August 2015

To: **All NSI NACOSS Gold, Systems Silver and ARC Gold approved companies and applicants**

TECHNICAL BULLETIN No. 0029

Guidance on the application of BS 8418:2015 – Installation and remote monitoring of detector-activated CCTV systems – Code of practice

(Supersedes BS 8418:2010)

BS 8418:2015 ("the new BS") is a full revision of the standard and there are many editorial changes to the wording compared to BS 8418:2010 ("the old BS"). This Technical Bulletin aims to provide information about most of the changes and does not include all the editorial changes.

Please refer to the new BS for full details of the requirements.

This Technical Bulletin paraphrases the wording of the new BS in some areas. Whilst every effort has been made to convey the true meaning of the new BS the actual wording of the new BS prevails in situations where there might be a perceived conflict.

NOTE REGARDING THE STATUS OF THE NEW BS: Please note we regard compliance with the recommendations in the new BS as mandatory for all organizations wishing to obtain or maintain an NSI approval subject to any clarifications and guidance included within this Technical Bulletin or issued subsequently.

You must please regard the recommendations given in the new BS as requirements of the relevant NSI approval schemes.

GENERAL OBSERVATIONS

The terms "installer" and "maintainer" have been replaced with the term "CCTV company" (similar to "alarm company" in other standards). The term "protected premises" has been replaced with the term "supervised premises" (similar to other standards). Also the term "owner" has been replaced with the term "customer".

References to BS EN 50132-7 have been replaced by specific clauses of BS IEC 62676-4. However BS EN 62676-4:2015 now supersedes BS IEC 62676-4:2014 and the content of both standards is identical. Therefore you can adhere to BS EN 62676-4:2015 or BS IEC 62676-4:2014 in relation to the relevant clauses.

The new BS (BS 8418:2015) recognises that contractual agreements may exist between the customer, the CCTV company and the RVRC, as opposed to existing only between the customer and RVRC. Furthermore the new BS places most of the onus on the CCTV company to set up these contractual agreements with the customer and the RVRC.

The majority of requirements for tamper detection and indication are now consolidated in Table 1 of the new BS. The majority of requirements for fault recognition and indication are now consolidated in Table 2 of the new BS.

SUMMARY OF KEY CHANGES FOR CCTV COMPANIES

Refer to the list below for a summary of changes affecting CCTV companies. Further details are given later in this Technical Bulletin.

1 The new BS (BS 8418:2015) came into effect on 31 January 2015. However, the new BS recognizes that suppliers of products and services will require time to comply. Therefore, BS 8418:2010 (“the old BS”) remains effective until 31 July 2015.

2 Remote monitored detector-activated CCTV systems can be installed to the old BS up until 31 July 2015. However from 1 August 2015 all new BS 8418 remote monitored detector-activated CCTV systems must be installed to the new BS.

3 To install remote monitored detector-activated CCTV systems to the new BS it is necessary to obtain supplies of components and equipment meeting the new BS. Therefore, please refer to suppliers for further information.

4 The new BS applies to permanent and temporary/portable CCTV systems irrespective of the length of time they are installed and/or whether the equipment can be re-used on another site (see clause 1 of the new BS).

5 A threat assessment and risk analysis must be performed in accordance with BS IEC 62676-4:2014, 4.2.1 (or BS EN 62676-4:2015, 4.2.1) prior to CCTV system design and to assist in understanding the purpose of the system (see 4.1.1 of the new BS).

6 The CCTV company (installer) must ensure that an Operational Requirements (OR) document is generated in accordance with BS IEC 62676-4:2014, 5.2 and 5.3 (or BS EN 62676-4:2015, 5.2 and 5.3), which clearly defines the needs, justifications and purpose of the CCTV system (see 4.1.2 of the new BS).

7 The CCTV system design proposal agreed between the CCTV company and the customer must be based on the content of the OR (see 4.2.1 of the new BS).

8 When displayed on the screen, the size of a person must conform to BS IEC 62676-4:2014, 6.7 (or BS EN 62676-4:2015, 6.7) in relation to the intended task (i.e. identification, recognition, observation or detection), the minimum requirement being detection (10 % of screen height) (see 4.4.1.2 of the new BS).

9 Known artificial illumination faults must be rectified as soon as practicable in accordance with the documented agreement between the RVRC, the CCTV company and the customer (see 4.4.2.5 of the new BS).

10 Audio challenges during the set state must be initiated by the RVRC only (see 4.5 of the new BS).

11 The written agreement about detector omission must be between the customer, the CCTV company and the RVRC (see 4.6.3 of the new BS) whereas previously the agreement was between the customer and the RVRC.

12 The written agreement about detector isolation must be between the customer, the CCTV company and the RVRC (see 4.6.4 of the new BS) whereas previously the agreement was between the customer and the RVRC.

13 Camera signals between the camera and control equipment must be monitored for video loss. If the video loss does not automatically restore within 30 s, it must be recorded in the event log at the premises. The system must ensure that video loss is clearly indicated locally (where a monitor is fitted) by an example of "no picture" or "video loss" message (see 4.6.5 of the new BS).

14 Means must be provided to detect and indicate the tamper conditions specified in Table 1 of the new BS. Tamper indications must be audible and/or visual. Local indication at the supervised premises must be indicated to the person setting the system (see 4.6.6 of the new BS).

15 The setting/unsetting device must be provided with tamper detection in accordance with Table 1 of the new BS. If the device is opened, it must not be possible to affect the correct functioning nor change the state of the CCTV system (see 4.6.6 of the new BS).

16 Means must be provided to recognize and indicate the fault conditions specified in Table 2. Fault indications can be audible and/or visual. Except where setting and unsetting is carried out by the RVRC, means of local fault indication at the supervised premises must be indicated to the person setting and unsetting the system (see 4.6.7 of the new BS).

17 Where wireless or semi-wired detectors are used, faults at the detector must be reported in accordance with Table 2. The loss of communication between the control equipment and any detector must be notified within a period not exceeding 20 min, in accordance with Table 2. Every detector must be uniquely identified to the CCTV system (see 4.6.8 of the new BS).

18 The control equipment must be located within the supervised premises such that access to the control equipment is restricted. Such an area could be a security office or a store room where the area is only accessible by designated staff and/or users of the system. Equally it could be the supervised premises, which only employees have access to in working hours. Where there is unrestricted access to the control equipment in the set condition, tamper detection must be provided in accordance with Table 1 (see 4.6.9 of the new BS).

19 Event log(s) at the control equipment must be maintained at the supervised premises in a dated and timed retrievable format. The total capacity of the event log(s) must be at least 2,000 events. The log(s) must be protected against the accidental or deliberate deletion or alteration of the contents (see 4.6.10 of the new BS).

20 A minimum of one data transmission path must be provided as the method of communication between the CCTV system and the RVRC. The transmission path must have the capability to transmit data to the RVRC. Failure of the transmission path must be reported to or detected by the RVRC within three minutes and in accordance with Table 2 (see 4.6.11 of the new BS).

21 The requirements for power supplies have been revised substantially and there is no need for an uninterruptible power supply (UPS). However there has to be an alternative power source (for example a battery). The alternative power supply must support the CCTV control equipment and the devices used to transmit data to the RVRC for a minimum period of 30 minutes following failure of the prime power source. Power supplies to detectors and semi-wired detectors must be fitted with an alternative power source capable of supplying power for a minimum of 4 hours (see 4.6.14 of the new BS).

22 The installation of camera equipment must be carried out in accordance with clauses 4.7 and 15 of BS IEC 62676-4:2014 (or clauses 4.7 and 15 of BS EN 62676-4:2015) (see 5.3 of the new BS).

23 The CCTV company must provide all the required information to the RVRC at least 24 h before the CCTV system is commissioned (see 6.1 of the new BS).

24 During commissioning, the CCTV company must review the day and night reference images to ensure that they meet the system design proposal. This includes each of the preset positions for functional cameras (see 6.4 of the new BS).

25 During commissioning the cameras must be checked on configuration to ensure that they are correctly focused both during the day and at night. At the end of the soak test period any performance issues must be recorded and resolved to the satisfaction of the customer, the CCTV company and the RVRC (see 6.6 of the new BS).

26 There are some important new (general) requirements for setting/unsetting (see 7.1 of the new BS).

27 The responsibilities and considerations are largely unchanged). However responsibility is placed on the CCTV company to create a documented agreement in consultation with the customer and the RVRC and to ensure the customer receives a copy of the response plan (see clause 8 of the new BS).

28 Adjustments have been made to the requirements for maintenance (see clause 14 of the new BS in particular clause 14.1.2).

29 The image of each detection area must be compared with the relevant stored reference images by the CCTV company in conjunction with the RVRC at each maintenance visit. If necessary new reference image(s) must be created and stored at the RVRC, e.g. in the event of a camera repair or replacement (see 14.1.2.6 of the new BS).

SUMMARY OF KEY POINTS FOR RVRCs

Refer to the list below for a summary of changes affecting RVRCs. Further details are given later in this Technical Bulletin.

A The new BS (BS 8418:2015) came into effect on 31 January 2015. However, the new BS recognizes that suppliers of products and services will require time to comply. Therefore, BS 8418:2010 (“the old BS”) remains effective until 31 July 2015.

B From 1 August 2015, RVRCs must monitor all BS 8418 CCTV systems to the new BS irrespective of whether the systems are installed to the old BS or the new BS.

C The RVRC must ensure the supervised premises documentation (see 6.1) provides a clear understanding of the layout of the supervised premises and the areas to be viewed when a detector initiates an activation. RVRC operators must be able to describe accurately the nature of incidents as they occur. In order to achieve this, the supervised premises plan [see 6.1c)] must show detailed information to include the detection and camera fields of view (see 9.1 of the new BS).

D The RVRC operator must authorize detector omissions. Where the RVRC authorizes the omission of a detector, it must be carried out by the RVRC operator. The RVRC must inform the CCTV company of all omissions (see 9.4 of the new BS).

E As a minimum, the construction and facilities of the RVRC must conform to BS 5979:2007, Category II or BS 8591:2014, Category II. This confirms BS 8591 ARCs alongside BS 5979 ARCs (see 9.4 of the new BS).

F Images received at the RVRC must be stored electronically on a medium such as a hard drive. Reference images must be stored electronically within the RVRC and must be accessible to the RVRC operator during live event handling for comparison purposes. For functional cameras, reference images relating to each of the preset positions must be stored (see 11.2 of the new BS).

G Where data and/or images are stored digitally and might be required as evidence for a crime, then this must be in accordance with clause 11 of BS IEC 62676-4:2014 (or clause 11 of BS EN 62767-4:2015) (see 11.3 of the new BS).

H Procedures must be established to authenticate the exchange of confidential information between the RVRC and the customer. Details must be agreed with the CCTV company and the customer (see 11.4 of the new BS).

I Adjustments have been made to the requirements for maintenance (see clause 14 of the new BS).

J The image of each detection area must be compared with the relevant stored reference images by the CCTV company in conjunction with the RVRC at each maintenance visit. If necessary new reference image(s) must be created and stored at the RVRC, e.g. in the event of a camera repair or replacement (see 14.1.2.6 of the new BS).

DETAILS ABOUT THE NEW BS

Details about the new BS are given below according the relevant clause.

Bold text is used to quote details about changes in the new BS.

Guidance or comment about the new BS is given in *italics*.

1 SCOPE

The new BS gives recommendations for the design, installation, commissioning, operation and remote monitoring of detector-activated CCTV systems, **whether "permanent" or temporary/portable**.

The new BS applies **irrespective of the length of time the CCTV systems are installed and/or whether the equipment can be re-used on another site**.

The standard gives recommendations to the following parties:

a) **CCTV companies** on best practice for the design, installation, commissioning, **maintenance** and operation of detector-activated CCTV systems;

Note This includes the installation and maintenance engineers working for the CCTV company.

b) Remote video response centres (RVRCs) monitoring CCTV systems; and

c) **Customers** regarding the management of CCTV systems.

The main change to the scope relates to the inclusion of temporary and portable CCTV systems. The term "CCTV companies" replaces "installers and maintenance providers" and the term "Customers" replaces the term "Owners and users"

Table 2 below illustrates how the standard applies to CCTV companies, RVRCs and customers (including users) and how all parties need to work closely together in order to meet the standard.

2 NORMATIVE REFERENCES

The following normative references have been added:

BS 8243:2010+A1:2014, Installation and configuration of intruder and hold-up alarm systems designed to generate confirmed alarm conditions – Code of practice

BS 8591:2014, Remote centres receiving signals from alarm systems – Code of practice

BS EN 62676-1-1, Video surveillance systems for use in security applications – System requirement – Part 1-1: General

BS IEC 62676-4:2014, Video surveillance systems for use in security applications – Part 4: Application guidelines

The following normative references have been deleted:

BS 8495, Code of practice for digital CCTV recording systems for the purpose of image export to be used as evidence

BS EN 50132-7, Alarm systems – CCTV surveillance systems for use in security applications – Part 7: Application guidelines.

Please note BS EN 62676-4:2015 now supersedes BS IEC 62676-4:2014 and BS 8495:2007. In addition BS EN 62676-4:2015 supersedes BS EN 50132-7:2012, which will be withdrawn on 13 April 2018.

TABLE 2 – Application of BS 8418:2015 to CCTV companies, RVRCs and customers

Clause	Content	Applies to
1	Scope	CCTV company, RVRC and customer
2	Normative references	CCTV company and RVRC
3	Terms, definitions and abbreviations	CCTV company, RVRC and customer
4	CCTV system planning and design	CCTV company and customer
5	Installation	CCTV company
6	Commissioning	CCTV company, RVRC and customer
7	Setting/unsetting procedures of the CCTV system on the supervised premises	CCTV company, customer and RVRC
8	Responsibilities and considerations	CCTV company, customer and RVRC
9	RVRC operator procedures	RVRC, customer and CCTV company
10	Management and operation of the RVRC	RVRC
11	RVRC procedures and documentation	RVRC, customer and CCTV company
12	Activation management	RVRC
13	Service levels	RVRC
14	General maintenance and personnel screening	CCTV company, RVRC and customer

3 TERMS, DEFINITIONS AND ABBREVIATIONS

The following definitions have been added to cover terms used in the standard:

3.1.2 activation delay procedure

operation of a CCTV system triggered by an event resulting in the transmission of images to an RVRC

3.1.4 alternative power source

power source capable of powering components of the CCTV system for a predetermined time when a prime power source is unavailable

3.1.5 as-fitted document

document in which details of the CCTV system actually installed are recorded

3.1.7 CCTV company

organization which provides installation and/or maintenance services for CCTV systems

The term "CCTV company" replaces "installer or maintenance provider".

3.1.10 customer

person or organization utilizing the services of a CCTV company

The term "customer" replaces "owner".

3.1.15 dormant period

period of time in which further activations do not occur

3.1.17 fault

condition of one or more components or interconnections that prevents the CCTV system or part thereof from operating normally

3.1.22 isolation

status of a detector in which an activation cannot occur, such status remaining until the detector is restored

3.1.23 omission

status of a detector in which an activation cannot occur, such status remaining until the CCTV system is returned to an unset state

3.1.25 operational requirement

key document for system designers, which clearly defines the functions of the CCTV system according to the customer expectations

NOTE Refer to BS IEC 62676-4:2014, Clause 5 "Operational requirements specifications".

3.1.27 power supply

device that stores, provides and modifies or isolates (electrical) power for a CCTV system or part thereof

3.1.28 prime power source

power source used to support components of a CCTV system under normal working conditions

3.1.35 supervised premises

site address, agreed by contract, at which there is one or more secure areas

The term "supervised premises" replaces "protected premises".

3.1.36 tamper

deliberate interference with a CCTV system or part thereof

3.1.37 uninterruptable power supply

electrical apparatus that provides emergency power to a load when the prime power source fails

Some other definitions have been deleted because they are no longer used. Also there are minor changes to the wording of some definitions.

4 CCTV SYSTEM PLANNING AND DESIGN

4.1 Planning

This is a new sub-clause on planning the CCTV system.

4.1.1 Threat assessment and risk analysis

A threat assessment and risk analysis should be performed in accordance with BS IEC 62676-4:2014, 4.2.1, prior to CCTV system design and to assist in understanding the purpose of the system.

A threat assessment and risk analysis must be carried out.

4.1.2 Operational requirement (OR)

The CCTV company should ensure that an Operational Requirements document is generated in accordance with BS IEC 62676-4:2014, 5.2 and 5.3, which clearly defines the needs, justifications and purpose of the CCTV system. The OR document should take account of the threats identified, and inform the design of the CCTV system as well as provide a mechanism for producing a technical specification and test procedures.

NOTE The Operational Requirements could be included within the System Design Proposal. See 4.2.

An operational requirements (OR) document must be generated.

4.1.3 Temporary and/or portable systems

Where temporary and/or portable systems are used, they should conform to all of the recommendations in this standard.

The provisions of BS 8418:2015 apply also to temporary and/or portable systems conforming to this standard.

4.2 CCTV system design proposal

4.2.1 The CCTV company should agree a CCTV system design proposal, based on the OR, with the customer.

The main change here is for the CCTV system design proposal to be based on the OR.

4.3 Detector selection, positioning and configuration

This clause has been re-structured to some degree with changes to sub-headings and re-wording of the some of the requirements. There are no significant changes to the requirements. However sub-clause 4.2.4 of the old BS relating to wireless and semi-wired detectors has moved to sub-clause 4.6.8 in the new BS.

4.4 Camera positioning and configuration

4.4.1 General

The requirements for checking the focus of cameras has been moved to 6.6 in the new BS (environmental soak test). There are no significant changes to the requirements except the following:

4.4.1.2 When displayed on the screen, the size of a person should conform to BS IEC 62676-4:2014, 6.7 in relation to the intended task (i.e. identification, recognition, observation or detection), the minimum requirement being detection.

The minimum requirement is to detect a person, which means the person must not be less than 10 % of screen height when that person is at the agreed location. Other percentages are 25 % for observation, 50 % for recognition and 100 % for identification (see Table 3 below).

TABLE 3 – Percentage of screen height filled by target to achieve objective

Objective	Percentage of Screen Height	Explanation
Monitoring	At least 5 %	*Monitoring means the operator viewing the display screens is able to assess the movement of people, for example in relation to crowd control activities.*
Detection	At least 10 %	*Detection means the operator viewing the display screens is able to determine with a high degree of certainty whether or not a human being is present.*
Observation	At least 25 %	*Observation means the operator viewing the display screens is able to see some characteristic details of the individual, such as distinctive clothing, whilst also being able to see some activity surrounding the incident being viewed.*
Recognition	At least 50 %	*Recognition means the operator viewing the display screen is able to determine with a high degree of certainty whether or not an individual shown is the same as someone they have seen before.*
Identification	At least 100 %	*Identification means with the target now occupying at least 100 % of the screen height, picture quality and detail is sufficient to enable the identity of an individual to be established beyond reasonable doubt.*

The above percentage figures relate to the use of PAL (576i) resolution. The figures are higher if NTSC (486i) resolution is used (for example 120 % for identification).

The influx of digital systems means there is variability in the capture, recording and display resolution depending on the format. Therefore a requirement for "recognition" cannot be equated simply to a 50 % screen height. Table 2 of 6.7 of BS IEC 62676-4:2014 provides commonly encountered resolutions and Table 3 of 6.7 of BS IEC 62676-4:2014 shows the equivalent screen heights (in %) needed to maintain the required resolution. The data in these Tables should be used as a guideline to the proportion of the screen to be filled by the target as other factors such as contrast and illumination can affect the available information in the image.

4.4.2 Illumination

There are no significant changes. However the requirements relating to known artificial illumination faults have been re-drafted as follows:

4.4.2.5 Known artificial illumination faults should be rectified as soon as practicable and in accordance with the documented agreement in 8.3.

NOTE 1 Until the fault is rectified and accepted as such by the RVRC, the secure area affected by the failure of artificial illumination might not be capable of being monitored by the RVRC.

NOTE 2 It might be desirable to have an agreement (see 8.3) between the RVRC, CCTV company and/or customer as to the

checks to be made to ensure the correct operation of the artificial illumination.

NOTE 3 It is advisable to implement a process for reporting artificial illumination failure back to the RVRC.

This requires illumination faults to be managed in accordance with the documented agreement detailed in 8.3 of the new BS. The old BS required action by the RVRC operator within 24 hours followed by action from the owner once notified.

The requirement in the old BS (4.3.2.9) that "IR illumination should not surround the camera lens on external cameras" has been deleted.

This permits IR illumination to surround cameras lenses when the circumstances are appropriate.

4.5 Audio challenge

There is a change to the standard as follows:

Audio challenges during the set state should be initiated by the RVRC only.

4.6 CCTV system performance and integrity

4.6.2 Data transmission system

This sub-clause has been re-worded as follows:

The data transmission system should be capable of sending continuous live video until the RVRC operator terminates the connection.

Compression required for transmission should not compromise the image presented to the RVRC operator (see 4.4.1.2).

The main change relates to making sure that compression of data does not compromise the images at the RVRC.

4.6.3 Detector omission

The written agreement about detector omission must be between the customer, the CCTV company and the RVRC whereas the agreement was between the customer (owner) and the RVRC under the old BS.

The change recognises the involvement of the CCTV company in the written agreement to manage detector omission.

4.6.4 Detector isolation

The written agreement about detector isolation must be between the customer, the CCTV company and the RVRC whereas the agreement was between the customer (owner) and the RVRC under the old BS.

The change recognises the involvement of the CCTV company in the written agreement to manage detector isolation.

Also detector isolation must be logged at the RVRC and/or in the event log at the supervised premises whereas under the old BS detector isolation had to be logged at the RVRC.

4.6.5 Video integrity

This clause has been re-written as follows:

Camera signals between the camera and control equipment should be monitored for video loss in accordance with Table 2. If the video loss

does not automatically restore within 30 s, it should be recorded in the event log at the premises. The system should ensure that video loss is clearly indicated locally (where a monitor is fitted) by an example of "no picture" or "video loss" message.

NOTE 1 It is advisable to implement procedures and/or technologies to detect camera masking in high-security applications.

NOTE 2 In some applications a video content detection system is necessary to determine whether an expected level of information exists within the image. This protects against deliberate masking of the camera(s) field(s) of view, failure of the lens, or inappropriate or inadequate illumination.

Table 2 of the new BS provides a comprehensive set of requirements for fault recognition and indication.

The time for recording video loss, if not automatically restored, has increased from 5 seconds to 30 seconds.

There is a new requirement to record video loss in the event log at the premises. Previously video loss was reported to the RVRC.

The system must ensure that video loss is clearly indicated locally (where a monitor is fitted) by an example of "no picture" or "video loss" message.

4.6.6 Tamper security

This clause, previously called “tamper detection”, has been re-written as follows:

4.6.6.1 Means should be provided to detect and indicate the tamper conditions specified in Table 1.

4.6.6.2 Tamper indications should be audible and/or visual. Local indication at the supervised premises should be indicated to the person setting the system.

4.6.6.3 The setting/unsetting device should be provided with tamper detection in accordance with Table 1. If the device is opened, it should not be possible to affect the correct functioning nor change the state of the CCTV system.

NOTE Examples of setting/unsetting devices include keypads and digital key readers.

Table 1 of the new BS clarifies the circumstances where tamper is required to be detected and indicated.

4.6.7 Fault detection

This new sub-clause consolidates the requirements for recognizing and indicating faults.

4.6.7.1 Means should be provided to recognize and indicate the fault conditions specified in Table 2.

4.6.7.2 Fault indications can be audible and/or visual.

4.6.7.3 Except where setting and unsetting is carried out by the RVRC, means of local fault indication at the supervised premises should be indicated to the person setting and unsetting the system.

Table 2 of the new BS provides a comprehensive set of requirements for fault recognition and indication.

4.6.8 Wireless and semi-wired detectors

This sub-clause (used to be 4.2.4 in the old BS) has been simplified.

Where wireless or semi-wired detectors are used, the following functions should be provided.

a) Faults at the detector should be reported in accordance with Table 2.

b) The loss of communication between the control equipment and any detector should be notified within a period not exceeding 20 min, in accordance with Table 2.

c) Every detector should be uniquely identified to the CCTV system.

4.6.9 Control equipment integrity

The first paragraph of 4.5.7.1 of the old BS has been clarified as follows:

4.6.9.1 The control equipment should be located within the supervised premises such that access to the control equipment is restricted.

NOTE Such an area could be a security office or a store room where the area is only accessible by designated staff and/or users of the system. Equally it could be the supervised premises, which only employees have access to in working hours.

4.6.9.2 Where there is unrestricted access to the control equipment in the set condition, tamper detection should be provided in accordance with Table 1.

The following requirement has been added:

4.6.9.7 The CCTV system should monitor the media used for communication between receiver(s) and control equipment, at least every 100 s to verify its continued availability to convey signals.

NOTE For example, this would be used to detect jamming.

4.6.10 Event log at the supervised premises

The requirements for event logs have changed:

Event log(s) at the control equipment should be maintained at the supervised premises in a dated and timed retrievable format. The total capacity of the event log(s) should be at least 2 000 events. The log(s) should be protected against the accidental or deliberate deletion or alteration of the contents.

The minimum number of events has decreased from 10,000 to 2,000.

It is now a requirement to protect the log(s) against the accidental or deliberate deletion or alteration of the contents. In addition the following extra requirements must be logged:

f) overriding of prevention of setting;

g) detector isolation not carried out by the RVRC; and

h) detector omission not carried out by the RVRC.

4.6.11 Data transmission to the RVRC

The requirements for data transmission to the RVRC (previously called communication integrity) have changed:

4.6.11.1 A minimum of one data transmission path should be provided as the method of communication between the CCTV system and the RVRC.

NOTE 1 Dependent on the risk of security breach to the supervised premises, an additional transmission path might be necessary.

NOTE 2 Standards covering data transmission include BS EN 62676-1-2, BS EN 62676-2-1, BS EN 62676-2-2 and BS EN 62676-2-3.

4.6.11.2 The transmission path should have the capability to transmit data to the RVRC.

4.6.11.3 Failure of the transmission path should be reported to or detected by the RVRC within three minutes and in accordance with Table 2.

NOTE It is advisable to use a transmission path dedicated to the CCTV system for added security and reliability of transmission.

The minimum requirement is to have one data transmission path although an additional path might be necessary dependent on the risk.

It is not necessary for data transmission to comply with BS EN 62676 though some contract conditions might dictate this.

4.6.12 Retry procedure

The requirements for the retry procedure have been simplified:

A retry procedure should be put in place in case the CCTV system fails to establish a connection with the RVRC. The CCTV system should attempt to connect to the RVRC a minimum of six times within ten minutes. If after ten minutes there is still no connection, an indication should be made in accordance with Table 2.

NOTE Communications receivers at an RVRC might be identified by the telephone number which routes to them or by an IP address, for example. This is dependent on the technology in use.

An indication must be made in accordance with Table 2 if there is still no connection after ten minutes.

4.6.13 Authorization procedure

The requirements for the retry procedure have been simplified:

4.6.13.1 Prior to the transmission of data relating to the event, an authorization procedure should be performed after a connection is established between the CCTV system and the RVRC. The authorization procedure should confirm the identities at each end of the connection.

This is the equivalent of a handshake between the CCTV system equipment and the receiver at the RVRC.

4.6.13.2 If the authorization procedure cannot be completed, the CCTV system should be configured to retry the authorization procedure. The authorization and retry procedure should take no more than ten minutes to complete. If after ten minutes there is still no authorization, a fault indication should be made in accordance with Table 2.

The authorization procedure is likely to work first time or not at all, except under abnormal circumstances. However a fault indication must be made in accordance with Table 2 if authorization has not been achieved after ten minutes.

4.6.14 Power supplies

The clause on power supplies has been substantially re-worded.

4.6.14.1 General

4.6.14.1.1 The power supply should be placed in the housing of one or more CCTV components or in a separate housing.

This allows power supplies to be distributed around the system, either integrated into system components or as discrete items.

4.6.14.1.2 Power supplies should be monitored for prime power source, alternative power source, charger and output faults and identifiable to each power supply or through one common fault output identifiable to each power supply.

4.6.14.1.3 Power supply faults should be indicated locally at the supervised premises and/or at the RVRC in accordance with Table 2.

Power supply fault indications were previously listed in various clauses in the old BS whereas the requirements are now consolidated in Table 2 of the new BS.

4.6.14.1.4 Wireless components (such as wireless detectors and keypads) should be supported by a prime power source (e.g. battery) that should be capable of operating continuously under all anticipated conditions of operation up to and including the next routine maintenance.

4.6.14.1.5 Power sources for wireless components should be replaced periodically, for example at routine maintenance visits.

4.6.14.1.6 Low battery voltage should be recognized and indicated in accordance with Table 2.

4.6.14.1.7 Where the need for a UPS is identified in the Operational Requirement, fault indications should be indicated in accordance with Table 2.

Previously all systems were required to be supported by a UPS or a UPS and a generator.

4.6.14.2 Alternative power source

4.6.14.2.1 There should be an alternative power source (or sources) for equipment listed in 4.6.14.2.4 and 4.6.14.2.5 in case the prime power source fails.

NOTE It is advisable to consider supporting equipment such as cameras and illumination with an alternative power source.

4.6.14.2.2 A change-over between the prime power source and the alternative power source and back again should not create an alarm condition or otherwise influence the status of the CCTV system.

NOTE An example of an alternative power source is a battery.

This is a new requirement.

4.6.14.2.3 If a battery is used as the alternative power source, the date of installation should be recorded.

4.6.14.2.4 The alternative power source should have a capacity to support the CCTV control equipment and the devices used to transmit data to the RVRC for a minimum period of 30 min following failure of the prime power source.

The previous requirement was for a UPS providing a minimum of 4 hours support.

4.6.14.2.5 Power supplies to detectors and semi-wired detectors should be fitted with an alternative power source capable of supplying power for a minimum of 4 h.

NOTE This excludes wireless components (such as wireless detectors and keypads) which have their own prime power source.

5 INSTALLATION

5.1 Wiring, cabling and connections

There are no significant changes to the requirements.

5.2 Detectors

There are no significant changes to the requirements.

5.3 Camera equipment

There has been a change to the requirements as follows:

The installation of camera equipment should be carried out in accordance with BS IEC 62676-4:2014, 4.7 and 15.

BS IEC 62676-4:2014 supersedes BS EN 50132-7.

6 COMMISSIONING

6.1 Supervised premises documentation prior to commissioning of a CCTV system

The CCTV company should provide the following information to the RVRC at least 24 h before the CCTV system is commissioned:

a) supervised premises address;

b) CCTV company details;

c) supervised premises plan (see 9.1.2);

d) operational schedule (set/unset times, etc.);

e) response plan (see 8.3);

f) user contact details/ESP details;

g) associated intruder alarm system information [third party alarm receiving centre (ARC), supervised premises details, etc.];

h) inventory of CCTV equipment installed; and

i) fault reporting procedure (see 6.7).

This places the onus on the CCTV company to provide all the information to the RVRC prior to commissioning. Previously (see 11.1 of the old BS) the responsibility was on the RVRC to obtain the information.

6.2 Checklist

There requirement to complete a commissioning checklist is the same. However there have been some minor changes and improvements to the commissioning checklist (see Annex E of the new BS).

6.3 Engineer walk test

The basic tests are the same except the new BS clarifies they need to be carried out with the CCTV system in the "set" condition.

6.4 Reference images

The text relating to reference images has been simplified:

6.4.1 Day and night reference images of the detection areas should be reviewed by the CCTV company to ensure that they meet the system design proposal.

6.4.2 For functional cameras, reference images relating to each of the preset positions should be reviewed by the CCTV company to ensure that they meet the system design proposal.

These requirements follow BS IEC 62676-4, which requires images to be checked during commissioning to ensure they comply with the specification in the system design proposal.

The need for reference images to be stored electronically within the RVRC and accessible to the RVRC operator during live event handling for comparison purposes is now contained in 11.2 of the new BS.

6.5 Night remote check

There are no significant changes to the requirements.

6.6 Environmental soak test

There are additional requirements as follows:

The cameras should be checked on configuration to ensure that they are correctly focused both during the day and at night.

This has been moved here from clause 4.3.1.10 of the old BS.

At the end of the soak test period any performance issues should be recorded and resolved to the satisfaction of the customer, the CCTV company and the RVRC.

This is a new requirement.

6.7 Faults

There are no significant changes other than a re-positioning of responsibility in relation to the contracted party. Therefore:

6.7.1 The RVRC should notify their contracted party of any CCTV system configuration faults.

6.7.2 The contracted party should arrange for configuration faults to be corrected.

6.7.3 Corrective actions should be carried out before the CCTV system is made live.

NOTE The contracted party might be the customer, CCTV company and/or another third party.

6.8 CCTV system acceptance certificate

There are no significant changes.

6.9 Liaising with the customer upon completion of the installation and leaving the supervised premises

In 6.9.3, as-fitted documentation (rather than the system design proposal) must be completed for the customer and left at the supervised premises.

7 SETTING/UNSETTING PROCEDURES OF THE CCTV SYSTEM ON THE SUPERVISED PREMISES

7.1 General

7.1.1 The first sentence of the first paragraph has been modified to state "The CCTV system should be configured not to cause activations during the setting or unsetting procedures (see **7.2** to **7.5**) **unless otherwise agreed in writing (for example, where the monitoring of people/traffic is a requirement of observation during an agreed operational practice)**.

Clearly any activations during the setting or unsetting procedures must be for a clear purpose and agreed in writing.

7.1.2 There is a new paragraph at 7.1.2 which reads:

The integrity of communication links between the control equipment and any wireless and/or semi-wired devices used for setting and/or unsetting should be notified within a period not exceeding 20 min. When communication cannot be verified a fault signal should be generated in accordance with Table 2.

7.1.3 The next of 7.1.3 is the same as the text of 7.1.2 of the old BS.

7.1.4 There is a new paragraph at 7.1.4 which reads:

Setting of the CCTV system should be prevented when a fault condition exists. A user should be able to override the prevention of setting provided this is included in the event log at the supervised premises (see 4.6.10).

7.1.5 There is a new paragraph at 7.1.5 which reads:

If a detector is in an active state at the time of setting, an indication should be given at the place of setting and if applicable at the RVRC.

This is taken from 7.3.2 e) of the old BS and modified to include **"and if applicable at the RVRC".**

7.1.6 There is a new paragraph at 7.1.6 which reads:

Setting and unsetting devices should have the following number of differs: logical (electronic) 10 000 and mechanical (key switch) 3 000.

7.2 Setting and unsetting outside secure areas at the supervised premises

7.2 a) and 7.2 b) of the old BS have been deleted. These relate to the housing of the setting/unsetting device and tamper detection for the setting/unsetting device. 7.2 c), 7.2 d) and 7.2 e) of the old BS have been re-numbered 7.2 a), 7.2 b) and 7.2 c) in the new BS.

Tamper security is now covered in sub-clause and Table 1 of the new BS.

7.3 Setting and unsetting inside secure areas

7.3.1 Unsetting

The provisions of 7.3.1 are essentially unchanged.

7.3.2 Setting

The provisions of 7.3.2 are essentially unchanged. However 7.3.2 e) of the old BS has been moved to 7.1.5 of the new BS and modified.

7.3.2 e) of the new BS (compare with 7.3.2 f) of the old BS) calls for **the CCTV company and/or customer** (previously the owner) **to produce written procedures** to be followed detailing the actions to be taken if the setting procedure is attempted when a detector is in an active state.

7.4 Automatically timed setting and unsetting

The provisions of 7.4 are essentially unchanged.

7.5 RVRC initiated setting/unsetting

The provisions of 7.5 are essentially unchanged apart from deletion of the sentence "The RVRC should agree a validation process for this procedure with the owner".

It is self-evident that the RVRC must ensure that all requests to set or unset a CCTV system are from authorised persons, for example by means of exchanging confidential passwords or codes or other secure means. This is now covered in 11.4 of the new BS.

8 RESPONSIBILITIES AND CONSIDERATIONS

8.1 General

The provisions of 8.1 are mainly unchanged.

However **the responsibility for creating a documented agreement now rests with the CCTV company** in consultation with the customer and the RVRC.

8.1 a) includes **maintaining the artificial illumination** as well as checking the correct operation of artificial illumination.

8.1 b) refers to **fault reporting** in place of failure reporting reflecting the overall change in terminology in the new BS.

8.1 g) is re-worded to read "**expected response on notification of failure of the control equipment**".

8.2 Information regarding the supervised premises

8.2.1 This has changed so the **CCTV company** (rather than the customer) has to ensure all the information required by 6.1 is provided to the RVRC before the CCTV system is commissioned.

8.2.2 This has changed so the **CCTV company** has to ensure that if the customer proposes changes after commissioning to the layout of the supervised premises, the location of materials or parked vehicles, or changes to site operational procedures, they should be discussed with the CCTV company and the RVRC.

8.2.3 The provisions are unchanged.

8.3 Response plan

8.3.1 The provisions of 8.3.1 have been re-worded as follows:

There should be a documented agreement in the form of a response plan, **agreed between the RVRC, the CCTV company and the customer,** detailing the action to be taken by the RVRC upon receipt of an activation, **fault or a reported failure. The CCTV company should ensure that the customer receives a copy of the response plan**. This response plan should form part of the supervised premises documentation (see **6.1**).

The text in bold highlights changes.

8.3.2 The provisions of 8.3.2 are unchanged apart from the addition of an extra Note:

NOTE 2 The normal mode of operation for these CCTV systems is not to display images at an RVRC unless there has been an event at the secure area. However, if stated in the contractual terms and conditions between the customer, CCTV company and the RVRC, the RVRC operator might be permitted to view the secure area at other times. The customer might also be able to view the secure area remotely.

8.3.3 There is a new paragraph at 8.3.3 which reads:

The response plan should include details of the actions in response to individual CCTV failures of the CCTV system such as failure of the artificial illumination, video loss, detector failure, control equipment restart failure, tamper indication and transmission path failure (see 8.1).

NOTE This agreement might involve additional criteria, such as whether the customer or a user should be informed. Some failures of the CCTV system might require the RVRC operator to review images from the supervised premises. Where the customer has other contractual obligations, e.g. insurers, third-party occupiers, it is recommended that the customer makes these parties fully aware of the agreement.

8.4 Staff access

The provisions of 8.4 are essentially unchanged apart from an important change to the effect **the CCTV company has to ensure the provisions are met** rather than the owner/customer.

9 RVRC OPERATOR PROCEDURES

9.1 General

The provisions of 9.1 have been re-written (simplified) as follows:

9.1.1 The RVRC should ensure the supervised premises documentation (see 6.1) provides a clear understanding of the layout of the supervised premises and the areas to be viewed when a detector initiates an activation.

9.1.2 RVRC operators should be able to describe accurately the nature of incidents as they occur. In order to achieve this, the supervised premises plan [see 6.1c)] should show detailed information to include the detection and camera fields of view.

9.2 Activation delay procedures

9.2.1 The provisions of 9.2.1 are essentially unchanged except that **the CCTV company and/or RVRC** (rather than the RVRC) must agree activation delay procedures with the customer.

Also a new Note has been added to clarify 'delayed activation procedure' as follows:

NOTE A delayed activation procedure is where there is a delay between an event being detected and an activation occurring.

9.2.2 The provisions of 9.2.2 are essentially unchanged.

9.3 Equipment faults

The term "failures" has been changed to "faults". Apart from this the provisions of 9.3 are essentially unchanged.

9.4 Omitting detectors

The text of 9.4 has been changed to read:

The RVRC operator should authorize omissions (see 4.6.3.2). Where the RVRC authorizes the omission of a detector, it should be carried out by the RVRC operator. The RVRC should inform the CCTV company of all omissions.

NOTE 1 By agreement, some customers might wish to be informed of omissions.

NOTE 2 Where omission has been carried out by the user, it is accepted the RVRC may not be aware of the omission and therefore will not be in a position to notify the CCTV company of its occurrence.

9.5 Construction and facilities

The text of 10.1 of the old BS has been moved to 9.5 in the new BS and the wording has changed to:

As a minimum, the construction and facilities of the RVRC should conform to BS 5979:2007, Category II or BS 8591:2014, Category II.

The requirement for a Category II (attack resistant) ARC stays the same and allowance is made for the new BS 8591 standard alongside BS 5979.

10 MANAGEMENT AND OPERATION OF THE RVRC

10.1 General

Previously 10.2.1 in the old BS, the provisions have not changed.

10.2 Lost monitoring

Previously 10.2.2 in the old BS, the provisions have not changed.

10.3 Logging and recording

There are no changes apart from adding the need for the RVRC to log or record the following:

g) detector isolation (see 4.6.4.3).

10.4 RVRC support

The provisions are unchanged.

10.5 Picture quality

The provisions are unchanged.

10.6 Transmitted audio

This clause has been deleted from the new BS.

11 RVRC PROCEDURES AND DOCUMENTATION

Clause 11.1 of the old BS has been moved to 6.1 of the new BS (documentation prior to commissioning) because **the CCTV company** now has the responsibility to provide the information to the RVRC.

Consequently all the remaining clauses in 11 have been re-numbered.

11.1 Non-image records and event logs at the RVRC

The provisions are unchanged.

11.2 Storage of images received

11.2.1 The text (previously in 11.3.1) has been changed to read:

Images received at the RVRC should be stored electronically on a medium such as a hard drive. Reference images (6.4.1) should be stored electronically within the RVRC and should be accessible to the RVRC operator during live event handling for comparison purposes. For functional cameras, reference images relating to each of the preset positions (6.4.2) should be stored.

The requirement for the RVRC to store reference images is made clear.

11.2.2 The provisions are unchanged.

11.2.3 The provisions are unchanged.

11.3 Images for evidential purposes

The text has changed to:

Where data and/or images are stored digitally and might be required as evidence for a crime, then this should be in accordance with BS IEC 62676-4:2014, Clause 11.

NOTE See BS 10008 for evidential weight and legal admissibility of electronic information.

The main change is from BS 8495 to BS IEC 62676-4:2014, Clause 11 due to the withdrawal of BS 8495. The importance of adhering to clause 11 of BS IEC 62676-4:2014 is to help enhance the evidential weight and legal admissibility of the information.

11.4 Confidentiality

This is a new clause on confidentiality as follows:

Procedures should be established to authenticate the exchange of confidential information between the RVRC and the customer. Details should be agreed with the CCTV company and the customer.

NOTE 1 Authentication can be achieved by use of passwords or codes.

NOTE 2 Examples of confidential information include changes to setting/unsetting times, requests to the RVRC to set or unset, the cancelling of activations, and names and addresses of users.

11.5 RVRC operator actions

The provisions are unchanged.

11.6 Image quality check

The provisions are unchanged.

11.7 Critical data omissions

The provisions are unchanged.

12 ACTIVATION MANAGEMENT

12.1 Classification of activations

The provisions are unchanged.

12.2 Multiple unwanted activations

The provisions are unchanged.

13 SERVICE LEVELS

13.1 General

The text has been changed to read:

The RVRC should conform to BS 5979 or BS 8591.

This recognises the new BS 8591 standard alongside BS 5979.

13.2 Activation response time

The provisions are unchanged.

13.3 CCTV system fault reporting

The provisions are unchanged.

13.4 Incident reporting

The provisions are unchanged.

14 GENERAL MAINTENANCE AND PERSONNEL SCREENING

14.1 CCTV system maintenance

14.1.1 Maintenance agreement and routine visits

14.1.1.1 The text has been changed to read:

Maintenance should be carried out at agreed intervals, which should be not less than twice annually.

There is no change to the frequency of routine (preventative) maintenance.

14.1.1.2 The text has been changed to read:

Documented criteria for the corrective and preventative maintenance of the CCTV system should be agreed between the customer and CCTV company.

NOTE Examples of maintenance can be found in BS IEC 62676-4:2014, Clause 17.

The main change is for the agreement to be between the customer and the CCTV company, rather than the maintenance engineer, which is logical.

14.1.1.3 The text has been changed to read:

Preventative maintenance should be scheduled to take place once during the sixth calendar month following the first month in which the CCTV system acceptance certificate is issued and at six monthly intervals thereafter. Preventative maintenance visits that occur during the month before or month after the scheduled month should not affect the preventative maintenance schedule.

The revised text is a simplification of the text in the old BS and, in addition, 14.1.1.4 and 14.1.1.5 of the old BS have been deleted. There is no change to the overall requirements.

14.1.2 CCTV company maintenance engineer actions

14.1.2.1 This is a new sub-clause as follows:

The maintenance engineer should inform the RVRC that maintenance/repair is due to take place.

This is adapted from 14.1.3.1 of the old BS where it was stated maintenance visits should be carried out in conjunction with the maintenance engineer.

14.1.2.2 Previously 14.1.2.1 in the old BS, the revised text is as follows:

At each visit to the supervised premises, the maintenance engineer should consider whether any of the environmental factors (see B.4) have changed to adversely affect the operation of the CCTV system. If this is discovered to be the case, remedial action should be documented and agreed with the customer.

The difference is that the remedial action must be documented and agreed with the customer.

14.1.2.3 Previously 14.1.2.2 in the old BS, the revised text is as follows:

As part of the preventative maintenance visit, the engineer should carry out a check of the night images (see 10.5).

There is now no requirement to carry out a remote maintenance check at night. Instead the engineer must check the night images to make sure the picture quality is at least sufficient to enable an RVRC operator to determine the nature and detail of a viewed event.

14.1.2.4 Previously 14.1.2.3 in the old BS, the revised text is as follows:

When changes to the CCTV system and configuration of transmission equipment are required, the RVRC should be informed of the changes that affect the monitoring response and, those parts affected, tested through to the RVRC in accordance with 14.1.3.1.

The main change is to focus on aspects affecting the RVRC monitoring response and testing the affected parts of the CCTV system through to the RVRC to make sure all is in order.

14.1.2.5 Previously 14.1.2.4 in the old BS, the provisions have not changed.

14.1.2.6 This is a new requirement for the CCTV maintenance company:

The image of each detection area should be compared with the relevant stored reference images by the CCTV company in conjunction with the RVRC at each maintenance visit. If necessary new reference image(s) should be created and stored at the RVRC, e.g. in the event of a camera repair or replacement.

14.1.3 RVRC maintenance actions

14.1.3.1 The provisions are essentially unchanged apart from the need for the RVRC to check repairs in conjunction with the CCTV company.

14.1.3.2 The provisions are essentially unchanged.

14.2 Personnel screening

The provisions are unchanged.

ANNEX A (INFORMATIVE)

Diagrams for positioning detectors

The provisions are unchanged.

ANNEX B (INFORMATIVE)

Factors affecting the design requirements for a detector-activated CCTV system

The provisions are unchanged.

ANNEX C (INFORMATIVE)

Types of technology used in detection equipment

The provisions are essentially unchanged.

ANNEX D (INFORMATIVE)

Illumination of the field of view of the camera

The provisions are unchanged.

ANNEX E (NORMATIVE)

Checklist criteria for the commissioning of a detector-activated CCTV system

The provisions are essentially unchanged.

ANNEX F (INFORMATIVE)

Setting procedure with a detector in the active state

The provisions are unchanged.

BIBLIOGRAPHY

The bibliography now includes references to the BS EN 62676 series for video surveillance systems for use in security applications, Protection of Freedoms Act 2012 and the Home Office Surveillance Camera Code of Practice 2013.