Requirements for using a voice assistant
as a non-I&HAS interface

bsia
british security industry association

Document change history

Date	Issue	Comment
03/08/2021	1.0	First Issue

Contents

Introduction

As technology evolves, we find new ways of interacting with our intruder alarm systems (IAS), this new technology is often not within the scope of our traditional standards regime, this leaves the security industry unable to take advantage of new technology. There are concerns with using new technology particularly when it is being used in a new way, as there are new risks to consider for both the installer and user, with possibly new processes to follow or even new best practice to develop.

This document has been produced by the BSIA to recognise the increased use of voice assistants being employed to interact with IAS and offers solutions based on risk as to how they can be deployed in the confidence that the customer (or user) has agreed to, and is aware of, the risk and their ongoing role in how the risk is being mitigated. As a result of our risk consideration, this document identifies grade dependent factors for the use of voice assistants and recognises that there are some circumstances where voice assistants should not be used.

The objective should always be to provide professional advice to the customer (or user) which is based on risk while taking into consideration the convenience benefits of using a voice assistant. The user should be provided with sufficient information required to make an informed decision regarding any proposed solutions.

1. General

For the purposes of this document a voice assistant is defined as a non-I&HAS interface including the capability for the user to control an IAS within the constraints of this document, examples - Amazon Alexa, Google Home, Apple Siri, Samsung Bixby, etc.

Note: Requirements for the use of non-I&HAS interfaces are given in BS EN 50131-3:2009, Annex C.

The use of voice assistants as a non-I&HAS interface to control an IAS should be limited to residential / domestic premises only and is not permitted to be used on grade 4 systems.

Note: The use of voice assistants to control an IAS have specific risks. It is important to ensure these risks are assessed and that the customer understands them and how to use the voice assistant in a secure manner.

For the purpose of this document, with regard to the interface to the voice assistant, the requirements of BS EN 50131-3:2009, Table C.1, 8.7.3 (monitoring of substitution) and 8.8 (security of communication) do not apply.

There should be a method of setting and unsetting of the IAS at the supervised premises using the CIE or ACE, e.g. a keypad.

Where it is claimed that the system conforms to BS 8243, the default method of setting and unsetting at the supervised premises should be as specified in BS 8243.

In all cases the use of a voice assistant for setting and/or unsetting should be considered as a supplementary method only.

For the purposes of this document a voice user is a user that issues a command to control an IAS via a voice assistant.

2. Abbreviations used in this document

CIE   Control and indicating equipment
IAS   Intruder alarm system
I&HAS   Intruder and hold-up alarm systems
PIN   Personal Identification Number

3. References used in this document

BS EN 50131-1:2006+A3:2020   Alarm systems. Intrusion and hold-up systems. System requirements
BS EN 50131-3:2009   Alarm systems. Intrusion and hold-up systems. Control and indicating equipment
BS 8243   Design, installation and configuration of intruder and hold-up alarm systems designed to generate confirmed alarm conditions. Code of practice

4. Authentication and authorisation

There are three defined levels of authorisation for voice assistants. Table 1 shows the permitted functionality at each grade for each level of authorisation:

- **Basic** - The IAS will only accept a command from an authorised voice assistant but cannot authenticate the voice user.
- **Enhanced** - The IAS will only accept a command from an authorised voice assistant when the voice user can be authenticated as an authorised user of the IAS.
- **Advanced** - The IAS will only accept a command from an authorised voice assistant when the voice user can be authenticated as an authorised user of the IAS using a minimum of two factor authentication.

Note: examples of user authentication:

- *Voice recognition technology*
- *'One time use' spoken PIN code, password or passphrase (i.e. code automatically changes on each use)*
- *Static spoken PIN code, password or passphrase (i.e. code remains constant until changed)*
- *Interactive notification (e.g. push notification that requires a non-spoken user response)*
- *Other biometrics (e.g. facial recognition, fingerprint)*

Table 1 – Minimum authorisation levels required by grade and function

Function	Grade 1	Grade 2	Grade 3	Grade 4
Set	B	B	E	NP
Unset	B	E	A	NP
Part set	B	B	E	NP
Non-I&HAS functions	B	B	E	NP
Event record retrieval	B	E	A	NP
Key B = Basic authorisation required E = Enhanced authorisation required A = Advanced authorisation required NP = The use of voice assistant is not permitted *Note: There is no requirement to provide all of the functions listed in this table.*				

Note 1: *For the purposes of this document account linking as a method of granting authorisation to a voice assistant is deemed to meet the requirements of basic authorisation. Account linking is a method of granting continuous authorisation to a voice assistant through the exchange of secure passwords and account details e.g. Amazon or Google. A voice assistant linked to an IAS in this manner will therefore be treated as a basic authorised voice assistant.*

Note 2: *For the purposes of this document, an account linked voice assistant is deemed to meet the requirements of BS EN 50131-1:2006+A3:2020, clause 8.3.2.*

5.   Use of voice assistant for setting of IAS

The use of voice assistants is grade dependent and provided that the minimum authorisation levels of Table 1 are satisfied then setting of the IAS via a voice assistant is permitted.

In all cases setting of the system is only permitted if the requirements of BS EN 50131-1:2006+A3:2020, 8.3.5 "Prevention of setting" are met (i.e. "Setting of an I&HAS or part thereof shall be prevented, unless overridden as permitted in 8.3.6, when one or more of the conditions shown in Table 4 is present.").

Initiation of setting should be by voice user command. Providing no conditions exist that would prevent setting of the IAS a timed setting procedure should begin. It should last for a minimum of 30 seconds and a maximum of 60 seconds. An audible indication should be provided throughout the supervised premises during the setting procedure so that any persons present are informed that the setting procedure has started.

Authorised IAS users at the premises should be able to cancel the setting procedure.
If, during the setting procedure, any intrusion detector is in an active condition the setting procedure should be cancelled. Optionally, according to CIE configuration, the setting procedure may instead automatically convert to the default method of setting, and the CIE should record this change in the event record.

If at the end of the setting procedure no conditions exist that prevent setting, the IAS should set.

Confirmation of whether the IAS has set, failed to set, or that an error has occurred should be provided to the voice user.

Silent, instant or timed exit is permissible on domestic/residential systems when the user is staying in the premises (e.g. at night).

6. Use of voice assistant for unsetting of IAS

The use of voice assistants is grade dependent and provided that the minimum authorisation levels of Table 1 are satisfied, then unsetting of the IAS via a voice assistant is permitted.

7. Use of voice assistant for non-I&HAS functions

The use of voice assistants is grade dependent and provided that the minimum authorisation levels of Table 1 are satisfied, then access to other functions not used for security purposes via a voice assistant is permitted e.g. lighting control.

8. Event record

The CIE should record in the event record all commands to and from the voice assistant. Event records related to the voice assistant should include identification of the IAS user or, if this is not possible, identification of the voice assistant.

9. Customer advice about voice assistants

If using a voice assistant to remotely set/unset IAS it is possible that users, by leaving a supervised premises unattended without its IAS set, might (inadvertently) be in breach of any interested insurer's policy wording, conditions or warranty.

The following warning, in bold type, should therefore be reproduced in the system design proposal and as-fitted document following the description of use of this facility.

"IMPORTANT If using a voice assistant to remotely set/unset your intruder alarm system, your attention is drawn to the fact that whenever a premises is unattended, but its intruder alarm system(s) is (are) not fully set, any related insurance cover might be made void. For advice on this matter, it is recommended that you consult your insurer(s)."

Additionally, if a static spoken PIN code, password or passphrase is used for authorisation then it may be possible for an unauthorised user to overhear it when used. The following warning, in bold type, should therefore be reproduced in the system design proposal and as-fitted document.

"IMPORTANT If using a voice assistant to control your intruder alarm system, and you use a spoken PIN code, password or passphrase, your attention is drawn to the fact that this may be overheard. If you suspect that an unauthorised user has overheard you, it is recommended that you change your spoken PIN code, password or passphrase immediately."

About the BSIA

The British Security Industry Association (BSIA) is the trade association representing over 70% of the UK's private security industry. Its membership includes companies specialising in all sectors of security. For security buyers, BSIA membership is an assurance of quality, with all member companies required to adhere to strict quality standards.

BSIA Ltd
Anbrian House
1 The Tything
Worcester
WR1 1HD

t: 01905 342 020
e: info@bsia.co.uk
www.bsia.co.uk

British Security Industry Association
Anbrian House (First Floor) | 1 The Tything | Worcester | WR1 1HD | 01905 342 020

ISO 9001: 2015 Certificate No. FS 14657

UK members of COESS and EURALARM • Registered office as above • Registered in England No. 487 9969 44 • The British Security Industry Association