**Appendix Two – Video Management System**

A minimum of two operator positions shall be required. Operators must also be able to review recorded images at their work station. Facility must also be given for a review station for the purposes of reviewing recorded images away from the CCTV Control Room’s two stations, though this can be potentially utilised as a third operator position if the service expands. Recording equipment must be able to record all cameras (at the defined bit / frame rate) with a 31 day retention period, with automatic over-writing after the 31 day period (excepting for those recordings / images saved to the evidence locker). The whole system must be flexible and expandable.

Maps are a key part of assessing a situation and getting to video quickly. The system must enable operators to manage both video and alarms from the map, and allow to Import map backgrounds in different formats, including bitmaps, JPEG images and AutoCAD drawings

To ensure maximum and efficient system use, there should not be reliance on operator knowledge of camera names and locations, but provisioned ability to click on a target point and all relevant cameras will be displayed. There should be real-time alarm source tracking enabling operators to visually see threats moving through the map as they happen

To enable fastest selection of cameras from a map the ability to “rubber band” a selection will auto display the several selected group cameras onto a monitor from the selected area. Also pursuit mode can be used to follow from one area to the next to track an event using maps and alarms.

PTZ cameras will have vectors which by clicking on an area will send the associated PTZ to a preset position and auto display on a monitor.

The location of an alarm source must be able to be easily identified, so operators can assess a situation and respond quickly. Alarms shall be easily assigned and acknowledged from a map, and associated video able to be displayed.

To enable Torbay Council to provide a flexible monitoring facility for different areas within the Council, as well as external Boroughs / client groups, an additional requirement is the facility for the display and control of third party security components from a map within Control System to provide additional and diverse integration. For example, the ability to unlock a door, or to flash an icon on a map if an access control / lift / smoke alarm etc. is raised.

With regards to peripheral interfacing, the system must fully support the Integration, monitoring and management of alarms from multiple sources, as noted above, from anywhere on the network, be able to:

* Distribute and escalate alarms ensuring incidents are handled correctly and efficiently. Automate response to events and alarms using flexible and configurable actions.
* Combine inputs from many different sources within alarm zones to reduce the volume of alarms handled by operators and maximise efficiency / flexibility.

A central requirement is that the adopted solution includes clearly defined and stated manufacturer support for a minimum 10 years, is fully ONVIF certified, and the manufacturer commits to (where applicable / appropriate, and subject to relevant NDAs etc.) SDK sharing and co-working with the Torbay Council adopted control system to enable a level of interfacing that would provide the ability for co-monitoring / system control (at Torbay Council) of third party systems (external clients)

To ensure the adopted solution fulfils the needs and requirements of Torbay Council, the following are required technical specification parameters relating to software / hardware for the system architecture as described above.

The system is not to use a central server for processing video or managing it and shall use a distributed network architecture model for maximum data management efficiencies to avoid data bottlenecks and subsequent latency.

For network security, the system is to support a Cybervigilant integrated solution to enable the future use of network monitoring to detect hacking. This can be added to the system at any time in the future.

The system is to support activity frame rate control (ACF) where camera streams can be dynamically managed to reduce bandwidth depending upon the scene activity and reduce transmission and NVR storage.

**Downloads of Recordings**

Torbay Council expect to be able to use a bespoke suite of software provided to them and installed by the supplier/contractor to enable connection to recorders over the existing IP system, and download video in a CAST compliant manner so that a Police Officer / Court / enforcement agency can take the resultant download and play it, rewind it, fast forward it etc.  Any download should include playback software either on the media Torbay Council copy it to (e.g., DVD-R, HDD, Flash Drive etc.), that will play on a Council or Police PC without Admin rights, **OR** should do all of these functions using commercially available software such as VLC.

**VIDEO MANAGEMENT SYSTEM**

*SOFTWARE*

* The software shall be run on any PC based on Microsoft Windows (Windows 10 ® 64-bit, Windows 8.1 ® 64-bit, Windows 8 ® 64-bit, Windows 7 ® 64-bit)
* The software shall consist of a single client application.
* The client software shall not be dependent on, nor require any connection to, a central management or configuration server.
* The client software shall be installable without any need for software or hardware license.
* The client software shall be ONVIF compliant and provide support for ONVIF compliant cameras.

*LIVE VIDEO*

Live Video on Workstation Screens

1. The Video Management System shall show live video from IP Cameras and Video Transmitters in MPEG4 and H.264 formats.
2. The Video Management System shall support cameras with resolutions ranging from Standard Definition, High Definition (HD) and up to 20 Megapixel.
3. The Video Management System shall show video across 4 displays per workstation - each display can have up to 25 viewing panes.
4. The Video Management System shall allow configuration of the video and audio transport types (TCP, UDP, Multicast) for each user.
5. The Video Management System shall allow configuration of the video and audio stream settings for each user, depending on the support hardware.

6. Users shall be able to change the video pane layout in each of the 4 screens independently:

a. Grid layouts: 1x1, 2x2, 3x3, 4x4, 5x5

b. Widescreen layouts: 2x3, 3x4, 4x6

c. Hotspot layouts based on 3x3, 4x3, 4x4, 5x5 larger pane in top, left

d. Hotspot layouts based on 4x3, 4x4, 5x5 larger panes in center.

7. Users shall be able to change the aspect ratio in each of the 4 video windows independently in order to display Standard Definition or High Definition video. Choose between:

a. Widescreen (16:9)

b. Standard (4:3)

8. Users shall be able view video at the correct aspect ratio or optionally stretch video to fit the available space, regardless of original aspect ratio.

9. Users shall be able to move any image from one display screen to another via drag-and-drop.

10. The Video Management System shall allow the overlay of time and date information on live video panes, either on all panes, or selected pane only.

11. The Video Management System shall allow users to view live video and review recorded video at the same time.

12. Users shall be able to digitally zoom up to 1000% and also digitally scroll live video from any camera using the mouse wheel.

13. Users shall be able to save the current zoom/scroll position as a camera view (virtual preset).

14. Users shall be able to display any camera view (virtual preset).

15. Administrators shall be able to configure hidden zones on fixed cameras.

16. The Video Management System shall allow users to reveal the hidden zone in live video if the user has the appropriate permission.

17. The Video Management System shall allow the removal of interlacing artifacts from 4SIF video using the following criteria:

a. Best performance

b. Best image quality

c. Smoothest rendering

18. The Video Management System shall allow the display objects detected via analytics on the video (up to 10 at once).

19. The Video Management System shall allow the display of analytics levels on video.

20. Users shall be able to take a snapshot of one image or all images currently displayed and save as a bitmap or JPEG image to a configurable location. This should include zoomed images.

21. Users shall be able to print a snapshot of an image displayed in a video pane direct on a printer (color or grayscale, depending on printer).

22. Users shall be able to replay currently viewed live video by a single mouse click for replays from 10, 15 or 30 seconds before current time or from alarm time.

23. Users shall be able to run a 3rd party "applet" from live video mode. The applet shall be passed the IP Address of camera in selected video pane as well as its name and the current user type. Up to 4 different applets shall be supported.

24. Users shall be able to configure the size for text and icons displayed on video panes. Text and icons can be fixed size or adjust automatically when video pane size changes.

25. Users shall be able to view stream statistics on all current video streams, including the following information:

a. Frame rate

b. Resolution (SIF, 2SIF, 4SIF,720p, 1080p, 4MP, 12MP, 20MP )

c. Current bit-rate

d. Audio bit-rate

26. In the event of the video connection failing, the Video Management System shall display a clear error message with the option to also display the last video frame received.

*Event Counting*

1. The Video Management System shall allow users to view a count of analytics events on the video pane while video is being displayed.

2. The Video Management System shall allow users to reset the event count for a camera.

*Live Video on Analog Monitors*

1. The Video Management System shall be able to display camera information in the On Screen Display (OSD) of an analog monitor

a. Camera name

b. Date and time

2. The Video Management System shall be able to record video to analog VCRs (via decoders.)

3. The Video Management System shall support point to point connections between encoders and decoders for the following data:

a. Video (SD only)

b. Audio transmit and receive

c. Serial

4. Users shall be able to specify whether a receiver is connected to an analog monitor or VCR.

*Audio in Live Video*

1. Users shall be able to listen to audio from multiple cameras through PC speakers.
2. Users shall be able to speak to one or more cameras through a PC microphone.
3. Users shall be able to listen to audio from a camera through an analog monitor’s speakers.
4. Users shall be able to speak to a camera displayed on an analog monitor through a microphone connected to a decoder.
5. Users shall be able to mute a client speaker.
6. The Video Management System shall have an option to allow or prevent simultaneous listen and speak (full duplex audio). If full duplex audio is off, the direction of audio will be switched automatically when the user listens or speaks.
7. Users shall be able to listen to audio streams that do not have associated video.

8. The Video Management System shall support the following for cameras through the ONVIF interface or Camera Gateway

a. Live audio through PC speakers\*

*Broadcast Audio\**

*\*For possible future adoption / utilisation of audio by TBC – system must have capability.*

1. Users shall be able to manually broadcast live audio from the user’s microphone to multiple remote speaker sets forming a PA group.
2. Users shall be able to play a pre-recorded message to a remote speaker or PA group.
3. Users shall be able to schedule the broadcast of pre-recorded messages to a remote speaker or PA group.

*PTZ Control*

1. All PTZ control shall be user-restricted (see users section).
2. Users shall be able to configure named preset positions with optional "tool tip" text.
3. Users shall be able to configure named custom commands with optional "tool tip" text. Commands can be per PTZ type or per camera, as required.
4. Users shall be able to copy custom PTZ commands from one camera to another.\*
5. Users shall be able to simultaneously pan and tilt a PTZ camera displayed in a video pane in any direction and at varying speed by moving the PC mouse on the video pane.
6. Users shall be able to zoom a PTZ camera in or out using the PC mouse.
7. Users shall be able to simultaneously pan, tilt AND zoom a PTZ camera displayed in a video pane or monitor using a joy stick on one of the supported CCTV keyboards.

8. Users shall be able to adjust the focus of a PTZ camera using the on screen PTZ controls or a CCTV keyboard:

a. Focus near

b. Focus far

c. Auto-focus\*

1. Users shall be able to adjust the iris of a PTZ camera using the on screen PTZ controls or a CCTV keyboard:-Open iris-Close-Auto-iris.\*
2. Users shall be able to move a PTZ camera to a preset position using the on screen PTZ controls or a CCTV keyboard.\*

11. Users shall be able to perform a custom command on a PTZ camera using the on screen PTZ controls (e.g. operate wipers.)\*

12. Users shall be able to enter the menu on a PTZ camera using the on screen PTZ controls or a CCTV keyboard (menu options navigated using pan and tilt.)\*

13. The Video Management System shall automatically drop the connection to a PTZ camera if not moved for 5 seconds to allow other users to control it.\*

14. Users shall be able to hold onto connections to PTZ cameras to prevent other users taking control if not moved (overrides the 5 second timeout.)\*\*

15. Users shall be able to take control of a PTZ camera if user has a higher priority than the user currently moving it (overrides PTZ hold.)\*\*

16. Inform user when can't take control of a PTZ camera because another user with a higher priority is controlling it.\*\*

17. Users shall be able to show or hide the on screen PTZ controls.

18. The Video Management System shall support the following for cameras using the ONVIF interface or Camera Gateway

a. Pan, tilt and zoom control with mouse and joystick

b. Go to preset

c. Set preset

*IP VIDEO WALL*

1. An IP video wall shall be able to be constructed using secondary workstations, each of which manages up to 4 monitors. The video wall shall be controllable over an IP network and have an unlimited number of primary workstations.
2. The video wall shall have the ability to be managed from primary workstations through a standard CCTV keyboard. The system shall support multiple primary and up to 98 secondary workstations giving a maximum video wall size of 9800 video panes.

C. Monitors within the video wall shall be able to display:

1. live video

2. guard tours

3. salvos

4. site maps

5. alarm status.

D. It shall be possible to constrict the video wall using any PC monitors e.g. CRT, Plasma, LCD, HD TV.

E. The IP Video Wall shall be fully scalable to meet any control room requirement. It shall be possible to add more slaves with monitors as needed up the limit of 98.

F. The IP Video Wall shall support unlimited master workstations.

G. The IP Video Wall shall support standard and High Definition widescreen video.

H. The IP Video Wall shall be controlled using standard CCTV keyboards.

1. The IP Video Wall shall be able to display site maps and alarm status.

J. The IP Video Wall shall support black-screen-monitoring features. See section 2.08B.

K. The IP Video Wall shall be able to dynamically change the video layout of a monitor.

*VIRTUAL MATRIX*

1. The Video Management System shall allow users to easily drag icons representing cameras, sequences, salvos and guard tours onto PC viewing panes and onto analog monitors.

B. Sequences

1. Users shall be able to configure sequences of cameras, camera views and or presets (PTZ cameras); each camera can have a separate dwell time (1 to 300 seconds).

2. Users shall be able to reorder the cameras within a sequence.

3. Users shall be able to run multiple sequences in video panes.

4. Users shall be able to run sequences on analog monitors.

5. Users shall be able to pause (hold) a sequence.

6. Users shall be able to display the next or previous camera in the sequence.

C. Salvos

1. Users shall be able to configure salvos containing cameras, camera views and or presets (PTZ cameras). Each salvo can optionally have an associated video pane layout.

2. Users shall be able to reorder the cameras within a salvo.

3. Users shall be able to display a salvo across a set of video panes within in any of the video windows (changes layout automatically if configured to do so).

4. Users shall be able to display a salvo across a set of monitors.

5. Users shall be able to view all cameras in a site as a salvo.

6. Users shall be able to view all cameras from a map as a salvo.

D. Guard Tours

1. Users shall be able to configure guard tours containing salvos – each salvo can have a separate dwell time (1 to 300 seconds.)

2. Users shall be able to reorder the salvos within a guard tour.

3. Users shall be able to run a guard tour in a set of video panes within a video window (one per window.)

4. Users shall be able to run a guard tour in a set of analog monitors.

E. Tasks

1. Users shall be able to configure scheduled tasks for users that display video (sequences, salvos, and guard tours) either automatically when the user logs in or on a daily time schedule.

2. Users shall be able to run scheduled tasks for the user while that user is logged in.

3. Users shall be able to disable or enable scheduled tasks on a PC.

F. Matrix Numbering

1. The Video Management System shall automatically allocate logical numbers to cameras, salvos, sequences, and guard tours so that they can be started by number using a CCTV keyboard.

2. The Video Management System shall allow the following options for configuring matrix numbers:

a. Display matrix numbers on user interface

b. Number of digits in numbering scheme (1-7)

c. Whether to put PC panes in the virtual matrix or otherwise

3. Users shall be able to manually renumber cameras, salvos, sequences, guard tours.

4. It shall be possible to allocate a matrix number to cameras, monitors, sequences, salvos, guard tours in the range 1 to 9,999,999.

*CCTV KEYBOARDS*

A. The Video Management System shall support a choice of analog surveillance keyboards to be connected to any user’s PC.

1. American Dynamics ADCC1100

2. American Dynamics (Sensormatic) AD2088

3. Proprietary (manufacturer’s own) Surveillance Keyboard

4. Pelco KBD300A

5. Pelco 9760 (PTZ control only)

6. Panasonic keyboard WV-CU650

1. The CCTV keyboard shall be connectable to any available PC COM port.
2. The CCTV keyboard shall allow users to control PTZ Cameras using a joystick.

D. Using the CCTV keyboard, users shall be able to make any PTZ camera go to a preset position.

E. Using the CCTV keyboard, users shall be able to start and stop video on video panes or external monitors by camera number and monitor number.

F. Using the CCTV keyboard, users shall be able to start and stop sequences on video panes or external monitors by sequence number and monitor number.

G. Using the CCTV keyboard, users shall be able to hold a sequence.

H. Using the CCTV keyboard, users shall be able to view the next/previous camera in sequence.

1. Using the CCTV keyboard, users shall be able to start salvos on video panes or external monitors by salvo number and monitor number.

J. Using the CCTV keyboard, users shall be able to start and stop guard tours on video panes or external monitors by tour number and monitor number.

K. Using the CCTV keyboard, users shall be able to change the video pane layout.

L. Using the CCTV keyboard, users shall be able to close error message popup windows within the Video Management System.

M. Using the CCTV keyboard, where the keyboard supports it, users shall be able control playback of recorded video, including the following functionality:

1. Switch between live and playback

2. Scroll forward and back along the timeline

3. Zoom in and out on the timeline

4. Set playback position

5. Play and pause footage

6. Synchronise playback

7. Control playback speed from the jog shuttle

8. Replay the last 10 seconds of footage

9. Return to live streaming (if replaying in live)

N. Using the CCTV keyboard, users shall be able to view the camera with the next or previous matrix number.

*VIDEO REVIEW*

A. Timeline and Calendar

1. Users shall be able to view the recorded video footage for a camera along a timeline. They shall be able to expand and contract the timeline to show a larger or smaller time range and to scroll the timeline backwards and forwards to show different time periods.

2. Users shall be able to use the mouse wheel to both scroll and expand/contract the timeline.

3. For a camera, users shall be able to see summary information about how much recording footage is available from which NVR.

4. Users shall be able to change the playback NVR associated with a camera.

5. The Video Management System shall provide one-button click controls to go to the beginning or the end of available recording footage.

6. The Video Management System shall provide a calendar control to allow navigation to any year / month /day in the recording library.

7. The Video Management System shall provide a go to “today” control for getting current recording footage.

8. The Video Management System shall provide a go to “hour / minute / second” control.

9. The Video Management System shall display alarms related to the selected camera along the timeline including summary counts of the number of alarms in each time period.

10. The Video Management System shall display video bookmarks along the timeline. Bookmarks can either be those from a selected camera or from current bookmark query as displayed in the bookmark list.

B. Playback on PC Screen

1. The Video Management System shall play back video recorded in MPEG4 and H.264 formats.

2. The Video Management System shall replay footage in same video pane, or navigate to recorded video panes.

3. The Video Management System shall play back video from up to 25 cameras at once in a single video window.

4. The Video Management System shall play back each camera separately or synchronize to playback from the same time.

5. The Video Management System shall play back synchronized recorded audio in each video pane.

6. The Video Management System shall display time and date information on recorded video panes, either on all video panes, or on the selected pane only. This should be able to be set independently of the settings for live video panes.

7. The Video Management System shall play back video using the following standard VCR operations:

a. Play-pause-fast forward at different speeds (x1/4, x1/2, x2, x4, x8, x16)

b. Rewind at different speeds (x1/4, x1/2, x2, x4, x8, x16)

c. Single frame forward-single frame back

8. The Video Management System shall provide a jog shuttle speed control for fast forward and rewind.

9. Users shall be able to move playback to a different time either using the timeline or entering a specific date and time.

10. Users shall be able to move playback to the time of the next alarm, bookmark or motion over threshold.

11. Users shall be able to move playback to the time of the previous alarm, bookmark or motion over threshold.

12. Users shall be able to digitally zoom up to 800% and scroll replayed video.

13. Users shall be able to reveal the hidden zone in recorded video if user has the appropriate permission.

14. Users shall be able to remove interlacing artifacts from 4SIF video.

15. Users shall be able to display analytics levels on video.

16. Users shall be able to take a snapshot of one image or all images currently displayed and save as a bitmap or JPEG image to a configurable location. This should include zoomed images.

17. Users shall be able to print a snapshot of an image displayed in a video pane direct to a printer (color or grayscale, depending on printer.)

C. Motion Search

1. Users shall be able to find motion in recorded footage from a selected time and display a motion profile on the timeline.

2. Users shall be able to adjust the motion threshold used for thumbnails and for moving playback to next/previous motion.

3. Users shall be able to configure a region of interest for motion search.

4. The Video Management System shall support the following options for motion search:

a. General motion search – for motion in any direction

b. Directional motion search - for objects moving in a particular direction

c. Museum mode search – for objects being removed from a scene

d. Object size.

5. It shall be possible to combine motion search modes to further refine the search.

6. Users shall be able to adjust the speed and granularity of the motion search.

D. Audio Search

1. Users shall be able to search for sounds in recorded footage from a selected time and display an audio level profile on the timeline.

2. Users shall be able to adjust the audio threshold used for thumbnails and for moving playback to next/previous sound.

E. Thumbnails

1. The Video Management System shall be able to display thumbnail images taken from the video footage in the current time line period. Thumbnails can be displayed by:

a. Time: At equal intervals across the timeline period depending on the number of thumbnails set for the user.

b. Alarms: One image for each alarm in the period.

c. Bookmark: One image for each bookmark in the period

d. Motion: One image for each time motion goes above a configurable threshold

e. Audio: One image for each time the audio goes above a configurable threshold

2. Users shall be able to play back a recording from a selected thumbnail.

F. Bookmarks

1. Users shall be able to add a bookmark to a recording for a camera at a specified time.

2. Users shall be able to find bookmarks by:

a. Site name

b. Camera name

c. Time range

d. A text string within the bookmark

3. Users shall be able to produce reports of bookmarks and export to RTF or CSV formats.

4. Users shall be able to delete one or more bookmarks (if created by the same user)

5. Users shall be able to delete bookmarks created by any user.

6. The Video Management System shall ensure that bookmarks are held alongside recordings on the NVR, not on a user’s PC.

7. Users shall be able to view recorded video associated with a bookmark.

8. It shall be possible for text information to be automatically fed into the IP Video System as Bookmarks via an SDK.

9. The Video Management System shall ensure that the text information is displayed in a scrolling bookmark comments window beside the playback window.

10. Detailed search options shall allow for filtering of bookmarks e.g. by time, by user.

11. Within the bookmark comments window the highlighted bookmark shall correspond to the current playback position.

12. Next and previous incident buttons shall automatically scroll the bookmark comments window keeping the highlighted text and associated video in synch.

13. In a live view pane, users shall be able to add a bookmark to the recording of that camera.

14. Users shall be able to view bookmarks as a transparent overlay on a live pane.

15. The Video Management System shall support permissions for bookmarks so that only those users with the appropriate security level can view bookmarks created by users at the same level as them or below.

G. Incident Export

1. Users shall be able to export video clips from a selected camera or cameras within a site to a named incident.

2. Time to export shall be no more than 30 seconds per hour of video recorded.

3. Users shall be able to queue video exports to be performed as a background process.

4. The Video Management System shall show progress and estimated time to completion in an export status window.

5. Users shall be able to add additional clips to existing incidents.

6. The Video Management System shall automatically digitally sign video clips on export.

7. Users shall be able to protect the original recordings to preserve the evidence.

8. Users shall be able to review incidents in a standalone incident player application, directly from CD/DVD.

9. Users shall be able to play back incidents with all the playback operations provided by the full Video Management System application.

10. Users shall be able to check and authenticate digital watermarks embedded within exported clips.

11. The Incident Player application shall be able to be run at the same time as the main Video Management System application so that users can easily verify the success of an export.

12. The Video Management System shall support the following ONVIF cameras and cameras streamed via Camera Gateway

a. Export of video recorded in MJPEG, MPEG4 and H.264

b. Playback of exported video in exported player

13. The Video Management System shall provide the option to include date and time on each frame of the recording when it is exported.

H. Playback on Analog Monitors

1. Users shall be able to play back recorded video on an analog monitor from a selected time.

2. The Video Management System shall support basic play back operations on an analog monitor:

a. Play

b. Pause

I. Audio in Playback

1. Users shall be able to listen to audio recorded with video from all cameras being played back or selected cameras only.

2. Users shall be able to listen to audio streams without the need to display anything in the video pane.

3. The Video Management System shall support the following for 3rd Party cameras through ONVIF:

a. Listen to recorded audio

*RECORDING*

A. Configuring Recording

1. Users shall be able to start an instant recording from live video viewed in a video pane. They shall have the option to start recording video only or both video and audio.

2. Users shall be able to configure the recording schedule for cameras on NVRs. Recording can be configured to be:

a. 24/7

b. Timed (from minute to weekly schedules)

c. On alarm or event

3. Users shall be able to specify the transport protocol to be used for recording (TCP, UDP, Multicast.)

4. Users shall be able to specify whether audio should be recorded with the video.

5. Users shall be able to specify whether the recording should be protected when an alarm or event occurs (from a specified time before the alarm / event.)

6. Users with appropriate permissions shall be able to enable or disable recordings temporarily.

7. Users shall be able to delete recording schedules.

8. Users shall be able to copy recording schedules from one camera to other cameras on the same NVR.

9. Users shall be able to copy all recording schedules from all cameras from one NVR to another NVR.

10. Users shall be able to specify an alternative NVR to record to during a video “lockout” for either a camera or a site. Lockout permission can be used to prevent all other users from viewing and recording from a selected camera or all cameras in a selected site.

11. The Video Management System shall support digital signing (watermarking) of recordings as they are recorded on the NVR.

B. Managing Recordings

1. Users shall be able to find recordings within a specified time period.

2. Users shall be able to protect recordings.

3. Users shall be able to unprotect recordings.

4. The Video Management System shall display a warning message if an NVR is unable to retain the number of days recording for which it was configured.

C. Configuring Recording Redundancy

1. The Video Management System shall support the configuration of failover NVRs for each primary NVR with the following options:

a. 1 to N: 1 primary NVR can have one or more failover NVRs

b. N to 1: multiple primary NVRs can have the same failover NVR

2. The Video Management System shall support two modes of failover recording:

a. Continuous recording to primary and failover NVRs

b. Recording to failover NVR only when primary NVR fails

3. The Video Management System shall automatically failover when a primary NVR is down.

4. In addition, users shall have the option to manually failover, for example to allow for routine maintenance of a primary NVR.

5. Users shall have the option to manually fail back to a primary NVR, with the option to restore the recording configuration from the failover NVR to the primary.

*ALARMS*

A. Alarm Configuration

1. The Video Management System shall support binary inputs on IP Cameras, encoders, decoders and alarm panels.

2. The Video Management System shall support video loss alarm inputs.

3. The Video Management System shall support network loss alarm inputs.

4. The Video Management System shall support NVR fault alarm inputs, including:

a. Raid degraded

b. License failure

c. Recording failure

d. Redundant power failure

e. Redundant network failure

5. The Video Management System shall support analytics alarm inputs, with separate events for each analytics filter.

6. The Video Management System shall support alarm inputs from 3rd party systems.

7. The Video Management System shall enable multiple alarm inputs (detectors) to be grouped into an alarm zone.

8. The Video Management System shall support inputs (detectors) that do not cause an alarm to be generated.

9. The Video Management System shall support AND logic between detectors so that the alarm input is activated only when both detectors are activated with a defined time period.

10. The Video Management System shall support detectors that are activated and deactivated by different inputs e.g. activate on a binary input from one device and deactivate on a binary input from another device.

11. Users shall be able to dock the alarm viewing window below the Live View or Playback View windows.

12. Users shall be able to sort the alarm information in various ways by clicking on column headings.

13. The Video Management System shall support set and unset of alarm zones such that alarms are only generated when the alarm zone is set.

14. Users shall be able to configure the time schedule for each alarm zone – different start and end times for each day and multiple time periods per day.

15. Users shall be able to define specific dates and times within time schedules so that exceptions for holidays etc. can be specified.

16. The Video Management System shall enable the same time schedule to be applied to multiple zones.

17. Users shall be able to manually set and unset zones.

18. Users shall be able isolate faulty alarm inputs (detectors) such that they do not cause false alarms. Users shall be able to easily identify which alarm inputs are isolated and the reason for isolation.

19. The Video Management System shall enable zones to be set and unset on an event.

20. The Video Management System shall enable detectors to be isolated and restored on an event.

21. Users shall be able to specify a priority for each alarm zone (1-10.)

22. Users shall be able to configure the alarm sound for all alarm zones in a site or for each alarm zone individually. Sound can be from any .wav file and can be sounded once or repeated while the alarm is active.

23. The Video Management System shall allow alarms to be configured to require text from a user at the point of acknowledging and at the point of clearing.

24. The Video Management System shall allow an alarm procedure document (.html, text or URL) to be associated with a site or to an individual alarm zone. This procedure document shall be displayed when an alarm happens.

25. Users shall be able to configure the actions that should be performed when an alarm occurs:

a. Show video from camera, camera view or salvo in specified monitors

b. Stop video when alarm cleared

c. Move camera to preset position

d. Send email to multiple recipients, with option to include snapshots

e. Perform a relay action automatically

f. Start recording one or more camera – records for specified duration

g. Auto-protect recording from a specified duration before the alarm

26. Users shall be able to configure a second authorizing user for alarm clearing and relay actions – second user has to enter a password to authorize these functions.

27. The Video Management System shall support the following for proprietary and 3rd Party cameras through native protocols and / or ONVIF:

a. Motion detection events

b. Record on motion

c. Video loss

d. Network loss

e. Change video quality on event, including frame rate, resolution and bitrate.

B. Black Screen Monitoring

1. Users shall be able to configure an unlimited number of alarm groups each containing a set of alarm zones and/or detectors.

2. For each user or user group, it shall be possible to associate one or more video panes with each alarm group. This should include analog monitors.

3. Users shall be able to choose a display mode for alarm video. As multiple alarms come in, the video can either be “cascaded” across the chosen viewing panes or “queued” behind the chosen viewing panes. As alarms are cleared, the associated video is cleared from the chosen viewing panes. Cascaded video can either remain in the same video pane until cleared, or can move to the first available pane as earlier alarms are cleared.

4. When all alarm video is cleared from a viewing pane the Video Management System shall display video from the camera being viewed before any alarm was displayed.

5. The Video Management System shall clearly mark black screen monitoring viewing windows as being distinct from normal live view windows through background color and icon.

6. The Video Management System shall remove any black screen monitoring analog monitors from the normal site hierarchy.

7. The Video Management System shall have permissions to determine which users or user groups get access to which alarm groups and which windows are used to display alarm video.

C. Spot Monitoring

1. Users shall be able to configure any of the available viewing panes or analog monitors as a spot monitor for viewing significant live footage.

2. The Video Management System shall provide a toolbar option on all live viewing panes to copy the current video stream into the spot monitor.

3. The Video Management System shall keep an audit record of what video was started and stopped in the spot monitor, by which user and what times.

4. The Video Management System shall allow the video sequence that was viewed in the spot monitor by a selected user in a selected time period to be exported as a single incident.

5. Users shall be able to review all video watched by a selected user in a selected time period in an incident player. The video should be played back as one sequence in a single video pane.

D. Alarm response

1. The Video Management System shall generate an alarm if any of the detectors within an alarm zone are activated.

2. The Video Management System shall not generate new alarms for subsequent detector activations within the same zone so that the user only has one alarm to handle.

3. The Video Management System shall alert new alarms with flashing icon and optionally a sound.

4. The Video Management System shall automatically perform the actions configured for the alarm zone or detector:

a. Show video from camera, camera view or salvo in specified video panes or monitors

b. Move camera to preset position

c. Stop video when alarm cleared

d. Send email to multiple recipients

e. Perform a relay action

f. Start recording one or more cameras

g. Auto-protect recording from a specified duration before the alarm

5. When an alarm happens, the Video Management System shall be able to show live video from a camera on one pane and beside it show a looped replay from just before the alarm to just after.

6. From a looped replay, users shall be able to quickly jump to continuous replay from the alarm time.

7. The users shall be able to display a map showing the location of the alarm.

8. Users shall be able to view pending alarms in a list ordered by priority and time.

9. Users shall be able to filter the alarm list to show alarms only from specific areas (sites and zones.)

10. The Video Management System shall be able to display alarm procedure document for the alarm.

11. The Video Management System shall allow users to acknowledge alarms, entering alarm response text as required.

12. The Video Management System shall allow users to edit the alarm response text at any time before the alarm is cleared.

13. The Video Management System shall allow users to clear alarms, entering alarm response text as required.

14. Users shall be able to find historical alarms matching specified criteria:

a. Alarm type

b. Alarm state (new, acknowledged, cleared)

c. From site(s)

d. From alarm zones(s)

e. User(s) who acknowledged or cleared

f. Time range

15. The Video Management System shall be able to escalate alarms to other user groups if the alarm is not acknowledged within a pre-defined time period.

16. The Video Management System shall be able to escalate alarms to other user groups if the alarm is not cleared within a pre-defined time period.

17. The Video Management System shall support different escalation time periods for different alarm priorities.

18. The Video Management System shall be able to propagate an alarm to other areas (zones) if the alarm is not acknowledged within a pre-defined time period.

19. Users shall be able to produce reports of historical alarms and events and export to RTF or CSV formats.

20. Users shall be able to authorize an alarm to be cleared, by a second user entering a password.

21. Users shall be able to view live or recorded video associated with the alarm.

22. The Video Management System shall ensure that alarms are held on an alarm server, not on a user’s PC.

2.07 RELAYS

A. Users shall be able to configure relay actions using binary outputs on IP Cameras, encoders and decoders.

B. Users shall be able to configure relay actions using external outputs to 3rd party systems.

C. The relay activation shall be pulsed with a configurable pulse time period.

D. The Video Management System shall support latched relay outputs.

E. Users shall be able to associate relay actions with specific cameras so that the actions are readily available when video is displayed from that camera.

F. The Video Management System shall perform relay actions on alarm and event.

G. The Video Management System shall be able to perform relay actions on a time-schedule.

*MONITORING AND DIAGNOSTICS*

A. The Video Management System shall automatically check for devices not on the network and notify users when not available.

B. It shall be possible to define the users who get notified if devices become unavailable.

C. Users shall be able to manage the bandwidth used for network scans by configuration of:

1. Monitor period (mins)

2. Minimum check interval (mS)

3. Perform fast check on log in

4. Perform fast check on refresh.

D. The Video Management System shall scan for devices using any combination of IP broadcast addresses, individual IP addresses or ranges of IP addresses.

E. Users shall be able to turn off scanning of devices.

F. Users shall be able to set sites to offline mode. In this mode, all automatic communication with the site will be halted, while still allowing requested traffic.

G. Users shall be able to manually refresh any diagnostics view.

H. The Video Management System shall notify users when device times are not synchronized with the viewing PC (more than 60 seconds out.)

I. The Video Management System shall notify users of problems with NVRs. The notifications will be those supported by each NVR.

J. Users shall be able to view the current status of an NVR with visual indicators showing whether each item is OK or indicates problems:

1. Total disk space

2. Minimum free disk space

3. Used disk space (total – free)

4. Percentage space used (used disk space / total disk space)

5. License expiry date

6. Maximum streams

7. Maximum third party streams

8. Number of cameras recording

9. Number of cameras not recording

10. Number of recordings

11. Maximum recordings

12. Age of last deleted recording (indicates storage being achieved for each camera)

13. NVR time (in UTC)

14. Any additional features supported by the NVR.

K. Users shall be able to view per camera disk utilization for an NVR. Display a list of cameras being recorded by an NVR, showing the cameras with the highest disk usage at the top. Display the following info. For each camera:

1. Start time of first recording

2. End time of last recording

3. Total size of all recording

4. Total duration of all recordings

5. Recording rate (total size / total duration), in kbps

L. The Video Management System shall have a green / amber / red status indicator for any user’s PC’s CPU workload.

M. The Video Management System shall provide a support information tool, which gathers together log files and site database into a zip file.

*INSTALLATION*

A. The Video Management System shall be able to install the user’s application on an unlimited number of PC workstations at no extra cost.

B. The Video Management System shall include a un-install application to cleanly remove the users’ application from a PC.

C. The Video Management System Installation Application shall create a new site database.

D. It shall be possible to share a single site database across multiple installations of the Video Management System.

E. Users shall be able to specify the location of a backup site database to be opened if the main site database cannot be opened when a user logs in.

F. The Video Management System shall automatically check for site database updates.

G. The Video Management System shall support 3rd party branding:

1. Display 3rd party supplied text in title bar

2. Display 3rd party supplied bitmap/logo in login window

H. The Video Management System shall provide online context sensitive help.

I. The Video Management System shall provide an electronic user’s guide in PDF format.

*USERS*

A. User Configuration

1. Users shall be able to configure named user groups. A group can be granted administrator rights:

a. Full (can configure everything)

b. Restricted (can configure everything except users and groups)

c. No configuration rights (limited user functions only)

2. The Video Management System shall be able to hide administration options from normal users. The user interface shall be cleanly split into administrative functions and operational functions. Users who do not have administrative rights shall get a much simpler interface so that they are not confused by visible but disabled features.

3. Users shall be able to configure named user accounts and allocate them to user groups.

4. Users shall be able to enable and disable user accounts.

5. Users shall be able to set-up a user to use either Windows authentication or a password when he logs into the Video Management System.

6. Users shall be able to limit the total number of video streams (live or recorded) that a user or member of a user group can display at once.

7. Users shall be able to limit the number of time-based thumbnail images that a user or member of a user group will display at once.

8. Users shall be able to allocate each user group or user a priority that is used when controlling PTZ cameras.

9. Users shall be able to grant global permissions to user groups or users (global permissions do not apply to specific objects such as cameras):

a. PTZ hold (allows a user to keep control of a PTZ camera when not moving it)

b. Video lockout (allows a user to perform a video lockout on any site of camera)

10. Users shall be able to grant permission for user groups and/or users to access any object in the system (sites, cameras, monitors, salvos, alarm zones, detectors and relays.) For each object access can be limited by function:

a. List – see object in the user interface

b. View – view video from cameras, sequences, salvos and guard tours

c. Transmit audio (speak) to a camera, speaker or PA group

d. Playback recording from a camera or salvo

e. Record – make an instant recording of a camera

f. Export video clips or take snapshots from a camera

g. Control a PTZ camera

h. Display video on a monitor or video wall or activate a relay

i. Respond to alarms from an alarm zone

j. Hidden zone (live or playback) – access video behind a hidden zone

k. Audio (live or playback) – receive audio from a device

l. Set and unset an alarm zone

m. Isolate and restore a detector

n. Work offline

o. Configure presets and access the camera menus

11. Users shall be able to reset access permissions on individual objects to use the access permissions of their parent site.

12. Users shall be able to configure application settings specific to each PC, including:

a. Enable or disable scheduled tasks

b. Enable or disable the application as the topmost window

c. Location for snapshot images

d. Format of snapshot image (bitmap or JPEG)

e. Folder for snapshot image

f. Replay incident in live or Playback view

g. Use software or hardware assisted video renderer

h. Use de-interlace filtering on live view by default

i. Use de-interlace filtering on playback by default

j. Set video de-interlacing

k. Enable or disable use of a CCTV keyboard

l. Serial port for CCTV keyboard

m. CCTV keyboard type

n. Video pane text scale factor (% of the default text size)

o. Resize text on video panes in proportion to video pane size

p. Video pane icon size (normal, medium, large)

q. Select icon size on video panes in proportion to video pane size

r. Date / time display on video panes (none, all, selected)

s. Load bookmarks on startup

t. Spot monitor (external monitor or specified video pane)

u. Protect recordings by default when exporting

v. Write date and time on exported recordings

13. Users shall be able to prevent simultaneous listen and speak (full duplex audio.)

14. Users shall be able to configure the use of buffered playback when reviewing recordings.

15. Users shall be able to enable or disable alert messages.

B. User Logon

1. Users shall be able to log into the Video Management System manually.

2. It shall be possible to start the Video Management System from the command line with the following options:

a. Username and password

b. Normal, full screen or video-only modes

c. Site database

3. The Video Management System shall allow users to log out and log in without closing the application.

4. The Video Management System shall have an option to require all users to re-enter their password when logging out.

5. The Video Management System shall remember display settings on a PC for each user at log off and restore settings at log in:

a. Which cameras are displayed in which video panes

b. PTZ controls displayed

c. Map window position

d. Alarm window position

e. Video window positions (default hidden)

f. Main window size and position and site explorer width

g. Recording calendar displayed

6. Users shall be able to change their own password (if given write permission to the site database).

7. Users shall be able to change their default location on the tree hierarchy.

C. Video Lockout

1. Users shall be able to lockout all other users preventing them from viewing or recording video from a selected camera or all cameras in a selected site.

*AUDIT TRAIL*

A. Audit Trail Requirements

1. The Video Management System shall support an audit trail that can log user actions to a SQL database (ODBC Compliant) e.g. SQL Server.

2. Users shall be able to specify the authentication method to be used between the client application and the audit trail database:

a. Local user password

b. Windows user password

3. The audit trail shall log the following user actions to the audit trail database:

a. User logged on

b. User attempted to log on and was denied access

c. User logged off

d. User changed "home" site

e. User acknowledged an alarm

f. User cleared an alarm

g. User received an alert message (e.g. device not available)

h. User starting playing back a recording (forward)

i. User started playing back a recording (backwards)

j. User stopped playing back a recording

k. User denied playing back a recording or playback failed

l. User took control of a PTZ camera

m. User released control of a PTZ camera

n. Second user authorized relay action

o. Second user authorized alarm to be cleared

p. Second user denied authorizing a relay or alarm to be cleared

q. Export recordings

r. Protect recordings

s. Manual start or stop recording

t. User log out denied

u. User starts playing live video from a specific camera

v. User stops playing live video from a specific camera

w. Creation, deletion or editing items stored in the Video Management System configuration database

x. User created a bookmark

4. The audit trail shall log the following information for each entry in the audit log:

a. Date and time that the user performed the action in UTC

b. Name of the user performing the action

c. DNS name of computer running CC

d. The name of the application writing to the log

e. A string naming the type of action performed e.g. Log on

f. Name and matrix number of the object that the action applies to e.g. camera name and number

g. Further information about the action, in a structured form e.g.: “Alarm Time: 16-Feb-06 10:11:41, Alarm Response: False alarm”

h. Severity (applies to error message received log entry only)

5. The user shall be able to export a report from the audit trail database into a standard reporting tool, e.g. Excel.

*SITE SETUP*

A. Site Setup Requirements

1. The Video Management System shall discover IP Video devices on a network either by broadcast address or unicast addresses for each device.

2. The Video Management System shall allow configuration of IP Video System devices via their web configuration interface.

3. The Video Management System shall enable mass configuration of devices, in particular encoder settings on IP cameras and encoders.

4. Administrators shall be able to view video from each stream at the same time as making changes to the media parameters on an encoder to aid configuration.

5. Administrators shall be able to upgrade the firmware on IP Video System devices - multiple devices can be upgraded in one go.

6. Administrators shall be able to create a hierarchy of sites and sub-sites for organizing cameras and other items by location.

7. Administrators shall be able to set the time-zone on a site - different sites can each have their own time zone.

8. Users shall be able to reorder sites under their parent site (sites are ordered by number.)

9. The Video Management System shall be able to automatically create a site hierarchy within a site database containing IP Video System devices visible on the network.

10. Users shall be able to create sequences and salvos within the sites, set up 24/7 recording for each camera and enable video loss and network loss alarms.

11. Users shall be able to add cameras, monitors, alarm panels, alarm servers and NVRs to sites by dragging and dropping, selecting from a list or manually entering the IP Address and name.

12. Users shall be able to remove devices from sites.

13. Users shall be able to move devices, and other items such as sequences, salvos, and sub sites from one site to another by dragging and dropping.

14. Users shall be able to enter a localized display name for cameras, monitors, alarm panels, alarm servers and NVRs which overrides the name stored on the device.

15. The Video Management System shall enable a copy of the configuration database to be cached locally on each user workstation to ensure continuity of operation when a connection to the central database is not available.

16. The Video Management System shall support a configuration database that is divided into multiple ‘segments’, e.g. one segment for each site. The Video Management System shall allow each segment to be configured and accessed independently.

17. The Video Management System shall support user access permissions so that only authorized users can access specific segments.

18. When the configuration database is divided into segments, the Video Management System shall allow all sites to monitored e.g. from a central monitoring facility.

*MAPS*

A. Configuration

1. Users shall be able to create one or more maps for each site by importing an image for the background. The following image formats shall be supported:

a. Bitmap (BMP)

b. JPEG (JPG)

c. Portable Network Graphics (PNG)

d. AutoCAD drawings (DWG)

2. Users shall be able to add links to other maps.

3. Users shall be able to reposition items by drag and drop or entering specific coordinates.

4. Users shall be able to add cameras to map via drag and drop.

5. Users shall be able to specify the field of view for each camera.

6. Users shall be able to add alarm zones and detectors to map.

7. For alarm zones, users shall be able to have options to not display the alarm icon and/or name unless the alarm is active.

8. For zones and detectors, users should be able to configure a detector/zone area on the map.

9. Users shall be able to specify the amount of detail displayed for each object including icons, matrix numbers and labels.

10. Color schemes shall be configurable to make text and fields-of-view more visible.

B. Navigation

1. The map shall be fully scalable with zoom and pan supported under mouse control.

2. Users shall be able to displays the previous maps viewed (back, forward).

3. Users shall be able to link to any map from any map.

4. Users shall have the option of scaling icons to a fixed zoom level.

5. The map should be viewable on a separate monitor from the main video(s).

C. Video

1. Users shall be able to display live and recorded video from any camera on a map (drag and drop.)

2. Users shall be able to view video from some or all of the cameras on a map via drag-select.

3. Users should be able to click on the field-of-view of any camera to view the video.

4. Where fields-of-view overlap, clicking on the convergent area should result in all cameras being displayed.

D. Alarms

1. Activated alarms shall be visually represented on the map.

2. Where detector/zones areas have been configured, these should be visually represented as being in an alarmed state.

3. Where detector/zones areas have been configured and in an alarmed state, the user should be able to start video from all cameras associated with that zone by clicking on it.

4. Users shall be able to:

a. Manage alarms from a map

b. Clear alarms

c. Acknowledge alarms

d. View Video associated with an alarm

e. Isolate/restore alarms

f. Set/unset detectors

E. Actions

1. Users shall be able to trigger events to binary outputs on cameras or encoders.

*RESTRICTED CLIENT INTERFACE*

A. The Video Management System shall include a restricted access version of the video viewing and replay application that prevents all users from accessing the setup screens even if they have an administrator login.

B. The Video Management System shall provide a restricted access site database management utility, which prevents creation of new site databases.

C. The Video Management System shall provide a restricted access version of the video viewing and replay application, which prevents all users from modifying the audit log configuration even if they have an administrator login.

*SDK*

A. Automation Interface

1. The Video Management System shall provide a COM interface to enable the functionality of the Video Management System user interface to be controlled by other applications.

2. The Automation Interface shall allow a 3rd party application to query for details of items within the Video Management System site database:

a. Sites

b. Cameras

c. Monitors

d. Video panes

e. Salvos

f. Sequences

g. Guard tours

h. Video windows

3. The Automation Interface shall allow a 3rd party application to:

a. Change the layout of a video window

b. Start or stop video from camera in video pane or monitor by matrix number

c. Move a PTZ camera to a preset position\*\*

d. Start a salvo in video pane or monitor by matrix number

e. Start a sequence in a video pane or monitor by matrix number

f. Playback a camera by matrix number at a specific time

g. Switch between Live, Playback, and Setup modes

h. Export video from a camera or all cameras in a site

i. Protect recordings for a camera or all cameras in a site

j. Set the PTZ type of a cameras and send PTZ commands\*

k. Start looped replay

l. Find a camera ID from an IP address

B. Binding Interface

1. The Video Management System shall have a tool to allow external networked systems to send events and instructions to the Alarm Server. Such commands shall include:

a. Send alarm

b. Send bookmark

c. Set/unset alarm

d. Isolate/restore detectors

e. Clear/acknowledge an alarm

2. The Video Management System shall have a tool to allow external networked systems to listen to the NVR and detect any new events received by the Alarm Server. Such events shall include:

a. Changes in alarm zone

b. Changes in alarm detector

c. Changes in relay output

\* Only on support cameras

\*\* Excluding ONVIF cameras