VisorALARM PLUS 2U

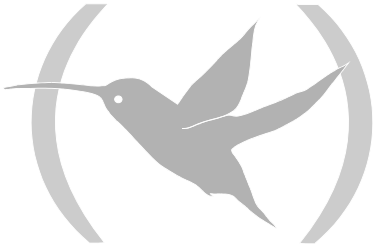
Installation Manual

Doc. *DM374-I* Rev. *1.0*

May, 2007

INDEX

Chapter 1
Introduction



1. VisorALARM PLUS 2U Introduction

The IP VisorALARM PLUS 2U receiver (Model VisorALARM PLUS 2U) is a communications device developed by Teldat for security environments. The IP VisorALARM PLUS 2U receiver's principal task is to receive alarms over an IP network and to subsequently send them to an automation software (SwAut). The functionality of the Teldat VisorALARM PLUS 2U is similar to any other alarm receiver which receives alarms over the telephone line.

The IP VisorALARM PLUS 2U receiver operates together with the IP Module (mIP/IPDACT), which receives the alarms from the alarm control panels and sends them to the Teldat VisorALARM PLUS 2U over an IP network. Additionally, the Teldat VisorALARM PLUS 2U monitors connectivity with all the registered mIP/IPDACTs. Should connectivity fail then the VisorALARM PLUS 2U generates alarms to the SwAut.

The VisorALARM PLUS 2U IP receiver has the network backup functionality added, which permits an mIP/IPDACT the possibility of IP backup towards another IP receiver. The main (or primary) receiver and the backup receiver are always synchronized at the configuration level.

The VisorALARM PLUS 2U is supplied with a display and a keypad in order to validate the signals received and monitor the device. The VisorALARM PLUS 2U includes interfaces to connect to an Automation Software and to a printer.

The user can access to the device configuration through an asynchronous serial data connection by using a serial terminal emulator. The configuration is a text level and permits the copy/paste functionality.

Figure 1. VisorALARM PLUS 2U 2U Receiver

2. Installation 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).

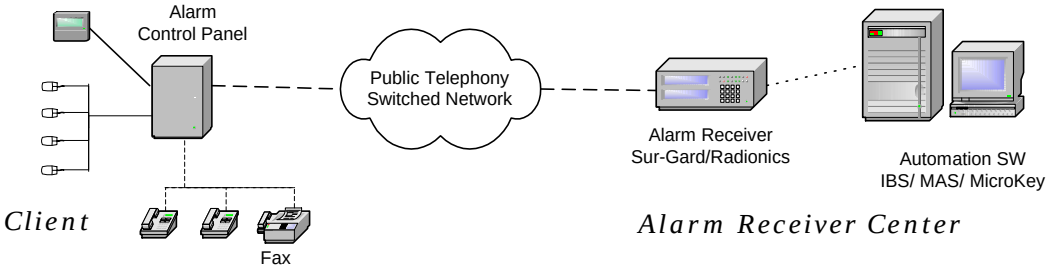


Figure 2. Traditional security scenario

The communication protocol varies depending on the manufacturers who usually tend to use their own solutions.

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

Within the general user scenario, the device in question is located in the client area, next to the control panel, intercepting the telephone line. This is displayed in Figure 3. The arrow in the figure demonstrates the preferred path to send alarms from the CP; in a Burglary application (using mIP devices) the telephone line is used as a backup in case there is a communication malfunction in the IP network. In a Fire Application (using IPDACT devices) a second telephone line is used as a backup.

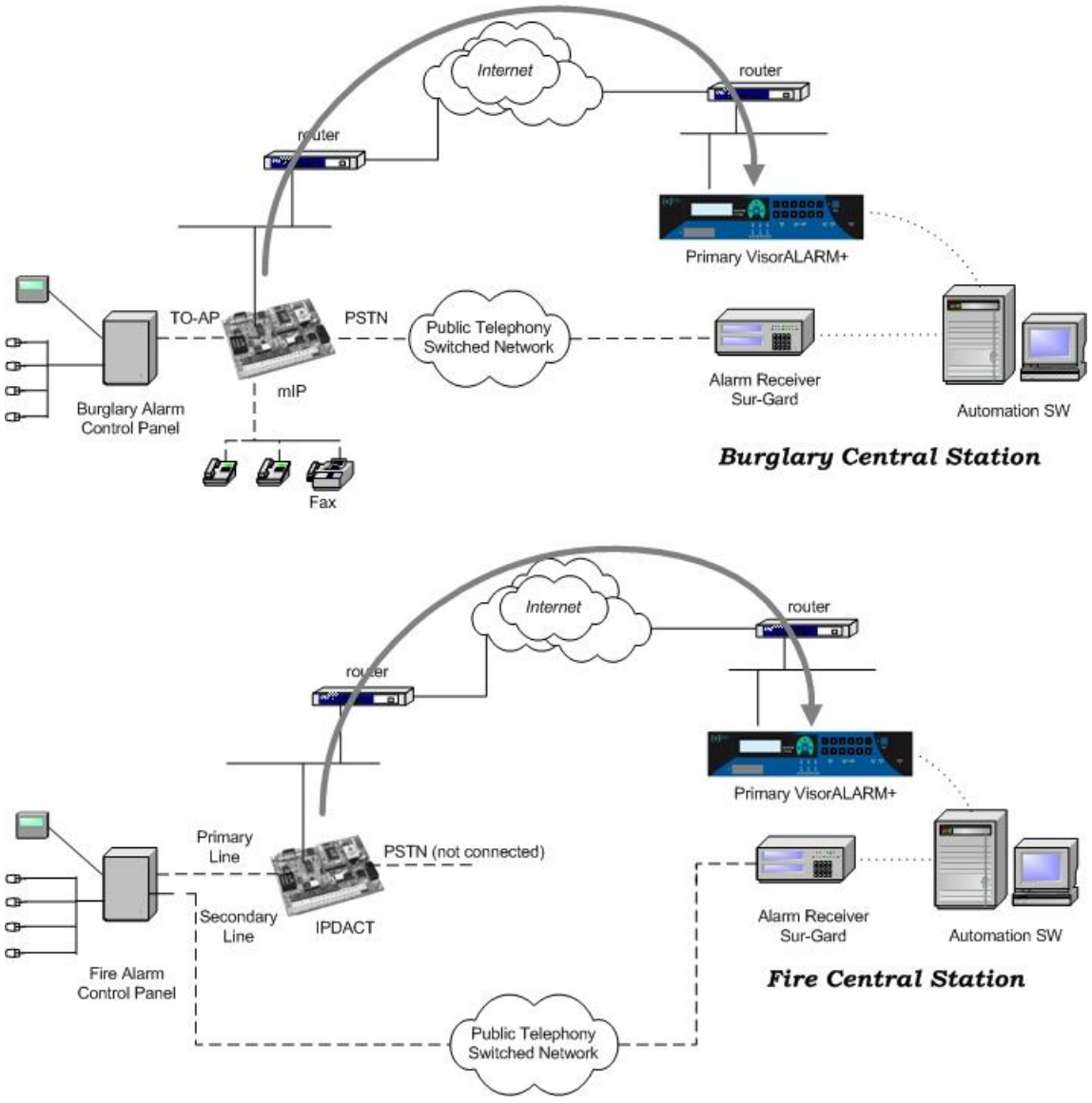


Figure 3. Teldat VisorALARM PLUS 2U and mIP/IPDACT operating scenario

There is a third scenario, thanks to the network backup functionality. In the previous scenario, if communications between the IP Module and the VisorALARM PLUS 2U fails, the former tries to send the alarms over the telephone network, as in a traditional scenario. Network backup permits you to add a second VisorALARM PLUS 2U configured as backup and which would be a second option of sending alarms in cases where the main VisorALARM PLUS 2U fails. If the probe over the main fails, the mIP/IPDACT (from release 2.2 onwards) tries to establish communications with the backup VisorALARM PLUS 2U. If this is achieved, the mIP/IPDACT will maintain the probe with latter and sends the alarms which are produced. In the meantime, the mIP/IPDACT continues to poll the main VisorALARM PLUS 2U until this becomes accessible once more. At this point the mIP/IPDACT returns from backup and reestablishes all the communications with the main VisorALARM PLUS 2U.

In cases where the backup VisorALARM PLUS 2U also fails, the mIP/IPDACT will release the telephone line so that the control panel, from this point, will take over and directly sends the alarms.

It’s advisable that the VisorALARM PLUS 2U devices have different gateways and different Internet access servers to ensure efficient network backup.

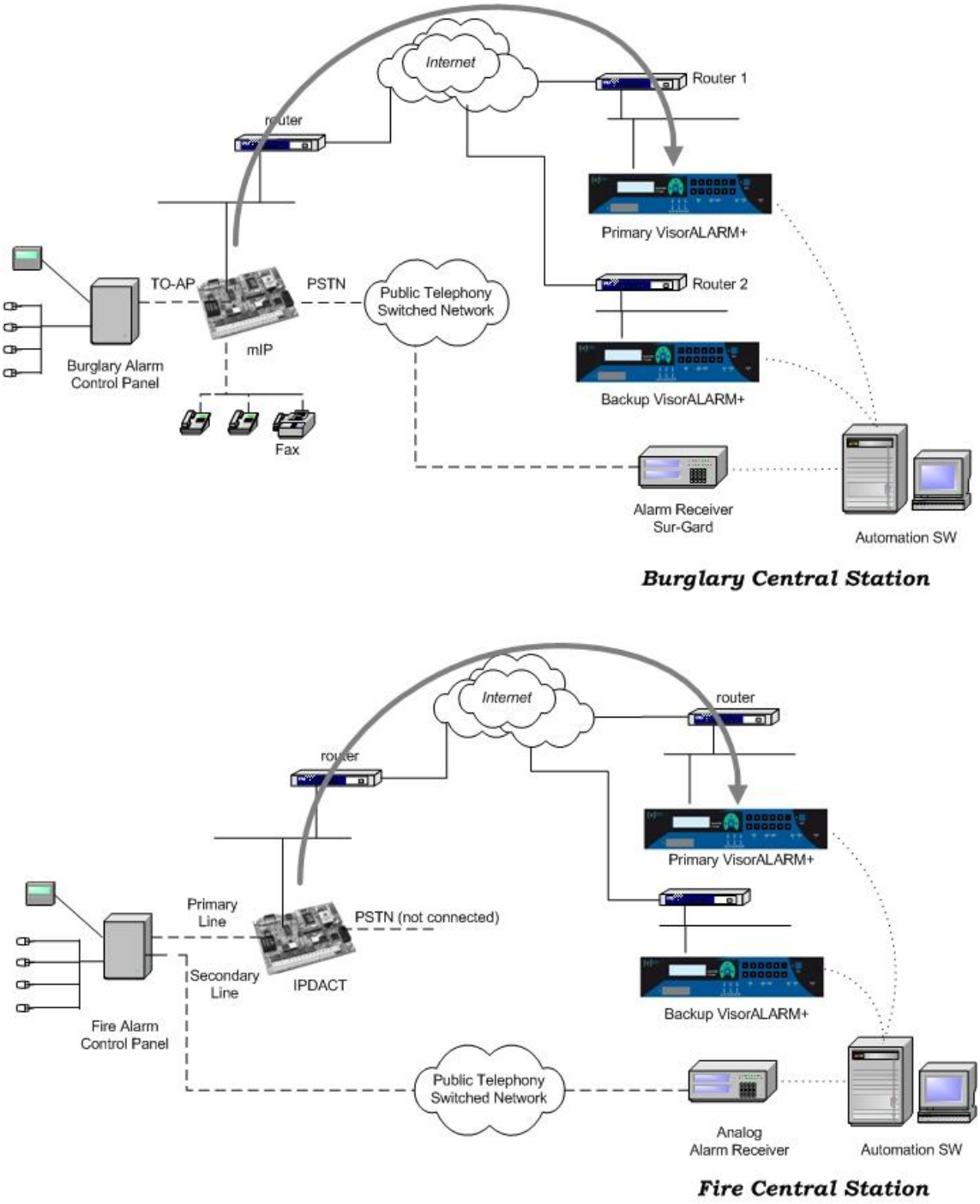


Figure 4. Operating scenario with network backup

3. Operating Mode

The IP Mode (mIP/IPDACT) connected to the client control panel carries out two tasks:

1) Capture the alarms sent by the control panel and send them over the IP network to which it is connected. These alarms are then received by the Teldat VisorALARM PLUS 2U in order to be sent to the corresponding automation software (SwAut).
2) Generate monitoring traffic so that both ends of the security environment check the IP connectivity, as it is this that permits the above task to be carried out.

3.1. Monitoring

The mIP/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 the Teldat VisorALARM PLUS 2U has been verified. The mIP/IPDACT - VisorALARM PLUS 2U connectivity is checked through a traffic monitor which the mIP/IPDACT periodically sends and to which the Teldat VisorALARM PLUS 2U responds. If this exchange of messages does not occur during the configured time, the mIP/IPDACT tries to resend. If, after a configurable number of attempts (between 1 and 9), a satisfactory response is not received, the connectivity is presumed lost. The time between polling messages is programmable between 0 and 90 seconds, a typical value being 15 seconds. The time between retries is also configurable, between 3 and 9 seconds.

If a network backup scheme is running, the mIP/IPDACT has a second IP receiver to establish communications and send alarms. If this second receiver does not respond to the communication established with it by the mIP/IPDACT (again after a configurable number of attempts), the telephone line access is returned to the control panel as if the mIP/IPDACT is no longer operative at the alarm level. From this point on, the mIP/IPDACT will try to re-establish communications with both the main Teldat VisorALARM PLUS 2U as well as the backup, if there is one. As soon as this is re-established with either of the two VisorALARM PLUS 2U, the mIP/IPDACT will once more intercept the telephone line.

The monitoring traffic is encrypted UDP traffic. The Ethernet frame size does not exceed 70 bytes. The monitoring interval, the number of retries and time between retries are all configurable, both for the main VisorALARM PLUS 2U as well as for the backup. The time between retries is an important parameter as it influences the global traffic supported by the VisorALARM PLUS 2U (polling over all the devices). You also need to bear in mind that polling is a tool to control the state of both the alarm reception center and the mIP/IPDACT. A long interval between polls can give rise to situations where the VisorALARM PLUS 2U delays in detecting a problem with the mIP/IPDACT and consequently a problem in a client. Finally, if the mIP/IPDACT accesses Internet via a device which executes NAT, traffic coming from the VisorALARM PLUS 2U (configuration for example) will not reach the mIP/IPDACT if the period between polls is inferior to the outgoing router NAT tables refresh time (a typical refresh value is 5 minutes).

The Teldat VisorALARM PLUS 2U received monitoring messages from the mIP/IPDACTs. If these are registered, they are assumed alive and an acknowledgement response is sent to them; if the mIP/IPDACTs are not registered, they are ignored. Periodically the status of all the registered mIP/IPDACTs is checked and an alarm is generated for all those which have not notified their availability (i.e. those which have not responded since the last check). This is a 350 code alarm from the Contact-ID protocol (*Communication trouble*) which is received in the SwAut. From release 10.1.27 onwards, the event code is configurable. Default is 350. As each mIP/IPDACT can have a

different polling time with the center, the VisorALARM PLUS 2U checks the status of each mIP/IPDACT starting with the polling time value for all of them.

In order to prevent the Teldat VisorALARM PLUS 2U 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 ICMP echo packets (ping) to a known address: if the echo packets towards this address fail then a code 356 alarm is generated from the Contact-ID protocol (*Loss of central polling*). From release 10.1.27 onwards, the event code is configurable. Default is 356.

Apart from the previous codes, the Teldat VisorALARM PLUS 2U with network backup functionality generates other codes that do not directly correspond with those pre-established by the CONTACT-ID protocol. These have default values which can be changed via the console.

A series of these codes are grouped indicating the states the VisorALARM PLUS 2U passes through. The device configured as main on startup sends a 396 restore code indicating that the device is active. The device configured as backup must send code 398 restore code indicating that the device is active. Once the main and backup VisorALARM are connected by polling, the main device sends a 358 restore code to indicate the backup device is up and the backup device sends a 399 restore code to indicate the main device is up. Both the main and the backup VisorALARM PLUS 2U can have communication problems (Loss of central polling) and consequently pass to a down state sending code event 396 for main and 398 for backup. If the backup device detects communication failure with the main device it will assume that as it cannot communicate with the VisorALARM PLUS 2U then nor will the mIP/IPDACTs. The backup will then activate sending a 399 event code (Primary VisorALARM is down) and the mIP/IPDACT polls should go to this device. Lastly, the main VisorALARM PLUS 2U can detect and indicate through a 358 code that the polls from the backup VisorALARM PLUS 2U are not reaching it and consequently there is a problem either with communications with the backup or with the main VisorALARM PLUS 2U device itself.

In addition to the above codes, we need to add a further two which provide information over particular cases. If in the mIP/IPDACT configuration there is an error where the main address is in fact the backup address, all communications from this mIP/IPDACT will be routing to the backup. The backup device, through a 395 code, will indicate this error by sending the code after each two programmed keep-alives have been executed. The second case indicates a situation where an mIP/IPDACT in backup is polling the backup device but this latter is not active, consequently there is a communication error between the mIP/IPDACT and the main VisorALARM PLUS 2U. This problem is indicated with a 394 code.

3.2. Sending of Alarms

When the mIP/IPDACT has connectivity with the Teldat VisorALARM PLUS 2U, the former intercepts the telephone line and processes all the incoming and outgoing calls taking place from the alarm panel.

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 mIP/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 mIP/IPDACT sends this alarm to the VisorALARM PLUS 2U.

The control panel is not given the frame sent acknowledgement (*kissoff*) until the said acknowledgement is received from the automation software. If the mIP/IPDACT does not receive the acknowledgement within 2 seconds, this carries on resending a configured number of times (between 5 and 10), after which connection with the Teldat VisorALARM PLUS 2U is assumed lost. As in the case of supervision where the alarm send fails, this can be sent again this time to the backup VisorALARM PLUS 2U if this functionality is configured. If communications also fail with the backup then the control panel sends the alarm over the telephone line. From this point, the mIP/IPDACT tries to re-establish communication with the two VisorALARM PLUS 2U as previously described.

The IP VisorALARM PLUS 2U receiver on receiving an alarm from an mIP/IPDACT stores this in a non-volatile internal memory. When the operation has successfully finished, it sends the acknowledgement to the mIP/IPDACT originating the alarm so that this in turn sends 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 PLUS 2U behaves as an alarm receiver that sends alarms received through a serial port. The Teldat VisorALARM PLUS 2U can emulate a Sur-Gard, a Radionics 6500 receiver or an Ademco 685. 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.)

4. Additional Features

In order to simplify installation and updating of the registered mIP/IPDACTs, the IP VisorALARM PLUS 2U receiver has additional facilities.

To install new mIP/IPDACTs, the Teldat VisorALARM PLUS 2U possesses configuration patterns associated to installer passwords. These permit you to automatically register new mIP/IPDACTs in the supported mIP/IPDACT list and at the same time enable the mIP/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 mIP/IPDACT to request the service.

From release 10.1.27 onwards, when a new mIP/IPDACT is registered an event is generated and sent to the automation software. The code for this event is configurable, default being 633 (*Module Added*).

In order to maintain and update the registered mIP/IPDACTs base, the Teldat VisorALARM PLUS 2U has commands available to remotely update one or multiple configuration parameters used by the mIP/IPDACTs.

5. Configuration and Management

The IP VisorALARM PLUS 2U receiver can be configured and monitored through a local console and also remotely (telnet). In both cases, the access is restricted to users who are identified by a user name and a password. The configuration is displayed in text mode consequently editing and support in other platforms is simpler and more comfortable.

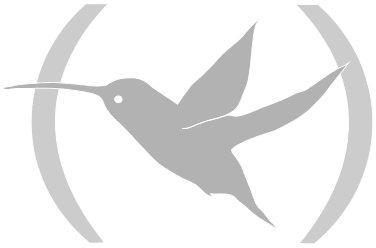
There are three types of users with different privilege levels to gain access to the configuration:

1. Manager: This sort of user can change the configuration and monitoring.
2. Supervisor: This user can only change the day and the time configuration and has total access to the monitoring.
3. Operator: This user can only access the monitoring.

The default login and password for the manager user is “manager/24680”.

The VisorALARM PLUS 2U is supplied with a display and keypad. The display is the means through which the user can access the signal information. The signals can be validated by using the keypad. For further information on using the keypad and the information showed on the display, please see manual “VisorALARM Operating Instructions”.

Chapter 2
Installation



1. Introduction

The IP VisorALARM PLUS 2U receiver is designed to be both a desktop and a rack device. In either case, in order to achieve correct installation, please follow the recommendations given below:

> ***BEFORE CONNECTING THE DEVICE PLEASE READ THE FOLLOWING INSTRUCTIONS CAREFULLY.***

1.1. General installation conditions

Conditions

Bear in mind the following recommendations:

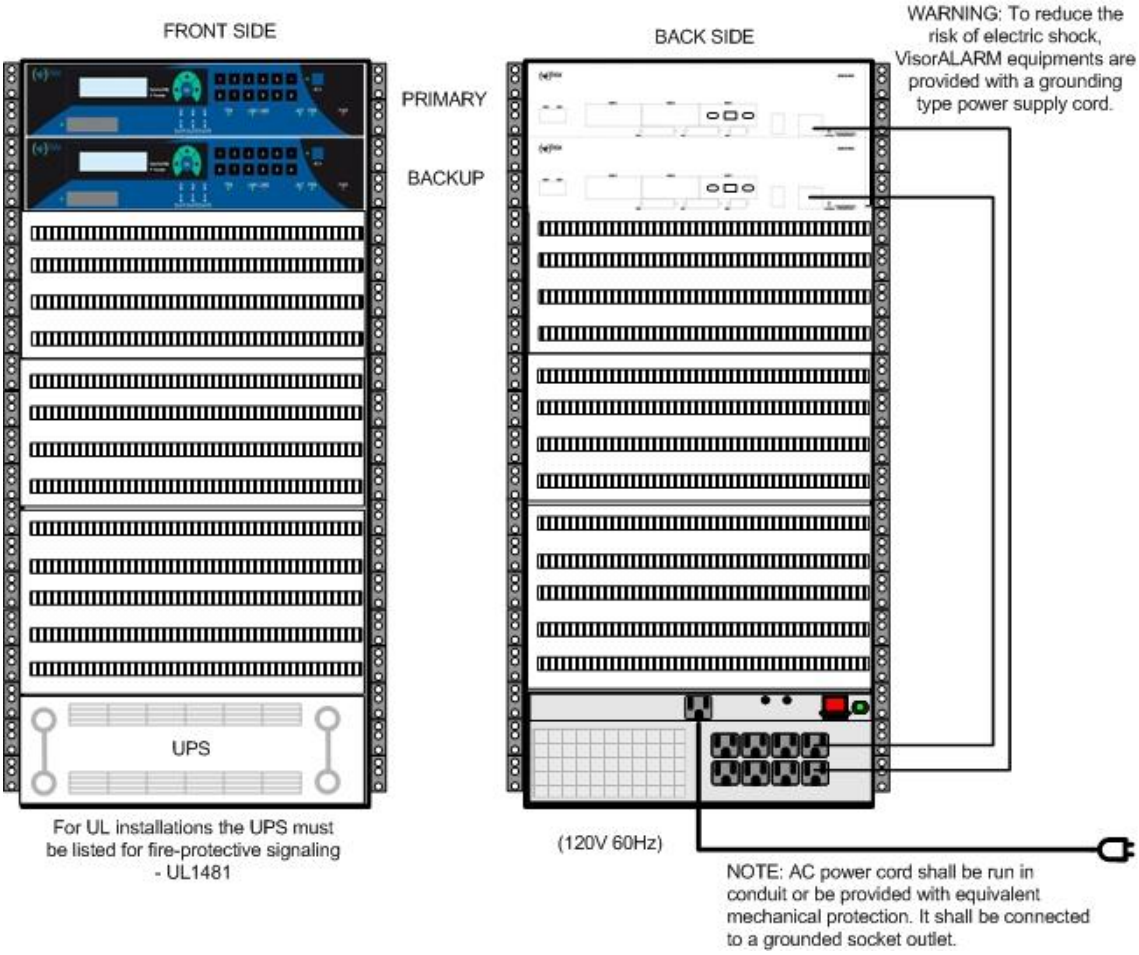
1. If the installation is UL listed, install the device in a 19" rack or box with a locking rear access door.
2. Excessive cold and heat should be avoided, as should humidity and dust. Direct exposure to sunlight should be avoided as well as other heat sources. The device should not be placed amongst papers, magazines or other elements that could hinder natural air circulation.
3. The device should not be placed very close to strong electromagnetic fields such as speakers, engines, etc.
4. Knocks and/or strong vibrations should be avoided during transport, operation and storage.

Power supply

The **VisorALARM PLUS 2U** device does not require special conditions as regards voltage stability or protection against power malfunctions as it is already protected.

To avoid electric shocks, residual current circulation and other unwanted effects, also affecting communications, the following is recommended:

- ***It is highly recommended that all interconnected communication devices be plugged to THE SAME GROUNDED POWER OUTLET, which should at the same time be of good quality (lower than 10ohms).***
- ***Whether the workplace is provided with an uninterrupted power supply system (UPS), regulated supply or it is independent from the rest (such as lighting, etc.); it is highly recommended that all data devices should be connected to the same power source. This will avoid operating and premature aging problems of drivers and other components.***
- ***For UL listed installations the device must be installed in an Alarm Central which is UL Listed where an independent generator provides uninterrupted power supply to all the equipment. It is also necessary to connect an uninterrupted power system to the device which permits it to carry on operating for at least 15 minutes.***


FRONT SIDE
BACK SIDE
WARNING: To reduce the risk of electric shock, VisorALARM equipments are provided with a grounding type power supply cord.
PRIMARY
BACKUP
UPS
For UL installations the UPS must be listed for fire-protective signaling - UL1481
(120V 60Hz)
NOTE: AC power cord shall be run in conduit or be provided with equivalent mechanical protection. It shall be connected to a grounded socket outlet.

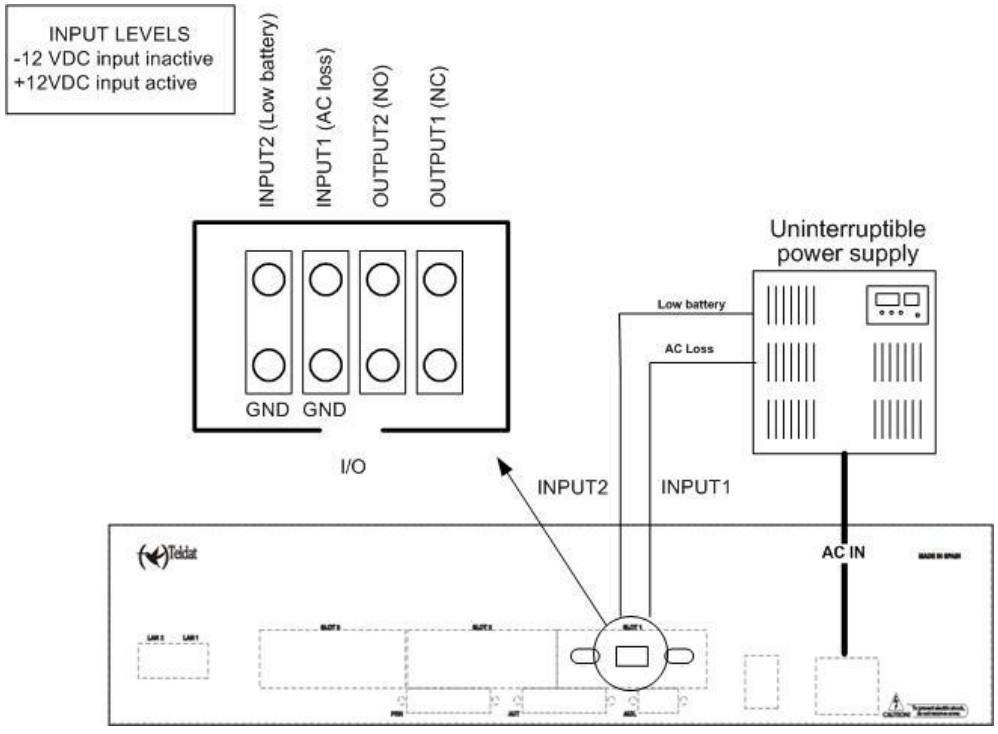

INPUT LEVELS
-12 VDC input inactive
+12VDC input active
INPUT2 (Low battery)
INPUT1 (AC loss)
OUTPUT2 (NO)
OUTPUT1 (NC)
GND GND
I/O
Uninterruptible power supply
Low battery
AC Loss
INPUT2
INPUT1
AC IN

Figure 5. 19" rack installation and device power connections

WARNING: Electric supply current, telephone and communication cables are dangerous. To prevent electric shock while installing, moving or opening the device covers, cables should be disconnected and connected as follows:

To connect the VisorALARM PLUS 2U
• Make sure that the device power supply switch is OFF. • Connect all the data cables. • Connect the power supply cable. • Switch on the device.

To disconnect the VisorALARM PLUS 2U
• Switch off the device. • Disconnect the power supply cable. • Disconnect the data cables.

1.2. Connection

a) LAN Ethernet connection

The device has two Ethernet 100baseT LAN interfaces to connect to the IP network. This LAN interface has a female RJ45 connector in order to connect to the Ethernet 10BaseT networks through a shielded twisted pair (STP) or unshielded (UTP) cables. These cables are not supplied with the equipment; please consult your supplier with regard to this.

Depending on the design of the Network, the connection is carried out through a HUB or directly to another terminal device Ethernet interface through a crossover cable (please consult your supplier for information on crossover Ethernet cables).

When the VisorALARM is connected to the Ethernet through the LAN1 connector, the LED on the front panel labeled LAN1 will light up in green. If there is no connection, the LED will light up in red. The same thing will happen with the other LAN2 Ethernet connector. Please note that in the factory configuration only the LAN1 connection is configured.

IMPORTANT: For UL listed installations it is mandatory to connect the VisorALARM ethernet interface to the ethernet building installatation through the device ESD-100 ethernet data line protector (Alerton Technologies, UL listed UUKL.S8105).

b) Connecting to the alarm server

Data connection to the alarm automation server is carried out through the serial interface labeled AUT in the device. This serial interface complies with the V.24 norm, behaves as DCE and has a female DB25 connector. You need to use a DB25 male serial cable to a DB9 female in order to connect to the server.

IMPORTANT: Do not use a null modem cable.

When the VisorALARM is connected to the Automation Server, the LED on the front panel labeled AUT will light up in green. If there is no connection, the LED will light up in red.

c) Connecting the printer

Connection to the printer is carried out through the serial interface labeled PRN in the device. This serial interface complies with the V.24 norm, behaves as DCE and has a female DB25 connector. You need to use a DB25 male serial cable to a DB9 female in order to connect to the printer.

IMPORTANT: Do not use a null modem crossover cable.

WARNING: in UL Listed Installations, always use a UL Listed printer.

When the VisorALARM is connected to a printer, the LED on the front panel labeled PTN will light up in green. If there is no connection, the LED will light up in red.

d) VisorALARM Expansion Card

The VisorALARM PLUS 2U is supplied with three slots where three VisorALARM Expansion Cards can be plugged in (Labeled as VA-UD in the rear panel). The device is supplied with one VA-UD in the factory configuration.

The following figure shows the VA-UD connectors:

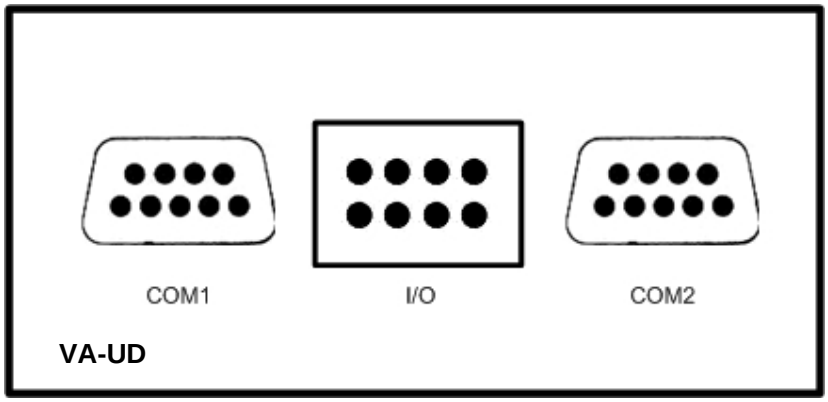


Figure 6. VA-UD Connectors

· Connectors COM1 and COM2

The data connection to Uploading/Downloading Software is carried out through these two connectors. The serial interface complies with the V.24 norm, behaves as a modem and has a female DB25 connector. At the same time two separate data connections can be made for each VA-UD.

· Connector I/0

The following figure shows the arrangement of the connector outputs and inputs.

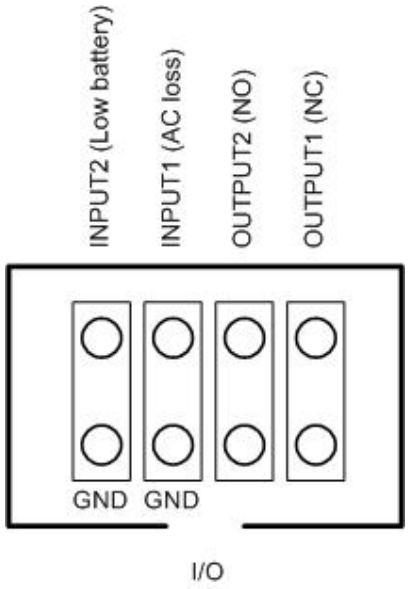


Figure 7. Arrangement of inputs/outputs in ConnectorI/O (VA-UD)

The two outputs are relays with a rated voltage of 30 volts CC and a rated amperage of 2A CC. The relays are normally open.

- Output1: This output is dedicated for watchdog indication.
- Output2: This is a general purpose output. The factory configuration for this output is to close the relay in cases where some unrestored trouble alarm s(3XX CONTACT-ID code) exist with account 0, i.e., an trouble alarm signaled by the VisorALARM and not restored.

The two inputs have RS-232 levels (-12V/+12V, -12V input inactive, +12V input active).

- Input1: This is a general purpose input. The factory configuration for this input is to detect a failure in the AC main signaled by a UPS device.
- Input2: This is a general purpose input. The factory configuration for this input is to detect a low battery signaled by a UPS device.

e) Configuration connection

The IP VisorALARM PLUS 2U receiver routers have a female DB-9 connector in the rear panel referred to as **"AUX"** which provides access to the device local console for configuration and monitoring purposes. In order to use this, you must connect to the **"AUX"** port to an asynchronous terminal (or to a PC with terminal emulation).

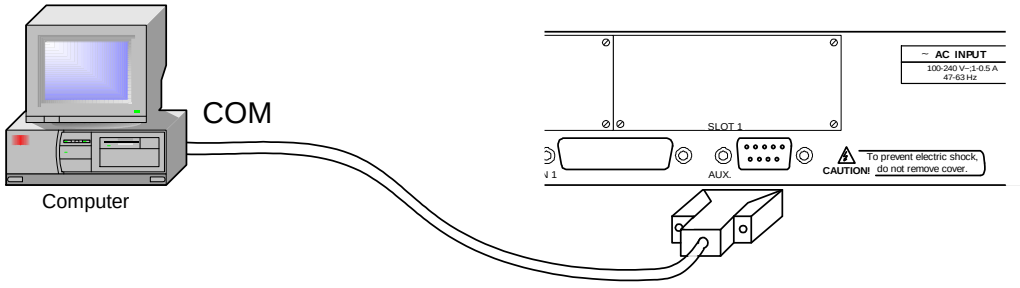


Figure 5. Connection for configuration/monitoring via console

The configuration of the terminal must be:

- ***Speed: 9600 bps***
- ***Eight data bits***
- ***No parity bit***
- ***One stop bit***
- ***No type of flow control***

Also expressed as 9600 8N1. The connection to the configuration port can be carried out with DB-9 female-DB-9 male cable provided with the equipment. In cases where the asynchronous terminal has DB25 connectors, you must use an additional DB9F-DB25F adapter (not included with the equipment).

1.3. Switching on the device

Once the device has been installed in the workplace following the steps previously given, you can switch on the device. Once this has been carried out, a process of auto-test and initialization, explained below, takes place.

Firstly, the device carries out a brief auto-test where it checks that the startup program is correct and a brief detection and initialization of the SDRAM present in the device. If any problems are detected the process stops and the TRB LED flashes in red. Once this process has completed, the console is available and begins to show data.

Once the booting process has terminated, an auto-test and auto-detection test of the motherboard hardware takes place. If the test is successful the TRB LED remains green. If any malfunctions are detected, the corresponding LED remains lit up in red and once the auto-test has completed, depending on the problem, the device resets and repeats the process or permits you to operate through the console in order to resolve the problem. (Note that once the VisorALARM is running, if the device has unrestored System Trouble Signals the TRB LED remains lit up in red while these signals remain unrestored).

Once the firmware decompression process is completed the application executes, the configuration is read and the access login is displayed.

If you have a terminal or a PC with terminal emulation connected to the device console, booting information similar to that shown below can be displayed:

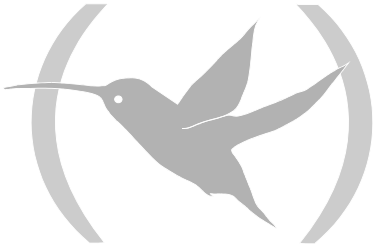
```
************************************************
************************************************
************************************************

BOOT CODE VERSION: 01.10  Oct 30 2006 17:17:43
  gzip  Oct 30 2006 17:08:44
P.C.B.: 75  MASK:0A01  Microcode:0070
START FROM FLASH
BIOS CODE DUMP.....................
BIOS DATA DUMP....
End of BIOS dump
 Boot-stack used: 0x00000788
 Boot-stack free: 0x00001878
BIOS CODE VERSION: 01.10
CLK=294912 KHz   BUSCLK=65536 KHz   PCICLK=32768 KHz   L1
Date: 11/20/06, Monday          Time: 17:28:05

SDRAM size: 128 Megabytes
   BANK 0: 128 Megabytes (detected)
I_Cache: ON
D_Cache: ON    Write-Back
FLASH: 16 Mb.
NVRAM: 128 Kb.
EEPROM: 2048 Bytes.
DPRAM: 16384 Bytes.
WAN1: DCE
WAN2: DCE
ISAC
RDSI_B
RDSI_B
FAST ETHERNET 1
FAST ETHERNET 2
PCI device: Host bridge
  (Bus: 0, Device: 0, Function: 0)
  (Subs. Vendor: 0x0000, Subs. Device: 0x0000)
Slot 1 - PCI device: bridge
  (Bus: 0, Device: 10, Function: 0)
  (Subs. Vendor: 0x5444, Subs. Device: 0x2301)
Current production date: 06 05
Current software license: 6 120
Current serial number: 472/05898
BIOS MAC Add: 00-a0-26-70-17-0a
>>
........
TRYING APP CODE DUMP
   (CONFIGURED) cit.bin ver.: 0.10.6.27 0.0.0.0 ..............................
................................................................................
.....................................................................
APP DATA DUMP.....................................................................
............
 Bios-stack used: 0x1498
 Bios-stack free: 0x2B68
 Aux-stack used: 0x124
 Aux-stack free: 0x1EDC
Running application
Flash configuration read
Initializing

Press any key to get started
```

Chapter 3
Configuration



1. Introduction

The aim of this chapter is to provide guidelines for the user regarding the VisorALARM PLUS 2U configuration process to ensure it runs correctly.

The basic VisorALARM PLUS 2U function is to receive alarms from the mIP/IPDACT devices via an IP network, and send to an automation software through a serial interface emulating one of the supported receivers. The VisorALARM PLUS 2U configuration consists of four basic steps:

- Common configuration: device name, user and password to access the console, etc.
- IP Configuration: parameters required to achieve IP connectivity with the mIP/IPDACT devices (IP address, mask and gateway).
- In cases where you have a network backup configuration, it is essential that the two VisorALARM PLUS 2U devices have their clocks synchronized. To do this you need to configure NTP clients (Network Time Protocol) in each of the devices.
- Configuring the alarm reception itself.

VisorALARM PLUS 2U configuration can be executed, as already said, with a serial connection to the device AUX interface and a terminal emulation software in a PC. Additionally, if you have IP connectivity with the device, you can achieve the same functionality through a telnet connection to the VisorALARM PLUS 2U IP address.

For further information on how to configure NTP (Network Time Protocol) clients, please see Teldat manual Dm 728-I "NTP Protocol".

The VisorALARM PLUS 2U configuration can only be executed by a manager user. The manager has a password so he can be recognized.

2. Common configuration

The VisorALARM PLUS 2U receiver is shipped from factory with a default configuration. This is the basic configuration that allows the manager to come into operation. For that reason, the installation process starts from this configuration.

The first step is to access the device configuration menu in order to adapt some configuration parameters to the client scenario.

The device configuration is accessed by the configuration connection as explained in point 1.2. Once the connection is established, the manager must use a terminal emulator program to access the configuration and to configure the serial port parameters as indicated in the above section.

If the manager switches the device on, the following lines will appear in the terminal emulator program:

```
************************************************
************************************************
************************************************

BOOT CODE VERSION: 01.10  Oct 30 2006 17:17:43
  gzip  Oct 30 2006 17:08:44
P.C.B.: 75  MASK:0A01  Microcode:0070
START FROM FLASH
BIOS CODE DUMP.....................
BIOS DATA DUMP....
End of BIOS dump
 Boot-stack used: 0x00000788
 Boot-stack free: 0x00001878
BIOS CODE VERSION: 01.10
CLK=294912 KHz   BUSCLK=65536 KHz   PCICLK=32768 KHz   L1
Date: 11/20/06, Monday          Time: 15:41:38

SDRAM size: 128 Megabytes
   BANK 0: 128 Megabytes (detected)
I_Cache: ON
D_Cache: ON    Write-Back
FLASH: 16 Mb.
NVRAM: 128 Kb.
EEPROM: 2048 Bytes.
DPRAM: 16384 Bytes.
WAN1: DCE
WAN2: DCE
ISAC
RDSI_B
RDSI_B
FAST ETHERNET 1
FAST ETHERNET 2
PCI device: Host bridge
  (Bus: 0, Device: 0, Function: 0)
  (Subs. Vendor: 0x0000, Subs. Device: 0x0000)
Slot 1 - PCI device: bridge
  (Bus: 0, Device: 10, Function: 0)
  (Subs. Vendor: 0x5444, Subs. Device: 0x2301)
Current production date: 06 05
Current software license: 6 120
Current serial number: 472/05898
BIOS MAC Add: 00-a0-26-70-17-0a
>>
........
TRYING APP CODE DUMP
```

```
(CONFIGURED) cit.bin ver.: 0.10.6.27 0.0.0.0 ..............................
.....................................................................................
.....................................................................
APP DATA DUMP.....................................................................
............
 Bios-stack used: 0x1498
 Bios-stack free: 0x2B68
 Aux-stack used: 0x124
 Aux-stack free: 0x1EDC
Running application
Flash configuration read
Initializing

Press any key to get started
```

The device prompts the user for the login and password to gain access to the configuration. The factory configuration for the login/password is “manager/24680”.

```
Press any key to get started


User: manager
Password: *****



Teldat               (c)2001-2006

Router model VISORALARM-PLUS US 6 120 CPU MPC8260      S/N: 472/05898
2 LAN, 4 WAN Lines
CIT software version: 10.6.27-Alfa Nov 17 2006 17:05:13


*
```

The next step is to enter the configuration through the “process 4” or “config” command.

```
Teldat               (c)2001-2006

Router model VISORALARM-PLUS US 6 120 CPU MPC8260      S/N: 472/05898
2 LAN, 4 WAN Lines
CIT software version: 10.6.27-Alfa Nov 17 2006 17:05:13


*config


Config>
```

The way to display the current receiver configuration is through the “show configuration” command as shown below:

```
Config>show configuration
```

```
; Showing System Configuration for access-level 15 ...
; VISORALARM-PLUS US Router 6 120 Version 10.6.27

log-command-errors
no configuration
description "Default configuration: VisorALARM standard"
set data-link arly serial0/0
set data-link sepi serial0/1
set data-link modem-emu serial1/0
set data-link modem-emu serial1/1
set sram-size 1024
cfg-mode binary
;
; -- Privilege Configuration --
set privilege 9 ">time" all
;
;
user manager password 24680
;
user supervisor password 13579
user supervisor access-level 9
;
user operator password 11111
user operator access-level monitor
;
network serial0/0
; -- ARLY Interface Configuration --
   alarm-receiver protocol ademco-685
   alarm-receiver receiver-id 1
   alarm-receiver line-id 1
;
   backup-alarm-receiver type main
   backup-alarm-receiver sync-port 35001
;
   printable-events alarm enable
;
;
   io-conf output system-trouble-unrestored
   io-conf input1 ac-loss
   io-conf input2 low-battery
;
   priority-standard ul
;
;
exit
;
network serial0/1
; -- SEPI Interface Configuration --
   serial-parameters speed 9600
exit
;
protocol ip
; -- Internet protocol user configuration --
   address ethernet0/0 192.168.0.200 255.255.0.0
;
;
;
exit
;
;
dump-command-errors
end
; --- end ---
```

The manager can configure a name for the device. The main aim of configuring a name is so it appears on the device console and can be distinguished from other devices should there be more than one Teldat device. This parameter is optional; the following example shows you how to configure this using **PRIMARY** as the device name. Where you have a configuration with another VisorALARM PLUS 2U as network backup, it is advisable to assign names to the devices to identify the main VisorALARM PLUS 2U and the backup.

Teldat recommends you to take the factory configuration and save it in a file. This configuration can be used in cases where the manager wants the device to start from scratch. The way to get the factory configuration is by using the “show configuration” command and to copy it over to the clipboard. Once you get the configuration in the clipboard, you can save it in a file. The VisorALARM console permits you to paste the clipboard contents into the configuration. The process ends while saving the configuration by using the “save” command and resetting the device.

3. Changing the IP Protocol Configuration

Communications between VisorALARM PLUS 2U and mIPs are carried out by the IP protocol. The factory configuration assigned IP address 192.168.0.200 and mask 255.255.0.0 to the Ethernet interface. In cases where the manager wants to change the IP address to pertain to the IP network, the following steps must be executed.

To access the IP configuration environment, enter the following command:

```
PRIMARY Config> PROTOCOL IP
PRIMARY IP config>
```

Subsequently, you need to assign the IP address together with its mask to the Ethernet interface. In the following example, address 128.185.123.22 with mask 255.255.255.0 is assigned.

```
PRIMARY IP config>address ethernet0/0 128.185.123.22 255.255.255.0
```

The next step is to configure the *gateway* IP address. The gateway is the device that allows the VisorALARM to access internet. The *gateway* IP address must pertain to the same subnet as the Ethernet interface IP address. In the following example this parameter is configured with the value 128.185.123.1. In cases where you are using a second VisorALARM PLUS 2U for backup, we recommend that each device has a different gateway.

```
PRIMARY IP config>route 0.0.0.0 0.0.0.0 128.185.123.1 1
PRIMARY IP config>
```

The configuration is for this menu is then displayed and subsequently returns to the general configuration menu.

```
PRIMARY IP config>show config
; Showing Menu and Submenus Configuration ...
; Router Visor Alarm 2 16 Version 10.1.19

;
   address ethernet0/0 128.185.123.22 255.255.255.0
;
;
   route 0.0.0.0 0.0.0.0 128.185.123.1 1
;
;
;
PRIMARY IP config>exit
PRIMARY Config>
```

4. Configuring the NTP Client

One of the key features of network backup is to get the configurations for the main and the backup equipments synchronized, i.e. if a mIP/IPDACT has been registered in the main VisorALARM PLUS 2U, that registration will automatically appear in the backup VisorALARM PLUS 2U given that at any time this can become the active receiver.

However, you must ensure that the current time and date of both receivers (main and backup) are the same because this time value greatly affects the synchronizing operations.

The way to get both equipments with the same time and date is through the NTP protocol (Network Time Protocol).

> ***If the VisorALARM has not configured the NTP protocol or this protocol is not working properly, the synchronization process is suspended. Furthermore, the device will signal a 397 event code (VisorALARM Time Inaccurate).***

The NTP protocol is based in a client-server model, where the NTP clients are synchronized with a NTP server that possesses a stable time. In our case the VisorALARM PLUS 2U receiver adopts the client role. There are several public lists of NTP servers, the system manager can choose any of the NTP servers included in those lists to synchronize main and backup receivers (one example of such servers is the Massachusetts Institute of Technology (MIT) with an 18.145.0.30 public address).

Thus, the Teldat NTP client functionality allows the VisorALARM PLUS 2U clock to be synchronized with a time base supplied by an NTP server. In cases where you do not have network backup, this configuration is unnecessary.

The basic parameters required to configure the client are as follows:

- NTP server IP address.
- The local address you want to appear in the NTP packets.

The rest of the parameters can be left with their default values.

To access the client configuration, enter the following command:

```
PRIMARY Config>feature ntp
PRIMARY NTP Config>
```

The server address is entered with the following command:

```
PRIMARY NTP Config> peer address 1 18.145.0.30
```

Various NTP servers can be added indicating the station number after the `peer-address` command.

The source address corresponds to that configured in the VisorALARM PLUS 2U Ethernet interface:

```
PRIMARY NTP Config> source-address 172.24.77.53
```

The last operation is to enable the protocol which is executed through the below command:

```
PRIMARY NTP Config> protocol
```

Subsequently, the configuration of this menu is displayed:

```
PRIMARY NTP config>show conf
; Showing Menu and Submenus Configuration ...
; Visor Alarm Router 2 16 Version 10.4.7

   protocol
   source-address 172.24.77.53
   peer address 1 18.145.0.30
MAIN NTP config>
```

5. ARLY alarm reception interface

The ARLY interface is a serial interface that provides the device with complete IP alarm reception functionality. The device performs the following tasks:

- Receives alarms from the registered mIP/IPDACTs through an IP network.
- Emulates a conventional alarm receiver sending the alarms through an asynchronous serial port in order to be processed in automation alarm software.
- Supervises the registered mIP/IPDACTs and generates the corresponding alarm in cases of loss of communication.
- Supports the installation and maintenance of the registered mIP/IPDACTs.

The process to configure the parameters concerning the VisorALARM PLUS 2U alarm reception is described below. For further information on the available commands, please see manual Dm 318-I "ARLY Interface.

In order to access the ARLY interface configuration, use the NETWORK command and the serial line associated to the ARLY interface:

```
PRIMARY Config>NETWORK SERIAL0/0

-- ARLY Interface Configuration --
PRIMARY ARLY-1 Cfg>
```

5.1. Alarm Receiver

The first step is to configure the parameters related to the behavior of the VisorALARM PLUS 2U as receiver. The VisorALARM PLUS 2U is capable of emulating three types of receivers:

- Sur-Gard
- Radionics 6500
- Ademco 685

Default behavior is to emulate the Sur-Gard receiver. To configure the type of receiver, use the "ALARM-RECEIVER PROTOCOL" command followed by the type of receiver to emulate.

Subsequently, the commands to respectively configure emulation for a Sur-Gard receiver, a Radionics and an Ademco are shown below. Execute the command corresponding to the type of receiver you wish to emulate.

```
PRIMARY ARLY-1 Cfg>alarm-receiver protocol sur-gard
PRIMARY ARLY-1 Cfg>alarm-receiver protocol radionics-6500
PRIMARY ARLY-1 Cfg>alarm-receiver protocol ademco-685
PRIMARY ARLY-1 Cfg>
```

There are also some additional parameters that require configuring depending on the type of receiver, which modify the behavior of the said receiver.

Sur-Gard Receiver

For Sur Gard, you can select the emulated receiver type from between MLR2000/MLR2E v1.2 and DLR-2. Default is MLR2000/MLR2E v1.2.

To emulate MLR2000/MLR2E v1.2, execute the following command:

```
PRIMARY ARLY-1 Cfg>alarm-receiver parameters r=0
PRIMARY ARLY-1 Cfg>
```

To emulate DLR-2, execute:

```
PRIMARY ARLY-1 Cfg>alarm-receiver parameters r=1
PRIMARY ARLY-1 Cfg>
```

Radionics 6500 Receiver

The following additional parameters require configuring when emulating a Radionics 6500:

- a: message ACK. Default is 6.
- n: message NACK. Default is 15.
- h: start of message: Default is not configured.
- t: end of message. Default is 14.

In all cases, the ASCII code for the character to be used is configured in decimal format.

The example below shows a configuration with values ACK 8, NACK 20, start of message 7 and end of message 16.

```
PRIMARY ARLY-1 Cfg>ALARM-RECEIVER PARAMETERS a=8,n=20,h=7,t=16
PRIMARY ARLY-1 Cfg>
```

Ademco 685 Receiver

If the emulated receiver is an Ademco 685, you can configure the following parameters:

- t: end of message. Default is 13. The ASCII code for the character to be used is configured in decimal format.
- p: Uses the ack/nack protocol for message exchange: 0 means it is not used, 1 it is used.

The following example shows the command to configure the Ademco 685 receiver with ACK/NACK:

```
PRIMARY ARLY-1 Cfg>ALARM-RECEIVER PARAMETERS p=1
PRIMARY ARLY-1 Cfg>
```

Once you have configured the type of receiver and the additional parameters, you need to configure the receiver identification. This identification is made up of two numbers: the receiver number and the line or group number. The receiver number uniquely identifies each of the receivers connected to an alarm server with the automation software. The line number identifies each of the line cards connected to the receiver. In the VisorALARM PLUS 2U, as communication is through an IP network, there are no line cards; however you must configure a line number as the said number is sent from the receiver to the server with the alarms.

The Sur-Gard receivers accept receiver numbers from 01 to FF, and line number from 1 to E. If the receiver is a Radionics 6500, the receiver identifier is a number from 00 to 99 and the line identifier is from 1 to 8. Lastly, if the receiver is an Ademco 685, the receiver number is from 0 to 9 and the line number is from 1 to 8.

The commands to configure these parameters are shown below, using **1** as the receiver number and **2** as the line number. Substitute these numbers for those corresponding to the installation you are implementing.

```
PRIMARY ARLY-1 Cfg>alarm-receiver receiver-id 1
PRIMARY ARLY-1 Cfg>alarm-receiver line-id 2
PRIMARY ARLY-1 Cfg>
```

Finally, you can configure the number of seconds between line tests sent from the VisorALARM PLUS 2U to the alarm server. The command used to configure this parameter is displayed below. In this example, this has been configured to **30** seconds. Substitute this value if you wish.

```
PRIMARY ARLY-1 Cfg>alarm-receiver link-test-timer 30
PRIMARY ARLY-1 Cfg>
```

WARNING: In UL Listed installations, the value for this parameter must be between 1 to 200 seconds.

5.2. Communicating with the Automation Server

Communication with the alarm automation server is carried out, as already said, through an asynchronous serial port. So the communication operates correctly, both ends (the VisorALARM PLUS 2U and the server) must have the same said serial line configuration. The parameters requiring configuration are as follows:

- Speed: common values are 110, 300, 600, 1200, 2400, 4800, 9600, 14400, 19200, 38400, 57600 or 115200.
- Number of data bits: normally 7 or 8.
- Parity type: Even, odd or none.
- Number of stop bits: 1 or 2.

Sur-Gard receivers normally use a speed of 9600, 7 data bits, even parity and one stop bit. Radionics 6500 respectively use 1200, 7, even and 2, for the said parameters. Ademco receivers use 685, 600, 8 without parity and 1, respectively.

The example given below shows these parameters configured at speed 1200, 7 data bits, even parity and 2 stop bits.

```
PRIMARY ARLY-1 Cfg>serial-parameters speed 1200
PRIMARY ARLY-1 Cfg>serial-parameters data-bits 7
PRIMARY ARLY-1 Cfg>serial-parameters parity even
PRIMARY ARLY-1 Cfg>serial-parameters stop-bits 2
```

Valid values for speed are from 300 to 115200. Data bits: 5, 6, 7 or 8. Parity: even, odd or none. Finality the stop bits valid values are 1 or 2.

5.3. Communication parameters with the printer

Connection to the printer is carried out through an asynchronous serial port. So the communication works correctly, both ends (the VisorALARM PLUS 2U and the printer) must have the same configuration in the serial line. Parameters requiring configuration are:

- Speed: common values are 110, 300, 600, 1200, 2400, 4800, 9600, 14400, 19200, 38400, 57600 or 115200.
- Number of data bits: normally 7 or 8.
- Parity Type: Even, odd or none

- Number of stop bits: 1 or 2

Check the printer manual to find out which parameters should be configured for your specific printer model.

Below you can see an example configuring these parameters: speed 9600, 8 data bits, without parity and 1 stop bit.

```
PRIMARY SEPI-serial0/1 Cfg>serial-parameters speed 9600
PRIMARY SEPI-serial0/1 Cfg>serial-parameters data-bits 8
PRIMARY SEPI-serial0/1 Cfg>serial-parameters parity none
PRIMARY SEPI-serial0/1 Cfg>serial-parameters stop-bits 1
```

Values valid for speed are from 300 to 115200. For the data bits 5, 6, 7, or 8. For parity, "even", "odd" or "none" and finally for the stop bits 1 or 2.

5.4. Communicating with the mIP/IPDACTs

Another aspect requiring configuration is the communication between the VisorALARM PLUS 2U and the mIP/IPDACTs. The parameters requiring configuration are as follows:

- VisorALARM PLUS 2U UDP port to which the mIP/IPDACTs send alarms and supervision traffic.
- Set time period to assume an mIP/IPDACT is "lost": if after this configured time, supervision traffic is not received from an mIP/IPDACT, an alarm (whose code is configurable) is sent to the automation server as there is a probable communication problem with the said mIP/IPDACT.

It is essential that this time is greater than the time between mIP/IPDACT retries to those providing the service in order to avoid 'false' alarms.

- IP address to check VisorALARM PLUS 2U IP connectivity: the device sends ICMP echo packets to the configured address. In cases where responses are not received, IP connection is considered lost and the device notifies the automation server through an event (whose code is configurable). mIP/IPDACT supervision is cancelled until connectivity is recovered to avoid loss of connectivity alarms being sent by each registered mIP/IPDACT. Additionally, you need to configure how often the connectivity should be polled.

Use the following command to configure the UDP port:

```
PRIMARY ARLY-1 Cfg>supervision port 1234
PRIMARY ARLY-1 Cfg>
```

The following command configures the address to poll the IP connectivity and the polling interval:

```
PRIMARY ARLY-1 Cfg>monitor-ip-addr 213.4.21.187 rate 30
PRIMARY ARLY-1 Cfg>
```

5.5. Network Backup Parameters

Network backup is the possibility of the mIP/IPDACT having a second receiver to send alarms to and keep-alive polls. From the VisorALARM PLUS 2U point of view, network backup consists of two devices, one configured as main and the other as secondary or backup. Both devices should have different gateways and if possible different Internet access providers. In this way, the possible problems of communications between the two devices are isolated.

Use the following syntax to configure each of the backup parameters:

```
PRIMARY ARLY-1 Cfg> backup-alarm-receiver option value
```

The available options are as follows:

- type: Defines the type of VisorALARM PLUS 2U. This can be main, secondary (backup) or maintenance. The mIP/IPDACT will always try and send alarms to the VisorALARM PLUS 2U configured as main. If the alarms do not reach this device, the mIP/IPDACT will send them to the backup device. Anyway, alarms are also sent to the maintenance receiver if it is configured. Once the type of VisorALARM PLUS 2U has been defined, the S LED will light up in green on the main and maintenance, and in yellow on the backup.
- address-main: This is the main VisorALARM PLUS 2U public address. This parameter is only used in the backup VisorALARM PLUS 2U.
- sync-port: This is the TCP port that listens in the main VisorALARM PLUS 2U to which the backup VisorALARM PLUS 2U connects each time the configurations need to be synchronized. Synchronizations are always produced each time either of the two VisorALARM PLUS 2U starts up and periodically once both are operating.
- poll-time: This is the time where the backup VisorALARM PLUS 2U periodically polls the main device to check its status.
- poll-failure-time: This is the time period within which the backup VisorALARM PLUS 2U considers that responses to the polls should have arrived. If during this period a response has not arrived, then a problem has possibly occurred, either in the communication or in the main VisorALARM PLUS 2U. The backup device will then begin a process of retries until the main device is considered down. The backup subsequently activates. In cases where the main device is considered down the backup device will signal the 399 event code (Primary VisorALARM down).
- retries-number: This is the number of necessary polling retries in order to consider that the main device is down.
- retry-time: Time between retries.
- polling-sync-time: Time between configuration synchronizations. This value is fixed to 30 seconds for the main receiver. For the secondary receiver this value can be programmed to a different value. Modifications in the configuration of either of the two devices, main and backup, are saved with a time mark associated. When the timer reaches the programmed time, a check is carried out to see if it is necessary to execute synchronization and if necessary this is executed.

The right election of the previous values is fundamental for the correct operation of the backup process. Specifically, these parameters affect the detection of service interruption for both the main and the backup receivers.

However, a receiver could decide that its complementary receiver (main or backup) has a failure as the polling between them has been interrupted, however that polling could have failed because the receiver itself doesn't have the Ethernet up or because it doesn't have Internet access.

So, it is very important that detection of poll failure is slower than detection of failure in the Ethernet interface or the Internet.

As guide to choose an adequate set of parameters it is strongly recommended that the values meet the following conditions:

Main VisorALARM PLUS 2U receiver:

$$2 \times POLL\text{-}TIME > 15^{1}$$

2 x POLL-TIME > 3 x MONITOR-IP-ADDRESS-RATE[2]

Backup VisorALARM PLUS 2U receiver:

POLL-FAILURE-TIME + RETRIES-NUMBER * RETRY-TIME > 15[1]

POLL-FAILURE-TIME + RETRIES-NUMBER * RETRY-TIME > 3 x MONITOR-IP-ADDRESS-RATE[2]

NOTES:

[1] The value 15 is the time in seconds that the equipment takes in detecting a failure in the Ethernet interface.

[2] MONITOR-IP-ADDRESS-RATE is the poll time of an external server in the Internet. It must be configured according with the MONITOR-IP-ADDR paragraph.

The default values for these parameters meet the previous conditions.

5.6. Maintenance Receiver

A maintenance alarm receiver permits you to configure the system so the trouble signals from the mIP/IPDACT devices are received and processed in an alternative location where the maintenance receiver is.

In addition to correctly configuring the 'mnt-ip-address' and 'mnt-password' parameters for the mIP/IPDACT device (see section 5.8) you must also configure the maintenance receiver to filter all the received signals except for the trouble ones.

Use the following command to configure a maintenance receiver so it only processes trouble signals:

```
PRIMARY ARLY-1 Cfg>alarm-receiver block alarm-signals
```

In the main and secondary receiver, filter the trouble signals through the following command:

```
PRIMARY ARLY-1 Cfg>alarm-receiver block trouble-signals
```

WARNING: For UL Listed Fire installations where you wish to transmit supervisory and trouble conditions to a location separate from that to which alarm signals are transmitted, you must have a maintenance VisorALARM PLUS 2U configured as already shown in this point. In the same way, the main and secondary VisorALARM PLUS 2U must be configured complying with this said point in order to block the trouble signals.

5.7. User Configurable Events

As previously mentioned, there are various situations where the VisorALARM PLUS 2U generates alarms which are sent to the automation software to notify the operator of the existence of certain situations. The event codes used are configurable, through the commands given below.

To configure the event code sent when connectivity is lost with an mIP/IPDACT, use the following command (the default value for this parameter is 350).

```
PRIMARY ARLY-1 Cfg> user-defined-events mip-loss 350
PRIMARY ARLY-1 Cfg>
```

To configure the event code sent when there is an IP connectivity problem in the VisorALARM PLUS 2U, use the following command (the default value for this parameter is 356).

```
PRIMARY ARLY-1 Cfg> user-defined-events network-failure 357
PRIMARY ARLY-1 Cfg>
```

Lastly, to configure the event code sent when an mIP/IPDACT installation (register) packet is received, the following command is used (the default value for this parameter is 531).

```
PRIMARY ARLY-1 Cfg> user-defined-events mip-registration 352
PRIMARY ARLY-1 Cfg>
```

5.8. Configuration pattern

To simplify the mIP/IPDACT installation task, the VisorALARM PLUS 2U has a feature which permits you to install an mIP/IPDACT by configuring a reduced set of parameters. Through a "register" operation you then receive the rest of the configuration from the VisorALARM PLUS 2U. The complete process is described below:

- The installer configures the following parameters in the mIP/IPDACT either through a serial console or telephone console:
  - Client account number
  - IP address and mask
  - Default gateway IP address
  - VisorALARM PLUS 2U public IP address
  - VisorALARM PLUS 2U UDP port
- Restart the mIP/IPDACT.
- Execute the "register" command, introducing the installer password.
- The mIP/IPDACT sends a "register" command to the VisorALARM PLUS 2U configured address and port, encrypting with the installer password.
- The VisorALARM PLUS 2U receives the message. It checks the configuration pattern list it has configured and tries to decode the message with the password for each pattern. If the message decodes correctly, the device assumes that it is this pattern it has to use and generates a configuration for the said mIP/IPDACT based on the configuration pattern parameters.
- Sends the configuration to the mIP/IPDACT, encrypted with the installer password.
- The mIP/IPDACT receives the configuration, activates it and subsequently saves it.

Therefore, you must configure at least one configuration pattern if you wish to use this type of installation. It makes sense to add more than one configuration pattern if you want to configure mIP/IPDACTs with different parameters.

It's possible to establish all the mIP/IPDACT parameters through configuration patterns with the exception of the client account number. However, you do not need to specify all the parameters which are configurable in an mIP/IPDACT, only those that you wish to change in the mIP/IPDACT. Those parameters which are not specified in the pattern remain configured in the mIP/IPDACT with the factory settings.

To create a configuration pattern, execute the following command. In this example, a pattern with identifier 5 will be created.

```
PRIMARY ARLY-1 Cfg>cfg-pattern 5 default
PRIMARY ARLY-1 Cfg>
```

To configure each of the parameters, use this syntax:

```
PRIMARY ARLY-1 Cfg>cfg-pattern 5 option value
```

The available options are all the mIP/IPDACT configuration parameters. These are detailed below. Some of the parameters the mIP/IPDACT uses with the main VisorALARM PLUS 2U, others with the backup device and others affect the maintenance VisorALARM PLUS 2U. The rest are common application.

- default: Creates a New pattern or sets the default values for an existing one.
- instalator-password: Establishes the installer password. This must be following by a string of up to 16 hexadecimal digits.
- receiver-ip: VisorALARM PLUS 2U public address (or behind which the VisorALARM PLUS 2U is located). This must be followed by an IP address.
- receiver-udp-port: UDP port where the VisorALARM PLUS 2U expects to receive the data. This must be followed by a number from 1 to 65535.
- usr-password: mIP/IPDACT console password. Must be followed by a 16-character string made up of hexadecimal digits or the letters UVWXYZ. The password sent to the mIP/IPDACT will be a string of 16 hexadecimal digits which is obtained by substituting the first digit of the mIP/IPDACT account number for the letter U, the V for the second and so on until Z for the sixth. I.e. if you configure 0000UVWXYZ, when you install the mIP/IPDACT whose account number is 123456, 0000123456 is sent as the user password. This way you can configure different passwords for each mIP/IPDACT using the same configuration pattern.
- mip-password: Password used by the mIP/IPDACT to encrypt the messages it sends. This must be followed by a password using the same form as the usr-password parameter.
- receiver-password: Password used by the VisorALARM PLUS 2U to encrypt the messages it sends. This must be followed by a password using the same format as the usr-password parameter.
- keep-alive-timer: Time between keepalives in seconds. This value must be between 0 and 90 seconds. Applied to the main VisorALARM PLUS 2U.
- keep-alive-retries: Number of keepalive retries in cases of failure. This value must be between 1 and 9. Applied to the main VisorALARM PLUS 2U.
- keep-alive-retries-timer: Time between keepalive retries in seconds. This value must be between 3 and 9 seconds. Applied to the main VisorALARM PLUS 2U.
- phone-length: Number of digits making up the telephone number called by the panel to send alarms.
- alarm-tx-retries: Number of alarm send retries in cases of failure. This is a number between 5 and 10.
- callback-phone[1]: Phone number that Alarm Panel dials to make a callback to the Central Station.
- bck-receiver-ip: Backup VisorALARM PLUS 2U IP address.
- bck-keep-alive-timer: This is the same keep-alive-timer option applied to the backup VisorALARM PLUS 2U.
- bck-keep-alive-retries: This is the same keep-alive-retries option applied to the backup VisorALARM PLUS 2U.

[1] Not available in US versions

- bck-keep-alive-retries-time: This is the same keep-alive-retries-time option applied to the backup VisorALARM PLUS 2U.

WARNING: In UL listed installations, the values for the keep-alive-timer', 'keep-alive-retries' and 'keep-alive-retries-timer' parameters are subject to restrictions.

UL1610 Installations:

keep-alive-timer + (keep-alive-retries * keep-alive-retries-timer) < 200

- mnt-ip-address: The is the maintenance VisorALARM PLUS 2U public address.
- mnt-password: Password used by the mIP/IPDACT to encrypt the messages sent to the maintenance receiver. It takes the same format as the usr-password parameter.

WARNING: For UL Listed installation where you wish to transmit supervisory and trouble conditions to a location separate from that to which alarm signals are transmitted, must have the mnt-ip-address and mnt-password parameters configured.

Subsequently the commands to configure a configuration pattern, with identifier 1, are shown. In this said pattern the VisorALARM PLUS 2U IP address and UDP port parameters have not been configured as they are already configured in the mIP/IPDACT (these are required for installation purposes) and do not require changing.

```
PRIMARY ARLY-1 Cfg>cfg-pattern 1 default
PRIMARY ARLY-1 Cfg>cfg-pattern 1 instalator-password 1234
PRIMARY ARLY-1 Cfg>cfg-pattern 1 usr-password 654321
PRIMARY ARLY-1 Cfg>cfg-pattern 1 mip-password 1234WXYZ90
PRIMARY ARLY-1 Cfg>cfg-pattern 1 receiver-password 0W8X6Y4Z2FEBA
PRIMARY ARLY-1 Cfg>cfg-pattern 1 keep-alive-timer 60
PRIMARY ARLY-1 Cfg>cfg-pattern 1 keep-alive-retries 2
PRIMARY ARLY-1 Cfg>cfg-pattern 1 keep-alive-retries-timer 3
PRIMARY ARLY-1 Cfg>cfg-pattern 1 phone-length 9
PRIMARY ARLY-1 Cfg>cfg-pattern 1 alarm-tx-retries 2
PRIMARY ARLY-1 Cfg>cfg-pattern 1 bck-receiver-ip 80.36.189.123
PRIMARY ARLY-1 Cfg>cfg-pattern 1 bck-keep-alive-timer 5
PRIMARY ARLY-1 Cfg>cfg-pattern 1 bck-keep-alive-retries 2
PRIMARY ARLY-1 Cfg>cfg-pattern 1 bck-keep-alive-retries 2
PRIMARY ARLY-1 Cfg>
```

If you do wish to change one of the options, simply introduce the configuration command that configures this with the new value. E.g.

```
PRIMARY ARLY-1 Cfg>cfg-pattern 1 keep-alive-retries-timer 2
PRIMARY ARLY-1 Cfg>
```

If you wish to leave one of the options with its default value, enter "no" followed by the command used to configure this. E.g.

```
PRIMARY ARLY-1 Cfg>no cfg-pattern 1 keep-alive-retries-timer 2
PRIMARY ARLY-1 Cfg>
```

Lastly, in order to completely delete a pattern, enter the command:

```
PRIMARY ARLY-1 Cfg>no cfg-pattern 5 default
PRIMARY ARLY-1 Cfg>
```

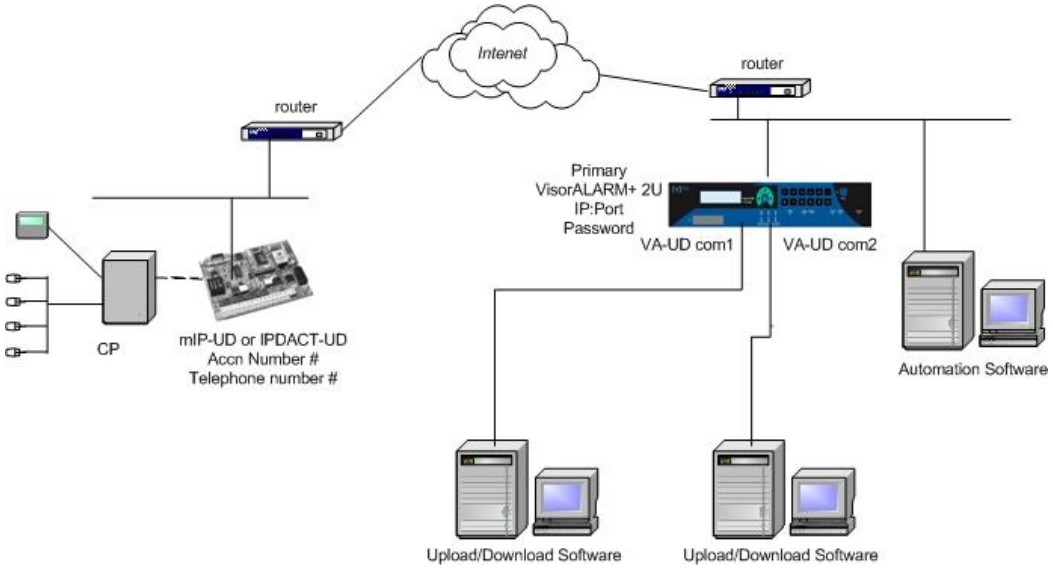
Once an mIP/IPDACT has registered, it saves the configuration in the ARLY interface configuration so that it remains between VisorALARM PLUS 2U reboots.

5.9. Upload/Download operation

The Upload/Download of a VisorALARM PLUS 2U receiver allows to establish management sessions from the currently available Upload/Download Software Packages to the Control Panels through Internet.

Usually, the system is composed by two workstations running Upload/Download software and connected through a Serial Port to a VisorALARM PLUS 2U receiver (VA-UD com1 and VA-UD com2) by means of the supplied Micro DB9 to DB9 cables. The VisorALARM is connected to Internet as usual.

In the client side a mIP-UD or IPDACT-UD device is connected to a Control Panel.



The VisorALARM emulates a modem in such a way that it responds to the AT commands that sends the Upload/Download Software in order to establish a call with the Control Panel.

The mIP/IPDACT-UD board has a built in V32 modem capable to establish a call with the Control Panel through the TO-AP interface.

When a call is requested the VisorALARM sends an order to the mIP/IPDACT device to establish the call with the Control Panel, then if the Control Panel accepts the call, the modems starts the negotiation and if it finish successfully a data call is established.

From this moment exchanged data between Control Panel and mIP/IPDACT are relayed through Internet to the VisorALARM receiver that sends/receives the data to/from the Upload/Download software through the Serial Port.

In order to interface with the Upload/Download software the VA-UD com ports of the VisorALARM PLUS 2U receiver must be programmed with the suitable serial port speed.

To change the speed of the serial ports used for Upload/Download, use the NETWORK command and the serial line associated to the Modem Emulation interfaces:

```
PRIMARY Config>list dev

Interface            Connector     Type of interface
ethernet0/0          FE0/LAN1      Fast Ethernet interface
ethernet0/1          FE1/LAN2      Fast Ethernet interface
serial0/0            SERIAL0/WAN1  ARLY Async Line
serial0/1            SERIAL1/WAN2  X25
x25-node             ---           Router->Node
serial1/0            SLOT1         AT Modem Emulation Interface (COM1)
serial1/1            SLOT1         AT Modem Emulation Interface (COM2)

PRIMARY Config>net serial1/0

-- MODEMEMU Interface Configuration --
PRIMARY MODEMEMU-serial1/0 Cfg>speed ?
  <300..115200>    Enter link speed
PRIMARY MODEMEMU-serial1/0 Cfg>speed 9600
PRIMARY MODEMEMU-serial1/0 Cfg>
```

Then use the command speed to set the serial port speed for the communications with the Management Computer.

To link a Control Panel Phone Number with a mIP/IDPACT device you must configure the number that the Upload/Download software will dial to communicate with the Control Panel for the associated mIP/IPDACT device.

This number ("Subscriber Telephone") is configured for each registered mIP by means of the command "subscriber-telephone"

```
PRIMARY ARLY-2 Cfg>mip <accountNumber> subscriber-telephone <phoneNumber>
```

Usually, it is necessary to program the Upload/Download software with a specific set of AT Initialization Strings to be used with VisorALARM PLUS 2U receivers. The next table shows the initialization strings for the supported Control Panels.

Software	AT Initialization strings		Serial Port Speed
PK-PLUS 9200UD, 9600 Fire-Lite	Initialization String: Hang-Up String:	&F;L1;F0;M1;E0;S7=255 H0	19200
WinLoad Digiplex, Spectra PARADOX	Initialization String 1: Initialization String 2: Initialization String 3:	Z0Q0E0V1S9=1&C0 F1B1S7=255S10=255T S13=1S17=2	300
Compass Vista ADEMCO	Initialization String 1: Initialization String 2: Initialization String 3: Initialization String 4: Reset String:	VEQ B1F1 S7=110S10=119&C1&D2&QX S13=3S15=5S17=1S19=8 Z	300
DL900 NetworX	Initialization String1: Initialization String2:	Q0E0V1S19=1 F1S7=255S10=255TS17=0	300

General Electric			
Comax HUNTER PRO 32 PIMA	Initialization String: Init. String (callback):	`F1S0=0S10=250S7=60S9=1` `F1S0=1S10=250S7=60S9=1`	300
RP Infinite Electronic Line	Default Initialization:	`E0V1S0=0`	As Windows Setup

Initialization modem strings for supported Upload/Download software packages

6. Final Adjustments

To finalize this process, we recommend enabling the ARLY interface events. These will help when diagnosing possible problems. To do this, execute the commands shown below:

```
PRIMARY ARLY-1 Cfg>exit
PRIMARY Config>event

-- ELS Config --
PRIMARY ELS config>enable trace subsystem arly all
PRIMARY ELS config>exit
PRIMARY Config>
```

In addition, it is possible to receive the events in a PC in order to store them for subsequent processing. This is achieved through the "syslog" functionality and requires a "syslog" server to be installed in a PC where you wish to receive the events (there are various free "syslog" servers available). To enable the ARLY events so they can be sent to a "syslog" server, execute the following command in the events menu:

```
PRIMARY ELS config>enable syslog subsystem arly all
PRIMARY ELS config> exit
PRIMARY Config>
```

It is also necessary to enable the "syslog" functionality and configure the address where the traces will be sent.

```
PRIMARY Config>feature syslog

-- SYSLOG client configuration --
PRIMARY SYSLOG config>
PRIMARY SYSLOG config>enable
PRIMARY SYSLOG config>server 172.24.51.51
PRIMARY SYSLOG config>exit
PRIMARY Config>
```

Lastly you need to save the configuration and restart the device so this activates. To exit the configuration menu after saving, press the 'CTRL' and the 'P' keys simultaneously.

```
PRIMARY Config>save
Save configuration (Yes/No) [No]? y
OK on Flash (not saved in SmartCard)
PRIMARY Config>
PRIMARY *restart
Are you sure to restart the system(Yes/No)? y

Restarting. Please wait ..............................................
APP DATA DUMP.....................................
Running application
Flash configuration read
Initializing

User:
```

7. Example

The aim of this example is to provide a view on the whole of the mIP/IPDACT installation process and system behavior during normal operation. The idea is as follows: a traditional security scenario wishes to adopt the Teldat solution which permits alarms from the control panel to be sent over IP and similarly supervise the connection.

To do this, a VisorALARM PLUS 2U is installed in the Alarm Receiver Center. The VisorALARM PLUS 2U operates as a Sur-Gard receiver. The emulated receiver configuration parameters are as follows: receiver ID is 6, line identifier 10, link-test 120 seconds, serial line is configured at 19200 bauds, 7 data bits, even parity and two stop bits.

On the client side, there is an alarm control panel whose account number is 1234. The mIP/IPDACT is installed next to this as described in the mIP/IPDACT installation manual. In Figure 8 the implicated devices are displayed.

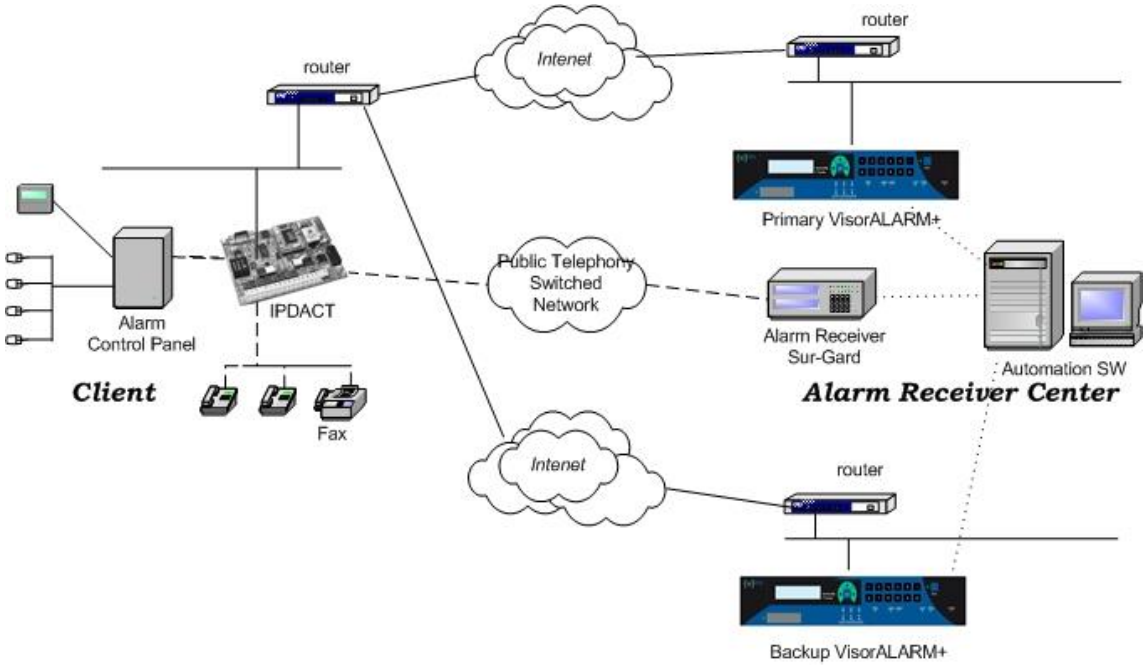


Figure 8. Example

The mIP/IPDACTs supervision interval will be one minute i.e. if this interval times out without received any response, a communication failure alarm is generated in the ARC Automation Software.

As regards the mIP/IPDACTs, you want to use passwords dependent on the account number (the mIP/IPDACT uses 00ZYXWV99, the VisorALARM PLUS 2U with this mIP/IPDACT uses 987ZZYYXX89, the console password is 5432Z), the number of retries when faced with a connectivity failure is 4 and the time between retries is one second. The number of retries when there are problems transmitting alarms is 3. Finally you need to configure the numeration plan value in the mIP/IPDACTs (number of digits making up a telephone number) to 7. The installer password is 99887766.

a) VisorALARM PLUS 2U initial configuration

Before installing any mIP/IPDACT, you need to configure the VisorALARM PLUS 2U.

The VisorALARM PLUS 2U needs to be configured to interact firstly with the mIP/IPDACTs so these can be registered and supervised, and secondly with the ARC Automation Sw. Additionally, in cases where the network backup functionality is installed, you need to configure the backup and the NTP client parameters.

In order to interact with the mIP/IPDACTs, it is essential that the VisorALARM PLUS 2U is accessible through IP and UDP. As regards IP, an IP address and mask must be configured in the VisorALARM PLUS 2U. In this example, the address is public and is the same as the one configured in the mIP/IPDACTs. A route is aggregated so that all the traffic is routed through the access gateway. As a result the IP configuration is:

```
Config>protocol ip

-- Internet protocol user configuration --
IP config>address ethernet0/0 172.28.1.30 255.255.0.0
IP config>address ethernet0/0 215.99.32.3 255.255.255.0
IP config>route 0.0.0.0 0.0.0.0 172.28.1.1 1
IP config>
```

In cases of network backup, you need to configure the NTP clients in both devices. The configuration is as follows:

```
Config>feature ntp

-- NTP Protocol user configuration --
NTP config>protocol
NTP config>source-address 215.99.32.3
NTP config>peer address 1 18.145.0.30
NTP config>
```

Together with the NTP client, you need to configure the backup parameters. For the VisorALARM PLUS 2U selected as main, the configuration is:

```
Config>net serial0/0
ARLY-1 Cfg>backup-alarm-receiver sync-port 20300
ARLY-1 Cfg>
```

The same port for supervision has been selected for the configuration synchronization port with the aim of not having to enable another transparent port in the input router.

For the VisorALARM PLUS 2U selected as the backup, the configuration is as follows:

```
Config>net serial0/0
ARLY-1 Cfg>backup-alarm-receiver type secondary
ARLY-1 Cfg>backup-alarm-receiver address-main 215.99.32.3
ARLY-1 Cfg>backup-alarm-receiver sync-port 20300
ARLY-1 Cfg>backup-alarm-receiver poll-failure-time 2
ARLY-1 Cfg>backup-alarm-receiver retries-number 2
ARLY-1 Cfg>backup-alarm-receiver retry-time 2
```

In order to use the UDP, it is necessary to configure the UDP port number that is going to be used. If you are going to use port 20300, the configuration is as follows:

```
IP config>exit
Config>net serial0/0

-- ARLY Interface Configuration --
ARLY-1 Cfg>supervision port 20300
ARLY-1 Cfg>
```

For interaction with the Automation Sw, you need to configure two distinct aspects in the ARLY interface: that relative to the communication and that relative to the type of receiver going to be emulated. If the VisorALARM PLUS 2U behaves as a Sur-Gard receiver where the receiver identifier

is 6, line identifier 10 and the communication data is that shown in the figure, the configuration is as follows:

```
ARLY-1 Cfg>alarm-receiver protocol sur-gard
ARLY-1 Cfg>alarm-receiver receiver-id 6
ARLY-1 Cfg>alarm-receiver line-id 10
ARLY-1 Cfg>alarm-receiver link-test-timer 120
ARLY-1 Cfg>serial-parameters speed 19200
ARLY-1 Cfg>serial-parameters data-bits 7
ARLY-1 Cfg>serial-parameters parity even
ARLY-1 Cfg>serial-parameters stop-bits 2
ARLY-1 Cfg>
```

Up to this point, everything configured can be viewed through the **SHOW CONFIG** command, which for the main VisorALARM PLUS 2U is:

```
Config>show config
; Showing System Configuration for access-level 15 ...
; VISORALARM-PLUS US Router 6 120 Version 10.6.27

log-command-errors
no configuration
description "Default configuration: VisorALARM standard"
set data-link arly serial0/0
set data-link sepi serial0/1
set data-link modem-emu serial1/0
set data-link modem-emu serial1/1
set sram-size 1024
cfg-mode binary
;
; -- Privilege Configuration --
set privilege 9 ">time" all
;
;
user manager password 24680
;
user supervisor password 13579
user supervisor access-level 9
;
user operator password 11111
user operator access-level monitor
;
network serial0/0
; -- ARLY Interface Configuration --
   alarm-receiver receiver-id 6

   alarm-receiver line-id 10
   alarm-receiver link-test-timer 120
;
   backup-alarm-receiver sync-port 20300
;
   supervision port 20300
   supervision rate 60
;
;
   serial-parameters data-bits 7
   serial-parameters parity even
   serial-parameters speed 19200
   serial-parameters stop-bits 2
exit
;
;
protocol ip
; -- Internet protocol user configuration --
   address ethernet0/0 172.28.1.30 255.255.0.0
   address ethernet0/0 215.99.32.3 255.255.255.0
;
;
   route 0.0.0.0 0.0.0.0 172.28.1.1 1
;
exit
;
dump-command-errors
end
; --- end ---
Config>
```

And for the backup VisorALARM PLUS 2U,

```
Config>show config
; Showing System Configuration for access-level 15 ...
; VISORALARM-PLUS US Router 6 120 Version 10.6.27

log-command-errors
no configuration
description "Default configuration: VisorALARM standard"
set data-link arly serial0/0
set data-link sepi serial0/1
set data-link modem-emu serial1/0
set data-link modem-emu serial1/1
set sram-size 1024
cfg-mode binary
;
; -- Privilege Configuration --
set privilege 9 ">time" all
;
;
user manager password 24680
;
user supervisor password 13579
user supervisor access-level 9
;
user operator password 11111
user operator access-level monitor
;
network serial0/0
; -- ARLY Interface Configuration --
   alarm-receiver receiver-id 6
   alarm-receiver line-id 10
   alarm-receiver link-test-timer 120
;
   backup-alarm-receiver type secondary
   backup-alarm-receiver address-main 80.26.96.183
   backup-alarm-receiver sync-port 1234
   backup-alarm-receiver poll-failure-time 2
   backup-alarm-receiver retries-number 2
   backup-alarm-receiver retry-time 2
;
   supervision port 20300
   supervision rate 60
;
;
   serial-parameters data-bits 7
   serial-parameters parity even
   serial-parameters speed 19200
   serial-parameters stop-bits 2
exit
;
;
protocol ip

; -- Internet protocol user configuration --
   address ethernet0/0 172.28.1.30 255.255.0.0
   address ethernet0/0 215.99.32.3 255.255.255.0
;
;
   route 0.0.0.0 0.0.0.0 172.28.1.1 1
;
exit
;
dump-command-errors
end
; --- end ---
Config>
```

When a parameter is not displayed, this means it coincides with a configuration default value. The configuration must be saved and the device restarted to activate the said configuration.

```
Config>save
Save configuration (Yes/No) [No]? y

Performing memory requirements calculations, please wait
Building system configuration, please wait
Configuration built, saving ...
OK on Flash
Config>
*restart
Are you sure to restart the system(Yes/No)? y
```

At this point you can check various aspects, both for the main and the backup devices. To simplify this, the checks are indicated for the main VisorALARM PLUS 2U; however they are also directly applicable to the backup.

Firstly check the status of the Automation Sw connection through the serial line. If there are no signals, the AUT LED will be red; if there are, the AUT LED is yellow. The signals status can be checked in the following way:

```
*p 3
Console Operator
+device serial0/0

                                    Auto-test   Auto-test     Maintenance
Interface            CSR    Vect      valids    failures        failures
serial0/0       FA200A00      5e           0           0               0
 Interface DCE
   V.24 circuits:105 106 107 108 109 125 141
   Nicknames:    RTS CTS DSR DTR DCD RI  LL
   State:        ON  ON  ON  ON  ON  --- ---

Speed   (bps)            =      19200
Throughput (bps)         =          0
Last throughput (bps)    =          0
Bits per character       =          7
Stop bits                =          2
Parity selected          =       EVEN
Parity errors            =          0
Data errors              =          0
Overrun errors           =          0
Last reset               = 11 minutes 12 seconds
+
```

When the Automation Sw responds to the link tests, the AUT LED lights up in green. If you enable the ARLY interface events and display them on screen, you can check the whole connection establishment send process. Additionally, if you wait for the time between *link-tests*, the heartbeat frames transmission and the response reception are checked.

```
+event

-- ELS Monitor --
ELS>enable trace subsystem arly all
ELS>view
ELS>09/01/03 16:12:20  GW.001 Copyright Teldat 2006
09/01/03 16:12:20  GW.002 Portable CGW VISORALARM-PLUS US Rel 10.6.27-Alfa strtd
09/01/03 16:12:20  GW.005 Bffrs: 2000 avail 2000 idle   fair 222 low 400
09/01/03 16:13:22  ARLY.008 FMS st 0 ev 0
09/01/03 16:13:22  ARLY.005 SL Tx Heartbeat
09/01/03 16:13:22  ARLY.004 SL Rx ACK
09/01/03 16:13:22  ARLY.008 FMS st 1 ev 1
09/01/03 16:15:23  ARLY.008 FMS st 2 ev 7
09/01/03 16:15:23  ARLY.005 SL Tx Heartbeat
09/01/03 16:15:23  ARLY.004 SL Rx ACK
09/01/03 16:15:23  ARLY.008 FMS st 3 ev 1
```

Another aspect that you can check is the IP connectivity. You need to check that the LAN LED is green and that the configured access gateway is correctly accessed. This can be done through the ping command, available from any console process in the device:

```
ELS>ping 172.28.1.1

PING 172.28.1.1: 56 data bytes
64 bytes from 172.28.1.1: icmp_seq=0. time=0. ms
64 bytes from 172.28.1.1: icmp_seq=1. time=0. ms
64 bytes from 172.28.1.1: icmp_seq=2. time=0. ms
64 bytes from 172.28.1.1: icmp_seq=3. time=0. ms

----172.28.1.1 PING Statistics----
4 packets transmitted, 4 packets received, 0% packet loss
round-trip (ms)  min/avg/max = 0/0/0
ELS>
```

Press the space bar to halt this process.

As regards the backup, it is a good idea to execute a ping from the backup device to the main VisorALARM PLUS 2U public address.

b) Configuring the configuration patterns in the VisorALARM PLUS 2U

Using configurations patterns permit you to automate the mIP/IPDACTs installation process and registration. All the parameters required by an mIP/IPDACT to run correctly are specified in these patterns. Adjusting to the parameters specified in the example and assigning all the configuration to pattern 10, the said pattern configuration will be:

```
ARLY-1 Cfg>cfg-pattern 10 default
ARLY-1 Cfg>cfg-pattern 10 default
ARLY-1 Cfg>cfg-pattern 10 instalator-password 99887766
ARLY-1 Cfg>cfg-pattern 10 receiver-ip 215.99.32.3
ARLY-1 Cfg>cfg-pattern 10 receiver-udp-port 20300
ARLY-1 Cfg>cfg-pattern 10 usr-password 5432Z
ARLY-1 Cfg>cfg-pattern 10 mip-password 00ZYXWV99
ARLY-1 Cfg>cfg-pattern 10 receiver-password 987ZZYYXX89
ARLY-1 Cfg>cfg-pattern 10 keep-alive-timer 45
ARLY-1 Cfg>cfg-pattern 10 keep-alive-retries 4
ARLY-1 Cfg>cfg-pattern 10 keep-alive-retries-timer 1
ARLY-1 Cfg>cfg-pattern 10 phone-length 7
ARLY-1 Cfg>cfg-pattern 10 alarm-tx-retries 3
ARLY-1 Cfg>cfg-pattern 10 bck-receiver-ip 215.99.32.3
ARLY-1 Cfg>cfg-pattern 10 bck-keep-alive-timer 5
ARLY-1 Cfg>cfg-pattern 10 bck-keep-alive-retries 2
ARLY-1 Cfg>cfg-pattern 10 bck-keep-alive-retries-time 2
ARLY-1 Cfg>
```

Subsequently the configuration, for the main VisorALARM PLUS 2U for example, will be:

```
CRA Config>show config
; Showing System Configuration for access-level 15 ...
; VISORALARM-PLUS US Router 6 120 Version 10.6.27

log-command-errors
no configuration
description "Default configuration: VisorALARM standard"
set data-link arly serial0/0
set data-link sepi serial0/1
set data-link modem-emu serial1/0
set data-link modem-emu serial1/1
set sram-size 1024
cfg-mode binary
;
; -- Privilege Configuration --
set privilege 9 ">time" all
;
;
user manager password 24680
;
user supervisor password 13579
user supervisor access-level 9
;
user operator password 11111
user operator access-level monitor
;
network serial0/0
; -- ARLY Interface Configuration --
   alarm-receiver receiver-id 6
   alarm-receiver line-id 10
   alarm-receiver link-test-timer 60
;
   backup-alarm-receiver sync-port 20300
;
supervision port 20300
   supervision rate 60
;
   cfg-pattern 10 default
   cfg-pattern 10 instalator-password 99887766
   cfg-pattern 10 receiver-ip 215.99.32.3
   cfg-pattern 10 receiver-udp-port 20300
   cfg-pattern 10 usr-password 5432Z
   cfg-pattern 10 mip-password 00ZYXWV99
   cfg-pattern 10 receiver-password 987ZZYYXX89
   cfg-pattern 10 keep-alive-timer 45
   cfg-pattern 10 keep-alive-retries 4
   cfg-pattern 10 keep-alive-retries-timer 1
   cfg-pattern 10 phone-length 7
   cfg-pattern 10 alarm-tx-retries 3
   cfg-pattern 10 bck-receiver-ip 215.99.32.3
   cfg-pattern 10 bck-keep-alive-timer 5
   cfg-pattern 10 bck-keep-alive-retries 2
   cfg-pattern 10 bck-keep-alive-retries-time 2
;
;

   serial-parameters data-bits 7
   serial-parameters parity even
   serial-parameters speed 19200
   serial-parameters stop-bits 2
exit
;
event
; -- ELS Config --
   enable trace subsystem ARLY ALL
exit
;
;
protocol ip
; -- Internet protocol user configuration --
   address ethernet0/0 172.28.1.30 255.255.0.0
   address ethernet0/0 215.99.32.3 255.255.255.0
;
```

```
;
   route 0.0.0.0 0.0.0.0 172.28.1.1 1
;
exit
;
dump-command-errors
end
; --- end ---
Config>
```

For validity purposes, save the configuration and restart the device.

```
ARLY-1 Cfg>exit
Config>save
Save configuration (Yes/No) [No]? y

Performing memory requirements calculations, please wait
Building system configuration, please wait
Configuration built, saving ...
OK on Flash
Config>
*restart
Are you sure to restart the system(Yes/No)? y
```

The pattern configuration can be repeated, if required, in the backup device. However, the synchronization software itself passes the VisorALARM PLUS 2U pattern configuration to the backup. Synchronization is not automatic; it depends on the `polling-sync-time` parameter which pertains to the backup parameters. The default value is 5 minutes. Consequently, the configuration changes which have been produced during this period are synchronized every five minutes, both in the main VisorALARM PLUS 2U and the backup.

c) *Installing and registering mIP/IPDACTs*

In the mIP/IPDACT, the installer must configure the mIP/IPDACT with the minimum installer configuration, as indicated in the mIP/IPDACT installation manual. The following parameters must be configured:

mIP/IPDACT IP address and mask:	192.168.80.100 255.255.255.0
mIP/IPDACT access gateway:	192.168.80.1
mIP/IPDACT account number:	101234
VisorALARM PLUS 2U IP address:	215.99.32.3
UDP port:	20300

Subsequently, the installer must proceed to the register using the password (99887766). If the ARLY interface events are enabled in the VisorALARM PLUS 2U, check for the arrival of the register petition and the sending of the configuration to the mIP/IPDACT, as well as the event sending which notifies the installation of a new mIP/IPDACT.

```
Config>09/02/03 09:01:28  ARLY.001 UDP Rx frm sz 80
09/02/03 09:01:28  ARLY.010 RSRVC Rx frm
09/02/03 09:01:28  ARLY.002 UDP Tx frm sz 152
09/02/03 09:01:28  ARLY.024 RREGSTR accnt 101234 inst 99887766
09/02/03 09:01:28  ARLY.008 FMS st 2 ev 8
09/02/03 09:01:28  ARLY.005 SL Tx 56 181234E53100000
09/02/03 09:01:29  ARLY.004 SL Rx ACK
09/02/03 09:01:29  ARLY.008 FMS st 4 ev 1
09/02/03 09:01:29  ARLY.020 STOR delete, 500 free
```

As a result of the register process, the mIP/IPDACT information is stored in the VisorALARM PLUS 2U so it is unnecessary to re-register the mIP/IPDACT if the VisorALARM PLUS 2U is restarted.

d) VisorALARM PLUS 2U normal functionality

On receiving the configuration from the VisorALARM PLUS 2U, the mIP/IPDACT tries to connect. If the ARLY interface events are enabled in the VisorALARM PLUS 2U, the connection petition (cntct) arrival and the sending of the response is checked.

```
09/02/03 09:35:57  ARLY.001 UDP Rx frm sz 80
09/02/03 09:35:57  ARLY.010 RSRVC Rx frm
09/02/03 09:35:57  ARLY.012 RSPVSN accnt 101234 cntct
09/02/03 09:35:57  ARLY.002 UDP Tx frm sz 56
09/02/03 09:35:57  ARLY.001 UDP Rx frm sz 32
09/02/03 09:35:57  ARLY.010 RSRVC Rx frm
09/02/03 09:35:57  ARLY.013 RSPVSN accnt 101234 alive
09/02/03 09:35:57  ARLY.002 UDP Tx frm sz 56
```

On receiving the response, the mIP/IPDACT transmits a *keep-alive* frame. Once the reply has been received, it switches the telephone relays and intercepts the control panel telephone line (the relay LEDs activate).

Once connection between the mIP/IPDACT and the VisorALARM PLUS 2U has been established, you can check the registered mIP/IPDACTs status from the monitoring process, as shown below:

```
*p 3
Console Operator
+net serial0/0
ARLY Monitoring
ARLY-1+list mip info
MIP Account[ffffffff]?
Account: 101234           State: alive
IP addr: 200.200.200.1    S/N: 0583/00251
Remote UDP port: 32770    Sw Rls: v4.1 US Oct 25 2006
Local UDP port:  20300

Keep-Alv tmr:    10       MIP pwd : 004321099
Keep-Alv retry:   5       Rcvr pwd: 98744332289
Keep-Alv_retry tmr:  3    Phone len: 7
Alarm retry:  5           Subs Phone:

ARLY-1+
```

If the ARLY interface events are enabled in the VisorALARM PLUS 2U, the *keep-alive* message reception and response to this is checked.

```
09/02/03 09:36:42  ARLY.001 UDP Rx frm sz 32
09/02/03 09:36:42  ARLY.010 RSRVC Rx frm
09/02/03 09:36:42  ARLY.013 RSPVSN accnt 101234 alive
09/02/03 09:36:42  ARLY.002 UDP Tx frm sz 56
09/02/03 09:37:27  ARLY.001 UDP Rx frm sz 32
09/02/03 09:37:27  ARLY.010 RSRVC Rx frm
09/02/03 09:37:27  ARLY.013 RSPVSN accnt 101234 alive
09/02/03 09:37:27  ARLY.002 UDP Tx frm sz 56
```

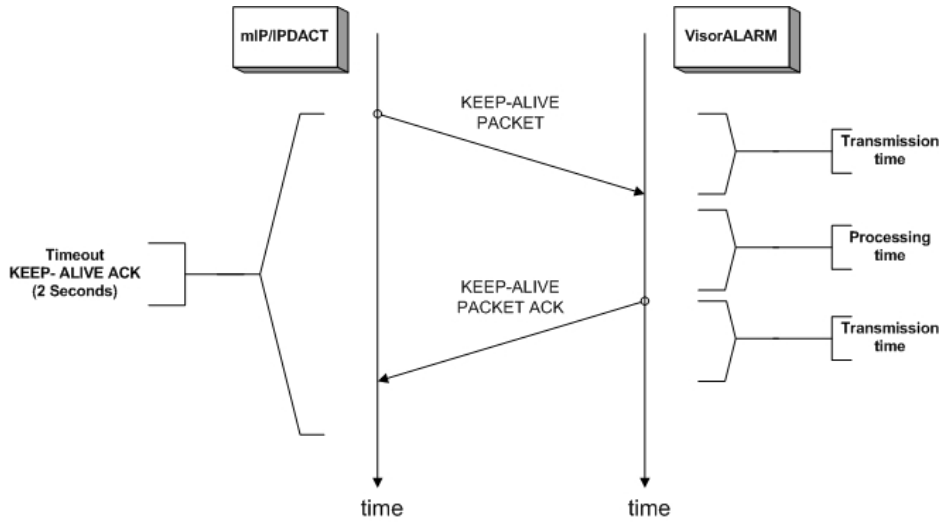
Similarly, the link-test frame send to the Automation Sw together with the response reception to these are checked through the events.

e) Loss of connection between the VisorALARM PLUS 2U and the mIP/IPDACT

Should the connection between the mIP/IPDACT and the VisorALARM PLUS 2U be lost (e.g. disconnecting the LAN from the mIP/IPDACT), this checks that once the supervision timer times out, a 350 code alarm is sent to the Automation Sw. This can also be checked through the ARLY interface events.

```
+09/02/03 10:36:35  ARLY.014 RSPVSN accnt 101234 TMOUT
09/02/03 10:36:35  ARLY.019 STOR save, 499 free
09/02/03 10:36:35  ARLY.008 FMS st 2 ev 8
09/02/03 10:36:35  ARLY.005 SL Tx 56 181234E35000000
09/02/03 10:36:35  ARLY.004 SL Rx ACK
09/02/03 10:36:35  ARLY.008 FMS st 4 ev 1
09/02/03 10:36:35  ARLY.020 STOR delete, 500 free
```

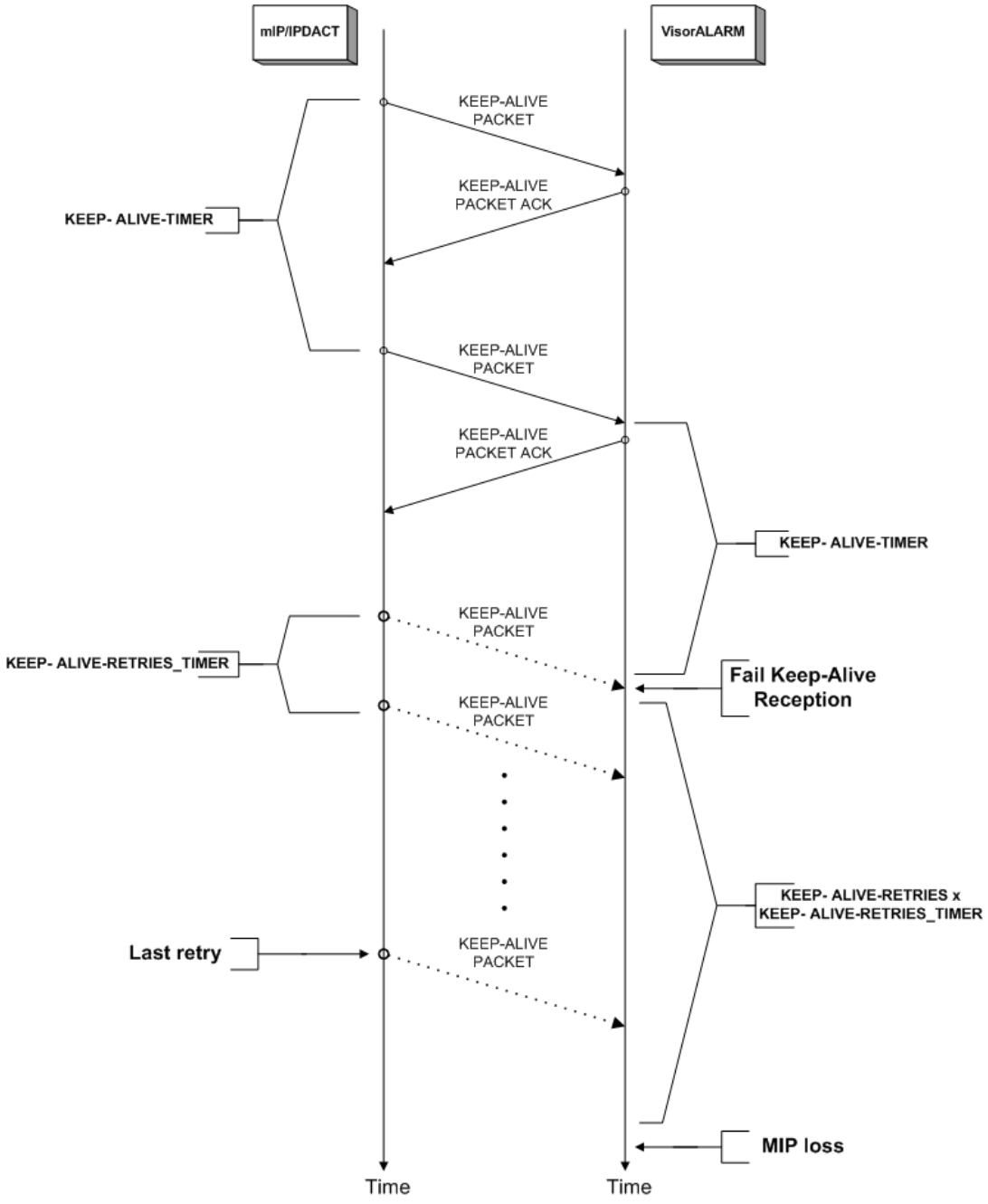
The next figure shows the process of sending supervision packets from a mIP/IPDACT to a VisorALARM receiver. When the mIP/IPDACT has transmitted a supervision packet to the receiver it waits for 2 seconds for the ACK replay. If the replay does not reach the mIP/IPDACT it retries for a maximum of "keep-alive-retries" times, with a time between retries of "keep-alive-retries-timer" seconds.



If the mIP/IPDACT does not receive replay to any of the transmitted packets, when a time of **"keep-alive-timer" + "keep-alive-retries" x "keep-alive-retries-timer"** has elapsed it considers that the communication link with the VisorALARM has lost. Two situations can arise:

1) If the mIP/IPDACT has configured a backup VisorALARM, it starts sending supervision packets to the backup and stay trying to contact with the Main each two seconds.
2) If the mIP/IPDACT has not a backup VisorALARM after the elapsed timeout it releases the line so allowing the Panel to send alarms through it.

The VisorALARM receiver uses a similar procedure to detect the communication failure with a mIP/IPDACT. If the VisorALARM does not receive supervision packets from a mIP/IPDACT for a time of **"keep-alive-timer" + "keep-alive-retries" x "keep-alive-retries-timer"** seconds it considers that the communication with the mIP/IPDACT has lost and it generates the "Communication Loss" alarm.



Monitoring the mIP/IPDACT state at this point through the **LIST MIP INFORMATION** monitoring command shows that the connection has been lost.

```
ARLY-1+list mip information
MIP Account[ffffffff]?
Account: 101234          State: alive
IP addr: 200.200.200.1   S/N: 0583/00251
Remote UDP port: 32770   Sw Rls: v4.1 US Oct 25 2006
Local UDP port:  20300

Keep-Alv tmr:    10      MIP pwd : 004321099
Keep-Alv retry:   5      Rcvr pwd: 98744332289
Keep-Alv_retry tmr:  3   Phone len: 7
Alarm retry:  5          Subs Phone:


ARLY-1+
```

If connection between the mIP/IPDACT and the VisorALARM PLUS 2U is recovered (e.g. by connecting the mIP/IPDACT to the LAN again), you can check reception for a contact and a *keep-alive* frame and the responses, and the connection recovery through the ARLY interface events. This is displayed through the **LIST MIP INFORMATION** monitoring command.

```
ARLY-1+09/02/03 10:41:27  ARLY.001 UDP Rx frm sz 80
09/02/03 10:41:27  ARLY.010 RSRVC Rx frm
09/02/03 10:41:27  ARLY.012 RSPVSN accnt 101234 cntct
09/02/03 10:41:27  ARLY.002 UDP Tx frm sz 56
09/02/03 10:41:27  ARLY.001 UDP Rx frm sz 32
09/02/03 10:41:27  ARLY.010 RSRVC Rx frm
09/02/03 10:41:27  ARLY.013 RSPVSN accnt 101234 alive
09/02/03 10:41:27  ARLY.002 UDP Tx frm sz 56

CRA ARLY-1list mip information
MIP Account[ffffffff]?
Account: 101234          State: alive
IP addr: 200.200.200.1   S/N: 0583/00251
Remote UDP port: 32770   Sw Rls: v4.1 US Oct 25 2006
Local UDP port:  20300

Keep-Alv tmr:    10      MIP pwd : 004321099
Keep-Alv retry:   5      Rcvr pwd: 98744332289
Keep-Alv_retry tmr:  3   Phone len: 7
Alarm retry:  5          Subs Phone:


ARLY-1+
```

f) Loss of connection between the VisorALARM PLUS 2U and the Automation Sw.

If you lose connection due to loss of signals (e.g. by removing the serial 1 line cable), the ARLY interface will drop and the LED labeled AUT will light up in red after one second. The signal state can be checked through the **DEVICE** monitoring command.

```
+device serial0/0

                                    Auto-test   Auto-test     Maintenance
Interface            CSR    Vect      valids    failures       failures
serial0/0       FA200A00      5e           5           5              0
 Interface DCE
   V.24 circuits:105 106 107 108 109 125 141
   Nicknames:    RTS CTS DSR DTR DCD RI  LL
   State:        OFF ON  ON  OFF ON  --- ---

Speed   (bps)            =      19200
Throughput (bps)         =      18386
Last throughput (bps)    =      22800
Bits per character       =          7
Stop bits                =          2
Parity selected          =       EVEN
Parity errors            =          0
Data errors              =          0
Overrun errors           =          0
Last reset               = 1 minute 24 seconds
+
```

If connection is lost due to lack of acknowledgement for the link-tests, or lack of response to alarm transmission, the interface drops and the AUT LED lights up yellow. On occasions this LED will temporarily light up in red.

From this point on the VisorALARM PLUS 2U will try and recover the connection transmitting link-test frames. If it receives a positive response (through an ACK) the ARLY interface will activate (UP) and the AUT LED will light up in green.

Should alarms arrive while the ARLY interface is down, these are stored and transmitted once the connection is recovered.

g) Alarm reception in the VisorALARM PLUS 2U

If the control panel generates a 131 code alarm in group 01, zone 15 (in Contact-ID format, this is the 1234 18 1131 01 015 8 frame) and the connection between the mIP/IPDACT and the VisorALARM PLUS 2U is established, the mIP/IPDACT will capture the alarm and send it to the VisorALARM PLUS 2U. If the ARLY interface is UP and the ARLY events activated, the following is displayed:

```
09/02/03 09:59:02  ARLY.001 UDP Rx frm sz 52
09/02/03 09:59:02  ARLY.019 STOR save, 499 free
09/02/03 09:59:02  ARLY.016 ALARM accnt 101234
09/02/03 09:59:02  ARLY.002 UDP Tx frm sz 48
09/02/03 09:59:02  ARLY.008 FMS st 2 ev 8
09/02/03 09:59:02  ARLY.005 SL Tx 56 181234E13101015
09/02/03 09:59:02  ARLY.004 SL Rx ACK
09/02/03 09:59:02  ARLY.008 FMS st 4 ev 1
09/02/03 09:59:02  ARLY.020 STOR delete, 500 free
```

As you can see, the alarm is received in the VisorALARM PLUS 2U and retransmitted to the Automation Sw complying with the emulated receiver format.

If the connection with the Automation Sw is not active, the alarm is stored until the connection has been reestablished and then sent. The alarms that could not be sent can be displayed through the **LIST ALARM INFORMATION** monitoring command.

```
ARLY-1+
ARLY-1+09/02/03 10:06:20  ARLY.001 UDP Rx frm sz 52
09/02/03 10:06:20  ARLY.019 STOR save, 499 free
09/02/03 10:06:20  ARLY.016 ALARM accnt 101234
09/02/03 10:06:20  ARLY.002 UDP Tx frm sz 48

ARLY-1+list alarm information
09/02/03 10:06:20- 101234 1234181131010158

ARLY-1+
```

h) Synchronizing Configurations

With the network backup, the changes in the configuration, either by dynamically registering new mIP/IPDACT devices or by configuration pattern changes performed through the console, are synchronized between the main and the backup receivers. The `polling-sync-time` parameter specifies the frequency of the synchronization process.

The synchronization procedure is as follows:

- The POLL-TIME parameter defines the poll time between the main and the backup VisorALARM PLUS 2U receivers.
- When there is any change in a configuration pattern or a mIP/IPDACT has been added or removed in the main receiver, a supervision protocol between main and backup is used to indicate that a change in configuration has been produced. The average time that the main spends to signal the change to the backup receiver is:

$$E[T] = 15 + \frac{POLL\text{–}TIME}{2}$$

- When the backup VisorALARM PLUS 2U receives the indication of a change in configuration, it establishes a TCP connection with the main receiver through which the changes in the configurations are exchanged.
- When the change in the configuration has been made in the backup, the average time to start the synchronization is:

$$E[T] = \frac{\text{POLLING-SYNC-TIME}}{2}$$

- In the same way than before, the backup receiver establishes a TCP connection with the main through which the changes in the configurations are exchanged.
- The synchronization process is also started when:
  a. A receiver is powered up.
  b. When there is a supervision failure between the equipments.
- The synchronization of configurations is only performed between the main and backup receivers. The maintenance receiver is not included in the process and it does not get synchronized automatically.
- While configurations are being updated it is not possible to change the equipments configuration either through console or through mIP/IPDACT registrations. It is strongly recommended that you do not switch off the equipment during this process because it could leave the equipment out of service.
- The changes in configurations are detected through time stamps. So it is mandatory that both the main and the backup receivers have the same time base. Therefore the NTP protocol must be correctly configured in both of them. In any other case the synchronization process will not be possible.

In cases regarding the network backup, the changes executed either in the dynamic configuration or in the static, are synchronized between the two VisorALARM PLUS 2U, main and backup. As

previously mentioned, the `polling-sync-time` parameter determines how often these updates are carried out.

The device provides some events which display the different phases of the synchronization protocol. One example of synchronization is when an mIP/IPDACT registration is produced. In this case the VisorALARM PLUS 2U dynamic configuration is modified.

The traces for the main VisorALARM PLUS 2U when the synchronization timer has completed are as follows:

```
03/04/05 17:44:10  ARLY.032 MAIN sync: Update commited.
03/04/05 17:44:11  ARLY.032 MAIN sync: Start sync.
03/04/05 17:44:13  ARLY.032 MAIN sync: Rcv HELLO.
03/04/05 17:44:13  ARLY.032 MAIN sync: Snd LIST.
03/04/05 17:44:13  ARLY.032 MAIN sync: Snd CFG_BCK
03/04/05 17:44:13  ARLY.032 MAIN sync: Rcv req MIP_CFG accn: 1234.
03/04/05 17:44:13  ARLY.032 MAIN sync: Snd MIP_CONFIG MIP 1234.
03/04/05 17:44:13  ARLY.032 MAIN sync: Rcv END_2.
03/04/05 17:44:13  ARLY.032 MAIN sync: Snd FIN.
```

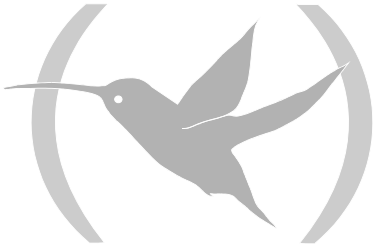
The first trace indicates that the main device needs the backup device to update due to an mIP/IPDACT register being received. The following event indicates that the TCP connection has established between both devices and therefore the updates are exchanged. The next phase of the protocol consists of both parts exchanging a list of updates, each of these made up of an mIP/IPDACT account number and a time mark which indicates if this is a final modification to take into account or not. Once each device has detected which account has been changed, the configuration for this is requested from the other device. If the modification implies deleting an account, the device directly deletes the affected mIP/IPDACT from its configuration.

The traces corresponding to the backup device are as follows:

```
03/04/05 17:44:11  ARLY.033 BCK sync: Update required from MAIN.
03/04/05 17:44:11  ARLY.033 BCK sync: Open
03/04/05 17:44:11  ARLY.033 BCK sync: Snd HELLO.
03/04/05 17:44:14  ARLY.033 BCK sync: Rcv LIST.
03/04/05 17:44:14  ARLY.033 BCK sync: Snd END_1.
03/04/05 17:44:14  ARLY.033 BCK sync: Rcv CFG_BCK.
03/04/05 17:44:14  ARLY.033 BCK sync: Snd MIP_CFG MIP 1234
03/04/05 17:44:14  ARLY.033 BCK sync: Rcv MIP_CFG_RCV accn: 1234.
03/04/05 17:44:14  ARLY.033 BCK sync: Snd END_2.
03/04/05 17:44:14  ARLY.033 BCK sync: Saving changes.
03/04/05 17:44:14  ARLY.033 BCK sync: Rcv FIN
03/04/05 17:44:17  ARLY.033 BCK sync: Changes saved.
```

In the above case it is the main device which requests the updating. The backup device can also initiate this.

Chapter 4
Appendices



1. Troubleshooting

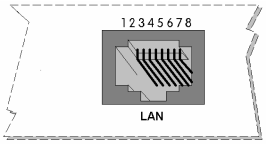
Below, you will find a table, which will help you to solve problems during the installation of the device. If you cannot resolve the problem, please consult your distributor for additional information.

Symptom	Solution
None of the LEDs lights up on the device.	Check the power supply to the device (power source, ON/OFF switch, main power outlet).
The local console does not respond.	Check that you are using the correct cable and that this is connected to the device and the asynchronous terminal. Check that the terminal has the correct port configured. Check that the terminal configuration is 9600 8N1. Check that the console is not in an events process. Check that the device is not being remotely accessed via telnet.
The local console is only displaying garbage	Check that the terminal has the correct port configured. Check that the terminal configuration is 9600 8N1.
The device does not initialize and the console displays the WARM-UP text.	Contact Teldat's Technical Service Department.
The device is very slow in displaying the application prompt.	Contact Teldat's Technical Service Department.
You have forgotten the password to access the device	Contact Teldat's Technical Service Department.
The *LAN* LED never lights up in green.	Check that the rear LINK LED is ON. Check the Ethernet cable and the connection to the network (you may need a crossover cable).

2. Connecting the connectors

2.1. LAN1/LAN2 connections (RJ45)

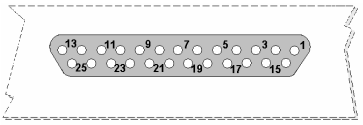
RJ45 LAN



RJ45 PIN	Ethernet
1	Tx+(input)
2	Tx-(input)
3	Rx+(output)
4	--
5	--
6	Rx-(output)
7	--
8	--

2.2. AUT/PRN Connectors

NOTE: Cables used for multi-purpose Teldat drivers must not be used in these connections. You must use end-to-end pin-to-pin connector cables.



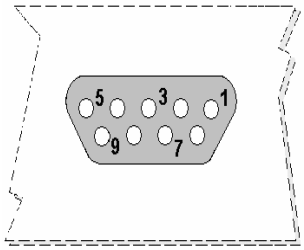
	STANDARD					
DB25 Connector	**V.24**					
Pin	**Signal**	**UIT**				
1	Ground	101				
2	TxD	103				
3	RxD	104				
4	RTS	105				
5	CTS	106				
6	DSR	107				
7	GND	102				
8	DCD	109				
9						
14						
15	TxC	114				
16						
17	RxC	115				
18						
19						
20	DTR	108				
24	ExTxC	113				

WARNING: For UL Listed installation the equipments connected to AUT/PRN connectors are restricted to be in the same room as the VisorALARM PLUS 2U

2.3. VisorALARM Expansion Card Connectors

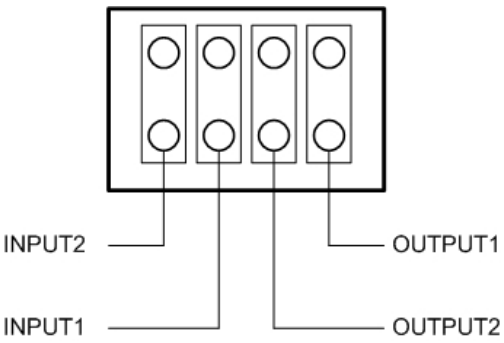
a) COM1/COM2 connectors

The VisorALARM needs special wires that are supplied with the device and are used with these connectors. These wires have a SUBD-9 V.24 termination.



DB25 Connector	V.24	
Pin	**Signal**	**UIT**
1	CD	109
2	RXD	104
3	TXD	103
4	DTR	108.2
5	Ground	102
6	DSR	107
7	RTS	105
8	CTS	106
9	RI	125

b) I/O connector

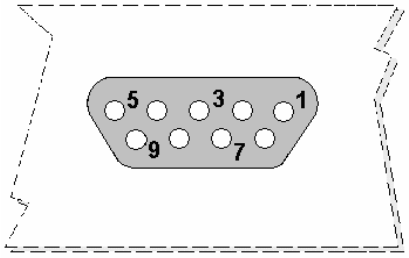


Pines	Signal
Output1	Relay RV:30Vcc RA:2A
Output2	Relay RV:30Vcc RA:2A
Input1	+12V/-12V
Input2	+12V/-12V

WARNING: For UL Listed installation the equipments connected to COM1/COM2 connectors and I/O connector are restricted to be in the same room as the VisorALARM PLUS 2U

2.4. AUX port Connections

This is used to locally configure and monitor the device. This permits the connection of an asynchronous terminal at 9.600 bps without parity and with one stop bit (9600 8N1). This is a female DB9 connector that behaves as DCE, permitting pin-to-pin connection with a PC asynchronous port or terminal.



Pin	Signal
3	TXD
2	RXD
5	GND
7-8	Joined pines
1-4-6	Joined pines

WARNING: For UL Listed installation the equipments connected to AUX Port connector are restricted to be in the same room as the VisorALARM PLUS 2U

3. Technical Specifications

Hardware Architecture

PROCESSOR	Motorola MPC8270, at 50, 66 or 80 MHz, depending on version
MEMORY	32, 64 128 or 256 Mbytes of SDRAM, depending on version
STORAGE UNIT	FLASH Memory, 4, 8 or 16 Mbytes depending on version EEPROM 2 Kbytes, NVRAM 128 Kbytes

LAN Interface

PROTOCOLS	Ethernet (802.3) / Ethernet blue book
SPEED	10 Mbps (10BaseT)/ 100 Mbps (100BaseT)
CONNECTOR	RJ45 female

Printer Interface

TYPE	V.24 DCE
SPEED	200 to 2048 Kbps
CONNECTOR	DB-25 Female

Computer Interface

PROTOCOLS	Sur-gard, Ademco 685 and Radionics 6500 emulation
TYPE	V.24 DCE
SPEED	200 to 2048 Kbps
CONNECTOR	DB-25 Female

Configuration Interface

LOCAL TERMINAL	V.24 9.600-8-N-1-without flow control
CONNECTOR	DB-9 female

VA-UD (VisorALARM Expansion Card)

COM1	V.24 DCE
COM2	V.24 DCE
OUTPUT1/OUTPUT2	Relay RV:30Vcc RA:500mA
INPUT1/INPUT2	RS-232 levels (+12V/-12V)

AC Power supply (UL installations)

INPUT VOLTAGE	120 VAC
INPUT CURRENT	1A
INPUT FREQUENCY	60 Hz

Dimensions and weight

TYPE	Rack mounted
LENGTH x WIDTH x HEIGHT	310 x 415 x 43 mm
WEIGHT	3,5Kg

Environmental Specifications

AMBIENT TEMPERATURE	0 to 49ºC
RELATIVE HUMIDITY	Maximum 93%

4. UL compliance installation

4.1. Requirements prior to installation

You must take the following requirements into consideration when installing a VisorALARM PLUS 2U in an Alarm Center.

a) Installing in a rack

The device must be installed in a 19-inch rack or box with a locking rear access door.

b) Uninterrupted power supply

The Central Station must have a continuous power supply system by means of an independent generator, which is capable of providing power to all the devices for at least 24 hours.

c) UPS

The VisorALARM PLUS 2U must have a UL listed UPS suitable for fire-protective signaling capable of allowing the receiver to operate during 15 minutes.

d) Communication devices

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

4.2. Installation requirements

a) General

1. The system provides encrypted line security via packet switched data network. The system may be installed to protect a single property, or non-contiguous properties under a single ownership. Employs the CFB code which is certified by NIST, Cert No. 280.

2. For the 200 sec. supervision, the system "polls" the VisorALARM PLUS 2U receiver via packet switched data network. Note, 90 sec. Supervision is required for commercial fire applications.

3. The number of separate signals on a single channel is limited to 1000.

4. Supervision signals between premises alarm equipment and supervising station alarm receiver equipment shall be managed by the supervising station receiving equipment and not an intermediary network agent, device or service.

5. Message authentication is conducted via procedural algorithmic processing.

6. Network addressing of devices must not make use of public Domain Name Servers.

7. Remote panel programming or configuration access shall require the use of a valid password, the panel's account or IP address number, and a receiver key code which is established between the panel and receiver automatically and without user knowledge of the specific code

8. The display message "350" (communication trouble) may Indicate compromise attempt.

9. The VisorALARM PLUS 2U supports the Contact-ID protocol.

10. For central station and proprietary use, the acknowledgement signal must be enabled.

11. The wiring connections between the mIP/IPDACT and the Listed control panel are to be made within 20 feet (6.1 m) and are to be enclosed in conduit.

12. For a dual signal line transmission system with encrypted line security, alarms are transmitted over both the IP and telco lines.

13. For Canadian Certifications (central station, proprietary), the signaling line or communication channel is designated as Level III.

14. For Canadian Certifications, the mIP/IPDACT is intended to be connected to a Listed panel that is ULC or cUL Listed to C1023, C1076, and S304.

b) BURGLAR ALARM (CENTRAL STATION): DACT, PACKET SWITCHED DATA NETWORK

1. The maximum total current draw is 1 A.

2. The control panel shall be programmed to transmit the required opening and closing signals.

c) BURGLAR ALARM (PROPRIETARY) DACT, PACKET SWITCHED DATA NETWORK

1. Same as Central Station.
2. The minimum platform redundant computer system including the receiver must be used to display and record panel status changes.

a. The Central Supervisory Equipment shall employ supply line transient protection complying with the Standard for Transient Voltage Surge Suppressors, UL 1449, with a maximum marked rating of 330 V.

b. The Central Supervisory Equipment shall employ signal line Transient protection complying with the Standard for Protectors for Data Communications and Fire Alarm Circuits, UL 497B, with a maximum marked rating of 50 V.

c. The Central Supervisory Equipment shall employ that communication circuits and network components connected to the telecommunications network shall be protected by secondary protectors for communication circuits. These protectors shall comply with the Standard for Secondary Protectors For Communications Circuits, UL 497A. These protectors shall be used only in the protected side of the telecommunications network.

d. The Central Supervisory Equipment shall be installed in a temperature controlled environment. A temperature controlled environment is defined as one that can be maintained between 13 – 35C (55 – 95F) by the HVAC system. Twenty-four hours of standby power shall be provided for the HVAC system. The standby power system for the HVAC system may be supplied by an engine driven generator alone. A standby battery is not required to be used.

d) Installation –

The control unit, accessories, and key stations are to be installed in accordance with the following UL, National and Canadian Standards:

NFPA 70 – National Electrical Code

UL 681 – Standard for Installation and Clasification of Mercantile and Bank Burglar Alarm Systems

UL 827 – Central Station Alarm Services

UL 1641 – Installation and classification of residential burglar alarm systems.

CAN/ULC-S302-M91º - Installation and Classification of Burglar Alarm Systems.

CAN/ULC-S310-M91º - Installation and Classification of Residential Burglar Alarm Systems

4.3. Configuration requirements

a) Fire Installations complying with UL864

- Configure the configuration profiles for all the IPDACT devices so they comply with the requirements established by the UL. This states that detection of any circumstances, which prevents transmission of a signal, must occur in a maximum time of 90 seconds. We strongly recommend you set the 'keep-alive-timer', keep-

alive-retries' and 'keep-alive-retries-timer', so they comply with the following formula.

keep-alive-timer + (keep-alive-retries * keep-alive-retries-timer) < 25

- Configure the configuration profiles for all the IPDACT devices so the "MIP Console Password" parameter contains the access password for the mIP devices.
- Add a password to the VisorALARM PLUS 2U receiver. This password is used both for connections via the console as well as via telnet. Make sure the administration staff at the Central Station both know it and keep it in a safe place for future use.
- Configure the 'link-test-timer' parameter for both the main receiver and the backup to a value between 60 and 90 seconds.
- It is essential that you have a spare device thus permitting you to substitute the VisorALARM PLUS 2U in a maximum period of time of 30 minutes. To do this, it is vital you have a backup copy of the VisorALARM PLUS 2U SmartCard so when this is inserted into the substitute device, the configuration is identical to the original device.
- Configure the 'automation-software-required' option.
- In these types of installations, the homologated panels that can be connected to a VisorALARM PLUS 2U through an IPDACT device are as follows:
  - § MS-9200UD
  - § MS-9600
  - § MS-9200UDLS
  - § MS-9600LS
  - § MS-9050UD
  - § MS-5UD, MS-10UD
  - § ADT-UNIMODE 200PLUS
  - § ADT-UNIMODE 9600
  - § UNIMODE 9050UD
  - § UNIMODE 9200UDLS
  - § UNIMDOE 9600LS
  - § UNIMODE 5, UNIMODE 10

b) ***Burglar Alarm Installations complying with UL 1610***

- Configure the configuration profiles for all the mIP devices so they comply with the requirements established by the UL. This states that detection of any circumstances, which prevents transmission of a signal, must occur in a maximum time of 200 seconds. We strongly recommend you set the 'keep-alive-timer', keep-alive-retries' and 'keep-alive-retries-timer', so they comply with the following formula.

  keep-alive-timer + (keep-alive-retries * keep-alive-retries-timer) < 200

- Configure the configuration profiles for all the mIP devices so the "MIP Console Password" parameter contains the access password for the mIP devices.
- Add a password to the VisorALARM receiver. This password is used both for connections via the console as well as via telnet. Make sure the administration staff at the Central Station both know it and keep it in a safe place for future use.

- Configure the 'link-test-timer' parameter for both the main receiver and the backup to a value between 60 and 200 seconds.
- It is essential that you have a spare device thus permitting you to substitute the VisorALARM in a maximum period of time of 30 minutes. To do this, it is vital you have a backup copy of the VisorALARM SmartCard so when this is inserted into the substitute device, the configuration is identical to the original device.
- Configure the 'automation-software-required' option.
- In these types of installations, the homologated panels that can be connected to a VisorALARM through an mIP device are as follows:
  - § DSC POWER 832/864
  - § VISTA-50P and VISTA50PUL

5. Alarm printing format

The format to print using 40 columns in the VisorALARM PLUS 2U includes the following fields:

MM/DD hh:mm:ss Date and time of the event

AAAA: Account code

P: Qualificator, E= New event or opening; R=Restoration or closing; P=Previous event

CCC: Type of event and code for this

XX: Number of group or partition.

ZZZ: Zone number or user identifier.

Descrip: Textual description for the event code. This contemplates the following values:

Event Code	Value
10x	Medical
11x	Fire
12x	Panic
13x	Burglar
14x, …, 1Fx	Alarm
2xx	Superv
3xx	Trouble
4xx	Opn/Cls
5xx	Dis/Byp
6xx	Test
Others	Other

```
---------------------------------------
 VisorALARM PLUS 2U v.10.5.15-Alfa
 TELDAT S.A.
 Receiver-Id=7 Line-Id=1
 Date: 01/13/06 18:23:05

MM/DD hh:mm:ss AAAA PCCC XX ZZZ Descrip
---------------------------------------
01/13 12:42:28 0000 E396 00 000 Trouble
01/13 12:42:28 0000 E633 00 000 Test
01/13 12:42:41 6000 E350 00 000 Trouble
01/13 12:42:41 7000 E350 00 000 Trouble
01/13 12:42:45 1770 E350 00 000 Trouble
01/13 12:42:45 5BA0 E350 00 000 Trouble
01/13 12:42:46 1771 E350 00 000 Trouble
01/13 12:42:46 1234 E350 00 000 Trouble
01/13 12:53:20 3456 E350 00 000 Trouble
01/13 18:24:48 3456 E531 00 000 Dis/Byp
01/13 18:24:53 3456 R120 01 001 Panic
01/13 18:24:54 3456 E121 01 001 Panic
01/13 18:24:56 3456 R121 01 001 Panic
01/13 18:24:58 3456 E122 01 001 Panic
01/13 18:25:00 3456 R122 01 001 Panic
01/13 18:25:02 3456 E110 01 001 Fire
01/13 18:25:04 3456 R110 01 001 Fire
01/13 18:25:05 3456 E124 01 001 Panic
01/13 18:25:07 3456 R124 01 001 Panic
01/13 18:25:09 3456 E125 01 001 Panic
01/13 18:25:11 3456 R125 01 001 Panic
01/13 18:25:13 3456 E110 01 001 Fire
```

6. Automation Software

The frame formats exchanged with the automation software through the serial port for each of the emulated receivers are as follows:

6.1. Frame formats

a) Sur-gard Format

MLR2000

- 5RRLLLs18AAAAQXYZGGCCC[T]

  Where:

  RR: Receiver number

  LLL: Line number

  s: Space

  18: Contact-Id format identifier

  AAAA: Four-digit account code

  Q: Qualificator, E= New event or opening; R=Restoration or closing; P=Previous event.

  XYZ: Type of event and code for this

  GG: Number or group or partition.

  CCC: Zone number or user identifier.

  [T]: 14 hex character as terminator

- Heartbeat

  1RR000sssssssssss@ssss[T]

  Where:

  RR: Receiver number

  s: Space

  @: Supervision character

  [T]: 14 hex character as terminator

MLR2D

- 5RRLs18AAAAQXYZGGCCC

  Where:

  RR: Receiver number

  L: Line number

  s: Space

  18: Contact-Id format identifier

  AAAA: Four-digit account code

  Q: Qualificator, E= New event or opening; R=Restoration or closing; P=Previous event.

  XYZ: Type of event and code for this

  GG: Number or group or partition.

  CCC: Zone number or user identifier.

  [T]: 14 hex character as terminator

- Heartbeat
  1011sssssssssss@ssss[T]
  Where:
  s: Space
  @: Supervision character
  [T]: 14 hex character as terminator

b) ***Radionics 6500 Format***

- [H]aRRLsAAAA18QXYZGGCCC[T]
  Where:
  [H]: 20 hex character (space) as header
  '**a**': Start indicator for Contact-Id message
  RR: Receiver number
  L: Line number
  s: Space
  18: Contact-Id format identifier
  AAAA: Four-digit account code
  Q: Qualificator, E= New event or opening; R=Restoration or closing; P=Previous event.
  XYZ: Type of event and code for this
  GG: Number or group or partition.
  CCC: Zone number or user identifier.
  [T]: 14 hex character as terminator
- Heartbeat
  [H]1RRLsssssssssss@ssss[T]
  Where:
  [H]: 20 hex character (space) as header
  '**1**': Start indicator for a heartbeat message
  RR: Receiver number
  L: Line number
  s: Space
  @: Supervision character
  [T]: 14 hex character as terminator

c) ***Ademco 685 Format***

- [H]RLsAAAAs18sQXYZsGGsUCCC[T]
  Where:
  [H]: 0A hex character (LF) as header
  RR: Receiver number
  L: Line number
  s: Space
  AAAA: Four-digit account code
  18: Contact-Id format identifier
  Q: Qualificator, E= New event or opening; R=Restoration or closing; P=Previous event.
  XYZ: Type of event and code for this
  GG: Number or group or partition.
  U: Zone event identifier ('C' character) or user event ('U' character)
  CCC: Zone number or user identifier.
  [T]: 0D hex character (CR) as terminator

- Heartbeat

  [H]RLsOKAYs@s[T]

  Where:

  [H]: 0A hex character (LF) as header

  RR: Receiver number

  L: Line number

  s: Space

  @: Supervision character

  [T]: 0D hex character (CR) as terminator

NOTE:

The field line number (LINE-ID) of the CONTACT-ID message can be encoded with 3 digits for the SURGAR MLR2000. For any other emulation the field is encoded with 1 digit.

When the account number of the mIP/IPDACT is of more than 4 digits the following must be considered:

4 bytes for the LINE-ID	4 bytes for the account number

The first four digits of the left will be taken as the account number of the Control Unit and they will be used in the Account field. The up to four digits of the right are used for the value of the field "LINE-ID", beginning with the most significant digit. For example, if the account number in the mIP is A2345678, the field LINE-ID will be:

Emulated receiver	LINE-ID
SUR-GAR MLR2000	A23
SURGAR MLR2D	A
RADIONICS 6500	A
ADEMCO 685	A

6.2. SIS Software

VisorALARM PLUS 2U is compatible with the SIS automation software for the three emulation modes (Sur-gard, Radionics 6500 and Ademco 685). To configure the automation software, simply select the type of receiver from among these three and configure the 'protocol' field from the group of VisorALARM PLUS 2U alarm-receiver parameters and configure the value corresponding to the selected emulated receiver.