Users Manual

ThorGuard
Intrusion Alarm System

92002703

Program version number: 6.00.00

Publication date: 051205

Revision history:

Ref. No.	*Revision remarks*	*Date*
92002701	First version	020911
92002701	Minor changes and corrections	030106
92002702	Major corrections to user interface and added functionality	030624
92002702	New battery test added	031027
92002703	Minor corrections to user interface and GPI-WDC Test Menu and Edit Holiday Menu added.	051205

Users Manual

ThorGuard
Intrusion Alarm System

Introduction

This manual provides the information needed to understand and operate the system at a daily basis. Included is also descriptions of the operation of the more specialized functions of the ThorGuard Intrusion Alarm System.

Disclaimer

Due to continuous research and development, the information contained in this document is subject to change without notice.

HI SEC International declines any liability for not respecting or incorrectly using the information in this manual, as well as errors or omissions and their consequences in the installations.

Date

The date of publication is: 051205.

Version

6.00.00

Reference

Reference number: 92002703.

Copyright

Comments and corrections

In our continuous effort to improve the documentation for our products, we need feedback from our users regarding usability, appearance, technical level of content as well as information about errors you may find.

You can mail your comment and corrections to the address: doc@hisec.com

Table of contents

This page is intentionally left blank.

1

This manual

Introduction

This manual is designed to provide the required information needed for using the ThorGuard Intrusion Alarm System.

This chapter

The chapter contains the following sections:

1.1 How to use this manual

This section contains a short description of the typographical conventions used in this manual and some guidelines for reading the manual.

1.1.1 Typographical conventions

Introduction

Typographical conventions are used throughout this manual to help you find the information you are looking for.

Sections and labels

Each section is divided into subsections that each deals with a distinct topic – e.g. this subsection. A subsection contains a number of blocks, usually labelled either in the margin or preceded by an unnumbered heading. You can use these labels and headings to glance quickly through the section. You can also ignore the labels and headings, reading only the text of the section.

Cautions and hints

Warnings, cautions and hints are items to which you should pay particular attention. They look like this:

! *Notes of caution tell you to pay special attention to certain subjects.*

☛ Hints are suggestions that will help you get along with a task.

Procedures

A procedure that tells you how to perform a task looks like this:

Step	*What to do ...*	*What takes place ...*
1	Press one of the function keys (except ⓒ-key)	This displays the menu for entry of your *User ID*.
2	Enter your *User ID*. An intermittent cursor – ▒ – prompts for entry of digits.	During entry, the entered digits are shown in the display
…	… … …	… … …

Lists

In a list that summarizes a number of facts, each item is preceded by a ● like this:

- Basic knowledge about the operation of the ThorGuard Intrusion Alarm System.
- Procedures for performing the operation of the ThorGuard Intrusion Alarm System.
- Reference information about the operation of the ThorGuard Intrusion Alarm System.

Keys and indicators

A key is represented by an image of the key like this:

... to which the operator can reply YES using the ⓞ-key or ...

An indicator is represented by an image of the indicator like this:

... battery operation in case of a mains fault is indicated by the flashing ▫ ...

Display texts

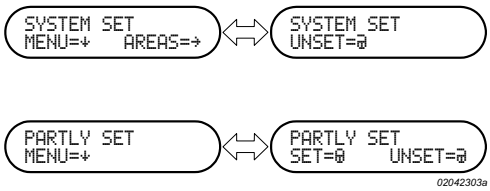
Texts appearing in the display are shown like this:

...the date and time can be displayed like this `18 APR. 02 12:02` ...

Arrows

In illustrations of operating procedures, arrows of this type ⇩ ⇨ are used for indication of an automatic change from one menu to another or the change from a menu – in which to enter digits – to the same menu with all digits entered as in the following two examples:

Menus that are alternately displayed are indicated by an arrow of this type ⇔ as in the following example:



HI SEC International terms

In the body text, terms of a specific meaning in this manual are shown like this:

The user identifies himself to the system by means of a *User ID* and a *PIN-code* ...

1.1.2 How this manual is organized

Types of information

To make it easier to find the information that you want each chapter deals with the Intrusion Alarm System primarily from a specific point of view. The same topic may appear in another chapter, but from different points of view. The contents of each chapter belong to one or two of the following categories.

- Basic knowledge about the operation of the ThorGuard Intrusion Alarm System.
- Procedures for performing the operation of the ThorGuard Intrusion Alarm System.
- Reference information about the operation of the ThorGuard Intrusion Alarm System.

Basic knowledge

A chapter of this category contains introductory descriptions of the operation of the ThorGuard Intrusion Alarm System or descriptions of concepts.

Procedures

A chapter of this category contains instructions about how to perform specific or typical tasks.

Reference

A chapter of this category contains more detailed information about the operation of the ThorGuard Intrusion Alarm System.

The chapters

This manual contains the chapters listed in the table below with content and point of view.

Chapter title	*Contents*	*Point of view*
1 This manual	Typographical conventions used in this manual and some guidelines for reading this manual	-
2 Introduction to operation	Introduction to the ThorGuard Intrusion Alarm System, a description of the controls of *Intrusion Terminals* plus an overview of the menu system used for the operation.	Basic knowledge/reference
3 Daily operation	Initial procedure to use when you access the ThorGuard Intrusion Alarm System for the first time plus procedures for log-in and log out, and for *unsetting* and *setting* the system.	Procedure/reference
4 System status menus	Description of the *System Status menus* used for viewing and changing the status of *Zones*, *Areas*, *Inputs*, for viewing *Alarm Log*, *Event Log* and *Log of Hidden Alarms*.	Procedure/reference
5 System test menus	Description of the *System Test menus* used for testing the system itself, parts of the system, and various components of the system.	Procedure/reference
6 System programming menus	Description of the *System Programming menus* used for simple programming tasks.	Procedure/reference
7 Technical service menus	Description of the *Technical Service menus* used during maintenance and repair of the system and during the initialization of the system.	Procedure/reference
8 Time lock menus	Description of the *Time Lock menus* used for the manual release, blocking or unblocking of *Time Locks* and display of the status of the release process.	Procedure/reference
9 Output control menus	Description of the *Output Control menus* used for the manual control of for example light, doors, Closed Circuit Television equipment (CCTV), etc.	Procedure/reference

2

Introduction to operation

Introduction

This chapter provides a short introduction to the operation of theThorGuard Intrusion Alarm System and explains the terms of *Areas*, *Zones*, *User Profile*, *Users* and operating rights before describing the controls of *Intrusion Terminals*. The last section of the chapter provides an overview of the menu system used for operation of the ThorGuard Intrusion Alarm System.

This chapter

The chapter contains the following sections:

2.1 Overview

Introduction

The ThorGuard Intrusion Alarm System can accommodate up to 250 users. With their individual rights, they can operate the ThorGuard Intrusion Alarm System via the *Intrusion Terminals*.

Intrusion Terminals

The operation of the *Intrusion Terminal* is simple and menu-driven. It takes place using a number of function keys, a numeric keyboard and a display showing the menus.

Fig. 2.1 *Examples of Intrusion Terminals.*

02041802a

User identification

The user identifies himself to the system by means of a *User* ID and a *PIN-code*, before access to operation of the system is obtained. The procedure to use for this operation (Log-in) is outlined on page 2-5 and described in detail in Section 3.2.

User ID

The *User ID* is an individual, personal number that may comprise up to eight digits. It is entered on an *Intrusion Terminal* prior to the entry of the *PIN-code*. The *User ID* is known by the organization as well as the user.

PIN-code

Each user has also a *Personal Identification Number* also called a *PIN-code*. To ensure a high security level a *PIN-code* of six digits is used. In general, the *PIN-code* is known by the user only if the initially allocated *PIN-code* is changed by the *User*.

Duress Code

In duress situations, the *User* may substitute the PIN-code with a *Duress Code* that can be a fixed code common to all *Users* or variable a code.
When the *Duress Code* is used during log-in, a silent alarm will be sent to the Control Station to which the ThorGuard Intrusion Alarm System is connected. Apart from this, the system will behave normally without any alarm indication.

User operating rights

Each user is assigned to a *User Profile* that determines the rights of one or more *Users*. The *User Profile* allocates rights to *unset* the ThorGuard Intrusion Alarm System through its assignment to one or more *Unset Week Programs as well as Reset Rights* and *Operating Rights*. See also Section 2.3.

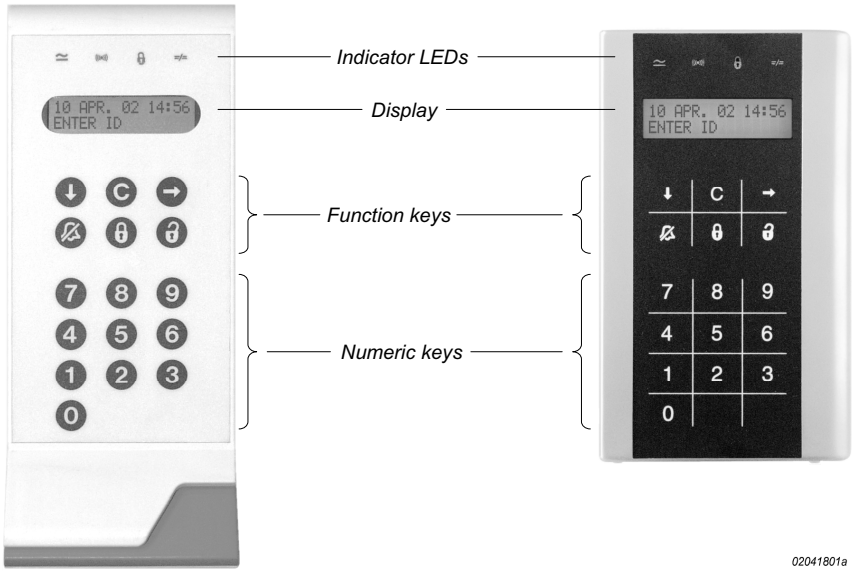
Getting along ...

To see how the *Intrusion Terminals* are operated in connection with the ThorGuard Intrusion Alarm System, see Section 2.2 on the following page.

2.2 The controls of the Intrusion Terminals

The operation of the *Intrusion Terminals* is menu-driven; thus, it takes place via a display showing the menus and a number of function keys and a numeric keyboard.

Fig. 2.2 *Examples of the controls of Intrusion Terminals. The controls are identical for both types of Intrusion Terminals.*



Indicator LEDs

The *Intrusion Terminal* is equipped with four LEDs above the display; one green LED, one red LED and two yellow LEDs with the following functions:

Symbol	*Name*	*Lit*	*Unlit*	*Flashing*
≃	Power (green)	Power is on	Power is off	Battery operation (Mains power fault)
(•)	Alarm (red)	*Alarm* [1] (Lit after log-in)	No *Alarm*	Not applicable
🔒	Set (yellow)	System is *set* [1] (Lit after log-in)	System is *unset* [2]	Not applicable
⎓	System Fault (yellow)	*System Fault* [1] (Lit after log-in)	No *System Fault* (All *Faults Cleared*)	Not applicable

[1] Within the area(s) covered by the *Intrusion Terminal* [2] One *Area*, *Zone* or *Input* is *unset*.

Display

It contains two lines each comprising sixteen characters. An intermittently shown cursor – ▒ – in the display may prompt for entry of digits.

When the *Intrusion Terminal* is not operated, the display shows the date and time with its back-light turned off and the text: ENTER ID. As soon as you start operating the *Intrusion Terminal*, the back-light of the display is turned on. It is automatically turned off two minutes (normally) after the last operation of any key.

When you perform operations, a number of menus and submenus can be shown, presenting you with either choices to make using the function keys or requesting the entry of numbers using the numeric keys.

Keys

The *Intrusion Terminal* is equipped with six function keys and ten numeric keys. The function of these is explained below.

Keys	***Function or description***
0 to 9	Numerical keys for entry of PIN-codes, user identity, menu numbers, and parameters.
	Key for *setting* of the ThorGuard Intrusion Alarm System. Indicated in the display as .
	Key for *unsetting* of the ThorGuard Intrusion Alarm System. Indicated in the display as .
	Key for *clearing* of *Alarms* and *Faults*. Indicated in the display as .
	Key for selecting a displayed menu function (YES) or for displaying additional information of a selected menu function. Indicated in the display as .
C	Key for clearing the last entry of a number, for stepping backwards in the menu system if no entry was made, and for log-out. Indicated in the display as .
	Key for stepping forwards (NO) in the menu system or for ending an entry, etc. Indicated in the display as .

Buzzer

The built-in buzzer of the *Intrusion Terminal* provides an acoustical indication of *Alarms* and *Faults* and of entry and exit periods. It is also activated when you activate a key or when you make operating faults or attempt to use a function not available to you. The five buzzer signals available have the following sounds and meanings:

Tone length	***Name***	***Meaning***
Very short tone	*Activation Signal*	You have activated a function key or a numeric key.
Short tone	*Attention Signal*	You have activated an illegal key or the function is not available. In the latter case, an explanation will be shown on the display. May sound as a double tone due to the activation signal and the following attention signal.
Three 1 s tones	*Error Signal*	You have made an operating error or tried to access a menu not available to you. An explanation will be shown on the display.
15 s tone	*Clearing Missing Signal*	You have attempted to *set* the system or log out without *clearing* current alarms.
Continuous tone	*Alarm Signal*	An *Alarm* or a *Fault* has occurred in the system or the *entry* or *exit timers* are running.

☛ Please note that the *Alarm Signal* as well as the other types of signals may have been set to off so that signals may not be provided.

If you operate the keyboard during a period where the *Alarm Signal* sounds, the *Alarm Signal* will be terminated so that the normal signals during operation can be heard. If the buzzer sounds during an entry or exit period, the normal signals during operation will not become enabled.

Area Mask

A programmable *Area Mask* may have been applied to the *Intrusion Terminal* during the programming of the ThorGuard Intrusion Alarm System.

This *Area Mask* ensures that most functions executed from the *Intrusion Terminal* keyboard will be performed only on the *Area(s)* covered by the *Area Mask* for the *Intrusion Terminal* in question.

Operation in general

The operation of the ThorGuard Intrusion Alarm System is menu-driven as described earlier. This means that all operating possibilities are presented on the display of the *Intrusion Terminal* as questions to which the operator can reply YES using the ➲-key or NO using the ⓿-key.

The menu includes a main menu for daily operation and submenus for status display or change of status, system test, time lock operation, etc.

As outlined in Section 2.1, access to operation requires a log-in by:

- Entry of your valid *User ID* on the *Intrusion Terminal*,

followed by:

- Entry of your valid *PIN-code* on the *Intrusion Terminal*.

The initial procedure for log-in for the first time that you use the ThorGuard Intrusion Alarm System is described in Section 3.1. After this you can use the ordinary procedure described in Section 3.2.

After log-in, the functions available to you will depend on the *User Profile* assigned to you and the *Reset Rights* and *Operating Rights* allocated to you through a number of options individually assigned during the programming of the ThorGuard Intrusion Alarm System.

Menu numbers

Most menus can be accessed directly after you have logged in using your *User ID* and *PIN-code*. This will present two menus alternately displayed. These menus are used for *setting* or *unsetting* the system or to select a menu by pressing the ⓿-key from which you can select the required menu by entering its number. See the example in Fig. 2.4.
The number of a menu is shown to the left in the lower left line of the display as indicated in Fig. 2.4.

Getting along ...

To get an overview of the menu system used for operation of the ThorGuard Intrusion Alarm System, see Section 2.4.

2.3 Zones, areas, user profiles and users

Introduction

To handle the *unsetting* and *setting* of the ThorGuard Intrusion Alarm System so that the security can be maintained at the highest possible level, the system can be divided into sections that can be individually *set* and *unset*.
This secures that only the sections of the monitored area or building that are manned, are *unset*. When the personnel leave their premises, the section in question can be *set* so that access without *unsetting* will generate an *Alarm*. However, access to *unset* sections is still possible.

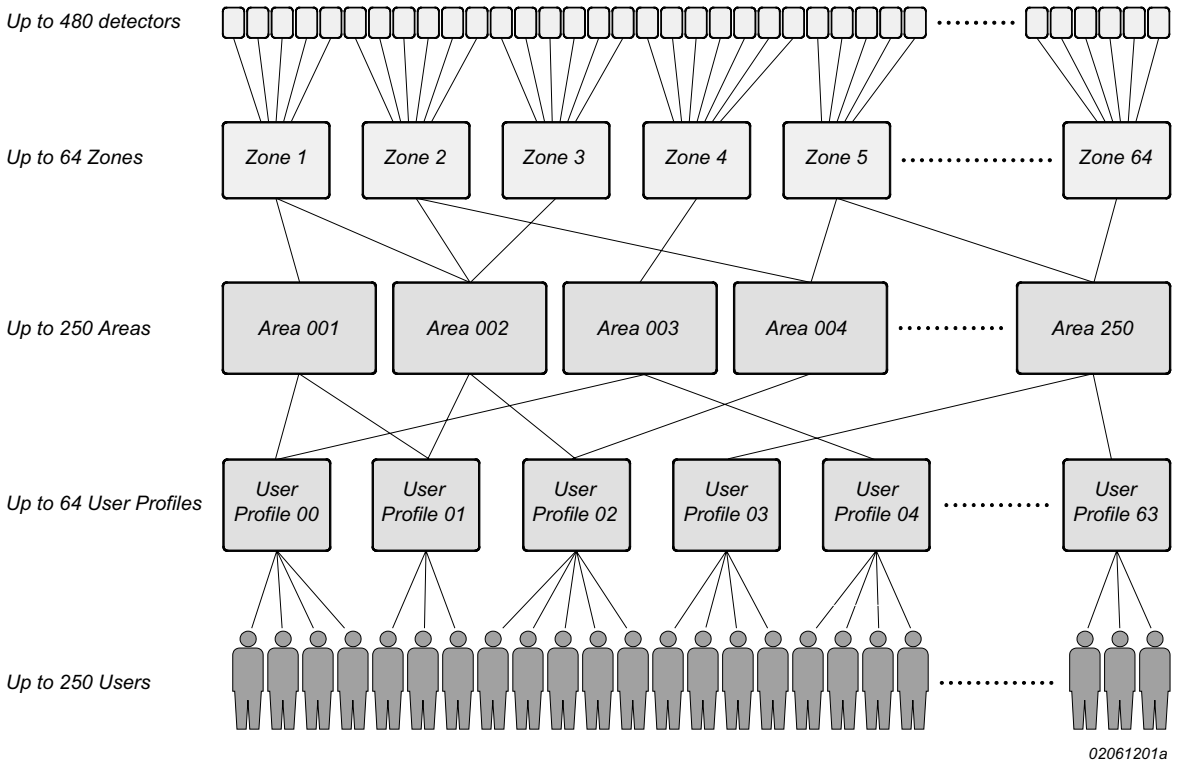
Areas and zones

This division into sections is performed by dividing the monitored area or building into *Zones* that can be combined into *Areas* that each comprises one or more *Zones*.

Users, user profiles and week programs

The operating right for the *Users,* i.e. the operations they are allowed to perform and the menus to which they have access is determined by the assigned *User Profile* and individually assigned rights.
The availability of these operating rights are controlled by one or more *Week Programs* assigned to the *User Profile*, so that the available rights to operate the system may vary with the time of the day, the weekday and the time of the year (*Holidays*).
In addition to this, an *Area Mask* may have been applied to the *Intrusion Terminal* to ensure that most functions executed from the *Intrusion Terminal* keyboard will be performed only on the *Area(s)* covered by this *Area Mask*.

Fig. 2.3 *A schematic example showing the relationship between Zones, Areas, Users and User Profiles.*



The concepts of *Zones* and *Areas* are explained in Section 2.3.1. The concepts of *Users* and *User Profiles* are explained in Section 2.3.2 while *Week Programs* are explained in Section 2.3.3.

2.3.1 Zone and area concepts

Zones

A *Zone* is a logical unit used for grouping of all *Inputs* and *Outputs* (Detectors, door contacts, buzzers, etc.) within a section of the monitored area, typically a confined space such as a single room. All *Inputs* and *Outputs* are identified by a 4-digit number (ID).

The ThorGuard Intrusion Alarm System itself may be divided into maximum 64 *Zones*.
To identify the *Zone* it is provided with a number between 1 and 64 and a name. The name may comprise up to ten characters.

Areas

An *Area* is a logical unit used for grouping of *Zones* to be able to *set* and *unset* a number of *Zones* in one operation. An *Area* contains typically *Zones* that are used daily by personnel belonging to the same department and includes the *Entry*/*Exit Zone* that in most cases is common for all personnel.
The individual *Area* may contain any number of *Zones* up to 64. Of these *Zones*, one or more may be contained in other *Areas* too.

The ThorGuard Intrusion Alarm System may be divided into maximum 250 *Areas*. To identify an *Area* it is provided with a number between 1 and 250 and a name. The name may comprise up to ten characters.

The ThorGuard Intrusion Alarm System can operate with two types of *Areas* – *Logical Areas* and *Physical Areas* – that differ with respect to the way in which their *Zones* are *set* and *unset*:

Logical Areas

A Logical Area is an *Area* in which:

- A *Zone* is *set* when all *Logical Areas* to which the *Zone* belongs are *set.*
- A *Zone* is *unset* when one *Area* to which the *Zone* belongs is *unset*.

Physical Areas

A Physical Area is an *Area* in which:

- *A Zone* is *set* when the *Physical Area* to which the *Zone* belongs is *set.*
- All *Zones* belonging to the *Physical Area* are *unset* when this *Area* is *unset*.

☛ For a *Zone* belonging to a *Physical Area*, the *setting* is independent of the status of other *Areas* to which the *Zone* may belong. If the *Zone* belongs to another *Area*, this *Area* will change to *partly set* status.
However, it may also change to *set* status if the *Zone* was the last to be *set* for this *Area*.

2.3.2 User profiles and users

User profiles

The operating rights in general are determined by the *User Profile* assigned to the *User*. The *User Profile* determines the rights of a group of *Users* through selection of:

- Optional rights
- Reset rights
- Unset week programs
- Access rights to menus

Optional rights

Selected optional rights allocate a number of rights to *Users* that are assigned to the *User Profile*. The options can assign rights to for example:

- *Unset* the system
- *Set* the system
- Use a *Duress Code*
- View all *Alarms* and *Faults* of the system

Reset rights

Selected *Reset Rights* for a *User Profile* allow *clearing* of *Alarms* and *Faults* for various types of *Inputs*.

Unset week programs

The selected *Unset Week Programs* determine the periods in which a *User* with this *User Profile* may *unset Areas* within the ThorGuard Intrusion Alarm System.

Access to menus

Selected access rights to menus determine the menus to which the *Users* with this *User Profile* may access when operating an *Intrusion Terminal*.

Users

For the individual *User*, a number of operating rights can be selected as follows:

- Rights to delay of *Autosetting* function
- Rights to log in when the system is in *Service Mode*

2.3.3 Week programs

Week Programs automatically control various functions in the ThorGuard Intrusion Alarm System. The following types of *Week Programs* are available:

- Autoset week programs
- Unset week programs
- Time Lock week programs
- General purpose week programs
- Holiday periods

Autoset week programs

Autoset Week *Programs* control the automatic *setting* and *unsetting* of the ThorGuard Intrusion Alarm System. They *set* and *unset* the system automatically at preselected times.
The *Autosetting* function can be delayed if the *User* has an individual right to do so.

Unset week programs

Unset Week Programs control the periods in which a *User* may unset *Areas* within the ThorGuard Intrusion Alarm System. This right is allocated through the *User Profile* assigned to the *User*.

Time Lock week programs

Time Lock Week Programs control the behavior of *Time Locks* associated with the ThorGuard Intrusion Alarm System. See also Chapter 8.

General purpose week programs

General Purpose Week Programs are used for control of functions in the ThorGuard Intrusion Alarm System that are not related to the setting and unsetting of the system.

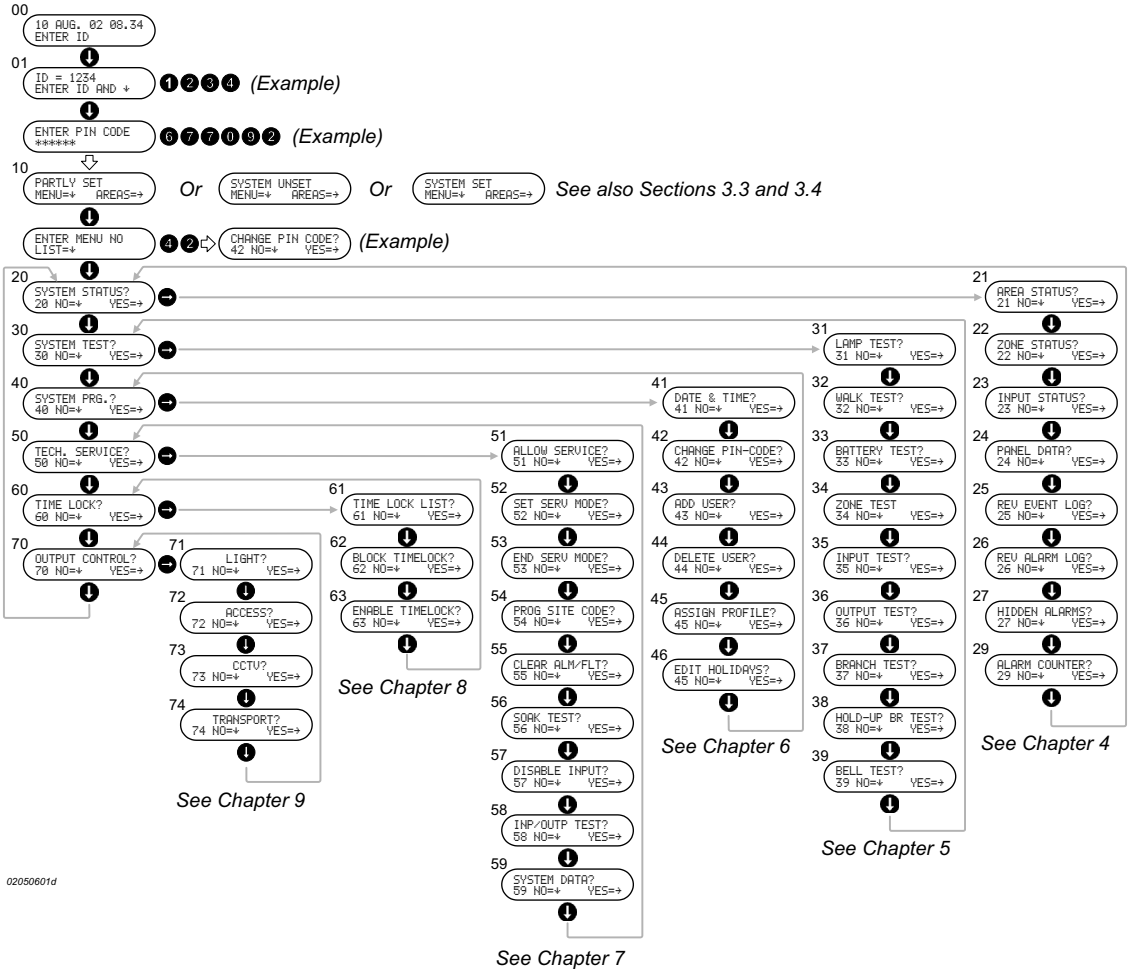
Holiday periods

Holiday Periods control the behavior of the ThorGuard Intrusion Alarm System during holidays.

2.4 Menu overview

The figure below shows the menu system used in the ThorGuard Intrusion Alarm System. Although it may seem complicated, it is fairly simple to use as explained in detail in the following chapters.
The menus are arranged in groups according to the main application and can be accessed either by stepping through the menu system using the ❶-key or by entering the number of the menu.

Fig. 2.4 *Overview of the menus available. The entered User ID and PIN-code,menu number and texts of the menus 71, 72, 73, and 74 are examples only. The example assumes that no alarms, faults, isolations or disabled inputs are present.*



Getting along ...

The description of the use of the various menus starts in Chapter 3 with the menus you will have to use daily for log-in to the system, and *unsetting* or *setting* of the system. This chapter also includes instructions for log-in with a *Duress Code*, *clearing* of alarms, delaying of *autosetting* functions, isolation of *Inputs*, and log-out.

The initial procedure for log-in for the first time that you use the ThorGuard Intrusion Alarm System is described in Section 3.1. After this you can use the ordinary log-in procedures described in Section 3.2.

☛ Please note that full programming of the ThorGuard Intrusion Alarm System requires the connection of a ThorGuard Configuration System.

This page is intentionally left blank.

3

Daily operation

Introduction

This chapter describes the initial procedure to use when you access the ThorGuard Intrusion Alarm System for the first time and the procedures to use for logging in and logging out on the system and the procedure for *unsetting* and *setting* the system.

This chapter

The chapter contains the following sections:

3.1 Starting

Introduction

Prior to the operation of the ThorGuard Intrusion Alarm System, you must be created as a user in the system, i. e. you must be registered with a *User ID* that may comprise any number of digits between one and eight.

In addition to this, you must register yourself with a *PIN-code* that you select yourself and enter the first time you log-in to the ThorGuard Intrusion Alarm System. This procedure is described in Section 3.1.1.

Daily operation

After this, the daily operation of the ThorGuard Intrusion Alarm System comprise for most users:

- Log-in (Section 3.2)
- *Unsetting* the parts of the system you are allowed to *unset* (Section 3.3)
- *Setting* the parts of the system you are allowed to *set* (Section 3.4)
- *Clearing* of *Alarms* and *Faults* (Section 3.5)
- Viewing data for *Isolations* and *Disabled Inputs* (Section 3.6)
- Delay of *Autoset* function (Section 3.7)
- Log-out (Section 3.8)

Other operations

In addition to this you may also have to:

- Check the status of *Areas*, *Zones* and *Inputs*, viewing contents of the *Alarm Log*, *Event Log*, etc. These tasks are described in Chapter 4.
- Perform a number of tests to check the operation of the system, its *Areas* and *Zones* and its components. These tasks are described in Chapter 5.
- Perform simple programming such as setting the date and time, changing *PIN-code*, adding and deleting *Users*. These tasks are described in Chapter 6.
- *Set* the system in *Service Mode*, *reset* the system, *clear Alarms* and faults, disable *Inputs*, etc. These tasks are described in Chapter 7.

Allowed operations

The parts of the system that you may *unset* or *set* and the operations that you are allowed to perform will depend on the *User Profile* assigned to you and the *Reset Rights* and *Operating Rights* allocated to you.
In addition, an *Area Mask* may be assigned to the *Intrusion Terminal* limiting operations with the system to be performed only on the *Area(s)* covered by the *Area Mask*.
Specific information about your allowed operations as well as information about your *User ID* is available from the person responsible for managing the ThorGuard Intrusion Alarm System in your company

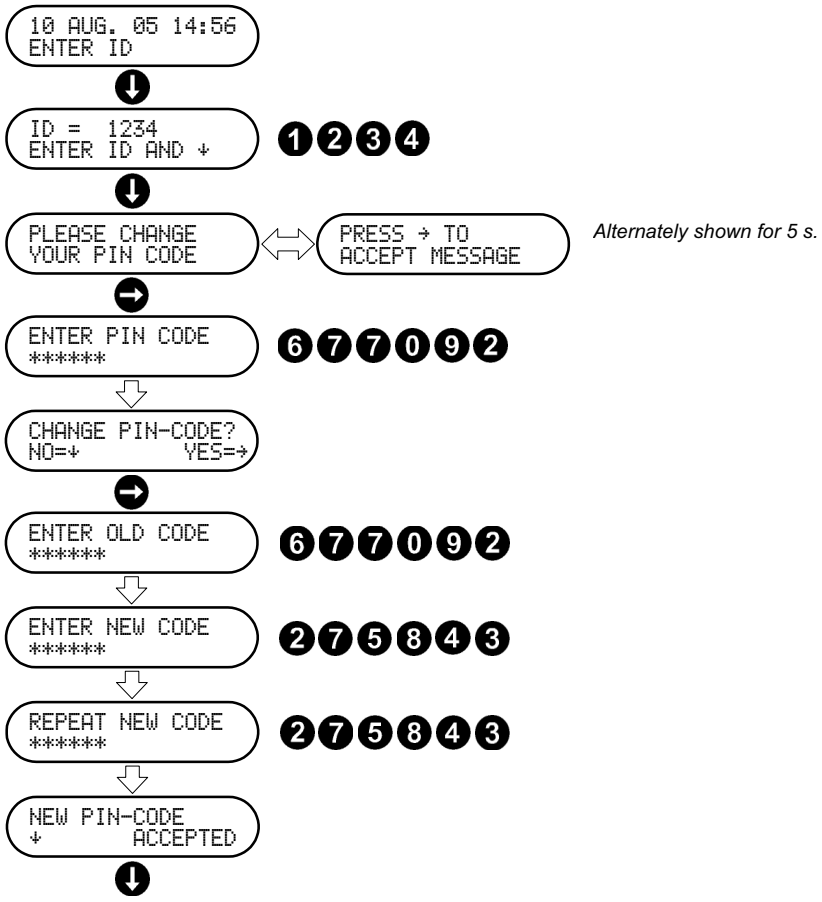
3.1.1 First time log-in

When you have been created as a *User* in the ThorGuard Intrusion Alarm System you are registered with a *User ID* that may comprise any number of digits between one and eight. You may also have been equipped with both a *User ID* and the corresponding *PIN-code*.

Depending on the programming of the ThorGuard Intrusion Alarm System, the *PIN-code* may be used as it is or you may be requested to change it.
In case it should be used as it is, please turn to Section 3.2.1 that describes the log-in procedure.

If you are requested to change your *PIN-code* during your first log-in to the system, you should use the procedure outlined in Fig. 3.1 below and described on the following page.

Fig. 3.1 *Example of the procedure and menus used for the first time log-in on an Intrusion Terminal. The example assumes that the User ID is 1234, the initial PIN-code is 677092 and you select the new PIN-code to 275843.*



Log-in procedure

Step	*What to do ...*	*What takes place ...*
1	Press one of the function keys (except the C-key)	This turns on the back-light and displays the menu for entry of your *User ID*.
2	Enter you *User ID*. An intermittent cursor – ▒ – prompts for entry of digits.	During entry, the entered digits are shown in the display
3	End the entry of the *User ID* by pressing the ↓-key.	This displays a message requesting the change of the *PIN-code* and instruction for accepting the message. Message and instructions are alternately displayed
4	Press →-key to accept the message	This displays a menu for entry of your old *PIN-code*
5	Enter your old *PIN-code*.	During entry, the entered digits are shown as * in the display. After entry of the old *PIN-code*, a menu requests the entry of a new *PIN-code*.
6	Enter your new *PIN-code*.	During entry, the entered digits are shown as * in the display. After entry of the new *PIN-code*, a menu requests the entry of the new *PIN-code* again.
7	Enter your new *PIN-code* again.	During entry, the entered digits are shown as * in the display. When the *PIN-code* is accepted, an acceptance message is displayed.
8	Press the ↓-key to accept the message.	This displays a menu in which you can respond by pressing either the ↓-key or the →-key.
9	Press the ↓-key.	This displays one of three menus for *unsetting* or *setting* the system. See Section 3.3 or Section 3.4 for more information.

PIN-code time limit

Your *PIN-code* can be set to be used indefinitely or for use only for a period *set* during the programming of the ThorGuard Intrusion Alarm System.
When this period is about to expire, the display of the *Intrusion Terminal* will show the message: PLEASE CHANGE YOUR PIN CODE when you log in. This means that you will have to repeat the procedure above from Step 4. After this a new validity period starts.

The message will be shown every time you log in until you have changed your *PIN-code* as requested.

When the validity period for your current *PIN-code* expires, you will no longer be able to operate the system. However, you will still be able to log in and change your *PIN-code*.

3.2 Log-in

Introduction

When you arrive to an *Intrusion Terminal* that has not been operated for a while (Programmable – normally two minutes) the back-light of the display is turned off and only the date and time is displayed. The back-light is turned on as soon as a key on the *Intrusion Terminal* is pressed.

General remarks

When you log-in on an *Intrusion Terminal*, the first key (❶-key, ❽-key or a numeric key) you press prior to the actual log-in procedure, will determine the menu displayed after log-in.

❶-key + log-in	You can use this method when you want to *unset* the system or parts of the system. The menu for *unsetting* the first *Area* you are allowed to *unset* is shown. See Section 3.3.1.
❽-key + log-in	You can use this method when you want to *set* the system or parts of the system. The menu for *setting* the first *Area* that you are allowed to *set* is shown. See Section 3.4.1.
Log-in only	You can use this method when you want to perform other operations on the ThorGuard Intrusion Alarm System. The menu showing the status of the system is displayed. From this, you can continue in the menu system to perform the operations that you are allowed to perform. The possibilities are described in Chapters 4 to 8. You can also step through a list of *Areas* and *unset* or *set* these as required. See Sections 3.3.2 (*Unsetting*) and 3.4.2 (*Setting*), respectively.

Log-in procedures

The procedure for log-in only on an *Intrusion Terminal* is described in Section 3.2.1.

Message to user

During log-in, you may receive a message after you have entered your *User ID*. The message handling is described in Section 3.2.2.

Alarms, faults, isolations and disabled inputs

If the ThorGuard Intrusion Alarm System contains *Alarms*, *Faults*, *Isolations* or *Disabled Inputs* or combinations of these when you log in, the display of the *Intrusion Terminal* will present a menu from which you can reach menus with display of the data of individual *Alarms*, *Faults*, *Isolations* or *Disabled Inputs*. This will always take place independent of the method you use for the log-in if Alarms, *Faults*, *Isolations* or *Disabled Inputs* are present.

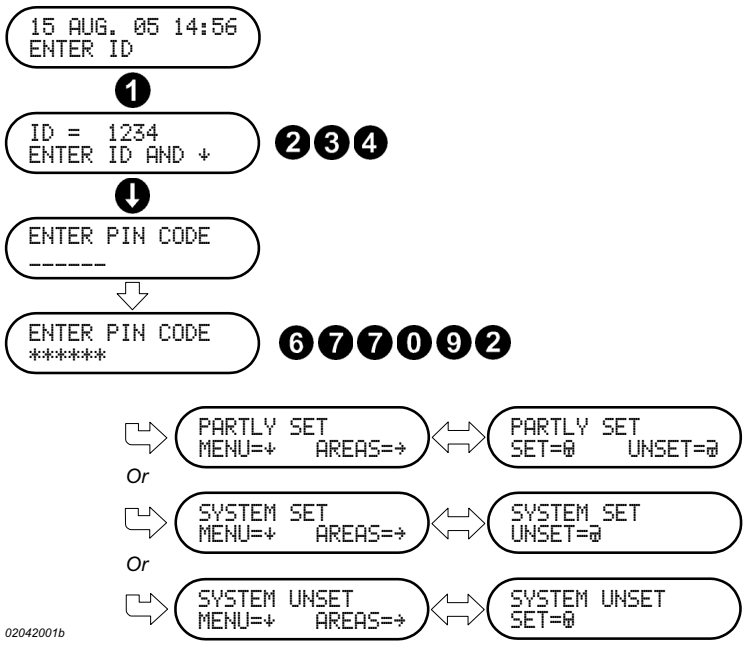
You can find more information about *Alarms* in Section 3.5.1, about *Faults* in Section 3.5.2, about *Isolations* in Section 3.6.1, and about *Disabled Inputs* in Section 3.6.2.

3.2.1 Log-in on an Intrusion Terminal

To log in on an *Intrusion Terminal*, enter your *User ID* (Example 1234) and *PIN-code* (Example 677092) as shown in the figure below and described in the procedure.

☛ If you pressed a numeric key instead of a function key, this digit is considered the first digit of your *User ID* and is thus shown in the display.

Fig. 3.2 *Example of the procedure and menus used for log-in on an Intrusion Terminal. The example assumes that the User ID is 1234 and the PIN-code is 677092.*



Log-in procedure

Step	*What to do ...*	*What takes place ...*
1	Press the key for the first digit of the *User ID* (Example ❶)	This displays the menu for entry of the rest of the digits of your *User ID*.
2	Enter the rest of your *User ID*. An intermittent cursor – ▒ – prompts for entry of digits.	During entry, the entered digits are shown in the display.
3	End the entry of the *User ID* by pressing the ❶-key. An intermittent cursor – ▒ – prompts for entry of digits.	This displays the menu for entry of your *PIN-code*.
4	Enter you *PIN-code*.	During entry, the entered digits are shown as ✳ in the display. If the *PIN-code* is accepted, one of three menus for *unsetting* or *setting* the system is displayed.

Illegal PIN-code

If you enter an illegal *PIN-code*, the buzzer sounds the *Attention Signal* and prompts for entry of another *PIN-code*. After three entries of a wrong *PIN-code*, the *Intrusion Terminal* is blocked for a period (programmable).

☛ Please note that the number of wrong *PIN-code* entries is programmable and may therefore be more or less than three entries.

Getting along ...

See Section 3.3 for information about *unsetting* and Section 3.4 for *setting*.

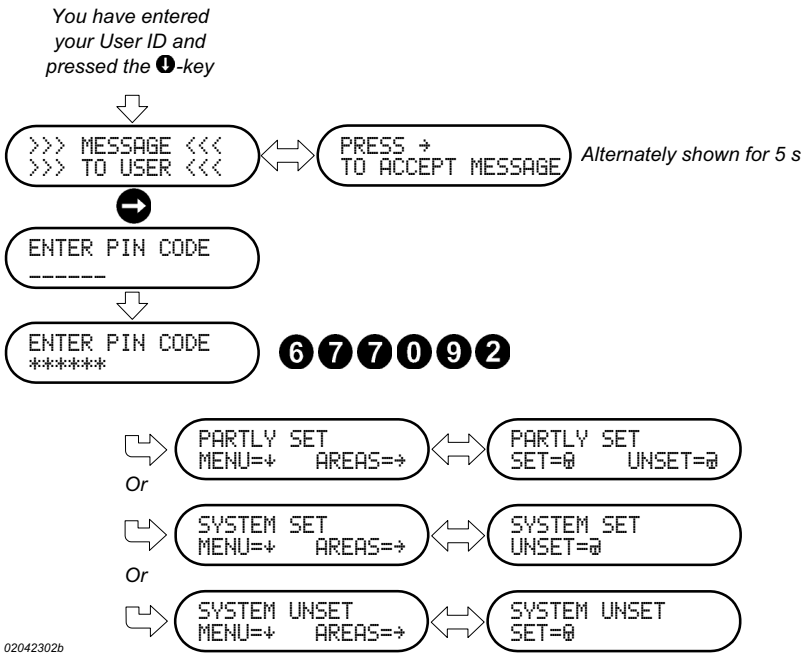
3.2.2 Messages to the user during log-in

During log-in, you may receive up to three messages after you have entered your *User ID*. Each message may consist of up to two lines of up to 16 characters. Three types of messages can be shown:

- A personal message
- A PIN-code expired message
- A general message

After you have read the messages proceed as shown in the figure below and described in the procedure.

Fig. 3.3 *Example of the procedure and the menus used for accepting a message followed by the entry of PIN-code. The example assumes that the PIN-code is 677092.*



Acceptance procedure

Step	*What to do ...*	*What takes place ...*
1	Enter your *User ID* and press the ⬇-key	The message and the instruction for accepting the message are alternately displayed.
2	Press ➔-key to accept the message	This displays the menu for entry of your *PIN-code*.
3	Enter you *PIN-code*. An intermittent cursor – ▒ – prompts for entry of digits.	During entry, the entered digits are shown as ✻ in the display. If the *PIN-code* is accepted, one of three menus for *Unsetting* or *Setting* the system is displayed.

Getting along ...

See Section 3.3 for information about *unsetting* and Section 3.4 for *setting*.

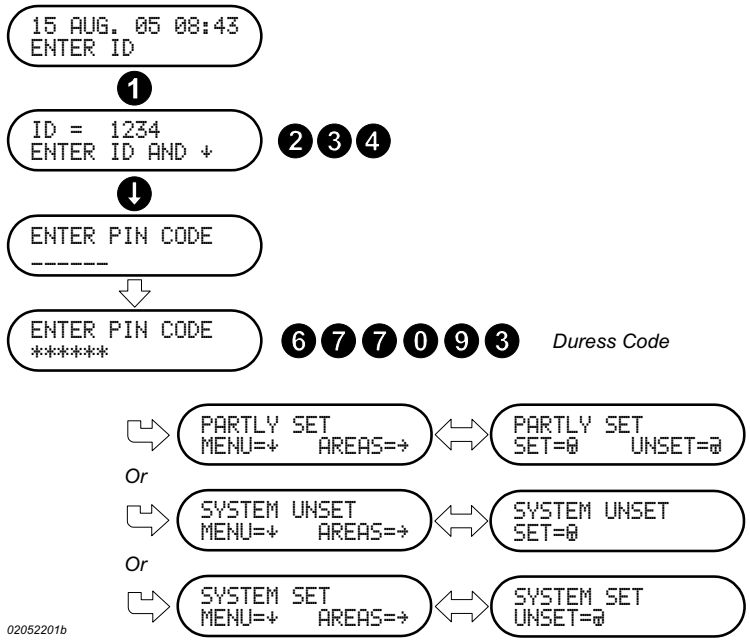
3.2.3 Log-in on an Intrusion Terminal using a Duress Code

Introduction

In duress situations, you can substitute your *PIN-code* with a *Duress Code*. The *Duress Code* is either a fixed code defined by the system manager or a variable code. More information about the *Duress Code* to use is available from your system manager.

When you use the *Duress Code* during log-in, a silent *Alarm* will be sent to the Control Station to which the ThorGuard Intrusion Alarm System is connected. Apart from that, the system will behave normally without any indication of *Alarm*.

Fig. 3.4 *Example of the procedure to use for log-in on an Intrusion Terminal with the Duress Code. The example assumes that the Duress Code is 677092.*



During log-in, you may also start the log-in using either the ❷-key or the ❶-key as described in Sections 3.3.2 and 3.4.2, respectively.

Resetting the duress state

After the *Duress Code* has been used, the *duress state* of ThorGuard Intrusion Alarm System must be *reset*. This *reset* is performed as described in Section 4.4.2.

3.3 Unsetting

Introduction

If you are the first to arrive in the morning, the ThorGuard Intrusion Alarm System is likely to be set. After you have logged in, you must *unset* the *Areas* of the system that you want to access and that you are allowed to *unset*.
You may also experience that the parts of the system are already *partly unset* and that you should *unset* only the parts of the system protecting the areas you want to access.
If the system is *set*, the 0-indicator on the *Intrusion Terminal* is lit after log-in. If *partly set* or *unset*, the 0-indicator remains unlit after log-in.
The actual status of the system (SYSTEM SET, SYSTEM UNSET or PARTLY SET) can be seen after you have logged in as described in Section 3.2.

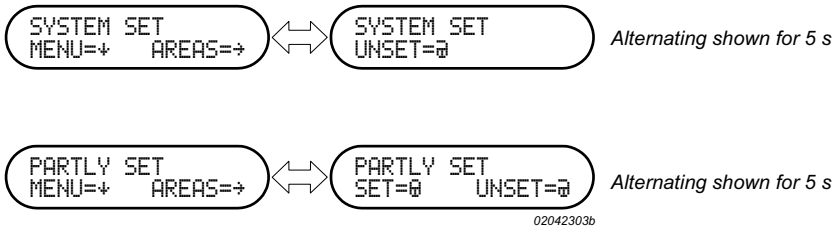
Allowed operations

The parts of the system that you may *unset* (or *set*) and the operations that you are allowed to perform will depend on the *User Profile* assigned to you and the *Reset Rights* and *Operating Rights* allocated to you. In addition, an *Area Mask* may be assigned to the *Intrusion Terminal* limiting operations with the system to be performed only on the *Area(s)* covered by the *Area Mask*.

Ordinary log-in

When you have logged in on the ThorGuard Intrusion Alarm System with the ordinary log-in procedure (Section 3.2.1) with the system *set* or *partly set*, one of two sets of menus is shown on the display of the *Intrusion Terminal* as shown in the Fig. 3.5 below. For more information, see Section 3.3.2.
If the status is SYSTEM UNSET you can log out and safely enter your *Area*.

Fig. 3.5 *Example of the menus that can be shown on the Intrusion Terminal after an ordinary log-in. The 0-indicator is lit if the system is set and extinguished if Partly Set or fully Unset.*



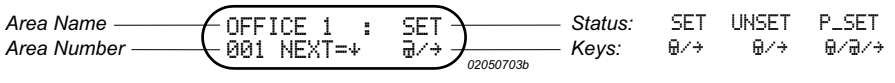
Available function keys

In both cases of Fig. 3.5, you can use the →-key to present a list of the *Areas* or the 0-key to jump to a menu with the first *Area* you are allowed to *unset*.
To proceed in the menu system, if you do not want to *unset*, press the ↓-key. See Fig. 2.4 for more information. With the status PARTLY SET, you can also use the 0-key to if you want to *set* your *Areas*. See Section 3.4 for more information.

Log-in starting with the 0- key

If you log-in with the purpose to *unset* the system or parts of the system, you can start the log-in procedure by pressing the 0-key, and then continue by entering your *User ID* and the *PIN-code*. This will display a menu of the type shown in Fig. 3.6 below. The status shown may be either SET, UNSET, or P_SET. For more information, see Section 3.3.1

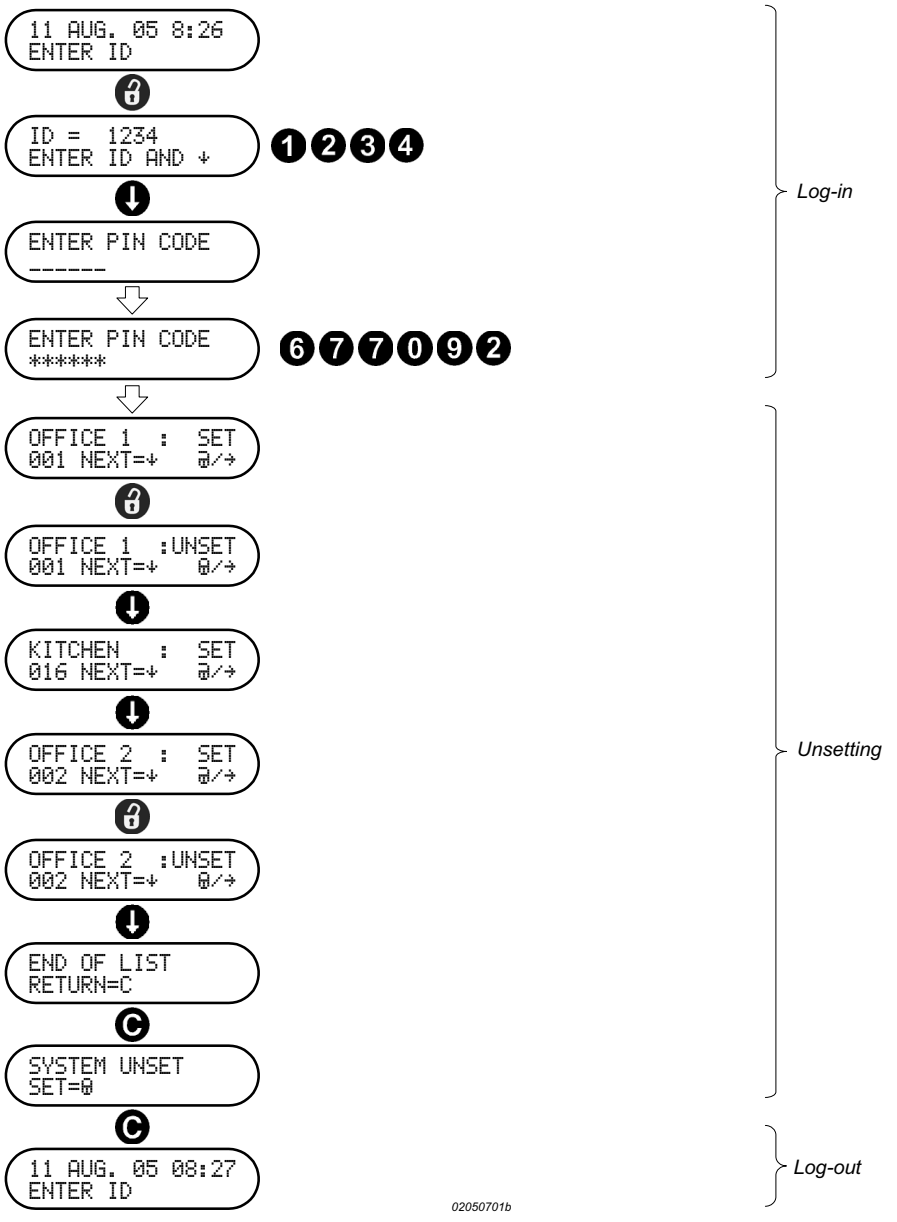
Fig. 3.6 *Example of the type of menu shown on the Intrusion Terminal after a log-in where you start by pressing the 0-key prior to the actual log-in.*



3.3.1 Unsetting after log-in starting with the ❶-key

After log-in using the ❶-key first, the first *Area* the *User* is allowed to *unset* will be shown in the display. The first line of the display shows the status of the *Area*; the following line shows the actions that can be performed with the function keys.

Fig. 3.7 *Example of unsetting after log-in with ❶-key first. The user unsets the areas with the names* OFFICE 1 *and* OFFICE 2 *and skips the unsetting of the area with the name* KITCHEN.



If you are allowed to *unset* more areas, you can display these by pressing the ❶-key and *unset* them as shown in the figure above. When you have stepped through all *Areas* accessible from this *Intrusion Terminal*, the display will show END OF LIST. To log out, press the ❍-key twice.

3.3.2 Unsetting after ordinary log-in

Introduction

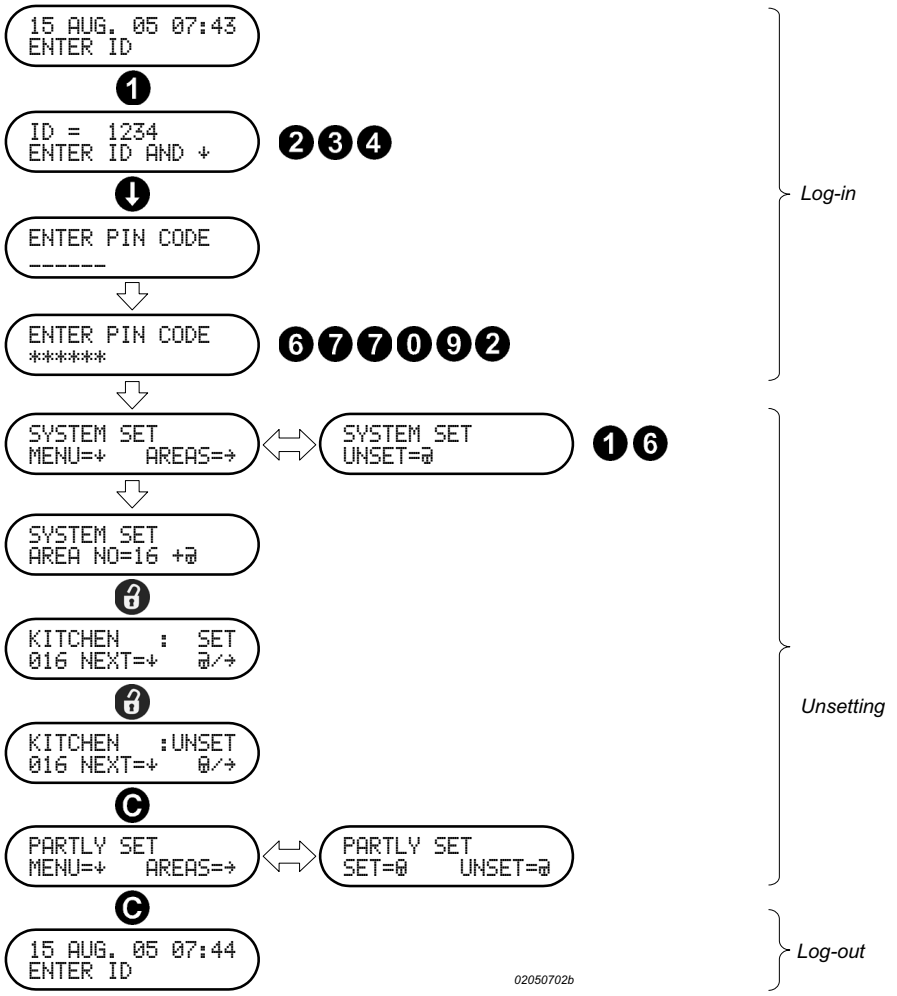
After log-in using the ordinary procedure, the system status will be shown in the display. The first line of the display shows the status of the system; the following line shows the actions that can be performed with the function keys. The display alternates between two menus to indicate the function keys to use to proceed with the *unsetting*.
However, you can also enter the number of the *Area* you want to *unset* to jump directly to the menu for *unsetting* this *Area* as shown in the example below.

Available function keys

You can use the ➔-key to present a list of the *Areas* or the 0-key to jump to a menu with the first *Area* you are allowed to *unset*.
However, you can also enter the number of the *Area* you want to *unset* to jump directly to the menu for *unsetting* this *Area* as shown in the Fig. 3.8 below.

To proceed in the menu system if you do not want to *unset*, press the ↓-key. See Fig. 2.4 for more information.
With the status PARTLY SET, you can also use the 0-key to if you want to *set* your *Areas*. See Section 3.4 for more information.

Fig. 3.8 *Example of unsetting after ordinary log-in. The user unsets the area with the name* KITCHEN *and the number* 16.



3.3.3 Unsetting an area containing a Time Lock

Introduction

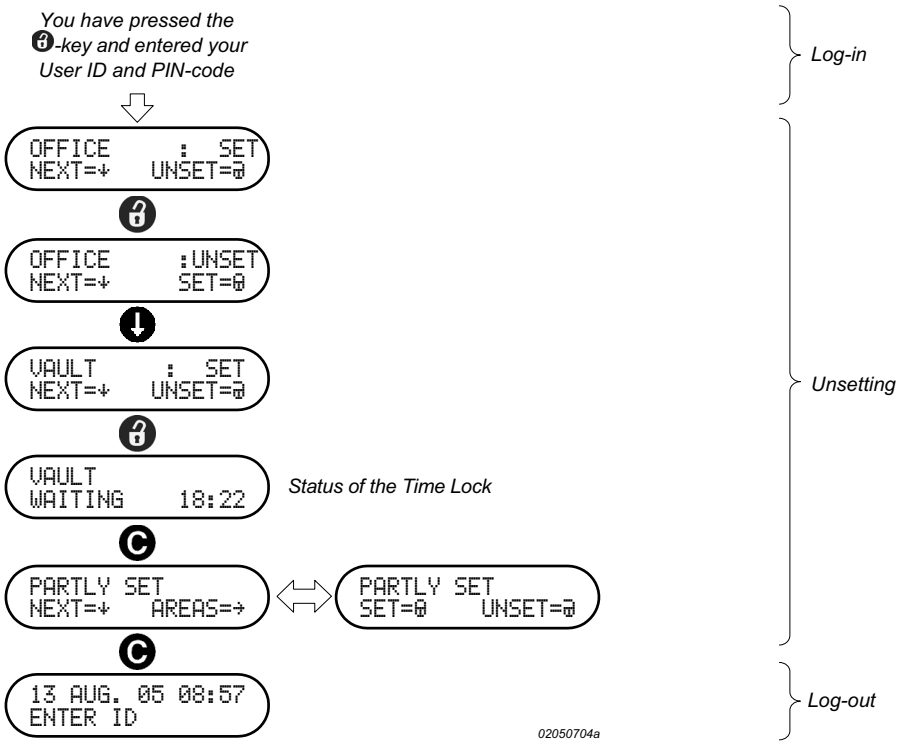
A *Time Lock* handles the time controlled access to a vault or a safe by electrically operating the securing device of the door of the vault or the safe while monitoring whether the lock is unlocked or locked. *Time Locks* can be operated manually or automatically.

Automatic release

If the automatic release of The *Time Lock* has been selected during the programming of the ThorGuard Intrusion Alarm System, the release of the lock will automatically be started when the *Area* to which it belongs is *unset*.

The *Time Lock* will be *unset* immediately. The release process of the *Time Lock* is time controlled and you can follow the count down of the various periods on the display of the *Intrusion Terminal* where also the status of the *Time Lock* is shown. If the *Area* contains more *Time Locks* that are automatically *unset* together with the *Area*, the release process of the *Time Lock* with the lowest number will be shown on the display of the *Intrusion Terminal*.
If you do not want to follow the release process, you can press the ❸-key to cancel the display of the release process. The display thus returns to the display of the current system status.
Although the release process is automatic, you will still have to unlock and lock the lock and to open and close the door. See Section 8.2.1 for more information.

Fig. 3.9 *Example of the Unsetting of an Area containing a Time Lock.*



Viewing the release process again

From the display of the system status, you can press the ❺-key plus the ❻-key and the ❶-key to jump to the TIME LOCK LIST menu if you want to follow the release process again. From this menu, you can press the ❿-key see the status of the *Time Lock* or step through a number of menus if more *Time Locks* are associated with the *Area*. See also Section 8.2.1.

☛ Please note that the release process is stopped automatically if the *Area* becomes *set*. Likewise, the *Area* becomes automatically *set* when the lock of the vault or safe becomes locked.

Manual release

Manual release of a *Time Lock* takes place via the TIME LOCK menu. See Section 8.2.1 for more information

3.4 Setting

Introduction

When you leave your *Area* or *Areas* as the last person, you must *set* your *Area* or the *Areas* of the system that you are allowed to *set*. You may experience that the system is *partly set* which in this context means that parts of the system are already *set* while the remaining parts are *unset*. This means that you must *set* the parts of the system protecting the *Area* or *Areas* you are about to leave.
The *unset* system and *partly set* system are both indicated by an unlit 🔒-indicator on the *Intrusion Terminal* after log-in. The actual status of the system (SYSTEM UNSET or PARTLY SET) can be seen after you have logged in as described in Section 3.2.

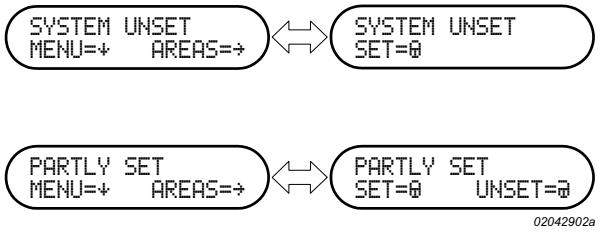
Allowed operations

The parts of the system that you may *set* (or *unset*) and the operations that you are allowed to perform will depend on the *User Profile* assigned to you and the *Reset Rights* and *Operating Rights* allocated to you.
In addition, an *Area Mask* may be assigned to the *Intrusion Terminal* limiting operations with the system to be performed only on the *Area(s)* covered by the *Area Mask*.

Ordinary log-in

When you have logged in on the ThorGuard Intrusion Alarm System with the ordinary log-in procedure (Section 3.2.1) with the system *unset* or *partly set*, one of two sets of menus is shown on the display of the *Intrusion Terminal* as shown in the Fig. 3.10 below. For more information, see Section 3.4.2.

Fig. 3.10 *Example of the menus that can be shown on the Intrusion Terminal after log-in. In both cases, the 🔒-indicator is extinguished after log-in.*



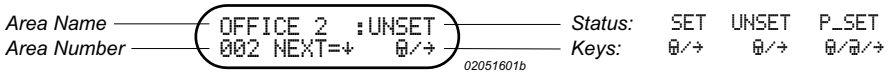
Available function keys

In both cases of Fig. 3.10, you can use the ➡-key to view a list of the *Areas* or the 🔒-key to jump to a menu with the first *Area* you are allowed to *set*.
To proceed in the menu system, if you do not want to *set*, press the ⬇-key. See Fig. 2.4 for more information. With the status PARTLY SET, you can also use the 🔓-key to if you want to *unset* your *Areas*. See Section 3.3 for more information.

Log-in starting with the 🔒- key

If you log-in with the purpose to *set* the system or parts of the system, you can start the log-in procedure by pressing the 🔒-key, and then continue by entering your *User ID* and the *PIN-code*. This will display a menu of the type shown in Fig. 3.11 below. The status shown may be either SET, UNSET, or P_SET. For more information, see Section 3.4.1

Fig. 3.11 *Example of the type of menu shown on the Intrusion Terminal after log-in with 🔒-key first. The 🔒-indicator will be extinguished if the system is Partly Set or Unset.*

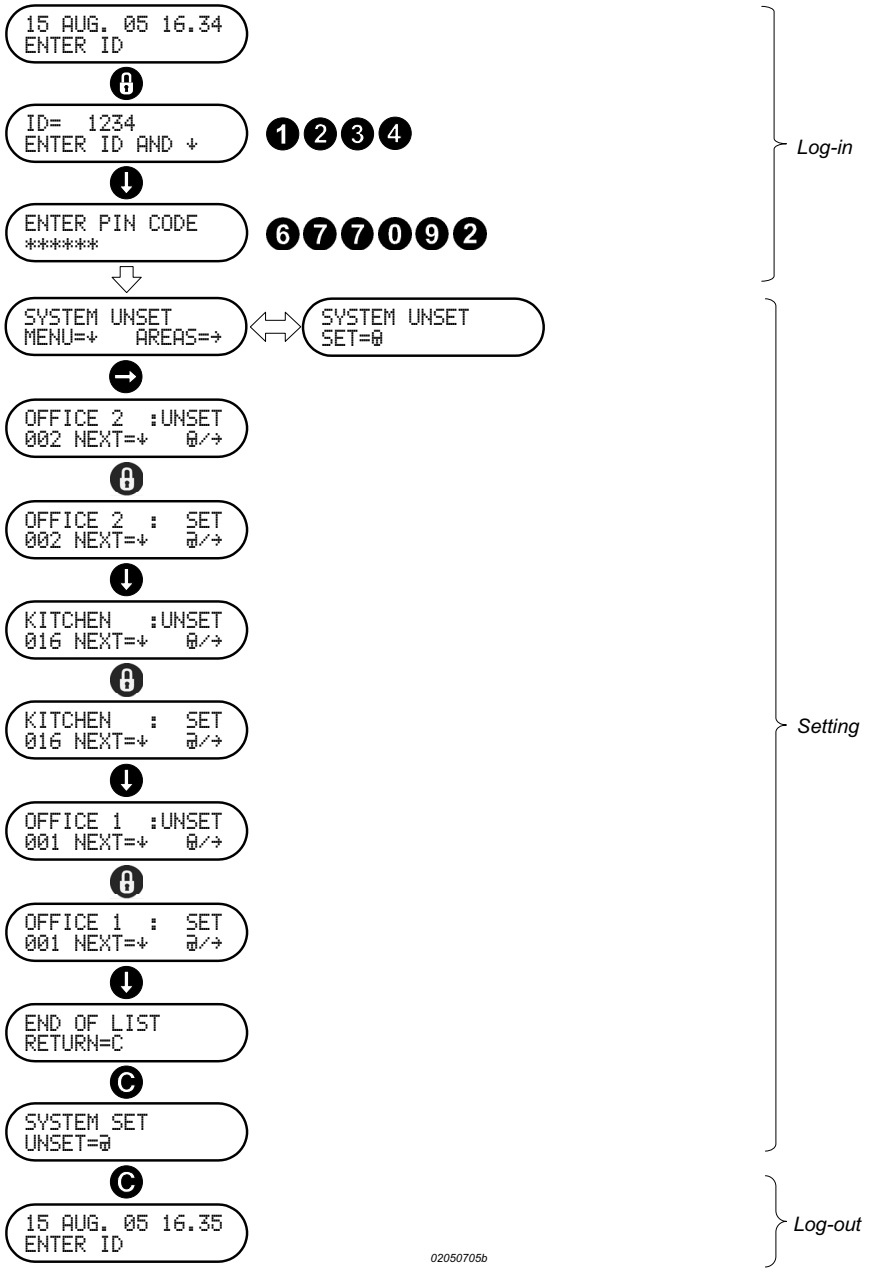


3.4.1 Setting after log-in starting with the ⓪-key

Introduction

When you start the log-in by pressing the ⓪-key, and then enter your *User ID* and the *PIN-code*, the first line display shows the status of the first *Area* that you are allowed to *set*; the following line shows the actions that can be performed with the function keys. See the example of Fig. 3.12 below.

Fig. 3.12 *Example of setting after a log-in that starts by pressing the ⓪-key. The user sets the areas with the names* OFFICE 2, KITCHEN *and* OFFICE 1.



Set faults

If *active Inputs* prevent the *setting* of the system (*Set Faults*), you may *isolate* the *Inputs* as described in Section 3.4.3 or you can make a *Forced Setting* as described in Section3.4.4.

3.4.2 Setting after ordinary log-in

Introduction

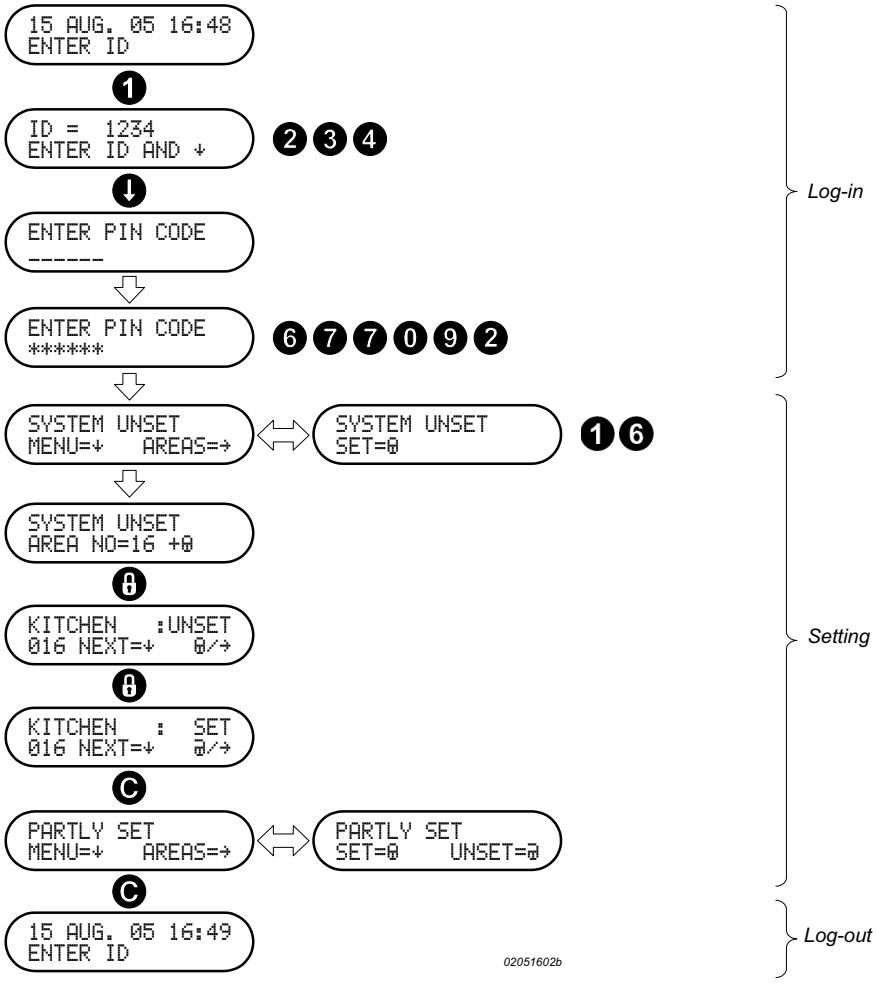
When you have logged in on the ThorGuard Intrusion Alarm System with the ordinary log-in procedure (Section 3.2.1) with the system *unset* or *partly set*, one of two sets of menus is shown on the display of the *Intrusion Terminal* (Fig. 3.10).

The first line of the display shows the status of the system; the following line shows the actions that can be performed with the function keys. The display alternates between two menus to indicate the function keys to use to proceed with the *setting*.

Available function keys

You can use the ➔-key to present a list of the *Areas* or the 🔒-key to jump to a menu with the first *Area* you are allowed to *set*.
However, you can also enter the number of the *Area* you want to *set* to jump directly to the menu for *setting* this area as shown in the Fig. 3.13 below.
To proceed in the menu system, if you do not want to *unset*, press the ⬇-key.
See Fig. 2.4 for more information.

Fig. 3.13 *Example of setting after ordinary log-in. The user sets the area with the name* KITCHEN *and the number* 16.



Set faults

If *active Inputs* prevent the *setting* of the system (*Set Faults*), you may *isolate* the *Inputs* as described in Section 3.4.3 or you can make a *Forced Setting* as described in Section 3.4.4.

3.4.3 Isolation of an active input during setting

Introduction

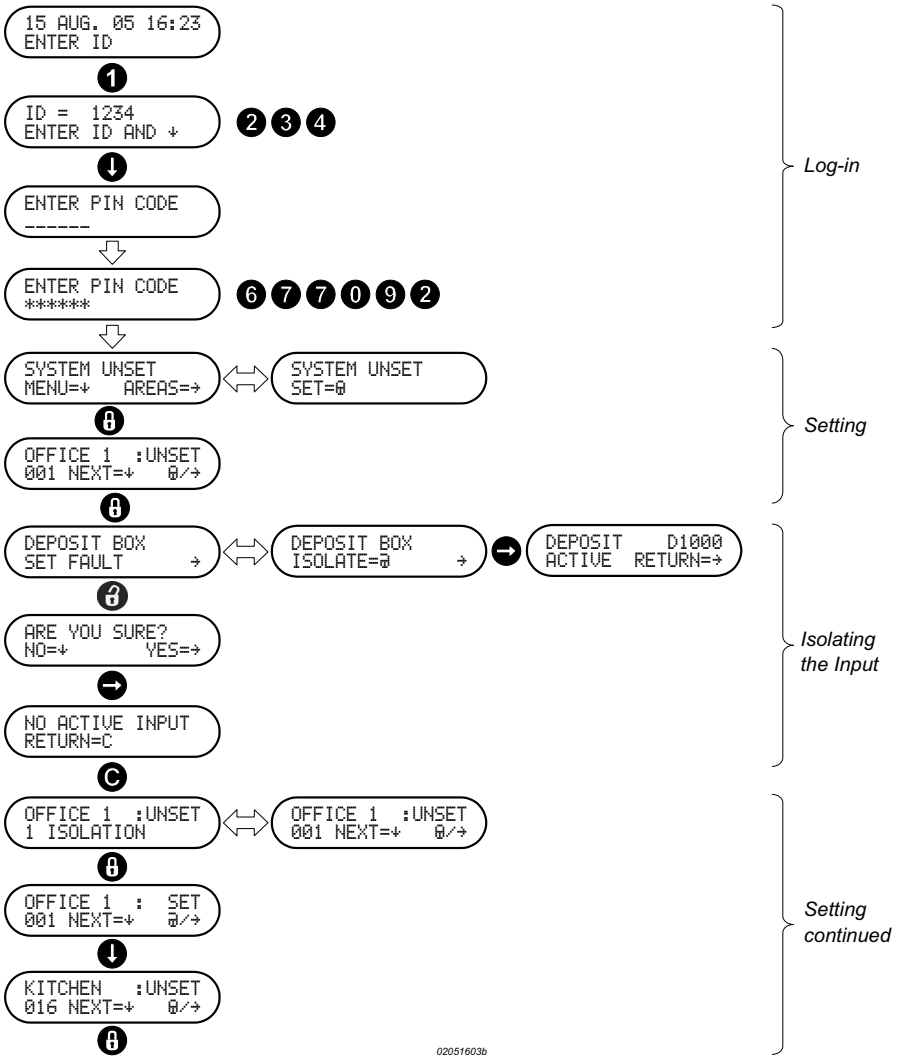
If an *Input* of an *Area* is *active* when you *set* the *Area*, the *setting* will be cancelled and the display of the *Intrusion Terminal* will show a *Set Fault* (SET FAULT) for the *Input* in question. The name of the *Input* will be shown in the display.
If the fault cannot be removed, the *Input* may be *isolated*, meaning that the *Input* is temporarily taken out of duty, so that no *Alarm* is generated when the *Area* is *set*.

Isolation rights

The rights to *isolate* an *Input* depend on the configuration of the *Input*, the *User Profile* and the number of *Isolations* allowed for this particular *Zone.* If you have no rights to *isolate Inputs* or the number of allowed *isolated Inputs* is exceeded, you can make a *Forced Setting* if this is allowed by your *User Profile.*

☛ When you *isolate* an *Input,* you must be aware that this will degrade the security level of the ThorGuard Intrusion Alarm System. To maintain the security level, you can perform a *Forced Setting*. See Section 3.4.4.

Fig. 3.14 *Example of setting and isolation of an input after an ordinary log-in. During setting of the area* OFFICE 1*, a set fault appears for the input* DEPOSIT BOX*. The input is isolated to allow the user to set other areas and log out.*



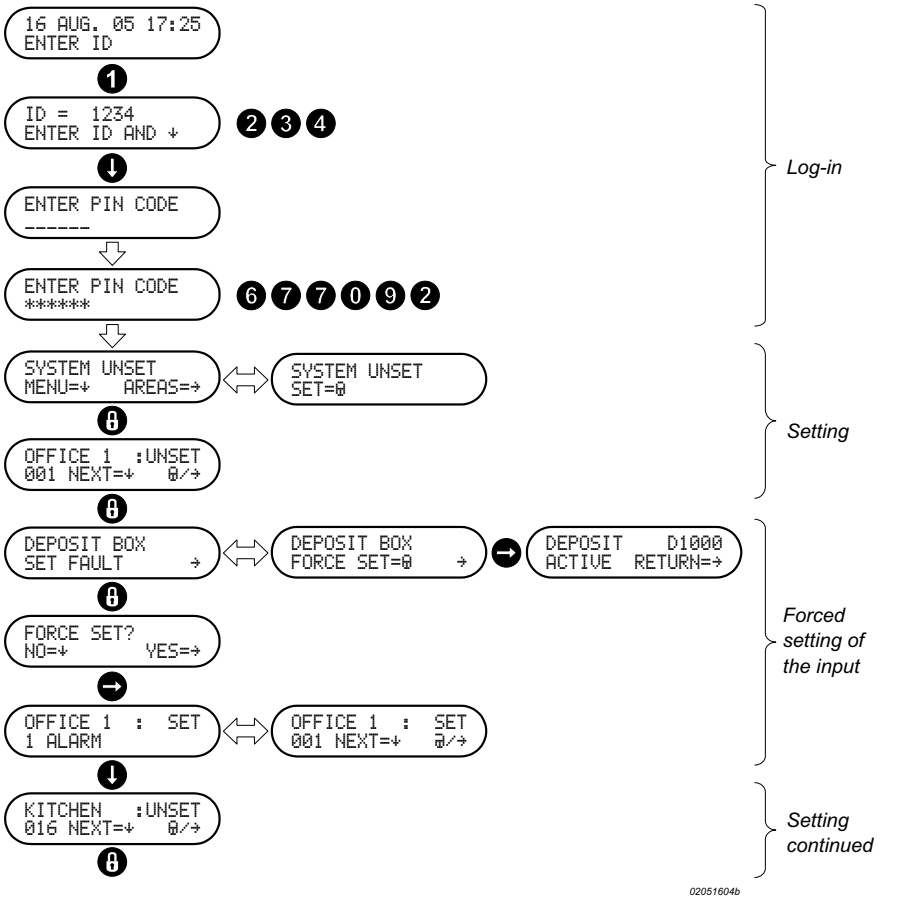
Continue the *setting* by using the ❶-key to jump to the next *Area* to set and the ❽-key to *set* the *Area*. When you have stepped through all *Areas* accessible from this *Intrusion Terminal*, the display shows END OF LIST. To log out, press the ❍-key twice.
*Isolation*s are cancelled when you *unset* the system or the individual *Inputs*. See also Section 3.6.1.

3.4.4 Forced setting of the system

If you are not allowed to *isolate Inputs* or have exceeded the number of allowed *Isolations*, you can make a *Forced Setting* of the system, if this is allowed by your *User Profile*.
The *Forced Setting* maintains the security level of the system instead of the degraded level caused by the *Isolation* of one or more *Inputs*. However, the *Forced Setting* of a system with one or more *active Inputs* – except those of the entry and exit paths – will always generate an *Alarm*.

The *Alarm* generated by the *Forced Setting* will be handled by the Central Alarm Station to which the ThorGuard Intrusion Alarm System is connected.

Fig. 3.15 *Example of forced setting of an area.*



3.5 Display and clearing of alarms and faults

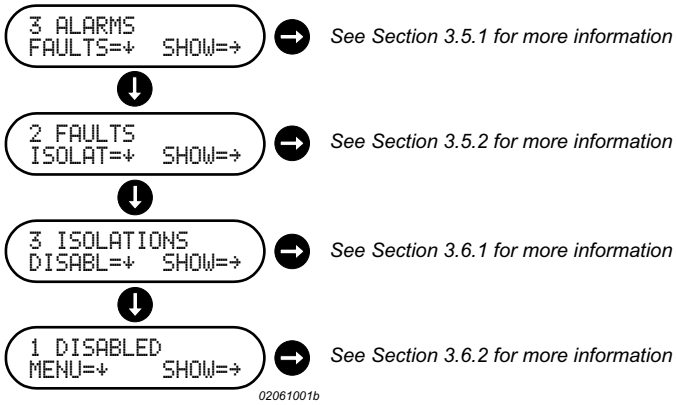
Introduction

As mentioned previously in Section 3.2, the ThorGuard Intrusion Alarm System logs various types of events such as:

- *Alarms*
- *Faults*
- *Isolations*
- *Disabled Inputs*

If *Alarms*, *Faults*, *Isolations* or *Disabled Inputs* are present when you log in, the display of the *Intrusion Terminal* will present a menu with the *Alarm* status. From this menu, you can reach menus with display of the status for *Faults*, *Isolations* and *Disabled Inputs*. See the example below.

Fig. 3.16 *Examples of the status menus available. Status menus for events that have not taken place are automatically omitted.*



The menus are accessible in the sequence listed above. Status menus for events that have not taken place are automatically omitted.
From the status menus, you can access menus with data for the individual *Alarms*, *Faults*, *Isolations* or *Disabled Inputs*.

3.5.1 Display and clearing of alarms

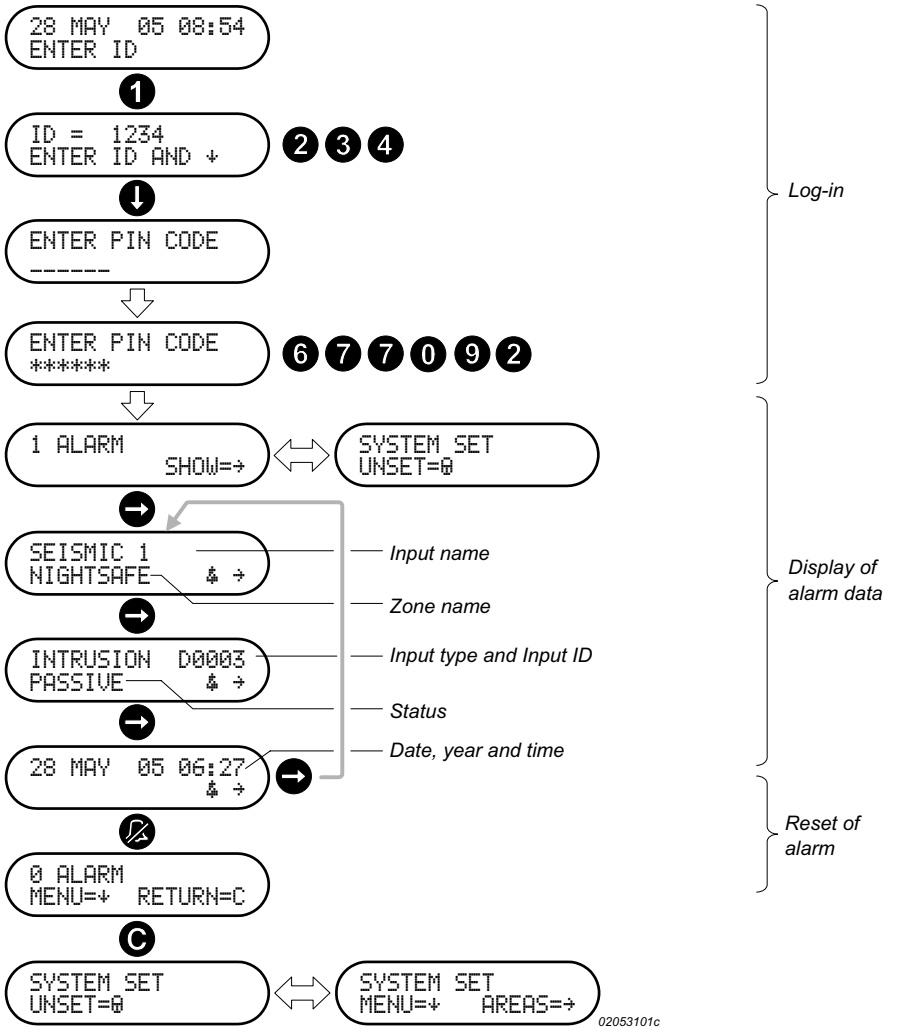
Introduction

If the system is in *Alarm* state, all local alarm indicators (Bells, buzzers, sirens, lights, etc.) will be passivated (switched off) when you log in and the *Alarm* status will be displayed (Fig. 3.17).
If the *Alarm* is generated after log-in, the local alarm indicators will be passivated when you press the C-key.

The display of the *Intrusion Terminal* will alternately show the *Alarm* status (Number of *Alarms*) and the system status (SET, UNSET, or PARTLY SET). From this, you can press the →-key to go to the beginning of a list of *Alarms* that contain information about the individual *Alarms*. The *Alarms* are listed in order of occurrence. However, *Hold-up Alarms* will always be displayed first, if present.

The *Alarms* can be *cleared* in case your *User Profile* includes rights to *clear Alarms* of the type you want to *clear*. The *Alarms* can be *cleared* one at a time or you can go through the list of *Alarms* and *clear* them one at a time as explained in the following paragraphs or you can combine the two methods.

Fig. 3.17 *Example of display of the data of a single Alarm and the clearing of the Alarm.*



Display and clearing of individual alarms

When the *Alarm* status display is shown, you can press the ➲-key to go to the beginning of the *Alarm* list. This displays the first *Alarm* in the list with the *Input name* and the *Zone* to which it belongs.
If you press the ➲-key once more, the display will show *Input Type* and *Input ID* plus the current status (*Active* or *passive*). Pressing the ➲-key once more, the date, year and time for the *Alarm* will be shown.

When displaying the *Alarm* data, you can press the ⍉-key to *clear* the *Alarm*. After this, you can press the ⓓ-key to display the next *Alarm* in the list and repeat the procedure for displaying *Alarm* data and *clearing Alarms*.
When the *Alarm* status display shows `0 ALARM`, you can press the ⓒ-key twice to log-out or the ⓓ-key to display any *Faults* (See Section 3.5.2).

Going through alarm list

When the *Alarm* status display is shown, you can press the ➲-key to go to the beginning of the *Alarm* list. Then you can press the ⓓ-key repeatedly to go through the complete list. For each *Alarm*, you can see the *Input name* and the *Zone* to which it belongs.
Alarms will be displayed in order of occurrence. However, *Hold-up Alarms* will always be displayed first, if present.

Clearing of all alarms

When you reach the end of the list, the display will show `RESET ALL ALARMS?`. By pressing the ➲-key, all *Alarms* will be *cleared* depending on your *User Profile* and the state of the *Input* (*Active* or *Passive*).
When the *Alarm* status display shows `0 ALARM`, you can press the ⓒ-key twice to log-out or the ⓓ-key to display any *Faults* (See Section 3.5.2).

Clearing fails

If it is not possible to *clear* an *Alarm*, an error message such as `NOT ALLOWED` is shown on the display. A failing *clearing* attempt may be caused by an *active Input* or that your *User Profile* does not allow you to *clear* this type of *Alarm*.

3.5.2 Display and clearing of faults

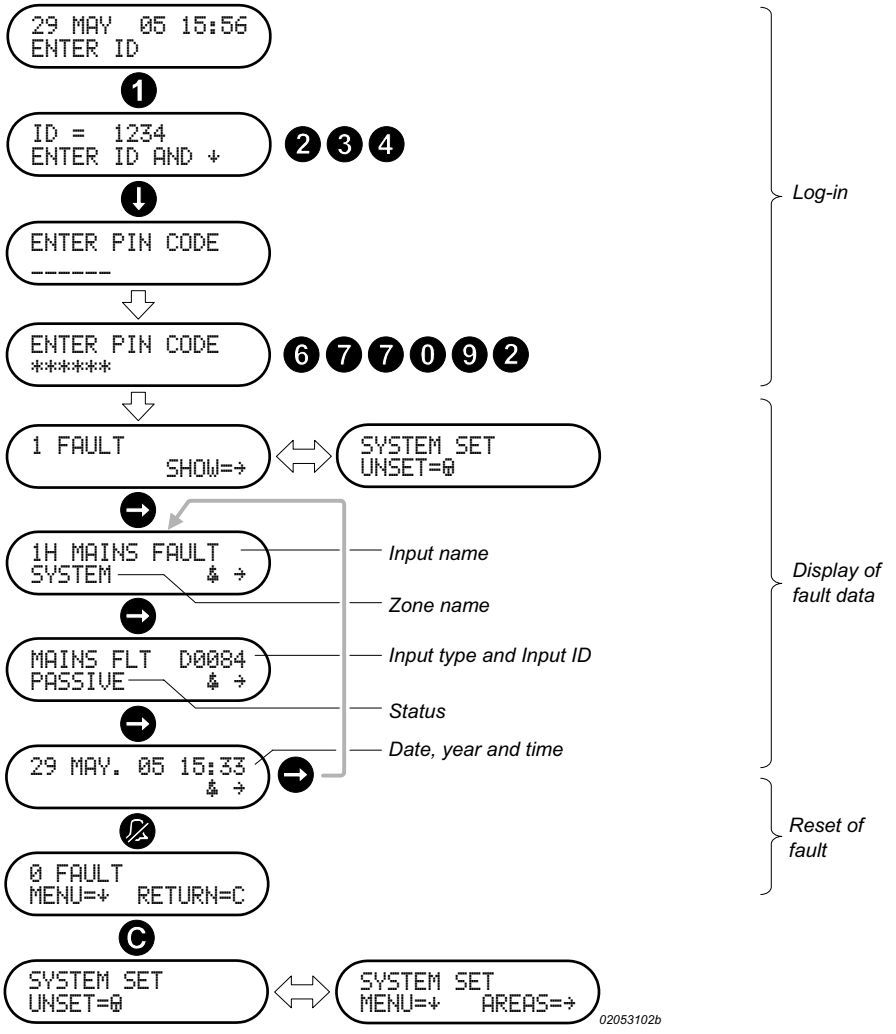
Introduction

If the system is in *Fault* state when you log in, the *Fault* status will be shown on the display of the *Intrusion Terminal* provided that no *Alarms* are present. If so these will be shown first.
The display will alternately show the *Fault* status (Number of *Faults*) and the system status (SET, UNSET, or PARTLY SET). See Fig. 3.18.

From this, you can press the ➔-key to go to the beginning of a list of *Faults* that contain information about the individual *Faults*. The *Faults, if more,* are listed in order of occurrence.

The *Faults* can be *cleared* in case your *User Profile* includes rights to *clear Faults* of the type you want to *clear*. The *Faults* can be *cleared* one at a time or you can go through the list of *Faults* and *clear* them one at a time as explained in the following paragraphs or you can combine the two methods.

Fig. 3.18 *Example of display of the data of a single Fault and the clearing of the Fault.*



Display and clearing of individual faults

When the *Fault* status display is shown, you can press the ➔-key to go to the beginning of the *Fault* list. This displays the first *Fault* in the list with the *Input name* and the *Zone* to which it belongs.
If you press the ➔-key once more, the display will show *Input Type* and *Input ID* plus the current status (*Active* or *passive*). Pressing the ➔-key once more, the date, year and time for the *Fault* will be shown.

When displaying the *Fault* data, you can press the ⎚-key to *clear* the *Fault*.
After this, you can press the ↓-key to display next *Fault* in the list and repeat the procedure for displaying the *Fault* data and *clearing* the *Fault*.
When the *Fault* status display shows `0 FAULT`, you can press the C-key twice to log-out or the ↓-key to display any *Isolation* (See Section 3.6.1).

Going through fault list

When the *Fault* status display is shown, you can press the ➔-key to go to the beginning of the *Fault* list. Then you can press the ↓-key repeatedly to go through the complete list. For each *Fault*, you can see the *Input name* and the *Zone* to which it belongs. *Faults* will be displayed in order of occurrence.

Clearing of all faults

When you reach the end of the list, the display will show `RESET ALL FAULTS?`.
By pressing the ➔-key, all *Faults* will be *cleared* depending on your *User Profile* and the state of the *Input* (*Active* or *Passive*).
When the *Fault* status display shows `0 FAULT`, you can press the C-key twice to log-out or the ↓-key to display any *Isolation* (See Section 3.6.1).

Clearing fails

If it is not possible to *clear* a *Fault*, an error message such as `NOT ALLOWED` is shown on the display. A failing *clearing* attempt may be caused by an *active Input* or that your *User Profile* does not allow you to *clear* this type of *Fault*.

3.6 Display of isolations and disabled inputs

Introduction

Isolated Inputs and *Disabled Inputs* are *Inputs* taken temporarily taken out of duty either by the *User* if he is allowed to do so (*Isolated Inputs* - Section 3.4.3) or by the service engineer (*Disabled Inputs* - Section 7.2.7)

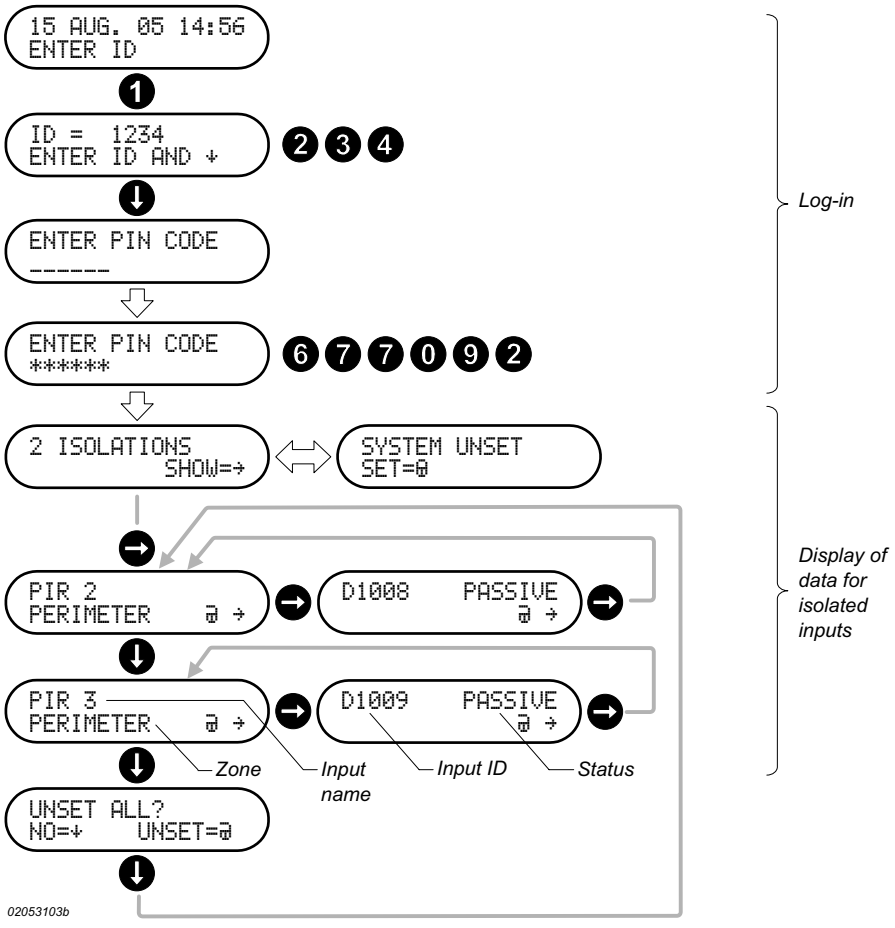
Data about *Isolated* and *Disabled Inputs* can be viewed by the *User* and *Isolated Inputs* can be put back into duty again if your the *User Profile* allows this (See Sections 3.6.1 and 3.6.2 more information. *Disabled Inputs* can be enabled only when the ThorGuard Intrusion is in *Service Mode* (See *Section* 7.2.7).

3.6.1 Display of data for isolated inputs

Introduction

If the system has *Isolated Inputs* when you log in, the status of *Isolations* (Number of *Isolations*) will be shown on the display of the *Intrusion Terminal* provided that no *Alarms* or *Faults* are present. If so, *Alarms* will be shown first, then *Faults* can be shown and finally, *Isolated Inputs*. The *Isolated Inputs*, if more, are listed in order of the *Input ID* (Number) of the *Input*.

Fig. 3.19 *Example of display of the individual data of two isolated inputs*



Display of individual isolations

When the *Isolation* status display is shown, you can press the ➔-key to go to the beginning of the *Isolation* list. This displays the first *Isolation* in the list with *Input name* and the *Zone* to which it belongs.
If you press the ➔-key once more, the display will show the *Input ID* and the current status of the *Input* (*Active* or *passive*).

Unset of individual isolations

When displaying the data of an *Isolated Input*, the *Input c*an be taken out of the *Isolation* by pressing the ⓘ-key. This *unsets* the *Input* and cancels the *Isolation*. When the *Isolation* status display shows `0 ISOLATIONS`, you can press the Ⓒ-key twice to log-out or the ⬇-key to display any *Disabled Input* (See Section 3.6.2).

Going through isolation list

When the *Isolation* status display is shown, you can press the ➔-key to go to the beginning of the *Isolation* list. Then you can press the ⬇-key repeatedly to go through the complete list. For each *Isolation*, you can see the *Input name* and the *Zone* to which it belongs

Unset of all isolations

When you reach the end of the list, the display will show `UNSET ALL?`. By pressing the ➔-key, all *Isolated Inputs* will be *unset* whereby their Isolation will be cancelled.

3.6.2 Display of data for disabled inputs

Introduction

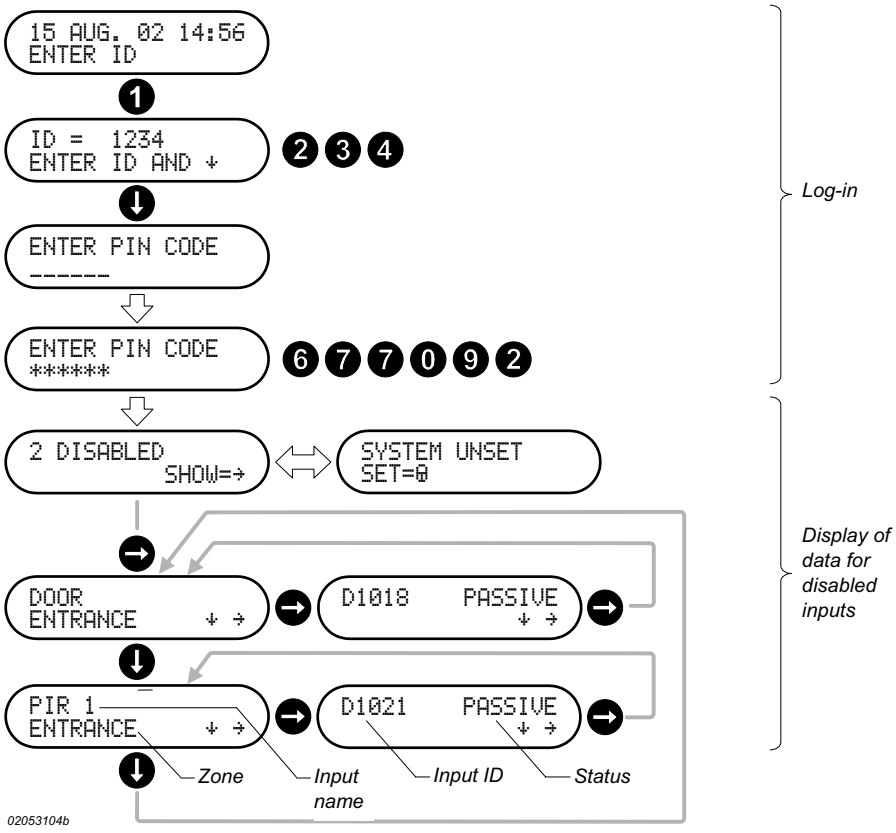
If the system has *Disabled Inputs* when you log in, the status of the *Disabled Inputs* (Number of *Disabled Inputs*) will be shown on the display of the *Intrusion Terminal* provided that the programming of the system allows data for *Disabled Inputs* to be shown and that no *Alarms* or *Faults* are present. If so *Alarms* will be shown first, then *Faults* can be shown, followed by *Isolated Inputs* and finally *Disabled Inputs*.

Display of disabled inputs

All data for the *Disabled Input* can be displayed including its relation to a *Zone*, the name of the *Input*, the current state of the *Input* (*Active* or *Passive*). The *Inputs* are shown in numerical order according to their *Input ID* (Number).

☛ If you want to enable a *Disabled Input*, you must use Menu 57 provided that your *User Profile* allows access to this menu. The same menu is used for *Disabling Inputs*, also.
Disabling of *Inputs* can only be performed when the ThorGuard Intrusion Alarm System is in *Service Mode*. See Section 7.2.7 for more information.

Fig. 3.20 *Example of display of the data of two disabled inputs*



3.7 Delay of the automatic setting function

Introduction

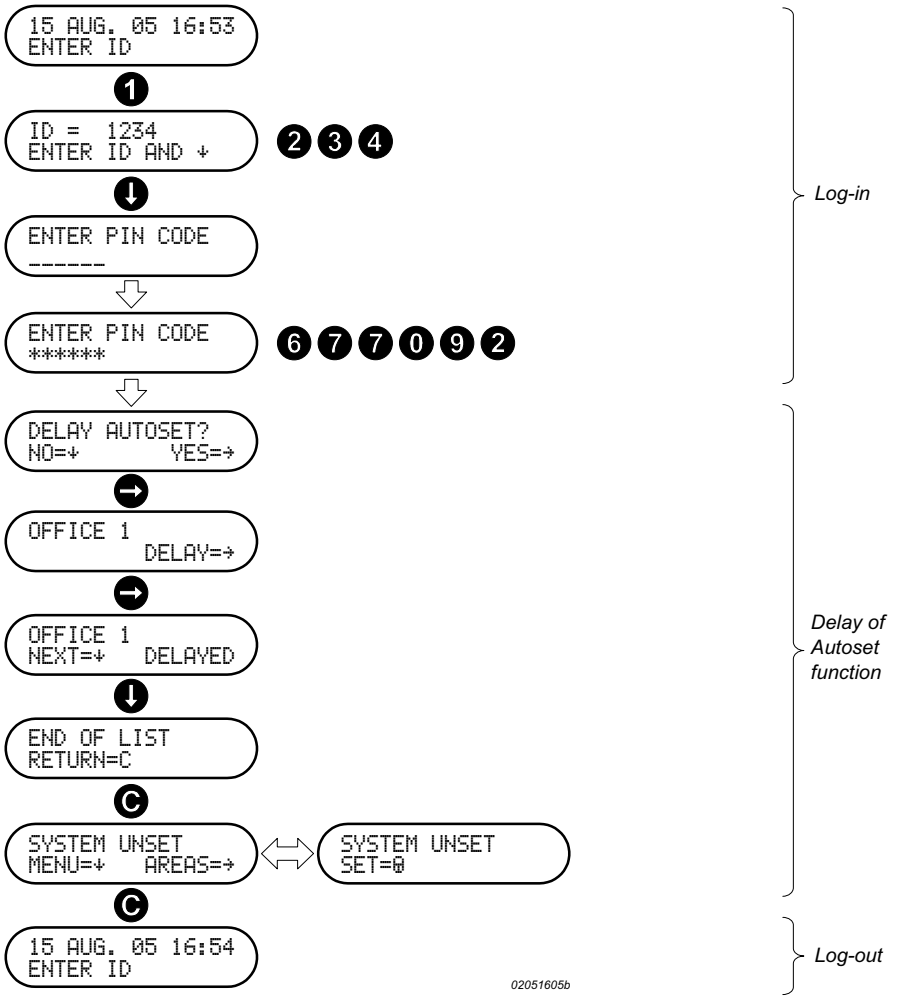
The *Autoset* function performs an automatic setting of one or more *Areas* controlled through a *Week Program*. In cases where work extends beyond the ordinary work time, the *Autosetting* must be delayed to avoid the generation of *Alarms* from persons still present in the *Area*. The delay obtainable is preset during the programming of the ThorGuard Intrusion Alarm System.

Warning signal and warning period

A *Warning Signal* is provided from the built-in buzzer of the *Intrusion Terminal* or from an external acoustical device for example a bell, a buzzer, etc. The *Warning Signal* starts ten minutes (*Warning Period*) before the *Autosetting* takes place.

When you log-in on the *Intrusion Terminal* to delay the *Autosetting*, you will automatically be presented for the menu to use as shown in the figure below.

Fig. 3.21 *Example of the delay of the Autoset function for the Area* OFFICE 1.



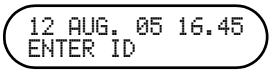
If more *Areas* are linked to the same *Autoset Period*, you can display these by pressing the ⓫-key and delay them by following the procedure outlined in the figure above. When you have stepped through all *Areas* accessible from this *Intrusion Terminal*, the display will show END OF LIST. To log out, press the ⓒ-key twice.

3.8 Log-out

Manual log-out

After you have operated the ThorGuard Intrusion Alarm System, you should log out. This is done by pressing the ⏻-key until a menu with date and time and the text ENTER ID is displayed.

Fig. 3.22 *Example of the display of the Intrusion Terminal after log-out.*



02050301b

Automatic log-out

If you do not log out, an automatic log-out is performed two minutes (normally) after the last operation of any key. At the same time, the back-light of the display is automatically turned off.

Warning

If you perform a log-out with *Alarms* or *Faults* not *cleared*, a warning will be shown on the display of the *Intrusion terminal*.
The warning will be shown for 15 s while the buzzer sounds for the same period. Pressing any key on the *Intrusion terminal* will stop the buzzer.

4

System status menus

Introduction

This chapter describes the System Status menus used for viewing and changing the status of Zones, *Areas*, *Inputs*, for viewing the various types of logs and for resetting the system after a *Duress Code* has been used.

☛ Please note that the access to the System Status menus is controlled by the *User Profile* assigned to you.

This chapter

The chapter contains the following sections:

4.1 Overview

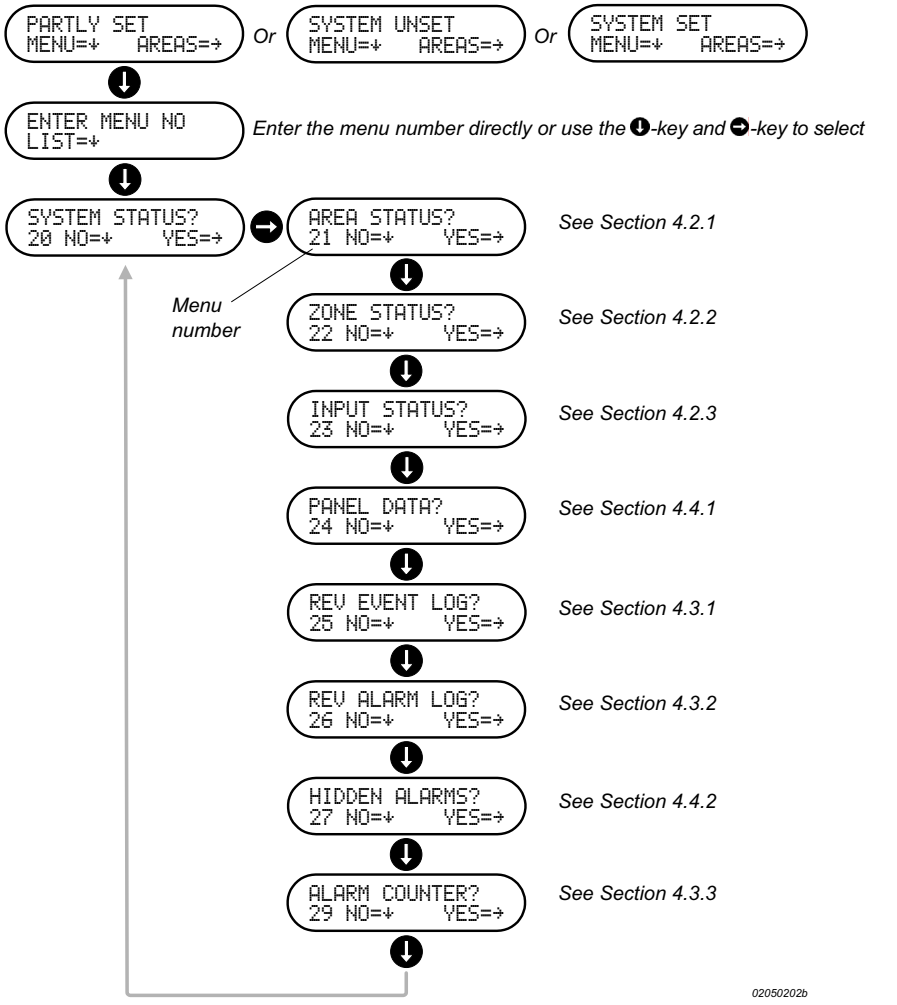
Introduction

The System Status menus comprise the menus shown in Fig. 4.1 below. To access these menus, you must log-in using the procedure of Section 3.2.1. This displays one of the three menus shown in the top of Fig. 4.1, provided that no *Alarms*, *Faults*, *Isolations* or *Disabled Inputs* are present (Section 3.5 and 3.6).

Navigating between menus

Press the ⬇-key to display a menu in which you can select the menu you want by entering its number (Menu 20, 21, 22, 23, 24, 25, 26, 27, or 29) or you can press the ⬇-key once to display the main *System Status menu* (Menu 20). From this, you can press the ➡-key to display the first of the *System Status menus* (Menu 21). The rest of the menus can be displayed one at a time by pressing the ⬇-key repeatedly as shown in Fig. 4.1.

Fig. 4.1 *Example of the menus available from the system status menu (20). The example assumes that no alarms, faults, isolations or disabled inputs are present.*



4.2 Viewing system status information

The menus 21, 22 and 23 provide information about the status of *Areas*, *Zones* and *Inputs* (Detectors), respectively.

4.2.1 Viewing area status (Menu 21)

Introduction

The Area Status Menu (21) allows you to view the *Alarm* status and the *Setting* status for each *Area* included in the *Terminal Area Mask* provided that you are allowed to access the submenus of the Area Status Menu.

Navigating between submenus

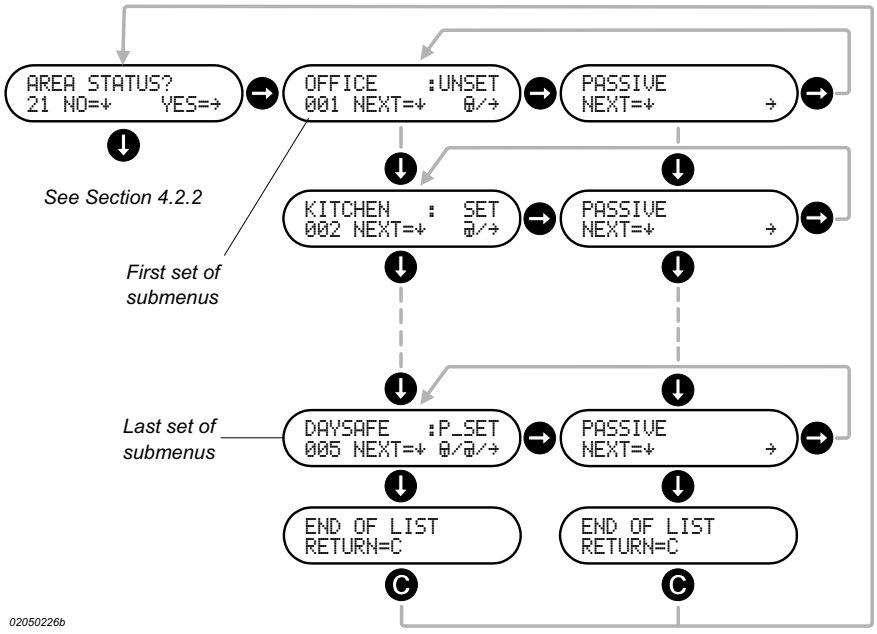
From the Area Status Menu, you can access the first submenu by pressing the ➔-key. The first submenu actually comprises two submenus that you can switch between by pressing the ➔-key. The two submenus comprise all available information about the *Area* in question. See Fig. 4.2 and Fig. 4.3.

From the first as well as the second of these submenus, you can step through the remaining submenus by pressing the ↓-key the appropriate number of times. For each submenu, you can switch between the submenus by pressing the ➔-key.

When you reach the last submenu, the display will show END OF LIST. Pressing the C-key now - or at any time during your way through the submenus - will return you to the Area Status Menu.

When the first of the submenus are shown, you can jump directly to the display of status information for another *Area* by entering its 3-digit number.

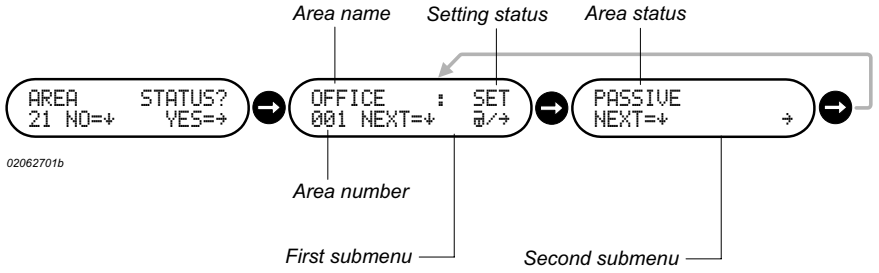
Fig. 4.2 *Example of the display of area status for three out of more areas.*



Setting or unsetting

If the *Alarm* status is *Passive*, an *unset* or *partly set Area* may be logically *set* by pressing the 0-key even though the *Area* may contain *Zones* that are not assigned to your *User Profile*. *Zones* – of the *Area* – assigned to your *User Profile* can be *unset* by pressing the 0-key.

Fig. 4.3 *Example of the status information available in the submenus of the Area Status Menu.*



Status information (first submenu)

The first line of this submenu shows the name of the *Area* plus the *Setting* status that may be one of the following:

SET	The *Area* is *set*.
P_SET	The *Area* is *partly set*.
UNSET	The *Area* is *unset*.

The second line of the submenu shows the *Area* number and indicates the function key to use for *setting* (a = 1) or *unsetting* (a = 2) depending on the *Setting* status and the keys to use for navigation between the submenus (↓ = ↓ and → = →).

Status information (second submenu)

The first line of this submenu shows the *Area* status that may be one of the following:

PASSIVE	No *Input* of the *Area* is activated.
ACTIVE	One or more *Inputs* of the *Area* are activated.
ALARM	One or more *Inputs* of the *Area* are in *Alarm* state.
FAULT	One or more *Inputs* of the *Area* are in *Fault* state.

The second line of the submenu indicates the function keys to use for navigation between the submenus (↓ = ↓ and → =→).

4.2.2 Viewing zone status (Menu 22)

Introduction

The Zone Status Menu (22) allows you to view the *Alarm* status and the *Setting* status for each *Zone* included in the *Terminal Area Mask* provided that you are allowed to access the submenus of the Zone Status Menu.

Navigating between submenus

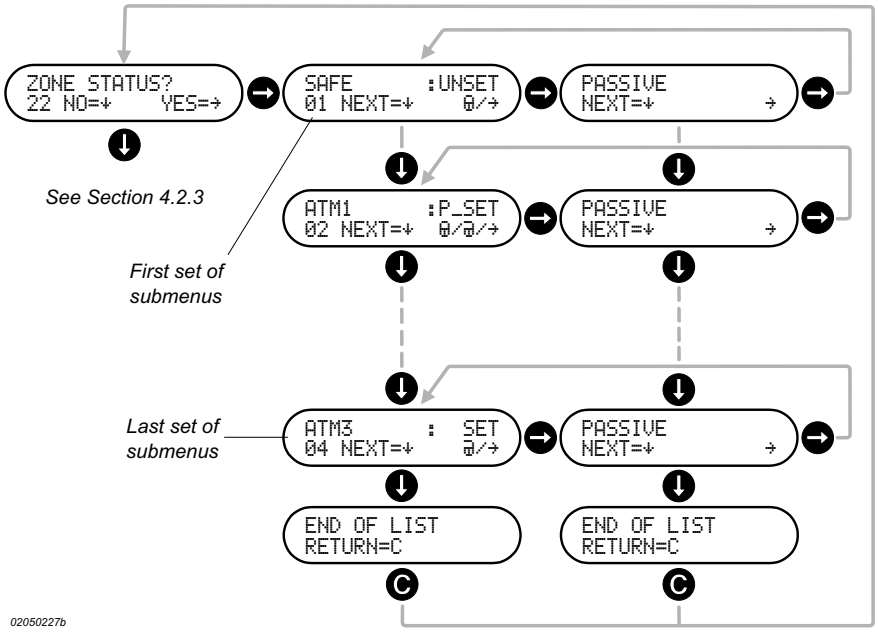
From the Zone Status Menu, you can access the first submenu by pressing the ➔-key. The first submenu actually comprises two submenus that you can switch between by pressing the ➔-key. The two submenus comprise all available information about the *Zone* in question. See Fig. 4.4 and Fig. 4.5.

From the first as well as the second of these submenus, you can step through the remaining submenus by pressing the ↓-key the appropriate number of times. For each submenu, you can switch between the submenus by pressing the ➔-key.

When you reach the last submenu, the display will show END OF LIST. Pressing the C-key now – or at any time during your way through the submenus – will return you to the Zone Status Menu.

When the first of the submenus are shown, you can jump directly to the display of status information for another *Zone* by entering its 3-digit number.

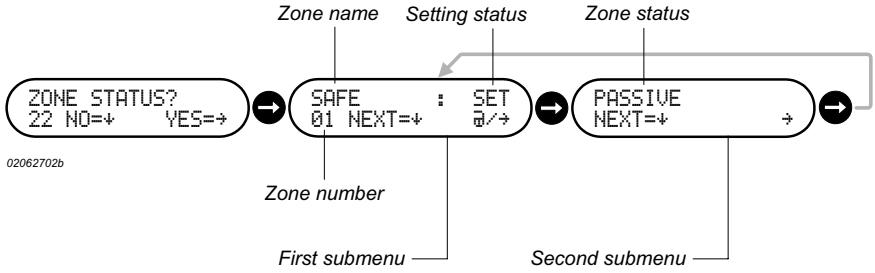
Fig. 4.4 *Example of the display of zone status for thee out of more zones.*



Setting or unsetting

If the *Zone* status is *Passive*, an *unset* or *partly set Zone* may be physically *set* by pressing the ❶-key even though the *Zone* may not be assigned to your *User Profile*.
If the *Zone* belongs to an *Area* assigned to your *User Profile* can be *unset* by pressing the ❷-key.

Fig. 4.5 *Example of the status information available in the submenus of the Zone Status Menu.*



Status information (first submenu)

The first line of this submenu shows the name of the *Zone* plus the *Setting* status that may be one of the following:

SET	The *Zone* is *set*.
P_SET	The *Zone* is *partly set*.
UNSET	The *Zone* is *unset*.

The second line of the submenu shows the *Zone* number and indicates the function key to use for *setting* (⌀ = ●) or *unsetting* (⌀ = ❶) depending on the *Setting* status and the keys to use for navigation between the submenus (↓ = ❶ and → = ➔).

Status information (second submenu)

The first line of this submenu shows the *Zone* status that may be one of the following:

PASSIVE	No *Input* of the *Zone* is activated.
ACTIVE	One or more *Inputs* of the *Zone* are activated.
ALARM	One or more *Inputs* of the *Zone* are in *Alarm* state.
FAULT	One or more *Inputs* of the *Zone* are in *Fault* state.

The second line of the submenu indicates the function keys to use for navigation between the submenus (↓= ❶ and → = ➔).

4.2.3 Viewing input status (Menu 23)

Introduction

The Input Status Menu (23) allows you to view various types of information from all *Inputs* included in the *Zones* common to the *Terminal Area Mask* and the *User Profile* assigned to you. A description of the status information available is described in detail on the following page 4-8.

Navigating between submenus

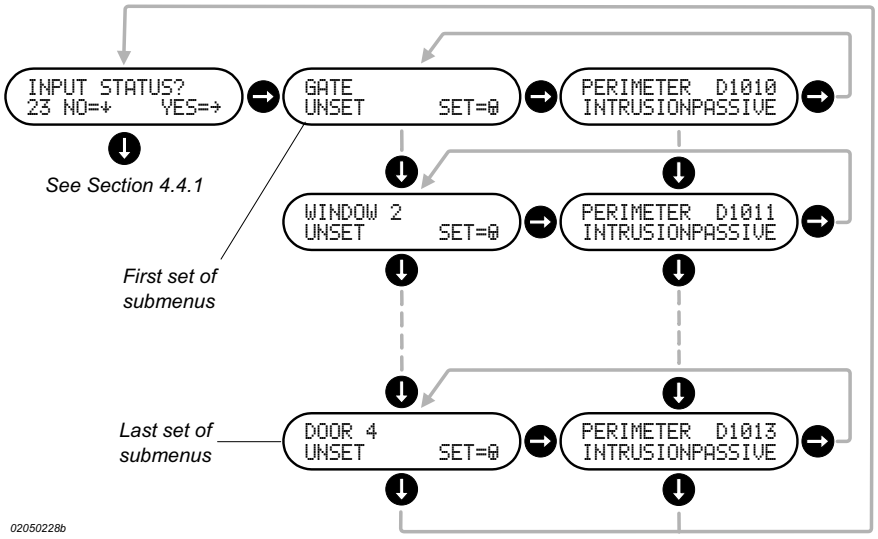
From the Input Status Menu, you can access the first submenu by pressing the ➔-key. The first submenu actually comprises two submenus that you can switch between by pressing the ➔-key. The two submenus comprise all available information about the Input in question. See Fig. 4.6 and Fig. 4.7.

From the first as well as the second of these submenus you can step through the remaining submenus by pressing the ↓-key the appropriate number of times. For each submenu, you can switch between the submenus by pressing the ➔-key.

When you reach the last submenu, the display will show `END OF LIST`. Pressing the C-key now – or at any time during your way through the submenus – will return you to the Input Status Menu.

When the first of the submenus are shown, you can jump directly to the display of status information for another *Input* by entering its 4-digit *Input ID* (Number). When you enter the first digit, a new menu with the text: `NEW INPUT` is shown. Continue to enter the required *Input ID* (Number). Then press the ↓-key to jump to the menu with the status information about the *Input*.

Fig. 4.6 *Example of the navigation between the submenus of the Input Status Menu.*



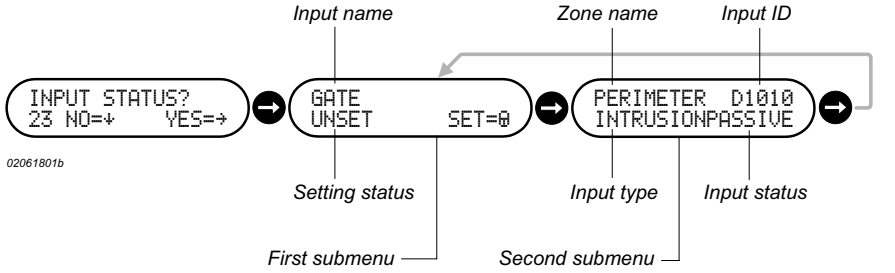
Unsetting or setting

Set Inputs may be *unset* (if allowed) by pressing the 0-key. *Unset Inputs* may be *set* by pressing the 1-key provided the actual *Input* status is passive.

Isolation

If you press the 0-key for an *Input* with the *Input* status passive, the *Input* in question will be *isolated*. *Isolated* inputs may be put in operation again by pressing the 1-key.

Fig. 4.7 *Example of the status information available in the submenus of the Input Status Menu.*



Status information (first submenu)

The first line of this submenu shows the name of the *Input* while the second line shows the *Setting* status that may be one of the following:

SET	The *Input* is *set.*
UNSET	The *Input* is *unset.*
ISOLATED	The *Input* is *isolated.*

The second line of the submenu also indicates the function key to use for *setting* (0 = ❶) or *unsetting* (1 = ❷) depending on the *Setting* status and the keys to use for navigation between the submenus (↓ = ❶ and → = ➔).

Status information (second submenu)

The first line of this submenu shows the name of the *Zone* to which the *Input* belongs plus the *Input ID* (Number) of the *Input*.

The second line shows the *Input* type, *Input* status and the function keys to use for navigation between the submenus (↓ = ❶ and → = ➔).

The *Input* type may be one of the following:

INTRUSION (Intrusion)	TAMPER (Tamper)	HOLD-UP (Hold-up)	FIRE (Fire)
TECH. (Technical)	FAULT (Fault)	SABOTAGE (Sabotage)	SOFT SAB (Soft Sabotage)
DURESS (Duress)	CU STATUS (Action)	MAINS FLT (Mains Fault)	SYS. FLT (System Fault)

The actual *Input* types that can be shown for an *Input* depends on the *Input Type* selected during the programming of the ThorGuard Intrusion Alarm System

The *Input* status – also shown in the second line – may be one of the following:

PASSIVE	(Passive)	The *Input* is not activated.
ACTIVE	(Active)	The *Input* is activated.

4.3 Viewing logs and alarm counter

The Menus 25 and 26 give access to view the *Event Log* and *Alarm Log*, respectively. By means of Menu 29 you can view the total number of *Alarms* occurred since the system was put in operation.

☛ The logging of events depends on the filters applied during the programming of the ThorGuard Intrusion Alarm System.

4.3.1 Viewing event log (Menu 25)

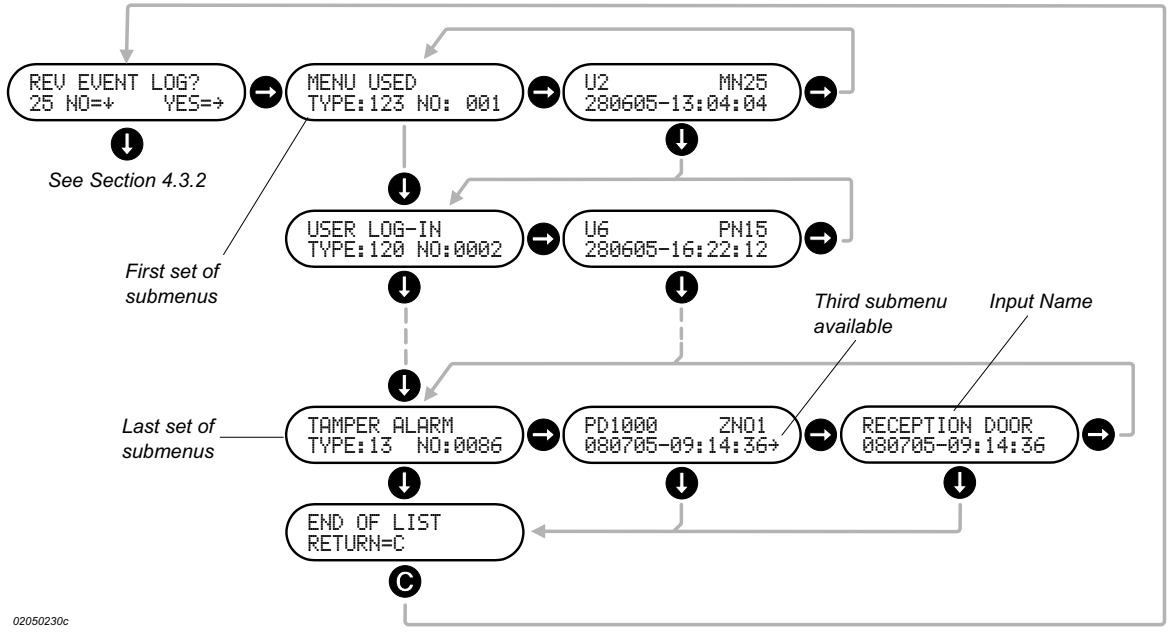
Introduction

The Rev Event Log Menu (25) allows you to view the events stored in the *Event Log* provided that it is allowed by the *User Profile* assigned to you. A description of the information available is described in detail on the following page 4-10.
The *Event Log* comprises all events – including *Alarms* – selected for logging during the programming of the ThorGuard Intrusion Alarm System.

Navigating between submenus

From the Rev Event Log Menu, you can access the first submenu by pressing the ➔-key. The first submenu actually comprises two or three submenus that you can switch between by pressing the ➔-key.
The first two submenus are always available while the third submenu is available only for certain events. The availability is indicated by a ~ in the second submenu.
The submenus – two or three – comprise all available information about a single record in the event log. See Fig. 4.8 and Fig. 4.9.

Fig. 4.8 *Example of the navigation between the submenus of the Rev Event Log Menu.*



From the first as well as the second (and third) of these submenus you can step through the remaining submenus by pressing the ➔-key the appropriate number of times. For each submenu, you can switch between the submenus by pressing the ➔-key.

When you reach the last submenu, the display will show END OF LIST. Pressing the C-key now – or at any time during your way through the submenus – will return you to the Event Log Menu.

When the first of the submenus are shown, you can jump directly to the display of information for another event by entering its 3-digit event number.

Event information (first submenu)

The first line of this submenu shows a text describing the type of event while the second line shows the event type number.

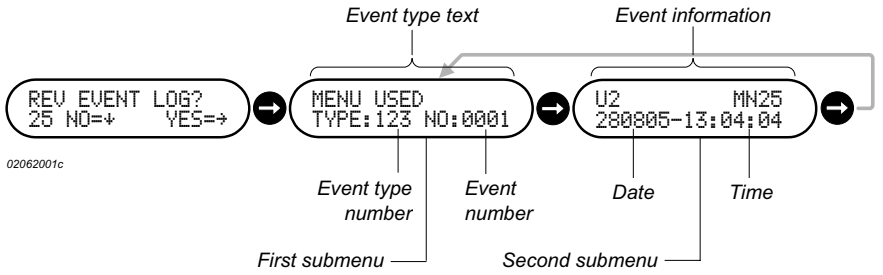
Event information (second submenu)

The first line of this submenu shows information about the actual event while the second line shows the date and time of occurrence.

Input information (third submenu)

Input Name information may be available in a third submenu as shown in Fig. 4.8 on the previous page.

Fig. 4.9 *Example of a single record in the submenus of the Rev Event Log Menu.*



Information about the individual types of events can be found in Section 4.5.

4.3.2 Viewing alarm log (Menu 26)

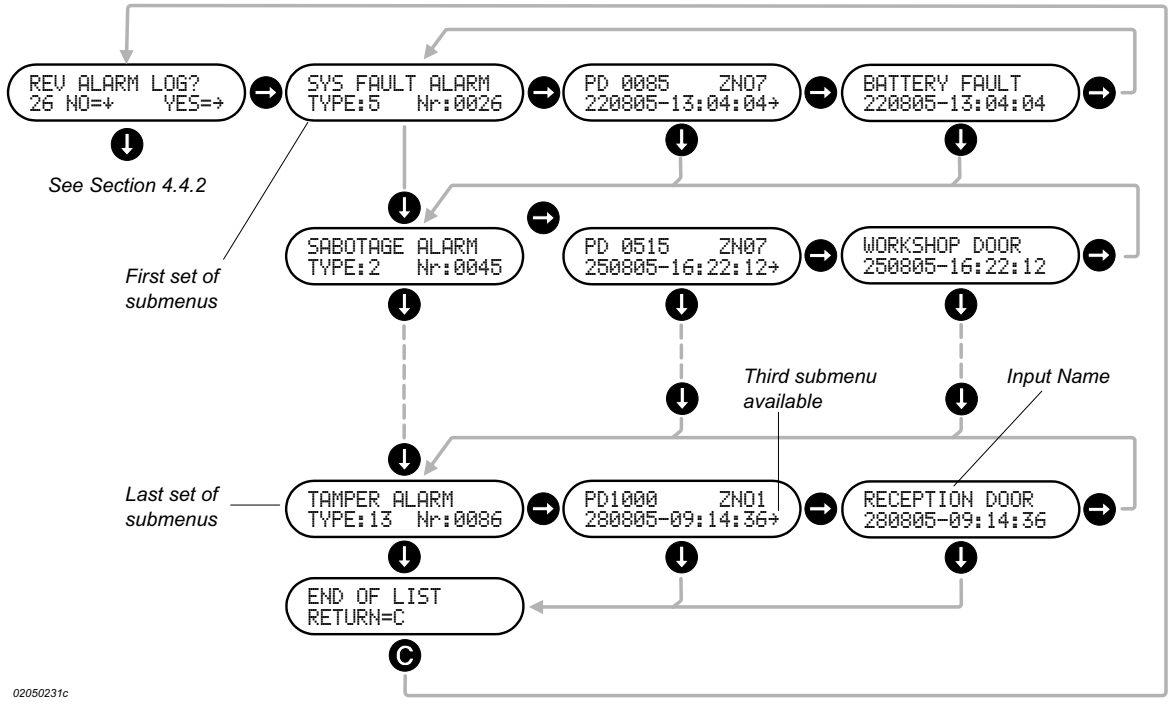
Introduction

The Rev Alarm Log Menu (25) allows you to view the *Alarms* stored in the *Alarm Log* provided that it is allowed by the *User Profile* assigned to you.
A description of the information available is described in detail on the following page 4-12.
The *Alarm Log* comprises all *Alarms* selected for logging during the programming of the ThorGuard Intrusion Alarm System. The logged *Alarms* are parts of the *Event Log* and can therefore also be viewed in the *Event Log*.

Navigating between submenus

From the Rev Alarm Log Menu, you can access the first submenu by pressing the ➔-key. The first submenu actually comprises two or three submenus that you can switch between by pressing the ➔-key.
The first two submenus are always available while the third submenu is available only for certain events. The availability is indicated by a + in the second submenu.
The submenus – two or three – comprise all available information about a single record in the event log. See Fig. 4.10 and Fig. 4.11.

Fig. 4.10 *Example of the navigation between the submenus of the Rev Alarm Log Menu.*



From the first as well as the second (and third) of these submenus you can step through the remaining submenus by pressing the ↓-key the appropriate number of times. For each submenu, you can switch between the submenus by pressing the ➔-key.

When you reach the last submenu, the display will show END OF LIST. Pressing the C-key now – or at any time during your way through the submenus – will return you to the Rev Alarm Log Menu.

When the first of the submenus are shown, you can jump directly to the display of information for another alarm by entering its 3-digit event number.

Alarm information (first submenu)

The first line of this submenu shows a text describing the type of *Alarm* while the second line shows the *Alarm* type number (Event type number).

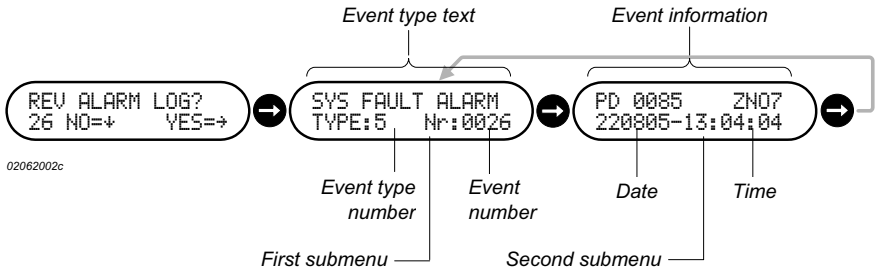
Alarm information (second submenu)

The first line of this submenu shows information about the actual *Alarm* (Event) while the second line shows the date and time of occurrence.

Input information (third submenu)

Input Name information may available in a third submenu as shown in Fig. 4.10 on the previous page.

Fig. 4.11 *Example of a single record in the submenus of the Rev Alarm Log Menu.*



Information about the individual types of *Alarms* can be found in Section 4.5.

4.3.3 Viewing alarm counter (Menu 29)

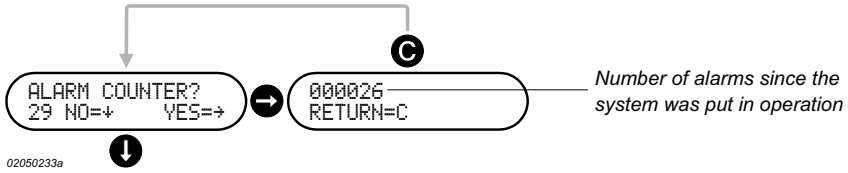
Introduction

The Alarm Counter Menu (29) allows you to view the total number of *Alarms* occurred since the system was put in operation.

Displaying alarm counter

From the Alarm Counter Menu, you can access the submenu by pressing the ➡-key. When in the submenu, pressing the C-key will return you to the Alarm Counter menu.

Fig. 4.12 *Example of the submenu of the Alarm Counter Menu.*



See Section 4.1

4.4 Viewing panel data and duress alarms

The Menu 24 gives access to view the data of the *Intrusion Terminal* (panel) that you are currently using. Menu 27 allows you to view the Duress state of the system and to reset this state.

4.4.1 Viewing panel data (Menu 24)

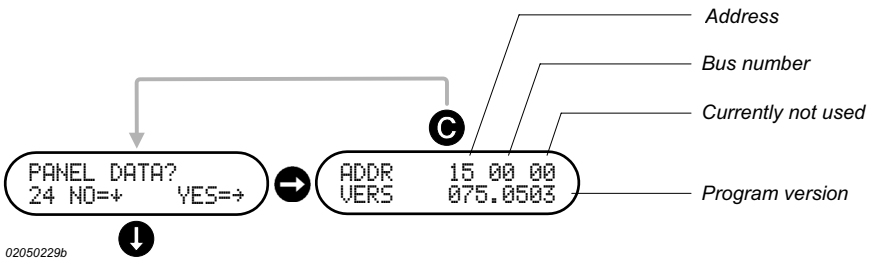
Introduction

The Panel Data Menu (24) allows you to view the address used by the Intrusion Terminal on the RS-485 bus, the number of this bus, and the version of the software installed in the *Intrusion Terminal*.

Displaying panel data

From the Panel Data Menu, you can access the submenu displaying the data by pressing the ➔-key. Pressing the Ⓒ-key when in the submenu will return you to the Panel Data Menu.

Fig. 4.13 *Example of the address of an Intrusion Terminal, the RS-485 bus that it is connected to, and its program version.*



See Section 4.3.1

4.4.2 Viewing and clearing hidden alarms (Menu 27)

Introduction

The Hidden Alarms Menu allows you to view and *clear Alarms* typically caused by the entry of a *Duress Code* and activation of inputs that generate *Hidden Alarms*.

Displaying number of alarms

From the Hidden Alarms Menu, you can press the ➔-key to display the *Alarms* status display.
The *Alarms* status display shows the number of *Duress Alarms* and other *Hidden Alarms*.
If no *Alarms* are present, the display shows NO ALARMS. You can then press the Ⓒ-key to return to the Hidden Alarms Menu
If *Alarms* are present, pressing the ➔-key once more brings you to the beginning of the list of *Duress Alarms* and other *Hidden Alarms*, displaying a submenu with the first *Hidden Alarm* in the list.

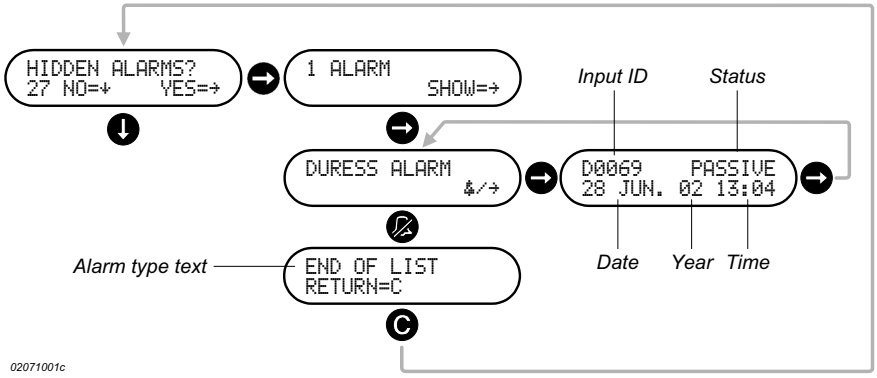
Displayind and clearing of individual alarms

This first submenu actually comprises two submenus that you can switch between by pressing the ➔-key. The first submenu shows the *Alarm* type, the second submenu shows the *Input ID* (Number) of the *Input* and the current status of the *Input* (*Active* or *passive*) plus the date and time of occurrence of the *Alarm*.

When displaying the *Alarm* data, you can press the ⓧ-key to *clear* the *Alarm*. After this, you can press the ↓-key to display the next *Alarm* in the list and repeat the procedure for displaying *Alarm* data and *clearing Alarms*.

When the last *Alarm* has been cleared, the display shows END OF LIST. You can now return to the Hidden Alarms Menu by pressing the C-key.

Fig. 4.14 *Example of display of the data of a single Alarm and the clearing of the Alarm.*



Clearing fails

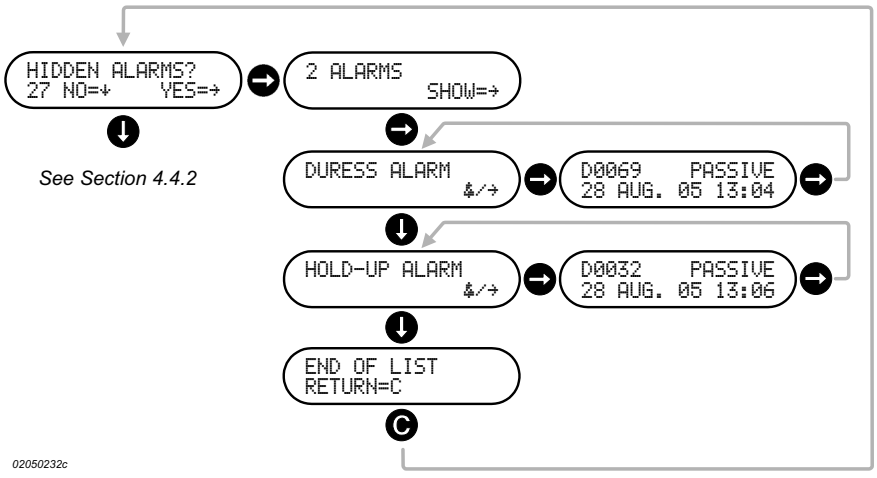
If it is not possible to *clear* an *Alarm*, an error message such as NOT ALLOWED is shown on the display. A failing *clearing* attempt may be caused by an *active Input*.

Going through alarm list

When the *Duress* status display is shown, you can press the →-key to go to the beginning of the *Alarm* list. Then you can press the ↓-key repeatedly to go through the complete list. For each *Alarm*, you can see the type of *Alarm*. *Alarms* will be displayed in order of occurrence.

When you reach the last submenu, the display will show END OF LIST. Pressing the C-key now will return you to the Duress Alarm Menu.

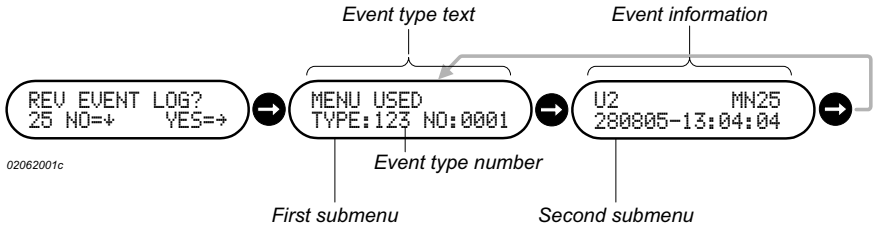
Fig. 4.15 *Example of the display of data for two Alarms.*



4.5 Event types and event descriptions

The tables of this section describe the events that can be shown in the display of the Intrusion Terminals. With reference to the example in the figure below, the columns of the tables contain the following information:

No.	Event type number from the lower line of the first submenu
Event type text	Event type text from the upper line of the first submenu
Event information	Short description of the actual event text from the upper line of the second submenu
Comments	If needed, an explanation is supplied in this column



Input name information (third submenu)

Input Name information may available in a third submenu for certain events as shown in Fig. 4.8 and Fig. 4.10. The availability of a third submenu is indicated by a → in the second submenu.

☛ Please note that the events that can be actually shown depend on the *Log Filter* applied.

4.5.1 Alarm events

This table describes the events generated when *Alarms* occur or are *cleared*. These types of events are always logged. They are available from the *Event Log* as well as the *Alarm Log*.

No.	*Event type text*	*Event information*	*Comments*
1	HOLD-UP ALARM	*Input ID* and *Zone No.*	A *Hold-up Alarm* has occurred.
2	SABOTAGE ALARM	*Input ID* and *Zone No.*	A *Sabotage Alarm* has occurred.
3	INTRUSION ALARM	*Input ID* and *Zone No.*	An *Intrusion Alarm* has occurred.
4	TECHNICAL ALARM	*Input ID* and *Zone No.*	A *Technical Alarm* has occurred.
5	SYS FAULT ALARM	*Input ID* and *Zone No.*	A *System Fault Alarm* has occurred.
6	FIRE ALARM	*Input ID* and *Zone No.*	A *Fire Alarm* has occurred.
7	DURESS ALARM	*Input ID* and *Zone No.*	A *Duress Alarm* has occurred.
8	SOFT SAB ALARM	*Input ID* and *Zone No.*	A *Soft sabotage Alarm* has occurred.
9	MAINS FLT ALARM	*Input ID* and *Zone No.*	A *Mains Fault Alarm* has occurred.
13	TAMPER ALARM	*Input ID* and *Zone No.*	A *Tamper Alarm* has occurred.

Continued …

No.	Event type text	Event information	Comments
14	MS CLEAR TAMPER	*Input ID* and *Zone No.*	A *Tamper Alarm* was *cleared* from the management system.
15	KEY CLEAR TAMPER	*ID* of *Input* that was *cleared* and *ID* of *Input* that performed the *clearing*	A *Tamper Alarm* was *cleared* from an *Action Input*.
16	RKP CLEAR TAMPER	*User ID* and *Input ID*	A *Tamper Alarm* was *cleared* from an *Intrusion Terminal*.
17	MS CLEAR ALARM	*Input ID* and *Zone No.*	An *Alarm* was *cleared* from the management system.
18	KEY CLEAR ALARM	*ID* of *Input* that was *cleared* and *ID* of *Input* that performed the *clearing*.	An *Alarm* was *cleared* from an *Action Input*.
19	RKP CLEAR ALARM	*User ID* and *Input ID*	An *Alarm* was *cleared* from an *Intrusion Terminal*.

4.5.2 Local alarm events

This table describes the events generated when local *Alarms* occur or are *cleared*. These events are only logged when selected for logging during the programming of the ThorGuard Central Unit. If logged, they are available from the *Event Log*.

No.	Event type text	Event information	Comments
20	LOCAL HOLD-UP	*Input ID* and *Zone No.*	A local *Hold-up Alarm* has caused a local alarm.
21	LOCAL SABOTAGE	*Input ID* and *Zone No.*	A local *Sabotage Alarm* has caused a local alarm.
22	LOCAL INTRUSION	*Input ID* and *Zone No.*	A local *Intrusion Alarm* has caused a local alarm.
23	LOCAL TECHNICAL	*Input ID* and *Zone No.*	A local *Technical Alarm* has caused a local alarm.
24	LOCAL SYS FAULT	*Input ID* and *Zone No.*	A local *System Fault Alarm* has caused a local alarm.
25	LOCAL FIRE	*Input ID* and *Zone No.*	A local *Fire Alarm* has caused a local alarm.
26	LOCAL DURESS	*Input ID* and *Zone No.*	A local *Duress Alarm* has caused a local alarm.
27	LOCAL SOFT SAB	*Input ID* and *Zone No.*	A local *Soft Sabotage Alarm* has caused a local alarm.
28	LOCAL MAINS FLT	*Input ID* and *Zone No.*	A local *Mains Fault Alarm* has caused a local alarm.
33	LOCAL TAMP	*Input ID* and *Zone No.*	A local *Tamper Alarm* has caused a local alarm.
34	MS ACCEPT TAMP	*Input ID* and *Zone No.*	*Alarm Signal* (Tamper) was *cleared* from the management system (See page 2-4).
35	KEY ACCEPT TAMP	*ID* of *Input* that was *cleared* and *ID* of *Input* that performed the *clearing*.	*Alarm Signal* (Tamper) was *cleared* from a key (See page 2-4).
36	RKP ACCEPT TAMP	*User ID* and *Input ID*	*Alarm Signal* (Tamper) was *cleared* from an Intrusion Terminal (See page 2-4).
37	MS ACCEPT ALARM	*Input ID* and *Zone No.*	*Alarm Signal* was *cleared* from the management system (See page 2-4).

Continued ...

No.	Event type text	Event information	Comments
38	KEY ACCEPT ALARM	*ID* of *Input* that was *cleared* and *ID* of *Input* that performed the *clearing*	*Alarm Signal* was *cleared* from an *Action Input* (See page 2-4).
39	RKP ACCEPT ALARM	*User ID* and *Input ID*	*Alarm Signal* was *cleared* from an an *Intrusion Terminal* (See page 2-4).

4.5.3 Miscellaneous alarm related events

This table describes various *Alarm* related events. These events are only logged when selected for logging during the programming of the ThorGuard Central Unit. If logged, they are available from the *Event Log.*

No.	Event type text	Event information	Comments
40	TECH PASSIVE	*Input ID* and *Zone No.*	The state of a *Technical Input* has changed to passive.
41	SYS FLT PASSIVE	*Input ID* and *Zone No.*	The state of a *System Fault Input* has changed to passive.
42	AUT ALM/TMP RES	*Input ID* and *Zone No.*	An *Input* was *cleared* by an *Auto Alarm Reset*.
43	MS/K CLR FAILED	*Input ID* and *Zone No.*	*Clearing* of a *Fault* (input still active) from management system failed.
44	MAINS FLT PAS	*Input ID* and *Zone No.*	The state of a *Mains Fault Input* has changed to passive.
47	MS CLEAR FAILED	*Input ID* and *Zone No.*	*Clearing* of an *Alarm* from the management system failed. The *Input* was still active.

4.5.4 System set or unset events

This table describes the events generated when *setting* and *unsetting* the complete system. These events are only logged when selected for logging during the programming of the ThorGuard Central Unit. If logged, they are available from the *Event Log.*

No.	Event type text	Event information	Comments
50	RKP SET SYSTEM	*User ID* and *Intrusion Terminal* address.	The system was *set* by a *User* from an *Intrusion Terminal*.
51	MS SET SYSTEM	No information shown.	The system was *set* remotely.
52	AUTOSET SYSTEM	No information shown.	The system was *set* by an *Autoset Week Program*.
53	KEY SET SYSTEM	*Input ID*	The system was *set* by *Input*.
54	SYSTEM SET	No information shown.	The system became fully *set*

4.5.5 Area set or unset events

This table describes the events generated when *setting* and *unsetting Areas*. These events are only logged when selected for logging during the programming of the ThorGuard Central Unit. If logged, they are available from the *Event Log*.

No.	Event type text	Event information	Comments
60	AUTOSET FAULT	*Input ID* and *Area No.*	A *Set At Start If Passive* function was executed by an *Autoset Week Program*. However, the *Area* was not passive and *setting* was cancelled.
61	RKP SET AREA	*User ID* and *Area No.*	An *Area* was *set* by a *User* from an *Intrusion Terminal*.
62	RKP UNSET AREA	*User ID* and *Area No.*	An *Area* was *unset* by a *User* from an *Intrusion Terminal*.
63	MS SET AREA	*Area No.*	An *Area* was *set* remotely.
64	MS UNSET AREA	*Area No.*	An *Area* was *unset* remotely.
65	AUTOSET AREA	*Area No.*	An *Area* was *set* from an *Autoset Week Program*.
66	AUTOUNSET AREA	*Area No.*	An *Area* was *unset* from an *Autoset Week Program*.
67	KEY SET AREA	*Input ID* and *Area No.*	An *Area* was *set* by an *Action Input*.
68	KEY UNSET AREA	*Input ID* and *Area No.*	An *Area* was *unset* by an *Action Input*.
70	OVRRL UNSET AREA	*User ID* and *Area No.*	An *Area* was *unset* outside the programmed *unset* period.
71	CHECK=AREA UNSET	*Area No.*	A function check for *Area set* was performed while the *Area* was in the *unset* state.
72	AUTOSET DELAYED	*User ID* and *Area No.*	An *Autosetting Time* was delayed.
73	MS AUTOSET DELAY	*Area No.*	An *Autosetting Time* was delayed from the management system.
74	TL SET AREA	*Area No.*	An *Area* was set by a *Time Lock*

4.5.6 Zone set or unset events

This table describes the events generated when *setting* and *unsetting Zones*. These events are only logged when selected for logging during the programming of the ThorGuard Central Unit. If logged, they are available from the *Event Log*.

No.	Event type text	Event information	Comments
80	RKP SET ZONE	*User ID* and *Zone No.*	A *Zone* was *set* by a *User* from an *Intrusion Terminal*.
81	RKP UNSET ZONE	*User ID* and *Zone No.*	A *Zone* was *unset* by a *User* from an *Intrusion Terminal*.
82	MS SET ZONE	*Zone No.*	A *Zone* was *set* remotely.
83	MS UNSET ZONE	*Zone No.*	A *Zone* was *unset* remotely.

4.5.7 Input set or unset events

This table describes the events generated when *setting* and *unsetting Inputs*. These events are only logged when selected for logging during the programming of the ThorGuard Central Unit. If logged, they are available from the *Event Log*.

No.	*Event type text*	*Event information*	*Comments*
90	RKP SET INPUT	*User ID* and *Input ID*	An *Input* was *set* by a *User* from an *Intrusion Terminal*.
91	RKP UNSET INPUT	*User ID* and *Input ID*	An *Input* was *unset* by a *User* from an *Intrusion Terminal*.
92	MS SET INPUT	*Input ID*	An *Input* was *set* remotely.
93	MS UNSET INPUT	*Input ID*	An *Input* was *unset* remotely.

4.5.8 Isolation events

This table describes the events generated when *isolating Inputs*. These events are only logged when selected for logging during the programming of the ThorGuard Central Unit. If logged, they are available from the *Event Log*.

No.	*Event type text*	*Event information*	*Comments*
100	RKP ISOL INPUT	*User ID* and *Input ID*	An *Input* was *isolated* by a *User* during *setting* from an *Intrusion Terminal*.
101	AUTOISOL INPUT	*Input ID*	An *Input* was *isolated* during *setting* by an *Autoset Week Program*
102	KEY ISOL INPUT	*ID* of *Input* that was *isolated* and *ID* of *Input* that caused the *isolation*.	An *Input* was *isolated* during *setting* by an *Action Input*.
103	MS ISOL INPUT	*Input ID* and *Zone No*.	An *Input* was *isolated* remotely.

4.5.9 Input enable or disable events

This table describes the events generated when *enabling* and disabling *Inputs*. These events are only logged when selected for logging during the programming of the ThorGuard Central Unit. If logged, they are available from the *Event Log*.

No.	*Event type text*	*Event information*	*Comments*
110	INPUT ENABLED	*User ID* and *Input ID*	An *Input* was *enabled* by a *User* from an *Intrusion Terminal*.
111	INPUT INHIBITED	*User ID* and *Input ID*	An *Input* was *disabled* by a *User* from an *Intrusion Terminal*.
112	SET INPUT INHIB	*User ID* and *Input ID*	An *Input* was *disabled* while *set* by a *User* from an *Intrusion Terminal*.

4.5.10 User interface events

This table describes the events generated when a *User* operates an *Intrusion Terminal*. These events are only logged when selected for logging during the programming of the ThorGuard Central Unit. If logged, they are available from the *Event Log*.

No.	*Event type text*	*Event information*	*Comments*
120	USER LOG-IN	*User ID* and *Intrusion Terminal* address.	A *User* logged in on an *Intrusion Terminal*.
121	USER LOG-OUT	*User ID* and *Intrusion Terminal* address.	A *User* logged out on an *Intrusion Terminal*.
122	RKP BLOCKED	*User ID* and *Intrusion Terminal* address.	An *Intrusion Terminal* was blocked because the number of allowed wrong *PIN-code* entries was exceeded.
123	MENU USED	*User ID* and *Menu No.*	A *User* has performed a menu operation from an *Intrusion Terminal*.
125	VIDEO TRIGGER	*Input ID* and *Zone No.*	An *Input* that triggers a video camera has changed to active.

4.5.11 Duress events

This table describes the events generated during use of *Duress Code* and reset of *Duress* state. These events are only logged when selected for logging during the programming of the ThorGuard Central Unit. If logged, they are available from the *Event Log*.

No.	*Event type text*	*Event information*	*Comments*
130	DURESS LOG-IN	*User ID* and *Intrusion Terminal* address.	A *User* has entered a *Duress Code* on an *Intrusion Terminal*.
131	RKP CLEAR DURESS	*User ID*	A *User* has *reset* the *Duress* state of the ThorGuard Central Unit.
132	MS CLEAR DURESS	No information shown.	The management system has *reset* the *Duress* state of the ThorGuard Central Unit.

4.5.12 Anti-assault events

This table describes events generated when starting and ending *Anti-assault Tours*. These events are only logged when selected for logging during the programming of the ThorGuard Central Unit. If logged, they are available from the *Event Log*.

No.	*Event type text*	*Event information*	*Comments*
135	UNSET TOUR BEGIN	*User ID* and *Area No.*	A *User* has started an *Anti-assault Unset Tour.*
136	UNSET TOUR END	*User ID* and *Area No.*	A *User* has ended an *Anti-assault Unset Tour.*
137	GUARD TOUR BEGIN	*User ID* and *Area No.*	A *User* has started a *Guard Anti-assault Tour.*
138	GUARD TOUR END	*User ID* and *Area No.*	A *User* has ended a *Guard Anti-assault Tour.*

4.5.13 Date and time events

This table describes events generated when changing date and time of the system. These events are only logged when selected for logging during the programming of the ThorGuard Central Unit. If logged, they are available from the *Event Log*.

No.	*Event type text*	*Event information*	*Comments*
140	RKP SET THE TIME	*User ID* and new time	A *User* has changed the date and time from an *Intrusion Terminal*.
141	MS SET THE TIME	*User ID* and new time	Date and time was changed remotely.

4.5.14 Test related events

This table describes events generated when performing the various tests that can be carried out. These events are only logged when selected for logging during the programming of the ThorGuard Central Unit. If logged, they are available from the *Event Log*.

No.	*Event type text*	*Event information*	*Comments*
150	BRANCH TEST BEG	*User ID* and *Intrusion Terminal* address.	A *User* has started a *Branch Test* from an *Intrusion Terminal*.
151	BRANCH TEST OK	*User ID and Intrusion Terminal address.*	A *Branch Test* was successfully completed.
152	BR TEST IN FAULT	*Input ID* and *Zone No.*	An *Input* has failed during a *Branch Test*.
153	BR TEST OUT FLT	*Output ID* and *Zone No.*	An *Output* has failed during a *Branch Test*.
154	BR TEST ABORTED	*User ID* and *Intrusion Terminal* address.	A *Branch Test* was aborted.
155	BR TEST TIME-OUT	No information shown.	A *Branch Test* exceeded the programmed time and was automatically stopped.
160	AUTOTEST-AT OK	No information shown.	An *Autotest At Time* was completed successfully.
161	AUTOTEST-AT FLT	*Input ID* and *Zone No.*	An *Input* has failed during an *Autotest At Time*.
162	AUTOTEST-AT OK	No information shown.	An *Autotest At Time* was started by management system and completed successfully.
163	AUTOTEST-AT FLT	*Input ID* and *Zone No.*	An *Input* has failed during an *Autotest At Time* started by management system.
164	AUTOTEST-AT OK	No information shown.	An *Autotest At Time* started by an *Input* was completed successfully.
165	AUTOTEST-AT FLT	*Input ID* and *Zone No.*	An *Input* has failed during an *Autotest At Time* started by an *Input*.
166	AUTOTEST-AT FLT	No information shown.	One or more *Inputs* have failed during an *Autotest At Time* started by an *Input*.
170	WALK TEST BEGIN	*User ID.*	A *Walk Test* was started by a *User* from an *Intrusion Terminal*.
171	WALK TEST END	*User ID.*	A *Walk Test* was stopped by a *User* from an *Intrusion Terminal*.

Continued ...

No.	Event type text	Event information	Comments
180	HU TEST BEGIN	*User ID* and *Intrusion Terminal* address.	A *Hold-up Test* was started by a *User* from an *Intrusion Terminal*.
181	HU TEST END OK	*User ID* and *Intrusion Terminal* address.	A *Hold-up Test* was successfully completed.
182	HU TEST FAULT	*Input ID* and *Zone No.*	An *Input* has failed during a *Hold-up Test*.
183	HU TEST ABORT	*User ID* and *Intrusion Terminal* address.	A *Hold-up Test* was aborted.
184	HU TEST TIME-OUT	No information shown.	A *Hold-up Test* exceeded the programmed time and was automatically stopped.
190	INPUT TEST BEGIN	*User ID* and *Input ID*	An *Input Test* was started by a *User* from an *Intrusion Terminal.*
191	INPUT TEST END	*User ID* and *Input ID*	An *Input Test* was stopped by a *User* from an *Intrusion Terminal*.
192	INPUT TEST ACT	*Input ID* and *Zone No.*	An *Input* went active during an *Input Test*.
193	IP TEST PASSIVE	*Input ID* and *Zone No.*	An *Input* went passive during an *Input Test*.
200	OP TEST START	*User ID* and *Output ID*	An *Output Test* was started by a *User* from an *Intrusion Terminal.*
201	OP TEST STOP	*User ID* and *Output ID*	An *Output Test* was stopped by a *User* from an *Intrusion Terminal.*
210	SOAK TEST BEGIN	*User ID* and *Input ID*	A *Soak Test* was started by a *User* from an *Intrusion Terminal*.
211	SOAK TEST END	*User ID* and *Input ID*	A *Soak Test* was stopped by a *User* from an *Intrusion Terminal.*
212	SOAK TEST IN ACT	*Input ID* and *Zone No.*	An *Input* went active during a Soak *Test*.
213	SOAK TEST IN PAS	*Input ID* and *Zone No.*	An *Input* went passive during a *Soak Test*.
214	SOAK TEST TA ACT	*Input ID* and *Zone No.*	A *Tamper Input* went active during a *Soak Test*.
215	SOAK TEST TA PAS	*Input ID* and *Zone No.*	A *Tamper Input* went passive during a *Soak Test*.
220	ZONE TEST BEGIN	*User ID* and *Zone No.*	A *Zone Test* was started by a *User* from an *Intrusion Terminal*.
221	ZONE TEST ACTIVE	*Input ID* and *Zone No.*	An *Input* was found active during a *Zone Test*.
222	ZONE TEST END	*User ID* and *Zone No.*	A *Zone Test* was stopped by a *User* from an *Intrusion Terminal*.
230	LOGIC TEST FAULT	*Input ID* and *Zone No.*	An *Input* has failed during an *Logical Test After Unset*
234	AUT BAT TEST OK	*Internal or external battery*	An Automatic *Battery Test* was successfully completed.
235	AUT BAT TEST FLT	*Internal or external battery*	An Automatic *Battery Test* has failed.
236	RKP BAT TEST OK	*User ID, internal or external battery*	A *Battery Test* started from an *Intrusion Terminal* was successfully completed.
237	RKP BAT TEST FLT	*User ID, Internal or external battery*	A *Battery Test* started from *Intrusion Terminal* has failed.
238	MS BAT TEST OK	*User ID, Internal or external battery*	A *Battery Test* started from management system was successfully completed.

Continued …

No.	Event type text	Event information	Comments
239	MS BAT TEST FLT	*Internal or external battery*	A *Battery Test* started from the management system has failed.
240	PRIM CONN FLT	No information shown.	An automatic *Host Interface Test* of the primary transmission channel has failed.
241	BACKUP CONN FLT	No information shown.	A *Host Interface Test* of the backup transmission channel has failed.
245	AUTOTEST-AU FLT	*Input ID*	An *Input* has failed during an *Autotest After Unset*.
246	AUTOTEST-AU OK	*Input ID*	An *Autotest After Unset* of an *Input* was successfully completed.

4.5.15 User database events

This table describes events generated when adding and deleting *Users* from the database and when changing the *PIN-code*. These events are only logged when selected for logging during the programming of the ThorGuard Central Unit. If logged, they are available from the *Event Log*.

No.	Event type text	Event information	Comments
250	USER CREATED	*User ID* of *User* that logged in and added *User ID*.	A *User* has been added to the user database.
251	USER DELETED	*User ID* of *User* that logged in and deleted *User ID*.	A *User* has been deleted from the user database.
252	PIN-CODE CHANGED	*User ID*	A *User* has changed his *PIN-code*.

4.5.16 Configuration events

This table describes events generated during transfer of programming data and programs to and from the ThorGuard Central Unit. These events are only logged when selected for logging during the programming of the ThorGuard Central Unit. If logged, they are available from the *Event Log*.

No.	Event type text	Event information	Comments
260	CONFIG CHANGED	*Class ID* and *Instance ID*	*Set Configuration* mail processed.
261	CONFIG READ	*Class ID* and *Instance ID*	*Get Configuration* mail processed.
262	FW INCOMPATIBLE	*Class ID*	*Power-on validation* of the transferred SW showed that previous SW was incompatible with current SW. One event generated for each incompatible *Class*.

4.5.17 Time lock events

This table describes events generated when operating *Time Locks*. These events are only logged when selected for logging during the programming of the ThorGuard Central Unit. If logged, they are available from the *Event Log*.

No.	*Event type text*	*Event information*	*Comments*
265	TL PROCEDURE BEG	*User ID* and *Time Lock ID.*	A *User* has started the *Release* of a *Time Lock*.
266	TL PROCEDURE END	*User ID* and *Time Lock ID.*	A *User* has stopped the *Release* of a *Time Lock*.
267	RKP BLOCKED TL	*User ID*	A *Time Lock* was *blocked* by a *User* from an *Intrusion Terminal*.
268	RKP UNBLOCKED TL	*User ID*	A *Time Lock* has been *unblocked* by a *User* from an *Intrusion Terminal*.
269	MS BLOCKED TL	No information shown.	A *Time Lock* was *blocked* from the management system.
270	MS UNBLOCKED TL	No information shown.	A *Time Lock* was *unblocked* from the management system.
271	UNLOCKED TL	*Input ID* and *Time Lock ID.*	A *Time Lock* was *unlocked* while *released*
272	TIME LOCK LOCKED	*Input ID* and *Time Lock ID.*	A *Time Lock* was *locked*.
273	TL TIME-OUT	*Input ID* and *Time Lock ID.*	The *unlocked* period expired and the *Time Lock* was not locked during warning period).
274	FORCED TL	*Input ID* and *Time Lock ID.*	A forced *unlocking* or *release* of a Ti*me Lock* was performed
275	TL RELEASE FAULT	*Input ID* and *Time Lock ID.*	The *release* of a *Time Lock* failed.
276	TL SECURE FAULT	*Input ID* and *Time Lock ID.*	The *securing* of a *Time Lock* failed.
277	TL UNEXP SECURE	*Input ID* and *Time Lock ID.*	A *Time Lock* was unexpectedly *secured*.
278	TL ABORT BY I-L	*Input ID* and *Zone No.*	The *Release* of a *Time Lock* has been aborted due to *interlock.*
279	TL SHORT PR BEG	*User ID* and *Time Lock ID.I*	Bypass of the *Waiting Time* as well as *Hold-up Waiting Time* has started.

4.5.18 Log events

This table describes events generated when events of the *Event Log* and the *Alarm Log* are overwritten by new events. These events are only logged when selected for logging during the programming of the ThorGuard Central Unit. If logged, they are available from the *Event Log*.

No.	*Event type text*	*Event information*	*Comments*
280	E-LOG OVERWR 1ST	Event type No. and time stamp of overwritten event	Starting to overwrite events in the *Event Log*
281	E-LOG OVERWR END	Event type No. and time stamp of overwritten event	Last overwritten event in the *Event Log*
282	A-LOG OVERWR 1ST	Event type No. and time stamp of overwritten event	Starting to overwrite events in *Alarm Log*.
283	A-LOG OVERWR END	Event type No. and time	Last overwritten event in *Alarm Log*.

No.	Event type text	Event information	Comments
		stamp of overwritten event	

4.5.19 System events

This table describes events generated when the ThorGuard Central Unit is restarted. These events are only logged when selected for logging during the programming of the ThorGuard Central Unit. If logged, they are available from the *Event Log*.

No.	Event type text	Event information	Comments
290	SYSTEM RESTARTED	SW version	System restarted.
291	OBJECT CORRUPT	*Class ID* and *Instance ID*	*Power-on validation* of object failed. Object configured to default value.
292	>20 CORRUPT OBJS	No information shown.	More that twenty objects have failed power-on validation. No more `OBJECT CORRUPT` events will be generated.
293	FW UPDATED	FW type (1, 2, or 3) and event (0, 1 or 2).	The firmware of the ThorGuard Central Unit has been updated. FW type: 1 = Main FW. 2 = GPI FW. 3 = S-ART FW. Event: 0 = Transfer initiated. 1 = Transfer aborted. 2 = Transfer completed.
294	GPI RESTARTED	SW version	The GPI of the ThorGuard Central Unit has been restarted.
398	ENGINEERING		Unexpected situation. Report to HI SEC
399	ENGINEERING		Unexpected situation. Report to HI SEC

This page is intentionally left blank.

5

System test menus

Introduction

This chapter describes the various tests that can be performed on the system itself, on parts of the system, and on the various components of the system.

During the tests a number of events are logged. Information about the logged events can be found in Sections 4.5.10 and 4.5.14.

☛ Please note that the access to the System Test menus is controlled by the *User Profile* assigned to you.

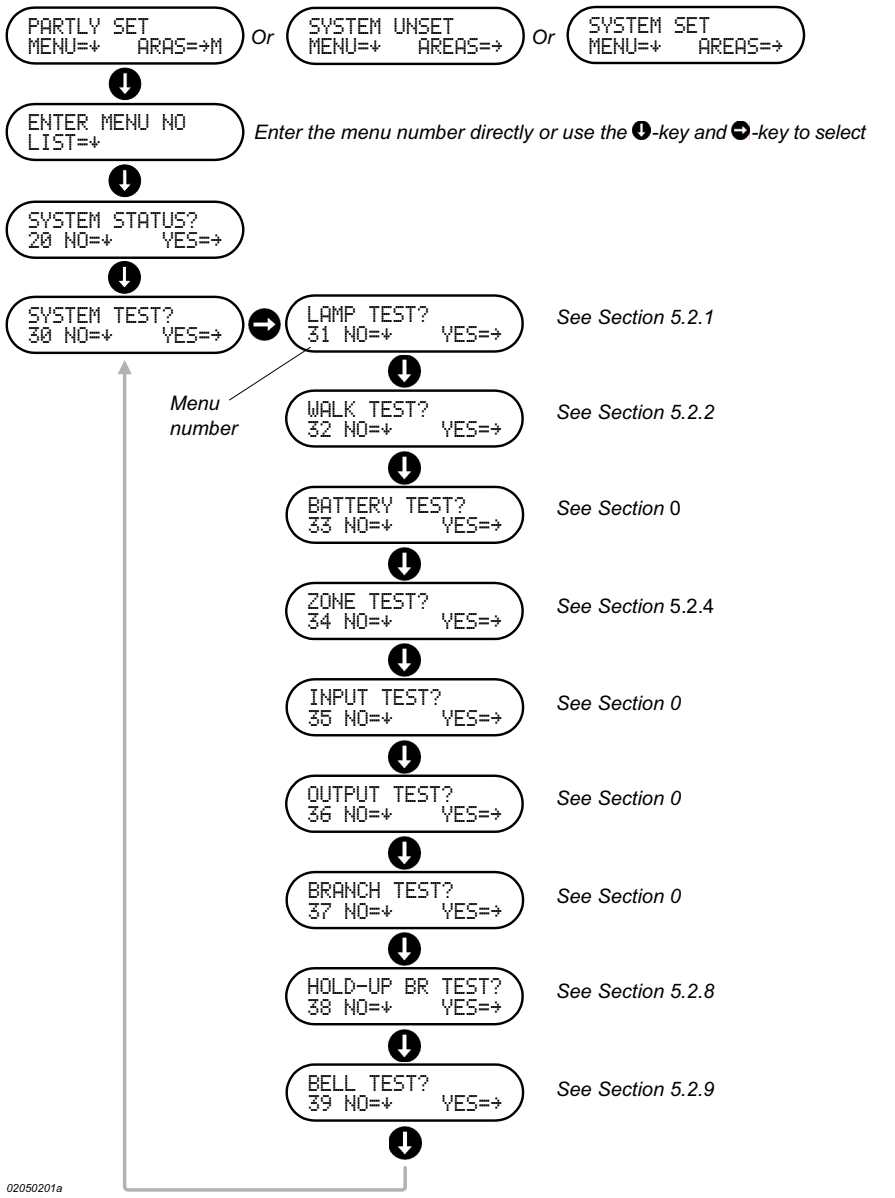
This chapter

The chapter contains the following sections:

5.1 Overview

The System Test menus comprise the menus shown in Fig. 5.1 below. To access these menus, you must log-in using the procedure of Section 3.2.1. This displays one of the three menus shown in the top of Fig. 5.1, provided that no *Alarms*, *Faults*, *Isolations* or *Disabled Inputs* are present (Section 3.5 and 3.6). Press the ⬇-key to display a menu in which you can select the menu you want by entering its number (Menu 30, 31, 32, 33, 34, 35, 36, 37, 38 or 39) or you can press the ⬇-key repeatedly until the main *System Test menu* (Menu 30) is displayed. From this, you can press the ➡-key to display the first of the *System Test menus* (Menu 31). The rest of the menus can be displayed one at a time by pressing the ⬇-key repeatedly as shown in Fig. 5.1.

Fig. 5.1 *Example of the menus available from the system test menu (30). The example assumes that no alarms, faults, isolations or disabled inputs are present.*



5.2 Performing the tests

Introduction

The following sections 5.2.1 to 5.2.9 describe the various tests that can be carried out from an *Intrusion* T*erminal*.
The access to perform the tests is determined by the *User Profile* assigned to you.

A number of these tests will be automatically terminated either after a period determined by the test itself or after a testing period common to more tests.
The common period (*Maximum Manual Test Time*) is set during the programming of the ThorGuard Intrusion Alarm System. The time can be set in the range from 1 to 120 minutes.

5.2.1 Lamp test (Menu 31)

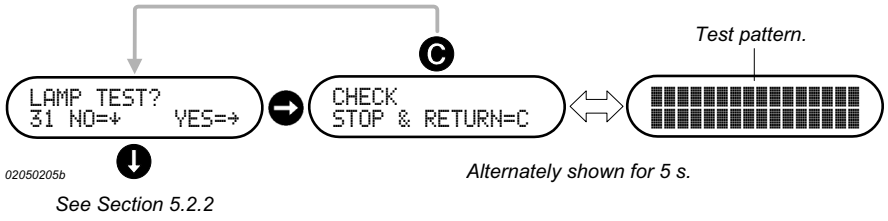
Introduction

The Lamp Test Menu (31) allows you to test the signal LEDs and the display of the *Intrusion Terminal*.

Starting the test

From the Lamp Test Menu, you can start the test by pressing the ➔-key. This will alternately show the submenu and the test pattern in the display. During this, the four signal LEDs of the *Intrusion Terminal* will flash.

Fig. 5.2 *Example of the menus shown during the test of the LEDs and the display of an Intrusion Terminal.*



Ending the test

Pressing the Ⓒ-key will end the test and return you to the Lamp Test Menu.

5.2.2 Walk test (Menu 32)

Introduction

The Walk Test menu allows you to test the passive infrared detectors (PIR) of the *Areas* assigned to the *Intrusion Terminal* by the *Terminal Area Mask*.
The *Areas* in which you want to perform the test should preferably be *unset* prior to the test otherwise *Alarms* will be generated during the test.

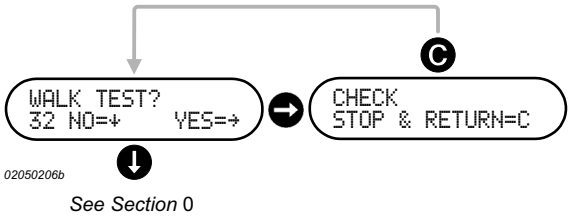
The *Walk Test* is a manual test of the PIR detectors where the built-in signal LEDs of the detectors is enabled when you start the test.
By walking in the area covered by a detector, its signal LED will become lit so that you can check that the detector operates correctly and that it covers the required area.

☛ Please note that only PIR detectors with a signal LED that can be remotely enabled can be tested by means of the *Walk Test*.

Starting the test

The test is started from the Walk Test Menu by pressing the ➔-key. After this, you can start your tour to check the detectors.

Fig. 5.3 *Example of the menu shown during the Walk Test.*



Ending the test

The test period is automatically terminated when *Maximum Manual Test Time* expires or when you press the Ⓒ-key. This will return you to the Walk Test Menu.

Error messages

If you attempt to carry out this test while another test is running, a message about conflicting tests will be shown on the display, for example: `CONFL. BRANCH TEST`.

5.2.3 Battery test (Menu 33)

Introduction

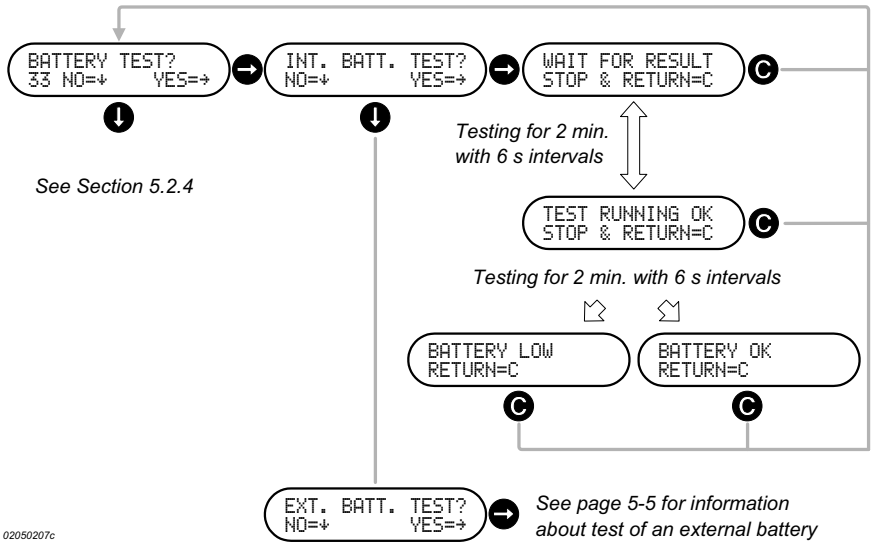
The Battery Test menu allows you to test the charging condition of the internal backup battery as well as an external backup battery (if mounted) of the ThorGuard Intrusion Alarm System. The battery is tested using a test load and with the battery charging circuit disconnected.

Starting the test

The test is started from the Battery Test Menu by pressing the ➔-key. Then you must press the ➔-key to start the test of the internal battery or the ↓-key to proceed to the menu for starting the test of an external battery. See Fig. 5.4 for more information.

Test of internal battery

Fig. 5.4 *Example of the menus shown during the test of the battery. If the battery condition is satisfactorily, the menu displays* `BATTERY OK` *after two minutes of testing, if not,* `BATTERY LOW` *is shown.*

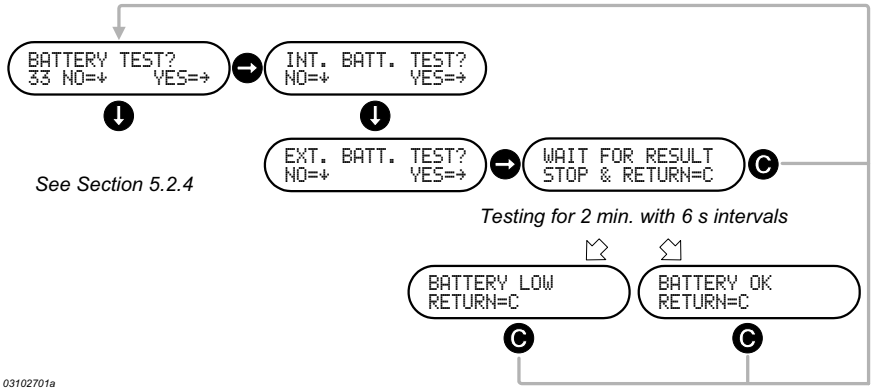


Ending the test

The testing is repeated every 6 s until it is automatically terminated two minutes after the start of the test. You may also terminate the test by pressing the C-key. This will return you to the Battery Test Menu.

Test of external battery

Fig. 5.5 *Example of the menus shown during the test of an external battery. If the battery condition is satisfactorily, the menu displays* BATTERY OK *after two minutes of testing, if not,* BATTERY LOW *is shown.*



Ending the test

The testing is repeated every 6 s until it is automatically terminated two minutes after the start of the test. You may also terminate the test by pressing the C-key. This will return you to the Battery Test Menu.

Error message

If no charger has bee configured during the set up of the system, the message NO CHARGER will be shown in the display.

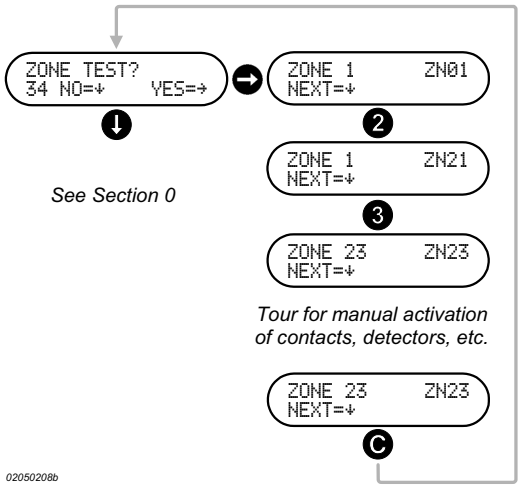
5.2.4 Zone test (Menu 34)

Introduction

The Zone Test menu allows you locate faulty detectors and contacts and to check – for the individual *Zones* – the operation of detectors, door contacts, window contacts, etc. by manually opening doors and windows, activating PIR detectors when passing these, etc.
The *Zones* that can be tested are determined by your *User Profile* and the *Terminal Area Mask*. During the *Zone Test*, the *Zone* must be *unset* or *partially set*. If *set* from for example an *Autoset Week Program* while being tested, the *Zone Test* will automatically be terminated.

☛ Detectors, contacts, etc. connected to *Hold-up*, *Duress*, *Tamper* and *Fire Inputs* cannot be tested using the *Zone Test*. To test these types of *Inputs*, you must use the *Input Test* described in the following Section 0.

Fig. 5.6 *Example of starting and ending a test of Zone 23.*



Starting the test

From the Zone Test Menu, you can start the test by pressing the ➔-key. This will start the test period for the first *Zone* allowed by the *Terminal Area Mask* and your *User Profile* by displaying a submenu with the *Zone* name and *Zone* number. If this is not the *Zone* you want to test, you can press the ↓-key the required number of times until you reach the *Zone* you want to test or you can simply enter the number of the *Zone* by means of the numeric keys of the *Intrusion Terminal* as shown in the example below.
Each time you enter or select a new *Zone* number, a test of this *Zone* is started.

During the test

You can now start your tour in the *Zone*. Each time you activate a contact, detector, etc. of the *Zone*, the buzzer of the *Intrusion Terminal* will sound for 3 s. Each activation of a contact or a detector will be logged in the *Event Log* (*Event* type 221) where the result of the *Zone Test* can be checked. See Section 4.5.14.

Ending the test

The test period will automatically be terminated when the *Maximum Manual Test Time* expires or when you press the C-key. This will return you to the Zone Test Menu.

Error messages

If you attempt to carry out this test while another test is running, a message about conflicting tests will be shown on the display, for example: `CONFL. BRANCH TEST`.

If you enter a *Zone* number that does not exist, the message `ZONE NOT AVAILB` will be shown in the display.

5.2.5 Input test (Menu 35)

Introduction

The Input Test Menu allows you to check any type of *Input* of the system including *Hold-up*, *Duress*, *Tamper* and *Fire Inputs*.
The *Input Test* is used for checking *Inputs* that cannot be checked by means of the *Zone Test* and to perform a more thorough investigation of faulty *Inputs* found during a *Zone Test*.

You can check one *Input* at a time regardless of whether the *Input* is *set* or *unset* because the normal function of the *Input* is suspended during the test. The *Inputs* that can be tested are not limited by a *User Profile or* the *Terminal Area Mask*.

☛ The test can only be performed from a single *Intrusion Terminal* at a time and it requires that the system has been put in *Service Mode* as described in Chapter 7.

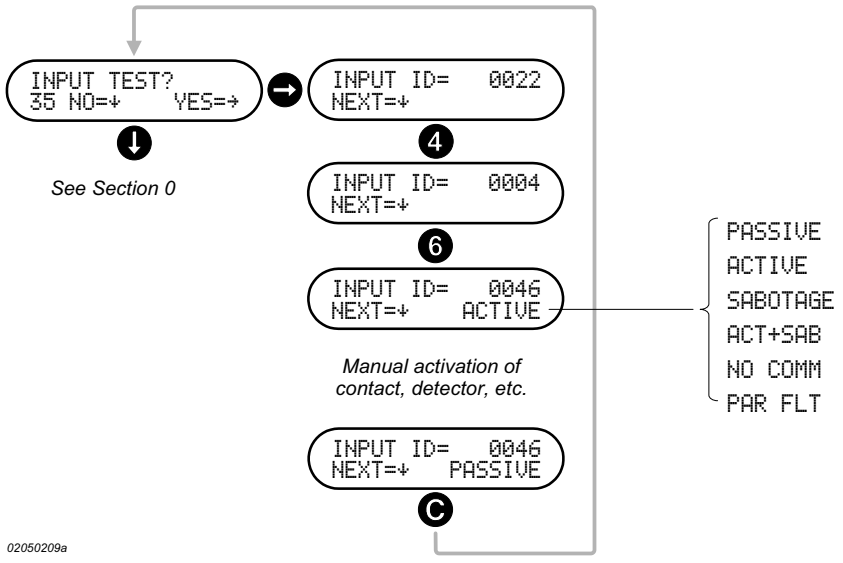
Starting the test

After the system has been put in *Service Mode*, you must locate the Input Test Menu as shown in Fig. 5.1. Then you must press the ➔-key to display the submenu for entry of the 4-digit *Input ID* of the *Input* you want to test.

The *Input ID* shown in the display is the lowest *ID* programmed in the system. If this is not the *Input* you want to test, you can press the ↓-key the required number of times until you reach the *Input* you want to test or you can simply enter the
4-digit *Input* ID by means of the numeric keys of the *Intrusion Terminal* as shown in the example below.

Each time you enter or select a new *Input ID*, a test of this *Input* is started. Shortly after, the status of the *Input* will be shown on the display of the *Intrusion Terminal*. The status that can be shown depends on the type of *Input* being tested.
A table with an explanation of status messages is provided on the following page.

Fig. 5.7 *Example of starting and ending a test of the Input with the Input ID 0046.*



During the test

You can now start to manipulate the contact, detector, etc., to change the state of its *Input*. Each time the state changes, the buzzer of the *Intrusion Terminal* will sound for 1 s and the display will indicate the current status.

Each change from *Passive* to *Active* and vice versa will be logged in the *Event Log* (*Event* types 192 and 193, respectively) where the change can be found. See Section 4.5.14 for more information

☛ Please note that only the transition from *Passive* to *Active* and vice versa is logged. The actual result of the transition (Status) - as displayed on the *Intrusion Terminal* - cannot be found in the *Event Log*.

Status

Status	***Description***
PASSIVE	The *Alarm Input* is passive.
ACTIVE	The *Alarm Input* is active (Alarm).
SABOTAGE	*Tamper Input* is active.
ACT+SAB	*Alarm Input* and *Tamper Input* are both active.
NO COMM	No communication.
PAR FLT	Parity fault.

Ending the test

The test period is not limited. The test is stopped you press the ⊖-key. This will return you to the Input Test Menu.

Error messages

If you attempt to carry out this test while another test is running, a message about conflicting tests will be shown on the display, for example: CONFL. BRANCH TEST.

If you attempt to carry out this test when the ThorGuard central Unit is not in the Service Mode, the message NOT SERVICE MODE will be shown in the display.

5.2.6 Output test (Menu 36)

Introduction

The Output Test menu allows you to test any *Output* of the *Areas* covered by the *Terminal Area Mask* of the *Intrusion Terminal.* You can check one *Output* at a time.
The *Areas* in which you want to perform the test must be *unset* before the test.

Starting the test

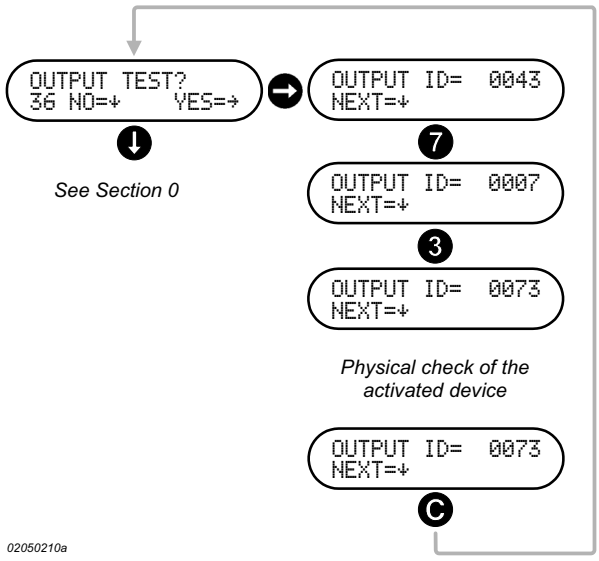
From the Output Test Menu, you can start the test by pressing the ➔-key. This will start the test period for the first *Output* allowed by the *Terminal Area Mask* by displaying a submenu with the *Output ID*.

The *Output ID* shown in the display is the lowest *ID* programmed in the system for the *Areas* assigned by the *Terminal Area Mask*. If this is not the *Output* you want to test, you can press the ↓-key the required number of times until you reach the *Output* you want to test or you can simply enter the 4-digit *Output ID* by means of the numeric keys of the *Intrusion Terminal* as shown in the example below.
Each time you enter or select a new *Output ID*, a test of this *Output* is started.

During the test

As soon as the full *Output ID* has been entered, the test period starts and the selected *Output* is activated so that you can check if the device connected to the *Output* operates correctly.

Fig. 5.8 *Example of starting and ending a test of the Output with the Output ID 0073.*



Ending the test

The test period is not limited. The test is stopped when you press the C-key. This will return you to the Output Test Menu.

Error messages

If you attempt to carry out this test while another test is running, a message about conflicting tests will be shown on the display, for example: `CONFL. BRANCH TEST`.

If you enter a *Zone* number that does not exist, the message `NO AVAILB OUTPUT` will be shown in the display.

5.2.7 Branch test (Menu 37)

Introduction

The Branch Test Menu allows you to perform a *Branch Test* that will test preselected *Outputs* and *Inputs* of all *Areas* covered by the *Terminal Area Mask* of the *Intrusion Terminal* from which the test is performed.
A *User* may perform *Branch Tests* on all *Areas* of the *Terminal Area Mask* although some of the *Areas* may not be assigned to him through his *User Profile*.
Preselection of the *Inputs* and *Outputs* that can be tested is performed during the programming of the ThorGuard Intrusion Alarm System.

The test is automatically stopped when the *Maximum Manual Test Time* expires or when you end the test as described below.
The results of the *Branch Test* are logged in the *Event Log* (*Event* types 150, 151, 152, 153, 154, and 155) where they can be viewed if required. See Section 4.5.14.

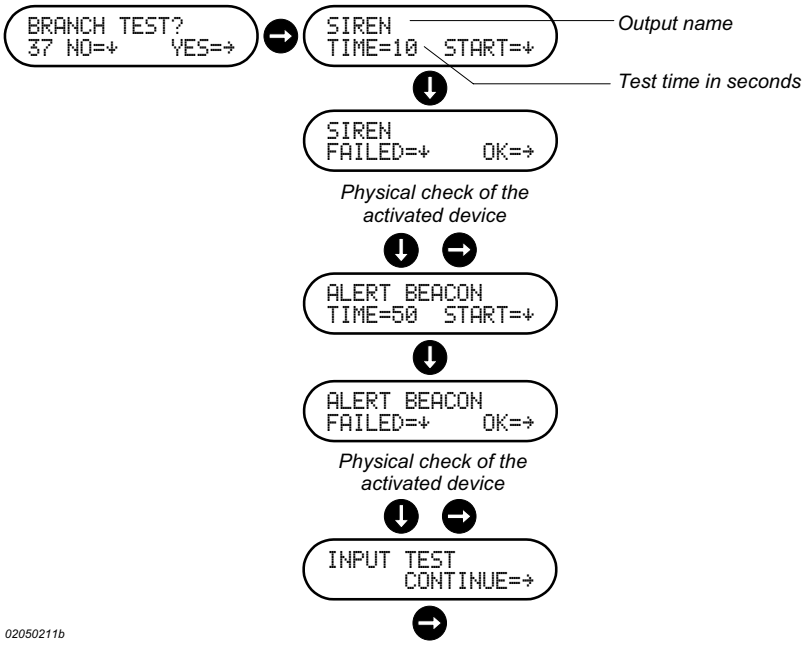
Before you start a *Branch Test,* you must ensure that the system is *unset*. If the system becomes *set* during the test, the test will automatically be terminated.

A *Branch Test* comprise a *Branch Output Test* during which the user physically checks that the output devices of the test are activated, followed by a *Branch Input Test* during which the user physically activates the detectors connected to the inputs of the test, for example door contacts, window contacts, passive infrared detectors (PIR). For detectors with built-in devices for activation during a test, such as most seismic detectors, the test device will automatically be activated.

Starting the Branch Test

From the Branch Test Menu, you can initiate the test by pressing the ➔-key. This will start the *Branch Output Test*.

Fig. 5.9 *Example of a Branch Output Test of the Branch Test. The test comprises two Outputs.*



See Fig. 5.10

Branch Output Test

After start, the display will show the name of an *Output* together with a test time (TIME) that is the time the *Output* is activated during this test. This time is selected in the range from 1 to 255 s during the programming of the system.

The *Output* shown will be the *Output* (preselected) with the lowest *ID* programmed in the system for the *Areas* covered by the *Terminal Area Mask* of the *Intrusion Terminal*.

During the activation, you must check that the device connected to the *Output* is activated. If it is activated, you can confirm this by pressing the ➔-key (OK) on the *Intrusion Terminal*. If the device is not activated, you must press the ↓-key (FAILED).

Pressing one of these buttons displays and activates the next *Output* that is programmed for this test. You must now repeat the procedure of checking the activation of this device and press the ➔-key (OK) if it is activated or the ↓-key (FAILED), if it is not activated.
You must repeat this procedure until all *Outputs* included in the test has been activated and checked. After the last *Output* has been checked and the result confirmed by either the ➔-key the ↓-key, the submenu for start of the *Input Branch Test* is displayed (See Fig. 5.9 and Fig. 5.10).

Branch Input Test

To continue with the *Input Branch Test*, press the ➔-key. This will start the *Branch Input Test*.
After start of the test, the display of the *Intrusion Terminal* will show the name of an *Input* that will be the *Input* (preselected) with the lowest *ID* programmed in the system for the *Areas* covered by the *Terminal Area Mask* of the *Intrusion Terminal*.

List of inputs

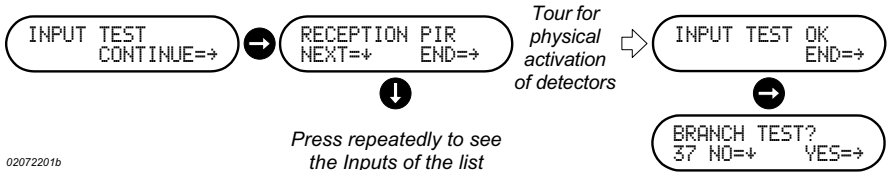
This *Input* name is the first of the list of *Inputs* to be tested. You can step through this list by pressing the ↓-key repeatedly until you reach the start of the list.

If the list contains *Inputs* for detectors with built-in devices for automatic activation during a test, you can see that these *Inputs* will be removed from the list when they have been tested successfully.
Detectors that require physical activation such as passive infrared detectors, (PIR) door contacts, etc. must be manually activated during a tour in the area.

Successful test

If the physical activation is successful, the *Inputs* for these detectors will also be removed from the list, so that the display of the *Intrusion Terminal* will show INPUT TEST OK (Fig. 5.10) when you return from your tour. You can now end the test by pressing the ➔-key. This will return you to the Branch Test Menu.

Fig. 5.10 *Example of a Branch Input Test completed successfully.*

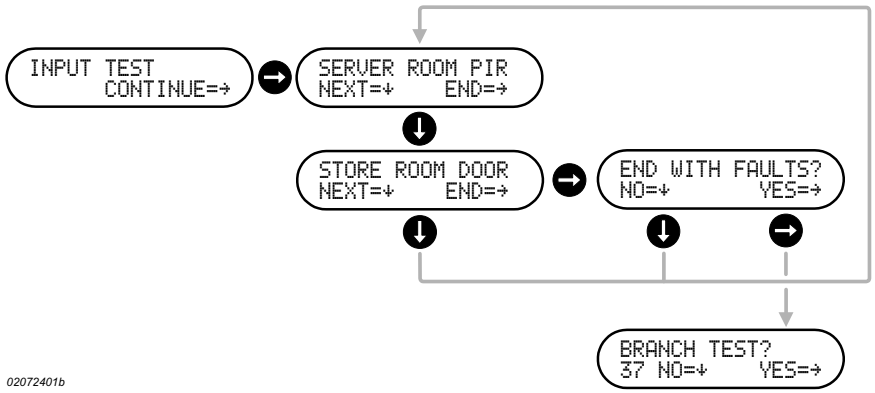


Failing inputs

If detectors fail during the test, the display will show the name of the failing *Input* or if more *Inputs* have failed, the *Input* with the lowest *ID*. You can press the ↓-key repeatedly to display all failing *Inputs* until you reach the start of the list (Fig. 5.11).

With one or more failing *Inputs*, you have two possibilities to get along. You can try to activate the contacts, etc., of the failing *Inputs* to delete the *Inputs* from the list until the display shows INPUT TEST OK as in Fig. 5.10 or you can end the test with the failing *Inputs* present as shown in Fig. 5.11.

Fig. 5.11 *Example of a Branch Input Test completed with two failing Inputs (Detectors).*



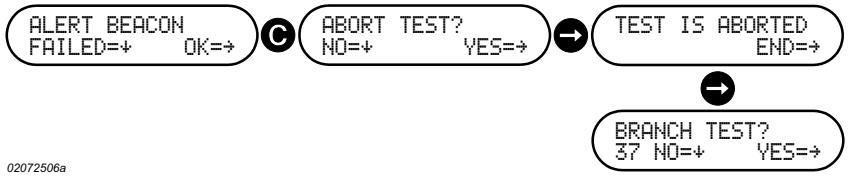
Ending the test

The test can be ended as described above or it can be automatically terminated when the *Maximum Manual Test Time* expires. If automatically terminated, no test results are logged, but the termination (*Event* type 155) of the test will be logged in the *Event Log*.
In both cases, you will be returned to the Branch Test Menu.

Aborting the test

The *Branch Test* can be aborted at any time during the test by pressing the C-key as shown in Fig. 5.12. When the test is aborted, no test results are logged, but the abortion (*Event* type 154) of the test will be logged in the *Event Log*.

Fig. 5.12 *Example of the abortion of a Branch Test during the Branch Output Test.*



Log out during test

During the test, you may log out in order not to leave the *Intrusion Terminal* accessible for operation by unauthorized personnel when you make your tour for activation or check of detectors, contacts, etc. When you return, you may log in again and continue the test from the stage of the test where you logged out.

Error messages

If you attempt to carry out this test while another test is running, a message about conflicting tests will be shown on the display, for example: CONFL. BRANCH TEST.

5.2.8 Hold-up branch test (Menu 38)

Introduction

The Hold-up Branch Test Menu allows you to perform a *Branch Test* that will test the preselected *Inputs* of hold-up pushbutton switches of all *Areas* covered by the *Terminal Area Mask* of the *Intrusion Terminal* from which the test is performed.
A *User* may perform a *Hold-up Branch Test* on all *Areas* of the *Terminal Area Mask* even though some of the *Areas* may not be assigned to him through his *User Profile*.
Preselection of the *Inputs* that can be tested is performed during the programming of the ThorGuard Intrusion Alarm System.

During the test during which the user physically activates the detectors connected to the inputs of the test, for example door contacts, window contacts passive infrared

The test is automatically stopped when the *Maximum Manual Test Time* expires or when you end the test as described below.

The results of the *Hold-up Branch Test* are logged in the *Event Log* (*Event* types 180, 181, 182, 183, and 185) where they can be viewed if required. See Section 4.5.14.

Before you start a *Hold-up Branch test* you must ensure that the system is *unset*. If the system becomes *set* during the test, the test will automatically be terminated.

Starting the test

To start the *Hold-up Branch Test*, press the ➔-key. After start of the test, the display of the *Intrusion Terminal* will show the name of an *Input* that will be the *Input* (preselected) with the lowest *ID* programmed in the system for the *Areas* covered by the *Terminal Area Mask* of the *Intrusion Terminal*.

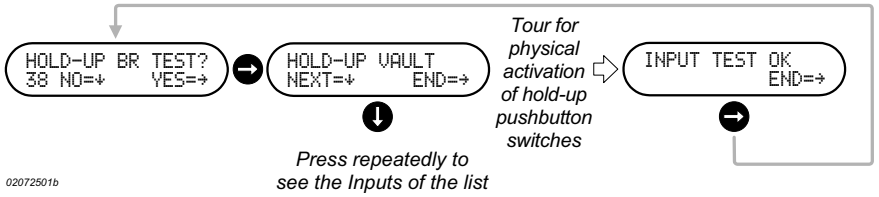
List of inputs

This *Input* name is the first of the list of *Inputs* to be tested. You can step through this list by pressing the ↓-key repeatedly until you reach the start of the list.

Successful test

After start of the test, you must make a tour in the area to activate (and reset) the hold-up pushbutton switches.
If the activation is successful, the *Inputs* for the hold-up pushbutton switches will be removed from the list, so that the display of the *Intrusion Terminal* will show `INPUT TEST OK` (Fig. 5.13) when you return from your tour. You can now end the test by pressing the ➔-key. This will return you to the Hold-up Branch Test Menu.

Fig. 5.13 *Example of a Hold-up Branch Test completed successfully.*

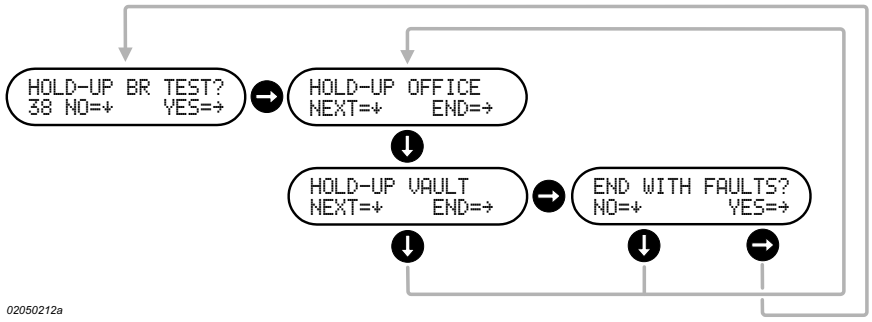


Failing inputs

If hold-up pushbutton switches fail during the test, the display will show the name of the failing *Input* or if more *Inputs* have failed, the *Input* with the lowest *ID*. You can press the ↓-key repeatedly to display all failing *Inputs* until you reach the start of the list (Fig. 5.14).

With one or more failing *Inputs*, you have two possibilities to get along. You can try to activate the hold-up pushbutton switches of the failing *Inputs* to delete the *Inputs* from the list until the display shows HOLD-UP TEST OK as in Fig. 5.13 or you can end the test with the failing *Inputs* present as shown in Fig. 5.14.

Fig. 5.14 *Example of a Hold-up Branch Test completed with two failing Inputs (Switches).*



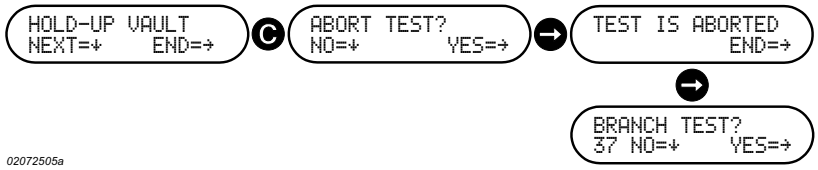
Ending the test

The test can be ended as described above or it can be automatically terminated when the *Maximum Manual Test Time* expires. If automatically terminated, no test results are logged, but the termination (*Event* type 184) of the test will be logged in the *Event Log*.
In both cases, you will be returned to the Hold-up Branch Test Menu.

Aborting the test

The *Hold-up Branch Test* can be aborted at any time during the test by pressing the C-key as shown in Fig. 5.15. When the test is aborted, no test results are logged, but the abortion (*Event* type 183) of the test will be logged in the *Event Log*.

Fig. 5.15 *Example of the abortion of a Hold-up Branch Test.*



Log out during test

During the test, you may log out in order not to leave the *Intrusion Terminal* accessible for operation by unauthorized personnel when you make your tour for activation or check of detectors, contacts, etc. When you return, you may log in again and continue the test from the stage of the test where you logged out.

Error messages

If you attempt to carry out this test while another test is running, a message about conflicting tests will be shown on the display, for example: CONFL. BRANCH TEST.

5.2.9 Bell test (Menu 39)

Introduction

The Bell Test Menu (39) allows you to test all local alarm *Outputs* that operate signalling devices such as bells, sirens, buzzers, beacons, etc. for the *Zones* contained in the *Terminal Area Mask* for the *Intrusion Terminal*.

Starting the test

From the Bell Test Menu, you can start the test by pressing the ➔-key. This will show the submenu and switch on the signalling devices.

Fig. 5.16 *Example of the menu shown during the bell test.*

See Section 5.1

Ending the test

The test period will automatically be terminated when the time set for the automatic log-out – usually two minutes – expires or when you press the C-key. This will return you to the Bell Test Menu.

Error messages

If you attempt to carry out this test while another test is running, a message about conflicting tests will be shown on the display, for example: CONFL. BRANCH TEST.

This page is intentionally left blank.

6

System programming menus

Introduction

This chapter describes the simple programming tasks that can be performed using the System Programming menus.

☛ Please note that the access to the System Programming menus is controlled by the *User Profile* assigned to you.

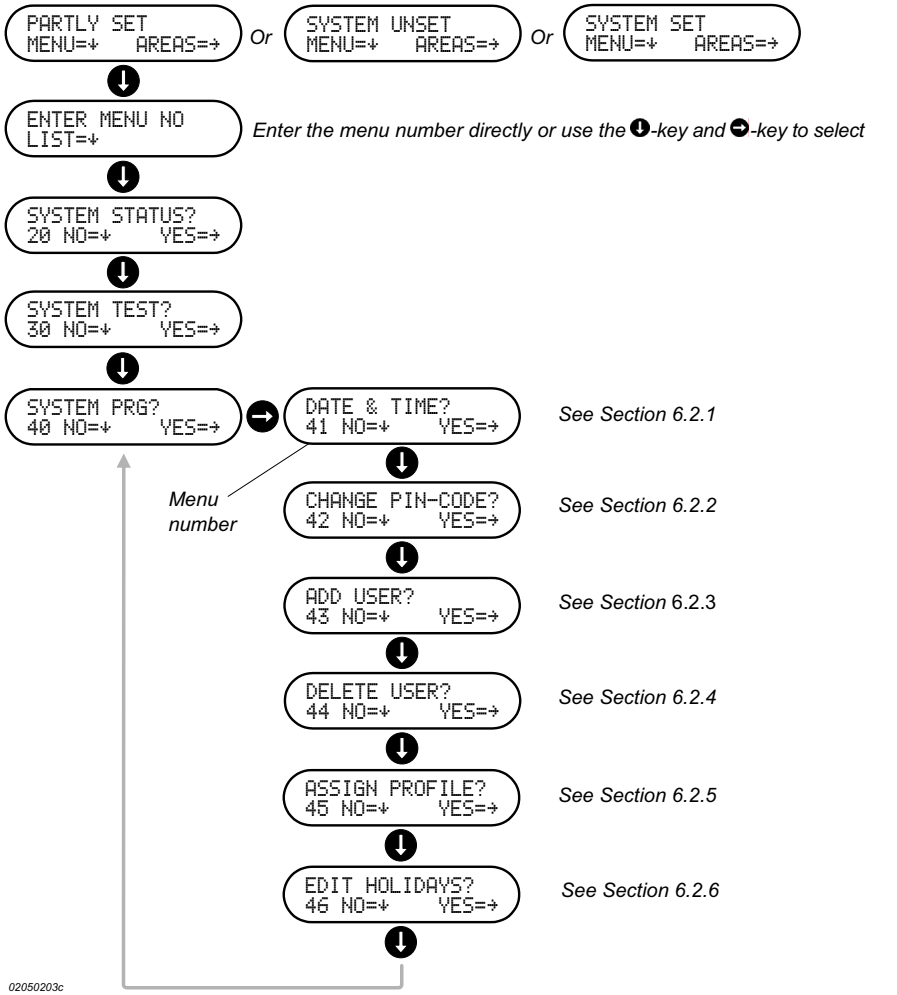
This chapter

The chapter contains the following sections:

6.1 Overview

The System Programming menus comprise the menus shown in Fig. 6.1 below. To access these menus, you must log-in using the procedure of Section 3.2.1. This displays one of the three menus shown in the top of Fig. 6.1, provided that no *Alarms*, *Faults*, *Isolations* or *Disabled Inputs* are present (Section 3.5 and 3.6). Press the ⬇-key to display a menu in which you can select the menu you want by entering its number (Menu 40, 41, 42, 43, 44, 45 or 46) or you can press the ⬇-key repeatedly until the main *System Programming menu* (Menu 40) is displayed. From this, you can press the ➡-key to display the first of the *System Programming menus* (Menu 41). The rest of the menus can be displayed one at a time by pressing the ⬇-key repeatedly as shown in Fig. 6.1.

Fig. 6.1 *Example of the menus available from the system programming menu (40). The example assumes that no alarms, faults, isolations or disabled inputs are present.*



6.2 Performing programming

The System Programming menus give access to perform simple programming of the ThorGuard Intrusion Alarm System. The programming tasks that can be performed are:

- Changing or viewing date and time.
- Changing your *PIN-code*.
- Adding a *User*.
- Deleting a *User*.

6.2.1 Changing or viewing date and time (Menu 41)

Introduction

The Date & Time Menu allows you to view and change the date and time of the ThorGuard Intrusion Alarm System.

Changing date and time

From the Date & Time Menu, you can view the current date by pressing the ➔-key; this displays a submenu showing the date.
To change the date (Fig. 6.2), enter the new date in the format:

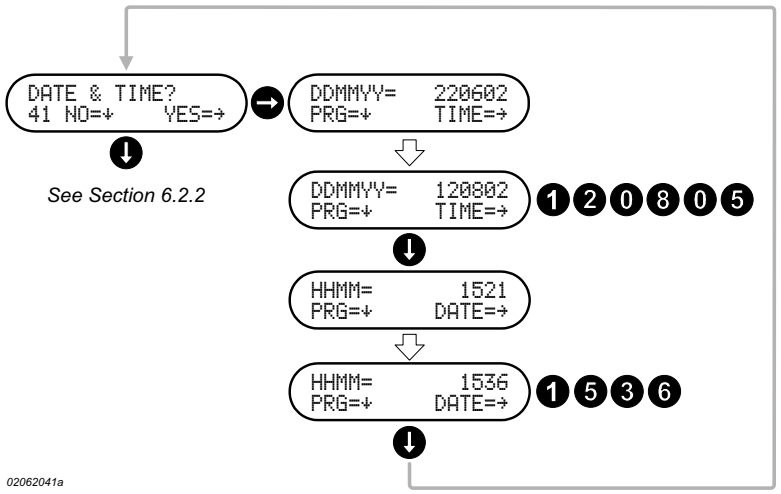
DD	Two digits	The number of the day; for example 02 for the 2nd day.
MM	Two digits	The number of the month; for example 05 for May.
YY	Two digits	The last two digits of the year; for example 02 for 2002.

Then press the ↓-key. This will program the change of the date and display the current time. To change the time (Fig. 6.2), enter the new time in the format:

HH	Two digits	The hour; for example 06 for 6 AM and 18 for 6 PM.
MM	Two digits	The minutes; for example 09.

Then press the ↓-key. This will program the change of the time and return you to the Date & Time Menu time (Fig. 6.2).

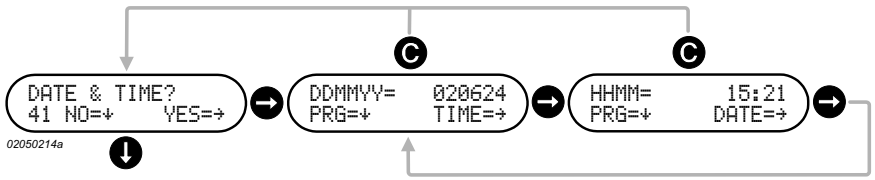
Fig. 6.2 *Example of the setting of date and time.*



Viewing date and time

From the Date & Time Menu, you can view the current date and time by pressing the ➔-key; this displays a submenu showing the date. If you press the ➔-key once more, the time is displayed in the next submenu. Pressing the ➔-key a third time returns you the Date & Time Menu.
If you press the C-key when in any of the submenus, you will return to the Date & Time Menu.

Fig. 6.3 *Example of viewing the date and time.*



See Section 6.2.2

Error messages

If you have entered a wrong date (for example 310205) or time (for example 16:72), the message WRONG DATA RETURN=C will be shown in the display. Press the C-key to return and enter a new date or time.

6.2.2 Changing your PIN-code (Menu 42)

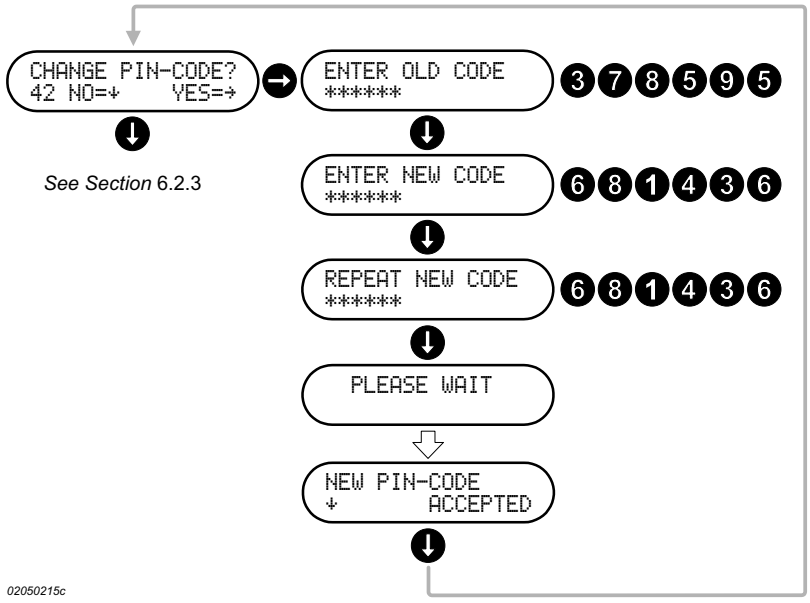
Introduction

The Change PIN-code Menu (42) allows you to change your *PIN-code* any time you want to do so. Your *User Profile* determines whether you have access to this menu.

Changing your PIN-code

To change your *PIN-code*, press the ➔-key to display the submenu for entry of your current PIN-code and enter this *PIN-code*.
Then press the ↓-key to display the submenu for entry of the new *PIN-code*. Enter this *PIN-code,* press the ↓-key again, repeat the new *PIN-code,* and press the ↓-key once more.

Fig. 6.4 *Example of change of PIN-code from 378595 to 681436.*



See Section 6.2.3

This displays the text PLEASE WAIT and shortly after the text, NEW PIN-CODE ACCEPTED, meaning that your new *PIN-code* is valid.

PIN-code time limit

Your *PIN-code* is only valid for the period set during the programming of the ThorGuard Intrusion Alarm System. When you change your *PIN-code,* a new validity period starts

If you have not changed your *PIN-code* before the validity period is about to expire, the display will show the message: PLEASE CHANGE YOUR PIN CODE when you log in. To change the *PIN-code* in this case, please refer to Section 3.1.1.

Please note that when the validity period for your current *PIN-code* expires, you will no longer be able to operate the system. However, you will still be able to log in and change your *PIN-code* as described in Section 3.1.1.

Error messages

If the *PIN-code* is rejected because it does not fulfill the rules of being sufficiently different from other *PIN-codes* the entered *PIN-code* will be rejected and the message WRONG PIN CODE RETURN=C will be shown in the display.

If the *PIN-code* is rejected during the on-line approval, the message NEW CODE NOT ACCEPTED ↓ will be shown in the display. Press the ⓫-key and enter another *PIN-code.*
If the on-line validation of the *PIN-code* is not completed within a certain time, the message TIME-OUT RETURN=C will be shown in the display.

6.2.3 Adding a user (Menu 43)

Introduction

The Add User Menu (43) allows you to add a *User* already programmed in the ThorGuard Intrusion Alarm System to the list of active *Users*.
Your *User Profile* determines whether you have access to this menu.

The *User* that should be added must have been created in the system during its programming, so that *User Profile* and access and operating rights are present in the database of the system.
The *User* to be added can be a *User* that has previously been deleted from the system (See Section 6.2.4) or a *User* that is activated for the first time.

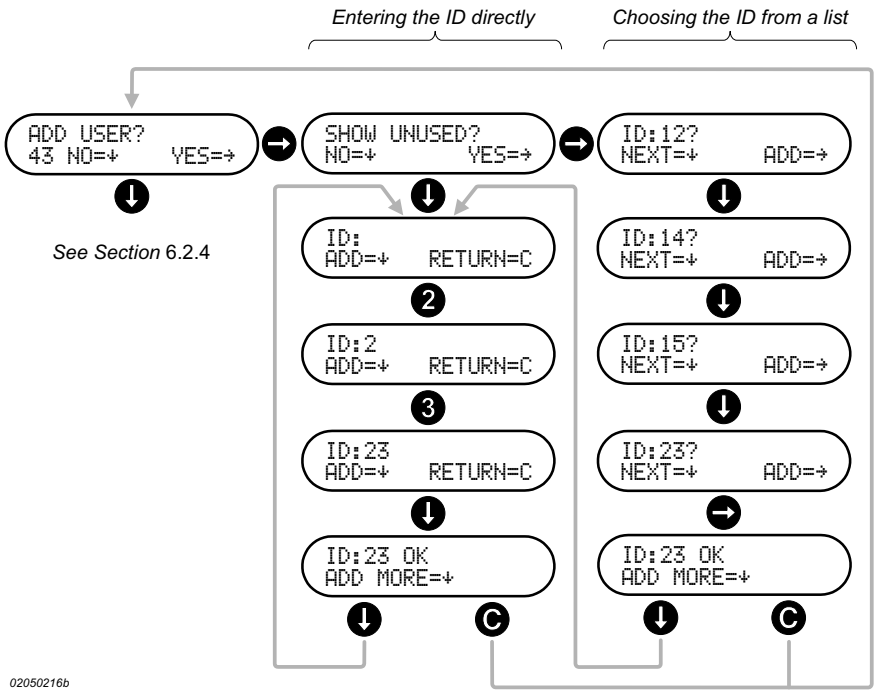
Adding a user

To add a *User*, press the ⓬-key to display the submenu – SHOW UNUSED – where you can select to enter the *User ID* directly or select the *User ID* from a list as described below.

Direct entry

If you know the *ID* of the *User* you want to add, you can press the ⓫-key, and enter the number – 23 in Fig. 6.5 above – using the numeric keys.
When entered, press the ⓫-key to add the *User.* This displays the text ID:23 OK on the *Intrusion Terminal* if the entered *ID* is not used. Otherwise an error message will be shown. If another *User* should be added, press the ⓫-key and enter the next *ID*. If finished, press the ⓒ-key to return to the Add New User Menu.

Fig. 6.5 *Example of adding a User by entering ID directly or by selecting ID from a list.*



Selecting from list

If you wish to ensure that the *User,* you want to add, can be added, you can display a list of *Id*s that is not yet added by pressing the ➔-key. This will display the first free ID. If this is not the one you want to add, press the ↓-key repeatedly until you reach the wanted ID – 23 in Fig. 6.5 above – then press the ➔-key to add the *User.* This displays the text `ID:23 OK` on the *Intrusion Terminal*.

If another *User* should be added, press the ↓-key. This displays a submenu where you can enter the next *ID*.
When finished, press the C-key to return to the Add User Menu.

Default PIN-code

The added *User* is by default equipped with the *PIN-code* 111111 that must be changed when he logs in for the first time. See Sections 6.2.2 and 3.1.1 for more information.

Error messages

When you have entered a *User ID* that is not known in the system, the message `UNKNOWN USER ID` will be shown in the display. Press the C -key and enter a valid *User ID*.
If the entered *User Id* cannot be accepted,the message `ADDING REJECTED TRY OTHER = ↓` will be shown in the display. Press the ↓-key and enter another *User Id.*

If the on-line validation of the *PIN-code* is not completed within a certain time, the message `TIME-OUT RETRY=↓` will be shown in the display. Press the ↓-key to retry.

6.2.4 Deleting a user (Menu 44)

Introduction

The Delete User Menu (44) allows you to delete a *User* from the list of active *Users*. Your *User Profile* determines whether you have access to this menu.

The way in which the *User* is deleted determines whether he is removed from the database or remains in the database and can be added again using the Add User Menu (42) as described in Section 6.2.3.

To delete a *User*, press the ➔-key to display the submenu – ENTER ID – and enter the *ID* of the *User* to delete – 37 in Fig. 6.6 below. Then press the ↓-key. This displays the text SAVE AS RESERVE?.

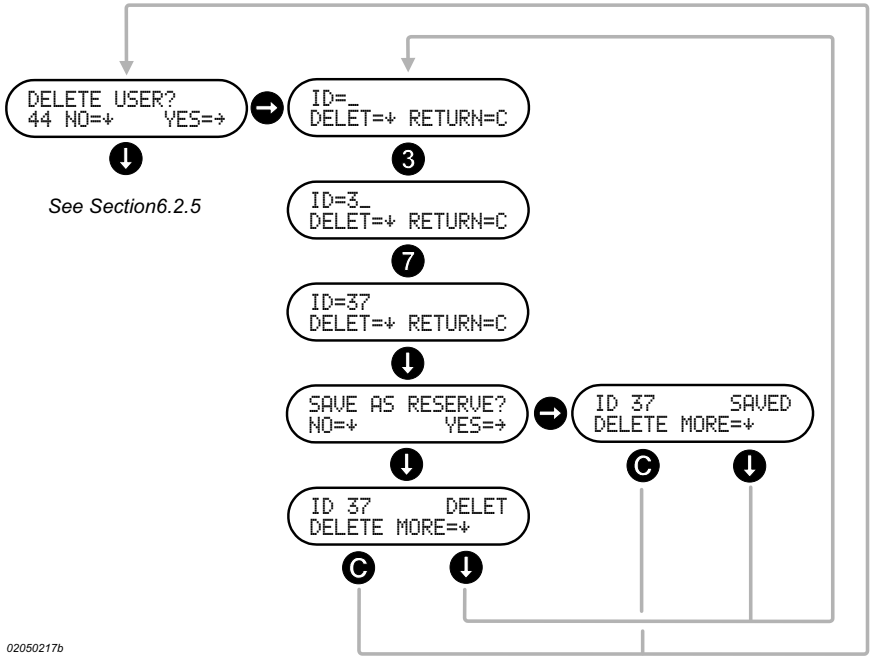
Deleting a user

To delete the *User* completely from the database, press the ↓-key. Deletion is confirmed by the text ID 37 DELET. If the *User* you want to delete does not exist in the database, an error message will be shown.

Save as reserve

If you do not want to delete this *User* from the database but just remove him as an active *User*, press the ➔-key. The User can be added as an active *User* again by means of the Add User Menu (43). See Section 6.2.3 for more information.

Fig. 6.6 *Example of deleting User with the ID 37.*



Error messages

When you have entered a *User ID* that is not known in the system, the message UNKNOWN USER ID will be shown in the display. Press the C -key and enter a valid *User ID*.
If you attempt to delete a *User*, you may receive the message ALREADY DELETED RETURN=C. This means that the *User* in question has already been deleted. However, the *User* has been saved as a reserve.

6.2.5 Assigning a user profile (Menu 45)

Introduction

The Assign Profile Menu (45) allows you to assign a *User Profile* to a *User* from the list of active *Users*. Your *User Profile* determines whether you have access to this menu.
The *User Profiles* that can be assigned must have been created during the programming of the ThorGuard Central Unit using the ThorGuard Configuration System or the ThorGuard Management system.

Selecting User

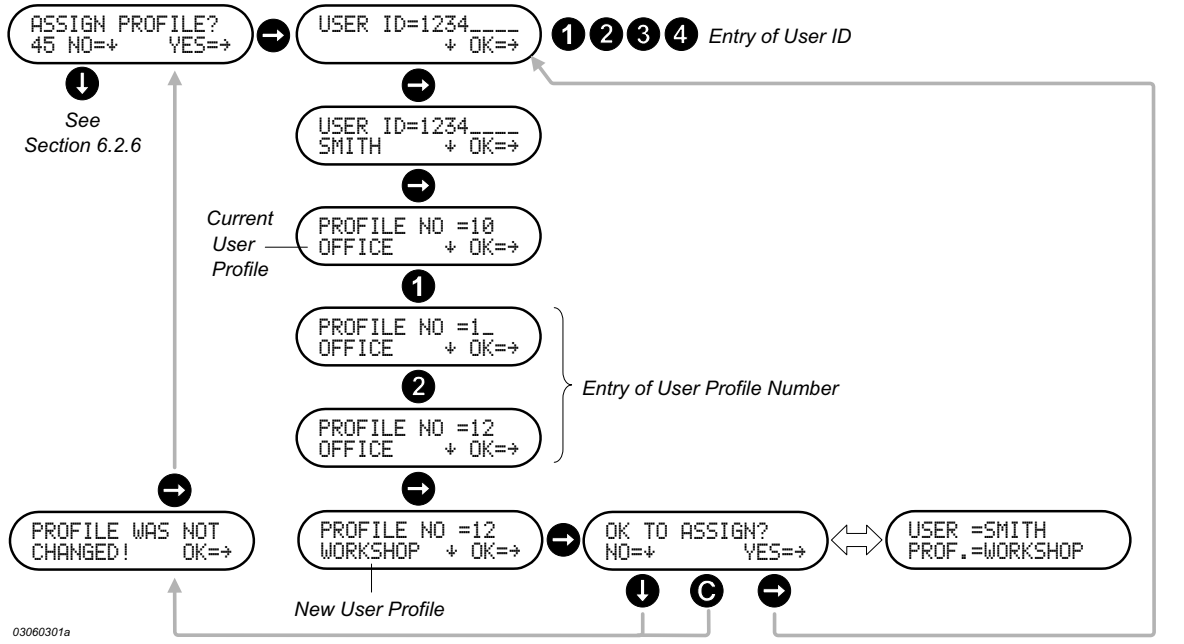
To assign a *User profile*, press the ➔-key of the Assign Profile Menu to display the submenu – USER ID – and enter the *User ID* by means of the numeric keyboard.
The *User ID* may comprise up to eight digits. When the complete *User ID* has been entered, the *User Name* will be shown in the lower line of the display when you press the ➔-key.
You can also use the ↓-key repeatedly to step through the available *User*s to locate the required *User*.

Selecting User Profile

Then press the ➔-key to display the submenu for selecting the *User Profile Number* and enter the *User Profile Number* that may comprise up to two digits using the numeric keyboard. When the complete *User Profile Number* has been entered, the *User Profile Name* will be shown in the lower line of the display when you press the ➔-key.
You can also use the ↓-key repeatedly to step through the available *User Profiles* to locate the *User Profile* that you want to assign.

Then press the ↓-key to display the submenu for confirming the entered *User* and *User Profile*.

Fig. 6.7 *Example of assigning a User Profile to a User.*



Error messages

If you select a profile that allows the user to log-in with his *PIN-code* only, the current *PIN-code* may not always fulfill the rules of being sufficiently different from other *PIN-codes* and the change be rejected during the on-line approval. The message CHANGE NOT ALLOWED will be shown in the display.

6.2.6 Editing a holiday (Menu 46)

The Edit Holiday Menu (46) allows you to edit existing *Holidays*, add (create) new *Holidays* and apply *Holidays* to *Week Programs* for once or repeatedly for the following years and to enable or disable *Holidays*. A total of 25 *Holiday Periods* can be edited or created.
Your *User Profile* determines whether you have access to this menu.

Holidays control which *Day Program* (schedules) to apply for all days of a specified period (*Holiday*) for one, more or all *Week Programs* of the ThorGuard Intruder Alarm System.
The *Day Program* to use is selected by selecting a *daytype* for example Saturday, Sunday, Special day 1 or Special day 2, that all usually differs from the remaining weekdays Monday through Friday.

You may edit *Holidays* created in the management and configuration system as well as *Holidays* created using this menu. However, you should note that the properties of the two types of *Holidays* differ and that the effect of the editing is different as well.

☛ The *Holidays* that you create using the keypad will always apply to all *Week Programs*, while the *Holidays* created in the management and configuration system and edited using the keypad will apply to the *Week Programs* to which they are originally applied. However they can be changed to apply to all *Week Programs*.

Selecting the holiday

When you want to program a new *Holiday* or change an existing, press the ➲-key when in Menu 46 and then select the wanted *Holiday* (1 to 25) by means of the ⓫-key. *Holidays* already programmed have a name or are represented by the dates of the period while unprogrammed *Holidays* are shown as UNUSED.

Entering the period

When you have selected the *Holiday* you want to program, press the ➲-key to display the submenu for entering a period using the numeric keys. After entry of the dates, press the ⓫-key to display the submenu for selecting the *daytype* to be used.

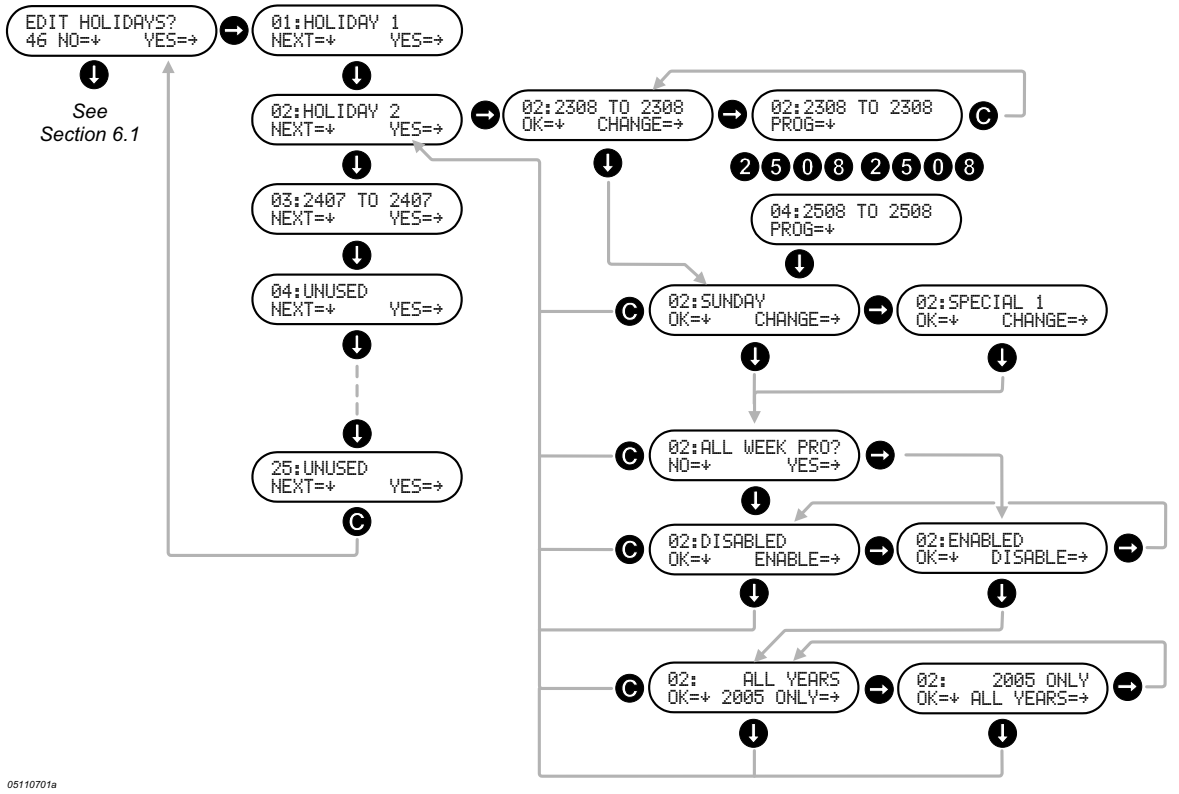
☛ If the *Holiday* does not have a name (UNUSED), the dates entered will be used as the name.

Selecting the daytype

The *daytype* is selected by pressing the the ➲-key the required number of times. You can also enter the number of the *daytype* by means of the numeric keys (1 to 9). *Monday* through *Sunday* are the numbers from 1 to 7 with 1 as *Monday*, while 8 and 9 are the *Special Days 1* and *2*.
After this, press the ⓫-key to display the submenu for selecting how the *Holiday* the should be applied to the *Week Programs*. The menu presented will depend on the status of the *Holiday* as explained on the following page.

! *Please note that you can use any daytype for the Holiday independent of the actual weekdays contained in the Holiday.*

Fig. 6.8 *Example of the editing of an Holiday created in the ThorGuard Configuration System (HOLIDAY 2). The Holiday is currently not applied to all Week programs, it is enabled and the application period is all years.*



Applying the holiday

The ALL WEEK PRO menu is only shown if the *Holiday* that you have edited or created does not already apply to all *Week Programs*. It allows you to make the *Holiday* apply to all *Week* Programs (Press the ➡-key) or to accept its current application (Press the ⬇-key). After this, either the DISABLED menu or the ENABLED status menu will be shown (See below).

☛ Please note that if the *Holiday* is originally created using the ThorGuard Configuration System, the *Holiday* can be applied to either all *Week Programs* (Press the ➡ -key) or only to the *Week Programs* to which it was originally applied (Press the ⬇-key).

Enabling or disabling the holiday

This menu shows the status of the *Holiday*. The status may be either enabled or disabled. The status can be altered by pressing ➡-key. When the status is as wanted, press the ⬇-key. This displays the ALL YEARS menu.

Selecting the application period

This menu shows the current application period, i. e. if the *Holiday* is applied only once or if it is repeated every year. The application period can be altered by pressing ➡-key. When application period is as wanted, press the ⬇-key.

If the *Holiday* should be applied for the next occurrence only, press the ➡-key. This displays the 2005 ONLY menu if the *Holiday* is later than the current date or - 2006 ONLY - if the *Holiday* is prior to the current date.

☛ Please note that the text in the 2005 ONLY menu will change according to the current year and that the text will change to the following year if the *Holiday* is prior to the current date.

7

Technical service menus

Introduction

This chapter describes a number of functions primarily used during maintenance and repair of the system and during the initialization of the system when it is put into operation.

☛ Please note that the access to the Technical Service menus is controlled by the *User Profile* assigned to you.

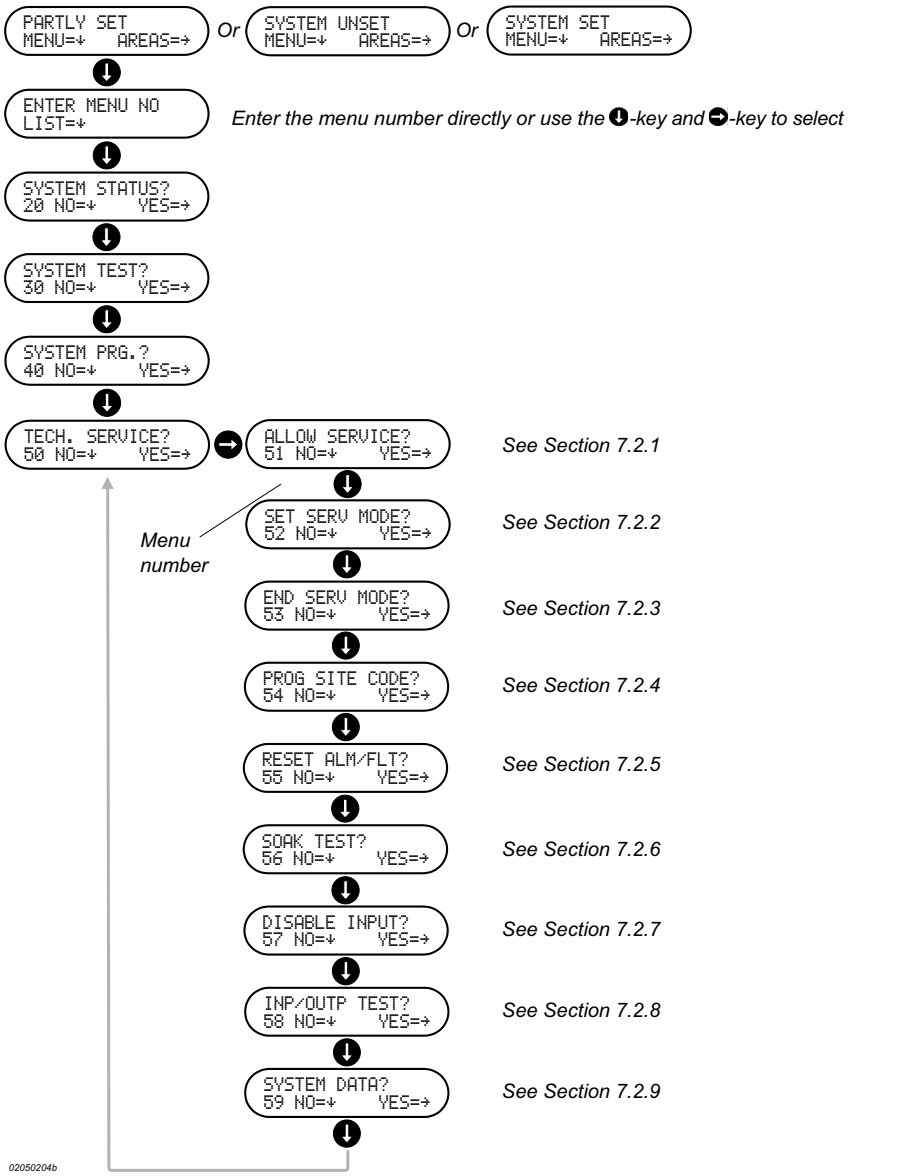
This chapter

The chapter contains the following sections:

7.1 Overview

The Technical Service menus comprise the menus shown in Fig. 7.1 below. To access these menus, you must log-in using the procedure of Section 3.2.1. This displays one of the three menus shown in the top of Fig. 7.1, provided that no *Alarms*, *Faults*, *Isolations* or *Disabled Inputs* are present (Section 3.5 and 3.6). Press the ⬇-key to display a menu in which you can select the menu you want by entering its number (Menu 50, 51, 52, 53, 54, 55, 56, 57 or 59) or you can press the ⬇-key repeatedly until the main *Technical Service menu* (Menu 50) is displayed. From this, you can press the ➡-key to display the first of the *Technical Service menus* (Menu 51). The rest of the menus can be displayed one at a time by pressing the ⬇-key repeatedly as shown in Fig. 7.1.

Fig. 7.1 *Example of the menus available from the technical service menu (50). The example assumes that no alarms, faults, isolations or disabled inputs are present.*



7.2 Using the technical service menus

The information and the functions available via these menus are primarily used during maintenance and repair of the system and during the initialization of the system when it is put into operation.

7.2.1 Allow service (Menu 51)

Introduction

The Allow Service Menu (51) enables you to allow for a single log-in for authorized personnel such as service engineers for special operations on the system. When the engineer logs out, a new log-in cannot be performed by these unless it is allowed again or the system is set in *Service Mode*. See Section 7.2.2 for more information.
The operation that can be performed during the log-in is determined by the *User Profile* of the person that logs in.

☛ During the programming, the ThorGuard Intrusion Alarm System may have been set to automatically allow for this special log-in by the authorized personnel, in case the system has been in the *Alarm* or *Fault* state for more than two minutes.

Allow service

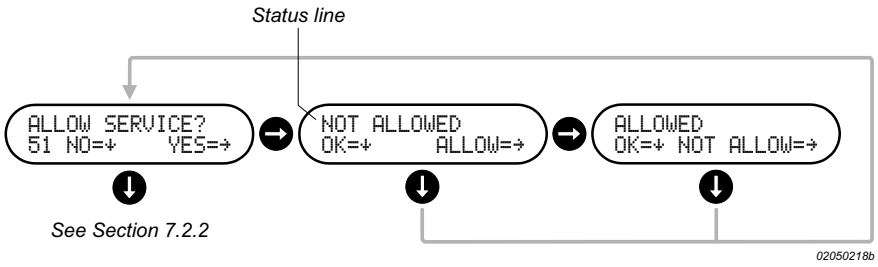
To allow the service, press the ➲-key to display the submenu. If service is not allowed, the status line shows NOT ALLOWED. To allow service, press the ➲-key. This displays the new status ALLOWED.

Cancel service

If you enter the submenu while service is allowed, the status line will show ALLOWED. You may cancel allowed service by pressing the ➲-key.

Please note that service – if allowed – is cancelled automatically when *Service Mode* is set to off using the End Service Mode Menu. See Section 7.2.3

Fig. 7.2 *Example of the use of the Allow Service Menu.*



7.2.2 Set in service mode (Menu 52)

Introduction

The Set In Service Mode Menu (52) is used for setting the ThorGuard Intrusion Alarm System in *Service Mode*. In this mode local *Alarms* will not activate related *Outputs*. However, external *Alarms* are not influenced.

The system must be in *Service Mode* in order to program a site code and select type of General Purpose Interface (GPI) as well for resetting the ThorGuard Central Unit. The system must also be *Service Mode* in order to use the Input Test Menu (35). See Section 0 for more information.

☛ The use of the *Service Mode* is not limited in time. Therefore, it is important that the *Service Mode* is set to off (ended) as soon as this mode is no longer required. To set *Service Mode* off, see Section 7.2.3

When *Service Mode* is on, a *User* with the required *User Profile* has a time unlimited access to operate the system within the operational limits of his *User Profile* until the *Service Mode* is set to off by means of Set Service Off Menu as described in Section 7.2.3.

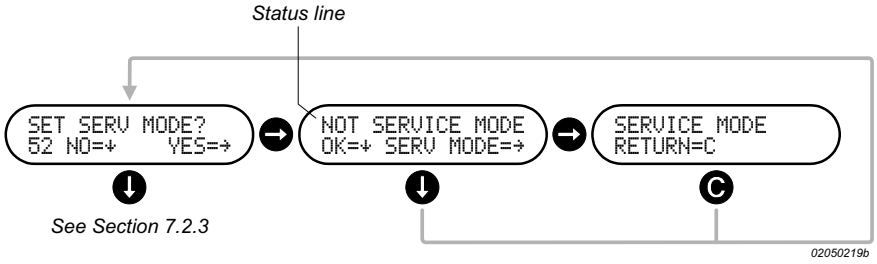
Setting Service Mode to on

To set the *Service Mode* on, press the ➔-key to display the submenu. If not set in *Service Mode*, the status line shows NOT SERVICE MODE. To set in *Service Mode*, press the ➔-key. This displays the new status SERVICE MODE. To return to the Set In Service Mode Menu, press the C -key.
If you enter the submenu while the system is in *Service Mode*, the status line will show SERVICE MODE. You can return to the Set In Service Mode Menu by pressing the C-key.

Log-out attention signal

If you log out while the system is still in *Service Mode*, an attention signal is provided from the *Intrusion Terminal*.

Fig. 7.3 *Example of the use of the Set In Service Mode Menu.*



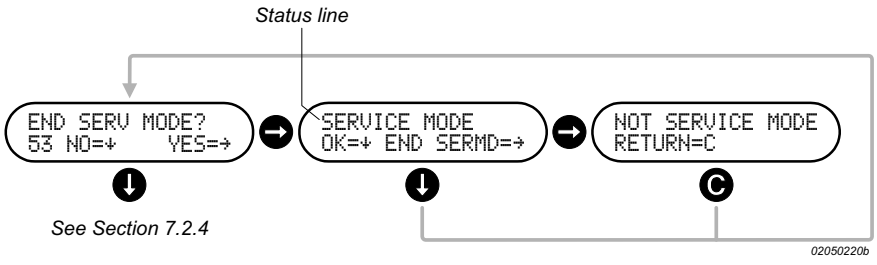
7.2.3 End service mode (Menu 53)

The End Service Mode Menu (53) is used for setting the system back to normal operation after being in *Service Mode* as described in Section 7.2.2.

Ending Service Mode

To end the *Service Mode*, press the ➔-key to display the submenu. If the system is in *Service Mode*, the status line shows SERVICE MODE. To end *Service Mode*, press the ➔-key. This displays the new status NOT SERVICE MODE. To return to the End Service Mode Menu, press the C -key.
If you enter the submenu while *Service Mode* is off, the status line will show NOT SERVICE MODE. You can return to the End Service Mode Menu by pressing the C-key.

Fig. 7.4 *Example of the use of the End Service Mode Menu.*



7.2.4 Entering site code and GPI type (Menu 54)

Introduction

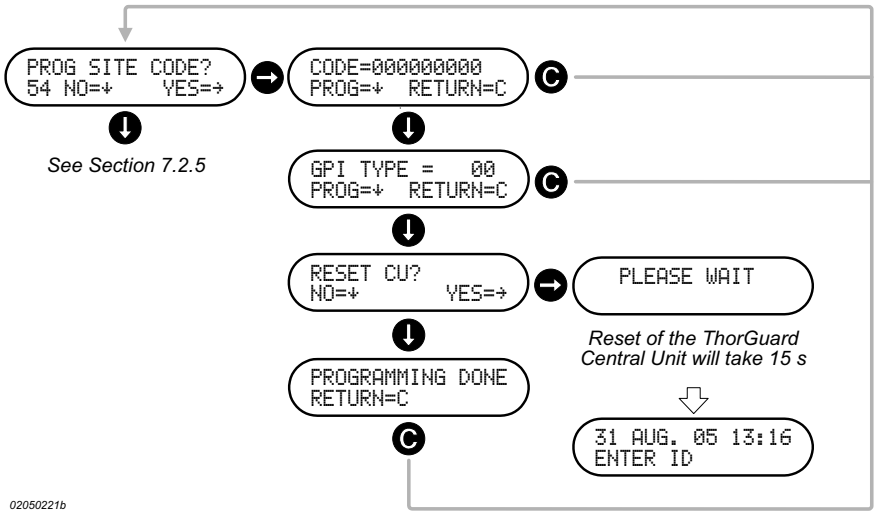
The Program Site Code Menu (54) is used for entry of the *Site Code* for the ThorGuard Intrusion Alarm System, for setting the type of its built-in General Purpose Interface (GPI) and for resetting the ThorGuard Central Unit. The ThorGuard Central Unit must be in Service Mode to perform this operation.

To access the menus for entry of *Site Code*, GPI type and reset of the Central Unit, press the ➔-key to display the first submenu from where you can reach the menus for entry of GPI type and reset of the Central Unit by pressing the ⬇-key once or twice, respectively. See Fig. 7.5 below.

Entry of site code

When in the first submenu, enter the required 9-digit *Site Code* by means of the numeric keys. Then press the ⬇-key to program the number. This displays the next submenu for entry of GPI type.

Fig. 7.5 *Example of menus for entry of site code, GPI type and reset of the Central Unit.*



Entry of GPI type

In this submenu, enter the required 2-digit GPI type by means of the numeric keys (See the table below).

GPI types

GPI type	*Application*
0	No built-in interface
10	PC Interface
20	SECOM transmitter interface
30	Intrusion Printer interface
41	Modem interface set up to default IP parameters
42	Modem interface set up to default HAYES parameters

Then press the ⬇-key to program the number. This will program the number and display the RESET CU menu.

Resetting the Central Unit

When in the RESET CU menu, press the ➔-key to perform the reset. This displays the text – PLEASE WAIT – that remains displayed until the ThorGuard Central Unit has been reset. Reset takes 15 s and is ended by showing the display for log-in. If you need to perform other operations with the system, you must log-in again.

Error messages

When you have entered a *Site Code* that is not allowed in the system, the message WRONG SITECODE will be shown in the display. Press the C -key and enter a valid *Site Code*.
When you have entered a *GPI Code* (Type) that is not allowed in the system, the message WRONG GPICODE will be shown in the display. Press the C -key and enter a valid GPI Code.
If the ThorGuard Central Unit is not in Service Mode while you attempt to perform one of these operations, the error message NOT IN SERVICE MODE SERVICE MODE RETURN=C will be shown in the display. Press the C -key and go to Set in service mode menu (Menu 52) to set the ThorGuard Central Unit in Service Mode See Section 7.2.2.

7.2.5 Clearing of alarms and faults (Menu 55)

Introduction

The Reset Alarms and Faults Menu (55) allows you to clear all *Alarms* or all Faults of the system one type at a time.
To access the menus for clear of *Alarms* and *Faults*, press the →-key to display the first submenu – CLEAR ALL ALRMS? – from where you can reach the submenu for clear of *Faults* by pressing the ↓-key once more. See Fig. 7.6 below.

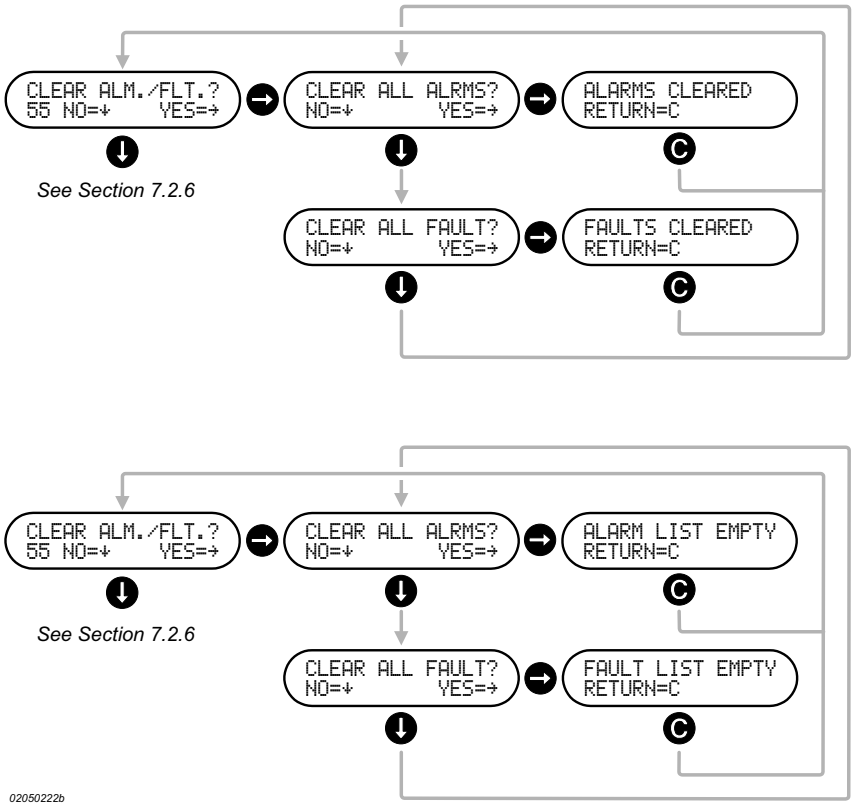
Clearing of all alarms

When in the RESET ALL ALRMS menu, press the →-key to clear all *Alarms*. This displays the text ALARMS CLEARED. Pressing the C-key returns you to the Reset Alarms and Faults Menu.

Clearing of all faults

When in the CLEAR ALL FAULT? menu, press the →-key to clear all *Faults*. This displays the text FAULTS CLEARED. Pressing the C-key returns you to the Reset Alarms and Faults Menu.

Fig. 7.6 *Example of menus for clearing of alarms and faults.*



No alarms or faults

If no *Alarms* or *Faults* are present, the ALARMS CLEARED and FAULTS CLEARED menus will be substituted by ALARM LIST EMPTY and FAULT LIST EMPTY, respectively, when you press the ➔-key to perform a clearing. After this you can return to the Clear Alarms and Faults Menu by pressing the C -key.

Error messages

If one or more *Alarms* cannot be cleared, the message NOT ALL ALARMS CLEARED! will be shown in the display.
If one or more *Faults* cannot be cleared, the message NOT ALL FAULTS CLEARED! will be shown in the display.

7.2.6 Soak test of inputs (Menu 56)

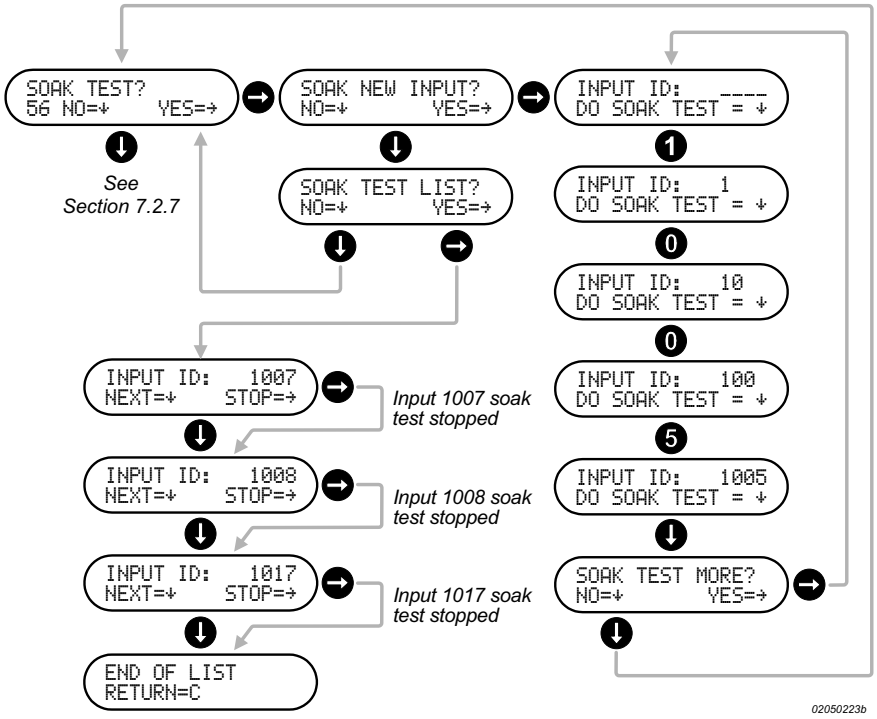
Introduction

The Soak Test Menu (56) allows you to take an *Input* temporarily out of service to investigate faults and instability of detectors.
When an *Input* is in *Soak Test*, an activation of the *Input* will not cause an *Alarm*. The results of the *Soak Test* are logged in the *Event Log* (*Event* types 212, 213, 214, and 215) where they can be viewed if required. See Section 4.5.14.
The *Soak Test* is automatically terminated when the *Soak Test Max Time* expires or when you terminate the test as described below.

☛ When an *Input* is in *Soak Test,* you must be aware that this will degrade the security level of the ThorGuard Intrusion Alarm System.

To access the submenus for setting an *Input* in *Soak Test* or removing it from the *Soak Test*, press the ➔-key of the Soak Test Menu to display the first submenu – SET NEW INPUT – from where you can reach the submenu for entry of the *Input ID* of the *Input* to be tested by pressing the ➔-key or the SOAK TEST LIST submenu by pressing the ↓-key for locating an *Input* to be removed from *Soak Test* . See Fig. 7.7 below.

Fig. 7.7 *Example of menus for soak testing of inputs.*



Starting the test

From the SOAK NEW INPUT submenu, press the ➔-key to display the submenu where you can enter the 4-digit *Input ID* of the *Input* you want to test by means of the numeric keys of the *Intrusion Terminal* as shown in the example below.
When you press the ⬇-key, the *Soak Test* is started.
This also displays the TEST MORE submenu. To set another *Input* in *Soak Test*, press the ➔-key and repeat the procedure above until the *Inputs* required have been put in *Soak Test*, then press the ⬇-key to return to the Soak Test Menu.

During the test

You can now start to manipulate the contact, detector, etc., to change the state of its input. Each change from passive to active and vice versa will be logged in the *Event Log* where the result of the test. See Section 4.5.14.

Ending the test

The *Soak Test* of an *Input* is automatically terminated when the *Soak Test Max Time* expires or when you terminate the test as described below.

From the SOAK TEST LIST submenu by press the ⬇-key the appropriate number of times to locate the *Input* for which to stop the test. When found, press the ➔-key to stop the test.

Error messages

When you have entered an *Input ID* that is not present in the system, the message ERROR:INPUT ID will be shown in the display. Press the Ⓒ -key and enter another *Input ID* if you want to *Soak Tes*t another *Input*.
When you have entered the *Input ID* of an *Input* that cannot be *Soak Tested*, the message NO SOAKTEST INP will be shown in the display. Press the Ⓒ -key and enter another *Input ID* if you want to *Soak Tes*t another *Input*.

7.2.7 Disabling of inputs (Menu 57)

Introduction

The Disable Input Menu (57) allows you to *disable Inputs* for detectors, contacts, etc. that cause trouble so that they are taken out of service until they can be exchanged or repaired. When working correctly again, they can be *enabled* using the same menu.

☛ When you *disable* an *Input,* you must be aware that this will degrade the security level of the ThorGuard Intrusion Alarm System.

To access the submenus for *disabling* or *enabling* an *Input*, press the ➔-key of the Disable Input Menu to display the first submenu – DISABLE NEW INP – from where you can reach the submenu for entry of the *Input ID* of the *Input* to *disabled* by pressing the ➔-key or the DISABLE LIST submenu by pressing the ⬇-key for locating an *Input* to be *enabled*. See Fig. 7.8 below.

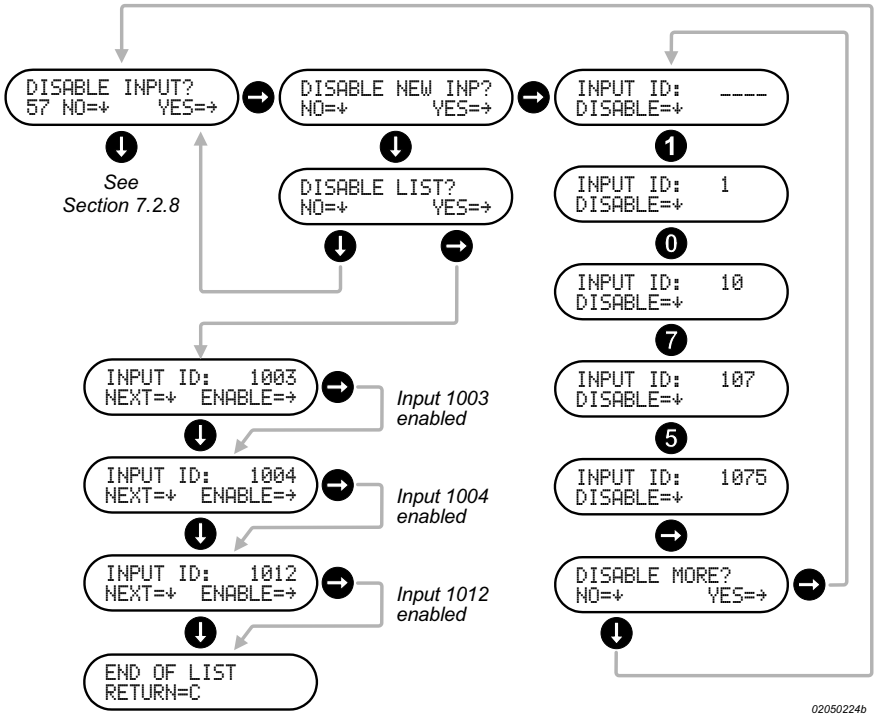
Disabling an input

From the DISABLE NEW INP submenu, press the ➔-key to display the submenu where you can enter the 4-digit *Input ID* of the *Input* you want to *disable* by means of the numeric keys of the *Intrusion Terminal* as shown in Fig. 7.8. When you press the ⬇-key, the *Input* is *disabled*.
This also displays the DISABLE MORE submenu. To *disable* another *Input*, press the ➔-key and repeat the procedure above until the *Inputs* required have been *disabled*, then press the ⬇-key to return to the Disable Input Menu.

Enabling an input

From the LIST OF DISABLED submenu by press the ⬇-key the appropriate number of times to locate the *Input* to be *enabled*. When found, press the ➔-key to *enable* the *Input*. Repeat the procedure until the *Inputs* required have been *enabled*.

Fig. 7.8 *Example of menus for disabling and enabling of inputs.*



Error messages

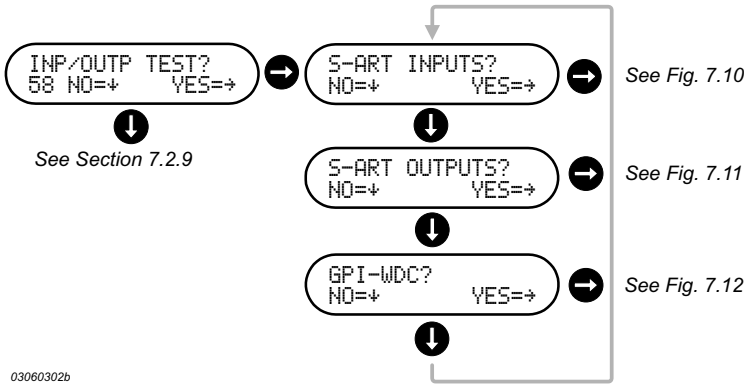
When you have entered an *Input ID* that is not present in the system, the message `ERROR: INPUT ID` will be shown in the display. Press the **C** -key and enter another *Input ID* if you want to *disable* another *Input*.
When you have entered the *Input ID* of an *Input* that cannot be *disabled*, the message `NO DISABLE INPUT` will be shown in the display. Press the **C** -key and enter another *Input ID* if you want to *disable* another *Input*.

7.2.8 Input/output testing (Menu 58)

The Inp/outp Test Menu allows you to perform a test of all S-ART inputs and outputs of the system one by one – also these not yet configured. However, the S-ART Expansion Board to which the S-ART Bus belongs must have been configured.
You may also test *GPI-WDC*s that are General Purpose Interfaces that are used for communicating the status of wireless detectorsto the ThorGuard Central Unit.

☛ This menu is only available when the ThorGuard central Unit is in *Service Mode*. See Section 7.2.2.

Fig. 7.9 *Example of the menus for selecting tests of Input or Output S-ARTs or Inputs connected to a GPI-IO.*



S-ART inputs

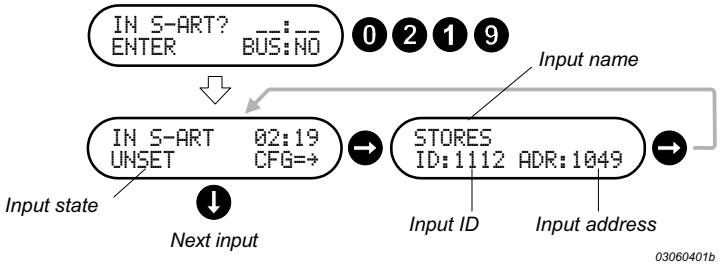
The S-ART input test will show the current state of the selected S-*ART input* and its name, *ID*, and *Address*.

To select the *S-ART input* you want to check, enter the *S-ART Bus* and *S-ART* numbers. In the example of Fig. 7.10, the *S-ART Bus* number 02 and *S-ART* number 19 has been entered. After the last entry, the state of the *S-ART input* will be shown.
You can now start to manipulate the contact, detector, etc., to change the state of its input. Each change from passive to active and vice versa is indicated by an *Activation Signal* and is logged in the *Event Log* where the result of the test can be viewed. See Section 4.5.14.

The numbering of *S-ART Buses* is explained in the Technical manual for the ThorGuard Intrusion Alarm System ref. No. 91001002 (English version) in Section 2.2.9.

If you press the ➔-key (CFG=→), the display will show the name of the *S-ART*, the *ID* of the *S-ART* and the *address*. If the S-ART Controller has not yet been configured, the CFG=→ is removed so that no more information can be shown.
To go to another *S-ART input*, press the ➔-key and enter a set of *S-ART bus* and *S-ART* numbers or simply press the ↓-key the required number of times to reach the next *S-ART input* that you want to check.

Fig. 7.10 *Example of menus for checking the state, name and ID and address of an S-ART input.*



S-ART outputs

The S-ART output test will change current state of the selected *S-ART input* and show this state, the name of the S-*ART output*, its *ID*, and *address*.

To select the *S-ART output* you want to check, enter the *S-ART bus* and *S-ART* numbers. In the example of Fig. 7.11, the *S-ART bus* number 11 and *S-ART*

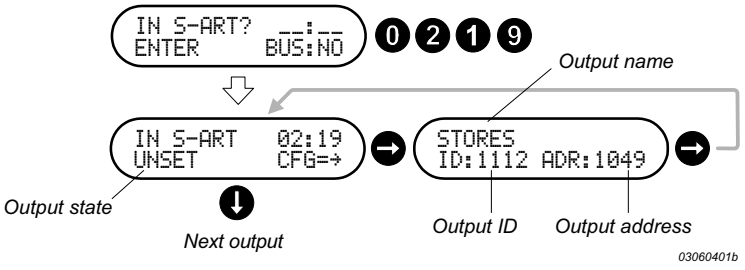
number 27 has been entered. After the last entry, the changed state of the *S-ART output* will be shown (ON or OFF).

You can hear or see the change of the state from on to off or vice versa. The change is not logged in the *Event Log*.

The numbering of *S-ART Buses* is explained in the Technical manual for the ThorGuard Intrusion Alarm System ref. No. 91001002 (English version) in Section 2.2.9.

If you press the ➔-key (CFG=➔), the display will show the name of the *S-ART*, the *ID* of the *S-ART* and the *address*. If the S-ART Controller has not yet been configured, the CFG=➔ is removed so that no more information can be shown.
To go to another *S-ART output*, press the ➔-key and enter a set of *S-ART Bus* and *S-ART* numbers or simply press the ↓-key the required number of times to reach the next *S-ART output* that you want to check.

Fig. 7.11 *Example of menus for checking the state, name, ID and address of an S-ART output.*

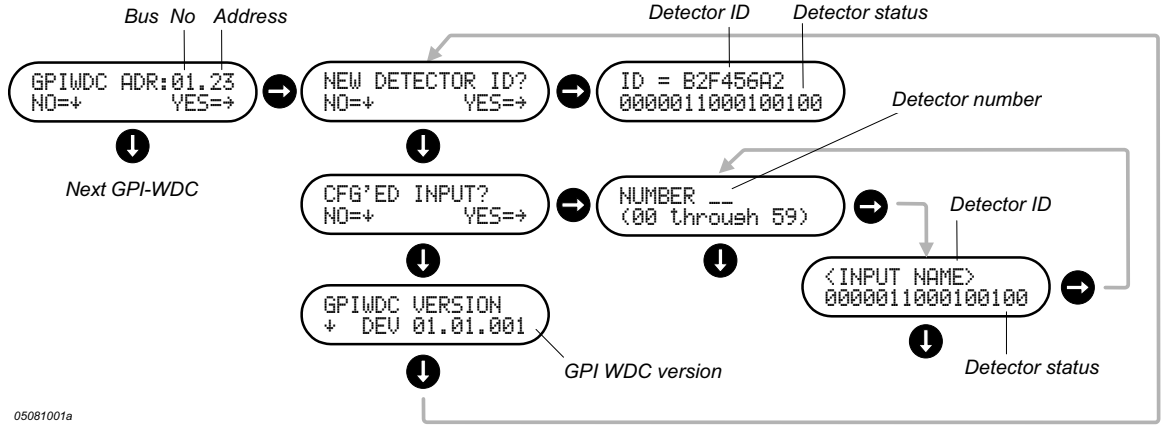


GPI-WDC test

The GPI-WDC menu allows you to check the status of a wireless detector or identify a detector manufactured by Inovonics® or to check the current version of a selected GPI-WDC . These wireless detectors communicate with the ThorGuard Central Unit through GPI-WDCs that each may accept up to 60 detectors (0 to 59).

☛ Please note that the GPI-WDC must be configured in the ThorGuard Central Unit. Otherwise the ThorGuard Central Unit will not recognize the GPI-WDC. Consequently, the GPI-WDC will not appear in the list.

Fig. 7.12 *Example of menus for testing or identifying detectors connected via GPI-WDCs.*



In order to check the status of or identify a detector or the version of a selected GPI-WDC, select the required GPI-WDC using the ⬇-key. The GPI-WDCs are identified by their MMP-bus addresses. When you find the GPI-WDC you want, press the ➡-key for submemus for identifying and checking a new detector (), for checking a configured detector () or for checking the version of the GPI-WDC (). These submenus are displayed when you press the ➡-key the required number of times (Fig. 7.12).

New detector ID

The NEW DETECTOR ID? submenu is used when you must find the identity (ID) of a new detector after it has been installed but before it is configured. After you have selected the NEW DETECTOR ID? submenu, press the ➡-key and reset the detector. When you have reset the detector, you will see its ID and the detector status (See the table below).

☛ For reset of the detector, please refer to the documentation supplied with the detector.

Configured detector ID

The CFG'ED INPUT? submenu is used when you want to check the ID and status of a configured detector. Press the ➡-key to to display the submenu for entering the ID of the detector. The number (From 0 to 59) is the position of the detector within the GPI-WDC. When you press the ➡-key after having entered the number, the display will show the detector ID together with the status of the detector (See the table below)

GPI-WDC version

The GPIWDC VERSION submenu provides information of the selected GPI-WDC.

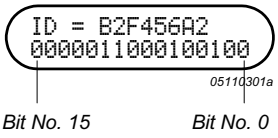
Error messages

If no GPI-WDC is recognized by the ThorGuard Central Unit, the message NONE FOUND is shown in the display.

Detector status

The status shown in the display can be interpreted by means of the table below. Please note that bit No. 15 is situated leftmost.

According to the table, the status for the detector shown to as an example to the right, the repeater has no battery (Bit 10 is 1) and has lost line power (Bit 9 is 1) in addition to this, low margin (Bit 5 is 1) and is in alarm state (Bit 3 is 1).

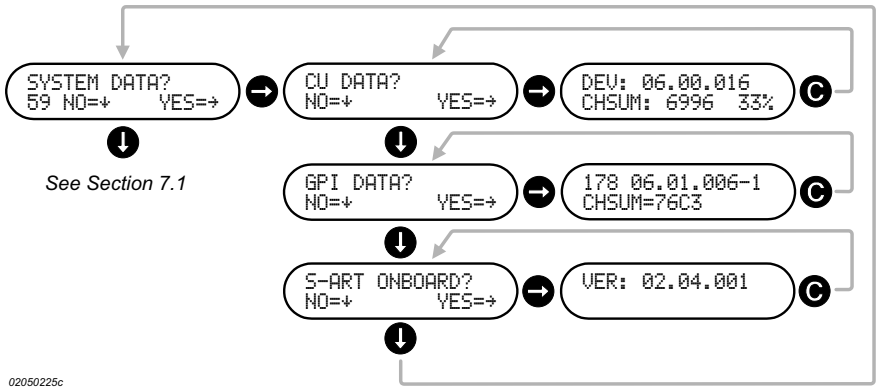


Bit No.	*Description*	*Receiver*	*Detector*	*Repeater*
15	Receiver jammed	√		√
14	Low battery		√	√
13	Case or wall tamper	√	√	√
12	Status unknown	√	√	√
11	Spare 2			
10	Battery missing			√
9	Loss of line power			√
8	Defective battery			√
7	No communication			
6	Clean me (Smoke detectors only)		√	
5	Low margin		√	√
4	Low level		√	√
3	Alarm		√	
2	Alarm		√	
1	Alarm		√	
0	Alarm 0 (Primary)		√	

7.2.9 Central Unit version and GPI version (Menu 59)

The System Data (59) is used for checking the software versions installed in the ThorGuard Central Unit (CU), its built-in General Purpose Interface (GPI), and the on-board S-ART Controller.

Fig. 7.13 *Example of menus for display of software versions of the Central Unit and the built-in General Purpose Interface.*



This page is intentionally left blank.

8

Time lock menus

Introduction

This chapter describes the menus used for the manual release, blocking or unblocking of *Time Locks* and the display of the status of the release process for an automatically as well as a manually operated *Time Lock*.

☛ Please note that the access to the Time Lock menus is controlled by the *User Profile* assigned to you.

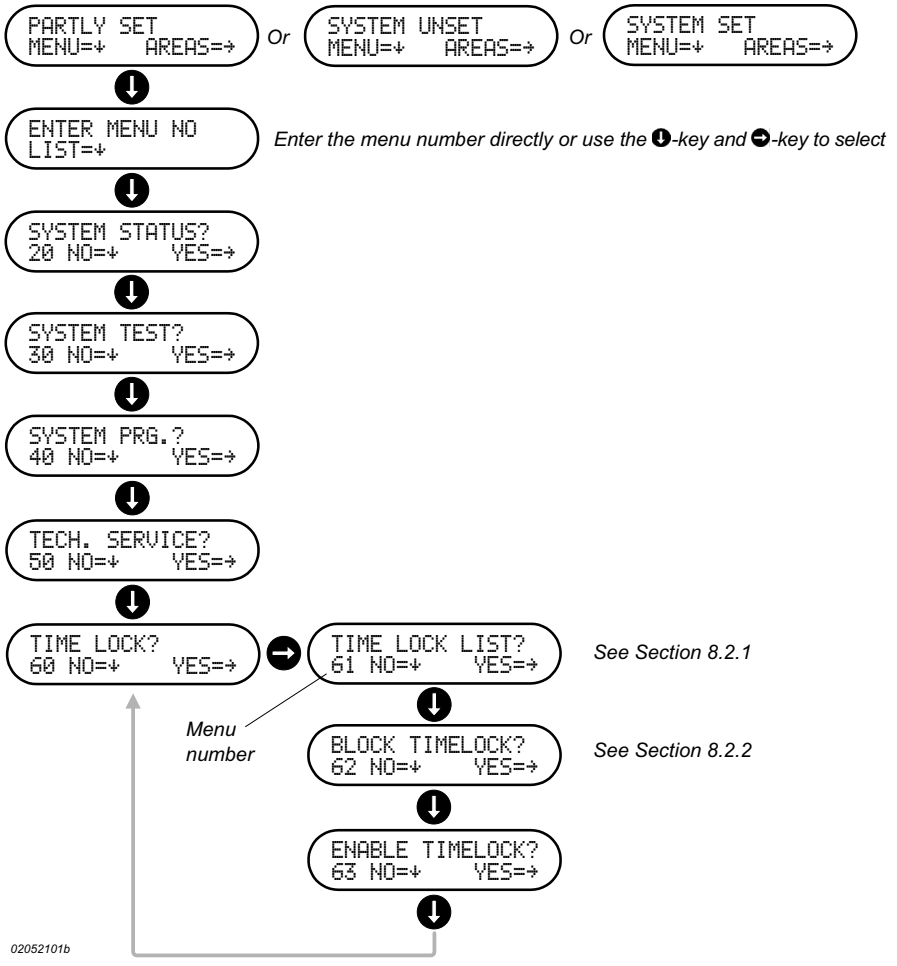
This chapter

The chapter contains the following sections:

8.1 Overview

The Time Lock menus comprise the menus shown in Fig. 8.1 below. To access these menus, you must log-in using the procedure of Section 3.2.1.
This displays one of the three menus shown in the top of Fig. 8.1, provided that no *Alarms*, *Faults*, *Isolations* or *Disabled Inputs* are present (Section 3.5 and 3.6). Press the ⬇-key to display a menu in which you can select the menu you want by entering its number (Menu 60, 61 or 62) or you can press the ⬇-key repeatedly until the main *Time Lock menu* (Menu 60) is displayed. From this, you can press the ➡-key to display the first of the *Time Lock menus* (Menu 61). The rest of the menus can be displayed one at a time by pressing the ⬇-key repeatedly as shown in Fig. 8.1.

Fig. 8.1 *Example of the menus available from the Time Lock menu (60). The example assumes that no alarms, faults, isolations or disabled inputs are present.*

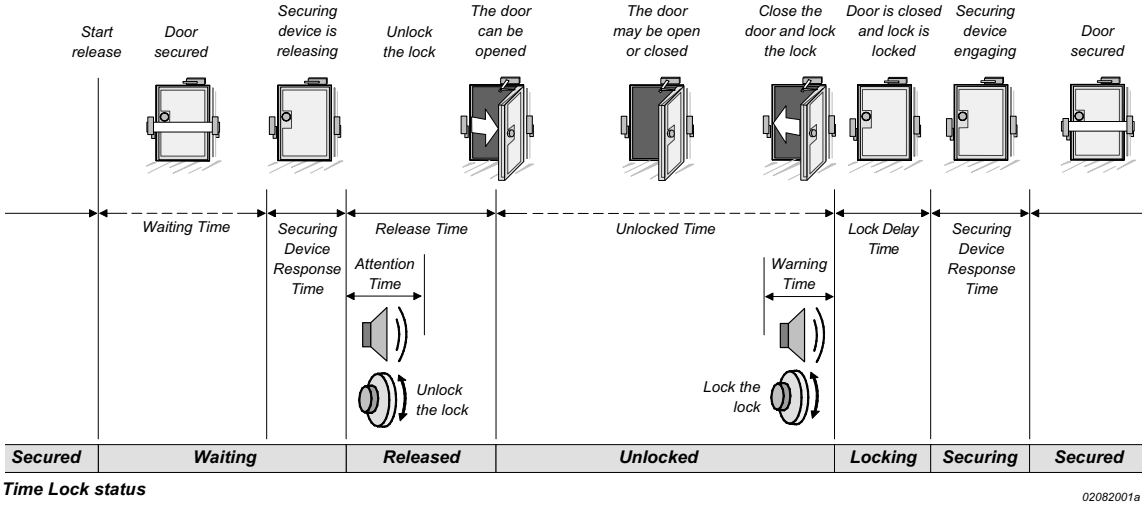


8.2 Using the time lock menus

Introduction

As previously described in Section 3.3.3, a *Time Lock* handles the time controlled access to a vault or a safe by electrically operating the securing device of the door of the vault or the safe while monitoring whether the lock is unlocked or locked.
If the *Time Lock* is automatically operated, the release process is started when the *Area* to which the *Time Lock* belongs is *unset* (Section 3.3.3).
If the *Time Lock* is manually operated, the release process is performed as described in the following section 8.2.1. For the automatic as well as the manual operation, the timing diagram is the same from the start of the release process to the end where the door is secured. See the example below.

Fig. 8.2 *Example of timing diagram for a time lock that is manually operated. Please note that only the status of the lock is monitored, the door may be opened or closed as required during the Unlocked Time until Warning Time starts.*



The release of the securing device – including the physical operation of the lock – is explained in the following section. The description applies to the automatic as well as the manual release of the lock from the time at which the release process starts and until the door is secured again.

☛ Please note that the above figure assumes the securing device and the lock is equipped with contacts to detect their state. No contact is used for detecting the position of the door.

All *Time Locks* of a ThorGuard Intrusion Alarm System can be blocked using the Block Locks Menu (Section 8.2.2). To unblock the *Time Locks*, you can use the Unblock Locks Menu (Section 8.2.3).

8.2.1 Time lock list (Menu 61)

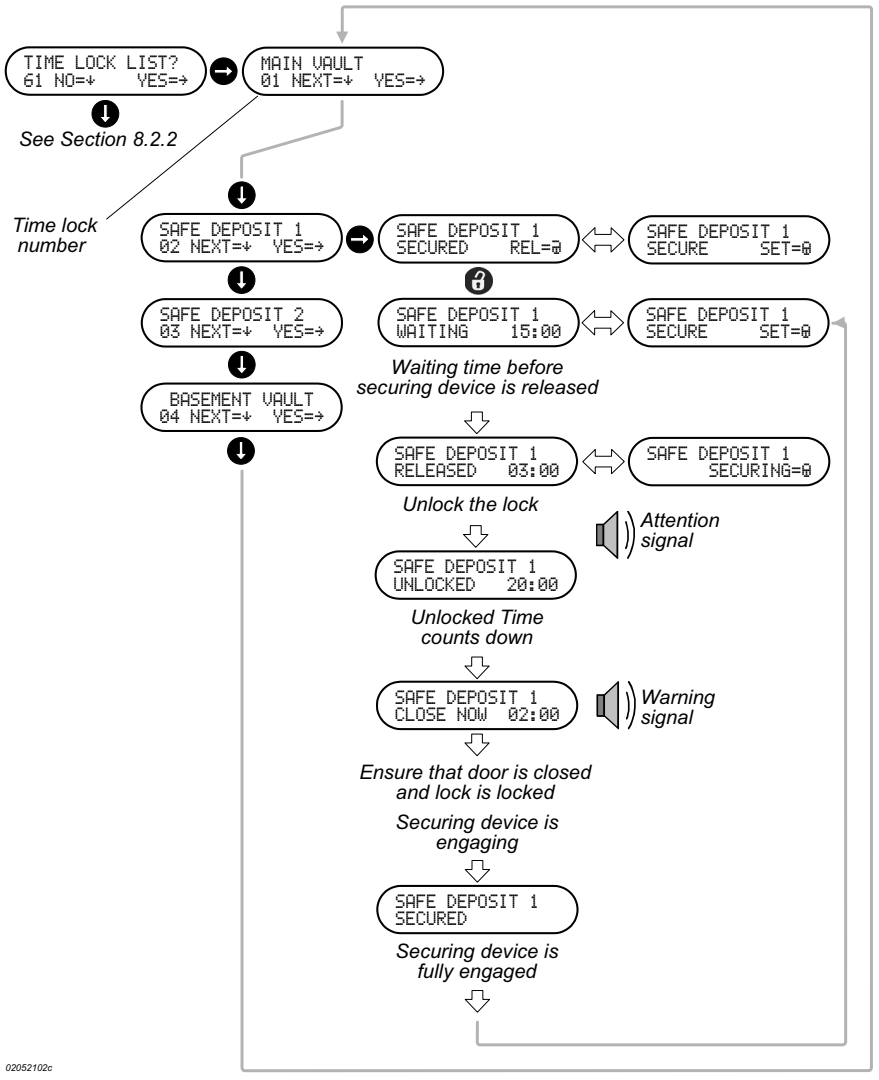
Introduction

If manual release of one or more *Time Locks* has been selected during the programming of the ThorGuard Intrusion Alarm System, the release of these *Time Locks* is performed using the Time Lock List Menu.
More *Time Locks* can be released at the same time unless their operation is interlocked.

Manual release

From the Time Lock List Menu, press the ➔-key to display the *Time Lock* with the lowest number. If this is not the *Time Lock* you want, you can press the ↓-key the required number of times until you reach the required *Time Lock* or you can enter the number of the *Time Lock*.

Fig. 8.3 *Example of the release of a time lock. In this case, the* SAFE DEPOSIT *with the time lock number* 02. MAIN VAULT 01, SAFE DEPOSIT 02 *and* BASEMENT VAULT 04 *are operated as* SAFE DEPOSIT 02.



Starting the release

When you have selected the required *Time Lock*, press the ➔-key and check whether the status is SET or SECURED. If SET, press the 🔒-key to *unset* and change the status to SECURED. Then you can press the 🔒-key to start the release of the electrically operated securing device. This displays the status WAIT together with the *Waiting Time* (Minutes and seconds) before release of the lock.

Release of the securing device

When *Waiting Time* expires, the display changes to RELEASED, and the built-in buzzer of the *Intrusion Terminal* provides an attention signal to indicate that the electrically operated securing device is released.

Unlocking the lock

The lock can be now unlocked and the door may be opened or stay closed as required. The remaining *Release Time* (Minutes and seconds) can be seen in the display.

☛ The lock must be unlocked before the *Release Time* expires. If not, the electrically operated securing device starts engaging and the display changes to SECURING. When fully engaged, the display changes to SECURED.

Unlocked

When the lock becomes unlocked, the display changes to UNLOCKED and the remaining *Unlocked Time* (Minutes and seconds) can be seen in the display. When you lock the door within the *Unlocked Time*, the *Time Lock* will enter the state LOCKING, proceeding with SECURING until SECURED.

Closing the door

When the *Unlocked Time* is about to expire, the display changes to WARNING, and the built-in buzzer of the *Intrusion Terminal* and any external signalling device provides a warning signal to indicate that the door must be closed – if open – and the lock must be locked.

☛ The door must be closed and the lock must be locked before the *Warning Time* expires. If not, the display will show ALARM LOCK OPEN.
The *Alarm* is maintained until the lock is locked. After this, the *Time Lock* will enter the state LOCKING, proceeding with SECURING until SECURED.

Lock Delay Time

When the *Warning Time* expires, the display changes to LOCKING, indicating that the *Lock Delay Time* is active. This delay ensures that the operator has time to lock the lock before the electrically operated securing device starts engaging. The remaining *Lock Delay Time* (minutes and seconds) can be seen in the display.

Securing device engaging

When the *Lock Delay Time* expires, the display changes to SECURING, indicating that the electrically operated securing device starts engaging. The remaining *Securing Device Response Time* (minutes and seconds) can be seen in the display.

Secured

When the securing device is fully engaged, the display changes to SECURED.

Reopening

For the individual *Time Lock,* a *Reopening Time* can be set during programming. Within this time, the *Waiting Time* is substituted with the usually shorter *Reopening Waiting Time*.

Extended Waiting Time

If the ThorGuard Intrusion Alarm System is in *Duress State*, the *Waiting Time* is extended with a *Hold-up Waiting Time*.

Bypass Waiting Time

The *Time Locks* may be controlled by device that enables the *Time Lock* to bypass the *Waiting Time* as well as *Hold-up Waiting Time* that the lock can be unlocked immediately.

Status during automatic release

For *Time Locks* that are automatically released, the progress of the release process can be followed when required.
From the System Status Menu (20), you can press the ❻-key and the ❶-key to jump to the TIME LOCK LIST menu if you want to follow the release process of a *Time Lock*. From this menu, you can press the ❵-key one or more times – if more *Time Locks* are associated with the *Area* – to locate the required *Time Lock* and press the ❷-key to see the status of the *Time Lock*.
In the listed order the following is displayed: WAITING - RELEASED - UNLOCKED - LOCKING - SECURING - SECURED - SET.

Error messages

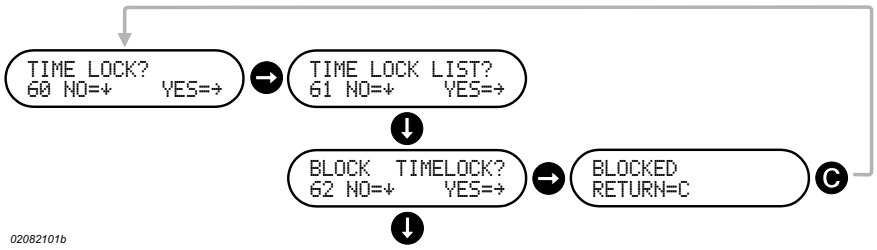
When you attempt to *unset* the the *Area* to which the *Time Lock* belongs, you may receive the message `UNSET NOT ALLOWED` plus a reason for this, for example `TL BLOCKED`.

8.2.2 Block Locks (Menu 62)

Introduction

If you want to prevent the release (Manual or automatic) of all *Time Locks* in a ThorGuard Intrusion Alarm System, you can use the Block Locks menu (62) as shown in Fig. 8.4 below.
The *Time Locks* can be unblocked again by using the Unblock Locks Menu (63).

Fig. 8.4 *Example of the blocking of the time locks. All time locks are blocked at the same time.*



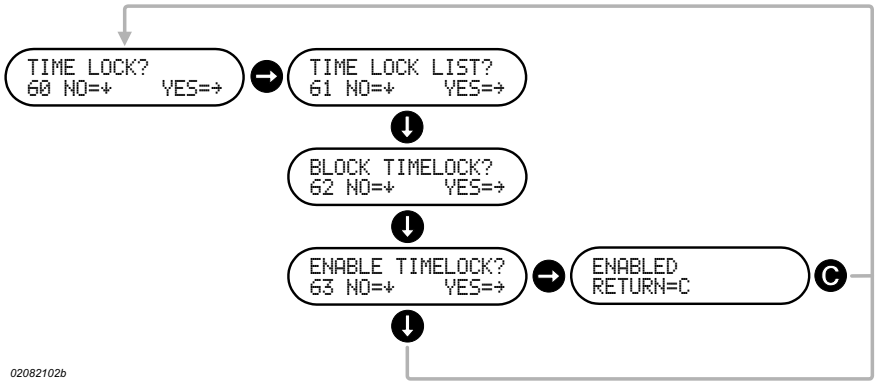
See Section 8.2.3

8.2.3 Unblock Locks (Menu 63)

Introduction

To unblock all blocked *Time Locks* in a ThorGuard Intrusion Alarm System, you can use the Block Locks Menu (62) as shown in Fig. 8.5 below.

Fig. 8.5 *Example of the unblocking of the time locks. All time locks are unblocked at the same time.*



9

Output control menus

Introduction

This chapter describes the menus used for the manual control of for example light, doors, Closed Circuit Television equipment (CCTV), etc.

☛ Please note that the access to the Output Control Menus is controlled by the *User Profile* assigned to you.

This chapter

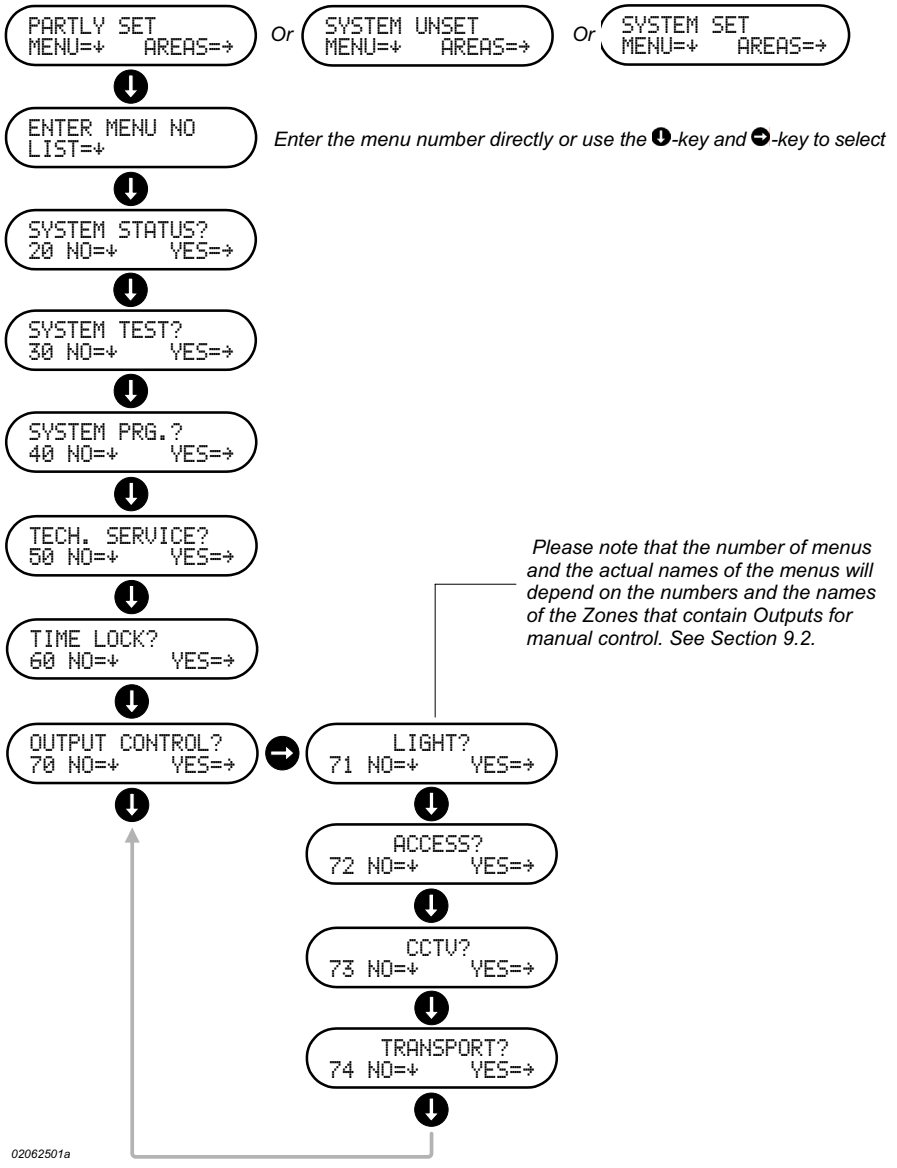
The chapter contains the following sections:

9.1 Overview

The Output Control Menus comprise the menus from 70 to 79. The figure below is an example from a system containing four *Zones* with outputs for manual control providing four submenus (71 to 74) for operating the outputs.

To access these menus, you must log-in using the procedure of Section 3.2.1. This displays one of the three menus shown in the top of Fig. 9.1, provided that no *Alarms*, *Faults*, *Isolations* or *Disabled Inputs* are present (Section 3.5 and 3.6). Press the ⬇-key to display a menu in which you can select the menu you want by entering its number or you can press the ⬇-key repeatedly until the main Output Control menu (Menu 70) is displayed. From this, you can press the ➡-key to display the first of the Output Control menus (Menu 71). The rest of the menus can be displayed one at a time by pressing the ⬇-key repeatedly as shown in Fig. 9.1.

Fig. 9.1 *Example of menus that may be available from the Output Control Menu (70). The example assumes that no alarms, faults, isolations or disabled inputs are present.*



9.2 Using the output control menus

Introduction

The Output Control Menus are used for manual control of for example light, doors, CCTV equipment (Closed Circuit Television), etc.

Number of menus

Up to nine submenus (Menu 71 to Menu 79) may be available via the main Output Control Menu (70). The actual number of submenus available will depend on the number of *Zones* programmed with *Outputs* for manual control.

Menu names

The names of the submenus are automatically the same as the names of the *Zones* with *Outputs* for manual control. The names are automatically allocated so that the name of the *Zone* with the lowest number is used for Menu 71, the Zone with next lowest number is used for Menu 72 and so on.
The names of the submenus for switching on or off an *Output* are automatically allocated so that the name of a submenu is the same as the name of the *Output*.

More than nine zones

If manually controlled *Outputs* are present in more than nine *Zones*, the *Outputs* from the remaining *Zones* are automatically allocated to Menu 79.

9.2.1 Output control menu examples (Menu 71 - 74)

Introduction

In the example shown in Fig. 9.2, four *Zones* have *Outputs* for manual control. The names of the Zones are LIGHT, ACCESS, CCTV and TRANSPORT.
The manually controlled *Outputs* of these *Zones* are accessible via Menus 71, 72, 73 and 74.

In the example of Fig. 9.2, the submenus for switching on or off the *Outputs* are shown for the Zones LIGHT and ACCESS; for the remaining *Zones*, only the menus for the *Zones* are shown.

Navigating between submenus

From Menu 71, you can access the first submenu by pressing the ➔-key. The first submenu actually comprises two submenus that you can switch between by pressing the ➔-key thereby switching on or off the *Output* depending on the current status of the *Output*. The submenu with the current status of the *Output* will always be shown first.

From the first as well as the second of these submenus, you can step through the remaining submenus by pressing the ⬇-key the appropriate number of times. This is indicated by the alternate display of the submenu itself and a submenu with the text NEXT=} as shown to the right in Fig. 9.2.
Also in this case, the submenu with the current status of the *Output* will be shown first.
For each submenu, you can switch on or off the *Output* – depending on the current status of the *Output* – by pressing the ➔-key.

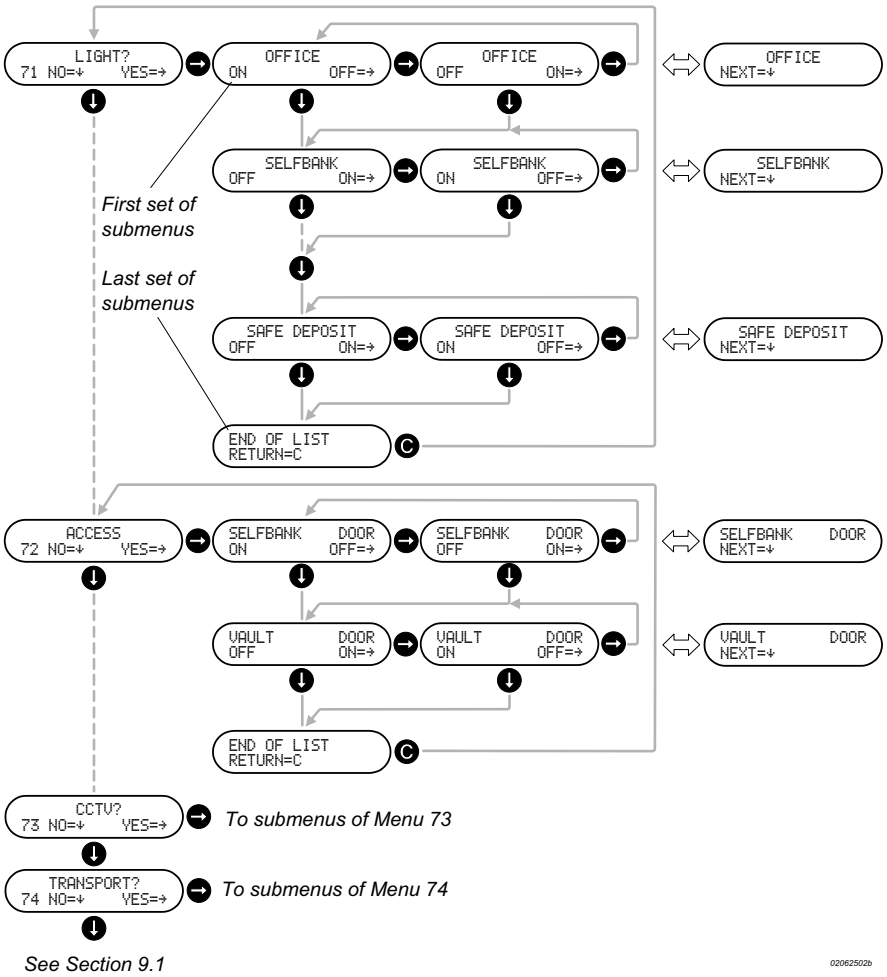
When you reach the last submenu, the display will show END OF LIST. Pressing the ⓒ-key now – or at any time during your way through the submenus – will return you to the Menu 71.

When in Menu 71, you can go on to menu 72 by pressing the ➔-key or to any of the remaining menus by pressing the ➔-key the appropriate number of times. From these menus, navigation between the submenus is performed as described above.

Example

In the example of Fig. 9.2, Menu 71 gives access to submenus for switching the light on various locations on or off. Menu 72 gives access to submenus for unlocking or opening various doors. Menu 73 gives access to submenus for starting and stopping recording on a Closed Circuit Television (CCTV).

Fig. 9.2 *Example of the Output Control Menus and their operation. The example deals with a ThorGuard Intrusion Alarm System containing four Zones with outputs for manual control. The menus,* CCTV *and* TRANSPORT *also have a number of associated submenus not shown in this example.*



Denmark

HI SEC International

Marielundvej 16
DK- 2730 Herlev
Denmark

Tel.: +45 44 50 78 00
Fax: +45 44 50 78 01
E-mail: dk @ hisec.com

United Kingdom

HI SEC International

4B Victoria Avenue
Camberley Surrey GU15 3HX
United Kingdom

Tel.: +44 (0) 1276 679 950
Fax: +44 (0) 1276 679 949
E-mail: gb @ hisec.com

France

HI SEC International

ZAC de Nanteuil
12, rue Jules Ferry
F-93561 Rosny sous Bois
France

Tel.: +33 (0) 1 48 12 90 10
Fax: +33 (0) 1 48 12 90 20
E-mail: fr @ hisec.com

HISEC
INTERNATIONAL