

Q Hub® BS8418 compliancy document

| Item | Description | Compliance Met in full | Comments/Implementation |
|--------------|---|---------------------------|--|
| 4 | CCTV System Design & Installation | | |
| 4.2.1 | General (cameras) | | |
| | f) PTZ cameras should be considered as multi -position fixed cameras by the utilisation of presets. | ✓ | |
| | i) All cameras should be uniquely identified using a name/label displayed with or within the camera view at the RVRC corresponding to name/label on site plan for that camera | ✓ | |
| 4.3 | Audio Challenge | | |
| | An audio challenge facility is recommended except where it may reduce the effectiveness of the system or generate noise pollution | ✓ | |
| 4.4.1 | Minimum Performance Requirements | | |
| | As a minimum, activation should initiate within 1 s of an event being detected, except where delayed procedures exist (entry/exit path) | ✓ | |
| 4.4.2 | Video Transmission Requirements | | |
| | The transmission system should send continuous video images while the RVRC operator is evaluating images | ✓ | |
| 4.4.3 | General (CCTV Performance & Integrity) | | |
| | Facilities might exist to omit any detector either by RVRC operator or automatically where there is a legitimate need do so i.e faulty detector, or repeating operation due to wind movement etc... | * | currently scheduled second release |
| | A 'log' entry at the RVRC must detail such action showing detector ID, time/date of omission and either duration or time to restore | * | currently scheduled second release |
| 4.4.4 | Video Integrity | | |
| | Cameras should be monitored for signal loss | ✓ | |
| | In some cases video masking detection is also required. Loss or masking should be immediately indicated to RVRC | | currently scheduled second release |
| 4.4.5 | Tamper | | |
| | All detector cabling should include tamper detect with: | | |
| | a) continuous tamper detection circuits | ✓* | *Inputs 1-4, and PIRs, have tamper detect. |
| | b) Tamper faults reported immediately to the RVRC when the system is 'set' | | |

| Item | Description | Compliance | Comments/Implementation |
|--------------|--|-------------|-------------------------|
| | | Met in full | |
| 4.4.6 | CCTV Control Equipment Integrity | | |
| | Control equipment protected by secure validation process to ensure no unauthorised access e.g password, or electronic key to avoid unauthorised access to the CCTV system | ✓ | |
| | The set/unset state should be determinable by the RVRC and the system parameters should be remotely programmable by the RVRC | ✓ | |
| | <i>NOTE: (Remote diagnostics and correction are highly desirable)</i> | | |
| | If the system fails the monitoring & control equipment should auto restart | | |
| | Failure to restart should be communicated as follows: | | |
| | a) To the RVRC if system is set in the 'set' condition to the RVRC | | |
| | b) To the RVRC & or locally if the system is unset in the unset condition locally and/or to the RVRC | | |
| | c) When a CCTV failure is communicated, the system should send a restart signal to the RVRC if the CCTV system automatically restarts at anytime. | | |
| 4.4.7 | Event Logs On Site | | |
| | An ongoing event log should be maintained on site in a consolidated, date/timed retrievable format for a minimum of 6 months, or until next maintenance (whichever is longer): Log should contain: | ✓ | |
| | a) Changes in the CCTV system status e.g. set, unset etc; | ✓ | Included in event log |
| | b) Tampering and/or operation of detectors resulting in incident or alert, initiating an entry sequence; | | as above |
| | c) unsuccessful attempts to communicate with the RVRC; | ✓ | Included in event log |
| | d) successful communication with the RVRC and confirmation of alarm reported; | ✓ | |
| | e) CCTV System exceptions such as restart after a mains supply failure, low battery and power failure; | ✓ | |
| 4.4.8 | Communication Integrity | ✓ | |
| | An alternative communication channel to the RVRC such as GSM or additional monitored telephone line should be provided to indicate primary transmission line failure to RVRC | ✓ | |
| 4.4.9 | Retry Procedure | ✓ | |
| | | | |
| | | | |
| | | | |

| Item | Description | Compliance Met in full | Comments/Implementation |
|---|---|---------------------------|---|
| 4.4.10 | Connection procedure | ✓ | |
| | An authentication process should be performed after connection but before data transfer to confirm identity and access level of the system at each end. If authentication fails the connection should be terminated and retried. There should be 9 retries to connect and authenticate. After this the alternative connection option, the procedure should take no more than 10 minutes to complete (see 4.4.9) | ✓ | There is an authentication "handshake" between Qhub and CSS |
| 4.4.11 | Power Supplies | | |
| | Power failure to the control system should be indicated to the RVRC. Use of a UPS should be considered. | ✓ | |
| 5 Commissioning | | | |
| 5.3 Reference Images | | | |
| | reference images should be captured for comparison during live operation checks | | May be added in later releases |
| 6 Site Operational procedures | | | |
| 6.1.1 General | | | |
| | The system should not cause activations during the setting or unsetting procedure when carried out in accordance with 6.1.2, 6.1.3, 6.1.4, 6.1.5 | | |
| 6.1.2 Local setting/unsetting inside secure area | | | |
| | a) <i>unsetting</i> | | |
| | 2) Activation should not occur in the defined entry route during this unsetting procedure | ✓ | |
| | 3) Additional detectors not on the entry route may be rendered inactive for the duration of the unsetting procedure | ✓ | |
| | 4) There should be a time limit for the unsetting which when exceeded should initiate an activation | ✓ | |
| | 5) detection of an event not on the entry route without prior initiation of the unsetting procedure, should initiate activation. | ✓ | |
| | b) <i>Setting</i> | | |
| | 2) detectors in the defined exit route should be disabled during setting | ✓ | |
| | 3) Setting should be completed by: | | |
| | i) manual user action (the preferred action) | ✓ | |
| | ii) timer expiring | ✓ | |

| Item | Description | Compliance Met in full | Comments/Implementation |
|--------------|---|---------------------------|---|
| 6.1.4 | Automatic timed setting and unsetting | | |
| | There should be an onsite indication of the current set state | ✓ | |
| 6.1.5 | RVRC driven setting/unsetting | | |
| | RVRC setting/unsetting of a system should be actioned as a result of a request to the RVRC and should not be part of a standard routine. Any such action should be logged at the RVRC | ✓ | |
| 8 | RVRC Operator Procedures | | |
| 8.1 | General | | |
| | Stored images on the intended field of views on all cameras on the system and site plans should be readily available to the operator to provide evidence of a camera being moved by an intruder. | ✓ | |
| 8.2 | Entry/Exit and other delayed procedures | | |
| | Where procedures involve a delay between event detection & responding activation, the RVRC operator should have direct access to at a single image or preferably a sequence of images from the point of detection and prior to activation | ✓ | |
| 8.3 | Equipment failure | | |
| | In the event of loss of monitoring facilities at the RVRC, data from the affected systems should be routed to another RVRC. If this is not achieved in 15h then the system should be monitored locally at the site | ✓ | The Qhub currently supports the idea of a backup CS |
| 9 | RVRC Specifications | | |
| 9.2 | Logging & recording | | |
| | The following should be logged or recorded at the RVRC: | | |
| | a) date/time of all activations | ✓ | |
| | b) transmitted images | ✓ | |
| | c) transmitted audio | | |
| 10 | RVRC Procedures | | |
| 10.2 | Non-image Records & Event Logs at the RVRC | | |
| | Records & logs should be kept for a minimum of 6 months and should include: | ✓ | |
| | a) date and time of any communication from a site | ✓ | |
| | b) time/date and identity of an operator making use of an RVRC workstation | ✓ | |
| | d) time at which an RVRC operator closes a session with any explanatory codes | ✓ | |

| Item | Description | Compliance Met in full | Comments/Implementation |
|--|---|---------------------------|--|
| | f) any system failures or exceptions within the receiving equipment or workstations | ✓ | |
| | h) time at which an RVRC operator starts and closes routine site patrol | ✓ | |
| 10.3 Storage of Images Received | | | |
| | All images received at the RVRC should be stored on a suitable medium (video tape, CDR) Procedure should exist for indexing and accessing particular incidents | ✓ | |
| | Retention should be determined by the owner in line with the the Data Protection Act. | ✓ | Clean-up background task on CS server removes images older than N days |
| 10.4 Images for evidential Purposes | | | |
| | All images should be audit trailed to ensure integrity and continuity of the recording at all times such that the images can be used for evidential purposes. Conformance to PD0008 may be required | | Need to define unique serial number setting procedures |
| 11 Activation Management | | | |
| 11.1 Classification of Activations | | | |
| | A method of classifying activations should be adopted by the RVRC | ✓ | |
| | As a minimum this should distinguish between alerts and incidents | ✓ | |
| | In addition activity per detector/camera combination should be recorded and classified according to cause to assist in management of faults/deficiencies of the sytem. | ✓ | |