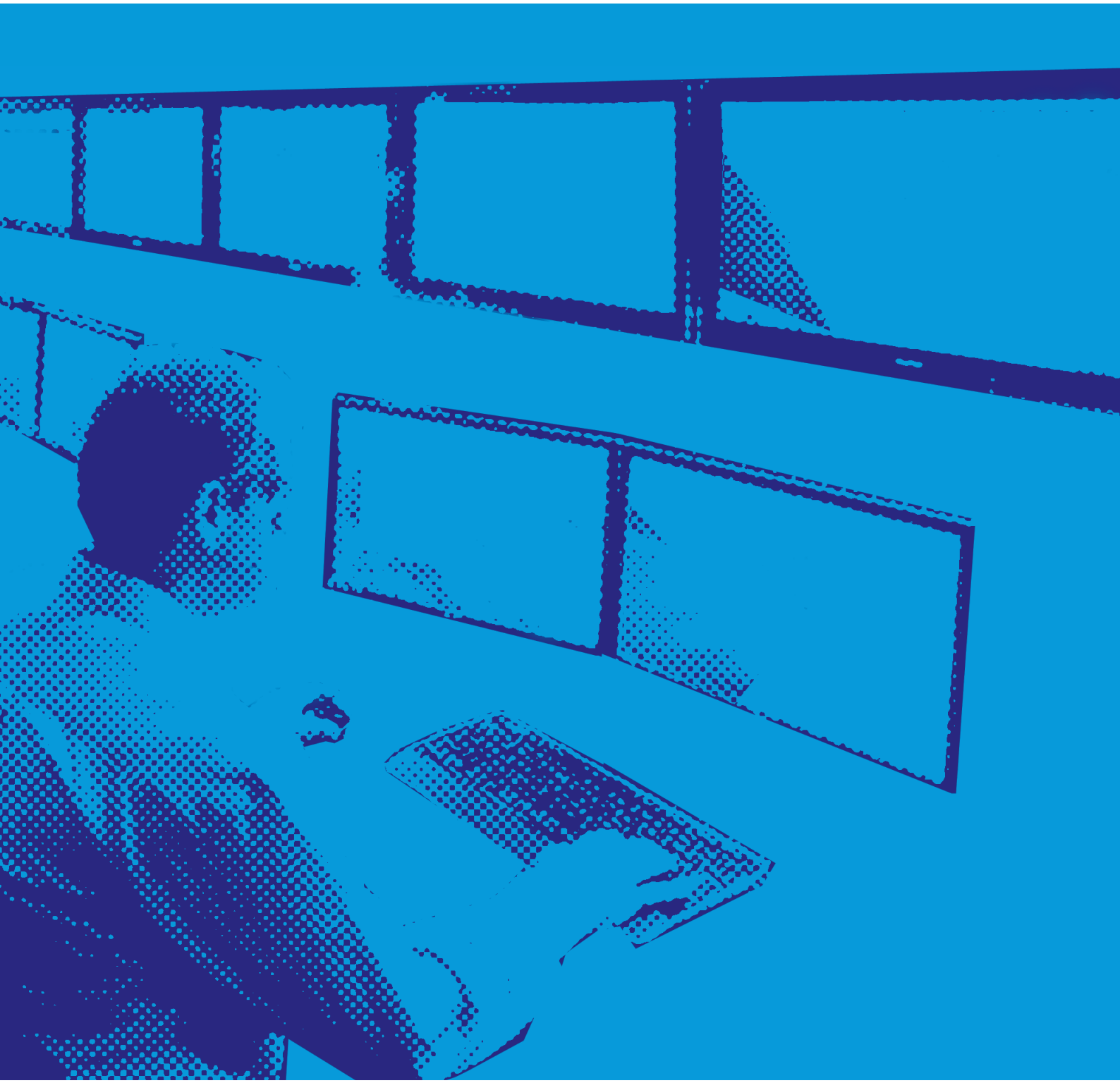
SB 02.2011
Version 01

Security Bulletin

Alarm Transmission Systems (ATS) – Loss Prevention Certification Board (LPCB) launches revised Loss Prevention Standard, LPS1277 3.0



RISCAuthority
formerly InFiReS

administered by
FPA
Fire Protection Association

IMPORTANT NOTICE

This document has been developed through the RISCAuthority and published by the Fire Protection Association (FPA). RISCAuthority membership comprises a group of UK insurers that actively support a number of expert working groups developing and promulgating best practice for the protection of people, property, business and the environment from loss due to fire and other risks. The technical expertise for this document has been provided by the Technical Directorate of the FPA, external consultants, and experts from the insurance industry who together form the various RISCAuthority Working Groups. Although produced with insurer input it does not (and is not intended to) represent a pan-insurer perspective. Individual insurance companies will have their own requirements which may be different from or not reflected in the content of this document.

The FPA has made extensive efforts to check the accuracy of the information and advice contained in this document and it is believed to be accurate at the time of printing. However, the FPA makes no guarantee, representation or warranty (express or implied) as to the accuracy or completeness of any information or advice contained in this document. All advice and recommendations are presented in good faith on the basis of information, knowledge and technology as at the date of publication of this document.

Without prejudice to the generality of the foregoing, the FPA makes no guarantee, representation or warranty (express or implied) that this document considers all systems, equipment and procedures or state-of-the-art technologies current at the date of this document.

Use of, or reliance upon, this document, or any part of its content, is voluntary and is at the user's own risk. Anyone considering using or implementing any recommendation or advice within this document should rely on his or her own personal judgement or, as appropriate, seek the advice of a competent professional and rely on that professional's advice. Nothing in this document replaces or excludes (nor is intended to replace or exclude), entirely or in part, mandatory and/or legal requirements howsoever arising (including without prejudice to the generality of the foregoing any such requirements for maintaining health and safety in the workplace).

Except to the extent that it is unlawful to exclude any liability, the FPA accepts no liability whatsoever for any direct, indirect or consequential loss or damage arising in any way from the publication of this document or any part of it, or any use of, or reliance placed on, the content of this document or any part of it.

CONTENTS

Following the recent publication of the RISCAuthority document S15: **Guidance on evaluating the performance of alarm transmission systems for use with intrusion and hold-up alarm systems**, LPCB has issued a guide to its revised approval scheme for alarm transmission equipment (ATE).

Titled **LPCB: The benefits of LPS 1277 – A specifiers guide**, the document can be viewed here. A copy of LPS 1277 can be downloaded from www.redbooklive.com

1. LPS 1277 – KEY FEATURES FOR I&HAS

The LPS 1277 scheme has been designed to cover products intended for use with both fire and security systems; this bulletin is limited to security systems (I&HAS). The LPCB believes that its scheme addresses many of the issues raised in the RISCAuthority S15 document.

The LPCB states that ATS products that achieve LPS 1277 approval have been assessed as meeting the relevant parts of the BS EN 50131/6: **Alarm systems** series plus some additional requirements including:

- For all ATS products, 'Availability' is assessed using a live network.
- For dual path ATS products, recognition that they may employ a third (duplicate) alarm transmission path, ie a path using the same general technology as another, eg radio, but a different transmission protocol; the aim being to maintain connectivity and thus avoid reporting spurious short-term path failures. Any such duplicate path is assessed and tested to ensure it comes into use within the relevant maximum fault reporting time of the path it is intended to replace, and once in use performs to the same level as that path.
- For dual path ATS products, creation of a maximum fault reporting category for catastrophic failure, ie total loss of both paths, for example if the power supply to the alarm transmission equipment (ATE) fails or it is destroyed (eg smashed by an intruder).
- For dual path ATS products, creation of a new fault reporting time category of ATS4+. This mirrors the requirements for ATS4 within the BS EN 50131/6 series except that it has an enhanced maximum primary path fault reporting time of 10 minutes and a catastrophic failure reporting time of 11 minutes. As such it may provide a more acceptable (lower cost) solution than 'grade' 4 (ATS5) ATS, eg for use in lower risk situations.
- For dual path ATS products, a requirement for the secondary path to be immediately checked for correct operation once the primary path has failed, for the secondary path to then 'step up' its performance to match that of the primary and to maintain this until either the primary path is restored or a period of 96 hours elapses – whichever is the sooner.

These various requirements are also said to be capable of being met, and are accordingly assessed, irrespective of the nature of the technology/systems used, ie whether or not the ATS might be regarded as using 'traditional' or 'IP' technology.

2. LPS 1277 - ANNEX C

This clarifies that the potential pitfalls of ATS products used with I&HAS do not necessarily relate to the designed performance alone.

It suggests that specifiers need to be alert to the adverse effects that may be introduced by the various installation/configuration practices adopted, controlled or influenced by others, e.g. the installer, Alarm Receiving Centre (ARC), the ATS provider's Management Centre or the customer. To help counter this, LPS1277 requires all ATS products that seek LPS1277 approval to reproduce in their supplied fitting instructions a set of good advice as may be found in LPS1277 Annex C.

The information contained in Annex C could be partially or wholly reproduced by specifiers in their own ATS related instructions.

Note: Some of the content of Annex C reflects issues previously raised by IPCRes (forerunner of the RISCAuthority Security Group) in their 'model' for accepting IP-based ATS.

To help specifiers understand the content of Annex C, it is reproduced as Appendix 1 of this document, by kind permission of the LPCB, together with a short explanatory RISCAuthority commentary in italics.

3. SUMMARY

In recent years, the introduction of new types of I&HAS, eg confirmation systems and European Grades, has greatly increased complexity for those parties who wish to specify or accept appropriate I&HAS at their customers' premises. The range of ATS products has become similarly complicated with the development of new technologies, eg radio and IP signalling.

Third party certification schemes and standards are already well embedded concepts for reliable and impartial product specification. By following such a course of action, the choice of which particular branded product to deploy can be delegated to the installer/end user, and thus reflect their own commercial and operating requirements.

LPCB reports that several ATS products have now received LPS 1277 3.0 approval and that others are being processed.

Other issues specifiers may wish to consider when specifying/recommending ATS products include:

- whether or not the available telephony networks or IT services at a customer's premises, or the customer's own telephony or IT infrastructure, is suited to a particular class or type of product. For example, some network services may not be available in some areas, may not have adequate reliability (eg poor radio signal strength or internet connection) or some ATS products may not work over certain networks.
- whether or not a reliable prime power source (eg mains power) exists at a customer's premises, and, if it does not, whether some or all of the ATS transmission paths will continue to operate in the event of loss of that power. For example, 'traditional' ATS typically use power provided via the (battery backed up) I&HAS control panel and/or from the connected telephony network; whereas, unless special arrangements are made, an IP alarm transmission path connected to the internet via a standard router will usually cease to work if power to the router is lost.
- whether the ATS product provider offers a 'managed' network service, ie accepts some responsibility for alarm/event transmission, fault diagnosis, etc.

APPENDIX 1 – ANNOTATED COPY OF LPS 1277 ANNEX C

10 ANNEX C

10.1 Installation guidance for LPCB-approved supervised premises transceivers (SPT) connected to intrusion and 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.

Installation (alarm company) information

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.

This reiterates current standards rules for such equipment.

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 retrofitted 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.

This reiterates current standards rules for such equipment, and the need to achieve adequate alarm protection (see Note a) below), with the second bullet recognising that with retro fits to older systems the layout of the premises vis a vis the installed CIE and its capabilities (eg type of entry/exit programming available) may make this impractical.

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, (eg 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].

This aims to ensure that certain vital equipment (see Note b) below) at the premises, and through which alarm signals may be routed, are located in an area having adequate alarm protection.

ii) Other 'site network equipment' [b], eg intermediate junction boxes, should be provided with 'direct alarm protection' [a].

This recognises that not all site network equipment can be located within an area with 'direct alarm protection' and that specific protection measures may need to be implemented.

* 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.

This recognises that it is not always possible to get good a radio signal with the aerial located inside the protected premises, and that it is sometimes better to site the aerial outside the protected area, either inside or outside the premises to achieve a good signal strength for stability and reliability.

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.

This aims to ensure the aerial of ATE using radio cannot simply be unplugged or removed, eg by locating the aerial and/or its terminations within a secondary enclosure.

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.

This excludes the use of local unsecured wireless links, such as Bluetooth, to provide the interconnection between the SPT and the first suitable alarm transmission network termination point within the protected premises.

Requiring the use of one continuous cable run minimises the number of termination points that must be protected and will no doubt provide better long term reliability.

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.

This statement is intended to draw the attention of installers to the potentially adverse effects that may occur if other equipment such as telephones or fax machines share the path and are in competition with system signal or, in the case of IP paths, the possibility at least that performance is affected by heavy use applications such as streaming video.

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 (eg 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.

This provides a definition of equipment that clarifies and expands upon standards rules.

ARC/ATS message holding

Where the alarm receiving centre (ARC) and/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 (eg pending the designation of a confirmed alarm as per BS 8243: 2010: **Installation and configuration of intruder and hold-up alarm systems designed to generate confirmed alarm conditions. Code of practice**), agreement to such an action shall be confirmed in writing by the customer (end user). The relevant notification should state 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.

This aims to ensure adequate records are maintained, and specifically, that the customer's attention is drawn to the implications of any such action, including any impact on their insurance cover.

It has generally been accepted in the past that with dual path ATS, any transmission path fault that exists beyond the maximum allowed fault reporting time should always be immediately notified to the ARC and that, thereafter, the ARC (nowadays typically treating such an event as an 'unconfirmed' event) will notify a keyholder. The usual insurer expectation would then be that the keyholder attends site to investigate/resolve the problem, not least as the performance/reliability of a 'secondary' path, if that is the one that remains, can vary so much.

However, where intruders may have initiated the path fault report, eg by cutting telephone lines, and they are waiting to see what happens next, this situation can introduce safety risks to keyholders attending premises and related risks (duress) to the security of the premises.

Because of the LPS1277 requirements for dual path ATS products to be able to quickly check that after a primary path failure report a secondary path is operating as expected and/or quickly report any catastrophic failure (failure of both paths within a short time (typically a maximum of one minute, or 30 seconds at ATS 5 and above) specifiers may consider that holding the first received path failure report message is a reasonable trade off, (ie safety versus security). This may be particularly true where the ATS performs at ATS5 or above, as if the remaining path of such systems fails outside of the allowed catastrophic failure report time it will be reliably and quickly detected within (in the context of typical criminal events) a relatively short time interval (ie a time equal to the normal primary path fault reporting time).

10.1.1 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 (eg 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 'incoming calls barred' (ICCB) telephone line dedicated to ATS use;

This aims to ensure that ATS do not cause inconvenience to end users, and by so doing minimise the possibility of them taking their own steps to reduce such interference and perhaps inadvertently affecting the ATS.

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;

This aims to ensure that equipment over which the end user has ongoing control, has a degree of security against unauthorised interference.

- 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;

This aims to ensure that equipment over which the end user has ongoing control, has a degree of protection against unauthorised power disconnection

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; and

This aims to ensure that the importance of wider services required for correct operation of the ATS, and over which customers have ongoing control, are brought to customers' attention.

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, eg an insurer.

This aims to ensure adequate records are maintained, and, specifically, that the customer's attention is drawn to the implications of any such change, including any impact on the their insurance cover.

Fire Protection Association
London Road, Moreton in Marsh
Gloucestershire GL56 0RH, UK
Tel: +44 (0)1608 812500 Fax: +44 (0)1608 812501
Email: administrator@riscauthority.co.uk
Website: www.riscauthority.co.uk

Electronic copies may be obtained from www.riscauthority.co.uk.

RISCAuthority
formerly InFiReS

administered by
FPA Fire Protection Association