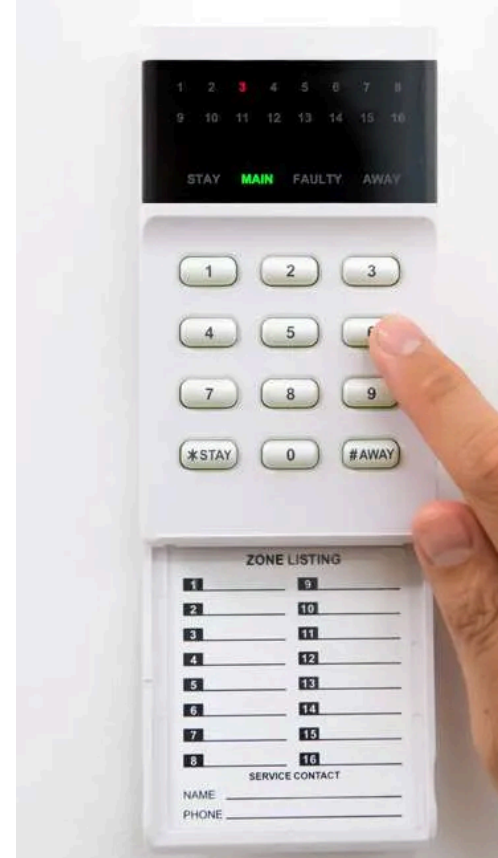




Security Equipment Manufacturer Scheme for Verification **To UK I&HAS Standards**

Contents

Introduction	3
Scheme Criteria	3
Application process	4
Step 1 – Pre-application equipment checks	4
Step 2 – Application.....	4
Step 3 – Testing conducted by the BSIA.....	4
Step 4 – Verification.....	4
Step 5 – Maintaining verification	5
Step 6 – Revising and updating the scheme.....	5
Recognition granted to verified CIE manufacturers.....	5
Annex A - UK specific testing for I&HAS (PD 6662 and BS 8243)	7

Introduction

The Security Equipment Manufacturer's UK Scheme has been developed to provide a clear, credible, and an independently administered verification process for demonstrating that Control and Indicating Equipment (CIE) meets the UK-specific requirements for systems requiring police attendance to Intruder and Hold-Up Alarm Systems (I&HAS).

At its core, the scheme provides a robust assurance mechanism, enabling manufacturers to demonstrate and evidence compliance with PD 6662:2017 and BS 8243:2021 through a structured, transparent, and recognised verification process conducted by the BSIA.

In an increasingly competitive and standards-driven market, customers, insurers, and police forces demand confidence that alarm signalling and control equipment performs reliably under UK operating conditions. This scheme directly supports that need by strengthening trust in products that have undergone independent verification, helping manufacturers reduce barriers to market access, and promoting consistent product performance across the industry.

Adoption of this scheme enables manufacturers to benefit from:

- Enhanced market differentiation through independently verified evidence of compliance
- Greater acceptance and recognition among police forces, inspectorates, insurers, and professional installers
- A structured three-year product verification model and clear testing requirements
- Direct alignment with NPCC policy direction

For stakeholders across the security ecosystem, the scheme provides a unified and authoritative benchmark that elevates product integrity, reduces risk, and supports continued confidence in UK-deployed alarm systems.

Scheme Criteria

For a CIE to be compliant with this scheme the requirements of PD 6662 and BS 8243 as prescribed in this scheme document shall have been verified through testing and assessment performed by the BSIA or its authorised representative.

For the purposes of this scheme, the following applies:

- A manufacturer is the organisation that takes responsibility for the design and manufacture of the security products.
- Where a manufacturer of CIE shares a common platform, (i.e., where the functionality is the same across different models of CIE) then testing of one model is sufficient to prove the compliance of the other CIE models.

Application process

Below is a step-by-step guide of how a security CIE manufacturer can obtain verification under this scheme:

Step 1 – Pre-application equipment checks

The manufacturer conducts self-assessment checks against the requirements in Annex A - *UK specific testing for I&HAS PD 6662 and BS 8243*.

Step 2 – Application

An application is submitted to the BSIA including a record of the manufacturers self-assessment against Annex A.

Where the manufacturers self-assessment indicates that the product meets the requirements, the BSIA shall contact the manufacturer to arrange a verification visit to conduct the test.

Step 3 – Testing conducted by the BSIA

The BSIA will attend a location provided by the manufacturer where the product is configured ready for testing.

The manufacturer will demonstrate to the BSIA as to how the product meets each test requirement set out in Annex A.

The BSIA will record the results of all tests and discuss any observations raised with the manufacturer as necessary.

If the results of the test indicate a noncompliance to Annex A, then a retest (in full or part) will be required.

Note 1: Costs agreed between the BSIA and the manufacturer include for the initial verification test only. Should a further verification be needed, then additional costs may be incurred.

Note 2: Where any disagreement exists regarding conformity with the tests in Annex A, the BSIA will refer the matter to its internal review panel. The panel will evaluate the information submitted and issue a validated outcome, specifying whether compliance has been confirmed, rejected, or cannot be determined without additional evidence. The decision of the BSIA review panel shall be final.

Step 4 – Verification

Where the tests are successfully completed the BSIA will issue a certificate of verification with this scheme.

Where the test results are unsuccessful no certificate will be issued and details of any noncompliance will be shared with the manufacturer.

Step 5 – Maintaining verification

To maintain the integrity of the scheme, certificates will be valid for a period of 3 yrs, after which time products will require re-verification.

In cases where the product functionality has changed that could impact compliance with this scheme, the manufacturer shall contact the BSIA for re-testing.

Note: Product functionality may change for a variety of reasons, including updates to relevant standards that alter the required compliance tests. Where such changes occur, retesting will be necessary to confirm continued conformity with this scheme.

Step 6 – Revising and updating the scheme

The BSIA shall periodically review and, where necessary, revise this scheme to ensure it remains aligned with applicable standards, regulatory requirements, and industry practices.

Where revisions are made, the BSIA will:

- Define any updated or additional verification requirements
- Communicate changes to participating manufacturers
- Specify any actions required to maintain valid verification status

Where changes to the scheme or relevant standards affect previously verified products, the BSIA may require partial or full re-verification to demonstrate continued conformity with the updated requirements.

Manufacturers shall ensure that products submitted under this scheme continue to meet the applicable requirements following any revision.

Continued recognition under the scheme, including the use of certificates and associated claims, is conditional upon maintaining valid verification status in accordance with the current version of this scheme.

Recognition granted to verified CIE manufacturers

Manufacturers whose CIE products have been successfully verified under this scheme will:

- be issued with a valid certificate of verification
- be permitted to display the scheme logo in connection with verified products in accordance with BSIA usage guidelines

be listed by the BSIA as a manufacturer with products holding verification status under this scheme

About the BSIA

The British Security Industry Association (BSIA) represents over 70% of the UK's private security market and comprises organisations operating across all areas of the security industry. As the recognised authority for professionalism and good practice, the BSIA requires all member companies to demonstrate compliance with rigorous quality, operational, and ethical standards. For end users and stakeholders, BSIA membership provides a trusted indicator of reliability, competence, and industry-leading performance.

British Security Industry
Association
t: 01905 342 020
e: info@bsia.co.uk
www.bsia.co.uk

Annex A - UK specific testing for I&HAS (PD 6662 and BS 8243)

Manufacturer name:
 CIE model number/part number:
 Date of inspection:
 Inspection conducted by:
 Location of where inspection conducted:

Step	Standard / clause ref.	Test condition	Action	Expected outcome	Pass / fail
PD 6662:2017 - PUBLISHED DOCUMENT Scheme for the application of European Standards for intrusion and hold-up alarm systems (manufacturer only)					
Test of Interconnections PD 6662:2017, A.4 (Amends the requirements of BS EN 50131-1:2006+A2:2017, clause 8.8 & table 19) <i>Note: BS EN 50131-1, table 19 allows fault signals or messages to be generated, these must be tamper signals or messages to comply with PD 6662 clause A.4. However, the times stated in BS EN 50131-1, table 16, remain the same.</i>					
1	A.4 Monitoring of interconnections (BS EN 50131-1, clause 8.8.3 & table 19) To demonstrate the ability of the CIE to comply with how PD 6662 A.4 amends BS EN 50131-1 clause 8.8.3 and table 19, with regards the monitoring of interconnections. <i>(The times specified in BS EN 50131-1, table 15 still apply)</i>	These tests consist of simulating the interconnection being disabled and monitoring the response.	Apply the test of EN 50131-3 clause 11.11 - The IAS shall be in the unset mode, with all inputs and outputs in normal condition. - Disable the interconnection, e.g. by short circuit. - If the system uses non-specific interconnections, simulate another application taking permanent control of the interconnection. - Record the response (and the time taken).	In all cases, the response shall generate a tamper signal or message. <i>(Within the times specified in BS EN 50131-1, table 15)</i> Recommendation, Test on Circuit/Zone on this test <i>(Table 15 for G2&3 is 100 seconds maximum)</i>	

Step	Standard / clause ref.	Test condition	Action	Expected outcome	Pass / fail
2	A.4 Periodic communication (BS EN 50131-1, clause 8.8.4.1 & table 19) To demonstrate the ability of the CIE to comply with how PD 6662 A.4 amends BS EN 50131-1 clause 8.8.4.1 and table 19, with regards periodic communication. <i>(The times specified in BS EN 50131-1, table 16 still apply)</i>	The manufacturer shall provide means to, either: a) Verify from system documentation that a tamper message or signal is generated. Or b) Identify a point at which periodic communication can be witnessed has taking place in order to test.	Apply the test of EN 50131-3 clause 11.11.2 The manufacturer shall provide documentation from which compliance with the requirements of PD 6662 clause A.4 regarding periodic communication can be verified Or - The IAS shall be in the set mode, with all inputs and outputs in normal condition. - apply a fault condition, i.e. a short circuit, to the interconnection, immediately following an identified periodic communication. - Record the response (and the time taken).	The manufacturer has provided enough information from which compliance with the requirements of PD 6662 clause A.4 regarding periodic communication can be verified. Or In all cases, the response shall generate a tamper signal or message, not a fault signal or message <i>(Within the appropriate grade times as specified in BS EN 50131-1, table 16, i.e. Grade 1 -240m, Grade 2 – 120m, Grade 3 – 100s or Grade 4 – 10s).</i> Recommendation – Test by disconnecting and shorting Bus.	
3	A.4 Security of communication (BS EN 50131-1, clause 8.8.5 & table 19) <u>This test is required for grade 4 systems only and is not required for grades 1, 2 and 3.</u>	The manufacturer shall provide means to verify that a tamper message or signal is generated.	Apply the assessment of EN 50131-3 clause 11.11.4 The manufacturer shall provide information from which compliance with the requirements of PD 6662 clause A.4 regarding security of communication can be verified.	The manufacturer has provided enough information from which compliance with the requirements of PD 6662 clause A.4 regarding security of communication can be verified. In all cases, the response shall generate a tamper signal or message. <i>(Within the times specified in BS EN 50131-1, table 16, plus 10s, i.e. Grade 4 – 20s).</i>	
A.5 Requirements (applicable to systems installed in compliance with BS 8243) for setting and/or unsetting using a remote device as a “Remote Non-I&HAS Interface”					
4	A.5.1 Use of remote devices for setting of IAS (Expands the requirements of BS EN 50131-3:2009, Table C.1, 8.7.3 monitoring of substitution, with regard to the remote non-I&HAS interface (remote device). <u>This test is required for grade 4 systems only and is not required for grades 1, 2 and 3.</u>	The manufacturer shall provide means to verify that the CIE is compliant with the requirements of PD 6662:2017, clause A.5.1. as regards the method of monitoring of substitution for the non-I&HAS interface used for remote setting.	Apply the test and assessment of EN 50131-3 clause 11.9 The manufacturer shall provide information from which it can be verified that the CIE is compliant with the requirements of PD 6662:2017, clause A.5.1. as regards the method of monitoring of substitution for the non-I&HAS interface used for remote setting.	The manufacturer has provided enough information from which it can be verified that the CIE is compliant with the requirements of PD 6662:2017, clause A.5.1. as regards the method of monitoring of substitution for the non-I&HAS interface used for remote setting. Substitution should be detected within 10s (Grade 4).	

Step	Standard / clause ref.	Test condition	Action	Expected outcome	Pass / fail
5	A.5.1 Use of remote devices for setting of IAS (Expands the requirements of BS EN 50131-3:2009, Table C.1, 8.8 security of communication , with regard to the remote non-I&HAS interface (remote device). <u>This test is required for grade 4 systems only and is not required for grades 1, 2 and 3.</u>	The manufacturer shall provide means to verify that a tamper message or signal is generated.	Apply the test and assessment of EN 50131-3 clause 11.11.4 The manufacturer shall provide information from which compliance with the requirements of PD 6662 clause A.5.1 regarding security of communication for the non-I&HAS interface used for remote setting can be verified.	The manufacturer has provided enough information from which compliance with the requirements of PD 6662 clause A.5.1 regarding security of communication for the non-I&HAS interface used for remote setting can be verified. For grade 4, the response shall generate a tamper signal or message. <i>(Within the times specified in BS EN 50131-1, table 16, plus 10s, i.e. Grade 4 – 20s)</i>	
A.5.1 Test of prevention of setting and overriding of prevention of setting procedure PD 6662:2017, A.5.1 (Expands the requirements of BS EN 50131-1:2006+A2:2017, clause 8.3.5 Prevention of setting and clause 8.3.6 Overriding prevention of setting , to cover setting using a remote device .					
6	A.5.1 Providing no conditions exist that prevent setting of the IAS a timed setting procedure should begin. See conditions listed below: Mandatory in grades 1, 2, 3 and 4 CIE • Intruder or hold up device in active condition (Intrusion detectors on an exit route may be excluded) • ATS and WD faults (Faults in all available ATS and WD's which prevent all notification) Mandatory in grades 2, 3 or 4, optional in grade 1 CIE • Intrusion detector fault • Tamper condition • Interconnection faults • Prime power source fault • Alternative power source fault • Alarm transmission system fault • Warning device fault Mandatory in grades 3 or 4, optional in grade 1 or 2 CIE • Detector masked.	This test will verify that setting shall be prevented should any of the conditions (grade dependant) be present from EN 50131-1 8.3.5 prevention of setting Table 4. See conditions listed to the left.	• The IAS shall be in the unset mode, with all inputs and outputs in normal condition. • Create each of the conditions listed to the left (one at a time), where it is mandatory (grade dependant) to prevent setting. • Attempt to initiate setting from a remote device.	In all cases setting shall not be possible.	

Step	Standard / clause ref.	Test condition	Action	Expected outcome	Pass / fail
7	A.5.1 Providing no conditions exist that prevent setting of the IAS a timed setting procedure should begin.	This test will verify that a time setting procedure begins if there are no conditions that would prevent settings/.	- The IAS shall be in the unset mode, with all inputs and outputs in normal condition. - Attempt to initiate setting from a remote device.	A timed setting procedure begins.	
8	A.5.1 If at the end of the timed setting procedure no conditions exist that prevent setting, the IAS should set.	This test is to verify that the IAS can be set by a remote device.	- The IAS shall be in the unset mode, with all inputs and outputs in normal condition. - Attempt to initiate setting from a remote device. - Allow the timed setting procedure to continue.	At the end of the timed setting procedure in test 7 above, the IAS will be set.	
9	A.5.1 Confirmation of whether the IAS has set, failed to set, or that an error has occurred should be provided to the user by the remote device based on information sent to it by the CIE.	This test is to verify that users receive indication or confirmation of setting from the CIE at the remote device.	- The IAS shall be in the unset mode, with all inputs and outputs in normal condition. - Attempt to initiate setting from a remote device. - Allow the timed setting procedure to continue until the IAS is in the set mode.	Following test 8 above, the user receives indication or confirmation of the IAS set, at the remote device.	
10	A.5.1 If, during the timed setting procedure, any intrusion detector is in an active condition the timed setting procedure should be either: a) cancelled. OR b) automatically convert to the configured method of completion of setting as per BS 8243. <i>(This option is not mandatory, however where this option is available in a CIE, the remote device should be informed that the setting procedure has changed and the CIE should record this change in the event record.)</i>	This is to verify that an active intruder detector will cancel the setting procedure (or revert to the configured BS 8243 method)	- The IAS shall be in the unset mode, with all inputs and outputs in normal condition. - Attempt to initiate setting from a remote device. - Once the timed setting procedure begins put an intruder alarm device into the active condition.	Setting procedure shall either be: a) cancelled and the IAS will not be set. OR b) automatically revert to the configured method of completion of setting as per BS 8243 and inform the remote device that the setting procedure has changed and the CIE should record this change in the event record. Observation: BS 8243 6.3.2 – “If this option is employed, the remote device user should be informed that the setting procedure has changed and the CIE should record this change in the event record.”	

Step	Standard / clause ref.	Test condition	Action	Expected outcome	Pass / fail
11	A.5.1 Confirmation of whether the IAS has set, failed to set, or that an error has occurred should be provided to the user by the remote device based on information sent to it by the CIE.	This test is to verify that users receive notification of failure to set from the CIE at the remote device.	- The IAS shall be in the unset mode, with all inputs and outputs in normal condition. - Attempt to initiate setting from a remote device. - Once the timed setting procedure begins put an intruder alarm device into the active condition. - Observe that the IAS does not set.	Following test 10 above, the user receives indication or confirmation of the IAS failure to set at the remote device.	
12	A.5.1 In respect of tests 9 and 10 the CIE should record in its event record the information that was sent to the remote device.	This test is to verify the CIE has a record of the information sent to remote device.	Inspect the IAS log to confirm a record of the test performed above.	CIE log confirms the correct information was sent to the remote device, e.g.: - Test 9 – the IAS has set. - Test 10 – the IAS has failed to set (e.g. - active detector) or there has been an error setting. Observation test 10 – PD 6662 & BS 8243 states setting should be cancelled!	
13	A.5.1 (Timed procedure) It should last for a minimum of 30 s and a maximum of 60 s.	This test will verify that the range of the timed setting procedure is between 30 - 60s	Check CIE programable parameters	The CIE provides the ability to configure the timed setting procedure to a value between 30 - 60s	
14	A.5.1 Authorized users at the premises should be able to cancel the setting procedure.	This test will verify that authorised user can cancel a remotely initiated setting procedure	- The IAS shall be in the unset mode, with all inputs and outputs in normal condition. - Attempt to initiate setting from a remote device. - Once the timed setting procedure is running at the CIE. - Attempt to cancel the setting using an authorised user credentials at the CIE. - Observe that the IAS does not set.	The setting procedure will be cancelled.	
15	A.5.2 Unsetting with remote device	This test is to verify that the IAS can be unset by a remote device.	- The IAS shall be in the set mode, with all inputs and outputs in normal condition. - Attempt to unset from a remote device. - Observe the IAS unset.	IAS will unset	

Step	Standard / clause ref.	Test condition	Action	Expected outcome	Pass / fail
16	A.5.3 Event record	This test is to verify that all instructions to initiate setting or unsetting that are received at the CIE are recorded in the event log and should include the identity of the user or the remote device.	Inspect the CIE log to confirm a record of the tests performed above.	CIE event log show record of remote setting and unsetting events, including identity of the user or the remote device used.	
C.2 BS EN 50131-1:2006+A2:2017, 8.3.9, Restore requirements					
17	C2 Restore requirements	If the CIE is configured as a BS 8243 installation, then the requirements of BS 8473 are enforced in relation to restoring.	- The IAS shall be in the set mode, with all inputs and outputs in normal condition. - Create a confirmed alarm condition (see tests 24 to 28). - Unset the IAS at the CIE. - Attempt to restore the IAS using at access level 2. - Observe that the IAS does not restore.	Level 2 user is prevented from restoring the IAS.	
Documentation requirements					
18	4.2 Components	The manufacturer should provide a statement that the product "is suitable for use in systems installed to conform to PD 6662:2017 at Grade N and environmental class Y".	Examine the documentation supplied with by the component to confirm the manufacturer has provided required statement	The manufacturer's statement shall have been provided within the supplied product documentation.	

BS 8243:2021 - Design, installation and configuration of intruder and hold-up alarm systems designed to generate confirmed alarm conditions - Code of practice (manufacturer only)

A.1 Where a hold-up or duress facility is provided by the CIE then the following tests should be followed.

19	A.1, a) HDs on CIE or ACE should be segregated from the main keys and dedicated, defined and contain two separate buttons.	This test is to verify that where a hold-up or duress facility is provided by the CIE or ACE, then HDs on CIE or ACE should be: - segregated from the main keys, - dedicated to the hold-up or duress facility, - defined appropriately, and	Visually inspect the CIE and/or ACE to confirm.	The hold-up or duress facility on the CIE and/or ACE is: 1) segregated from the main keys 2) dedicated to the hold-up or duress facility 3) defined appropriately 4) 2 separate buttons	
----	--	---	---	--	--

Step	Standard / clause ref.	Test condition	Action	Expected outcome	Pass / fail
		2 separate buttons.			
20	A.1, b) HDs on CIE or ACE may be engineer configurable as either single or synchronized dual button activation or off.	This test is to verify that where a hold-up or duress facility is provided by the CIE or ACE, the default configuration for HDs on CIE or ACE should only be programmable at access level 3 (Engineer).	- The IAS shall be in the unset mode, with all inputs and outputs in normal condition. - Using access level 3 authorisation change the configuration between single (optional) or synchronized dual button activation or off. - Also try this at other access levels.	At access level 3 the configuration of the hold-up or duress facility provided by the CIE or ACE may be configurable between single or synchronized dual button activation or off. Please note: There is not a requirement to offer both options. However, as a minimum you should have Dual, as this is specified as the default option, once it is enabled. Other access levels should not allow this.	
21	A.1, c) HDs on CIE or ACE are defaulted to off.	This test is to verify that where a hold-up or duress facility is provided by the CIE or ACE, then the default configuration for HDs on CIE or ACE should be off.	- The IAS shall be in the unset mode, with all inputs and outputs in normal condition, and using the default configuration. - Press the hold-up buttons on the CIE/ACE in the following sequence and record the response from the CIE/ACE following each step below: 1) Press button 1 only 2) press button 2 only 3) Press buttons 1 and 2 simultaneously	The correct default operation is that a HDs on CIE or ACE are defaulted to off, therefore the CIE should respond by ignoring all button presses.	
22	A.1, d) Where portable HDs (wireless devices) provide the hold-up facility for the CIE, this should be dedicated, should not incorporate any other functionality and should have two separate buttons with synchronized push to activate.	This test is to verify that where a hold-up or duress facility is provided by the CIE or ACE, via wireless devices, then HDs on the wireless device should be dedicated, should not incorporate any other functionality and should have two separate buttons with synchronized push to activate.	- Visually inspect the wireless device and manufacturer's instructions. - The IAS shall be in the unset mode, with all inputs and outputs in normal condition, and with the hold-up facility enabled. - Press the hold-up buttons on the wireless device in the following sequence and record the response from the CIE following each step below: 1) Press button 1 only 2) press button 2 only 3) Press buttons 1 and 2 simultaneously	The hold-up or duress facility on the wireless device: - is dedicated to the hold-up or duress facility. - does not incorporate any other functionality. - has 2 separate buttons that activate only when both buttons are pressed simultaneously.	

Step	Standard / clause ref.	Test condition	Action	Expected outcome	Pass / fail
23	A.1, e) Duress facility on CIE or ACE are defaulted to off and only configurable at access level 3.	This test is to verify that where a duress facility is provided by the CIE or ACE, then the duress facility is defaulted to off and only configurable at access level 3 (Engineer).	Check CIE default configuration. - The IAS shall be in the unset mode, with all inputs and outputs in normal condition, and using the default configuration. - Attempt to activate a duress signal, this should be executed by following the manufacturer's instructions. - Try enabling/disabling duress using other access levels (other than access level 3). - Enable the duress facility using access level 3. - Attempt to activate a duress signal, this should be executed by following the manufacturer's instructions.	The duress facility should be disabled by default and can only be enabled at access level 3.	
A.2.1 The CIE should recognize the following combinations of the alarm types as a sequentially confirmed intruder alarm.					
24	A.2.1, a) Two independent detector activations occur when the IAS is set.	This test is to verify that the CIE processes a confirmed alarm when the events listed in A.2.1 are presented to the CIE.	- With a CIE configured for sequential intruder alarm confirmation. - Set the IAS with all inputs and outputs in normal condition. - Activate two independent detectors. <i>Note: The first detector activation must not be the final exit or entry door as this will start the entry timer.</i>	CIE processes a confirmed alarm.	
25	A.2.1, b) Two independent detector activations (off the entry route) occur when the entry timer is running.	This test is to verify that the CIE processes a confirmed alarm when the events listed in A.2.1 are presented to the CIE.	- With a CIE configured for sequential intruder alarm confirmation. - Set the IAS with all inputs and outputs in normal condition. - Activate the entry timer, e.g. final exit or entry.	CIE processes a confirmed alarm. (refer to BS 8243 A.3.4 & Annex G – G1)	

Step	Standard / clause ref.	Test condition	Action	Expected outcome	Pass / fail
			• Activate two independent detectors (not on the entry route) while the entry timer is running. • Allow the entry timer and the remote notification delay timers to expire		
26	A.2.1, c) A single detector activation combined with a tamper alarm from a separately identifiable detector.	This test is to verify that the CIE processes a confirmed alarm when the events listed in A.2.1 are presented to the CIE.	• With a CIE configured for sequential intruder alarm confirmation. • Set the IAS with all inputs and outputs in normal condition. • Activate a single detector (not on the entry route). • Generate a tamper alarm on a separate detector.	CIE processes a confirmed alarm.	
27	A.2.1, d) A single detector activation off the entry route combined with the expiry of entry time or the remote notification delay (the timer that expires last).	This test is to verify that the CIE processes a confirmed alarm when the events listed in A.2.1 are presented to the CIE.	• With a CIE configured for sequential intruder alarm confirmation. • Set the IAS with all inputs and outputs in normal condition. • Activate a single detector (not on the entry route). • Activate the entry timer, e.g. final exit or entry, entry timer starts. • Allow the entry timer and the remote notification delay timers to expire.	CIE processes a confirmed alarm following expiration of the timers.	
28	A.2.1, e) Failure of communication to multiple devices on a data bus system that cannot be identified as a fault when the IAS is set.	This test is to verify that the CIE processes a confirmed alarm when the events listed in A.2.1 are presented to the CIE.	• With a CIE configured for sequential intruder alarm confirmation. • Set the IAS with all inputs and outputs in normal condition. • Create a condition where there is a failure of communication to multiple devices on the system, e.g. disconnect a data bus.	CIE processes a confirmed alarm or identifies the failure of communication as a fault.	

A.2.2 Hold-up alarm systems (HAS) - The CIE should recognize the following combinations of the alarm types as a sequentially confirmed hold-up alarm.

Note on multi-action HDs: Where multi-action HDs are utilised then BSI's GW1/2 Clarification of multi-action HD, from January 2023, should be taken into account. Compliant multi-action HDs should be used when testing

Step	Standard / clause ref.	Test condition	Action	Expected outcome	Pass / fail
<i>the multi-action function, the manufacturer's instructions should describe how on how to activate them.</i>					
29	A.2.2, a) two HD activations from separately identifiable HDs or two HD activations from a multi-action HD.	This test is to verify that the CIE processes a confirmed hold up alarm when the events listed in A.2.2 are presented to the CIE.	- With a CIE configured for sequential HUA confirmation, with the system unset and all inputs and outputs in normal condition. - Generate 2 signals or messages from 2 separately identifiable HD. OR - Generate a confirmed alarm from 1 multi-action HD.	CIE processes a confirmed HUA.	
30	A.2.2, b) single HD activation combined with a tamper alarm from a separately identifiable HD.	This test is to verify that the CIE processes a confirmed hold up alarm when the events listed in A.2.2 are presented to the CIE.	- With a CIE configured for sequential HUA confirmation, with the system unset and all inputs and outputs in normal condition. - generate 1 HUA signal or message from an HD. - then generate a tamper message from a separately identifiable HD.	CIE processes a confirmed HUA.	
31	A.3.1 The CIE should provide means to implement at least one of the methods of setting described in 6.3.	Verify that the CIE can support one of the methods listed in 6.3.	Check that the manufacturers documentation states that at least one of the methods listed in 6.3 is supported by the CIE.	The CIE supports at least one of the methods for setting listed in 6.3.	
32	A.3.1 Where the method of confirmation is sequential, at least one of the methods of unsetting described in 6.4.	Verify that the CIE can support one of the methods listed in 6.4. where the confirmation is sequential.	Check that the manufacturers documentation states that where the method of confirmation is sequential, at least one of the methods of unsetting described in 6.4. is supported by the CIE.	The CIE supports at least one of the methods for unsetting listed in 6.4.	
33	A.3.1 The CIE should provide a short delay feature (settle timer) so that the bouncing of a protective switch (i.e. door contact) upon closure of the door does not give rise to a false alarm.	Verify that the CIE has a short delay feature (settle timer).	Check that the manufacturers documentation states that the CIE includes a short delay feature.	The CIE supports a short delay feature.	
A.3 Methods of setting and unsetting					
34	A.3.3 Entry timeout with no alarm condition	To verify that the CIE generates an unconfirmed alarm when the entry timer expires (with no other alarms present).	With a CIE configured for sequential intruder alarm confirmation.	An unconfirmed alarm is generated at the expiry of the entry time.	

Step	Standard / clause ref.	Test condition	Action	Expected outcome	Pass / fail
			- Set the IAS with all inputs and outputs in normal condition. - Activate the entry detector to start the entry time. - Let the entry time expire and observe the CIE outputs.		
35	A.3.4 Entry timeout before expiry of minimum 30 s operation of indicator or WD	To verify that the entry timeout before expiry of minimum 30 s operation of indicator or WD.	- With a CIE configured for sequential intruder alarm confirmation and an entry time shorter than the remote notification delay. - Set the IAS with all inputs and outputs in normal condition. - Activate the entry detector to start the entry time. - Activate a detector (not on the entry route).	Upon activation of the detector (not on the entry route) an indication or warning device will be activated, but no remote signalling shall occur. When both the entry timer and remote notification delay timers have expired, an unconfirmed and confirmed alarm condition will be notified remotely. Refer to G.1 timing diagram in BS 8243	
36	A.3.5 Entry timeout after expiry of minimum 30 s operation of indicator or WD	To verify that the entry timeout after expiry of minimum 30 s operation of indicator or WD	- With a CIE configured for sequential intruder alarm confirmation and an entry time longer than the remote notification delay. - Set the IAS with all inputs and outputs in normal condition. - Activate the entry detector to start the entry time. - Activate a detector (not on the entry route).	Upon activation of the detector (not on the entry route) an indication or warning device will be activated, but no remote signalling shall occur. When both the entry timer and remote notification delay timers have expired, an unconfirmed and confirmed alarm condition will be notified remotely. Refer to G.2 timing diagram in BS 8243	
37	A.3.6 Entry timeout before expiry of minimum 30 s operation of indicator or WD (second detector before end of 30 s delay)	To verify that the entry timeout before expiry of minimum 30 s operation of indicator or WD (second detector before end of 30 s delay)	- With a CIE configured for sequential intruder alarm confirmation and an entry time shorter than the remote notification delay. - Set the IAS with all inputs and outputs in normal condition. - Activate the entry detector to start the entry time. - Activate a detector (not on the entry route).	Upon activation of the 1st detector (not on the entry route) an indication or warning device will be activated, but no remote signalling shall occur. Upon activation of the 2nd detector (not on the entry route) an unconfirmed and confirmed alarm condition will be notified remotely. Refer to G.3 timing diagram in BS 8243	

Step	Standard / clause ref.	Test condition	Action	Expected outcome	Pass / fail
			• Activate a second detector (not on the entry route).		
38	A.3.7 Intruder alarm before entry and detector off the entry route during entry	To verify that a confirmed alarm is generated when a detector before entry and detector of the entry route during entry	• With a CIE configured for sequential intruder alarm confirmation. • Set the IAS with all inputs and outputs in normal condition. • Activate a detector (not on the entry route). • Activate the entry detector to start the entry time. • Activate a second detector (not on the entry route) within the confirmation time.	Upon activation of the 1st detector an indication or warning device will be activated, and an unconfirmed alarm shall be remotely notified. Upon activation of the entry detector the entry timer begins. Upon activation of the 2nd detector (not on the entry route), no additional actions occur. Upon expire of the entry timer a confirmed alarm shall be remotely notified. Refer to G.4 timing diagram in BS 8243	
A.4 Confirmation time					
39	A.4 Confirmation time facility - IAS.	Verify that the CIE has a confirmation timer which is configurable from 30 mins to 60 mins.	Check that the manufacturers documentation states that the confirmation timer is configurable from 30 mins to 60 mins.	The CIE provides the ability to configure the confirmation timer to a value between 30 and 60 mins.	
40	A.4 Confirmation time facility - HAS.	Verify that the CIE has a confirmation timer which is configurable from 8 hours to 20 hours.	Check that the manufacturers documentation states that the confirmation timer is configurable from 8 hours to 20 hours.	The CIE has configurable confirmation timer of between 8 and 20 hours.	
41	A.4 Confirmation time operation - IAS.	Verify that a confirmed alarm cannot be generated after expiry of the confirmation timer	• With a CIE configured for sequential intruder alarm confirmation. • Set the IAS with all inputs and outputs in normal condition. • Activate a detector (not on the entry route). • Wait for the confirmation timer to expire.	Upon activation of the 1st detector an unconfirmed alarm shall be remotely notified. Upon activation of the 2nd detector, no additional actions occur. A confirmed intruder alarm is NOT processed.	

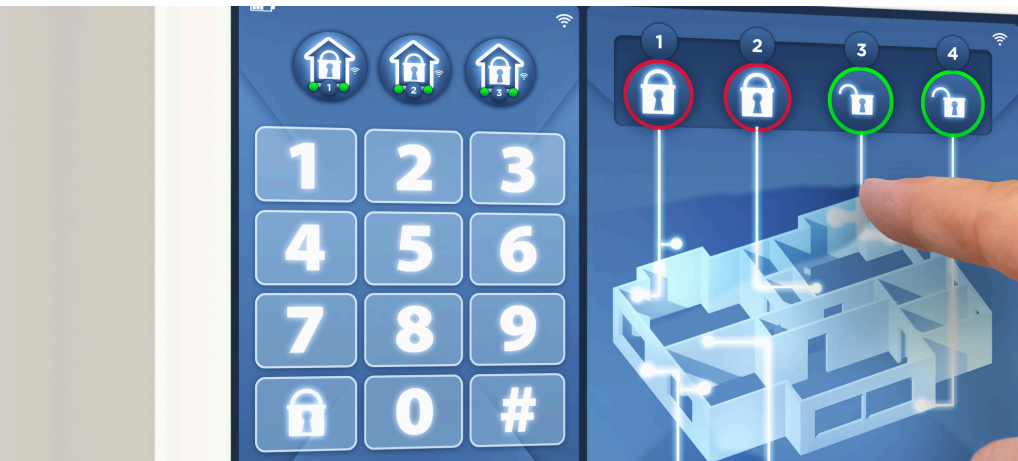
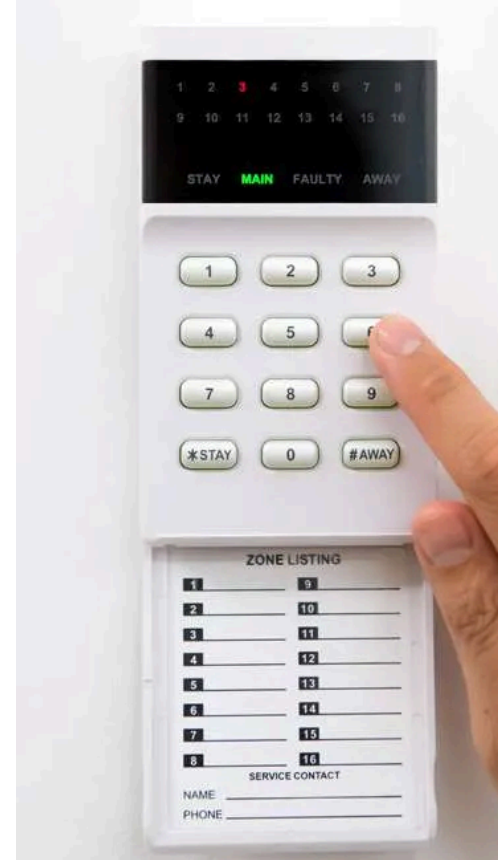
Step	Standard / clause ref.	Test condition	Action	Expected outcome	Pass / fail
			• Activate a second detector (not on the entry route).		
42	A.4 Confirmation time operation - HAS.	Verify that a confirmed HUA cannot be generated after expiry of the confirmation timer	• With a CIE configured for sequential HUA confirmation, with the IAS unset and all inputs and outputs in normal condition. • Activate one HD to generate an unconfirmed HUA signal or message. • Wait for the confirmation timer to expire. • Activate a second HD.	Upon activation of the 1st HD an unconfirmed hold-up alarm shall be remotely notified. Upon activation of the 2nd HD, no additional actions occur. A confirmed hold-up alarm is NOT processed.	
A.5 Reinstatement					
43	A.5.1 Reinstatement, General (IAS)	To verify that reinstatement occurs at the end of the confirmation timer and that the CIE is prepared for further alarm events.	• With a CIE configured for sequential intruder alarm confirmation. • Set the IAS with all inputs and outputs in normal condition. • Activate a detector (not on the entry route) and ensure that detector returns to the normal condition. • Wait for the confirmation timer to expire. • Activate the same detector.	At the end of the confirmation timer, any active warning devices shall cease. Upon the 2nd activation of the same detector an unconfirmed alarm is generated and the confirmation timer starts again.	
44	A.5.2 Sequentially confirmed IAS reinstatement	To verify that reinstatement occurs at the end of the confirmation timer and that any active detectors are inhibited.	• With a CIE configured for sequential intruder alarm confirmation. • Set the IAS with all inputs and outputs in normal condition. • Activate a detector (not on the entry route) and ensure that detector remains activated. • Wait for the confirmation timer to expire. • Restore that detector.	At the end of the confirmation timer, the CIE shall inhibit the active detector and notify this. Any active warning devices shall cease. Upon the 2nd activation of the same detector there will be no alarm generated.	

Step	Standard / clause ref.	Test condition	Action	Expected outcome	Pass / fail
			• Activate the same detector.		
45	A.5.1 Reinstatement, A.5.1 General (HAS)	To verify that reinstatement occurs at the end of the confirmation timer and that the CIE is prepared for further alarm events.	• With a CIE configured for sequential HUA confirmation, with the IAS unset and all inputs and outputs in normal condition. • Activate one HD to generate an unconfirmed HUA signal or message and ensure that HD returns to the normal condition. • Wait for the confirmation timer to expire. • Activate a that same HD.	At the end of the confirmation timer, any active warning devices shall cease. Upon the 2nd activation of the same HD a new unconfirmed alarm is generated and the confirmation timer starts again.	
46	A.5.3 Sequentially confirmed HAS reinstatement	To verify that reinstatement occurs at the end of the confirmation timer and that any active HDs are inhibited.	• With a CIE configured for sequential HUA confirmation, with the IAS unset and all inputs and outputs in normal condition. • Activate a HD and ensure that the HD remains activated. • Wait for the confirmation timer to expire. • Restore that HD. • Activate a that same HD.	At the end of the confirmation timer, the CIE shall inhibit the active HD and notify this. Any active warning devices shall cease. Upon the 2nd activation of the same HD there will be no alarm generated.	
A.5 Reinstatement					
47	A.6 restore	To verify that the CIE restricts the restoring of an IAS confirmed alarm activation to access level 3.	• With a CIE configured for sequential intruder alarm confirmation. • Set the IAS with all inputs and outputs in normal condition. • Create a confirmed alarm condition (see tests 24 to 28).	It is <u>not</u> possible to restore the CIE with level 2 credentials. The CIE restores with level 3 credentials.	

Step	Standard / clause ref.	Test condition	Action	Expected outcome	Pass / fail
			- Unset the IAS - Attempt to restore the CIE using a valid level 2 user credentials. - Attempt to restore the CIE using a valid level 3 user credentials.		
a.7.2 additional signals or messages					
48	a) mis-operation (sometimes referred to as an abort signal)	To verify the CIE can generate the additional signals or messages required in A.7.2.	Create a mis-operation (abort) condition on the CIE. (Refer to the manufacturer's instructions on how this condition is created).	CIE generates a mis-operation signal or message.	
49	b) Confirmed alarm		Create a confirmed alarm condition (see tests 24 to 28).	CIE generates a confirmed alarm signal or message.	
50	c) Reinstatement		Create a reinstatement condition on the CIE. (see test 43)	CIE generates a reinstatement signal or message or removes the active signal.	
51	d) detector inhibited		Create a detector inhibited condition on the CIE. (see test 44)	CIE generates a detector inhibited signal or message.	
52	d) HD inhibited		Create a HD inhibited condition on the CIE. (see test 46)	CIE generates a HD inhibited signal or message.	
53	If the unconfirmed alarm is generated by a tamper condition, a tamper signal only should be notified.	To verify that the CIE only generates a tamper signal or message if the cause of an unconfirmed alarm is a tamper event.	- With a CIE configured for sequential intruder alarm confirmation. - Set the IAS with all inputs and outputs in normal condition. - Create a tamper alarm.	CIE generates a tamper signal or message only.	
54	A.7.3 notification of confirmed alarm	To verify that the CIE uses the prescribed codes for SIA and Contact ID according to A.7.3.	Check that the manufacturers documentation states what codes are used by the CIE.	The CIE uses the SIA and/or Contact ID codes as prescribed in A.7.3.	
A.8 Indications					

Step	Standard / clause ref.	Test condition	Action	Expected outcome	Pass / fail
55	a) Confirmed alarm	To verify the CIE can indicate the conditions listed in A.8.	• Create a confirmed alarm condition (see tests 24 to 28). • Unset the IAS.	CIE indicates a confirmed alarm.	
56	b) Reinstatement		• Create a reinstatement condition on the CIE. (see test 43) • Unset the IAS.	CIE indicates a reinstatement.	
57	c) Detector inhibited		• Create a detector inhibited condition on the CIE. (see test 44) • Unset the IAS.	CIE indicates a detector inhibited.	
58	c) HD inhibited		• Create a HD inhibited condition on the CIE. (see test 46). • Unset the IAS.	CIE indicates a HD inhibited.	
A.9 Event Recording					
59	a) Confirmed alarm	To verify the CIE can record the events listed in A.9 in the event log.	• Create a confirmed alarm condition (see tests 24 to 28). • Unset the IAS. • Check event log.	CIE records a confirmed alarm.	
60	b) Reinstatement		• Create a reinstatement condition on the CIE. (see test 43) • Unset the IAS. • Check event log.	CIE records a reinstatement.	
61	c) Detector inhibited		• Create a detector inhibited condition on the CIE. (see test 44) • Unset the IAS. • Check event log.	CIE records a detector inhibited.	
62	c) HD inhibited		• Create a HD inhibited condition on the CIE. (see test 46). • Unset the IAS. • Check event log.	CIE records a HD inhibited.	

Step	Standard / clause ref.	Test condition	Action	Expected outcome	Pass / fail
63	d) instructions received from a remote device, including identification of the user or, if this is not possible, the remote device.		Issue an instruction to the CIE from a remote device. (e.g. see tests 6 to 16).	CIE records instruction received from the remote device, including identification of the user, or identification of the remote device.	
A.10 Interface to audio confirmation equipment					
64	A.10 Interface to audio confirmation equipment	To verify that the CIE interface meets the requirements of A.10.	Inspect manufacturers documentation.	The CIE interface meets the requirements of A.10.	
A.11 Interface to visual confirmation equipment					
65	A.11 Interface to visual confirmation equipment	To verify that the CIE interface meets the requirements of A.11.	Inspect manufacturers documentation.	The CIE interface meets the requirements of A.11.	
A.12 Documentation					
66	A.12 Documentation	To verify that the manufacturers documentation meets the requirements of A.12.	Inspect manufacturers documentation.	The manufacturers documentation meets the requirements of A.12.	



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.