
ipTNA
openTAS® IP end-user terminal

User Manual V2.4

Document: 70 BS 221011-60004-TS 0 1.4/b en

Created by: Marc Vontobel

Status: released

Version Overview

Vers.	Date	Author	Modification
1.0	25.07.05	Marc Vontobel	First release
1.1	02.03.06	Marc Vontobel	English release
1.2	13.11.06	Bruno Martinelli & Marc Vontobel	Corrections and adaptations
1.3	17.05.07	Marc Vontobel	Shielded Ethernet cable (Chapter. 3.2)
1.4a	12.07.07	Bruno Martinelli	Adapted to Release 2.4.x
1.4b	04.09.07	Bruno Martinelli	corrections after review

Document Management

Word Text File: ipTNA User Manual_E1.4.doc
 Word Template: Dok A4_e.dot
 Number of Pages: 41
 Release: This document was released following formal review
 on: 05.09.07
 by: Martin Vogt

Contents

1	Introduction	5
2	Installation Instructions	6
2.1	Installation	6
2.1.1	Preparations	6
2.1.2	Equipment	6
2.1.3	Installation procedure	6
3	Operating Instructions	8
3.1	Layout.....	8
3.2	Interfaces	9
3.2.1	Plug interface and indicators.....	9
3.2.2	Ethernet connection.....	9
3.2.3	RS232 serial interface	9
3.2.4	GSM connection	10
3.2.5	Parallel interface.....	11
3.3	Functions	13
3.3.1	LEDs	13
3.3.2	Monitoring.....	17
3.3.3	Cover contact	19
3.3.4	Real time clock	19
3.4	Commissioning and replacement.....	19
3.4.1	IT environment.....	19
3.4.2	Installation diagnostics.....	19
3.4.3	Set to factory defaults	19
3.4.4	Local configurations.....	20
3.4.5	Communication parameter of RS232 interface	20
3.4.6	ipTNA basic data	20
3.4.7	Local configuration procedure.....	21
3.4.8	ipTNA initial configuration	27
3.4.9	Diagnostics	28
3.4.10	Software update (remote)	28
3.5	Power supply	29
3.5.1	Power supply	29
3.5.2	Back-up battery (battery)	29
3.6	Mounting	30
3.6.1	ipTNA wall-mounting case	30
3.6.2	Wall mounting.....	31
3.7	Cable connections.....	32
4	Appendix.....	33
4.1	Monitoring classes	33
4.2	Alive interval in dual channel mode	33
4.3	Repetition of user messages	35

4.4 Reconnection intervals35

4.5 Fixed time values.....37

4.6 Time synchronisation.....37

4.7 Error outputs for PAD profiles 7xxx.....38

4.8 Software download progress indications38

4.9 List of Abbreviations and Terminology.....39

4.10 Declaration of conformity40

4.10.1 TNA-IPSN-1.....40

4.10.2 TNA-IPSN-GSM-141

1 Introduction

The ipTNA (IP end-user terminal) is used in telecontrol and alarming applications. It allows the input and output of bivalent messages. A serial interface is used for data traffic with a primary system.

The ipTNA device is available in two configurations:

- ipTNA (Ethernet transmission medium)

Used as:

- Single mode Ethernet

- ipTNA GSM (Ethernet and GSM/GPRS transmission media)

Used as:

- Single mode Ethernet
- Single mode GSM
- Dual mode Ethernet and GSM

The ipTNA end-user terminal was developed specially for IP-based networks. An Ethernet interface is used for the primary connection to the central IP platform (openTAS server). To safeguard the TCP/IP connection a second transmission medium is available as a redundant secondary communication path using an optional GSM/GPRS socket module. An internal antenna is integrated in the housing. If it is insufficient for fault-free signal reception, it is possible to connect an additional external antenna (not included in the equipment supplied by Ascom (Switzerland) AG).

An external AC/DC power supply unit powers the ipTNA. An optional battery pack allows mains-free operation for a limited period and acts as a backup in the event of short power outages.

Most of the explanations in this document, which is intended for the installer, focus on the installation procedure as well as the functions and interfaces.

2 Installation Instructions

2.1 Installation

2.1.1 Preparations

The following measures need to be taken before an ipTNA is installed:

- Determine the installation site
- Socket outlet for power supply (external AC/DC power supply unit)
- 10/100 Mbit Ethernet connection (RJ45), e.g. via ADSL (broadband)
- Configuration of the ipTNA at the openTAS - Platform
- SIM card of a local provider (ipTNA GSM only)

2.1.2 Equipment

To install an ipTNA, the installer will require the following equipment:

- ipTNA or ipTNA GSM
- External AC/DC power supply unit
- Battery pack (optional)
- a shielded RJ45 Ethernet patch cable (connection between Ethernet connection and ipTNA)
- Wall-mounting auxiliaries (dowels, screws, etc.) (see chapter 3.6.1)
- Installation cable for connection of the parallel interface (max. cross-section 1.5 mm²)
- I/O connection diagram (provider)
- Also required for the ipTNA GSM:
 - SIM card of a local GSM/GPRS provider ipTNA GSM only with deactivated PIN code
 - Connecting cable for external antenna (optional)
 - External antenna (optional; not included in the equipment supplied by Ascom (Switzerland) AG)

2.1.3 Installation procedure

This Chapter contains the step-by-step procedure to be followed by the installer when installing an ipTNA. *All optional items are in italics and are to be carried out only as required.*

To install an ipTNA proceed as follows:

1. Lay out the equipment and check that it is complete

2. Remove the ipTNA cover
3. Secure the housing base to the installation site using the appropriate assembly auxiliaries (see chapter 3.6)
4. *GPRS SIM card*
 - a. *Check whether PIN code is deactivated. If activated, deactivate using commercial cell phone*
 - b. *Insert SIM card into GSM module holder*
5. Power supply
 - a. Connect external AC/DC power supply unit (10 to 30 VDC, 15W) to terminal X5 and feed connecting cable outwards with neat strain relief device
6. *Battery pack installation (optional)*
 - a. *Affix Velcro strips (for securing the battery pack) in the space provide on the housing base (see chapter 3.6.1)*
 - b. *Secure battery pack using fleece tape*
 - c. *Plug battery pack connecting cable into terminal X4*
 - d. *The battery pack (supplied uncharged) now charges automatically.*
 - e. *L1 LED:*
 - i. *flashes while the battery is being conditioned*
 - ii. *is steadily lit during charging*
 - iii. *off while charging is completed*
7. *GPRS Network integration*
 - a. *LED L*
 - i. *is steadily lit during GSM log-on procedure*
 - ii. *flashes once GSM log-on is achieved*

For signal strength indication on LED L2 to L5 see chapter 3.3.1.6
8. Use shielded patch cable to connect Ethernet connection with terminal X21
 - a. ipTNA runs initial configuration procedure automatically
9. Connect signal inputs and outputs to parallel interface X1 in accordance with operator's instructions
10. Adapt cable outlet cover according to requirements
11. Conduct tests in accordance with security service provider
12. If all OK, screw housing cover into place.

3 Operating Instructions

3.1 Layout

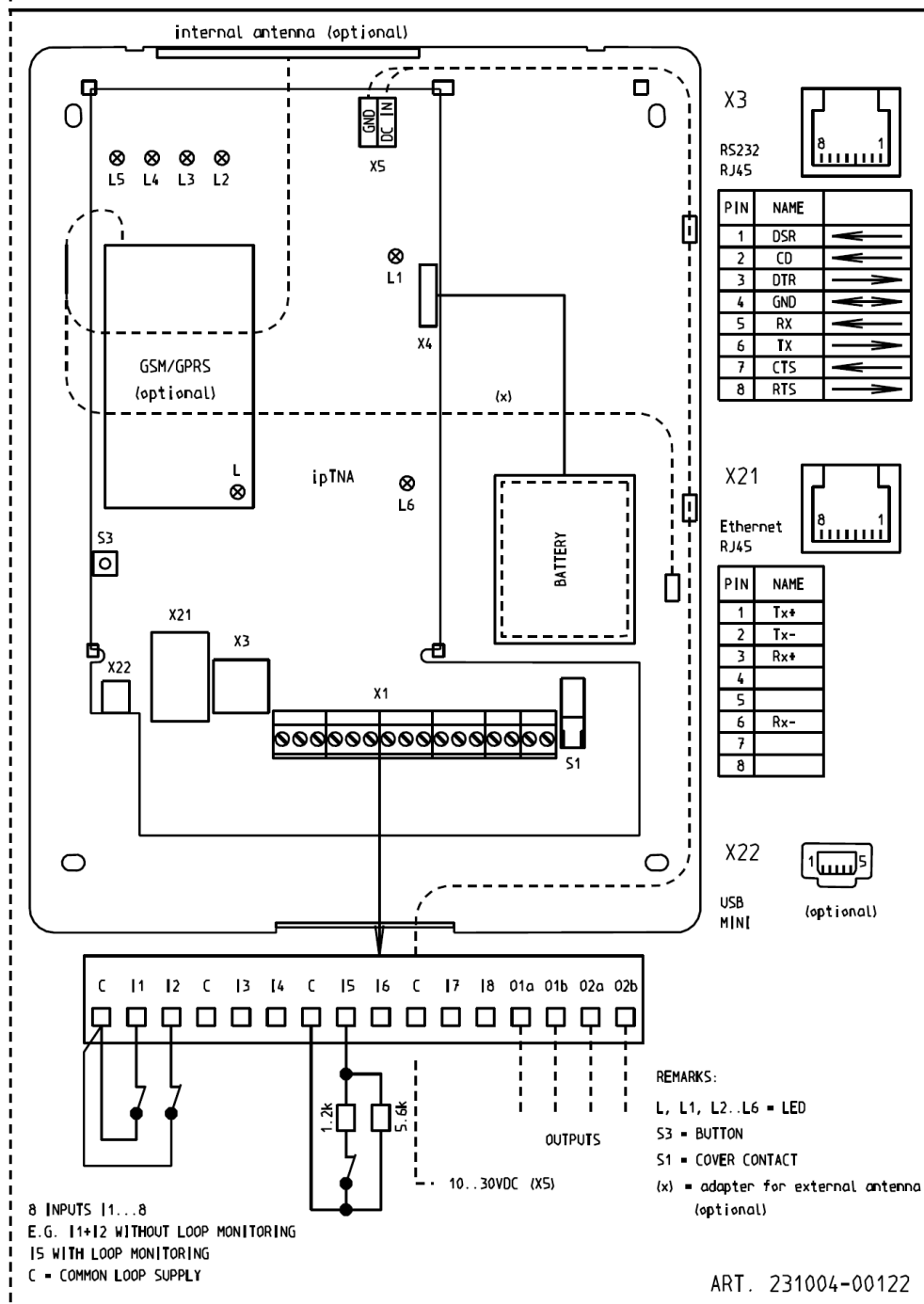


Fig. 1 ipTNA Layout

The ipTNAs are assembled by the manufacturer in accordance with the customer's requirements and supplied as complete units. This ensures that the equipment can be tested as a whole in its specific configuration and guarantees fault-free operation.

3.2 Interfaces

3.2.1 Plug interface and indicators

- Ethernet interface (8-pin RJ45 socket)
- RS232 serial interface (8-pin RJ45 socket)
- Parallel interface (terminal strip for 8 inputs and 2 outputs)
- 1 micro-pushbutton (S3)
- 7 status LEDs (function and status display)

3.2.2 Ethernet connection

The connection to a 10/100 Mbit/s Ethernet (10Base-T/100 Base-Tx) is implemented using a shielded cable CAT-5 (e.g. S/FTP, F/FTP or SF/FTP).

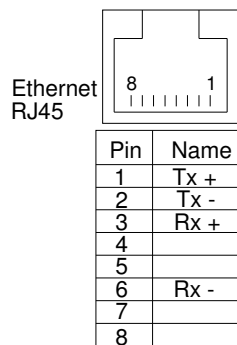


Fig. 2 Pin assignment, Ethernet interface

3.2.3 RS232 serial interface

The ipTNA is considered as a modem and is therefore the DCE (Data Communication Equipment); the primary installation as the data source/sink represents the DTE (Data Terminal Equipment).

Electrically: RS-232C (V.28)

The interface of the connected terminal equipment (TEE) must comply with the requirements for a safety extra-low voltage circuit (SELV circuit) in accordance with EN60950.

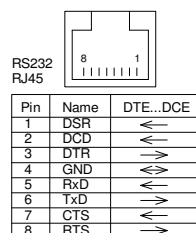


Fig. 3 Pin assignment, RS232 interface

3.2.3.1 PAD profiles

The following standardised profiles are supported:

2000, 2200, 2400, 2401, 2600, 2800

7400, 7401, 7600, 7800

New profiles: TSS14 with TSS17 header

The “TSS14 with TSS17 header” mode allows connection to existing alarming platforms that operate with TSS17.

The following restrictions apply:

- First message is always of the type TSS17 (90Hex)
- Second message is always of the type block display (30Hex)
- The header information is not transmitted to the openTAS platform. The user data is sent as TSS14 message
- Each message of the openTAS platform has the standardised header TSS17 (configurable for each ipTNA)
- Time information is not sent
- Messages from the alarming platform are confirmed either with "transmission successful" or "fault"
- No other messages are accepted or sent
- Window size = 1
- No repetition if return confirmation is negative (the alarming platform must repeat the faulty message)

3.2.4 GSM connection

ipTNAs shipped with GSM/GPRS module have an internal antenna. If the signal strength is insufficient it can be replaced by an optional external antenna (not included in the equipment supplied).

The L LED on the module indicates the GSM status (lit during the log-on phase, followed by short flashing).

3.2.4.1 SIM card

ipTNAs shipped with the GSM module require a SIM card from a local provider. The SIM cards should be supplied with the PIN code deactivated. Any PIN code already activated should be deactivated using a commercial cell phone before the SIM card is inserted into the ipTNA.

It is also possible to disable the PIN code via the console with help of AT commands (see 3.4.7.3).

Before insert or remove the SIM card into the SIM card holder, the ipTNA has to be separated from the power supply (main supply and battery)!

3.2.4.2 Internal antenna

The ipTNA GSM is factory-fitted with a GSM/GPRS module. The relevant antenna is inserted in the holder provided and connected with the module. The plug-in coupling should not be disconnected unnecessarily as it is not designed for connecting repeatedly.

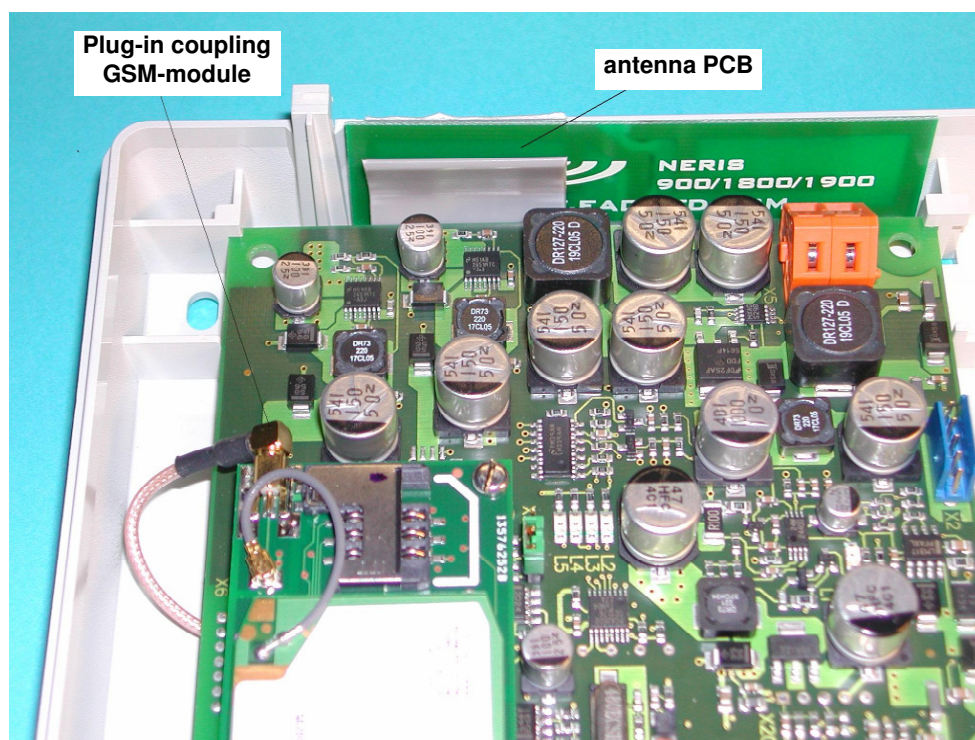


Fig. 6 internal antenna

3.2.4.3 Connecting an external antenna

If the internal antenna is insufficient for a clear reception of the GSM signal, it is possible to connect an external antenna (not included in the equipment supplied by Ascom (Switzerland) AG). Order an optional connecting cable from the manufacturer. Carefully disconnect the plug-in couple and remove the internal antenna. Connect the connecting cable to the module's plug-in coupling and feed outwards. Ensure proper strain relief at the clamping bar.

3.2.5 Parallel interface

The parallel interface has 8 inputs and 2 outputs.

The maximum cross-section of the connecting cables must not exceed 1.5 mm².

3.2.5.1 Signal inputs

The inputs are **not** electrically isolated. The alarm signalling device must offer floating contacts as transfer interface. These contacts must be in a safety extra-low voltage circuit (EN60950: SELV circuit).

Requirements per signal input:

Closed state < 300 Ω
 Open state > 50 kΩ
 Distance between alarm signalling device and ipTNA < 100m

Depending on the electromagnetic environment in the vicinity of the alarm loop input faults cannot be excluded (e.g. line routed in parallel with power installations). In such cases it is advisable to screen the alarm loop. The screening is to be connected with a reliable neutral point (e.g. mains protective earth).

To save power, the common loop supplies (C) are supplied with one pulse (one pulse for the eight inputs). Therefore the loop must not contain any capacitors (integrations are specified by configuration). The loop states are checked during the pulse.

Common loop supplies C													Outputs			
Inputs I1 to I8																
C	I1	I2	C	I3	I4	C	I5	I6	C	I7	I8	01a	01b	02a	02b	

Tab. 1 Pin assignment, plugs

Monitored current loops are often used in security systems.

With this configuration the ipTNA is able to determine and transmit not only closed and open contact loops but also interruptions and short-circuits in the alarm loop.

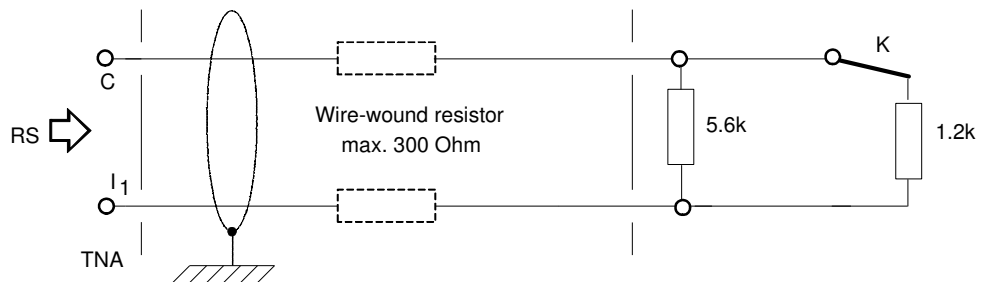


Fig. 4 Loop monitoring on ipTNA

The inputs can be configured with or without loop monitoring.

3.2.5.2 Signal outputs

The ipTNA has two signal outputs. By configuration on the openTAS system, they can be customized for use as device status signalling or as control output for other applications. The device status signalling uses two outputs to display the status:

Fault signalling:

- Connection interrupted
- Power interrupted (battery fitted and option activated)
- Other hardware faults

Local alarms:

- Destination not reached
- Output activated during message repetition.

The relay contacts may only switch signals that are also in a safety extra-low voltage circuit (EN60950: SELV circuit).

Relay technical data:





- max. voltage → 30V_{eff}
- max. switching current → 1A
- max. switching capacity of the contact → 30W
- max. voltage (as per SELV) → 60V DC or 42.4V AC (for a max. current of 0.5A)
- min. voltage → 10mVDC / 0.01mA
- Electrical isolation → max. isolating voltage 500 V_{eff}
- in the event of loss of voltage the relay positions are retained
- service life → 100,000 switching operations

3.3 Functions




3.3.1 LEDs

The ipTNA has seven monochrome LEDs: L1 – L6, L. For autonomy reasons the LEDs are switched off when the cover contact is closed (except LED L).




Each LED has four states:

	off		on		slow flashing		rapid flashing
---	-----	---	----	---	---------------	---	----------------

3.3.1.1 Battery status indication

L1	Battery status
	Battery conditioning or no battery fitted
	Battery charging
	Battery charged or no battery fitted

3.3.1.2 GSM status indication

L	GSM status (on GSM/GPRS module)
	GSM log-on established
	Log-on phase
	Deactivated

3.3.1.3 Bootloader status indication

L6	<i>for internal use only</i>
-----------	------------------------------

3.3.1.4 Function indications on LED L2 to L5

During regular operation the ipTNA provides diagnostic information by using button S3.

There are 4 different diagnostic modes to support the entire installation procedure. Mode 1 is enabled in regular operation and does not effect regular operation at all. Mode 2 to 4 are specific 'installation diagnostic' modes that may have slight influence on the regular operation due to the necessity of accurate connection information on Ethernet and GPRS.

While 'installation diagnostic' modes are enabled, the cycle times for alive check are constantly 10 s and the reconnection intervals are fixed at 3 s. In Mode 1 the ipTNA gets back to the defined (configured) alive check cycle times.

Every press (>200ms < 4sec) on button S3 will increase the diagnostic mode by one level and after Mode 4 it will start again with Mode 1. At any time by closing the cover switch S1 the diagnostic ends and it returns to Mode 1.


When button S3 is pressed more than 5 seconds, the ipTNA will perform a restart.




After a timeout of 30 minutes since the last activity on button S3, the ipTNA enables automatically Mode 1.





Diagnostic modes on LED L2 to L5



regular operation	Mode 1	Status overview
Installation Mode (alive check 10s)	Mode 2	GSM signal strength
	Mode 3	Ethernet status
	Mode 4	GPRS status

3.3.1.5 Mode1 – Status overview

L2	Run LED
	The ipTNA is running

L3	Log-on over Ethernet
	No connection
	Connecting phase
	Connected





















L4	Log-on over GPRS
	No connection
	Connecting phase
	Connected
	No module or no SIM card

L5	ftp check result indication (for the first 30s on every power-up)
	firstStart ftp check not successful
	firstStart ftp check successful

3.3.1.6 Mode2 – signal strength

In this mode the signal strength level as indicated by the GSM module is displayed with a refresh rate of 3s.

For an error free operation at least 2 LED should be ON.

L5	L4	L3	L2	Signal strength level
				GSM not used
				0 – 9
				10 – 14
				15 – 19
				> 20

3.3.1.7 Mode3 – Ethernet status

For an error free operation all LED should be ON

L5	L4	L3	Signal strength level
<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	no IP address available or Ethernet not used
<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	fix IP adr or IP adr received from DHCP server
<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	IP address received and connection to openTAS mediation established
<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	IP address received, connection to openTAS established and logged on

L2	first start ftp check result
<input type="radio"/>	not successful
<input checked="" type="radio"/>	check successful

3.3.1.8 Mode4 – GPRS status

For an error free operation all LED should be ON

L5	L4	L3	L2	Signal strength level
<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	not registered or GSM not used
<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	registered, home network or roaming
<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	registered, IP address received
<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	registered, IP address received and connected to the openTAS mediation
<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	registered, IP address received, connected and logged on to the openTAS

3.3.2 Monitoring

The following message types are integrated:

Alarm messages: digital input (TSS11), digital output (TSS12)

Status messages: voltage (battery, DCin), hardware status, serial interface, status (DTR)...

Block message: TSS14, TSS14 with TSS17 header

Control message: Logon, restart, time synchronisation...

Each message is confirmed by the server. In the event of a communication error the message is buffered and resent at regular intervals.

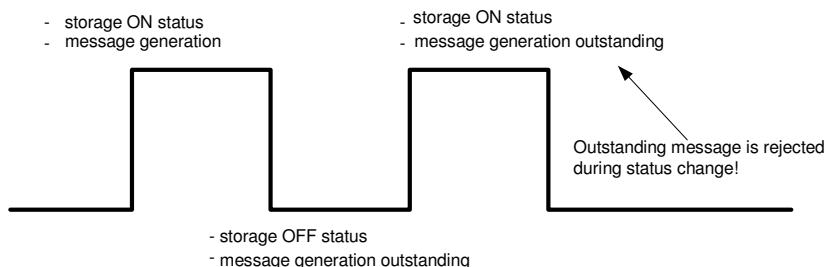
The use of hysteresis definition and/or the restriction of messages per time unit prevents the server from being flooded with unnecessary recurring messages.

3.3.2.1 Message storage

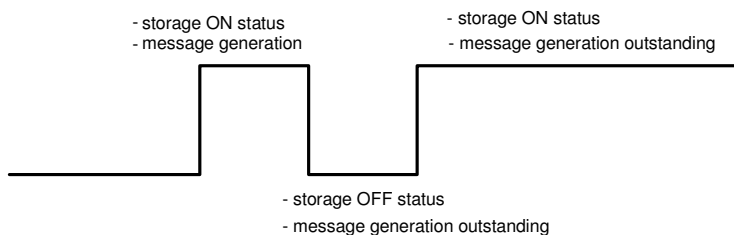
The following rules apply to the storage of outstanding messages:

Alarm and status messages

- A maximum of two states are stored
- A message is generated only once the preceding display has been confirmed by the server



With standing connection, server receives the following message:
ON message → OFF message



With standing connection, server receives the following message:
ON message

Fig. 5 Messages

Block messages (TSS14):

- The ipTNA stores a maximum of 5 messages (window size = 5). Other messages are accepted only if the first has been confirmed. The CTS interface signal is used for controlling the data flow.

Block messages (TSS14 with TSS17 header):

- Only one message is stored (window size = 1). The CTS interface signal is again used for controlling the data flow.

None of the messages is stored persistent, i.e. if the ipTNA fails (power outage), all outstanding messages are deleted.

3.3.2.2 Alive messages

The ipTNA sends alive messages at regular intervals via the primary (and secondary, where available) communication channel. The resulting functionality complies with the requirements of standard EN50136-1-1 [2].

3.3.2.3 Retransmissions

Status messages are used for monitor the communication channels. The repeat interval depends on the quality of the service level. In the event of a negative retransmission with other messages (alarm, status, blocking display, etc.), the ipTNA activates the local alarm output (if configured) and starts with the repeats. The repeats are made at predefined or shorter intervals (minutes/hours) of categories S20 - T25.

The repeat takes place immediately in the case of a new alarm from the same source.

Each possible alarm source (digital input 1, digital input 2..., serial input ...) has its own independent repeat controller (with identical algorithm).

3.3.2.4 Serial interface monitoring

The monitoring of a connected alarming system is implemented using the DTR interface signal. No messages are transmitted or accepted via the serial interface while the DTR signal is inactive. The DTR signal state can be mapped to an alarm state.

3.3.2.5 GSM signal

The threshold and interval (hours – days) can be set for the monitoring of the GSM signal strength. In the configured interval, the signal strength is compared to the threshold level. If the measured value is below the threshold, the ipTNA sends the platform an appropriate warning. A positive acknowledge is sent to the server as soon as the signal strength is once again above the threshold. There is no separate local alarm on the ipTNA for insufficient signal strength.

The signal strength can be displayed via the local console access during the initialisation process, but not during operation.

3.3.3 Cover contact

The ipTNA has a cover contact to secure it against opening. When the cover contact is closed, individual LEDs (except LED L) stay off to save power.

3.3.4 Real time clock

The ipTNA has a real time clock, which is periodically synchronised by the openTAS system. The first synchronisation takes place during login. The time function is maintained only with DC or battery power supply.

3.4 Commissioning and replacement

3.4.1 IT environment

On the firewall, ports 9203, 9213 and 9223 have to be open to allow external communication. Per default dynamic IP address assignment is used; static address assignment is possible but not necessary.

The DHCP (Dynamic Host Configuration Protocol) allows the dynamic assignment of an IP address and other configuration parameters to the ipTNA. With this method a new ipTNA can be integrated without requiring major configuration work.

The NAT (Network Address Translation) process is used to reduce the public IP addresses required. Private IP addresses are used within private networks. To allow communications with the internet nonetheless, the internal private addresses have to be converted into public address at the gateway to the public network. This is also a data security measure, as the network's internal structure remains hidden to the outside.

3.4.2 Installation diagnostics

For installation diagnostics indications on the LEDs see chapter 3.3.1

3.4.3 Set to factory defaults

The ipTNA can be set to the factory defaults either by the appropriate point of the local configuration menu (5) or by the following procedure.

If the cover contact (S1) and the micro-pushbutton (S3) are pressed while the ipTNA is connected to the power supply, a set to factory defaults is performed.

The ipTNA then does a first start on the key mediation.

Button S3	Cover switch S1	Operation at power - on
inactive	don't care	regular startup operation
active	closed	set to factory default
active	open	local configuration - menu

3.4.4 Local configurations

A password-protected console access is possible via the RS232 interface for a short period of time during startup.

The configuration menu is used for the following functions:

- Setting own IP address (if DHCP is not used)
- Setting own IP mask (if DHCP is not used)
- Setting the gateway (if DHCP is not used)

For security reasons the IP address of the alarm server and the port number are only displayed; they cannot be changed.

3.4.5 Communication parameter of RS232 interface

Bits per second: 9600
 Data bits: 8
 Parity: None
 Stop bits: 1
 Flow control: None

3.4.6 ipTNA basic data

The following data is permanently stored on the ipTNA on delivery:

- Equipment ID (MAC address as the equipment number)
- IP address of the mediation key

During manufacturing each ipTNA is given its own unique identity and an initial dataset, which determines where it has to log in during startup. This is the IP address of the mediation key. The ipTNA is shipped with operating software. The newest software can then be downloaded via the IP network. This ensures that the appropriate software is downloaded to each ipTNA.

If the ipTNA is installed into a network with DHCP servers, it is assigned a private IP during startup.

For networks without DHCP server the installer has to carry out a permanent configuration:

- Equipment IP within the network
- Network netmask
- Network gateway (router to the outside)

This configuration can be carried out via the serial interface during startup.

3.4.7 Local configuration procedure

If the cover contact (S1) is in the open position and the micro-pushbutton (S3) is pressed while the ipTNA is connected to the power supply, the following information appears after 10 seconds in the window of any terminal program, e.g. the Windows XP Hyper Terminal:

```

*****
*****
*openTAS 880TNA-IP1, Copyright © 205 Ascom (Schweiz) AG*
*****

NET+WORKS Version 6.3
Copyright (c) 2000-2004, NETsilicon, Inc.

PLATFORM: BP880_TNA_V0.5
APPLICATION: ipTNA Version 2.0.0
-----
NETWORK INTERFACE PARAMETERS:
  IP address on LAN is 139.79.53.89
  LAN interface's subnet mask is 255.255.255.0
  IP address of default gateway to other networks is 139.79.53.10
  IP address for firstStart MediationKey is 10.150.6.23, Port 9203
HARDWARE PARAMETERS:
  Serial channels will use a baud rate of 9600
  This board's serial number is 0543912821
  This board's MAC Address is 08:00:64:00:01:9F
  After board is reset, start-up code will wait 5 seconds
  Default duplex setting for Ethernet connection: phy Default
-----

Press any key in 5 seconds to change these settings.

```

Fig. 7 Example of a startup window for local configuration

If as described in the last line no key is pressed within 5 seconds, the ipTNA starts up with the predefined settings.

If any key is pressed, the following prompt appears on the screen:

Press A to Accept the settings, M to Modify or D for installation Dialogue?

Fig. 8 Selection menu

A accepts the predefined settings; the ipTNA starts up automatically.

M (Modify) or D (installation Dialogue) prompts the user to enter a password. The password is to be requested from the operator beforehand. Menu item D (installation Dialogue) is for the installer. It is briefly described below.

If an incorrect password is entered 4 times in a row, the terminal automatically starts up with the predefined parameters.

Press A to Accept the settings, M to Modify or D for installation Dialogue?D

Enter the configuration password: *

FAILURE: password incorrect

Enter the configuration password: *

FAILURE: password incorrect

Enter the configuration password: *

FAILURE: password incorrect

Enter the configuration password: *

FAILURE: password incorrect

continue...

Fig. 9 Incorrect password input

Once menu item D (installation Dialogue) is selected and the password correctly entered, the following dialog box is displayed on the screen:

Press A to Accept the settings, M to Modify or D for installation Dialogue?D

Enter the configuration password: *****

continue to installation dialogue...

ipTNA Installation

1 : Parameters

2 : Communication

- 3 : Inputs / Outputs
 - 4 : Reset disconnectOnLocking
 - 5 : Set to factory defaults
 - 6 : E x i t and startup application
- Choice :

Fig. 10 Installation dialog box

3.4.7.1 ipTNA installation menu tree

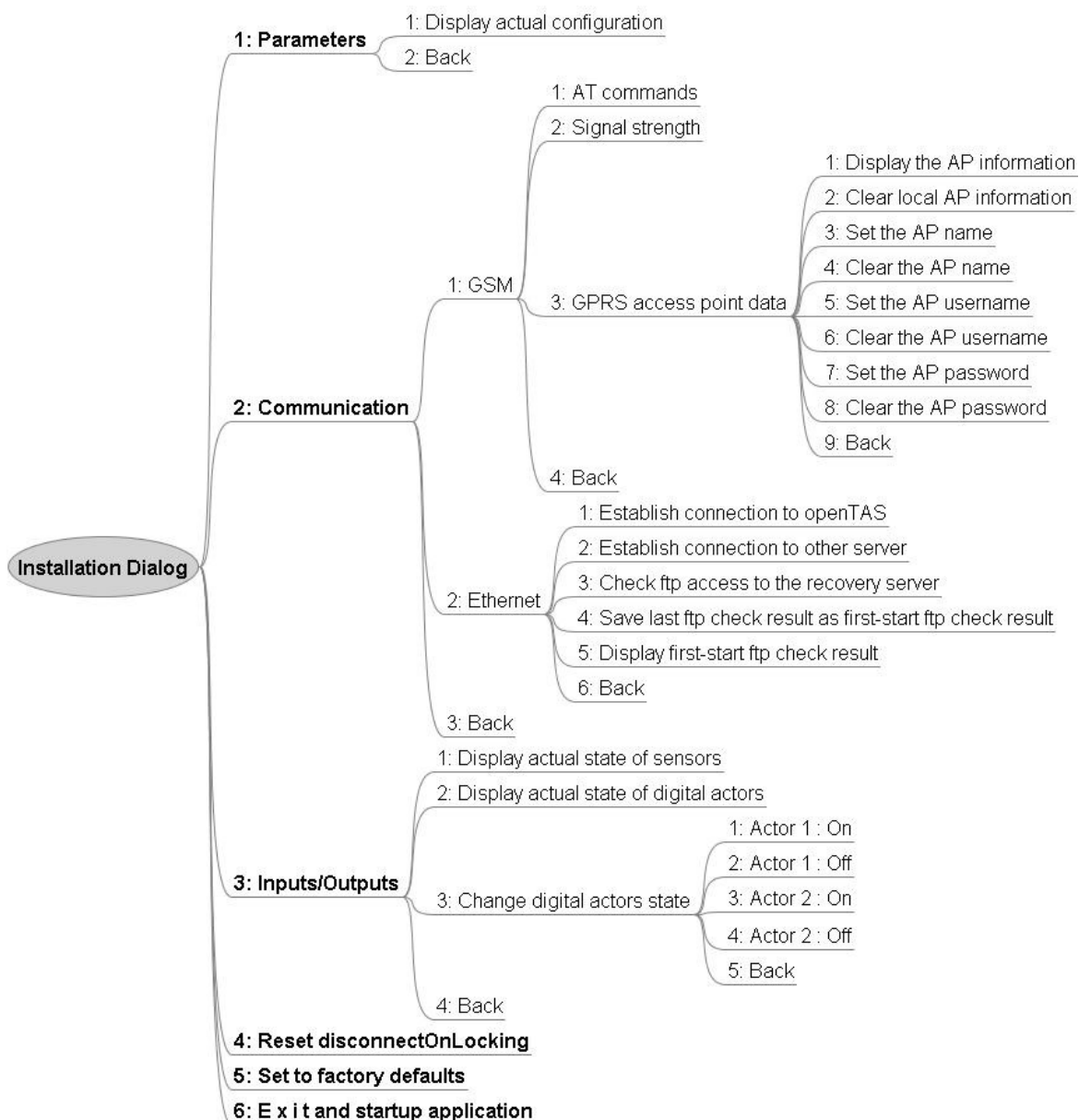


Fig. 11 Installation menu overview

Figure 11 shows an overview of the installation menu. The individual menu items are selected using the corresponding digit. Use the “Back” function to exit a submenu and return to the next higher-level menu.

3.4.7.2 GSM signal strength

To find the optimum location for the terminal, the installer can use menu item 2.1.2 (Communication – GSM – Signal strength) to display the current GSM signal strength at periodic intervals.

Output example:

```
at+CSQ
+CSQ: 31, 0
```

The first value (e.g. 31) is the receive signal strength and the second value is the channel bit error rate (e.g. 0)

The effective signal field strength can be read off from the table below:

Output value	Signal strength
0	-113dBm or less
1	-111dBm
2 to 30	-109 to -53 dBm
31	-51 dBm or more
99	unknown or not identified

For a stabile communication a level of at least 10 (output value) is necessary.

The bit error rate is in the range 0...7

0	BER < 0,2 %
1	0,2 % < BER < 0,4 %
2	0,4 % < BER < 0,8 %
3	0,8 % < BER < 1,6 %
4	1,6 % < BER < 3,2 %
5	3,2 % < BER < 6,4 %
6	6,4 % < BER < 12,8 %
7	12,8 % < BER

Rule:

Level : the higher the better

BER: the lower the better

3.4.7.3 PIN code

AT commands can be used to verify the PIN code status and to deactivate but also reactivate any PIN Code.

A PIN code consists of 4 to 8 characters. In the explanations below, 1234 is used as the PIN code example.

Checking the PIN status

Input:

AT+CLCK?

Response:

+CLCK:("PS",0),("SC",x),("FD",0),("PN",0),("PU",0),("PP",0),("PC",0)

Explanation:

PIN activated: ("SC",1)

PIN deactivated: ("SC",0)

Deactivating the PIN code

Input:

AT+CLCK="SC",0,1234

Response:

AT+CLCK="SC",0,1234

OK

For operation, the PIN must not be activated!

3.4.7.4 GPRS access point information (menu 2.1.3 / 1...8)

Usually the access point information (name, user, password) for the GPRS access is predefined by the MCC (MobileCountryCode) / MNC (MobileNetworkCode) read out of the SIM card. If for any reason other access point information should be used, the predefined values can be overwritten by locally entered ones. If a user or password has to be defined locally, the AP name has also to be defined locally (i.e. the local defined user and password don't care with an empty local access point name).

If local values are defined, the MCC / MNC of the SIM card don't care.

To clear the local AP data, the menu points 2.1.3.2,4,6, or 8 must be used (do not try to clear the acces point info by entering spaces ...).

3.4.7.5 Establish connection to openTAS (menu 2.2.1)

The ipTNA establishes a socket connection with the predefined ip address and port info. If the first start has already successfully been done, a connection to the Ethernet Mediation is performed. If the first start has not been done yet, a ethernet connection to the mediation key is tried.

If the connection can be established successfully, the mediation will disconnect it after 10s because no data is sent.

If the mediation cannot be reached, the ipTNA retries every 10s and so the test may take about 2 minutes !

3.4.7.6 Establish connection to other server (menu 2.2.2)

For general connection tests, arbitrary ip- and port – values can be entered, whereto the ipTNA establish a tcp socket connection.

If the ipTNA is unable to connect the test may take 2 minutes.

3.4.7.7 Check ftp access to the recovery server (menu 2.2.3)

At the first start, the ftp recovery server acces test is performed automatically and the result of this test is saved persistent.

With help of this menu point, the ftp server access tests can be released manually. The test step include a connection to the ftp recovery server, a directory change and the beginning of a file transfer.

The parameters cannot be changed and are the same as used on first start test or on a real recovery.

Possible results:

- Successfully c o n n e c t e d and received data
- Could n o t connect to the server !
- Connection o.k., could n o t enter working directory !
- Connection o.k., could n o t receive any data !
- Internal error, test n o t performed !

3.4.7.8 Display first-start ftp check result (menu 2.2.5)

Displays the result of the first start ftp check. Possible results see 3.4.7.7

3.4.7.9 Save last ftp check result as first-start ftp check result

If a manually released ftp check has been performed, this result can be saved as the first start result. So it is possible to clear the 30s error indication on LED L5 (see 3.3.1.3), once the ftp check is successful.

3.4.8 ipTNA initial configuration

The diagram below shows the automated initial configuration of an ipTNA after connection to an IP network.

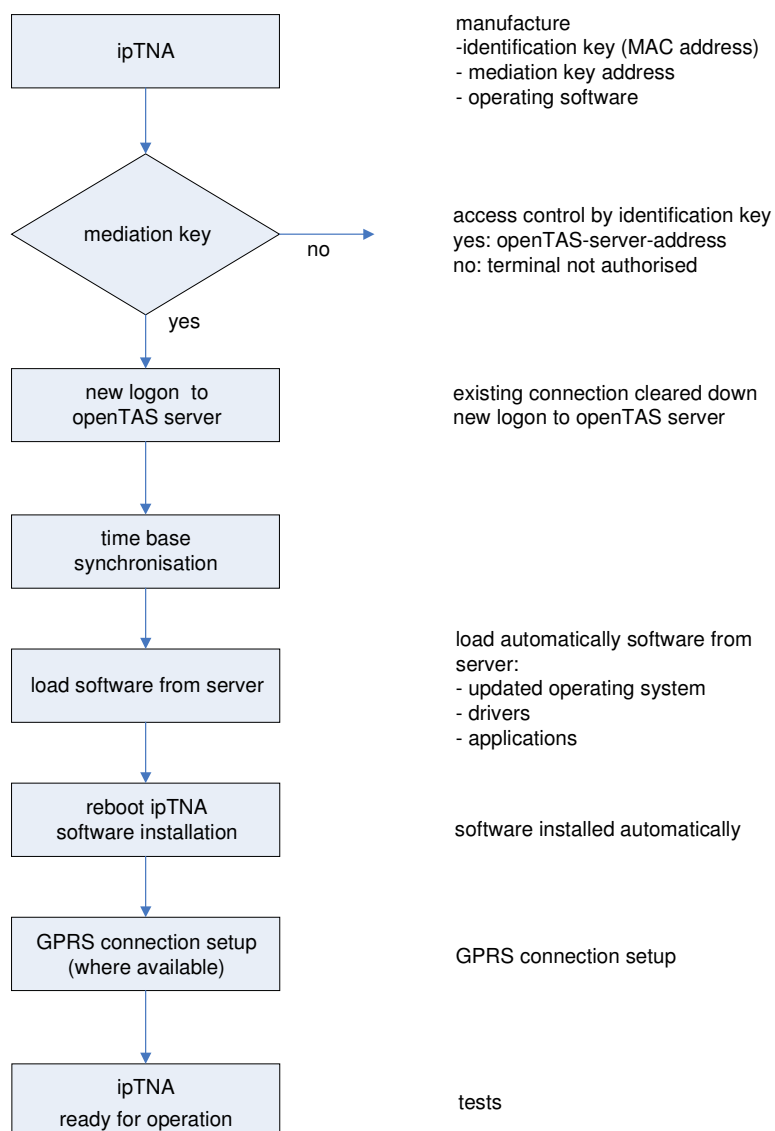


Fig. 12 Sequence for ipTNA initial configuration

The vast majority of configuration parameters are predefined remote attributes. The alarm server sends the complete set of parameters to the ipTNA during the first LOGON (special initial LOGON). Each subsequent logon message to the server contains the checksum of all parameters. If the checksum does not match the checksum on the server, the parameters are once again sent to the ipTNA. The parameters are stored permanently.

The configuration parameters can be adapted during operation. The user is responsible for the correct functionality of the connected devices (e.g. when changing the PAD profiles...).

3.4.9 Diagnostics

The ipTNA runs a self-test each time it restarts following a power loss.

The communication channels are monitored with the aid of the status message. No additional remote diagnostics possibilities are provided.

The ipTNA contains a monitoring function to run a restart due to a software failure.

3.4.10 Software update (remote)

A software update consists of the following steps:

- The openTAS server sends the FTP server access information to the ipTNA (server IP, user ID, password, file name...)
- The ipTNA retrieves the image from the FTP server and stores it in the volatile memory.
- The ipTNA interrupts its normal operation.
- The new image is programmed into the Flash memory.
- The ipTNA is restarted with the new software.

The following conditions are fulfilled:

- There is always at least one boot loader on the ipTNA. The boot loader is used to establish a connection with the server in the event of loss of the user software. (e.g. voltage loss during the programming of the Flash memory)
- The transmitted software image file is checked prior to programming in the Flash (checksum). If the check is negative, the ipTNA is started with the old software.

3.5 Power supply

3.5.1 Power supply

The ipTNA is powered by an external AC/DC power supply unit (10 to 30VDC). Power supply variants include an optional power supply module, a commercial plug-in power supply unit or the power supply from the alarm system. We recommend that the power supply unit be rated for a voltage of 15V and an output of 15W.

As auxiliary equipment an appropriate power supply is available (item no. 80 000 588)

3.5.2 Back-up battery (battery)

A battery charger is integrated in the ipTNA. Two optional battery packs of 6 cells each (NiMH) are available:

- Battery NiMH 7.2V, 2700mAh (item no. 80 000 423)
- Battery NiMH 7.2V, 4500mAh (item no. 80 000 675)

The battery packs are supplied uncharged and are secured to the housing base by a Velcro fastening.

If the supply fails (DCin), the ipTNA automatically switches over to battery mode.

The stored energy time depends greatly on the functions to be processed. The average stored energy time at 2700mAh is about 18 hours.. The 30 hours autonomy according to the standard EN 50131 can be reached with the 4500mAh battery.

When the ipTNA is running on battery, various function blocks may switch to power-saving mode after a set amount of time.

Replacing batteries:

Improper replacement of the battery can pose an explosion hazard. Replace only with the same type or an equivalent type recommended by the manufacturer. Dispose of used batteries in accordance with manufacturer's instructions.

3.6 Mounting

3.6.1 ipTNA wall-mounting case

- Space for:
- ipTNA ("snapped into place")
 - Battery (secured with Velcro fastener)
- Material: Plastic, UL 94 V0
 - Colour: grey
 - Dimensions: H = 252 mm, W = 191 mm, D = 43 mm
 - IP class of protection: min. IP30, max. depending on installation (surface-mounted, flash-mounted or sealed).
 - Location plan

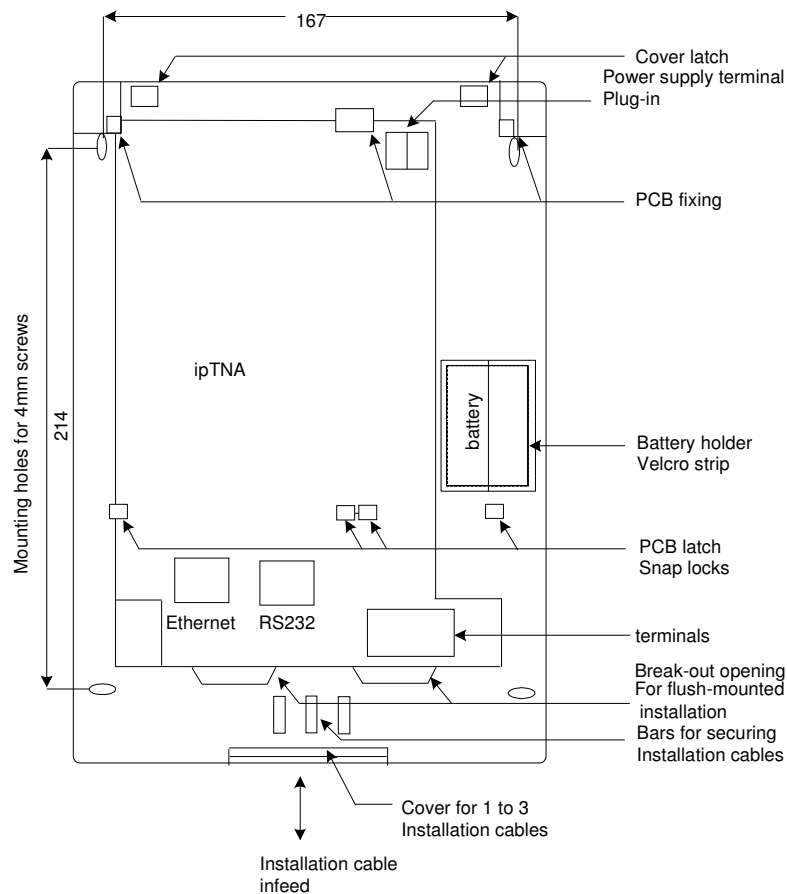


Fig. 13 Wall-mounting case for ipTNA

3.6.2 Wall mounting

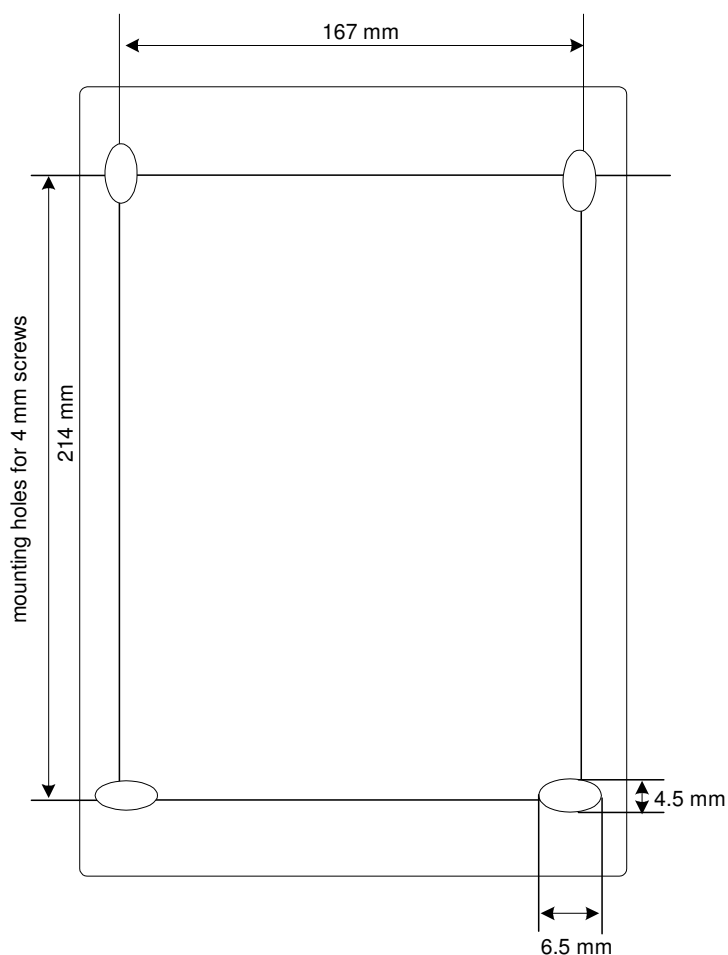


Fig. 14 Housing base

Fixing elements required:

- on concrete/masonry:
Nylon dowel plug 6 mm \varnothing x 30 mm and screw 4 mm \varnothing x 30 mm
- on timber:
with wood screws 4 mm \varnothing x 35mm
- on metal: with screws M4 x 8 mm

Each screw is to be used with a washer \varnothing 4.5 mm.

3.7 Cable connections

The connection of the cables to the corresponding terminals can be found in the Figure in Chapter 3 Operating Instructions.

Make sure the cables are fed cleanly through the openings in the cable entry panel. Make sure the appropriate strain relief device is provided.

4 Appendix

4.1 Monitoring classes

Traffic type	Time interval between Alive msg. on primary communication	Time interval between Alive msg. on secondary communication	Poll freq if only secondary communication is operative
S20	10 sec	300 min	tbd
M3	2.5 min	300 min	tbd
M15	12 min	300 min	tbd
M30	20 min	300 min	tbd
T1	45 min	25 hours	tbd
T5	4.5 hours	24 hours	tbd
T25	24 hours	NA	NA

4.2 Alive interval in dual channel mode

(in this example the ethernet channel is the primary path)

- t1 Supervision cycle on Ethernet (configurable)
- t2 Alive response waiting time (fix and less than t1, t3 and t4)
- t3 Supervision cycle on GSM (configurable)
- t4 SecondaryToPrimary supervision cycle on GSM (configurable)

temporary using of the secondaryToPrimary interval on secondary channel (if no special interval is defined, the primary path interval is used instead)

Ethernet (primary)		GSM (secondary)	
timeout t1	start t1, start t2 tx alive	:	:
<i>rx ack</i>	stop t2	:	:
:	:	timeout t3	start t3, start t2 tx alive
timeout t1	start t1, start t2 tx alive	<i>rx ack</i>	stop t2
<i>rx ack</i>	stop t2	:	:

:	:	:	:
timeout t1	start t1, start t2 tx alive	:	:
:	:	:	:
1. timeout t2	start t1, start t2 tx alive	→	start t4 , start t2 tx alive
2. timeout t2	start t1, start t2 tx alive	<i>rx ack</i>	stop t2
3. timeout t2	start t2 aliveCheck fails to control 1)	:	:
timeout t2	start t2	timeout t4	start t4 , start t2 tx alive
timeout t2	if logged on then start t2 and tx alive else start t2	<i>rx ack</i>	stop t2
logged on	start t2 and tx alive	timeout t4	start t4 , start t2 tx alive
:	:	<i>rx ack</i>	stop t2
:	:	:	:
rx ack	stop t2 start t1	→	start t3, start t2 tx alive
:	:	<i>rx ack</i>	stop t2
timeout t1	start t1, start t2 tx alive	:	:
<i>rx ack</i>	stop t2	:	:
:	:	timeout t3	start t3, start t2 tx alive
timeout t1	start t1, start t2 tx alive	<i>rx ack</i>	stop t2
<i>rx ack</i>	stop t2	:	:
		:	:

1) control closes and reopens the connection, if connected again, the logon sequence is exchanged

4.3 Repetition of user messages

Unacknowledge messages are retransmitted at the following moments:

- the repetition timer expires and a connection exists
- there is a new change of the same input
- change of the communication status (disconnected to connected) and the repetition timer has expired while disconnected

Repetition intervals (assumed that a connection is established):

case 1: Error response received

The reason for an error response can be the absence of the target ARC. As long as an error response is received, the messages are retransmitted in the following intervals (in seconds) :

- 10, 10, 10, 10, 30, 30, 60, 300, 600, 3600, 3600, 3600...

case 2: No response received

If there is no response at all e.g. communication error, the repetition intervals are

- 7, 7, 7, 10, 10, 30

the 1st and 3rd repetition are sent over the secondary path. As soon as the primary path is marked as disturbed, all further messages are (re)transmitted on the secondary path.

If no communication path is available, the repetitions are suspended until a new connection is established. (see reconnection times)

4.4 Reconnection intervals

There are the following three possibilities for the ipTNA to detect a communication interruption:

1. a socket close is received
this is the normal graceful way, which never happens, because the openTAS system never closes a working connection to an ipTNA
2. the ethernet physical interface or the gsm module detects an interruption

3. the second repetition of the alive message isn't responded by openTAS

In this situation the ipTNA closes its connection

If the actual connection is closed by one of the above-mentioned reasons, the reconnection tries are done in an increasing time interval (in seconds)

on ethernet	3...5, 5...17, 17...53, 53...139, 139...257, 139...257, ...
on gprs	1...3, 3...5, 3...5, 5...7, 7...17, 17...139, 139...557, 557...1759, 557...1759, ...

The values in the table are the time ranges. The value is chosen randomly out of the actual range. If the connection cannot be established, the next range is used.

Remark:

The reconnection intervals in the table are the duration of the pauses between two tries. The duration of the try itself is not contained in this time. An unsuccessfully try on ethernet takes about 2 minutes and on gprs it varies depending on the actual connection possibilities to the GPRS system and/or to the openTAS system.

4.5 Fixed time values

Name	Value [s]	
input blockingTime	3	for all digital inputs, a new reading of the actual value is suspended for the duration of the blocking time, after a successful evaluation.
DTR active to inactive integration time	10	DTR signal of serial interface
DTR inactive to active integration time	10	DTR signal of serial interface
Accu active to inactive integration time	1	accu voltage falls below lower limit
Accu inactive to active integration time	60	accu voltage rises lower limit
DC with accu active to inactive integration time	3600	DC voltage falls below lower limit and an alternative power supply is available
DC without accu active to inactive integration time	1	DC voltage falls below lower limit and no alternative power supply is available
DC inactive to active integration time	60	DC voltage rises lower limit
LocalFaultContact delay timer	20	a configured local fault contact is only activated, if the detected failure is present for longer than a minimal time
S3 activating time	5	minimal S3 activating time for a device reset
ftp result indication on L5	30	indication time of the ftp check result at startup
SW DL max time for instruction file	60	maximal time for the download of the instruction file (not for the ftp transfer !)
SW DL max time for ftp transfer	600	maximal time for the download of the imagefile from the ftp server

4.6 Time synchronisation

Each alive response contains the actual openTAS time. If the ipTNA receives 3 successive responses with a time difference > 2 seconds to its own time, the time of the ipTNA is synchronised.

4.7 Error outputs for PAD profiles 7xxx

code	name	meaning
03	data failure	format not : 90 (code for tss17) 12 character (tss17 header) 30 (code for Blockmessage) min. 1 character (user data)
05	communication failure	no communication path available
06	destination failure	negative acknowledge (error message) from openTAS received (e.g. ARC not connected)

4.8 Software download progress indications

download Progress	Meaning
0	<i>no download active</i>
1	<i>instruction file received</i>
2	<i>SW image download from ftp server started</i>
3	<i>Writing of SW image into FLASH memory started</i>
Abort causes	
40	<i>UndefinedCause</i>
41	<i>ModeChangeError</i> Change from Ethernet to Gprs downloadmode not possible due to a running download
42	<i>InstrFileChecksumError</i> Checksum of instruction file is wrong
43	<i>InstrFileTimeout</i> Instruction file download time exceeded
44	<i>InstrFileFormatError</i> Instruction file has wrong format
45	<i>InstrFileAuthenticError</i> (actual not supported) Authentication failure of instruction file
50	<i>FtpClntTimeout</i> ftp connection time exceeded
51	<i>FtpClntNoConnection</i> No connection to the ftp server possible
52	<i>FtpClntNoFile</i> Requested file not found on server

53	<i>FtpClntTransferError</i> ftp transfer error
54	<i>FtpClntNoDataError</i> no more data received from server
55	<i>FtpClntGsmInitError</i> GSM ftp connection could not be established
56	<i>FtpClntGsmConnError</i> Internal GSM ftp error

4.9 List of Abbreviations and Terminology

CAT-5 S/FTP	Category 5 S creened / F oilshielded T wisted P air cable
CAT-5 F/FTP	Category 5 F oilshielded / F oilshielded T wisted P air cable
CAT-5 SF/FTP	Category 5 S creened and F oilshielded / F oilshielded T wisted P air cable
DCE	D ata C ommunication E quipment (Modem)
DHCP	D ynamic H ost C onfiguration P rotocol
DTE	D ata T erminal E quipment (Terminal)
DTR	D ata T eminal R eady
FTP	F ile T ransfer P rotocol
GPRS	G eneral P acket R adio S ervice
GSM	G lobal S ystem for M obile communication
IP	I nternet P rotocol
ipTNA	Ip end-user terminal
MAC address	M edia A ccess C ontrol (LAN address)
NAT	N etwork A ddress T ranslation
openTAS	open T eleaction S ystem
PAD	P acket A ssembler / D isassembler
PCB antenna	P rinted C ircuit B oard
Primary installation	Customer-specific equipment
RJ45	R egistered J ack (standardised socket)
RS232	R adio S ector 232 (EIA-232 interface)
SIM – Card	S ubscriber I dentity M odule (chipcard)
TEE	T erminal equipment with serial interface
TEG	T erminal with contacts
TNA	End-user terminal
TSS	User-network interface between TEE/TEG and TNA

4.10 Declaration of conformity

4.10.1 TNA-IPSN-1



**EU/UE
KONFORMITÄTSERKLÄRUNG
DECLARATION OF CONFORMITY
DECLARATION DE CONFORMITE**

Wir, We, Nous **Ascom (Schweiz) AG**

(Name des Anbieters) (supplier's name) (nom du fournisseur)

Glutz-Blotzheim-Strasse 1
CH-4503 Solothurn

(Anschriřt (address) (adresse)

**erklären in alleiniger Verantwortung, dass das Produkt
declare under our sole responsibility that the product
déclarons sous notre seule responsabilité que le produit**
TNA-IPSN-1

Typ: TNA-IPSN-1
Artikelnummer: 80000428
Hersteller: Ascom (Schweiz) AG, Solothurn, CH

(Bezeichnung Typ oder Modell, Los-, Chargen- oder Seriennummer, möglichst Herkunft und Stückzahl)
(Name, type or model, lot, batch or serial number, possibly sources and numbers of items)
(nom, type ou modèle, no de lot, d'échantillon ou de série, éventuellement sources et nombre d'exemplaires)

**auf das sich diese Erklärung bezieht, mit der/den folgenden Norm(en) oder normativen
Dokument(en) übereinstimmt.
to which this declaration relates is in conformity with the following standard(s) or other
normative document(s).
auquel se réfère cette déclaration est conforme à la (aux) norme(s) ou autre(s) document(s)
normatif(s).**

EN 61000-6-3:2001
EN 55022/A2:2003 (ClassB)
EN 50130-4/A2 :2003

(Titel und/oder Nummer sowie Ausgabedatum der Norm(en) oder der anderen normativen Dokumente)
(title and/or number and date of issue of the standard(s) or other normative document(s))
(titre et/ou no et date de publication de la (des) normes(s) ou autre(s) document(s) normatif(s))

**Gemäss den Bestimmungen der Richtlinie(n); following the provisions of Directive(s);
conformément aux dispositions de(s) Directive(s).**
(falls zutreffend) (if applicable) (le cas échéant)

RL 89/336/EWG, RL73/23/EWG

Solothurn, 10. Februar 2006

Martin Pfander 

Ort und Datum der Ausstellung) (Name und Unterschrift oder gleichwertige Kennzeichnung des Befugten)
(Place and date of issue) (name and signature or equivalent marking of authorized person)
(Lieu et date) (nom et signature du signataire autorisé)

4.10.2 TNA-IPSN-GSM-1



**EU/UE
KONFORMITÄTSERKLÄRUNG
DECLARATION OF CONFORMITY
DECLARATION DE CONFORMITE**

Wir, We, Nous **Ascom (Schweiz) AG**

(Name des Anbieters) (supplier's name) (nom du fournisseur)

Glutz-Blotzheim-Strasse 1
CH-4503 Solothurn

(Anschrift (address) (adresse)

**erklären in alleiniger Verantwortung, dass das Produkt
declare under our sole responsibility that the product
déclarons sous notre seule responsabilité que le produit**
TNA-IPSN-GSM-1

Typ: TNA-IPSN-GSM-1
Artikelnummer: 80000429
Hersteller: Ascom (Schweiz) AG, Solothurn, CH

(Bezeichnung Typ oder Modell, Los-, Chargen- oder Seriennummer, möglichst Herkunft und Stückzahl)
(Name, type or model, lot, batch or serial number, possibly sources and numbers of items)
(nom, type ou modèle, no de lot, d'échantillon ou de série, éventuellement sources et nombre d'exemplaires)

**auf das sich diese Erklärung bezieht, mit der/den folgenden Norm(en) oder normativen
Dokument(en) übereinstimmt.
to which this declaration relates is in conformity with the following standard(s) or other
normative document(s).
auquel se réfère cette déclaration est conforme à la (aux) norme(s) ou autre(s) document(s)
normatif(s).**

EN 61000-6-3:2001
EN 55022/A2:2003 (ClassB)
EN 50130-4/A2 :2003

(Titel und/oder Nummer sowie Ausgabedatum der Norm(en) oder der anderen normativen Dokumente)
(title and/or number and date of issue of the standard(s) or other normative document(s))
(titre et/ou no et date de publication de la (des) norme(s) ou autres(s) document(s) normatif(s))

**Gemäss den Bestimmungen der Richtlinie(n); following the provisions of Directive(s);
conformément aux dispositions de(s) Directive(s).**
(falls zutreffend) (if applicable) (le cas échéant)

RL 89/336/EWG, RL73/23/EWG

Solothurn, 10. Februar 2006

Martin Pfander

(Ort und Datum der Ausstellung) (Name und Unterschrift oder gleichwertige Kennzeichnung des Befugten)
(Place and date of issue) (name and signature or equivalent marking of authorized person)
(Lieu et date) (nom et signature du signataire autorisé)