FIRE-LITE ALARMS

IP Communicator

IPDACT

Installation Manual

Document DM373-I
Version 2.0
March, 2007

Table of contents

I - Chapter. Introduction I-1

I - 1. IPDACT Introduction I-1
I - 1.1. User Scenario I-1
I - 1.2. Operation Mode I-3
I - 1.2.1. Monitoring I-3
I - 1.2.2. Alarm sending I-5
I - 1.3. Additional features I-6

II - Chapter. IPDACT Description II-7

II - 1. General Description II-7
II - 2. LEDs II-10
II - 3. Jumper II-11
II - 4. Connection points to the Control Panel and external II-11
II - 5. LAN II-13
II - 6. Console II-13

III - Chapter. Installation and cabling III-17

III - 1. Installation III-17
III - 1.1. Assembly Instructions for the IPDACT box III-19
III - 2. Wiring III-20
III - 2.1. Wiring for UL Listed Fire Installations III-20
III - 2.1.1. Installation scheme III-20
III - 2.1.2. Installation instructions III-22

IV - Chapter. Configuration IV-27

IV - 1. Configuration modes IV-27
IV - 2. DHCP IV-27
IV - 3. Telephonic Console IV-29
IV - 3.1. Configuration IV-30
IV - 3.1.1. Default Configuration IV-32
IV - 3.1.2. Register description IV-32
IV - 3.1.3. Minimum configuration for the installer ... IV-38
IV - 3.1.4. Configuration Example IV-39
IV - 4. Asynchronous Console IV-41
IV - 4.1. Accessing the console IV-41

IV - 4.2. Main Menu IV-41
IV - 4.3. IPDACT generic configuration..... IV-42
IV - 4.4. Monitoring configuration and sending of alarms. IV-42
IV - 4.5. IPDACT Quick Configuration IV-43
IV - 4.6. Monitoring IV-44

IV - 5. Telnet IV-46

V - Chapter. Appendix V-47

V - 1. UL Compliance..... V-47

V - 2. Control Panels..... V-47

V - 3. Technical Specifications..... V-48

The manufacturer reserves the right to introduce changes and improvements to the appropriate features of both the hardware and the software of this product, modifying the specifications included in this manual without prior notice.

I - Chapter. Introduction

I - 1. IPDACT Introduction

The IP module (IPDACT) is a device which, when connected to a security control panel, carries out three basic tasks:

- To send over an IP network the alarm information sent by the panel to which this is connected.
- To check the connectivity between the control panel and the alarms reception center.
- In cases where it is not possible to transmit over the IP network, the IPDACT will stop intercepting the alarms from the panel. At this point the alarms will be sent over the telephone line.

The IPDACT operates together with the Teldat **VisorALARM** device, located in the alarm receiver center. This behaves as an alarm receiver which receives the alarms through an IP network (instead of the traditional public switch telephone network) and sends them through a serial port to automation software in order to be processed. Additionally, this receives monitoring messages from multiple IPDACT and generates the corresponding alarm in cases where communication fails with one or more of these. For further information on how the IP **VisorALARM** receiver operates, please see manual Dm 357-I.

I - 1.1. User Scenario

A traditional security scenario consists of a control panel (CP), located in the client environment and an alarm receiver center (ARC) located in the security company's control center. The CP contains a group of sensors which trigger a series of alarms or events which, when produced, are sent to the ARC to be processed.

Communication between the above is traditionally carried out over the telephone line so that both ends can initiate a call to the remote end: the CP in order to notify events and the ARC for bi-directional tasks (activation, teleloading and general control).

The communication protocol varies depending on the manufacturers who usually tend to use their own solutions. The IPDACT supports Contact-ID protocol.

The CP is placed as the first connection element to the PSTN so that it can prioritize the customer's telephone line.

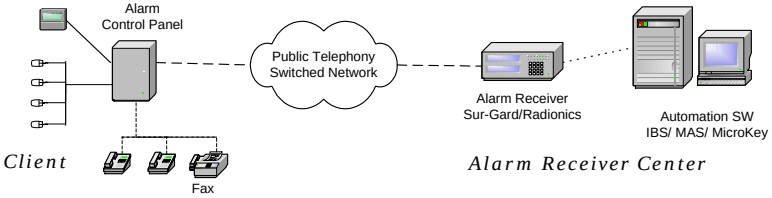


Figure 1. Traditional security scenario

Within the general user scenario, the IPDACT device is located in the client area, next to the control panel, intercepting the telephone line. This is displayed in **Figure 2**. The arrow in the figure demonstrates the preferred path to send alarms from the CP; here the telephone line is used as a backup in case there is a communication malfunction in the IP network.

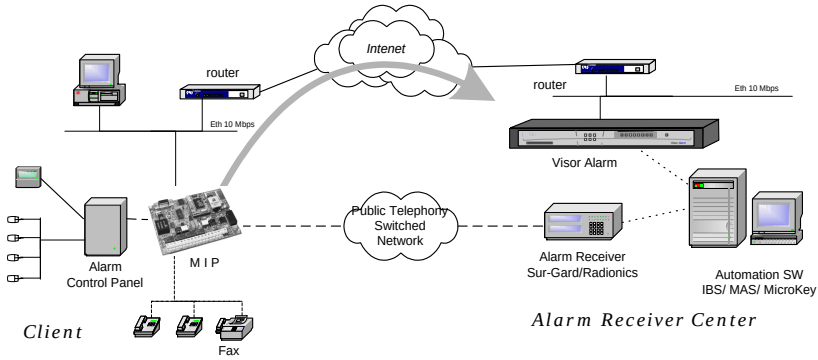


Figure 2. Teldat VisorALARM and IPDACT operating scenario

From firmware release 2.2 onwards, the IPDACT has a new functionality incorporated giving rise to a third possible scenario: network backup. In the previous scenario, where communication fails between the device and the ARC, the IPDACT hands over the communications to the control panel. With the new functionality, the IPDACT tries to open communications with a second device, the backup **VisorALARM**. Only in cases where there are problems with this second device does the control panel take over. Meanwhile, even in this state, the IPDACT continues to try and communicate with the ARC until one of the **VisorALARMs** responds.

In UL compliance installations, the IPDACT must have firmware version 4.0.

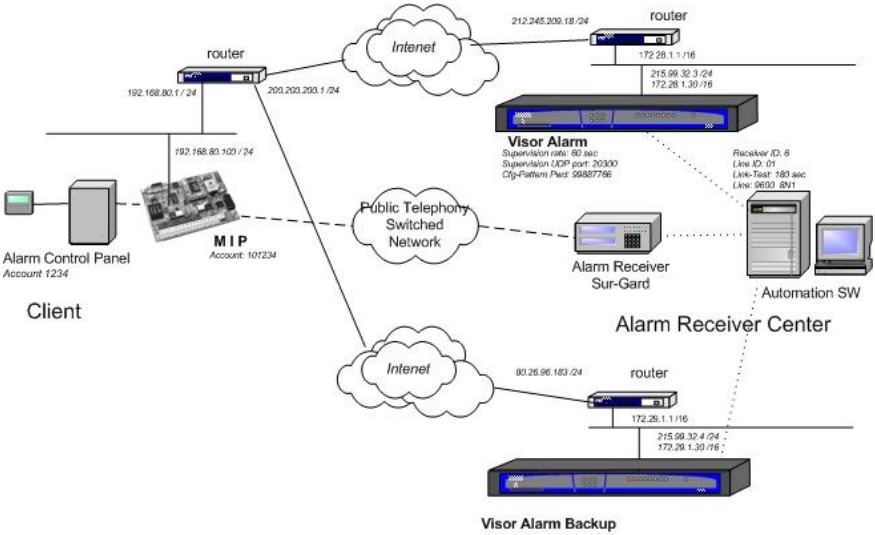


Figure 3. Network backup function scenario.

I - 1.2. Operation Mode

The IP Module (IPDACT) connected to the client control panel carries out two tasks: sending alarms from the panel and monitoring the connection with the IP receiver. The network backup option has implications in connection monitoring. The alarms reception center is composed of two **VisorALARM** devices, one main and the other backup. The IPDACTs release 2.2 onwards has had their monitoring procedures modified in order to contemplate the presence of two devices in the central.

I - 1.2.1. Monitoring

The IPDACT is a device that intercepts the control panel telephone connection with two aims: firstly to detect when the panel sends an alarm in order to capture it and retransmit over the connected IP network and secondly to allow the telephone line to be used at the same time as sending alarms.

The interception of the telephone line takes place ONLY in cases where connectivity with either of the Teldat **VisorALARM** devices has been verified. The IPDACT-**VisorALARM** connectivity is checked through a traffic monitor which the IPDACT periodically sends and to which the main Teldat **VisorALARM** responds. (Through configuration, the main **VisorALARM** IP

address is given to the IPDACT and is the primary communication option. The backup **VisorALARM** IP address is also configured and is used in cases where the main device fails). If the exchange of messages does not occur during the configured time, the IPDACT tries to resend. If, after a configurable number of attempts, a satisfactory response is not received, the connectivity with the main **VisorALARM** is presumed lost. At this point the IPDACT tries to communicate with the backup **VisorALARM**, to which it will now try and send the alarms, polls, etc. In cases where communication with this second device also fails, the telephone line access is returned to the control panel as if the IPDACT was not present. From this point on, the IPDACT will try to re-establish communications both with the main Teldat **VisorALARM** and the backup, communication with the main device taking priority. The moment communications are reestablished with either of the two ARC devices, the IPDACT intercepts the telephone line once more.

The supervision traffic is encrypted UDP. The Ethernet frame size does not exceed 70 bytes. The monitoring interval, the number of retries and time between retries are all configurable, and are values that must be carefully considered. Normally the monitoring interval in the control panel is high as this implies a telephone call. However, in the case of IPDACT, this cost is irrelevant as it is dealing with traffic which in all likeliness is running over a flat rate connection. In addition, a high value here is not advisable in cases where the IPDACT connects to Internet through a router executing NAT, a very probable situation. This is because traffic coming from the ARC towards the IPDACT reaches this thanks to the router maintaining the entry in the NAT table active during a period of time, the entry being refreshed with supervision traffic. If the supervision interval is greater than the residence time for the entry in the NAT table, communications from the ARC will not be possible. There is no rule to say how long an entry in the NAT table must last for. In cases of the TELDAT devices, this is around 5 minutes. A low value has the problem that the traffic the **VisorALARM** must process is high, the same as the bandwidth requirements. If ARC Internet access is ADSL, you need to consider that the upstream channel is smaller than the downstream one and that supervision traffic returned to the IPDACTs is slighter larger than the incoming.

The incoming traffic to the ARC is:

$$C = 528 * T_{KEEP-ALIVE} * N_{mips}$$

The minimum supervision time can be 1 second and a VisorALARM can have 3000 IPDACTs registered that give an input traffic of 1,58 Mbps. The return traffic is approximately 6% larger.

The Teldat **VisorALARM** received monitoring messages from the IPDACTs. If these are registered, they are assumed alive and an acknowledgement response is sent to them; if the IPDACTs are not registered, they are ignored. Periodically the status of all the registered IPDACTs is checked and all those which have not notified their availability (i.e. those which have not responded

since the last check) an alarm is generated. This is a 350 code alarm from the Contact-ID protocol (*Communication trouble*) which is received in SwAut.

In order to prevent the Teldat **VisorALARM** from sending hundreds or thousands of communication failure alarms when faced with a situation of general failure of IP traffic reception, the device itself monitors the network access through echo ICMP packets (ping) to a known address: if the echo ICMP packets (ping) towards this address fail then a code 356 alarm is generated from the Contact-ID protocol (*Loss of central polling*).

Apart from the above codes, the **VisorALARM** also generates others related to network backup. For further information on this, please see manual Dm 298-I "VisorALARM Installation Manual".

I - 1.2.2. Alarm sending

When the IPDACT has connectivity with the Teldat **VisorALARM**, the former intercepts the telephone line and processes all the incoming and outgoing calls taking place.

The supported alarm sending protocol is Contact-ID. This format sends alarms through DTMF digits complying with the following format:

AAAA MM QEEE GG CCC S

where *AAA* is the client number, *MM* the type of message, *Q* an event qualifier, *EEE* the type of alarm, *GG* the group or partition number, *CCC* the zone number and lastly *S* is the frame validation digit.

When the panel opens to send an alarm, the IPDACT provides power and emits the dialing tone. When the control panel dials the alarm center telephone number, it issues the Contact-ID *handshake* and receives the alarm frame. From this point, the IPDACT sends this alarm to the **VisorALARM**.

The control panel is not given the frame sent acknowledgement (*kissoff*) until the said acknowledgement is received from the Teldat **VisorALARM**. If the IPDACT does not receive the acknowledgement within 2 seconds, this carries on resending a configured number of times after which connection with the Teldat **VisorALARM** is assumed lost and the control panel sends the alarm over the telephone line. From this point, the IPDACT tries to re-establish communication with the **VisorALARM** as previously described. In cases where the network backup functionality is operative, a failure in sending an alarm to the main **VisorALARM** changes into an attempt to establish communications with the backup **VisorALARM** and to send the alarms to this second device. If this attempt also fails, then the control panel takes over the process of sending the alarms.

It's essential that the total time, in which the IPDACT deactivates in cases where communications fail with both the IP receivers, is greater than the control panel's highest retry time.

The IP **VisorALARM** receiver on receiving an alarm from an IPDACT stores this in a non-volatile internal memory. When the operation has successfully

finished, it sends the acknowledgement to the IPDACT originating the alarm so that in turn this is sent to the associated control panel. If the alarm storage memory cannot store the alarm, no acknowledgement is given.

As regards the SwAut, the Teldat **VisorALARM** behaves as an alarm receiver that sends alarms received through a serial port. The Teldat **VisorALARM** can emulate a Sur-Gard, an Ademco 685 or a Radionics 6500 receiver. The serial line parameters are configurable as well as those relative to the emulated receiver (link-test, receiver and line identifier, start and end frame characters, etc.)

I - 1.3. Additional features

In order to simplify installation and updating of the registered IPDACTs, the IP **VisorALARM** receiver has additional facilities.

To install new IPDACTs, the Teldat **VisorALARM** possesses configuration patterns associated to installer passwords. These permit you to automatically register new IPDACTs in the supported IPDACT list and at the same time enable the IPDACT to request the necessary configuration for start up. The device can simultaneously have multiple patterns; the choice of one or other depends on the installer password used in the IPDACT to request the service.

In order to maintain and update the registered IPDACTs base, the Teldat **VisorALARM** has commands available to remotely update one or multiple configuration parameters used by the IPDACTs.

Additionally, in order to simplify the IP parameters configuration, something that is not always easy, the IPDACT has a DHCP client program, release 2 onwards, which attempts to automatically obtain all the IP connectivity information (address, mask and gateway) on startup. To do this, you need to have a DHCP server in the local network. If the IPDACT does not automatically obtain the IP address, use the parameters that have been statically configured, permitting you to make sure that the device operates even when the said server is down. From release 2.2 onwards, the DHCP client can be deactivated.

With the aim of adding to point 38.1.5 on UL864, the IPDACT allows trouble signaling to be sent to a maintenance **VisorALARM** receiver, which is a different device from the main and backup **VisorALARM**s. **The IPDACT does not discriminate between sending to one receiver or another depending on the type of signal (alarm or trouble), but sends the same signal to both the operating receiver and to the maintenance receiver**. It is the receiver's task to filter the signals to be sent to the automation software.

Receivers that can be configured as maintenance are those containing firmware version 10.5.16 and superior. These receivers are characterized as they do not execute IPDACTs supervision functions, nor carry out any remote operations over the IPDACTs, nor do they admit IPDACT registration. These are repeat alarms coming from the IPDACTs and simply filter the signals, sending only the required signals to the automation software.

II - Chapter.
IPDACT Description

II - 1. General Description

The figure displayed below, represents the IPDACT hardware.

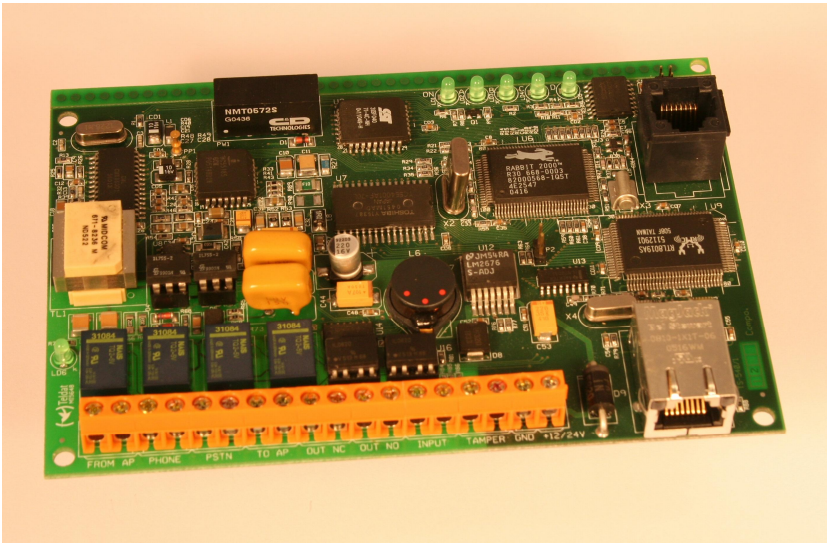


Figure 4. IPDACT

The hardware version and release is identified through its board number which is TS-540/X where X is the release number.

The following figure shows the identifier details and how to locate it.

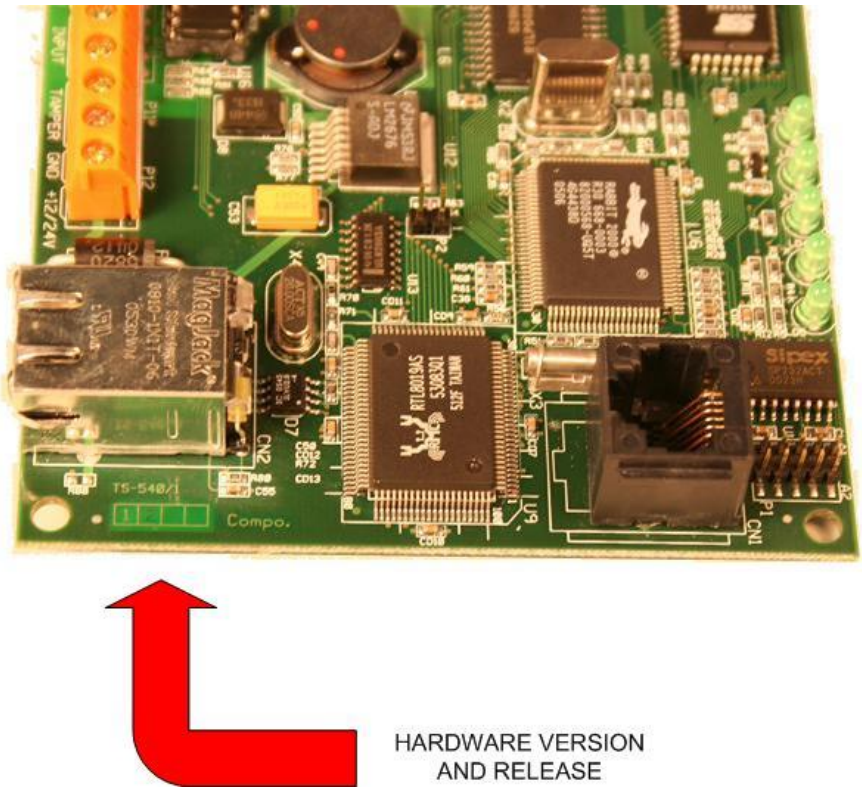


Figure 5. Board identification details

The IPDACT basically consists of two elements: the control module and the telephonic module.

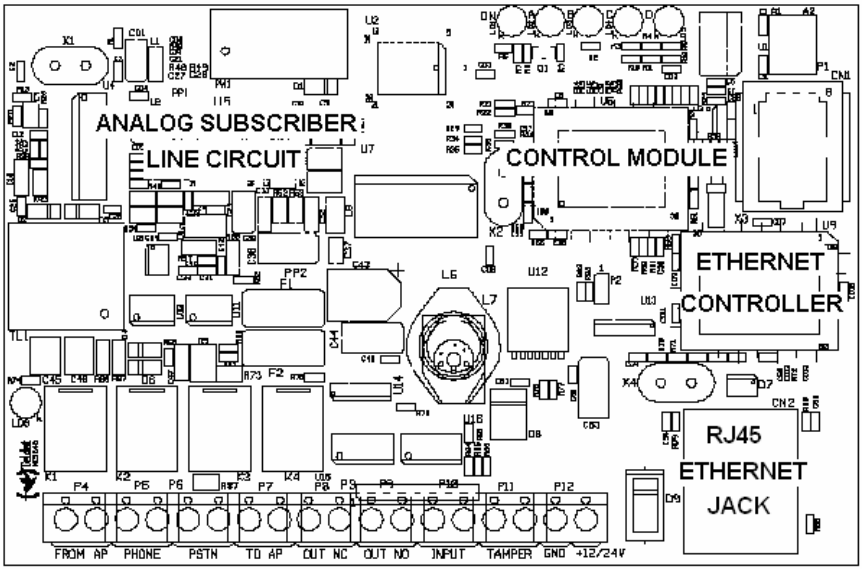


Figure 6. IPDACT circuit details.

The device CPU, memory and the LAN (identifiable through the RJ-45 connector) are found in the control module. This manages all the information procedure and the sending of the information through an IP network over the LAN.

The telephonic module physically supports the control and contains all the connection points with the control panel. This manages the entire telephonic interface with the control panel and the client telephone network (public telephone network termination point and client phone wiring).

From a configuration / monitoring point of view, the IPDACT possesses LEDs that permit you to view the status of the various elements, from the P2 jumper to control various aspects and a telephonic console. This telephonic console is accessible from the connection to the control panel (TO-AP) and requires an analog telephone with tone dialing.

The IPDACT has an asynchronous console which permits you to monitor / configure the device through an asynchronous terminal.

II - 2. LEDs

The IPDACT has three groups of LEDs that provide information on the status of each type. These are displayed in the following figures:

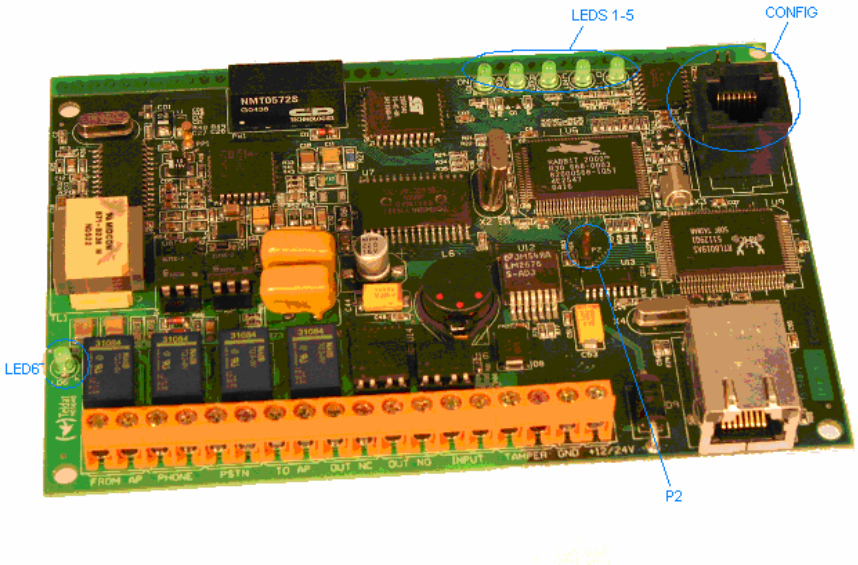


Figure 7. LEDs and pins for a IPDACT

The LED labeled “ON” (LD1 for all the versions and releases) is green and indicates that the IPDACT is powered.

Line status LED: Next to the relays there is a LED labeled LD6. In green this indicates that the telephone relays are active i.e. the IPDACT intercepts the telephone line. In normal working mode, this only occurs when the IPDACT has connectivity with the configured **VisorALARM**. The relays also activate when the telephone console activates (please see section IV.2 for further information). When the control panel is executing maintenance tasks due to a bi-directional call, the relays are inactive.

LEDs LD2, LD3, LD4 and LD 5 each have an independent connotation:

- LED A LD2: Supervision information.

ON: a management frame is sent to the **VisorALARM** (*contact* or *keep-alive*).

OFF: a response is received to the sent management frame. If there is no response, this remains active, indicating the lack of connectivity with the **VisorALARM**.

- LED B LD3: TO-AP terminal status

ON: the alarms panel telephone line is off hook.

OFF: the alarms panel telephone line is on hook.

- LED C LD4: alarm sending to the **VisorALARM**.

ON: an alarm has been sent to the **VisorALARM**.

OFF: a response has been received to the sent alarm.

- LED D LD5: a bi-directional call to the alarm panel is in progress.

ON: there is a bi-directional call to the alarm panel. The LED located next to the relays is off as the alarm panel has directly accessed the telephone line.

OFF: no bi-directional call in progress. The panel is operating normally.

II - 3. Jumper

The bridge labeled P2 operates by short-circuiting both pins through a metallic element such as a screwdriver or a clip. This permits two tasks:

a) On device startup this permits you to configure the IPDACT with the default configuration. For further information on how to activate the default configuration, please see section IV.2.1.1.

b) Access the telephonic console. This permits you to configure / monitor the IPDACT through a telephone connected to the said IPDACT. For further information, please see section IV.2.

II - 4. Connection points to the Control Panel and external

In order to connect the IPDACT to the control panel and to power this, there is a row of choc blocks. All the connections are limited in power. As can be seen in the following figure, the connections are grouped in the following manner:

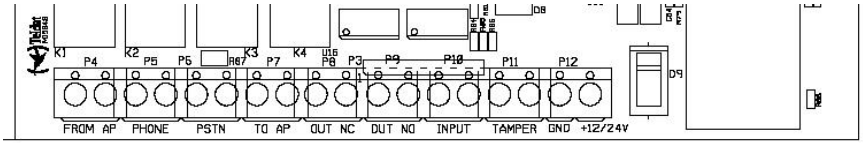


Figure 8. Connection choc block

Choc block connection to the control panel

- TO-AP: terminals proving telephonic connection to the control panel. This must be connected to the control panel connection which this is using to access the PSTN.
- FROM-AP: terminals receiving telephonic connection from the control panel. This must be connected to the control panel connection which this uses to provide a line to the subscriber numbers.

Choc block connection to the Public Switched Telephone Network

- PSTN: access terminals to the public switched telephone network. This connection is supervised. In cases where there is a failure, the analog output activates.

Choc block connection to the client telephone numbers

- PHONE: terminals providing telephonic connection to the telephone numbers possessed by the client at home or at installations.

Choc block associated to the analog output control

- OUT NC: terminals whose state is normally short-circuited. On activating the output, these terminals stop being short-circuited. Short circuit is carried out through an electric-mechanical relay. The technical data for this can be found in appendix V.3.
- OUT NO: terminals whose state is normal open. On activating the output these terminals pass to a short circuit state. Short circuit is carried out through an electric-mechanical relay. The technical data for this can be found in appendix V. 3.

This output is also related to the input status of the PSTN and LAN and with the IP connectivity status with the alarms reception center. When there is IP connectivity, the OUT NO terminals will be in their normal state i.e. open. If there is a failure in IP connectivity, then these terminals pass to a closed state.

Choc block associated to an analog input

- INPUT: terminals associated to the input. This input is supervised and considered inactive when a 1K ohms resistance is detected between its ends. When an open circuit is detected, the device, which should be connected to this input, is regarded as having been disconnected i.e. it has been sabotaged.

In UL compliance installations, this input should not be used and must be bridged with a 1K resistance.

Tamper Chock Blocks

- TAMPER: An additional input connecting to a box tamper which indicates if the box is open. The input is normally closed.

Choc block power connections

+12/24V: It is possible to power the unit at either 12 or 24 volts. For UL Listed Installations, the power source is regulated, limited in power and UL compliant.

- GND: power ground terminal.

II - 5. LAN

The device connects to the LAN through an RJ45 (CN1) connector.

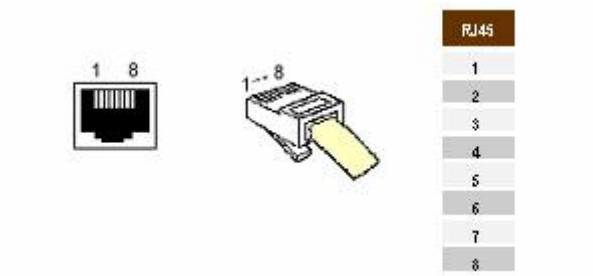


Figure 9. LAN Connector and cable.

Failure detection in the Ethernet interface is indicated by the analog output activating.

II - 6. Console

An asynchronous console is available for configuration / monitoring tasks.

The IPDACT has a black RJ45 connected labeled CNI for console connection. Consequently you will need a DB9 to RJ45 converter for the said connection which is provided by Fire-Lite. The following figures show both the converter and the connector respectively.

Figure 10. DB9-RJ45 converter for the console connection

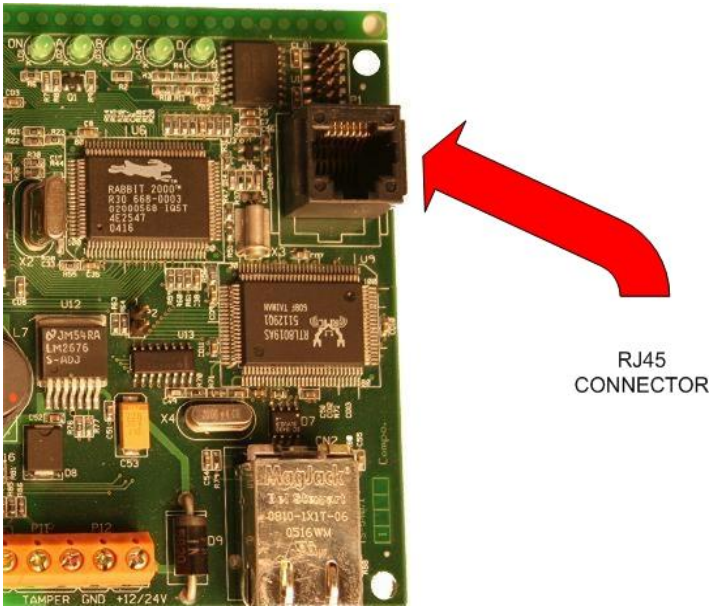
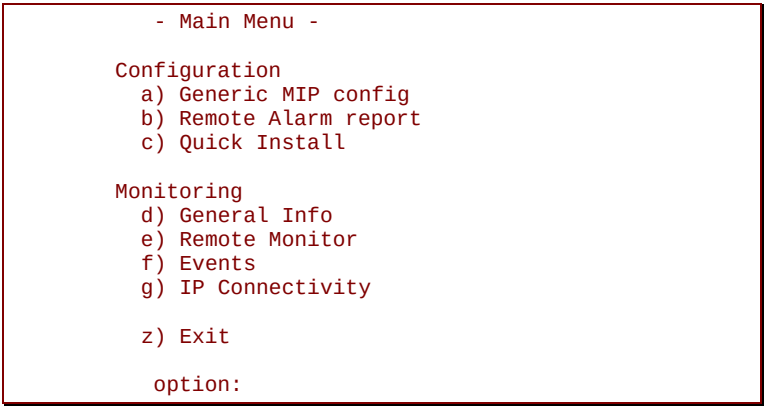


Figure 11. Console connector details

The access configuration is 9600 8N1 (8 bits, without parity, 1 stop bit).

The environment is a simple one orientated to menus. The main menu is displayed in the following figure.



III - Chapter. Installation and cabling

III - 1. Installation

The IPDACT device is designed to connect a conventional control panel, which uses the telephone network to transmit alarms, to an IP network. The module can be connected to a wide variety of panels although only the panels given in the list in the appendix V.2 should be used for UL compliant installations.

The IPDACT is installed in a separate box from the panel.

The box is shown in the following figure:

Figure 12. IPDACT Box.

The placement of the IPDACT within the box is as follows:

Figure 13. Box with IPDACT.

The following diagram shows the IPDACT installation within the box:

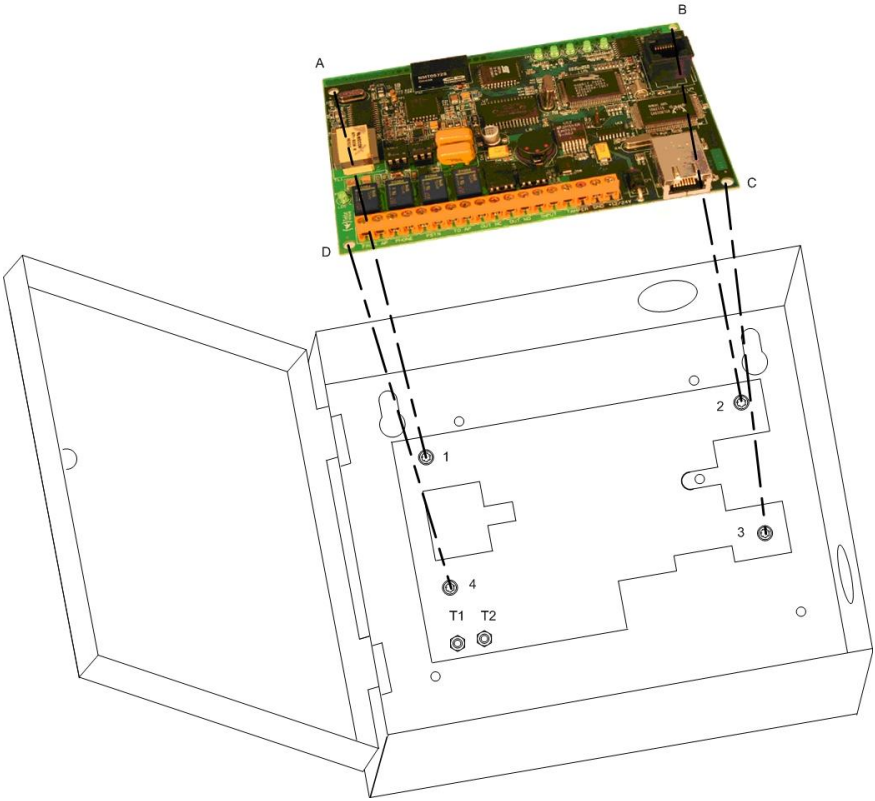


Figure 14. IPDACT installation in the box.

III - 1.1. Assembly Instructions for the IPDACT box

The instructions in order to assemble the IPDACT in its box are as follows:

1. Attach the box to the wall; the maximum distance this can be from the control panel is 6.1 meters (twenty feet).
2. Remove screws 1, 2, 3 and 4.
3. Place the IPDACT board so orifices A, B, C and D coincide with the bolts.
4. Insert the four bolts into the orifices and slowly tighten them until the board is firmly attached to the box.
5. The box has two ground connections (T1 and T2).
6. Connect the T1 earthed ground to the panel earth using an AWG 14 cable.
7. The stamped openings available in the box permit wiring to both enter and exit the box through conduits. Please remember that in

cases of UL listed fire installations (UL864) the conduits must be able to bear any attempts of mechanical injury.

8. The power cables +12V/+24V and GND, from the TO-AP and FROM-AP telephone, the OUT-NO and the cable connected to the box earthed ground (T1) leave through an opening and are fed through a conduit in order to reach the panel.
9. The PSTN and PHONE telephone wires can also enter through the opening indicated in point 9, if the said cables come from the panel.
10. The Ethernet cable can also enter through the opening indicated in point 9 if it comes from the panel. The Ethernet cable must be a CAT 5.

III - 2. Wiring

III - 2.1. Wiring for UL Listed Fire Installations

III - 2.1.1. Installation scheme

The IP module can be used in UL Listed fire installations provided that any of the fire panels, listed in the appendix, section V.2, are used and the following mandatory assembly is carried out:

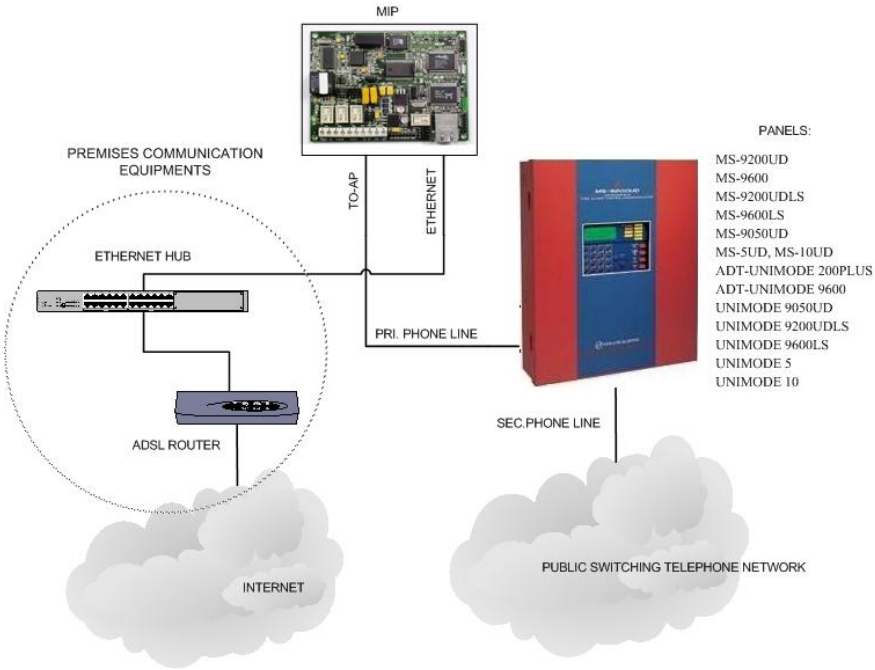


Figure 18. Installing an IP Modem with the fire alarm panels.

The IPDACT box must be placed to one side of the control panel. The conduit carrying the wires between the IPDACT and the panel must be horizontally placed.

So that it is unnecessary to supervise the wiring between the IPDACT box and the Control Panel, the following must be fulfilled:

The circuit connections extended to additional fire alarm control unit equipment when these wiring connections are intended to be made within 20 feet (6.1 m) of each other and are enclosed within conduit or equivalently protected against mechanical injury.

Wiring not connected to the panel, and therefore does not have to be where the IPDACT and the panel are installed, is supervised. This refers to PSTN lines and Ethernet.

The electrical installation must comply with the NFPA-72 norm, appropriately adjusted for each installation.

The IPDACT wiring is limited in power. Therefore all the wiring between the IPDACT box and the panel can be enclosed in the same metal conduit.

III - 2.1.2. Installation instructions

The following instructions are specific to wiring between the IPDACT and the Firelite MS-9200UD panel. For any other panel, please consult the manufacturers' documentation and instructions.

- Before carrying out any type of operation on the wiring, make sure you have disconnected all power sources.
- In these installations the IPDACT must be integrated in its box. Connect the IPDACT box ground to the same ground point where you have connected the panel ground. This is to prevent current traveling through grounded circuits. Grounding is essential to avoid unwanted electrostatics discharges.

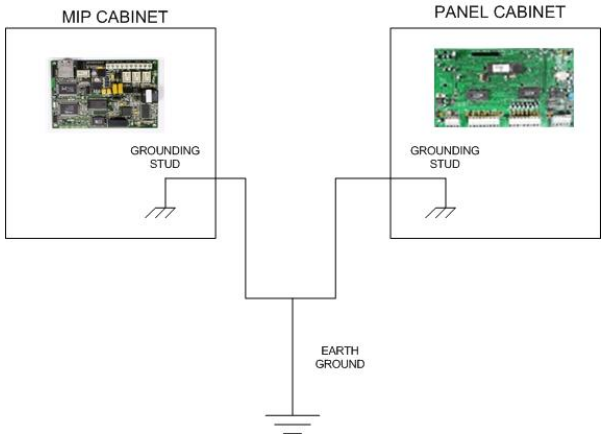


Figure 19. Earth ground for the IPDACT and panel boxes.

- Connect the IPDACT power inputs to the panel TB1 connector, terminals 1 and 2. These terminals can be configured as *resettable* or *non-resettable* power. The latter implies an uninterrupted power source from the panel and is the one we recommend.

  The IPDACT GND terminal is not connected to the box earth ground.

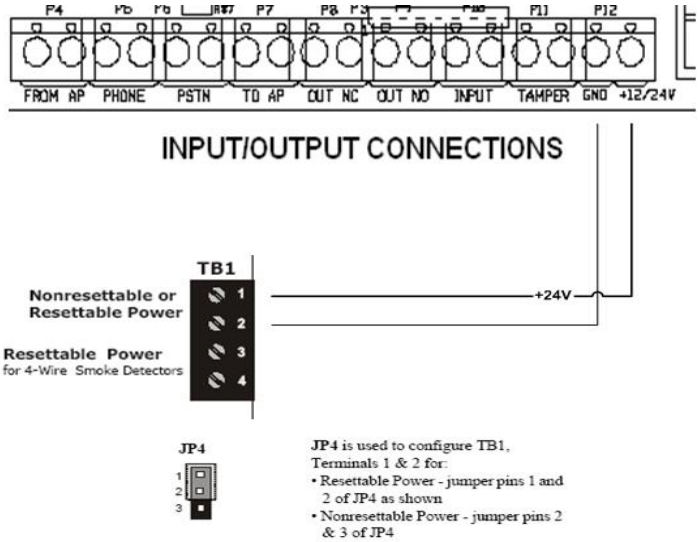


Figure 20. Power connection.

Due to FCC requirements, ferrites must be used for power lines. This is to avoid electromagnetic interferences being conducted to inside the devices.

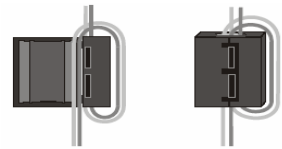


Figure 21. Ferrites for power cables.

- The fire panel has two telephone lines in order to send alarm. One is the main line and the other the backup. The main line, *PRI. PHONE LINE*, is connected to the IPDACT TO-AP output. The secondary line is connected to the client telephone connection.

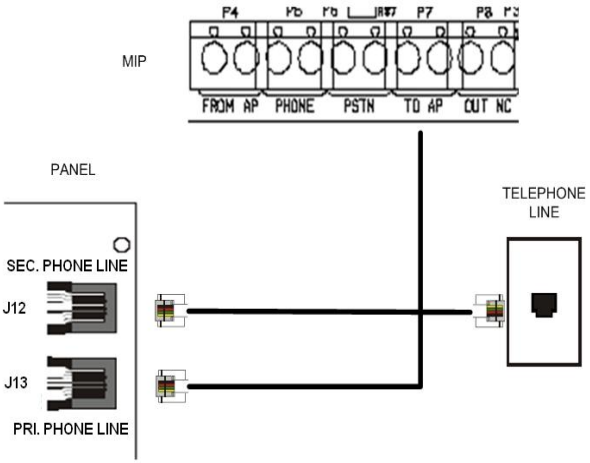


Figure 22. IPDACT-panel MS-9200UD telephone connection.

The following figure shows the connection between the IPDACT and the main telephone line in greater detail.

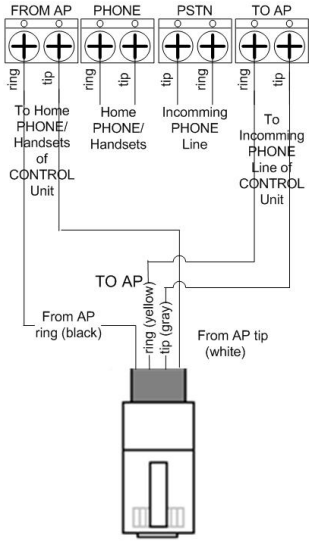


Figure 23. IPDACT Connection. Main telephone line.

- Do not connect any telephone connection to the PSTN input. To prevent the IPDACT from executing any of the anticipated actions

when this detects a line supervision failure, configure the IPDACT to take no actions whatsoever.

The panel's *PRI. PHONE LINE* has converted into an IP line. All alarms sent over the *PRI. PHONE LINE* are captured and transmitted over the IP network.

- If the IP line supervision detects connectivity failure, the IPDACT switches its relays so the PSTN input connects to the TO-AP output i.e. connects the telephone network to the panel's *PRI. PHONE LINE* input. However given that the PSTN input is not operative, there isn't a line. Nor is there a telephone line to the panel's *PRI. PHONE LINE* input. This situation provokes an alarm in the panel, which is then sent to the central. This is how the panel detects IP connectivity failure.
- Apart from the IPDACT supervising the IP line, the control panel must, in order to comply with the UL, have receiver supervision functionality configured. The IPDACT treats the supervision as an attempt to send a signal.
- The user installations will have telecommunication devices which allow the IP module to reach Internet.

For UL Listed Fire Installations, shared on-premises communications equipment is required to be UL Listed for Information Technology Equipment.

IV - Chapter. Configuration

IV - 1. Configuration modes

The IPDACT can be configured both locally and remotely.

1. Locally:
    a. Telephone console: through a normal analog telephone connected to the TO-AP labeled choc blocks.
    b. Asynchronous console: from a PC with terminal emulated and a cable for this.
2. Remotely:
    a. From the **VisorALARM** IP receiver: through a register operation carried out by the IPDACT installer or through 'update' commands from the **VisorALARM** console.
    b. From a telnet session: from the IPDACT software release 2, the remote configuration can also be carried out through a telnet session to the IPDACT IP address, provided that the said IP address is available (if this is in the same LAN for example). In cases of a telnet session, the given interface is identical to the asynchronous console interface.
    c. Through DHCP: this is also from release 2, the parameters for the IP address, IP mask and gateway can by dynamically obtained from a DHCP server that is located in the same local network as the IPDACT. From release 2.2 onwards, the DHCP client can be disabled.

The following sections will show each of the above methods in more detail.

Accessing the device configuration, both for telephone and serial port, always requires an access password.

IV - 2. DHCP

DHCP stands for "*Dynamic Host Configuration Protocol*". DHCP is an Internet protocol used to automate the configuration of devices using the TCP/IP

protocol stack. DHCP can be used to automatically assign IP addresses and other TCP/IP configuration parameters such as the network mask and the default router (or gateway) among others.

In the IPDACT environment, this is used to automatically obtain the IP communication parameters (IPDACT IP address, network mask and gateway), simplifying the device installation process.

So this runs correctly, you need to have a DHCP server correctly configured in the local network where the IPDACT is connected. Normally the access routers (in ADSL for example) have the possibility to act as a DHCP server, therefore in these environments, start up is immediate.

The IPDACT functioning mode is as follows: when the device boots up, it tries to dynamically obtain the IP configuration from any DHCP server which is in the network. If this is achieved, it activates the said configuration and displays a message on the console.

```
Teldat      (c)2003

Config file... read
Trying to get DHCP lease...Lease obtained
```

Address assignment in the DHCP protocol is defined so that this can be permanent or expire after a certain period of time (configurable in the DHCP server). If the assignment is permanent, the IPDACT will not renew the address until the next time it is rebooted. Contrariwise, before the validity of the address times out, the IPDACT will automatically request the server to renew the assignment.

If during the first attempt (or during the renewal attempt) the IPDACT cannot get the IP address from a DHCP server, and with the aim of not leaving the device without IP connectivity, the device will use the IP parameters which have been statically configured in the device console and will operate with these parameters until the next time the IPDACT is restarted. Therefore, if you need to force to IPDACT to renegotiate an address, you will need to reboot.

The following message is displayed by the IPDACT on console if it cannot obtain an assignment through DHCP.

```
Teldat      (c)2003

Config file... read
Trying to get DHCP lease...Lease not obtained.
DHCP server may be down.
Using static IP configuration.
```

From release 2.2 onwards, the DHCP client can be enabled/disabled. In the previous releases this was always operating. In the default configuration it is

enabled. To enable/disable the client, enter the IPDACT generic configuration:

```
            -- Generic MIP config --

        IP Connectivity
          a) DHCP client: OFF
          b) IP addr: 192.168.0.202  msk: 255.255.255.0
          c) Gateway IP: 192.168.0.250

        User Access Control
          d) Password: 1234

        Miscellaneous
          e) Date & time: 01/16/1980 17:37:28
          f) Events: PHON RMON CID RALA RCFG
          g) PC verifying digit: OFF

          z) Exit

           option:
```

In the DHCP client section, you can configure the client as enabled/disabled.

```
option: a
 DHCP client: (0:OFF - 1:ON)
```

IV - 3. Telephonic Console

In order to use the telephonic console, a normal analog telephone connected to the choc blocks labeled TO-AP is required. This telephone must be configured to dial through tones. These choc blocks are used to connect the IPDACT to the control panel consequently the telephonic console is not always available and it's necessary to activate it.

To activate the telephonic console, short circuit the P1 jumper in board versions up to 4 and P2 in board version 5, for a little more than a second with some metallic element. You can use a small screwdriver or a simple clip. During this process the telephone must be on hook. On activating the console, if the telephone relays are inactive (line status LED off), they activate (i.e. the LED lights up); if they are already active, they will briefly deactivate to indicate that the telephonic console is available.

On picking up the phone, you will hear an intermittent tone which requires you to introduce an access password. In order to introduce the password, you need to press "**#" (asterisk, asterisk, pad) and the access password. By default the access password is **24680**. If this is correct, you will hear three

beeps (the OK signal) and subsequently the telephonic console dialing tone (a continuous low frequency tone). You have 4 or 5 seconds for this process after which you return to the initial situation; if the relays are inactive, you also return to the start. If the password is incorrect, the telephonic console will automatically deactivate and return to the initial position; if the relays are inactive then you return to the initial position.

If at any point you hang up the phone, the telephonic console deactivates.

IV - 3.1. Configuration

Configuring the various parameters is carried out through the access and register writing. A register is used for each parameter to be configured. Each register is made up of one or various fields. The number of fields and size of each depends on the type of register. All the fields pertaining to one register have the same size. In order to access a register, press * and the two digits corresponding to the register to be configured. After selecting a register you will hear a simple beep indicating that this register can be configured. From this point you can configure the first field in the register. Should you select an invalid register, an error signal is emitted. This consists of a long tone.

The access process for a register can be terminated at any point using the escape sequence *# (asterisk, pad). In this case an escape signal is emitted which consists of three short tones.

The available configuration registers are as follows:

Types of register	register	fields	Field size	Default value
IPDACT IP address and mask	01	8	(3+1)	192.168.000.100 255.255.255.000
IPDACT access gateway	02	4	(3+1)	192.168.000.200
Access password for the console	03	2	Variable, max. 16 characters, these must be the same.	24680
Remote configuration request	04	1	Variable	None
IPDACT Reset	05	1	Variable	N/A
IPDACT account number	11	1	(6+1)	000000
Visor Alarm IP address	12	4	(3+1)	None
UDP port	13	1	(5+1)	00080
IPDACT message encryption key	14	2	Variable, max. 16 characters, these must be the same.	None
VisorAlarm message encryption key	15	2	Variable, max. 16 characters, these must be the same.	None
Interval between *keep-alive* (sec)	16	1	(5+1)	00010
Retries after failed *keep-alive*	17	1	(1+1)	3
Time between retries for sending *keep-alives* (sec).	18	1	(1+1)	3

Number of digits for a telephone number.	19	1	(2+1)	09
Retries for sending an alarm	20	1	(1+1)	5
Backup VisorALARM IP address	21	8	(3+1)	None
Interval between *keep-alives* (seconds) with the backup VisorALARM	22	1	(5+1)	00010
Retries after failed *keep-alives* with the backup VisorALARM	23	1	(1+1)	3
Time between retries for *keep-alive* sendings (seconds) with the backup VisorALARM	24	1	(1+1)	1
DHCP Client activation / deactivation	27	1	(1+1)	1
Output relay switch time	28	1	(3+1)	0
Action to take when the telephone line fails	29	1	(1+1)	2 (Alarm sending)
Maintenance VisorALARM address	36	4	(3 +1)	None
Key to encrypt packets sent to the maintenance receiver.	37	2	Variable, max. 16 characters, these must be equal	None
Installation key for remote configuration automatic request	38	2	Variable, max. 16 characters, these must be equal	None
Use of the checking digits	49	1	(1+1)	1

Through the syntax (n+1) this indicates that n is the number of significant digits and with +1 this indicates that the last figure is the checking digit depending on the data. This is done as such to prevent errors when configuring the device and to reduce the time required for the process. The passwords are verified through repetition. The checking digit is obtained through the MIPDATA.exe program in the PC which supplies the data to be configured. This characteristic enabled and disabled through register 49.

A register's fields are configured by entering the number of data required and finally # (pad). If the number of digits is incorrect or the data invalid, an error signal composed of a long tone is emitted. At this point you must wait to repeat the value for the said field. If the data is correct an acknowledgement signal made up of two short tones is emitted and subsequently you move on to the next field. If this is the last field, all the fields are stored in the configuration and an OK signal made up of three short beeps is emitted. At this point, the dialing tone is emitted in order to dial the telephonic console (continuous low frequency tone).

In some cases it may be necessary to enter A, B, C, D, E or F. These digits can be obtained through the key sequence * and a number between 1 and 6. I.e. digit A is obtained through * 1, B through * 2, and so on.

Configuration changes are dynamic, i.e. you do not need to restart the device to activate the said changes.

IV - 3.1.1. Default Configuration

Through a short circuit in the IPDACT P2 jumper during the start up process, you can configure the IPDACT with the factory settings. This configuration is displayed in the previous table.

The process for this is as follows: 1) switch off the IPDACT, 2) short circuit the P2 jumper, 3) switch on the device, 4) maintain the P2 short circuited during the first burst from LEDs A, B, C and D (they light up and switch off consecutively) and open it half way through the second burst. If the process has executed successfully, the IPDACT will display a third burst indicating the default configuration has been activated.

IV - 3.1.2. Register description

IPDACT IP address and mask

IP address and mask associated to the IPDACT in order to operate in the client's local network. From IPDACT software release 2.0 onwards, this parameter is only necessary in cases where you do not have a DHCP server or as a backup configuration in cases where the said DHCP server is down.

The register is made up of 8 fields; both the IP address as well as the mask is composed of 4 numbers between 0 and 255. Each number has a verification digit. This contains the following value by default:

192	168	000	100	255	255	255	000

IPDACT access Gateway

IP address associated to the access gateway in the client local network. This gateway gathers all the traffic from the IPDACT and ensures that it reaches the next hop to the Teldat VisorALARM. From IPDACT software release 2.0 onwards, this parameter is only necessary in cases where you do not have a DHCP server or as a backup configuration in cases where the said DHCP server is down.

The register is made up of 4 fields corresponding to the 4 numbers in the IP address; this admits values between 0 and 255. Each number has a verification digit. This contains the following value by default:

192	168	000	200

Access password for the console

Access password for the telephonic console which prevents unauthorized access. This is also used to verify some operations. This must be entered twice in order to validate it.

The register is made up of one field with up to 16 digits. The default value is 24680.

The password field cannot be left empty.

Remote configuration request

This permits you to prompt the Teldat **VisorALARM** for the complete configuration required by the IPDACT in order to function. This register does not require you to configure any parameters and is limited to simply execute a request. In order to do this, you require the installer password.

The configuration the IPDACT receives has been configured in the **VisorALARM** through a profile. The parameters common to a set of IPDACTs are in the said profile.

The register mechanism permits you to quickly configure a set of IPDACTs with common parameters. Only those parameters which uniquely identify an IPDACT must be configured by the installer: account number, local IP parameters, output switch and actions to take should the PSTN fail.

The register is composed of one field with up to 16 digits. By default this register is not configured with a value. Should you enter a value, it is not maintained between requests. For further information, please see section IV-2.1.3.

IPDACT Reset

Permits you to reset the IPDACT so that some parameters have validity. So that the operation is effective you need to provide the access password for the console.

The register is made up of a single field, corresponding to the access password. If the password is valid, the device will reset; should this be incorrect an error tone will be emitted followed by the console dialing tone. This register does not store any data in the IPDACT configuration.

IPDACT account number

Account number identifying the IPDACT to the IP Visor Alarm receiver and the security company's automation software. In order to simplify the identification process, we recommend that the last four figures in this parameter coincide with the account number assigned to the control panel to which this is designated.

The register is made up of one 6-digit field. The default value is 000000.

Teldat VisorALARM IP address

IP address for the IP **VisorALARM** receiver which receives both the monitoring traffic as well as the traffic corresponding to the alarms generated by the control panel.

The register is made up of 4 fields corresponding to the 4 numbers in the IP address; this admits values between 0 and 255. Each number has a verification digit. This contains the following value by default:

000	000	000	000

UDP Port

UDP port used to send and receive monitoring, alarms and remote configuration information. This port must coincide with that programmed in the IP VisorALARM receiver.

The register is composed of one 5-digit field which admits values within the range of 00000 to 65535. The field contains a verification digit of the configured number. Default value is 00080.

A 0 value is not permitted.

IPDACT message encryption key

This key is used to encrypt the messages sent to the Teldat VisorALARM. This must be entered twice in order to validate it.

The register is composed of one field containing up to 16 DTMF digits. By default there is no configured value.

VisorALARM message encryption key

The Teldat VisorALARM uses this key to encrypt the messages sent to the IPDACT. This must be entered twice in order to validate it.

The register is composed of one field containing up to 16 DTMF digits. By default there is no configured value.

Keep-Alive Interval (sec.) (KEEP_ALIVE_INTERVAL)

Time interval when the IPDACT executes a connectivity test with the Teldat **VisorALARM**. For this, a *keep-alive* frame is sent and a response is expected from the IP receiver.

The register is made up of one 5-digit field. The interval is expressed in seconds and admits values between 00000 and 90 seconds. The range of values this register can take comply with the UL1610 section 62.10. The field contains a verification digit for the number. Default value is 00010.

Retries after failed *keep-alive* (KEEP ALIVE RETRIES)

If the IPDACT, on executing the connectivity test with the Teldat **VisorALARM**, does not receive a response within the "*time-between-send-keep-alive-retries*" seconds, the IPDACT repeats the process of sending the *keep-alive* frame. Should there be no response within same time interval, the IPDACT repeats the process until the number of retries configured in the register has been completed. The connection with the Teldat **VisorALARM** is considered down once the number of configured retries in this register has been executed and subsequently the control panel can access the telephone network.

The register is made up of one single digit field. This admits values between 1 and 9. Default value is 3.

Time between send *keep-alive* retries (secs) (KEEP_ALIVE_RETRIES_TIME)

Time measured between sending of *keep-alive* frames when a possible connectivity problem has been detected with the IP **VisorALARM** receiver.

The register is made up of one single digit field. This is expressed in seconds and admits values between 3 and 9.

The field contains a verification digit for the number. Default value is 3.

UL listed installations comply with the following:

KEEP_ALIVE_INTERVAL + KEEP_ALIVE_RETRIES x KEEP_ALIVE_RETRIES_TIME < 25

Backup Teldat VisorALARM IP address

This is the IP address that the backup **VisorALARM** IP receiver has, which receives both monitoring traffic as well as traffic corresponding to the alarms generated by the control panel in cases where the main **VisorALARM** fails.

The register is made up of 4 fields, corresponding to the 4 numbers in the IP address; this admits values between 0 and 255. Each number has a verification digit for this. Default is:

000	000	000	000

Interval between backup *keep-alives* (seconds)

Time period where the IPDACT executes a check on connectivity with the backup Teldat **VisorALARM**. To do this, the IPDACT sends a keep-alive frame and waits for a response from the IP receiver.

The register is made up of a 5-digit field. The interval is expressed in seconds and admits values between 00000 and 90 seconds. The field contains one verification digit for the number. Default value is 00010.

Retries after failed *keep-alives* to backup

If the IPDACT, on checking connectivity with the backup Teldat **VisorALARM**, does not receive a response to this within "*interval-between-retries-to-send-keep-alives*" seconds, the IPDACT repeats the keep-alive sending process. If there is no response within the same time interval, the sending process is repeated and so on until the configured number of sending times in this register has been completed. After this number of configured retries, the connection with the Teldat **VisorALARM** is considered down and the control panel subsequently accesses the telephone network.

The register is made up of one 1-digit field. This admits values between 1 and 9. Default value is 3.

Interval between retries to send *keep-alives* (seconds) for the backup

Time interval between sending *keep-alive* frames when a possible connectivity problem with the backup **VisorALARM** IP receiver has been detected.

The register consists of one 1-digit field. This is expressed in seconds and admits values between 3 and 9.

This field contains one verification digit for the number. Default value is 3.

Number of digits for a telephone number

This is the number of digits containing the telephone number which the control panel must dial to carry out a call. Depending on the country, if there is a switchboard, etc.

This register is composed of one 2-digit field. Admits values between 1 and 15. The field contains a verification digit for the number. Default value is 9.

Alarm sending retries (ALARM RETRIES**)**

Number of times that the IPDACT sends an alarm to the Teldat **VisorALARM** to ensure that this receives the alarm and sends an acknowledgement to the IPDACT. Connection with the main IP receiver is considered lost once this number of retries has been completed, in which case the IPDACT is forced into backup and once again tries to send to the backup receiver. If the IPDACT doesn't succeed in communicating with the backup after all the retries have been executed, the telephone relays switch to allow the control panel to send the alarm over the telephone line.

The register is made up of one single digit field. This admits values between 5 y 10. The field contains a verification digit for the number. Default value is 5.

It is essential to consider what effect the number of alarm send retries parameter configured in the panel has. The first attempt from the panel activates alarm send through the IPDACT. If this fails, the panel does not need to try again in order to force the IPDACT to send the previous alarm to the backup **VisorALARM** as the IPDACT does this automatically. However, the panel is responsible for backup over the telephone line should there be IP connectivity failure, i.e. the number of retries must be high enough so once these have been completed with both the main and backup **VisorALARM**s, the panel takes over the process of sending the alarm over the telephone line.

This means that the time between the first and the last attempt by the panel to send an alarm must be greater than the number of alarm sending retries programmed in the IPDACT by 2 seconds (time between retries) and moreover twice, given that the same number of retries are executed with the backup **VisorALARM**. The time used in the rest of the operations carried out by the IPDACT is negligible as this can be counted in milliseconds.

DHCP Client activation/deactivation

The DHCP client is a device functionality permitting a DHCP server to assign an IP address and mask to the Ethernet interface plus an output gateway. The majority of the ADSL routers have a DHCP server so the IPDACT automatically configures and can connect to Internet through the router.

The registrar consists of a one-digit field which admits a value of 1 to activate the client and a value of 0 to deactivate it. The field contains a number verification digit. By default this is configured to 1 i.e. the client is activated.

Switch time for the output relay

The two output relays in the device (terminals OUT NO) have two complementary states, i.e. when the first is open the other one is closed. These states show device connectivity with the IP receiver (**VisorALARM**) so when the IPDACT loses connectivity the relay closes (the other stays open) remaining in this state while connectivity is lost. This behavior can be modified by introducing periodicity in the status of the relays, i.e. that this remains closed during a programmable period of time, open for a set time (2 seconds) and returning to the closed state. This behavior is maintained while there is no connectivity.

Switch time can take values between 0 and 300 seconds. A zero value means that the relay permanently remains in a closed position provided that the connectivity state does not change.

Action to execute when a telephone line failure occurs

The IPDACT supervises the telephone line so if a failure is detected, it can carry out three actions:

- Send an alarm to the **VisorALARM** (programmed value 2).
- Activate the output relay in the same way as if a communication failure had been detected (programmed value 1).
- Both of the above actions (programmed value 3).

The possibility of not doing anything at all exists together with the above actions (programmed value 0).

In UL listed fire installations, this value must be programmed to 0.

Maintenance VisorALARM address

Apart from the main **VisorALARM**s and the backups, you can send trouble alarms (300-388 CONTACT-ID group) to a third **VisorALARM** known as maintenance. This device does not have IP module registers, nor monitors its status and does not have backup. The main VisorALARMs and the backups execute those functions. The maintenance device only receives trouble alarms and resends them to the automation software.

The register is made up of four fields corresponding to the 4 numbers of the IP address; this admits values between 0 and 255. Each number has a verification digit. The default value is:

000	000	000	000

Alarm encryption key for the IPDACT to the maintenance receiver

This is the key used by the IPDACT to send alarms to the Teldat maintenance **VisorALARM**. So the configuration is valid, this must be repeated twice.

The registrar consists of one field with up to 16 DTMF digits. By default, no value is configured.

Installation key for remote configuration automatic request

This key is used to encrypt the remote configuration request packet. This manner of request is automatic, e.g., the IPDACT sends a request packet until a remote configuration was received from the VisorALARM+.

In the case of the installation key was empty the automatic request process will be terminated, if existed.

The register is composed of one field containing up to 16 DTMF digits. By default there is no configured value.

Using the testing digits

In order to increase the reliability of the telephonic console, some registers require an additional testing digit in each of their fields so that if the control digit does not adjust to the introduced value, the data is considered invalid and an error tone is emitted. This facility can be enabled or disabled through this register.

The register is made up of a single digit field which admits a value of 1 to activate the use of the testing digits and value 0 to deactivate. The fields contain a verification digit for the number. Default value is 0.

IV - 3.1.3. Minimum configuration for the installer

By using the configuration patterns in the Teldat **VisorALARM**, you can simplify the IPDACT installation process. So that the whole of the process is possible, it is essential that there is a configuration pattern configured in the **VisorALARM**. In the pattern, an installer password is associated to a given IPDACT configuration. This configuration includes the passwords through which information is exchanged between the IPDACT and the **VisorALARM**, monitoring time, etc.

The minimum configuration for an IPDACT which permits an installer to use this installation mechanism is as follows:

a) If you do not have a DHCP server

Type of register	Register

IPDACT IP address and mask	01
IPDACT access gateway	02
IPDACT account number	11
Main VisorAlarm IP address	12
Backup VisorAlarm IP Address	21
UDP Port	13

b) If you have a DHCP server

Type of register	Register
IPDACT account number	11
Main VisorAlarm IP address	12
Backup VisorAlarm IP Address	21
UDP Port	13

After configuring these parameters and restarting the device, the installer must re-access the telephonic console as previously described and access register 04. Here the installer password configured in the **VisorALARM** must be configured. If the IPDACT has IP connectivity with the **VisorALARM** and the password is correct, the IPDACT will receive the configuration defined in the profile configured in the **VisorALARM**.

Through this mechanism, the installed IPDACT is registered in the Teldat **VisorALARM** which from this point begins to monitor the former and the IPDACT receives the necessary configuration in order to exchange information with the Teldat **VisorALARM**.

If the whole process has gone smoothly, the IPDACT will begin to exchange monitoring messages with the VisorALARM and from this point onwards the IPDACT telephone relays activate (the line status LED lights up).

IV - 3.1.4. Configuration Example

In cases of configuring the IPDACT with the following data:

IP address: 192.168.1.100, mask 255.255.255.0

Access GW: 192.168.1.20

IPDACT account number: 1234

Main VisorAlarm IP: 10.24.6.1

Backup VisorAlarm IP: 80.6.189.123

UDP port: 3000

The registers and the data are, in cases where the testing digit is disabled (through register 49):

```
IP Address del IPDACT            *01 192# 168# 001# 100# 255# 255# 255# 000#
Gateway                        *02 192# 168# 001# 020#
CID                            *11 001234#
IP VisorAlarm principal        *12 010# 024# 006# 001#
IP VisorAlarm backup           *21 080# 036# 189# 123#
UDP Port                       *13 03000#
```

And in cases where the testing digit is enabled:

```
IP Address del IPDACT            *01
1928#1684#0018#1008#2550#2550#2550#0005#
Gateway                        *02 1928#1684#0018#0206#
CID                            *11 001234#
IP VisorAlarm principal        *12 010#024#006#001#
IP VisorAlarm backup           *21 0808#0368#1894#1238#
UDP Port                       *13 03000#
```

IV - 4. Asynchronous Console

You have the same access from the telephonic console as from the asynchronous console which also provides a better display of the processes taking place in the IPDACT. The console is orientated to menus whose options permit the monitoring and configuration of the various IPDACT parameters. The asynchronous console access parameters are 9600 bps, 8 bits, without parity, 1 stop bit. The console is password protected.

IV - 4.1. Accessing the console

The asynchronous console is protected by a user password. This password is the same as that configured in the telephonic console register 03. This is **24680** by default. Entering the valid password accesses the main menu.

```
Password:
```

IV - 4.2. Main Menu

This provides access to the configuration and monitoring menus. If you select an invalid option, the main menu is displayed once more. When configuring an option, if you press the ESC key, the operation is aborted and the parameter does not change. If you press INTRO in the parameters being handled as character strings, these are deleted. The z options releases the asynchronous console and requests the access password as described in the above section.

```
          - Main Menu -

       Configuration
         a) Generic MIP config
         b) Transmission Parameters
         c) Quick Install

       Monitoring
         d) General Info
         e) Remote Monitor
         f) Events
         g) IP Connectivity

         z) Exit

          option:
```

IV - 4.3. IPDACT generic configuration

Configures data pertaining to the IPDACT which is not related to the monitoring function and the sending of alarms. Data included here is the IPDACT IP address, the access gateway to the Teldat **VisorALARM**, the console access password, the events you wish to view, use of the check digit in the telephone console, etc.

In the following figure, the default values are displayed. Press z to return to the previous menu.

```
              -- Generic MIP config --

       IP Connectivity
         a) DHCP client: OFF
         b) IP addr: 192.168.0.100  msk: 255.255.255.0
         c) Gateway IP: 192.168.0.200

       User Access Control
         d) Password: 24680

       Miscellaneous
         e) Date & time: 06/16/2003 12:41:25
         f) Events: PHON
         g) PC verifying digit: 0

         z) Exit

          option:
```

IV - 4.4. Monitoring configuration and sending of alarms

Configures everything relative to the IPDACT as a security element. Permits you to configure the account number associated to the IPDACT, the Teldat **VisorALARM** IP address and the UDP port used for communication, the passwords used to encrypt the IPDACT messages (local password) and that used to decrypt the Teldat **VisorALARM** messages (remote password), the interval used to send the monitoring messages (*keep-alive*) and the number of retries and the time between these in cases where the Teldat **VisorALARM** does not acknowledge them. Lastly this also permits you to configure the number of digits a telephone number has, the number of times an alarm is sent to the Teldat **VisorALARM** until this can be sent over the telephone line.

The following figure displays the default values. Press *z* to return to the previous menu.

```
        -- Alarm Report --

       Supervisory VisorALARM

        Main
         a)  Remote IP addr: 80.26.96.183

        Backup
         b)  Remote IP addr: 80.36.189.123

       Maintenance VisorALARM
         c) Remote IP addr: 172.24.51.32

       Common Params
         d) Account Number: 9005
         e) Port: 1222
         f) Local Password: 1234567890
         g) Remote Password: 0987654321

       VisorAlarm Main Keep-Alive
         h) Timer: 60
         i) Retries: 3 Timer 3

       VisorAlarm backup Keep-Alive
         j) Timer: 3
         k) Retries: 3 Timer 3

       Remote Alarm
         l) Telephone len: 3
         m) Tx retries: 5

       Output
         n)Output Switching Period: 20

       PSTN Survaillance
         o)Action due to Alarm: BOTH

         z) Exit

          option:
```

IV - 4.5. IPDACT Quick Configuration

This allows an installer to completely configure an IPDACT from a single menu. This includes all the parameters described in section IV.2.1.3. Additionally, this also permits you to reset the device, execute the device register in the configured Teldat **VisorALARM** and trigger the automatic device register.

The IPDACT registration process (option i) in the Quick Menu) implies registering the device in the **VisorALARM**. The result of the register operation is dumped in the console. If the process has successfully

completed, an OK will appear on the console. If however there has been as error, this could be either:

- "VA unreachable": It has not been possible to send the register command over the IP network.
- "No answer": The register command has been sent but a response has not been received from the **VisorALARM**.
- "Error on answer": The answer from the VisorALARM for the register command is wrong.

The automatic device register consist on the attempts of the IPDACT to register in the VisorALARM without the operation from the console. When the option k) is chosen form the Quick Menu the IPDACT triggers a process in which the IPDACT attempts to register until a response from the VisorALARM is received.

During the automatic register none message is dumped in the console. The way to know the status of the automatic register is by checking the LED_A. This LED is blinking while the IPDACT does not received the response from the VisorALARM and will turn off when the register took place.

The following figure displays the default values. Press z to return to the previous menu.

```
          -- Quick Install --
          a) DHCP client: ON
          b) IP addr: 192.168.0.100 mask: 255.255.255.0
          c) Gateway IP: 192.168.0.200
          d) Account Number: 0
          e) Supervisory Main:
          f) Supervisory Backup:
          g) Maintenance:
          h) Port: 80
          i) Register MIP
          j) Reset
          k) AutoRegister MIP

          z) Exit

           option:
```

IV - 4.6. Monitoring

The rest of the options permit you to inspect the distinct IPDACT aspects and to monitor the state and view the enabled events. In order to exit each option, press any key which will return you to the main menu.

Option d) displays the IPDACT general parameters, such as the serial number, firmware release, etc.

```
        General Info
Teldat MIP
S/N: 8209/01101      FF190504        0
v4.1 Apr 06 2006

01/02/1980 09:16:20

LAN
 MAC: 0-A0-26-30-3-E9      state: up
INPUT, OUTPUT
 Input:OFF    Output:INACT
Reset/Phone console jumper
 state:OPEN
Press any key to continue...
```

Option `e)` displays the state of the connection with the **VisorALARM** IP receiver.

```
State: Active (4)
Press any key to continue...
```

Option `f)` displays the enabled events. To return to the menu, strike any key.

Option `g)` displays the IP parameters that are running in the device. If the device has not obtained an address through DHCP, this displays the IP address, mask and gateway configured in the "`a) Generic MIP config`" menu. If on the other hand, IP configuration has been dynamically obtained from a DHCP server, these parameters will be displayed together with other parameters pertaining to the DHCP protocol: remaining time for the obtained address value, remaining time until the next attempt to renew the said address and the DHCP server the parameters were taken from.

```
My IP Address: 61.156.44.3
Netmask: 255.255.252.0
Gateway: 61.156.44.1
DHCP information.
  Remaining lease = 107559 (sec)
  Renew lease in 53559 (sec)
  DHCP server: 61.156.44.1
Press any key to continue...
```

IV - 5. Telnet

As previously mentioned, it is possible to access the IPDACT console through a telnet client, from a PC or any other workstation. To do this, simply execute the telnet client, indicating the IPDACT IP address. The interface for this said console is identical to the one for the asynchronous console, so for further information on this please see the section on this console.

The following figure shows an example of accessing through telnet from the default client program in the Windows operating system.

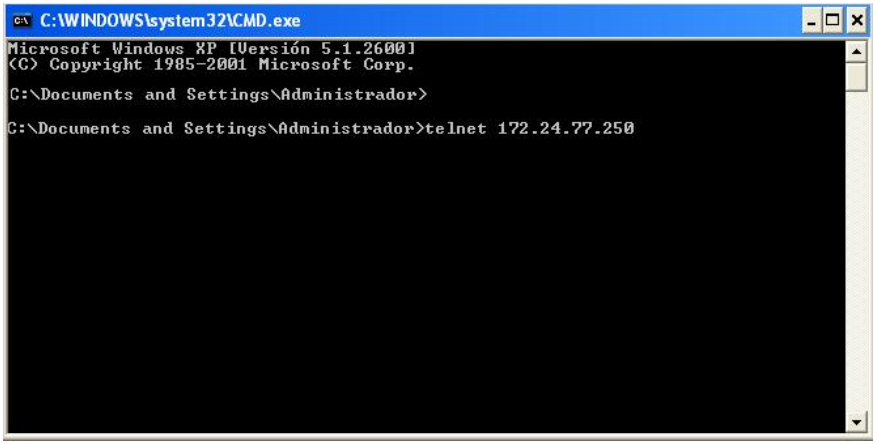


Figure 27. Example of accessing through Telnet

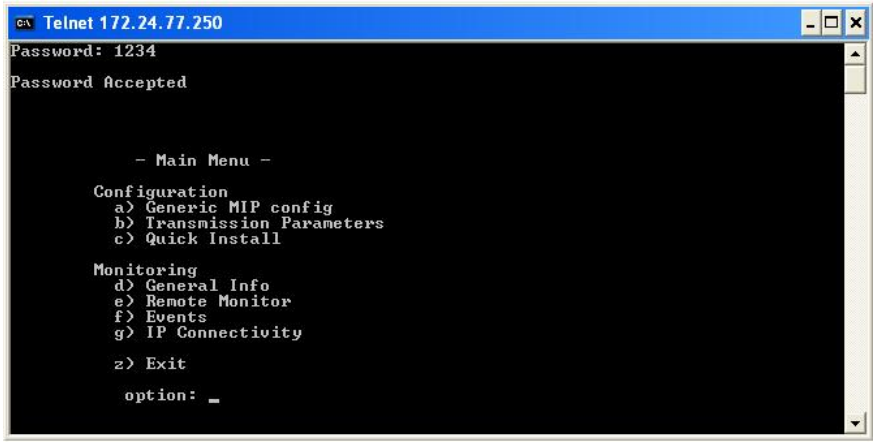


Figure 28. Access Results

V - Chapter. Appendix

V - 1. UL Compliance

- UL 864 (Ninth Edition): The Standard for Control Units and Accessories for Fire Alarm Systems.

V - 2. Control Panels

The above standards are guaranteed with the following lists of panels:

Fire Panels:

- MS-9200UD
- MS-9600
- MS-9200UDLS
- MS-9600LS
- MS-9050UD
- MS-5UD, MS-10UD
- ADT-UNIMODE 200PLUS
- ADT-UNIMODE 9600
- UNIMODE 9050UD
- UNIMODE 9200UDLS
- UNIMODE 9600LS
- UNIMODE 5
- UNIMODE 10

V - 3. Technical Specifications

Power Supply

NOMINAL VOLTAGE RANGE	10 V_{DC} – 24 V_{DC}
MAX CURRENT[1]	12V: Idle: 190 mA Alarm: 240 mA Transient[2]: 500mA 24 V: Idle: 100 mA Alarm: 120 mA Transient[2]: 300mA

Dimensions and weight

LENGTH x WIDTH x HEIGHT	140 x 92 x 29 mm
WEIGHT	150 gr

Environmental Specifications

OPERATING TEMPERATURE	0º to 49º C (32º to 120º F).
RELATIVE HUMIDITY	Maximum: 93%

LAN Port

CONNECTOR	RJ45 female
SPEED	10 Mbps
PROTOCOLS	UDP, IP, ARP, DHCP, Telnet, Ethernet Blue Book

Other Characteristics

OUTPUT	2A max. if V ≤ 30 V_{DC} for resistive loads
INPUT	1A max.

[1] The IPDACT power consumption should be subtracted from the maximum power of the output delivered by the control panel. A 750mA power source is recommended in all cases.

[2] Transient lasting 75ms is produced when the control panel takes over the telephone line to call the control center.