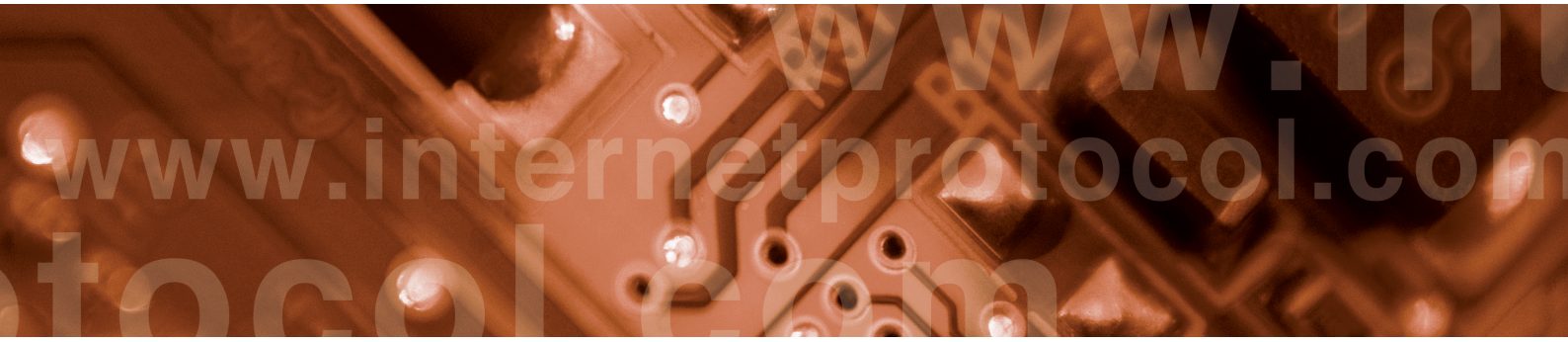
bsia
british security industry association

installation of IP-based
secure signalling systems for I&HAS
– an industry guide



May 2008

For other information please contact:

British Security Industry Association
t: 0845 389 3889
f: 0845 389 0761
e: info@bsia.co.uk
www.bsia.co.uk

Form No. 234. Issue 1

© This document is the copyright of the BSIA and is not to be reproduced without the written consent of the copyright owner.

Contents

Foreword

Information about this document

This guidance has been drawn up to assist all parties in the design and installation of IP-based secure signalling systems for use with Intruder and Hold Up Alarm Systems (I&HAS). It is intended to be used in conjunction with PD6662, Scheme for the Application of European Standards for Intruder and Hold-up Alarm Systems.

Use of this document

This document takes the form of guidance and recommendations. It should not be quoted as if it were a specification.

Introduction

The introduction of Internet Protocol (IP)-based technology into the field of secure signalling for I&HAS has led to confusion and uncertainties which have inhibited the exploitation of the benefits available by adopting it.

This guidance has therefore been prepared to provide a stable platform from which such systems can be designed, installed and maintained in a way that is acceptable to the industry as a whole, and can be inspected in a consistent way.

This guide may be supplemented by specific requirements of insurers on a system-by-system basis, see Annex A.

1. Scope

This guide applies to the design, installation and maintenance of I&HAS installed to comply with PD6662:2004, and which utilise IP-based technology for the notification of alarms and other information to an Alarm Receiving Centre (ARC). It is applicable to all forms of IP-based communication, e.g. “broadband” via PSTN, wireless, etc.

2. Normative references

PD6662:2004	Scheme for the Application of European Standards for Intruder and Hold-up Alarm Systems
prEN50131-1:2004	Alarm systems - Intrusion systems - Part 1: System requirements
TS 50131-7:2003	Alarm systems – Intrusion systems – Part 7: Application guidelines
EN50136-1-1:1998	Alarm systems - Alarm transmission systems and equipment Part 1-1: General requirements for alarm transmission systems
EN50136-2-1:1998	Alarm systems - Alarm transmission systems and equipment Part 2-1: General requirements for alarm transmission equipment
prEN50136-1-5:2006	Alarm systems - Alarm transmission systems and equipment Part 1-5: Requirements for Packet Switched Network PSN

3. Terms, definitions and abbreviations

Definitions and abbreviations used are as shown in EN50131-1; EN50136-1-1 and prEN50136-1-5, except as shown below:

Alarm transmission equipment (ATE)
Equipment which is used primarily for the transmission of alarm messages.

Alarm transmission system (ATS)
Equipment and network used to transfer information concerned with the state of one or more I&HAS to one or more alarm receiving centre.

Ethernet module or interface
This term is used in prEN50136-1-5 to identify the interface between the alarm system equipment (covered by EN50136-2-1) and the transmission network components.

Local area network (LAN)
A physical network installed and managed entirely by the user.

Receiving centre transceiver (RCT)

Supervised premises transceiver (SPT)
These terms (as defined in EN50136-1-1) are more specific than the generic "alarm transmission equipment" (ATE) and therefore preferred where relevant.

Transmission network components
Components, e.g. router, etc. forming part of the transmission network between SPT and RCT, some of which may be located at the supervised premises but do not form part of the ATE (see clause 4) and hence are not required to meet the requirements of EN50136-2-1.

This would typically be the case where alarm messages utilise the routing equipment of a client's LAN.

Wide area network (WAN)
A computer network that allows the connection of LANs and other networks to allow users and computers to communicate from one location to another.

4. Transmission network components

EN50136-1-1 clause 4.5 defines "alarm transmission equipment" as that "primarily" used for the transmission of alarm messages from the supervised premises. Note 2 permits exemptions for certain equipment, which could include modems/routers used for general purposes. The term "primarily" will have to be defined on a site-by-site basis by agreement with the client, and if applicable insurer, as part of the risk assessment.

In this connection, prEN50136-1-5, section 5 states:

Note 1: Transmission network components:

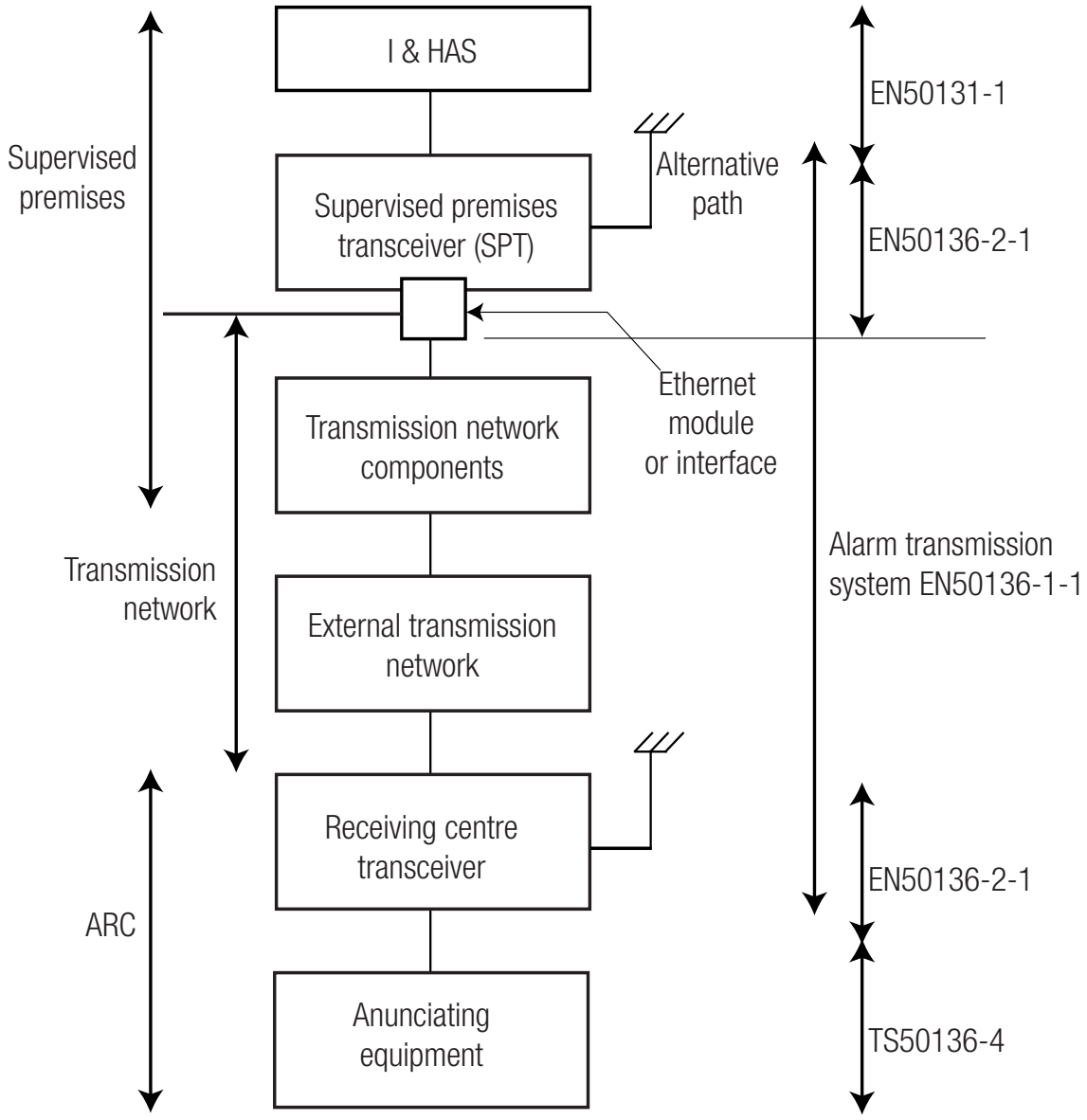
Network components including ADSL modems, SDSL modems, routers, ethernet switches, ethernet hubs, external firewalls and network wiring etc. may not meet the requirements in the standard for alarm transmission equipment in EN 50136-2-1.
Ethernet modules/interfaces at the alarm transceiver are not part of the transmission network.

Such transmission network components, which may be the responsibility of the client, may thus, under some circumstances, be considered part of the transmission network. In that case, these components are not part of the SPT and are thus not required to comply with the requirements of EN50136-2-1.

prEN50136-1-5 identifies that the ethernet module/interface at the SPT is NOT part of the transmission network. This therefore should meet all requirements of EN50136-2-1. This is true of the interface to any type of IP connection.

This is clarified by the Figure 1, illustrating which standards are applicable to the various equipment and interconnections. See also Annex A.

Figure 1



5. Recommendations

5.1 Location of equipment

The SPT (which includes the ethernet module or interface) should be located as close to the control and indicating equipment (CIE) as is practicable (see TS50131-7 clause 7.3.2). The network connection point should be as close to the I&HAS ethernet module or interface as is practicable.

If a wireless IP connection (example GPRS connection from SPT) is used, the antenna should be located in the most secure position possible commensurate with adequate signal strength. The wireless signal level at the time of installation should be recorded and a check made that it meets requirements.

5.2 Dual path systems

The point of decision as to the path to be used should be within the SPT or CIE (see Fig 1).

Where one path is routed via network transmission components not part of the ATE, the other path should comply with the relevant requirements of EN50136-2-1 and EN50131-1 table 11. All paths should have a contractual basis – e.g. not using a "pay-as-you-go" SIM.

5.3 Fault responses.

Fault, disconnection or loss of power of any network component, of any interconnection between those components or of any interconnection between the I&HAS ethernet module or interface and the network components within the supervised premises should result in an "ATS fault" response at the ARC and at the I&HAS within the reporting time specified, according to grade, by EN50131-1 Table 11.

Note: It is recommended that this fault response be available within 3 minutes, by use of ATS with fault reporting time of T4 at all grades.

5.4 Tamper security

The provision of tamper protection and detection for housings of transmission network components installed at the supervised premises is not mandatory.

Where such protection is not provided, design of the I&HAS should ensure that this equipment is located such that, when the I&HAS is set, it cannot be accessed without generating a confirmed alarm.

5.5 Interconnections

The provision of tamper detection for the ATS path, including intermediate interconnections between network components within the supervised premises, is not mandatory.

Where such detection is not provided, precautions should be taken to prevent accidental or unauthorised disconnection (example: connections requiring a tool for removal).

5.6 Power supply

5.6.1 Mains supply

Whilst secure connections (example: hard-wired fused spur) are preferred for mains connections to transmission network components within the supervised premises, these may be by plug and socket.

Where this is the case, precautions should be taken to prevent unauthorised disconnection (example: labelling or fixed cover to connection).

5.6.2 Secondary power supply

prEN50136-1-5, section 5 (Transmission network requirements) states:

Note 2: Network power fails reporting to alarm receiving centre:
Network equipment which is located at the supervised premises which is not classified as being part of the alarm transmission equipment is not required to have a secondary power supply.

Thus a secondary power supply is not mandatory for transmission network components installed at the supervised premises. The reference to "alarm transmission equipment" in this note should be understood to refer to the SPT.

5.6.3 Prime Power Source (PPS) Fault message

If a "PPS Fault" message for the I&HAS is required to be sent to the ARC (or other remote centre) in order to reduce the battery standby time as permitted by EN50131-1 clause 9.2, and the signalling path is dependent upon the presence of mains to transmission network components at the supervised premises, there should be means to transmit this message.

Note: The EN50131 family of standards is in the process of replacing PPS by "EPS – External Power Source."

Examples:

a) Provision in a single path system of a PSTN modem path.

b) The I&HAS may be provided with a second ATS path independent of the ethernet connection operating using an APS.

5.7 Integrity of performance

Where transmission network components at the supervised premises are excluded from the SPT, there is potential for disruption to the transmission of such messages in the event of failure of or disconnection of parts of the IT system. The following warning should be reproduced in the system design proposal and as-fitted document in bold type:

> **Important:** If your security system makes use of your broadband router/switch, any loss of service resulting from disconnection, failure, etc. of your equipment will generate a fault alarm resulting in the ARC contacting your premises or a keyholder.
>
> In these circumstances, alarm messages will not be sent currently to the ARC. They may be lost or delayed at your premises until the service is restored (dependant upon equipment type).
>
> The intention to transmit alarm messages and information via your IT equipment should be specifically advised to your insurers.
>
> Such IT equipment should be suitably managed, as required by clause 6.

Note: Assessment of the availability of the overall ATS (i.e. including equipment not dedicated for the I&HAS but forming part of the ATS) for a period of time is recommended in order to ensure that the system is fit for its intended purpose. Guidance may be found in EN50136-1-1, clause 6.4.

6. Management of IT system

Where transmission network components at the supervised premises used for alarm message transmission are excluded from the SPT and are the responsibility of the client, the system to which this equipment is connected should be managed to

a) Prevent unauthorised access to cables and connections affecting the integrity of the ATS whilst the I&HAS is unset.

b) Prevent unauthorised disruption to messages to/from the I&HAS.

c) Minimise disruption to messages to/from the SPT during planned or emergency maintenance

d) Ensure that the ARC and the I&HAS maintenance company are notified of such maintenance in advance.

Contractual agreement should detail the responsibilities of the client and I&HAS maintenance company in these areas and the responsibility for security issues during such periods. See also clause 5.8.

7. Service provision matters

7.1 Internet Service Provider (ISP)

The Broadband (Digital Subscriber Line) connection contract should not allow for service interruption resulting from excessive usage.

Changes to the DSL connection contract or ISP provider could result in breaks of service or other problems. The following warning should therefore be reproduced in the system design proposal and as-fitted document in bold type:

> **Important:** Your attention is drawn to the fact that changes to your broadband connection contract or Internet Service Provider could affect the ability of the system to deliver its designed performance and thus invalidate your insurance cover. You should therefore consult your alarm company and insurer before making any such changes.

7.2 GSM / GPRS Service Provider

The SIM should have a full contractual basis, not “pay-as-you-go” or otherwise subject to service interruption.

Changes to the SIM contract or provider could result in breaks of service or other problems. The following warning should therefore be reproduced in the system design proposal and as-fitted document in bold type:

> **Important:** Your attention is drawn to the fact that changes to your SIM contract or service provider could affect the ability of the system to deliver its designed performance and thus invalidate your insurance cover. You should therefore consult your alarm company and insurer before making any such changes.

8. Maintenance

The I&HAS should be maintained in accordance with the requirements of Annex D of PD6662:2004, according to grade, in particular the requirement for all transmission paths to be checked. Responsibility for maintenance of the IT equipment through which alarm messages are transmitted or other transmission network components should rest contractually in accordance with clause 6.

A review of the ATS performance should be included as part of the system maintenance programme, as required by EN50136-1-1.

The signal level of a wireless connection should be checked at each service and compared to the level at installation.

9. Documentation and records

The System Design Proposal and As-Fitted Documentation should include the following information:

a) If applicable, a statement that transmission network components at the supervised premises used for alarm message transmission are the responsibility of the client. (see clause 4 and 5.8).

b) Details of the client's responsibilities in managing and maintaining any IT equipment that forms part of the ATS (see clauses 6 and 8).

c) Record of the service providers and contracts (see clause 7).

d) A warning that changes to service contract(s) or provider(s) could affect system performance (see clause 7).

Note: Where information is supplied by the client for incorporation into the system documentation, this should be noted.

Acknowledgements

The BSIA would like to thank the IP technical committee for its contribution to the production of this guide.

Bibliography

IPCRes Guidance Documents:

Alarm Signalling using the internet protocol: Part 1: An overview.

Alarm signalling using the internet protocol: Part 2: Considerations for insurers.

BSIA Guidance Documents:

A basic user guide to the use of Internet Protocol in the security industry (Form 211).

An installer guide to Internet Protocol in the security industry (Form 210).

Annex A (informative)

IPCRes Guidance

Appendix 1 of the IPCRes guidance document "Alarm signalling using the Internet Protocol: Part 2: Considerations for insurers" includes a model for IP-based alarm signalling systems, with two levels of installation. The appendix **IP Signalling Part 2** may be downloaded from: **www.infires.co.uk/downloads**

The model is summarised below:

Note: the IPCRes model uses the term "signalling equipment" to include the SPT and all transmission network components located at the supervised premises.

(i) SINGLE PATH SYSTEMS:

All "signalling equipment" at the supervised premises, is subject to the EN50131-1 requirements for PS back up, fault recognition and tamper security.

(ii) DUAL PATH SYSTEMS:

Level A:

All "signalling equipment" at the supervised premises, for all paths, is subject to the EN50131-1 requirements for PS back up, fault recognition and tamper security.

Level B:

All "signalling equipment" at the supervised premises, for one path, is subject to the EN50131-1 requirements for PS backup, fault recognition and tamper security.

"Signalling equipment" for the other path is located in an area where entry will immediately generate a full alarm activation whilst the I&HAS is set. This is clarified to mean that it should NOT be sited in an area configured as part of an "entry route," but is to be sited in an area where a confirmed alarm can be generated.

Note: Figure 1 of this guide (with transmission network components at the supervised premises not part of the ATE) is equivalent to a level B installation.