

S7
First published 2007
Version 02

Security

Security guidance for fog devices



➤ 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

1. Introduction	3
2. How security fog devices work	3
3. Applications	3
3.1 Intruder (forcible and violent entry to the premises)	3
3.2 Hold-up (personal attack at protected premises)	3
4. Emergency service considerations	4
5. Police response	4
6. Fire service response	4
7. Alerting neighbouring premises	4
8. False alarms	4
9. Recommendations	4
9.1 Installing company	4
9.2 The security fog system	4
9.3 Insurers	4
10. Related RISCAuthority documents	5

1. INTRODUCTION

These guidelines have been produced to assist specifiers and potential users in understanding certain factors that need to be considered before installing a security fog device.

A security fog device (sometimes also referred to as a 'smoke' security device) is an electronic security system which, on activation, produces dense 'fog' in order to disorientate a potential thief and deter/hinder further access into the protected area.

When a security fog device activates, the fog is produced rapidly with the intention that the protected area will be quickly filled (in a matter of seconds) to completely obscure an intruder's vision. Dispersion of the fog will occur either naturally over a period of time or more rapidly with venting via opened (or broken) doors and windows.

Security fog devices generally employ a glycol-based (or similar) liquid. Devices using a liquid with an irritant added are not recommended due to liability considerations.

BS EN 50131-8: **Alarm systems. Intrusion and hold-up systems. Security fog device/systems** provides manufacturers, suppliers, specifiers and installers of security fog devices with information on the minimum standards required for the adequate protection of property, safety of personnel and the prevention of damage to contents in premises protected by fog. The standard also includes provisions relating to equipment, system design, installation and maintenance.

2. HOW SECURITY FOG DEVICES WORK

In simple terms, the 'fog' is produced by passing the glycol (or other) fluid through a heating block, where it vaporises before being emitted into the area to be protected. The fluid may be pumped through the heating block or released from a pressurised container. As the vapour is released into the atmosphere it instantly condenses to form a dense white fog.

Activation of a security fog device is usually initiated by receipt of a suitable signal from a conventional intrusion and hold-up alarm system (I&HAS) to which it is connected, or by a stand-alone intruder sensor or hold-up ('personal attack') device(s) connected to the security fog device.

Following activation, a timer and/or sensor will normally be used to determine the volume of fog produced and the duration of operation. Some devices have an automatic density monitoring system which tops up the vapour should pre-determined obscuration levels fall, eg due to intruders endeavouring to ventilate the area or in the event of delayed site attendance by response personnel.

Although they have battery back up, security fog devices require mains power for full operation, failure of which will result in the heating block gradually cooling. Once the block cools below a certain level, a triggering input signal can still cause the device to activate, but it may no longer be able to produce adequate levels of fog, if any. In certain circumstances liquid may be ejected instead.

3. APPLICATIONS

3.1 Intruder (forcible and violent entry to the premises)

Security fog devices were originally designed primarily to combat out of hours 'break-in and grab' style theft, where more conventional security devices might fail to prevent or deter losses.

Nowadays they are also regarded as providing useful protection during the time interval between an intruder alarm activating following a break in, and the arrival at the premises of response personnel, for example, by police and/or keyholders.

Security fog devices are available in a variety of sizes and specifications, depending on the volume of the premises/area to be protected. They can be integrated into the intruder alarm system either individually or grouped together, again depending on the size of the premises/area to be protected.

It is possible to incorporate an audible voice message warning intruders to leave the premises before, or as, the device is activated.

Although, in their early days, some problems were encountered from damage to contents of premises from the occasional over-production of fog, improvements in the reliability and effectiveness of these systems have led to a general acceptance by many specifiers and insurers. By way of reassurance, most providers have effected public/products liability insurance cover against any claims for damage arising from such mis-operation.

3.2 Hold-up (personal attack at protected premises)

Protection is achieved by deploying a short, controlled activation to create a fog curtain between the attacker and the vulnerable staff with the intention of forcing the attackers to retreat from the premises. Usually the fog cloud is aimed directionally allowing the attackers a corridor by which to leave the premises, thus helping ensure the safety of the staff and limiting property damage. Adequate warning signs displayed at normal entry/exit points of the premises improve the initial deterrent value. It is possible to incorporate an audible voice message upon activation that re-assures members of the public/staff, eg that the product is harmless and/or assistance is on its way, etc.

However, advisors and specifiers such as consultants and insurers must carry out a very careful risk assessment before sanctioning or lending any degree of support for the technology in this application – an assessment that takes account, not only of the rationale and expectations for the system, but also the impact on legitimate occupiers of the premises – staff, visitors and customers.

It is suggested that satisfactory completion of a sufficiently thorough assessment would require collaboration with the manufacturer's representative and the installer of the triggering (ie hold-up alarm) system. Security fog products differ in their operation and it will be necessary to evaluate whether the operational requirement can be met by the way the equipment is expected to operate, including the required pattern of fog emission and the time that elapses before the fog in the intended area of operation reaches the required density.

It is widely recognised that where hold-up rather than premises intrusion is the hazard being addressed by a BS EN 50131-8 conforming system, the requirements for the minimum degree of reduction of visibility and the maximum time to achieve that level, are inadequate. Experience of actual system performance in the field clearly demonstrates that, in the hold-up application, significantly more rapid obscuration is essential.

Steps are being taken to revise the standard so that specific requirements are included for robbery prevention. Meanwhile specifiers are urged to thoroughly research the performance of equipment on a product-by-product and case-by-case basis if unacceptable results are to be avoided. Consideration should be given to witnessing a test firing before a commitment is made.

The advisor or specifier should also take steps to establish that the installer of the triggering system will integrate and connect both systems fully in accordance with the fog system manufacturer's instructions, will correctly commission the equipment and will ensure that the equipment is kept fully functional at all necessary times (eg is not left deactivated in error following routine I&HAS or security fog system maintenance).

➤ 4. EMERGENCY SERVICE CONSIDERATIONS

It is essential that the relevant police force and fire service be advised in writing of the proposed installation of a security fog system. Both organisations were represented during the discussions leading to the current standard BS EN 50131-8 and, as a result, both have developed guidelines for their personnel when attending premises where a security fog system may have activated.

➤ 5. POLICE RESPONSE

Police records for premises fitted with remote signalling I&HAS will indicate the presence of a security fog device, if installed. This allows prior warning to be given to those officers attending alarm activations at the protected premises.

Police policy is normally that officers should not enter the premises until the keyholder has arrived and disarmed the system, irrespective of evidence of either a genuine break-in or of intruders still on the premises. To avoid risk of injury, police officers will not normally enter the premises until the fog has dispersed, although officers are trained to be alert for anybody attempting to escape from the premises.

In recognition of cases where there is no remote alarm monitoring provided, and thus no advance warning given to police officers who may still be called to site, there should be external warning notices in place to indicate the presence of a security fog device.

➤ 6. FIRE SERVICE RESPONSE

The police control room may advise the fire service of the existence of 'fog' at a premises. This would normally be the result of a security fog device activating alongside an intruder alarm. As the fog produced is similar in appearance to smoke from a fire, the fire service may also be alerted to a possible fire by a member of the public. In such circumstances, it will be a matter for the fire service to judge whether to attend the premises or not.

There could potentially be a problem if the fire service arrives before the police or keyholder, as they may effect an entry to the premises if they suspect that a real fire may be in progress. However, as fire services maintain an extensive hazard database on which all security fog installations should be listed, any fire crew attending a reported fire in such premises should be aware in advance of the presence of a security fog system. Additionally, the fog or 'smoke' produced is similar to that used by fire services for training purposes and most fire officers will recognise it by its physical characteristics (smell and low temperature).

Where automatic fire detection systems exist at premises fitted with security fog devices, care should be taken not to activate them during any test firing of fog.

➤ 7. ALERTING NEIGHBOURING PREMISES

Where security fog devices are fitted, the owner/occupier should alert the occupiers of neighbouring premises, especially in multi-tenure properties. Neighbouring premises should also be warned before any test discharges are undertaken.

➤ 8. FALSE ALARMS

As security fog devices are detector-operated (whether by a stand-alone system or integrated with an I&HAS), they will operate irrespective of whether the source of the detection signal is genuine, accidental or otherwise 'false' (for example, caused by innocent environmental stimuli). To minimise this risk, systems are usually configured to require a second detector or hold-up device (or a 'confirmed' hold-up device) to activate before fog is produced.

➤ 9. RECOMMENDATIONS

9.1 Installing company

The installing company should:

- be fully trained and authorised by the manufacturers of the system;
- install in accordance with the manufacturer's specifications;
- comply with BS EN 50131-8;
- notify in writing the police, the fire service and any alarm receiving centre of a security fog system installation;
- give specific warning to the police and fire service prior to any testing of the system which will generate fog;
- provide annual service and maintenance; and
- provide appropriate training to keyholders in relation to the intruder alarm system and security fog device, in order to reduce the risk of operator-induced false activations.

9.2 The security fog system

The system should:

- preferably be linked to a remotely monitored intruder alarm system;
- be carefully designed not to interfere with any designated fire escape route or the operation of any automatic fire alarm system;
- be incapable of operation unless the appropriate part of the triggering I&HAS is set (note the hold-up part of I&HAS is usually permanently set);
- not be installed in an area designated as an entry/exit route of an intruder alarm system;
- not be installed in such a manner that it forms a 'man trap' or is likely to result in personal injury to intruders or innocent parties; and
- be provided with external warning notices/stickers to deter a break-in or hold-up and otherwise reduce the likelihood of any legal liability for possible injury to trespassers.

9.3 Insurers

Insurers should:

- ensure such systems are only installed by suitably trained and competent installers and in accordance with BS EN 50131-8;
- regard security fog devices as a supplement to, not a replacement for, conventional security measures against intruders, unless the construction, layout and nature of a premises precludes adequate physical security at economic cost;

- not regard a fog system as a substitute for the robust protection measures required where hold-up is the hazard being addressed – adequate surveillance, access controls, physical barriers and manning levels are still required;
- on the assumption that security fog devices will generally be used at higher risk premises, ensure that they are used in conjunction with a remotely monitored I&HAS and that the alarm transmission system (ATS) is of sufficiently quality, eg performs at or near ATS 5 ('grade' 4) to resist or quickly report criminal attack/failure;
- ensure the security fog device is wired and programmed to detect loss of mains power and immediately signals this to the alarm receiving centre (note, relevant standards, eg BS EN 50131, otherwise permit I&HAS to locally hold reports of mains power failure for up to 1 hour);
- despite the non-toxic nature of the fog, consider carefully the use of such systems in premises where contents may be particularly susceptible to contamination, eg the food preparation industry, pharmaceuticals etc;
- ensure adequate warning signs are posted at all likely entry points to the premises; and
- emphasise the necessity for an immediate keyholder response following reports of loss of mains power, faults and tamper signals in respect of both the security fog device(s) and a connected I&HAS.

➤ 10. RELATED RISCAUTHORITY DOCUMENTS

S2: **Alarm signalling using the Internet Protocol Part 1 – An overview.**

S5: **Alarm signalling using the Internet Protocol Part 2 – Considerations for insurers.**

S6: **Electronic security systems: guidance on keyholder selection and duties.**

S9: **Intrusion and hold-up alarm systems (I&HAS): considerations for installers and other stakeholders.**

S12: **Police response intruder alarm systems: ten-step guide for purchasers.**

S14: **Police response intruder alarm systems: summary of insurers' typical requirements.**

S17: **Intrusion and hold-up alarm systems: guidance on event processing and handling.**

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

2013 © The Fire Protection Association
on behalf of RISC Authority

