iris touch

IP security to go

IRIS Touch and Honeywell GT Dialler Installation Guide for LPS1277 Compliant Applications

Version 1.3

Now certified and compliant with EN50131, EN50136 Security Grade 4 ATS6

Contents

1. Background

The IRIS Touch range of alarm over IP diallers is certified to be compliant with the European standards for Intruder and Fire Alarm transmissions and also to the additional requirements for the UK specific standard LPS1277: Requirements for LPCB Approval and Listing of Alarm Transmission Equipment. The same is true for the Honeywell GT range of diallers, but for Intruder Alarms only, not Fire.

For this LPS standard there are special instructions for the installer, which are detailed in this document.

2. Requirements for the Monitoring Centre

For support of IRIS Touch and Honeywell GT diallers at the supervised premises, the monitoring centre must use Chiron's IRIS Secure Apps alarm receiving system.

The IRIS Secure Apps system must be set up so that in System Settings, System Features, 'Automatic Security Key Change' is enabled (ticked).

Each dialler is given a 'template' that defines its operating parameters such as fault reporting period. To ensure compliance with LPS1277, the following settings must be applied to these templates:

- 'Enable auto security key'.
- Peripheral connection 'Panel' if the dialler is from the IRIS Touch range and connection between the alarm system and the dialler is the 'dial capture interface', or the dialler is from the Honeywell GT range.
- Peripheral connection 'Pins' if the connection between the alarm system and the dialler is the dialler 'pin' inputs.
- In the IRIS Secure Apps System Settings -> Global Settings, the 'General Poll Overdue Margins' should all be set as follows:

  Fixed = 0 seconds

  Percentage = 0%

  Threshold = 0 seconds

Templates settings depend on the ATS performance parameters required (ATS 1 to 6) and should be set as maximum to the values shown in the table below.

A) Poll period
B) Poll overdue margin
C) Ethernet reporting time (where dual path is used)
D) GPRS reporting time (where dual path is used)
E) Background checking interval (where dual path is used)
F) Background retry interval (where dual path is used)

ATS	A	B	C	D	E	F
1	24h	50m	0s	4h	24h	10m
2	24h	50m	0s	4h	24h	10m
3	24h	50m	0s	4h	24h	10m
4	4h	50m	0s	4h	24h	10m
4 plus	6m	3m	0s	4h	24h	10m
5	1m	100s	0s	4h	4h	10m
6	10s	0s	0s	0s	4h	10 m

s = seconds
m = minutes
h = hours

Note – if a faster polling period is required, e.g. to offer quicker remote access, it is allowable to decrease the poll period (A) and increase the poll overdue margin (B) as long as the sum of the two is no higher than the sum of the two in the table above.

3. Installation guidance for LPCB approved supervised premises transceivers (SPT) connected to Intrusion & Hold up Alarm Systems (I&HAS)

This 'Best Practice' guidance on installation practices will help enhance general Alarm Transmission System (ATS) security/ resilience, avoid undue (false) path failure reports and reduce customer inconvenience.

Important Notes

1) A claim to have installed LPCB approved SPT will be invalid if this guidance has not been followed.

2) Within this guidance the word 'shall' indicates a mandatory requirement. Use of the word 'should' indicates a requirement unless practical constraints prevent compliance.

3.1. Installation (alarm company) Information

3.1.1. Location and alarm protection of the Supervised Premises Transceiver (SPT)

i) The SPT part of the Alarm Transmission Equipment (ATE), shall be located within the I&HAS Control and Indicating Equipment (CIE), or within an enclosure that shares the same mains power supply, and has the same level of battery back up and tamper protection, as is required for the associated CIE.

ii) The location of the CIE, or other enclosure, containing the SPT;

- shall, when installed as part of a new I&HAS; be in an area provided with 'direct alarm protection' [a)] and be located where it is not visible to, or readily accessible by, members of the public.
- should, when retro-fitted to a pre-existing I&HAS; be in an area provided with 'direct alarm protection'[a)] and be located where it is not visible to, or readily accessible by, members of the public.

3.1.2. Alarm protection of Site Network Equipment

i) 'Site Network Equipment'[b)] that can be switched off or which has a locally or remotely accessible and changeable function, (e.g. a telephone switchboard

or IP router), together with Alarm Transmission Path (ATP) aerials* and network access termination points, shall be located in an area provided with 'direct alarm protection' [a)].

ii) Other 'Site Network Equipment' [b)], for example intermediate junction boxes, should be provided with 'direct alarm protection' [a)].

* Where an ATP aerial cannot be located in an area readily provided with 'direct alarm protection' [a)] and still achieve the recommended minimum signal strength for adequate performance, it may be installed elsewhere (preferably indoors but otherwise outdoors), subject to positioning it where its discovery and/or ready access by intruders is considered unlikely.

3.1.3. Connections between the SPT and Site Network Equipment b)

i) Any radio based ATP shall have a cable connection between the SPT and the required aerial, with all cable termination points, including those at any intermediate connections, using termination components (or housings) that protect against cable removal without the use of a tool.

ii) Any landline based ATP shall have a cable connection between the SPT and the first suitable alarm transmission network termination point within the premises. This shall be made in one continuous run and use termination components (or housings) that protect against cable removal without the use of a tool.

The connection to the alarm transmission network shall be made in such a manner that where non-alarm related apparatus/services are also connected to that network, they do not prevent, or interfere with, the correct operation of the ATS.

Notes.

a) The phrase 'direct alarm protection' shall mean that sufficient detection devices are installed to ensure that, when the I&HAS is set, access to the protected equipment results in a full (e.g. a 'confirmed') alarm condition. Where an I&HAS uses a time delayed entry/exit route as part of the facility for unsetting, detection devices programmed to act as entry/exit route detection shall not be regarded as providing 'direct protection'.

b) The phrase 'Site Network Equipment' shall be regarded as all equipment installed within the alarmed premises through which signals from the SPT to the alarm transmission network beyond the perimeter of the premises are transmitted. For example, non-alarm dedicated (shared use) IP routers, telephone switchboards/Private Automatic Branch Exchanges (PABX), network access termination points, ATP aerials and communication network junction boxes/switches.

3.1.4. ARC/ATS message holding

Where the Alarm Receiving Centre (ARC) &/or ATS provider offers, or requests use of, a facility to block the receipt of, or hold information relating to, ATS fault notification signals or messages pending receipt of further alarm information (e.g. pending the designation of a confirmed alarm as per BS 8243), agreement to such an action shall be confirmed in writing by the customer (end user); with the relevant notification stating that this action is compatible with the risk assessment and/or the requirements of any interested party, for example an insurer.

In such cases the installer shall make suitable arrangements, which shall be confirmed in writing, for the customer to be alerted to any such ATS fault notification signals/messages when their alarm system is next unset, or after a period of 96 hours, whichever is the sooner.

3.2. Customer (end user) Information

Installers shall advise the customer:

i) of any potential for normal ATS functions, including normal or 'stepped up' checking of ATS availability (e.g. by sending test signals), which could interfere with, or prevent use of, any non-alarm related apparatus/services connected to a telephone line shared with the ATS. In such cases customers should be recommended to consider use of an ex-directory 'In Coming Calls Barred' (ICCB) telephone line dedicated to ATS use.

ii) of the adverse effect on reliable operation of their intruder alarm system that may result where 'Site Network Equipment' [b)] used by the ATS:-

- could have its correct operation/settings locally or remotely accessed and changed/disabled, for example a non-alarm dedicated (shared use) IP router. In such cases customers should be recommended to consider protection against unauthorised access by the use of an access password (not the factory default) and, if their equipment has wireless connectivity having the wireless network Access Point Name (APN) hidden.

- would cease to work in the event of loss of mains power; for example a Private Automatic Branch Exchange (PABX) or non-alarm dedicated (shared use) IP Router. In such cases customers should be recommended to consider protecting the power supply against disconnection by use of an unswitched fused spur connection or by having such equipment or its power supply connections located in an area/room to which unauthorised access is restricted.

iii) of the adverse effect on reliable operation of their intruder alarm system that may result from cessation of any communication service(s) necessary for correct operation of the ATS; for example telephony services such as 'three way calling' (Star Services) or access to internet services (via an ISP). In such cases customers should be recommended to take steps to ensure that availability of these services is maintained at all times when their alarm system is likely to be in use.

iv) that, where the performance of the SPT is capable of being changed after installation, such changes shall be confirmed in writing by the customer; with the relevant notification stating that any such change is compatible with the risk assessment and/or the requirements of any interested party, for example an insurer.

The future of security, secured

IP by security professionals, for the professional security industry

Telephone: +44 (0)118 988 0228
E: sales@chironsc.com
www.chironsc.com

Chiron Security Communications Ltd,
Wyvols Court, Swallowfield,
Reading, Berkshire, RG7 1WY UK