

Commissioning and preventative maintenance of intruder alarm systems installed to PD6662:2004 -- Code of practice

Incorporates specifications for the remote support
of intruder alarm systems

March 2005

BSIA Form No 177

Contents

	Page	
1	Introduction	3
2	Scope	3
3	Normative References	3
4	Definitions and Abbreviations	4
5	Security	5
6	Inspection, Functional Testing and Commissioning	6
	Table 1: Commissioning Requirements	6
7	Preventative Maintenance	10
8	Remote System Checks	10
	Table 2: Preventative Maintenance Requirements	11
9	Remote Support of Intruder Alarm systems	14
	Table 3: Remote Initiation of Commands.	16
	Annex A: Verification of health of Alternative Power Source	17

1. INTRODUCTION

Commissioning of any intruder alarm system is vital to ensure the system is fully functional. At the commissioning stage, the status of all parts of the system should be recorded to be used as the basis against which any future maintenance is measured.

Preventative maintenance of an intruder alarm system is required to ensure that the system's integrity is maintained and that it is fully functional. Such maintenance prevents minor problems becoming major problems, enables alarm company personnel to correct physical, electrical and electronic faults and allows software updates to take place.

Remote support of intruder alarm systems permits a range of tasks to be carried out from simple exchange of system event logs or other parameters through to full maintenance checks – under manual or automatic control – using the self-diagnostic capabilities of the system. Hence an analysis of the system to a level similar to that by alarm company personnel on site may be possible remotely. Remote system checks can therefore be used to check the electronic integrity of a system, but not the physical condition of the system. A combined approach of both physical visits to the site and remote system checks offers greater confidence to the client.

2. SCOPE

The requirements of this document apply to all intruder alarm systems installed to PD6662:2004. They are intended to ensure that a common policy is used for all systems. They cover commissioning, on site maintenance, remote system checks and remote support

3. NORMATIVE REFERENCES

The following normative documents contain provisions which, through reference in this text, constitute provisions of this part of this document. For undated references, the latest edition of the publication referred to applies.

PD6662:2004	Scheme for the application of European Standards for intruder and hold-up alarm systems
prEN 50131-1:2004	Alarm systems – Intrusion systems – Part 1: General requirements
DD CLC/TS 50131-7:2003	Alarm systems – Intrusion systems – Part 7: Application guidelines
DD 245 (current issue)	Management of False Alarms

4. DEFINITIONS AND ABBREVIATIONS

4.1 Definitions and Abbreviations

For the purposes of this document, the definitions listed in PD6662:2004, prEN 50131-1:2004 and DD CLC/TS EN 50131-7 apply, together with the following. For clarity certain definitions from those standards have been included:

4.1.1 alarm company personnel

Personnel from a company responsible for commissioning, repairing and/or maintaining an alarm system.

4.1.2 alternative power source

A power source (e.g. a battery) capable of powering the system for a predetermined time when the external power source is unavailable.

4.1.3 audit trail

A record of remote dialogues, changes made, etc.

4.1.4 authentication

Verification, by the exchange of a code or codes, of the correct identity of the host computer and the I&HAS.

4.1.5 authority

The person giving the instruction to initiate a remote dialogue.

NOTE: This procedure may be automated.

4.1.6 client

Individual or corporate body responsible for acquiring the I&HAS.

4.1.7 data encryption

Coding, translation or other modification of information whereby the manner in which it is modified varies with time in a pseudo-random manner.

4.1.8 downloading

Generic term (along with uploading) to describe the action of transferring data between host computer and I&HAS.

NOTE: Because of the established non-standardisation of the meaning of this term, its use is avoided in this document.

4.1.9 external power source

The power source used to support the intruder alarm system or part thereof under normal operating conditions.

4.1.10 frequently used detectors

Those detectors which are expected to operate during normal use of the premises.

4.1.11 on-line restore

Restore of an I&HAS performed remotely, after confirming system integrity by the use of diagnostic facility. Use is subject to the conditions described in DD245.

NOTE: "on-line restore" is preferred over "remote restore" to avoid confusion with other established usages of that term.

4.1.12 operator

Personnel at remote location operating the computer controlling a remote dialogue.

Note: This operation may be automated.

4.1.13 parallel connected ATE

ATE using parallel communication from host CIE – ie an individual connection per output channel.

4.1.14 peripheral equipment

Equipment other than the CIE, ACE and WD used for supplementary purposes (e.g. output devices).

4.1.15 remote location

Site other than the supervised premises from which it is possible to process remote dialogues.

NOTE: This definition differs from that in PD6662:2004, recognizing that certain remote communications may be controlled by the user / client. This is confined to functions permitted for level 2 users on site, as itemized in Table 3.

4.1.16 remote support

The ability to exchange data between an I&HAS at supervised premises and a computer at a remote location.

4.1.17 ringback

Additional security procedure where the remote location initiates a dialogue via a communications medium and the I&HAS acknowledges after authentication by clearing the initial connection and itself establishing dialogue with the authorised host before permitting data (other than authentication data) to be exchanged.

4.1.18 serial connected ATE

ATE using serial communication from host CIE – ie information for multiple signals conveyed by the same serial link.

4.1.19 site visit

Preventative maintenance visit carried out on site.

4.1.20 soak

Attribute of an alarm circuit/point preventing signals or messages that normally create notifications from doing so, but continuing to record in the event log.

4.1.21 system configuration

The site specific data which is required for correct operation of the I&HAS.

4.1.22 user

Person authorised to operate an I&HAS (with access level 2).

4.2 Abbreviations

For the purposes of this document, the following abbreviations apply:

ARC	-	Alarm Receiving Centre
ACE	-	Ancillary Control Equipment
ATE	-	Alarm Transmission Equipment
ATS	-	Alarm Transmission System
CIE	-	Control and Indicating Equipment
IAS	-	Intruder Alarm System
I&HAS	-	Intruder and Hold Up Alarm System
WD	-	Warning Device

5. SECURITY

5.1 General

prEN 50131 –1:2004 details 4 security grades of intruder alarm system, each of which has different requirements for functions and access. The maintenance of an

I&HAS will need to take into account these grades and associated functional requirements.

5.2 Security Measures

The prEN 50131-1:2004 requirement that a user must give permission before any access to the CIE is obtained is applicable to both site and remote operations. Specific approval is required if remote access is to be used whilst the system is set, or if the operation of the I&HAS will be adversely affected during the operation.

A remote dialogue must not delay the initialisation of the transmission sequence of an alarm signal for more than 10 seconds.

Additional security measures required when remote support is used, including a secure authentication process for initialising remote communication to a commissioned system, are described in section 9.

A user must agree any change to the site specific data that is implemented remotely, at the time of the change. All such changes to the system must be recorded and sent to the client/user, if prior written authorisation has not been obtained.

The security of the premises supervised by the I&HAS is paramount whilst carrying out maintenance and the system should be left fully functional or any irregularities reported to a user and actioned as soon as possible.

6. INSPECTION, FUNCTIONAL TESTING AND COMMISSIONING

The inspection, functional testing and commissioning of any system should be carried out in accordance with DD CLC/TS EN 50131-7 clause 10.

Commissioning can only be completed when the I&HAS has been installed to the Installation plan, including any agreed changes and has been fully functionally tested.

Commissioning of the system should fulfil the requirements shown at Table 1.

Table 1 **COMMISSIONING REQUIREMENTS**

Note: Not all checks will be applicable to every installed I&HAS or every part of an installed I&HAS. In such cases, NA (Not Applicable) should be inserted into the brackets; otherwise a tick [✓] should be inserted to indicate that the check is complete.

COMMISSIONING REQUIREMENTS		Notes
1. GENERAL		
a. Check that installed system meets the Installation plan and any agreed changes	[]	
b. Client/user documentation is complete and left on site.	[]	
2. CONTROL AND INDICATING EQUIPMENT		
a. Check that system programming is correct and agrees with the Installation plan and any agreed changes	[]	
b. Ensure date and time is correct.	[]	
c. Measure and record input voltage from power supply (if power supply is not integral with CIE)	[]	

COMMISSIONING REQUIREMENTS		Notes
d. Check the current drawn from each output is within manufacturers ratings.	[]	
e. Check that all control points are fully operational.	[]	
f. Check that all system timers function correctly.	[]	
g. Check system setting procedure functions correctly.	[]	
h. Check "set" indicates correctly.	[]	
i. Activate each type of alarm and check system response.	[]	G
j. Check entry route functions correctly.	[]	
k. Check system unsets correctly (including indication)	[]	
l. Check all annunciation equipment is functioning correctly.	[]	
m. Check operation of tamper switch(es).	[]	
n. Record details of alarm circuits/ points used/isolated	[]	
o. Record details of any alarm circuits/ points on soak test.	[]	
p. Check duress facility is operational.	[]	G
q. Check hold-up alarm facility is operational	[]	
r. For testing of alternative power supply see 3. e, f & g (POWER SUPPLIES).	-	
s. If a memory support battery is used, check that installation date is recorded on the device and in the system record.		
3. POWER SUPPLIES		
a. Ensure that installation checks specified in Electrical Wiring Regulations (BS 7671) for power connections have been carried out.	[]	
b. Measure and record output voltage and ensure within specifications.	[]	
c. Measure and record output current (quiescent).	[]	
d. Measure and record output current (alarm condition) and ensure within specification.	[]	
e. Check transition to alternative power source.	[]	
f. Check health of alternative power source (see footnote).	[]	
g. Restore external power source and check that charge current flows to alternative power source	[]	
h. Check signalling of all appropriate faults to CIE.	[]	
i. Measure and record induced AC voltage on DC output.	[]	i. Measured by using voltmeter on AC volts range, measuring between DC +/- outputs and mains earth connection.
j. Check operation of tamper switch(es).	[]	
k. Label alternative power source with date of installation.	[]	
4. DETECTORS		
a. Check detectors are correctly fitted, secure, etc.	[]	
b. Check siting suitable for environment and site risk.	[]	
c. Measure and record supply voltage.	[]	
d. Check anti-masking.	[]	G
e. Check range reduction.	[]	G
f. Check operation of tamper switch(es) and detection of orientation adjustment	[]	G

COMMISSIONING REQUIREMENTS		Notes	
g. Walk test all detectors, including check of range correctly set.	[]		
h. For detectors containing a type C power supply, check the date of installation is recorded on the storage device.	[]		
5. HOLD-UP DEVICES			
a. Check devices are correctly fitted, secure, etc.	[]		
b. Check all devices operate correctly.	[]		
c. Check all devices reset correctly.	[]		
6. WARNING DEVICES			
a. Check devices are correctly fitted, secure, etc.	[]		
b. Measure and record supply voltage.	[]		
c. Check health of alternative power source (see footnote).	[]		
d. Verify WD is capable of charging alternative power source.	[]		
e. Measure and record current in alarm condition.	[]		
f. Check operation when triggered from CIE.	[]		
g. Check operation when self-actuated.	[]		
h. Check operation of tamper switch(es).	[]		
i. Check date of installation is recorded on alternative power source and included in system record.	[]		
7. ALARM TRANSMISSION SYSTEMS			
a. Measure and record supply voltage.	[]		
b. Test all signals to the ARC by all paths.	[]	(Testing should be done in conjunction with ARC, placing the system on test before commencing)	
c. Test restoration of all signals.	[]		
d. Test transmission path fault signal monitor and CIE response (all paths).	[]		
e. Test transmission path fault signal to ARC if multi-path equipment fitted.	[]		
f. Check restoration of all transmission paths.			
g. Check sequential confirmation signals in conjunction with the ARC.	[]		
h. Check audio confirmation in conjunction with the ARC.	[]		
i. Check visual confirmation in conjunction with the ARC.	[]		
j. Check operation of tamper switch(es).	[]		
k. Check health of alternative power source	[]		
l. Check date of installation is recorded on alternative power source.	[]		
8. INTERCONNECTIONS			
a. Check that the correct type of interconnections have been fitted, as per manufacturer's recommendations.	[]		

COMMISSIONING REQUIREMENTS		Notes
b. Check interconnections used are capable of safely carrying the expected current.	[]	b. As a guide, 'standard' 7/0.2mm alarm cable is rated to carry up to 1.4A
c. Check interconnections are secured, and routed to avoid potential sources of interference and physical damage.	[]	
d. Measure and record resistance of all interconnections ensuring that this is commensurate with the length of interconnections installed.	[]	d. As a guide, 'standard' 7/0.2mm alarm cable measures approximately 8 ohms per 100 metres per core.
e. Check continuity and correct termination of all interconnection screens.	[]	
9. OTHER PERIPHERAL EQUIPMENT		
a. Measure and record supply voltage,	[]	
b. Measure and record quiescent current.	[]	
c. Check communication with CIE is functional.	[]	
d. Ensure all outputs are used within manufacturer's specification.	[]	
e. Check operation of tamper switch(es).	[]	
10. REMOTE SUPPORT		
a. Confirm remote communication is available.	[]	
b. Confirm panel data has been correctly transferred.	[]	
11. TRAINING		
a. Train user(s) and ensure they understand the operation of the system.	[]	
b. Record names of users trained on site.	[]	

G = some aspect(s) of the requirement is grade-dependent.

Footnote: An alternative power source is deemed to be healthy if it is capable of supporting the required load at the correct voltage. See Annex A

7. PREVENTATIVE MAINTENANCE

7.1 Frequency of maintenance

The frequency of maintenance should, as a minimum, be:

Grade 1 & 2X	one site visit per year
Grades 2 A, B, C, D & 3	<i>Either:</i> two site visits per year <i>or:</i> one site visit and one remote system check per year
Grade 4	two site visits per year

Note: The interval between preventative maintenance should not exceed 7 months (13 months for grade 1 and 2X).

7.2 Preventative maintenance requirements

As a minimum, the checks should be in accordance with the mandatory requirements of Table 2.

There should be a written agreement with the client detailing the remote system checks that will be carried out.

Where practicable, any faults discovered should be corrected before leaving site and/or any irregularities found must be reported and the appropriate action taken as soon as practicable. If this is not possible or if the fault/irregularities are discovered through a remote system check, arrangements should be made for the faults/irregularities to be corrected as soon as is practicable.

The system history should be kept up to date with details of the maintenance carried out, and of any corrective measures taken or required.

8. REMOTE SYSTEM CHECKS

8.1 General

Remote system checks should not generate any false alarms. The remote system check should leave the I&HAS in the same set/unset status it was before the remote system check took place. Any faults/irregularities found (corrected or otherwise) should be logged and reported to the user/client as soon as possible.

8.2 Review of the event log

The system log should be interrogated. Any technical fault/irregularity found which may adversely affect the system performance is to be reported to the user as soon as is practicable and any prior agreed corrective action taken.

The maintenance report should include the date and time when the system was last successfully Set and Unset.

The CIE internal clock should be checked and adjusted if necessary for the correct date and time.

The remote system check should be used to confirm, against the system record, any detectors that are on soak test and/or inhibited/isolated. There must be prior agreement with the user/client for any detectors that have been put on soak test or inhibited/isolated. If any others are found during the remote system check then the user should be informed as soon as is practicable or any prior agreed action taken.

8.3 External power source/Alternative power source

The remote system check should show that the external power source is available, that the alternative power supply is charging (if applicable) and that the alternative power source is capable of running the I&HAS if a power failure occurs. See Annex A for details. If a fault is found, the user should be informed as soon as is practicable.

8.4 Detectors

The remote system check should show the activity of detectors that would be expected to operate during the normal occupation of the supervised premises. There should be a written agreement with the client that details the detectors that will operate during the normal occupation of the supervised premises.

Note: It may be necessary for the user to 'walk test' certain detectors prior to the setting of the system (this is optional and depends on the agreed procedure).

8.5 Alarm transmission system

A check for the correct operation of any alarm transmission system should be made. Where multiple transmission paths are provided, all should be tested. This should be done in conjunction with the ARC, eg by using ARC logs to verify correct receipt of these test signals.

8.6 Records of remote system checks

Detailed records of the checks undertaken should be recorded and the results logged. The date, time, results of the remote system checks, faults found, and the identity of any personnel and/or automated system carrying out the checks are the minimum that should be recorded.

Records should be kept for a minimum of 15 months.

Table 2 PREVENTATIVE MAINTENANCE REQUIREMENTS

Note: Not all checks will be applicable to every installed I&HAS or every part of an installed I&HAS).

PREVENTATIVE MAINTENANCE REQUIREMENTS		SITE VISIT	REMOTE CHECK
1. GENERAL			
a. Client/user documentation is up to date and on site		M	-
b. Check that installed system meets the As-Fitted Document		M	-
2. CONTROL AND INDICATING EQUIPMENT			
a. Check that all ACE is operational.		M	O
b. Check all peripheral equipment is 'on-line'.		M	O
c. Interrogate system log and action as required.		M	M
d. Check the system sets (may be taken from event log).		M	M
e. Check set and unset indications are correct.		M	O
f. Activate intruder alarm.		M	O
g. Activate duress facility.	G	M	O

PREVENTATIVE MAINTENANCE REQUIREMENTS		SITE VISIT	REMOTE CHECK
h. Activate any hold-up alarm facility		M	O
i. Check the system unsets (may be taken from event log).		M	M
j. Check all annunciation equipment is functioning.		M	O
k. Check no adverse tamper conditions exist on the system		M	M
l. Check no adverse fault conditions exist on the system		M	M
m. Check any alarm circuits/ points that are on soak test.		M	M
n. Check any alarm circuits/ points that are inhibited/ isolated		M	M
o. Ensure time and date of clock are correct.		M	M
p. Check auxiliary outputs are operating.		M	O
q. For testing alternative power source see 3. d (POWER SUPPLIES).			
3. POWER SUPPLIES			
a. Check all voltages and current levels are within manufacturers ratings.		M	M
b. Check 'expiry date' of alternative power source. Replace if necessary		M	O
c. Check health of alternative power source (see footnote)		M	M
4. DETECTORS			
a. Check physical condition (clean, fitted correctly, no damage, etc).		M	O
b. Check environmental conditions.		M	O
c. Check operation of all detectors.		M	O
d. Check current anti-masking status of required detectors.	G	M	M
e. Check current range reduction status of movement detectors.	G	M	M
f. Check that 'frequently used' detectors are operating (eg during the last 7 unset periods or since last maintenance).		O	M
5. HOLD-UP DEVICES			
a. Check physical condition.		M	O
b. Operate Hold-up devices.		M	O
c. Reset Hold-up devices.		M	O
6. WARNING DEVICES			
a. Check physical condition is satisfactory.		M	O
b. Check correct functioning of device (eg if remote check, visual, current sensing, etc).		M	O
c. Check expiry date of alternative power source; replace if necessary.		M	O
d. Check health of alternative power source (See footnote)		M	M
7. ALARM TRANSMISSION SYSTEM(S)			
a. Test correct operation by all paths		O	M
b. For parallel connected ATE test all relevant signals through to the ABC (alarm control panel)		M	O

PREVENTATIVE MAINTENANCE REQUIREMENTS		SITE VISIT	REMOTE CHECK
the ARC (alarm, restore, etc).			
c. For serial connected ATE test a typical signal through to the ARC, including 'restore.'		M	O
d. Test transmission path fault signal (all paths) to the ARC and the CIE response.		M	O
e. Check sequential confirmation signals in conjunction with the ARC.		M	O
f. Check audio confirmation in conjunction with the ARC.		M	O
g. Check visual confirmation in conjunction with the ARC.		M	O
h. Check expiry date of alternative power source. Replace if necessary.		M	O
i. Check health of alternative power source. (See footnote)		M	M
8. INTERCONNECTIONS			
a. Check interconnections are secure and as per As-Fitted Document.		M	O
b. Check interconnections are not subject to detrimental effects.		M	O
c. Check interconnections for potential problems		O	M
9. TRAINING			
a. Confirm users understand the alarm system operation.		M	O
b. Train any untrained users during visit or arrange for training.		O	O
c. Record names of users trained on site.		M	O

M = Mandatory

O = Optional

G = some aspect(s) of the requirement is grade-dependent.

Footnote: An alternative power supply is deemed to be healthy if it is capable of supporting the required load at the correct voltage. See Annex A.

9 REMOTE SUPPORT

9.1 GENERAL

9.1.1 Remote support permits the exchange of data between supervised premises and remote locations, controlled by a computer to allow interaction.

9.1.2 Typical examples of information that may be accessed / exchanged remotely include:-

- Client identification
- I&HAS status and fault report
- I&HAS event log
- On-line restore
- Site specific system configuration details
- Setting and unsetting the system
- Remote system checks
- Remote system diagnostics
- Remote omission of faulty alarm circuits or points

9.1.3 A company that applies remote support for I&HAS should have written procedures that:

- i. lead to precise definitions for the levels of authorisation, including client/insurer authorisation, that are associated with each remote command as itemised in Table 3;
- ii. ensure that in all cases written agreements exist with clients (and insurers where appropriate) concerning levels of authorisation;
- iii. ensure strict control of the proper use of remote dialogues by authorised persons in accordance with the agreements with clients/insurers.

9.2 INITIALISATION OF REMOTE COMMUNICATIONS

9.2.1 Methods

There are three main methods of initialising remote communication and these are listed below:-

- i Automatic* The CIE initiates a dialogue in response to a system event.
- ii Manual* A user or engineer initiates a dialogue from the protected premises
- iii Remote* Dialogue is initiated from a remote location. This may be by Direct or Ringback methods, used after success of authentication process.

9.3 SECURITY OF DATA

9.3.1 Recommendations

The following security measures are considered to be the minimum which should be implemented:

Area of Security	Recommendations
i Authentication	Mandatory
ii Encryption of data sent	Optional
iii Full audit trail of remote activity	(1) Mandatory
iv Levels of security for operators	(2) Mandatory

Note 1: If the dialogue is initiated from the CIE, or remotely by ring-back, it should be possible to identify the remote location.

Note 2: Operator access to the computer used at the remote location requires permission equivalent to the requirements of prEN50131-1:2004 clause 8.3.2

9.3.2 Authentication

A secure validation process where both the I&HAS at the protected premises and the computer at the remote location exchange a code or codes to authenticate the identity of both the originator and respondent before proceeding with a remote support operation.

Codes used should have at least one million differs, be unique for each I&HAS and be changed in a non-sequential manner for every system and should not predictably be repeated within 100 systems.

Should either the originator or answering identity not be validated on the first attempt, then the established communication path should be broken.

9.4 AUDIT TRAIL

A log of remote dialogues should be recorded at the remote location, with at least the following information:

- i) date and time of the remote dialogue;
- ii) identification of the operator carrying out the dialogue;
- iii) full details of any changes to site specific parameters.
- iv) the user / client authorising such changes (1);

Note 1: This authorisation must be recorded, even though it may be impractical to obtain a written signature from the user (see 5.2).

This audit trail should be retained for a minimum period of 15 months.

9.5. REMOTE INITIATION OF COMMANDS

Sources of initiation of downloading commands are classified as follows:

- | | | |
|----|-----------------------------------|---------|
| 1. | Alarm receiving centre | Level 3 |
| 2. | Alarm company/Maintaining company | Level 3 |
| 3. | User / Client | Level 2 |

Recommendations for the remote initiation of commands are shown in Table 3.

Table 3 – INITIATION OF COMMANDS

Note: Permission to carry out these functions does NOT imply that it is mandatory for equipment to include them. Where the function is provided, it should be used as follows. Functions not included in this table may be used with the agreement of the client/insurer.

	COMMANDS	INITIATED BY			IAS UNSET	IAS SET
		ARC	ALARM Co.	USER/ CLIENT	ALARM TRANSMISSION SYSTEM TO HAVE PRIORITY	
a	Request for information (system status) eg battery checks, time base check	\$	P	P	P	P
b	Remote signal test (initiate call)	\$	P	N	P	P
c	Set system	*	*	P	P	
d	Unset system	*	*	P		P
e	On-line restore	P	P	N	P	N
f	Remote isolation of part of system (permanent change)	*	*	N	P	P
g	Remote removal of isolation	*	*	N	P	P
h	Remote inhibit of part of system (temporary measure, removed at unset)	*	*	P	P	P
i	Remote removal of inhibit	*	*	P	P	P
j	Adjust system date and time	\$	P	P	P	P
k	Put circuit on test	*	*	N	P	N
l	Remove circuit / device from test	*	*	N	P	P
m	Transfer initial system configuration to I&HAS	\$	P	N	P	N
n	Transfer initial system configuration to remote location	\$	P	N	P	P
o	Transfer changes to system configuration	*	*	N	P	P
p	Tel No change (for alarm notification)	\$	P	N	P	P
q	Tel No change (for remote support)	\$	P	N	P	P
r	Change engineers code	\$	P	N	P	P
s	Change user access code	*	*	P	P	P
t	Update I&HAS operating firmware	€	€	N	P	N
u	Lock out system (eg in event of non-payment) – only after customer has not responded to written requests, or has refused access to the I&HAS.	\$	P	N	P	Δ
v	Remove system lock-out	\$	P	N	P	N
w	Activate auxiliary outputs (switch on/off equipment, plant, lights)	\$	P	P	P	P
x	Activate/silence warning devices	%	†	N	P	P
y	Suppression of warning devices	∞	N	N	P	P

KEY:

- P – Permitted
- N – Not permitted
- * - Only with agreement of client / insurer
- \$ - Only under contract to alarm company
- € - With approval of equipment manufacturer in addition to client / insurer.
- Δ - Command may be sent whilst set, but may not take effect until I&HAS is unset.
- % - In conjunction with confirmation procedures or as part of remote system checks (under contract to alarm company and with agreement of client / insurer).
- † - Only as part of remote system checks (with agreement of client / insurer).
- ∞ - Where receipt of signal at ARC can be confirmed during a WD delay period

ANNEX A

Verification of Health of Alternative Power Source

An alternative power source (APS) is deemed to be healthy if it is capable of supporting the required load at the correct voltage. The following are examples of methods deemed to meet this requirement.

- a) With the APS disconnected from the I&HAS (which is therefore operating from the External Power Source only), a load is applied to the APS at least equal to the maximum peak expected system load and for a minimum time period appropriate for the type of Storage Device (SD) in use; see Table 4 below. During application of this load the voltage at the output of the APS must not fall below the minimum acceptable level declared by the equipment manufacturer and there must be no impact upon the normal operation of the I&HAS.
- (b) The voltage of a programmable power supply may be reduced in a controlled manner to a level such that the APS is switched into circuit as the power source for the I&HAS for a minimum time period appropriate for the type of Storage Device (SD) in use, see Table 4 below. During the test period, the system load should be equivalent to the peak expected system load. The voltage at the output of the APS must not fall below the minimum acceptable level declared by the equipment manufacturer during the test period and there must be no impact upon the normal operation of the I&HAS. Should the APS be detected as unhealthy, the power supply to the I&HAS must immediately be returned to operation from the EPS without any transients that may cause erroneous behaviour of the I&HAS.

Table 4. MINIMUM LOAD TIMES FOR COMMON STORAGE DEVICES

<i>Type of Storage Device</i>	<i>Minimum Load time</i>	<i>Notes</i>
Lead Acid Battery	10 s	Based upon Skafor+ recommendations
Other re-chargeable battery	1 s	e.g. NiCad, NiMH, etc.

+ Skafor is the Scandinavian national approvals body.

Note: In the case of primary (eg dry cell) batteries, verify that the terminal voltage exceeds the minimum acceptable level declared by the equipment manufacturer. Loading is NOT required.