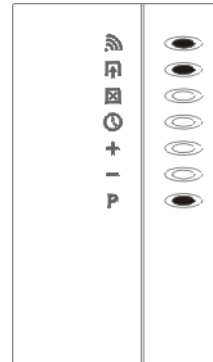**Set Open Time-out operation:**

1. Normal   2. Program Master, enter Program mode   3. Program Master **5x** (skip steps)
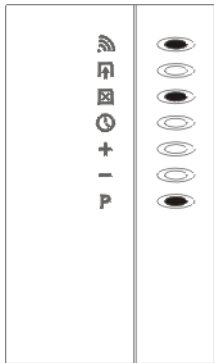
Outputs: Inactive
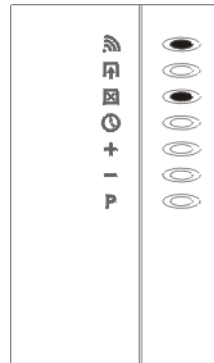Inputs:

4. Set Open Time-out to N seconds: 5. Program Master   6. Resume normal operation
   present tag N times (N= 1-255)

Any
Tag*
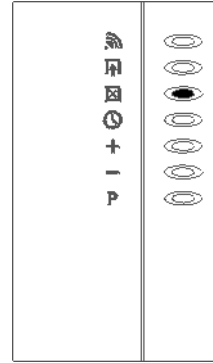
Program
Master

* Except Program Master

I/O1 active; connect to GND.

Remarks:
- The Open Time-out period can also be set by means of a Remote Programmer (see Remote Programmer in this manual).
- After a certain period of no operation the *XM3* will generate an error tone after which it will resume normal operation. This period known as Overall Time-out is by default set to 30 seconds.

Possible errors:
None listed.

16.5 Close Time-out

The *XM3* has a special internal timer which can be used to check whether the gate or door was closed within a pre-set period of time: the *Close Time-out*.

16.5.1 Setting the Close Time-out

The Close Time-out period can be adjusted from 0 up to 255 seconds. The default for the Close Time-out period is 0 indicating that the timer is not active (Access mode I); the 'door open' contact is ignored. By means of a Program Master the Close time-out period can be set (see Access mode II).

Set Close Time-out operation:

1. Normal

2. Program Master, enter Program mode

   Program Master

3. Program Master, **4x** (skip steps)

   Program Master

4. Set Close Time-out to **0** seconds

   Any Tag*

   * Except Program Master

5. Set Close Time-out to N seconds: present tag N times (N= 1-255)

   Any Tag*

   * Except Program Master

6. Program Master **2x** (skip steps), resume normal operation
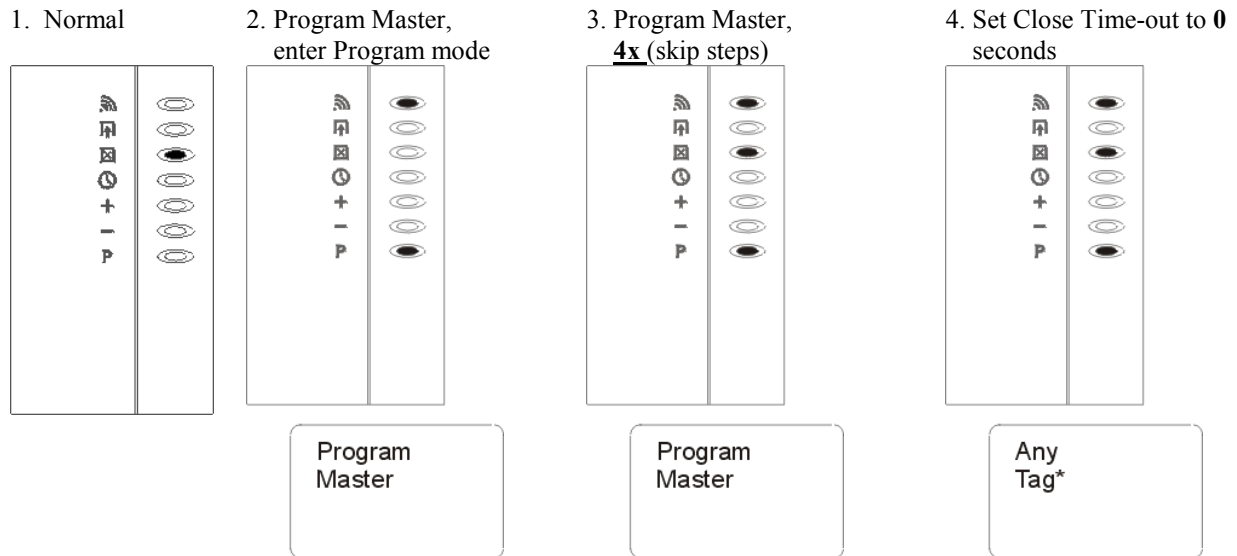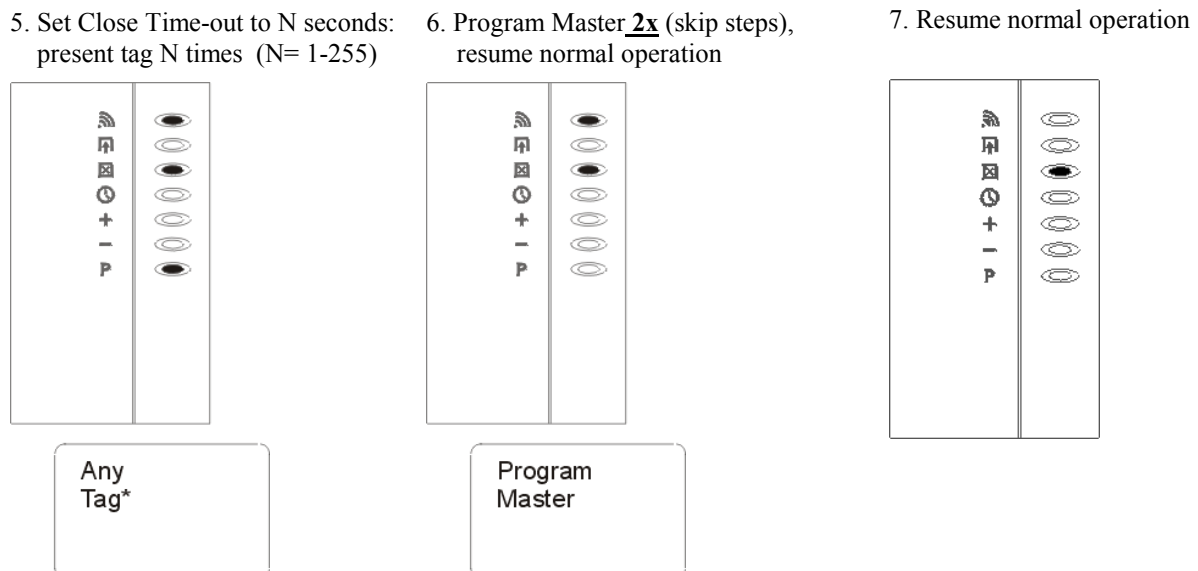
   Program Master

7. Resume normal operation

Outputs: Inactive
Inputs: I/O1 active; connect to GND.

Remarks:
- The Close Time-out period can also be set by means of a Remote Programmer.
- After a certain period of no operation the *XM3* will generate an error tone after which it will resume normal operation. This period known as Overall Time-out is by default set to 30 seconds.

Possible errors:
- After exiting Program mode having set the Close Time-out, an alarm sounds while the open LED flashes; I/O1 was not connected to GND and/or I/O1 has not been connected to the door contact, or the door or gate is currently open. Check that the Close Time-out was set correctly; check the door or gate, or check for a defect in the door contact. The contact I/O1 should normally be closed (connected to GND).
- Program Close Time-out can be deactivated by repeating the programming procedure and setting the close time to zero. To enter program mode while the *XM3* is in an alarm condition (called 'bypassing'), the power to the *XM3* must be switched off and on again while presenting the Program Master.

16.5.2 Access mode II

Access mode II will continuously check the status of the door open contact. This is to ensure that the solenoid of the door or gate is turned off, locking the door immediately. This is valid only when the *XM3* is not in the program mode. This mode is operational whenever the Closed Time-out is set larger than zero. The default for the *XM3* door check is by default disabled.

Access mode II operation:
A number of different cases are described below:

Case 1: The door or gate is opened, and closed again within the Open Time:

1. Normal   2. Access   3. Open Time   4. Resume normal operation

User
Tag
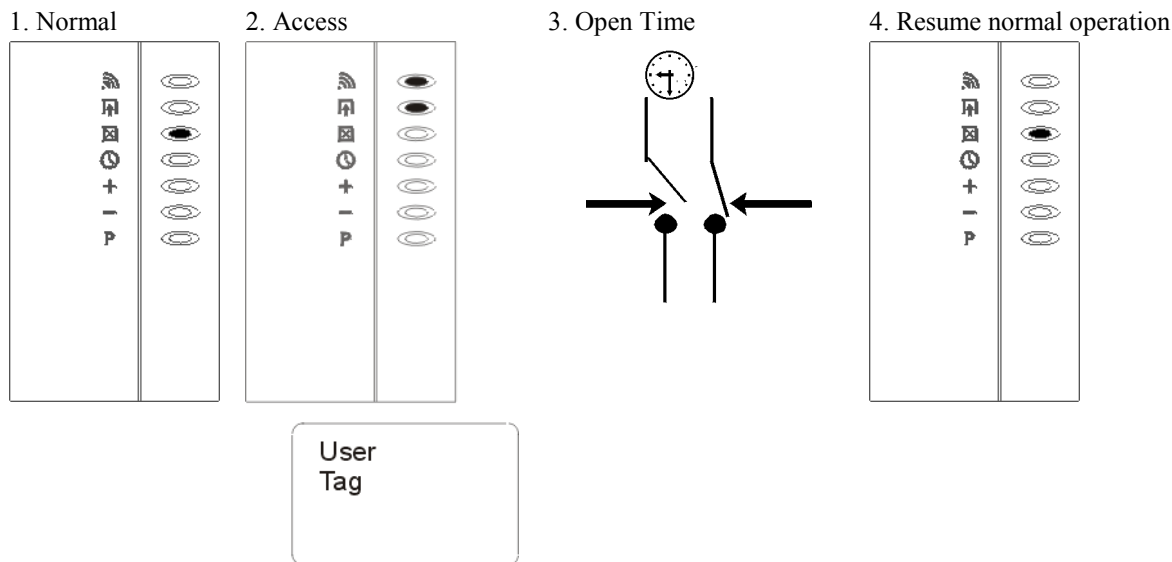
Outputs:	Relay activated	Relay deactivated
Inputs:	I/O1 deactivated (open)	I/O1 activated (closed)

Case 2: The door or gate is opened (within the Open Time), and closed within the Close Time:

3. Open Time   4.   5. Close time   6. Resume normal operation
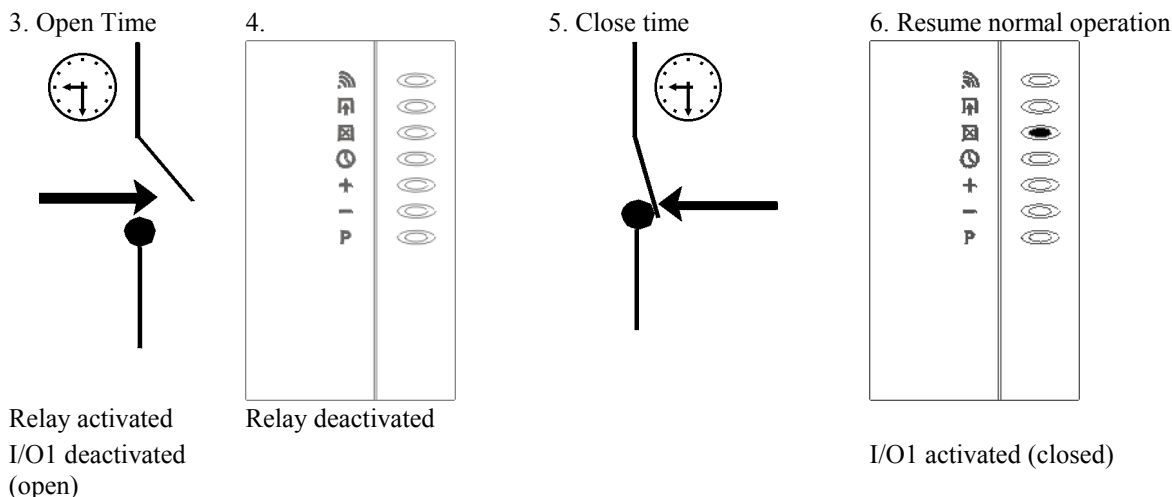
Relay activated   Relay deactivated
I/O1 deactivated
(open)   I/O1 activated (closed)
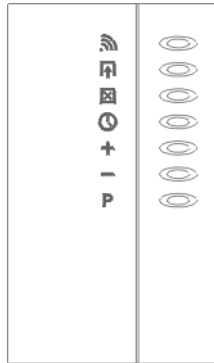
Case 3: The door or gate is opened (within the Open Time) but <u>not</u> closed within the Open Time or Close Time. (A visual and acoustical alarm is activated until the door or gate is closed again):

3. Open Time

4.
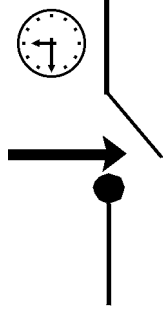
5. Close time

6. ALARM

Relay activated
I/O1 deactivated (open)

Relay deactivated
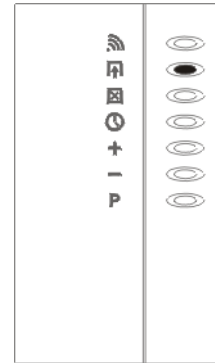
I/O3 activated (high)

7. Gate being closed

8. Resume normal operation
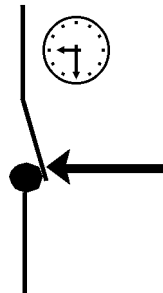
Outputs: inactive
Inputs: I/O1 activated (closed)
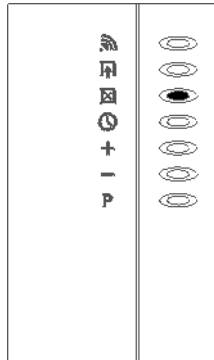
Remarks:
- Open Time and Close Time can both be adjusted and set to Program Mode.
- I/O3 (Forced Entry Output) is only activated at user level. At installer level it is not activated. The visual and audible alert signs are working at both levels.
- After a certain period of no operation the *XM3* will generate an error tone, after which it will resume normal operation. This period known as Overall Time-out is by default set to 30 seconds.

Possible errors:
See Access mode I.

16.5.3 Bypassing the Close Time option

If a door tamper situation or forced entry situation occurs that can not be recovered, a continuous alarm will sound. This happens also when the door contact is defective. This alarm can be deactivated by repeating the programming procedure for setting the Close Time to zero. To enter Program Mode while in alarm, the power of the *XM3* must be switched off and on again, while presenting the Program Master. This procedure enters Program mode immediately bypassing the check of the door contact. This procedure should be undone as soon as the tamper situation is recovered.

Bypass Close Time-out operation:

| 1. Power off (at alarm) | 2. Power on with Program Master | 3. Program mode | 4. Continue by setting Close Time-out to zero |
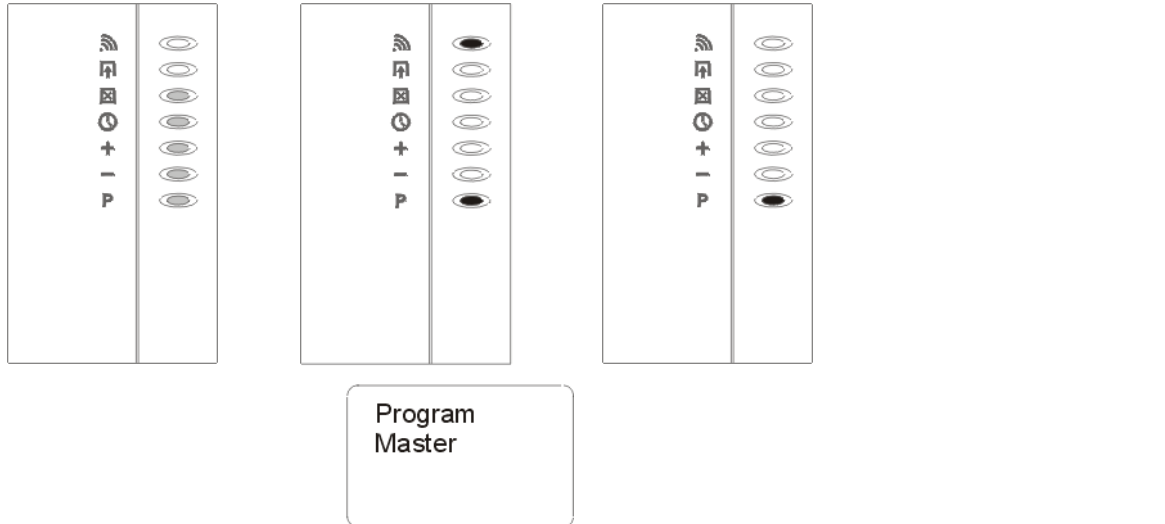
Outputs: Inactive
Inputs: Inactive

I/O3 active (forced entry)

Remarks:
- During a Forced Door Open Alarm, I/O3 in conjunction with I/O4 Night Lock is active. If required a burglar alarm can be triggered.
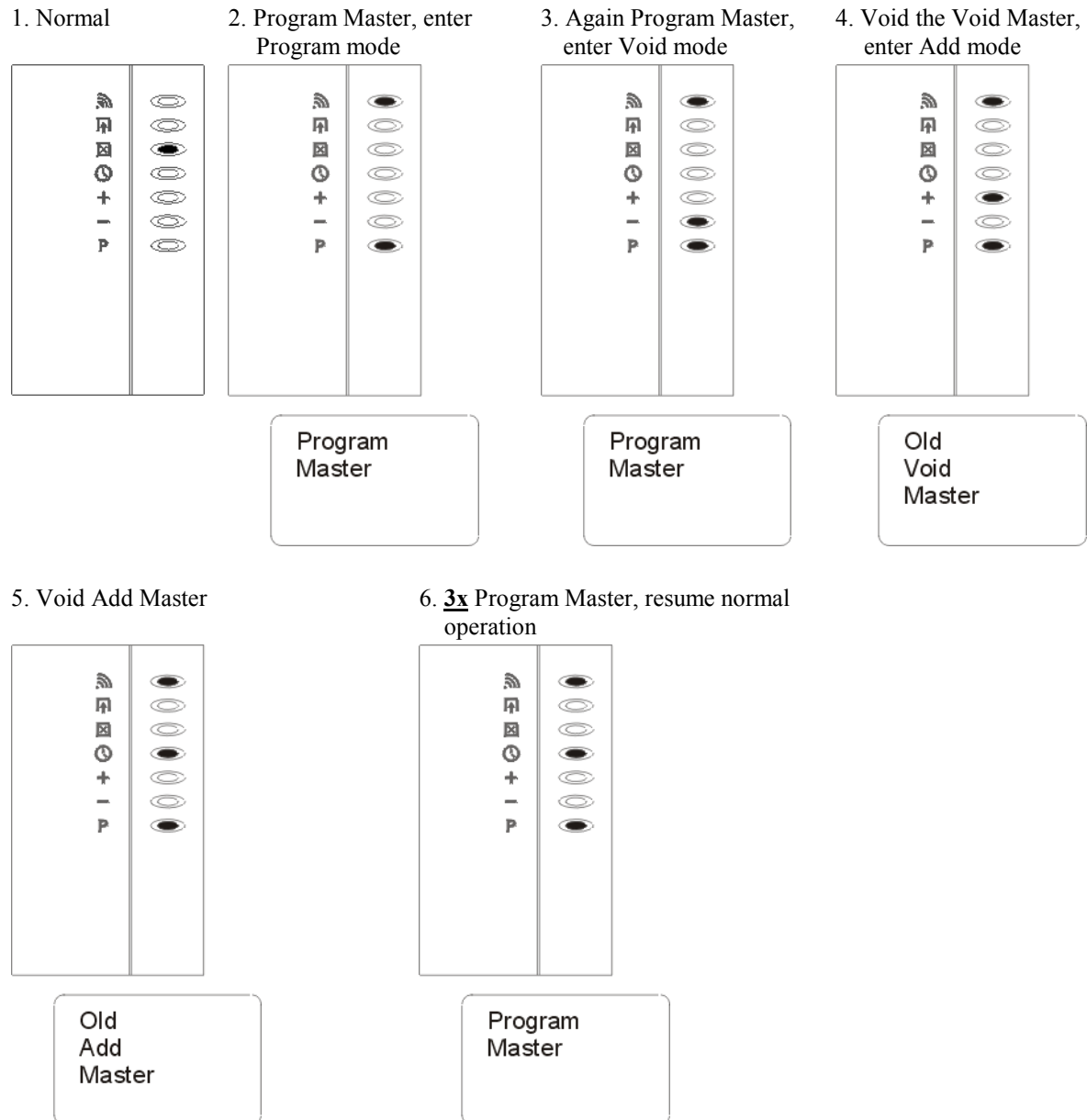

Possible errors:
- If the Program Master was not within reading range while re-powering the *XM3* will not enter Program mode. Repeat the procedure with the Program Master as close as possible to the *XM3.*

16.6 Voiding the Add and Void Master

The Void Master and the Add Master are used to initiate the adding to and voiding from memory of user tags. If necessary these Masters can be voided with a Remote Programmer. If no Remote Programmer is available, the Void Master and Add Master can be used together with a Program Master to void themselves by following the procedure below.

Voiding the Add and Void Master operation:

1. Normal

2. Program Master, enter Program mode

Program Master

3. Again Program Master, enter Void mode

Program Master

4. Void the Void Master, enter Add mode

Old Void Master

5. Void Add Master

Old Add Master

Outputs: Inactive
Inputs: Inactive

6. **3x** Program Master, resume normal operation

Program Master

Remarks:

- For this procedure to work, both the Void Master and the Add Master must be physically available, and they must be present as such in the *XM3* internal memory. Furthermore, they must be presented in the proper order: first the Void Master, then the Add Master.
- If the two Masters are not present in memory, they will be *added* instead of voided. If in doubt, check for their presence in memory by presenting them to the *XM3* both before and after executing this procedure.
- If the old Add and Void Masters were labeled with their function and are not to be used in that function on other *XM3*, remove the labels to avoid mistakes.
- Keep records of the ID numbers and users of voided Master tags.
- After a certain period of no operation the *XM3* will generate an error tone after which it will resume normal operation. This period known as Overall Time-out is by default set to 30 seconds.

Possible errors:

- A presented tag was not an Add or Void Master. Do it again using the correct Master Card.
- The tags presented as Void and Add Master were not present in memory. In this case they will be added in stead of voided. Repeat the procedure with the same tags to void them again.
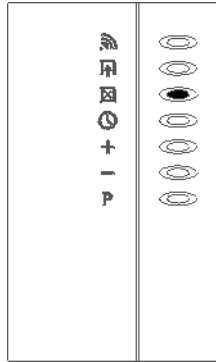
16.7 Voiding groups of tags (by level)

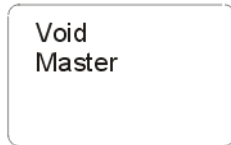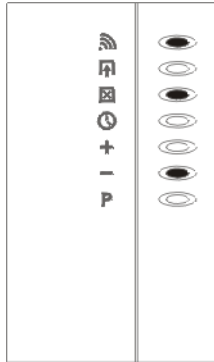This function voids entire groups of tags and Programmers from the *XM3* memory.
To determine which group(s) must be erased a so-called Void level must be determined by presenting a tag with the specific level in step 4. All tags at and below the Void level will be erased.
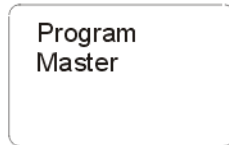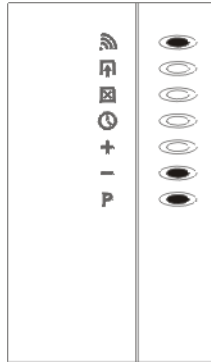
Erase operation:

1.Normal

2. Void Master, enter Void mode

3. Program Master, enter Erase mode

4. Set Void level, using appropriate tag or Master

Void Master

Program Master

Any Tag*
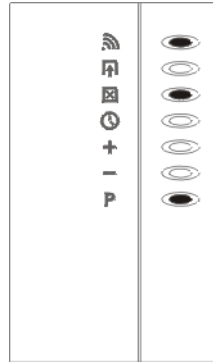
* Tag must be present in memory

5. Void (short beep for each erasure)
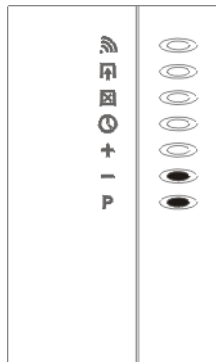
6. Resume normal operation
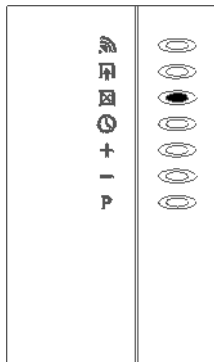
n_1 n_2 Programmer level, Void level

10 ── User Programmer, Program Master
9 ── Void Master
8 ── Add Master
7 ── Night Lock Master
6 ── PIN keypad
3-5 ── Undefined
2 ── Status III tags, night lock only tags
1 ── Status II, special user tags
0 ── Status I, user tags
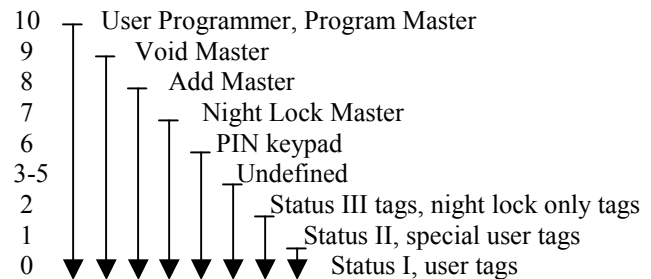
Possible errors:
- **Warning**: if not set at Operation level '0' (user level) after voiding at level 10, the *XM3* will not enter Sleep mode although all tags and User Programmers have been erased from memory. This situation is irreversible! Make sure the *XM3* is operating at level '0'; other operating levels are intended for dealers/installers only!

Remarks:
- If a Program Master is presented the User Programmers will also be erased from memory because they are at the same level.
- All tags at and below the entered Void level value will be voided from memory.
  At operating level (0) erasing at the highest level (10) will put the *XM3* into Sleep mode.

17 APPENDICES

17.1 Appendix 1 – XM3 Software Configuration Switch Form

XM3 SOFTWARE CONFIGURATION SWITCH FORM.

For receiving a software configuration switch, Cross Point needs to know some information about the XM3's current configuration.

Please fill in this form and fax it to Cross Point.

XM3 serial number:

XM3 hardware version:

Extension board type: *

Extension board version: *

Bootloader version:

Operating system:

Cross Point application version: **

Current software configuration:

Wanted software configuration:

Description of XM3 usage:

NOTE:

* Only if Extension board is present (with use of HID, Microchip or Mifare).*
*** In some case custom application version.*

17.2 Appendix 2 – ASCII Table

ASCII TABLE:

HEX	DEC	CHR
00	0	NUL
01	1	SOH
02	2	STX
03	3	ETX
04	4	EOT
05	5	ENQ
06	6	ACK
07	7	BEL
08	8	BS
09	9	HT
0A	10	LF
0B	11	VT
0C	12	FF
0D	13	CR
0E	14	SO
0F	15	SI
10	16	DLE
11	17	DC1
12	18	DC2
13	19	DC3
14	20	DC4
15	21	NAK
16	22	SYN
17	23	ETB
18	24	CAN
19	25	EM
1A	26	SUB
1B	27	ESC
1C	28	FS
1D	29	GS
1E	30	RS
1F	31	US

HEX	DEC	CHR
20	32	SPC
21	33	!
22	34	"
23	35	#
24	36	$
25	37	%
26	38	&
27	39	'
28	40	(
29	41	)
2A	42	*
2B	43	+
2C	44	,
2D	45	-
2E	46	.
2F	47	/
30	48	0
31	49	1
32	50	2
33	51	3
34	52	4
35	53	5
36	54	6
37	55	7
38	56	8
39	57	9
3A	58	:
3B	59	;
3C	60	<
3D	61	=
3E	62	>
3F	63	?

HEX	DEC	CHR
40	64	@
41	65	A
42	66	B
43	67	C
44	68	D
45	69	E
46	70	F
47	71	G
48	72	H
49	73	I
4A	74	J
4B	75	K
4C	76	L
4D	77	M
4E	78	N
4F	79	O
50	80	P
51	81	Q
52	82	R
53	83	S
54	84	T
55	85	U
56	86	V
57	87	W
58	88	X
59	89	Y
5A	90	Z
5B	91	[
5C	92	\
5D	93	]
5E	94	^
5F	95	_

HEX	DEC	CHR
60	96	`
61	97	a
62	98	b
63	99	c
64	100	d
65	101	e
66	102	f
67	103	g
68	104	h
69	105	i
6A	106	j
6B	107	k
6C	108	l
6D	109	m
6E	110	n
6F	111	o
70	112	p
71	113	q
72	114	r
73	115	s
74	116	t
75	117	u
76	118	v
77	119	w
78	120	x
79	121	y
7A	122	z
7B	123	{
7C	124		
7D	125	}
7E	126	~
7F	127	DEL