CathexisVision 2018 A&E Specification

005-20170712-142 Rev 1.2 8 September 2017 G Brecher; R Solomon; D Buhrmann

Contents

1 Introduction

This document outlines the general requirements for the CathexisVision Video Management Software (which may hereinafter be referred to as “the VMS”) and/or peripheral devices as produced by Cathexis Technologies and supplied by Cathexis distributors in selected regions.[1]

Please contact support@cat.co.za for any queries.

[1] While Cathexis has made every effort to ensure the accuracy of this document, there is no guarantee of accuracy, neither explicit, nor implied. Specifications are subject to change without notice.

2 General System Requirements

2.1 System Architecture

2.1.1 The system shall be the CathexisVision Video Surveillance System.

2.1.2 The system shall be of an enterprise nature, able to manage multiple sites remotely.

2.1.2.1 The system shall provide a complete, remote setup and maintenance client.

2.1.2.2 The system shall not rely on remote desktop applications for remote connection.

2.1.3 The system shall not require a dedicated management server, thus requiring less hardware.

2.1.4 The system shall not require a dedicated SQL database for recording.

2.1.5 The system shall be of a 'client/server' nature with the following components:

2.1.5.1 Recording Management Servers.

2.1.5.2 On and off-site client viewing and management stations.

2.1.5.3 Off-site Cell Phone/Tablet clients.

2.1.5.4 Alarm Management Server.

2.1.6 The system shall be capable of running in Windows (32/64-bit) or Linux operating system environments.

2.1.7 The system shall be capable of running in a virtual machine environment.

2.1.7.1 The system shall be aware of running in a virtual server environment, and will have knowledge of the underlying hardware.

2.1.8 The system shall be licensed for use with the application of various site-wide licenses.

2.1.8.1 The system shall be easily expandable by the addition of IP camera, 3rd party systems integrations, video analytics, and/or analogue system hardware licenses.

2.1.8.2 The system shall provide certain built-in features which may be unlocked for use with a software key, enabling quick activation of the required features.

2.1.8.3 The system shall be easily upgradeable to later versions via a CD, USB key, or other similar means.

2.1.9 The system shall be easily expanded by the addition of recording servers, viewing and management servers and storage.

2.2 System Configuration

2.2.1 The system shall enable remote connection to the system via ADSL, VPN, or any other source of communication.

2.2.1.1 The system shall be able to perform all setup and viewing functions via this remote connection.

2.2.2 The system shall store complete site configuration on- or off-site for retrieval in the event of hard drive failure.

2.2.2.1 The system shall allow this configuration to be easily re-instated.

2.2.3 The system shall maintain user activity logs.

2.2.4 The system shall enable all sub-systems on site to be time-synchronised.

2.2.5 The system shall manage an unlimited number of Inputs and Relay Outputs.

2.2.6 The system shall provide setup wizards for fast, simple addition and configuration of certain devices and objects, such as camera, integrated devices, site maps, etc.

2.2.7 The system shall use Universal Plug and Play (UPnP) and ONVIF Device discovery to discover IP devices and retrieve the settings from those devices.

2.2.8 In order to ensure that there is fast access and bandwidth management for remote client connections, all site resources, maps, and other site-specific parameters shall be downloaded and stored locally at the remote client's location. If they have been modified at site they are to be re-loaded from the site to the remote client connection upon re-connection.

2.3 Audio and Video Capabilities

2.3.1 The overall system shall have no limit to the number of cameras/video streams.

2.3.2 The system shall be a digital video/audio recording and remote monitoring system with the capability of simultaneously displaying, recording, replaying, searching, and transmitting both video and audio.

2.3.3 The system shall be truly hybrid in nature, and shall be capable of supporting the following video sources:

2.3.3.1 IP video cameras.

2.3.3.1.1 A separate list of supported IP cameras is to be provided, or as listed on the CathexisVision website.

2.3.3.2 IP video encoders (Cathexis and 3rd party).

2.3.3.3 Cathexis Analogue Video systems.

2.3.3.4 ONVIF compliant devices.

2.3.4 Each recording management server shall be capable of managing multiple IP camera video streams, limited only by hardware processing capability, and available local/remote system storage.

3 Video and Audio Streaming

3.1 General Capabilities

3.1.1 The system shall manage the live streaming, recording, and reviewing of both video and audio from the various sources.

3.2 Video Streaming

3.2.1 The system shall be capable of managing video from both analogue video cards, and IP video sources simultaneously.

3.2.2 The system shall be capable of managing simultaneous MJPEG, MPEG4, H264, H265 and MxPEG, and a combination thereof, according to the camera capability.

3.2.3 The system shall be capable of managing either Unicast or Multicast video streams.

3.2.4 The system shall be capable of routing selected video streams to selected Video monitors, for viewing and reviewing video.

3.2.5 The system shall be capable of displaying video in HD or higher where required.

3.2.6 The system shall be capable of managing dynamic streams, and intelligently selecting the camera stream based on the display resolution of either client, server and/or video wall to improve live viewing efficiency and reduce resource usage.

3.2.7 The system shall be capable of "trans-coding" video streams to a lower bandwidth, for off-site monitoring (subject to the availability of suitable video streams & the processing power of the video servers).

3.3 Audio Streaming

3.3.1 The system shall be capable of receiving, and storing, synchronised audio from cameras with audio capability.

3.3.2 The system shall be able to record and playback synchronised audio and video.

3.3.2.1 Assuming that the source audio and video is synchronised on the camera, the system shall be capable of maintaining this synchronisation to less than 500 milliseconds.

3.3.3 The system shall be capable of managing bi-direction audio, from the system to a remote IP device, or camera, with the relevant audio capability.

3.3.4 The system shall be capable of streaming/storing and playback of an unlimited number of camera audio streams.

4 User Management and Access Rights

4.1 User Management

4.1.1 The system shall be capable of site-based user management, and shall apply all users and their access rights to all servers on the site.

4.1.2 The system shall allow administrators to configure site users and assign usernames, user access levels and passwords.

4.1.2.1 The system shall have thirty user levels, with the top-most level in the hierarchy being 30 and the bottom-most level in the hierarchy being 1.

4.1.3 The system shall allow individual site users to be assigned the rights to:

4.1.3.1 View all site resources.

4.1.3.2 Connect remotely.

4.1.3.3 Change own password.

4.1.4 The system shall be accessed by user name and password, and all user actions shall be recorded against the user's name in an operator audit trail. This audit trail shall be accessible, printable, and access-controllable.

4.2 LDAP/Active Directory

4.2.1 The system shall support importing of users from a LDAP (Lightweight Directory Access Protocol) user management system on Professional and Premium sites only.

4.2.2 The system shall support assigning VMS access rights to imported LDAP users.

4.2.3 The system shall use LDAP to communicate with user management systems like Active Directory and OpenLDAP.

4.2.4 The system shall query the management system server on each login of an LDAP registered user for credential validity.

4.2.5 Logins from LDAP users using the system mobile I/O or API will not be permitted or validated.

4.3 Access Rights

4.3.1 The system shall be capable of limiting availability of site resources to users based on the access rights assigned to them by administrators.

4.3.2 The system shall allow administrators to assign access rights to user levels, either locally or remotely.

4.3.3 The system shall restrict access to the setup tab (in which site configuration is done, e.g. setup, viewing and control of databases, cameras, video analytics, etc.) to administrator users only.

4.3.4 The system shall allow administrators to assign users the following access rights to site resources (such as cameras, inputs/outputs, monitors, etc.):

4.3.4.1 Live View.

4.3.4.2 Review.

4.3.4.3 PTZ manual Control, PTZ menu options, set PTZ presets, control PTZ tours.

4.3.4.4 Audio listen.

4.3.4.5 Hide privacy zones.

4.3.4.6 Export data.

4.3.4.7 Reset camera tamper.

5 Recording, Archiving and Storage

5.1 Recording

5.1.1 The system shall be capable of:

5.1.1.1 Recording frame rates of more than 30 frames per second, depending on camera capabilities.

5.1.1.2 Recording to various, configured databases.

5.1.1.3 User-initiated recordings. Users with the correct access rights may manually trigger a recording.

5.1.1.4 Event recording. Events may be configured to trigger a recording on the relevant camera.

5.1.1.5 Scheduled recordings. Cameras may be set to record on a fixed schedule.

5.1.1.6 Continuous recording. Devices (such as integrated devices and cameras) are continuously recorded and create time markers in the recording.

5.1.2 The system shall provide a screen recording feature, which enables the recording of any computer screen connected to any Windows/Linux computer. This will be recorded to the VMS as if it were a standard IP camera.

5.2 Archiving (Exporting)

5.2.1 The system shall be capable of the following video archiving abilities:

5.2.1.1 Exporting audio and video from the software in a proprietary video format, with an optional standalone player.

5.2.1.2 Marking start and end times of video to be archived.

5.2.1.3 Archiving multiple cameras simultaneously.

5.2.1.4 All video meta-data visible at the time of archiving will be retained in the archive.

5.2.1.5 Archiving selected footage from one or multiple cameras to DVD, USB Memory device, local or remote Hard Drives in formats allowed by the operating system.

5.2.1.6 Saving the archive “player” along with the video.

5.2.1.7 Archiving and viewing files containing non-ASCII characters (e.g. Arabic).

5.2.1.8 The system shall be able to export video from an archive.

5.2.1.8.1 The system shall allow video exported from an archive to be in MP4 or archive format.

5.2.1.9 The system shall provide the capability to perform a scheduled archive as follows:

5.2.1.9.1 Archive selected cameras.

5.2.1.9.2 Archive only a selected period of recorded footage.

5.2.1.9.3 Archive at a selected time of day.

5.2.2 The system shall employ the following security features with regard to archiving video and exporting video from an archive:

5.2.2.1 The ability to archive shall be an access rights controlled feature.

5.2.2.2 The system shall allow administrators to create user-level based 'archiving profiles' for which archiving passwords and watermarks are configured.

5.2.2.2.1 Depending on the password and archiving options configured in the relevant archiving profile, the system shall require users to set a password and/or apply a watermark when archiving video.

5.2.2.2.2 For prosecution, and other legal purposes, archived images shall be digitally signed with the unique identifier of the original archiving server that is lost if an attempt is made to manipulate the image.

5.2.2.2.3 The system shall be able to restrict the ability to export from an archive.

5.2.2.2.3.1 The system shall remove the server signature from video exported from an archive in MP4 format.

5.3 Storage

5.3.1 The system shall be capable of storing selected video streams to selected video databases.

5.3.1.1 The system shall be capable of storing video footage from the same cameras to multiple databases simultaneously.

5.3.2 The system shall be capable of creating and managing multiple databases.

5.3.3 The system shall be capable of managing databases spanning multiple local or Network Storage (NAS) devices.

5.3.4 The system shall be capable of accessing Windows network shares from within the software.

5.3.5 The system shall be capable of warning the user when disk/network shares containing databases in use by the software are detached from storage management.

6 Graphical User Interface (GUI)

6.1 General GUI Capabilities

6.1.1 The system shall provide a graphical user interface (GUI) which enables users to easily see all resources (Cameras, Audio components, databases, Inputs, Outputs, Layouts etc.) on a complete site, and shall not be limited to specific I.P. Network Video Servers.

6.1.1.1 The system shall provide two interface facets of the overall GUI; the operator interface and the setup interface:

6.1.1.1.1 The system shall only allow administrator users to access the setup interface, in which all site configuration is done.

6.1.1.1.2 The system shall allow all user levels to view the resources available in the operator interface to varying degrees (depending on their assigned access rights).

6.1.2 From the operator interface, it shall be possible to open multiple sites simultaneously and display them on selected monitors on the system. This includes associated site recourses, such as site maps, camera feeds, etc.

6.1.3 The GUI shall be capable of being viewed over up to 6 monitors from one client software computer. The user shall be able to customise the monitors so that they can view different components (e.g. maps, cameras, 3rd party systems integration transaction data etc.) on different monitors or on window “tabs” on the same monitor.

6.1.4 The layout of the operator interface shall be customizable, as in the following:

6.1.4.1 System functions or features that are not activated, or to which the user does not have access shall be hidden from view – the user shall only see functions that he/she uses.

6.1.4.2 Resources to which the user does not have access shall be inaccessible to the user.

6.1.4.3 The location of the Resources Panel can be set to either right or left of the cameras tab screen.

6.1.5 The system shall provide a **status bar** at the bottom of the GUI to indicate information about the software using status icons, all of which can be clicked for further information. For example:

6.1.5.1 The system shall show a license warning for site resources that are incorrectly licensed.

6.1.5.2 The system shall display username and access level of logged in user.

6.1.5.3 The system shall display the applied site license.

6.1.5.4 The system shall display a camera notification if a camera goes down.

6.1.5.5 The system shall display a performance monitor which indicates performance statistics of the system.

6.1.5.6 The system shall display the connection status of the current unit to the site.

6.1.5.7 The system shall display a video analytics notification when an error has occurred with one or more of the site’s video feeds.

6.1.5.8 The system shall display a failover notification which provides information about the status of existing failover servers.

6.1.5.9 The system shall display a tamper warning when one or more of the site cameras are considered to have been tampered with.

6.2 Cameras

6.2.1 **Setup Interface**

6.2.1.1 The system shall restrict access to site camera configuration in the setup interface to administrators.

6.2.1.2 The system shall provide a camera addition and setup wizard.

6.2.1.3 The system shall provide a “copy and paste” capability which will enable users to easily copy camera settings, including information from multiple video streams, across multiple cameras.

6.2.1.4 During camera configuration, the system shall display the URL/web page of the camera which can be loaded in the browser.

6.2.1.5 The system shall enable the administrator to designate a camera as “covert”. In this case, the camera should only be seen and viewed/reviewed by administrators

6.2.2 **Operator Interface**

6.2.2.1 The system shall enable users to view and interface with cameras to varying degrees, depending on the assigned access rights.

6.2.2.2 The system shall enable the user to select specific cameras to be viewed on selected monitors, or selected panels within selected monitors.

6.2.2.3 The system shall provide the capability to drag-and-drop cameras from a resource panel into selected monitors, or panels on the monitor.

6.2.2.4 The system shall enable the synchronisation of cameras during playback.

6.2.2.5 The system shall enable users to pause playback of video and print, copy to a clipboard, or save an image to a select storage location

6.2.2.6 The system shall enable users to drag-and-drop cameras, from a map, into selected monitors or panels on the monitor.

6.2.2.7 The system shall enable the configuration and initiation of tours (sequences) of cameras on selected monitors or on panels within a selected monitor.

6.2.2.8 The system shall provide the capability to create and save multiple “layouts” of cameras that can then be easily selected, either manually by a user, or automatically on an event.

6.2.2.9 The system shall allow the initiation of tours (sequences) of “layouts” (also known as a “salvo”) to selected monitors.

6.2.2.10 The system shall enable the user to “de-warp” video from 180 or 360-degree panoramic cameras.

6.2.2.11 The system shall enable the user to view up to 64 cameras on a single monitor.

6.2.2.12 The system shall enable users to digitally zoom into specific camera views.

6.2.2.13 The system shall allow users to choose which stream to show if multiple camera streams have been designated for live viewing.

6.3 Site Resources

6.3.1 Setup Interface

6.3.1.1 The system shall allow administrators to configure which site resources are visible in the operator interface.

6.3.1.2 The system shall enable administrators to create folders, and allocate resources to selected folders.

6.3.2 Operator Interface

6.3.2.1 User access to site resources shall be access-controlled by username and password, whether local or remote viewing, restricted by the access level of the individual user.

6.3.2.2 The user shall be able to see input triggers from the GUI.

6.3.2.3 The user shall be able to control outputs from the GUI.

6.4 Text and Graphical Overlays

6.4.1 Operator Interface

6.4.1.1 The operator interface shall optionally display graphical information from resident and 3rd party devices as overlays on the camera panels.

6.4.1.2 The system shall enable repositioning of overlay blocks and changing of overlay sizes, text sizes, transparency and colour.

6.4.1.3 The operator interface shall be able to optionally show analytics algorithms functioning by displaying overlays.

6.5 PTZ Controls

6.5.1 Operator Interface

6.5.1.1 The system shall be able to control Pan-Tilt-Zoom (PTZ) cameras from the operator interface and via the event actions.

6.5.1.2 The system shall also enable users to control PTZ cameras from an attached keyboard/joystick.

6.5.1.3 PTZ controls include:

- 6.5.1.3.1 Pan, Tilt and Zoom.
- 6.5.1.3.2 Variable PTZ movement speed.
- 6.5.1.3.3 Focus and Iris control.
- 6.5.1.3.4 Define PTZ camera pre-set positions.
- 6.5.1.3.5 Assign unique names to PTZ camera pre-set positions.
- 6.5.1.3.6 Move to PTZ camera default positions.

6.5.1.4 The system shall be capable of priority control of a PTZ camera.

- 6.5.1.4.1 An administrator user is afforded highest priority control over PTZ camera, after which the priority hierarchy runs down from user level 30 to user level 1.

6.5.1.4.2 Two users of the same level will afford the first user priority control, and the seconds user must wait until 'Dome override' period has elapsed.

6.6 Live View

6.6.1 **Operator Interface**

6.6.1.1 The system shall enable users to view and pause live cameras (depending on assigned access rights).

6.6.1.2 The system shall allow specific cameras to be viewed live, and played back simultaneously, and synchronised together if requested.

6.6.1.3 The system shall allow the same camera to be viewed live on multiple monitors or panels on one monitor.

6.6.1.4 The system shall be capable of displaying Activity Trails for up to 15 minutes in live mode. See Section 7.10.

6.7 Review

6.7.1 The system shall allow review of cameras in the same window, and same panel, as live video is played, without needing to open a separate review or database window/tab.

6.7.1.1 The system shall enable users to playback recorded footage by click-and-dragging the camera timeline to the desired review point.

6.7.1.2 The system shall enable users to easily review any camera on the system, from any/multiple clients connected to the system, either off-site or on-site.

6.7.2 The system shall prompt the user to select which database to review from if the selected camera has been configured to record to multiple databases.

6.7.3 The system shall be capable of reviewing multiple cameras simultaneously, and synchronising the review times of those cameras.

6.7.4 The system shall retain review times across different cameras selected for the same panel. If a camera is in review mode, and a new camera is opened in that panel, the new camera will go to the same review time as the original camera.

6.7.5 The system shall control access rights for archiving and reviewing of archived video footage.

6.7.6 The system shall be able to perform smart searches using the following review tools:

6.7.6.1 Snap-Search. See Section 6.8.

6.7.6.2 Motion Area Search. See Section 7.11.

6.7.6.3 Displaying thumbnail image previews of a recording by hovering the mouse over the timeline.

6.7.7 The system shall be capable of displaying Activity Trails for up to 60 minutes in review mode. See Section 7.10.

6.8 Snap-Search

6.8.1 Operator Interface

6.8.1.1 In review, the system shall be capable of dividing a user-defined time period into a user-defined matrix of thumbnail images.

6.8.1.2 The system shall allow the user to narrow the defined search period between displayed snapshots by click-and-dragging between desired thumbnails.

6.8.1.3 The thumbnail matrix will be reconfigured for this new search period.

6.8.1.4 The system shall be capable of defining search time periods according to seconds, minutes, hours, days, and weeks.

6.8.1.5 The system shall be capable of playing recorded footage starting from a particular thumbnail in both the operator interface video player and in the Snap-Search window embedded video player.

6.8.1.6 The system shall be capable of archiving video from within the Snap-Search window embedded video player.

6.9 Privacy Zones

6.9.1 Setup Interface

6.9.1.1 The system shall allow administrator users to create and remove Privacy Zones in the camera feed.

6.9.1.1.1 Privacy Zones shall be configurable black polygons that obscure sensitive areas of the camera feed.

6.9.1.2 The system shall allow administrators to assign users the rights to hide/show privacy zones.

6.9.2 Operator Interface

6.9.2.1 The system shall show privacy zones live, review, and archived video footage.

6.9.2.2 The system shall allow users with the correct access rights to either hide/show privacy zones.

6.9.2.3 The system shall show/hide privacy zones in archived footage depending on whether or not they have been hidden/shown by the user at the time of archive.

6.10 Video Wall

6.10.1 The system shall provide Video Wall software to be run on computers dedicated to showing video feeds.

6.10.2 The system shall be capable of displaying multiple site cameras on video wall monitors.

6.10.3 The system shall be capable of controlling multiple monitors attached to multiple computers from a single point via a MIMIC panel.

6.10.4 The system shall be able to drag-and-drop cameras into place for display on the video wall from sites other than the monitor site.

6.10.5 The system shall allow administrators to configure video wall camera layouts, tour of layouts (salvo), and access rights to video walls.

7 Video Analytics

7.1 General Capabilities

7.1.1 The system shall have its own analytics and algorithms, built in to the software, to be used as event triggers.

7.1.1.1 This will include video motion detection, and object tracking analytics.

7.1.2 The system shall allow video analytics to be configured on live and recorded footage.

7.1.3 The system shall restrict access to analytics configuration to administrators only.

7.1.4 The system shall be capable of utilising the on-board analytics on the I.P. camera or encoder to initiate an event with which selected actions can be associated.

7.1.5 The system shall be capable of integrating with third-party analytics suites.

7.2 Motion Detection Analytics

7.2.1 The system shall have built-in Video Motion Detection (VMD) algorithms, and will be capable of performing these on video streams received.

7.2.2 The system shall offer the following Basic and Smart VMD options.

7.2.2.1 Basic VMD

7.2.2.1.1 Basic motion detection algorithm.

7.2.2.1.2 Basic noise suppression.

7.2.2.2 Smart VMD

7.2.2.2.1 Advanced filtering out of repetitive motion like trees or grass.

7.2.2.2.2 Tracking light charges.

7.2.2.2.3 Advanced motion detection algorithms designed for outdoor scenes.

7.2.3 The Basic and Smart built-in motion detection shall have the following features:

7.2.3.1 Variable sensitivity.

7.2.3.2 Size masking.

7.2.3.3 Reject objects smaller/larger than a specified size.

7.2.3.4 Multi-zone VMD areas per camera with the ability to vary sensitivity in each zone.

7.2.3.5 A day/night setting capability to enable different VMD settings for day and night.

7.2.3.6 Automatic day/night switching or switching at specified times are to be optional.

7.2.3.7 A schedule which enables/disables selected VMD event triggers at certain times of day.

7.2.4 For VMD setup, the system shall enable users to view live or recorded video, for VMD setup/testing purposes

7.2.5 The system shall have the capability to show masking areas of VMD, including:

7.2.5.1 VMD triggers.

7.2.5.2 VMD detection areas.

7.3 Basic, Intermediate and Advanced Analytics

7.3.1 The system shall be capable of providing basic, intermediate, and advanced video analytics options.

7.3.2 The system shall be able to trigger events based on the triggers generated by the basic, intermediate, and advanced analytics.

7.3.3 The system offers the following event trigger options:

7.3.3.1 Basic Analytics.
7.3.3.2 Basic line crossing triggers.
7.3.3.3 Basic presence triggers.
7.3.3.4 Intermediate Analytics.
7.3.3.5 Advanced line crossing triggers.
7.3.3.6 Advanced presence triggers.
7.3.3.7 Advanced Analytics.
7.3.3.8 Advanced line crossing triggers.
7.3.3.9 Advanced presence triggers.
7.3.3.10 Speed detection.
7.3.3.11 Size and direction filters.

7.4 Head Counting

7.4.1 The system shall provide the following head counting algorithms and capability options:

7.4.1.1 Top-down head tracker; algorithm on a 3D/standard colour camera looking straight down offers event triggering when heads cross a line.

7.4.1.2 Oblique Head Tracker; algorithm on a 3D/standard colour camera mounted at an angle offers event triggering when heads cross a line.

7.5 Queue Length Algorithm

7.5.1 The system shall offer event triggering when a queue exceeds a certain length.

7.6 Still Object Algorithm

7.6.1 The system shall offer event triggering when an object has been left for a period of time.

7.7 Camera Tamper Detection

7.7.1 The system shall come standard with camera tamper detection video analytics.

7.7.2 Camera tampering includes:

7.7.2.1 Lens covering (e.g. spray-painting)
7.7.2.2 Camera moving,
7.7.2.3 Lens re/un/de-focusing.

7.7.3 Setup Interface

7.7.3.1 The system shall allow any configured camera to have camera tamper detection added to it.

7.7.3.2 The system shall allow camera tamper to trigger events.

7.7.4 Operator Interface

7.7.4.1 The system shall display an alarm notification in the operator interface when tamper is detected.

7.7.4.2 The system shall eliminate false alarms by requiring a tamper to persist for 60 seconds before being considered a true tamper.

7.7.4.3 The system shall restrict user ability to reset a camera tamper based on the access rights assigned by the administrator.

7.8 Motion Database

7.8.1 Setup Interface

7.8.1.1 The system shall allow the creation of a Motion Database which collects motion data from selected cameras.

7.8.1.1.1 The system shall allow motion data from the Motion Database to be used to inform the Activity Trails and Motion Area Search features of the operator interface on the selected cameras.

7.8.1.2 The system shall allow the tracking of motion data to be set to varying sensitivity levels; the higher the sensitivity, the more finely motion is tracked.

7.8.1.3 The system shall allow the size of the grid in which motion data is tracked to be set using either:

7.8.1.3.1 Aspect Ratio and Granularity Settings (the finer the granularity, the more motion is detected in smaller areas of the image).

7.8.1.3.2 Manually Set Grid Size.

7.9 Adjacent Camera Mapping

7.9.1 The system shall provide the facility to link physically proximate cameras in the software, and to be able to be able to easily navigate between the linked cameras in the operator interface to follow objects/suspects which move across multiple cameras.

7.9.2 **Setup Interface**

7.9.2.1 The system shall provide a mapping screen to configure adjacent cameras.

7.9.2.2 The system shall be able to select cameras from the available site resources to be configured as adjacent cameras.

7.9.2.3 The system shall be able to define the bi-directional relationships between each pair of adjacent cameras.

7.9.2.4 The system shall be able to display the Adjacent Camera page manager, where:

7.9.2.4.1 The system shall be able to create and delete pages, which can be further organised into sub-folders and folders, to which adjacent cameras may be added.

7.9.2.4.2 The system shall allow the same camera to be added to multiple different pages, sub-folders and folders.

7.9.2.5 The system shall allow a camera and all associated directional links to other mapped cameras to be removed from either:

7.9.2.5.1 A single page, sub-folder or folder without removing it from other pages, sub-folders or folders; or

7.9.2.5.2 All pages, sub-folders or folders.

7.9.3 **Operator Interface**

7.9.3.1 The system shall display arrows as overlays on configured cameras, pointing in the directions of physically adjacent cameras.

7.9.3.2 The system shall switch to adjacent cameras on selection of the relevant adjacent camera arrow.

7.9.3.3 The system shall enable the user to select Adjacent Camera from the Resources dropdown menu in the Cameras Tab.

7.9.3.4 The system shall display adjacent cameras by clicking on the relevant camera in the Resource dropdown menu.

7.10 Activity Trails

7.10.1 The system shall be capable of displaying where and how recently activity has occurred in various areas of the camera feed by displaying activity trail overlays.

7.10.2 The system uses motion data collected to the Motion Database, and camera recordings, to generate activity trails.

7.10.3 The system shall display activity trail overlays in colours ranging from green to red to indicate past and present activity in an area.

7.10.3.1 The greener an overlay, the further back in time the activity in that area occurred.

7.10.3.2 The redder an overlay, the more recent the activity in that area is.

7.10.4 The system shall display the Activity Time (in minutes and seconds) on top of the activity trail overlay to indicate how far back from the current time the activity in that area occurred.

7.10.5 The system shall be capable of displaying activity trail overlays for certain periods of time which are determined by viewing mode and camera recordings;

7.10.5.1 In live view, and/or if camera recordings have not been configured, the system is capable of displaying activity trails for activity which has occurred within the last 15 minutes of the current time.

7.10.5.2 In review (provided camera recordings have been configured), the system is capable of displaying activity trails for activity which has occurred within the last 60 minutes of the current time.

7.10.6 The system shall be capable of toggling Activity Trails on and off.

7.10.7 The system shall be capable of switching to the time of activity indicated by an activity trail overlay by double-clicking on the desired activity trail overlay.

7.10.8 The system shall display motion in the camera feed as red motion bars along the camera review timeline; the higher the motion bar, the more motion in the camera feed at that point in the recording.

7.11 Motion Search

7.11.1 Operator Interface

7.11.1.1 In review, the system shall be capable of selecting certain areas of the camera image to search recent motion within the selected area.

7.11.1.2 The system uses motion data collected to the Motion Database to indicate recent motion in the selected area.

7.11.1.3 The system shall display all motion in the selected area as red motion bars along the camera review timeline; the higher the motion bar, the more motion in the selected area at that point in the recording.

8 Triggers, Events, and Actions

8.1 General Capabilities

8.1.1 The system shall restrict access to events management to administrators only.

8.1.2 The system shall be capable of generating a system event based on configured system triggers, and performing configured event actions.

8.1.3 The system shall be capable of automatically storing all system events in a system Events database, even when no video is associated with the event. See the Databases section for more.

8.2 Event Triggers

8.2.1 The system shall have the ability to generate events from the following triggers:

8.2.1.1 Trigger from cameras/encoders on the network. This includes physical inputs or Video analytics triggers from the cameras.

8.2.1.2 System's own motion detection and analytics.

8.2.1.3 3rd Party Devices (e.g. Access control, Fire Panels, Alarm Panels, Point-Of-Sale, etc.).

8.2.1.4 Local user events (events initiated by an operator).

8.2.1.5 Recordings initiated by a time schedule.

8.3 Event Configuration

8.3.1 The system shall have an "AND" function which will prevent triggers occurring unless an event trigger AND an I/O input is present.

8.3.2 The system shall be capable of assigning schedules to an event, during which time the event is considered valid. The event will not be active during times outside of the specified hours in the assigned schedule.

8.3.3 The system shall provide a setting to limit the frequency of triggers.

8.3.4 The system shall provide a setting which discards short event triggers, resulting in events only being triggered if the trigger levels remain high for the duration of (or exceed) the filter period.

8.3.5 The system shall provide a "priority level" setting for events which are to be sent as alarms to the operator interface or alarm management gateway.

8.4 Event Actions

8.4.1 The system shall be able to perform one or more of the following actions upon the receipt of an event trigger:

8.4.1.1 Perform an action either "while" an event is occurring or "when" an event occurs.

8.4.1.2 Record video footage from one or more cameras to a selected database.

8.4.1.3 Record pre-events from one or more cameras.

8.4.1.4 Record synchronised video and audio.

8.4.1.5 Switch or toggle one or more relay outputs which are provided by the system or cameras/encoders connected to the system.

8.4.1.6 “Pulse” one or more relay outputs which are provided by the system or cameras/encoders connected to the system.

8.4.1.7 Control a virtual input.

8.4.1.8 Move one or more PTZ cameras to “preset” positions.

8.4.1.9 Switch one or more selected cameras to one or more selected monitors connected to the system.

8.4.1.10 Switch a camera “layout” to a selected monitor.

8.4.1.11 Record data from a 3rd party system (e.g. Point-Of-sale, Access control, Alarm panels).

8.4.1.12 Initiate a graphical action on a map.

8.4.1.13 Play a pre-recorded audio clip via the local client server OR via an audio output on an I.P. camera or encoder.

8.4.1.14 Send an email to selected recipients.

8.4.1.15 Send an alarm to the operator interface and Alarm Management Gateway (see Section 12).

8.4.1.15.1 Upon sending a notification to an Alarm Gateway, the system shall allow the user to define video previews to be sent with the event notification.

8.4.1.15.2 Events configured with “priority levels” will present users with alarms with corresponding priority levels.

8.4.1.16 Stop a previously initiated action.

8.4.1.17 The system shall allow all actions to be subject to user defined time schedules.

8.4.1.18 The system shall provide the ability to create “event templates” which will enable users to easily associate common actions across multiple cameras.

9 Integration

9.1 General Capabilities

9.1.1 The system shall have the capability to integrate 3rd-party products and devices.

9.1.2 The system shall not run 3rd-party integrations as plug-ins in the client of the software.

9.1.3 The system shall not require additional management servers to run the 3rd-party integration services.

9.1.4 The system shall centralise all integrations to one point in the software.

9.1.5 The system shall be capable of configuring databases specific to each integration, using integration specific drivers. See Databases section for more.

9.1.6 The integration capability will be dependent on the integrated device, but the system shall be capable of the following features:

9.1.6.1 Reception of data from the 3rd party device.

9.1.6.2 Retrieve specific event triggers and perform event actions dependent on specific data received.

9.1.6.3 Store the data in logical fields in a selected database.

9.1.6.4 Associate one or more cameras with integration device objects and their associated events.

9.1.6.5 Display received data as an overlay on the associated cameras in live and review mode (where possible).

9.1.6.6 Display and configure integration device properties, such as:

9.1.6.6.1 Configure integration device objects;

9.1.6.6.2 Set and view status properties of integration device objects;

9.1.6.6.3 View integration device events,

9.1.6.6.4 Configure integration device object groups,

9.1.6.6.5 Configure other integration device settings such as overlays, timeouts, etc.

9.2 Integration Device List

9.2.1 The system shall be capable of integrating with various 3rd party products and devices, including (but not limited) to the following:

9.2.1.1 Access Control;

9.2.1.2 Point-of-Sale;

9.2.1.3 Alarm Panels;

9.2.1.4 Fire Panels;

9.2.1.5 Automatic Number Plate Recognition;

9.2.1.6 Fence and Perimeter Monitoring;

9.2.1.7 Environmental Monitoring;

9.2.1.8 3rd-party Video Analytics;

9.2.1.9 Keyboards and Controllers.

9.2.2 The system shall integrate with I/O devices to control outputs and receive inputs from the I/O devices. These devices may be on a network camera, encoder (server), or on a dedicated network I/O device.

10 Automatic Number Plate Recognition (ANPR)

10.1 General Capabilities

10.1.1 The system shall include automatic license plate recognition as an optional feature.

10.1.2 The system shall integrate with three categories of ANPR engines:

10.1.2.1 3rd-party ANPR algorithms, which send ANPR triggers to CathexisVision;

10.1.2.2 ANPR Cameras, with built in ANPR-detection, which send triggers to the VMS; and

10.1.2.3 ANPR engines which are built-in to the VMS, and which are unlocked with the relevant licenses.

10.1.3 The built-in system shall have the following capabilities:

10.1.3.1 Support multiply libraries of languages and licence plate characters, including Arabic.

10.1.3.2 Support the configuration for detection of number plates for the following detection solutions:

10.1.3.2.1 Triggered Solution, which uses a physical trigger to initiate a detection (such as a ground loop, IR beam or VMD solution), and

10.1.3.2.2 Free Flow Solution, which detects license plates of moving vehicles.

10.1.3.3 Support the overlay of the detected number plate data on the live and recorded video streams.

10.1.4 The system shall include the ability to import/export existing ANPR data in a CSV file format.

10.2 Built-in System ANPR Detectors

10.2.1 The system shall allow multiple ANPR detectors to be configurable within the setup interface on already installed cameras subject to the availability of the required licenses.

10.2.2 The system shall support the following detector options:

10.2.2.1 Camera specific configuration such as resolution and frame rates.

10.2.2.2 Selection of the capture area of the vehicle number plate.

10.2.2.3 Configuration of the number plate character size, slope and slant.

10.2.2.4 Configuration of the number plate analysis based on an input trigger such as a ground loop or on motion.

10.2.2.5 Testing (number plate analysis) of the ANPR configuration using recorded site footage for fine tuning of the algorithm.

10.3 ANPR Rules

10.3.1 The system shall include the ability to group number plate data into specific categories such as Visitors, Staff, Whitelist, Blacklist etc.

10.3.2 The system shall be capable of configuring the following traffic analysis rules which generate system messages when defined traffic patterns are detected:

10.3.2.1 Visit location rule triggers if a license plate is seen at the same location multiple times.

10.3.2.2 Visit area rule triggers if a license plate is seen at multiple locations in a given time period.

10.4 ANPR Events

10.4.1 The system shall be capable of creating events triggered using number plate recognition.

10.4.2 The system shall be capable of configuring events based on the specific licence plate and event data.

10.4.3 The system shall be capable of configuring events based on the specific licence plate group data.

10.4.4 The system shall be capable of triggering event actions which include but are not limited to the triggering of IO devices for access control.

10.4.5 The system shall be capable of generating ANPR event reports:

10.4.5.1 Event reports shall be exportable in a PDF or CSV file format.

10.4.5.2 Event reports shall be generated based on data filters pertaining to vehicle ANPR data.

10.4.5.3 Event reports shall be generated base on specific time periods.

10.5 ANPR Alarms

10.5.1 The system shall be able to generate alarms based on ANPR events, such as:

10.5.1.1 ANPR event data appearing on a data blacklist shall create an alarm.

10.5.1.2 ANPR event data for the same vehicle being recorded multiple times within a specified time period shall create an alarm.

10.5.1.3 ANPR event data for the same vehicle being recorded multiple times within multiple zones within a specific time period shall create an alarm.

11 Alarm Management Gateway

11.1 General Capabilities

11.1.1 The system shall provide an alarm management facility to report and manage local and remote system triggered alarms.

11.1.2 The system shall be capable of connecting to an AMG unit via the operator interface.

11.1.3 The system shall enable systems to be connected using TCP/IP, over LAN/WAN.

11.1.4 The system control room solution shall be capable of bi-directional audio transmission and monitoring.

11.1.5 The alarm management system shall monitor connections to remote units via a site heartbeat at set intervals. It will generate a trigger when a remote alarming unit fails to send its heartbeat.

11.1.6 It shall be possible to send technical and event alarm SMS's from the alarm management system

11.1.7 The alarm interface shall be access-controlled, independent of the rest of the software, and shall have its own user management utility.

11.2 AMG Interface

11.2.1 The system shall allow control room operators to use multiple monitor interfaces, with Alarm, Resources, Map desktops, and other software spread across the monitors.

11.2.2 The system alarm interface shall feature a clearly-visible graphical indicator of the gateway-connection status (connected or disconnected). The system shall be optionally configured so that, on connection, the operator shall see the client-customized desktop / screen configuration, alarm information, and map pertaining to that particular alarm.

11.2.3 The system shall allow configuration of the map so that an event alarm icon flashes at the appropriate point where the alarm was initiated.

11.2.4 The system shall display alarms in separate panes according to status:

11.2.4.1 Incoming (awaiting handling by an operator),
11.2.4.2 Current (being handled by an operator),
11.2.4.3 Archived (already handled by an operator).

11.2.5 The system shall allow incoming alarm audio notifications to be customized.

11.2.6 The system shall display alarms according to priority, indicated by different colours, as configured for event alarms.

11.2.7 In an incoming queue of unhandled alarms, the system shall sound the audio notification of the highest priority alarm for thirty seconds until handled.

11.2.8 Where multiple operators are handling alarms, the system shall keep all operators informed as to an alarm's status, and who is handling which alarm.

11.2.9 Even when navigated away from the alarm-queue desktop, the system shall display an alarm status bar indicating the number of incoming, un-handled alarms by color-coded priority.

11.3 Operator Actions

11.3.1 The system shall allow operators to respond to an alarm and automatically connect to the site from where the alarm initiated.

11.3.2 The system shall be able to temporarily disable (block) repetitive invalid alarms for specified periods. This blocking shall be specified from the gateway unit, and shall require explanatory comment by the blocking operator.

11.3.3 The system shall allow operators to simultaneously clear multiple alarms from the incoming queue.

11.3.4 The system shall allow operators to handle multiple remote alarms simultaneously - a separate interface tab shall represent each connection.

11.3.5 The system shall allow operators to add comments to Current and Archived alarms. To facilitate fast responses, default comments shall be selectable from a menu, but it shall also be possible to add custom text comments.

11.3.6 The system shall allow operators to modify the default comments menu with more appropriate custom comments.

11.3.7 The system shall allow operators to electronically escalate an alarm to a “case”, and assign people to investigate, thereby alerting and involving security management structures.

11.3.8 The system shall notify users to whom cases have been escalated of case assignments.

11.3.9 The system shall allow operators to create a case independently of an alarm.

11.3.10 The system shall provide a case management utility with which to manage cases, enable electronic collaboration between all assigned parties, commit important personnel to the process, and ensure that the case has to be properly resolved/signed off before it can be “closed”.

11.3.11 The system shall allow case managers to further escalate cases, to higher levels of inspection.

11.3.12 The system shall allow operators to filter historical alarms using their associated recordings and metadata. Filter parameters shall include:

11.3.12.1 Alarms, Sessions (where multiple alarms may have been sent through on a single connection).

11.3.12.2 Control-room Operator (based on login information).

11.3.12.3 Cases (alarms that were escalated for further investigation).

11.3.13 The system shall allow operators to double-click an entry (Alarm, Session, Operator Login, Case) from the historical alarms interface, to display a more detailed information/action screen related to that entry, from which it shall be possible to do the following:

11.3.13.1 View alarming site name.

11.3.13.2 View alarming server name.

11.3.13.3 View alarm description.

11.3.13.4 View control-room Operator who handled an alarm or a session.

11.3.13.5 View the name of the control-room unit through which an alarm or session was handled.

11.3.13.6 View time of an alarm event.

11.3.13.7 View time that an alarm event was dispatched to the control room.

11.3.13.8 View an alarm's arrival time at the control room.

11.3.13.9 View time taken to handle an alarm by the control-room Operator.

11.3.13.10 View Comments associated with alarms, sessions and cases.

11.3.13.11 View recordings associated with an alarm.

11.3.13.12 Connect to the historical alarming site to fetch further recordings associated with the alarm, if they still exist in the remote site's database/s.

11.3.13.13 View Cases associated with an alarm.

11.3.13.14 Show the entire Session in which an alarm was handled.

11.3.13.15 Add further Comments to historical alarms, sessions and cases.

11.3.13.16 Escalate a historical alarm to a Case for further investigation and resolution.

11.3.13.17 Show control-room Operator logins associated with an alarm session.

11.3.13.18 View all alarms associated with a session.

11.3.13.19 View a control-room Operator's login duration, start time and end time.

11.3.13.20 View the number of Sessions handled by a control-room Operator during a Login.

11.3.13.21 View all Sessions handled by a control-room Operator during a Login.

11.3.13.22 View a Case description.

11.3.13.23 View the name of the user who escalated an alarm to a Case, with the date-time.

11.3.13.24 View the name of the user who closed a Case, with the date-time.

11.3.13.25 View a list of Case users, with their Status relating to a Case (Active - still working on it, or Inactive – no longer working on it).

11.3.13.26 View a Timeline of user actions relating to a Case.

11.3.13.27 View the Status of a Case.

11.3.13.28 View all Alarms associated with a Case.

11.3.13.29 View all Comments associated with a Case.

11.4 AMG Reporting

11.4.1 The system shall provide detailed, customizable reports based on connections, response times, logins, and handling times.

11.4.2 The system shall establish an audit trail and timeline of case responses.

11.4.3 The system shall record operator logins, and responses to incoming calls, and protect this information from manipulation.

11.4.4 The system shall be capable of scheduling the system to run reports automatically, and to perform automated actions with the reports, such as emailing the report to recipients.

12 Integrated Keyboard

12.1 Native Keyboard/Controller

12.1.1 The system shall feature an integrated keyboard control.

12.1.2 The system shall allow the pan/tilt/zoom sensitivity to be configured in the software.

12.1.3 The keyboard shall feature fast key-selection of cameras, presets, monitors, outputs, camera tours (sequences) and screen layouts.

12.1.4 PTZ camera function buttons shall be accessible to the fingers of the joystick hand, so that operators need not relinquish control of the joystick.

12.1.5 The keyboard LCD display shall be writable by the digital surveillance system.

12.1.6 The keyboard key LEDs shall indicate the state of keys and functions.

12.2 Third-Party Keyboard/Controller

12.2.1 The system shall support the integration of third-party keyboards and controllers.

13 Databases

13.1 General Capabilities

13.1.1 The system shall provide quick and easy access to all databases from within the operator interface.

13.1.2 The system shall allow multiple databases to be configured, and multiple cameras and/or camera groups to be directed to one or more databases.

13.1.3 The system shall restrict viewing of database entries by only allowing users with the appropriate camera-view access rights to view certain cameras in the database.

13.2 Video Database

13.2.1 The system shall provide a proprietary video database system, not reliant on third-party database engines (such as PostgreSQL and MySQL).

13.2.2 The system shall be split databases across multiple disks and/or network storage devices.

13.2.3 The system shall continue writing to a database even if one/multiple disks fail.

13.2.4 The system supports the following database features:

13.2.4.1 Variable disk sizes

13.2.4.2 Distribute writing load across multiple disks.

13.2.4.3 Databases can be exported and moved from one NVR to another.

13.2.4.4 Expansion of existing database by adding more storage space.

13.2.4.5 Provide recoverability from file system corruption with minimal data loss.

13.2.5 The system shall be able to view database entries according to date and time stamp selection.

13.2.6 The system shall allow a maximum recording period to be configured.

13.3 Integration Database

13.3.1 The system shall be capable of creating dedicated integration databases for each integration. The integration databases shall:

13.3.1.1 Have an integrated video player.

13.3.1.2 Link the integrated device data with the video data pulled through from associated cameras.

13.3.1.3 Play back video and data simultaneously and synchronously in the integrated database video player.

13.3.1.4 Display all cameras associated with device events.

13.3.1.5 Perform an ‘easy search’ via a drop-down user interface which instantly filters the entries according to the available easy-search options (unique to each integration).

13.3.1.6 Provide the ability to “mine” the database to find selected data/transactions and the associated video data, using integration specific filters and view/search/sort options.

13.3.1.7 Be capable of exporting database entries in PDF and CSV file format.

13.3.1.8 Be capable of archiving video and associated meta-data from the integration database video player.

13.4 System Events Database

13.4.1 The system shall be capable of creating an event-specific database to which all system events are directed automatically.

13.4.2 It is not necessary to configure an event action to record to the events database in order for an event to be directed to the events database.

13.5 ANPR Integration Database

13.5.1 The system shall be capable of creating a designated ANPR integration database.

13.5.2 The system shall be able to view, sort and 'easy-search' the ANPR database by the following:

13.5.2.1 License plates.

13.5.2.2 License plate groups.

13.5.2.3 ANPR (LPR) detectors.

13.5.3 The system shall be able to filter the ANPR database by a number of options, including but not limited to the following:

13.5.3.1 Time/Date.

13.5.3.2 License plates/Groups

13.5.3.3 Confidence (license plate capture accuracy in percentage).

13.5.3.4 ANPR detector.

13.5.3.5 Camera.

13.5.3.6 Driver/company name.

13.5.3.7 Vehicle type/make/model/colour.

13.5.3.8 Place of Issue (region specific)

13.5.3.9 Background colour, text colour and shape of license plate.

13.5.3.10 Position of license plate on car (front/back).

13.5.3.11 Position of car in lane (entry/exit).

14 Failover

14.1 General Capabilities

14.1.1 The system shall be capable of n:1 and n:n server failover.

14.1.1.1 A failover server can assume the functions of any failed server.

14.1.1.2 A hot-spare structure will be used to accomplish this.

14.1.2 The system shall be capable of failing over the Master/Management Server, and all associated functions, including but not limited to:

14.1.2.1 Recording and reviewing video.

14.1.2.2 Viewing live video, including video wall control functions.

14.1.2.3 Events configuration and management.

14.1.3 The system shall provide the option of a simple failover setup during the installation process of the VMS software.

14.1.4 The system shall provide a failover database which resides on the failover server itself

14.2 Failover Process

14.2.1 The failover server will continually monitor management and recording servers.

14.2.2 The failover server will assume the functionality of a failed server, allowing site functions to continue.

14.2.3 The system will automatically re-insert video on the original recording server’s database on recovery of the failed server.

14.2.4 The system shall generate an alarm if a site server fails and is failed-over.

14.2.5 The system shall generate an alarm if a failover server is down.

14.2.6 The system shall provide a Site Overview feature which displays all site servers, indicating the server being failed-over.

15 System Health

15.1 Technical Reports

15.1.1 The system shall offer extensive reporting on hardware and software comprising the site by keeping technical logs and allowing for the generation of technical reports.

15.1.2 The system shall restrict access to configuration of technical reports to administrators only.

15.1.3 The system shall allow users to save their reports as “templates” for easy generation of future reports.

15.1.4 The system shall allow users to export reports in compressed html format.

15.1.4.1 In html format, the system shall allow automatic generation of a table of contents, and hyperlinks to sections.

15.1.5 The system shall allow reports to be emailed, printed, and archived (saved).

15.1.6 The system shall be capable of automatically compiling and emailing selected reports to selected recipients according to a specified schedule.

15.1.7 The system shall be capable of generating server/hardware-specific technical reports on the following:

15.1.7.1 Camera failures, logs, status and time to repair.

15.1.7.2 Database Usage:

15.1.7.2.1 Breakdown by camera.

15.1.7.2.2 Rate by camera/hour/camera per hour.

15.1.7.2.3 Event frequency histogram.

15.1.7.2.4 Events by hour.

15.1.7.3 Disk.

15.1.7.4 Environment.

15.1.7.5 Events.

15.1.7.6 File Systems.

15.1.7.7 Hardware.

15.1.7.8 License Features.

15.1.7.9 Licenses.

15.1.7.10 NTP Queries.

15.1.7.11 Reboots and cause of reboots, including:

15.1.7.12 Software server reboots.

15.1.7.13 Power failure reboots.

15.1.7.14 User reboots.

15.1.7.15 Remote user reboots.

15.1.7.16 Time of reboot.

15.1.7.17 Recording setup and configuration, times (of the system per camera), and recording failures.

15.1.7.18 System setup and configuration.

15.1.7.19 Software server failures.

15.1.7.20 Unit Up-time.

15.1.7.21 VMX:

15.1.7.21.1 Counters.

15.1.7.21.2 Temperatures.

15.2 Technical Alarms

15.2.1 The system shall be capable of generating server/hardware-specific technical alarms, including but not limited to:

15.2.1.1 Heartbeat failure alarms.

15.2.1.2 Camera faults, if:

15.2.1.2.1 E.g. Cameras failed more than a specified number of times in a specified time period.

15.2.1.2.2 E.g. Cameras were down for more than a specified percentage of time in a specified period.

15.2.1.3 Database alarms (generated when an event triggers but no video is received).

15.2.1.4 Disk alarms.

15.2.1.4.1 E.g. Hard drive SMART parameters outside system required norms.

15.2.1.5 Environment alarms (server/hardware-dependent).

15.2.1.5.1 E.g., Temperature, fan speed.

15.2.1.6 Failover alarms.

15.2.1.7 Server is failed over.

15.2.1.8 Failover server fails.

15.2.1.9 Integration database alarms.

15.2.1.10 Network I/O alarms.

15.2.1.11 Network Connectivity alarms.

15.2.1.11.1 E.g. If a communications medium has failed, such as Ethernet or Modem.

15.2.1.11.2 E.g. If an automated routine Alarm Management Gateway ping of a capture station has failed.

15.2.1.12 Reboot alarms, E.g. If the reboot frequency is unusually high.

15.2.1.13 Recording period/failure alarms.

15.2.1.13.1 E.g. If the number of recorded events on any particular day is less than it should be (based on an historical mean), indicating a possible technical fault.

15.2.1.14 Scheduled archive alarm.

15.2.1.15 Server monitoring alarm.

15.2.1.15.1 E.g. If an unusual shutdown sequence has occurred (e.g. a user pulls out the power lead).

15.2.1.15.2 E.g. All systems shall continuously test all other systems on the site for “up-time” and if any systems do not respond, then an alarm may be sent.

15.2.1.16 Software failure alarm.

15.2.1.17 Test alarm.

15.2.1.18 It shall be possible to trigger a test technical alarm from a single unit within a site of units.

15.2.1.19 The sending of alarms shall have filters to enable users to limit the number of alarms sent. These settings shall include:

15.2.1.19.1 Send alarm each time an event occurs.

15.2.1.19.2 Send alarm immediately and then every specified time period.

15.2.1.19.3 Send alarm once only.

16 Audit Logs

16.1 General Capabilities

16.1.1 The system shall allow site and servers to be audited, providing an historical log of all user-based actions.

16.1.2 The system shall restrict access to auditing sites and servers to administrators only.

16.1.3 The system shall allow audit logs to be filtered by the following:

16.1.3.1 Time/Time Period
16.1.3.2 Users
16.1.3.3 Resources
16.1.3.4 User Actions

16.1.4 The system shall allow audit logs filtered by users to display a historical log of operator actions, across all user login names.

16.1.5 The system shall allow audit logs to be exported in CSV file format.

17 Forensic Tool

17.1 General Capabilities

17.1.1 The system shall have provision for a forensic tool which offers site analysis and troubleshooting to obtain the following historical site server data:

17.1.1.1 Network camera summary – total network throughput, drop ratio, and count of camera stalls.

17.1.1.2 Database writes - disk writing bitrate, and drops to local or network storage.

17.1.1.3 Dropped packets – external network, internal UDP between servers, and internal video frames.

17.1.1.4 Video streaming – sent, received, and decoded for live viewing.

17.1.1.5 Software compressor – encoded and decoded pixel rate, and percentage of frames.

17.1.1.6 Internal messaging – UDP packets missed and received between processes, and number of logs per minute sent.

17.1.1.7 Video frames – missed and received between internal processes.

17.1.1.8 The system shall have provision for a forensic tool to troubleshoot and obtain the following historical camera-specific data:

17.1.1.9 Network cameras – bitrate, dropped packets, cameras stalls, camera down, and number of events per camera.

17.1.1.10 Database cameras – bitrate, bytes written to disk, camera down, and number of events per camera.

17.1.2 The system shall have provision to present the forensic data in a graphical format based on the following:

17.1.2.1 Date and time selection.

17.1.2.2 Time frame selection.

17.1.2.3 The system shall have provision whilst in the Graph Window to facilitate the following:

17.1.2.4 Zoom in on a time period of data.

17.1.2.5 View the data values.

17.1.2.6 Export as a Comma Separated Values (CSV) file.

18 Map Editor

18.1 Map Editor Software

18.1.1 General Capabilities

18.1.1.1 The system shall automatically install a multi-layer interactive map facility upon installation of the VMS server/client software.

18.1.1.2 The map facility shall be hierarchical with “drill-down” capability.

18.1.2 Interface

18.1.2.1 The Map Editor interface shall be able to do the following:

18.1.2.2 Add/configure map objects (such as shapes, images and text).

18.1.2.3 Add site resources to map (such as cameras, integration devices, events).

18.1.2.4 Add actions to map objects.

18.1.2.5 Connect to site(s) and view site resources.

18.1.3 Functions

18.1.3.1 The system shall include, but is not limited to, the following map creator functions:

18.1.3.1.1 Map Setup Wizard to offer a quick-create feature.

18.1.3.1.2 Importing of graphics in JPG or PNG format.

18.1.3.1.3 Create hyperlinks from within the map to other site maps.

18.1.3.1.4 Map objects can be configured to perform map actions upon the receipt of certain triggers.

18.1.3.1.5 Map layers; Layers have transparency / hide- show options.

18.1.3.1.6 Ability to associate layers with preset PTZ positions.

18.1.3.1.7 Ability to switch layers on or off in response to a system event (e.g. to indicate a door opening/closing).

18.1.3.1.8 PTZ with associated, editable presets.

18.1.3.1.9 Drag all available site resources from a site resources list directly to the map.

18.1.3.1.10 Adding cameras with drag-and-drop icons (fixed or PTZ).

18.1.3.1.11 Adding of I/O via drag-and-drop icons.

18.1.4 Map Object Actions

18.1.4.1 Map objects can be configured to perform certain actions upon the receipt of certain triggers. Examples of triggers which can trigger a map object action include, but are not limited to, the following:

18.1.4.1.1 Left-click in Map tab in VMS user interface.

18.1.4.1.2 Right-click in Map Tab in VMS user interface.

18.1.4.1.3 Input change,

18.1.4.1.4 Device status change,

18.1.4.1.5 Integration device events.

18.1.4.1.6 Examples of actions which map objects can perform when a trigger is received include, but are not limited to, the following:

18.1.4.1.7 Connect to a Site,

18.1.4.1.8 Go to a camera preset,
18.1.4.1.9 Perform an Animation,
18.1.4.1.10 Show a popup menu,
18.1.4.1.11 Set a relay output.

18.2 Maps in VMS Operator Interface

18.2.1 The system shall allow maps created in the Map Editor software and saved to be uploaded to the Map Tab in the VMS operator interface.

18.2.2 The system shall allow multiple maps to be added to a site.

18.2.3 The system shall optionally enable remote users to automatically view the site map.

18.2.4 The system shall enable remote clients to download and store the maps locally to remove the need to download the map for each connection.

18.2.5 The system shall allow site maps to be managed, which involves:
18.2.5.1 Setting a default map,
18.2.5.2 Deleting maps,
18.2.5.3 Adding maps.

18.2.6 The system shall allow all map object actions which were configured for the object in the Map Editor software to be visible/working/interactive (where relevant) in the map in the VMS user interface.

18.2.7 The system shall allow the user to:
18.2.7.1 Zoom in/out of the map,
18.2.7.2 Drag-and-drop cameras from the map to monitors for viewing,
18.2.7.3 Hide/show map objects,
18.2.7.4 Hide/show/change transparency of layers.

19 Mobile App

19.1 General Capabilities

19.1.1 The system shall provide a free mobile application.

19.1.2 The system shall not require the installation of extra server-side software, additional plug-ins, or a special mobile server to enable the mobile viewing and reviewing of video.

19.1.3 The system shall make this application available on the Apple iStore and Google Play Store.

19.1.3.1 It shall be accessible via an HTTP interface.

19.1.4 The app shall support the following functions:

19.1.4.1 PTZ control of cameras.

19.1.4.2 Zooming in/out.

19.1.4.3 I/O Control.

19.1.4.4 Multiple camera view (up to four cameras).

19.1.4.5 Save details for multiple servers.

20 Application Programming Interface

20.1 General Capabilities

20.1.1 The system shall include an Application Protocol Interface (API) which shall enable third party software to retrieve and manage information from the VMS, as well as control system resources.

20.2 Site List Information

20.2.1 The system shall include the following regarding List Site information:

20.2.1.1 Access to the site shall be via digest authentication, and restricted based on the user's preconfigured access levels. The API shall have access to the details of the site, via the login server. This includes the Site's name and unique identification number.

20.2.2 The system shall include the following regarding Camera Resources:

20.2.2.1 The API shall provide the ability to list all cameras and camera resources on a site.

20.2.3 Camera feed information must contain the following:

20.2.3.1 Name
20.2.3.2 Unique ID
20.2.3.3 Audio feed (yes/no)
20.2.3.4 Access level information
20.2.3.5 PTZ status
20.2.3.6 Patterns/pre-set information
20.2.3.7 Live video track information
20.2.3.8 Review video track information

20.2.4 The system shall include the following regarding Live Feed Streaming:

20.2.4.1 The API shall allow for live camera video feed streaming, using RTSP protocol.

20.2.4.2 Live video feed streaming shall require client authentication.

20.2.4.3 Switch cameras to monitors.

20.2.5 The system shall include the following regarding Camera Review:

20.2.5.1 The API shall allow for the review of recorded video footage.

20.2.5.2 This shall be accessed via the RTSP protocol.

20.2.5.3 The API must allow for review video footage to be retrieved from a specific date and time.

20.2.5.3.1 If no video footage is present at the time specified, the server will return the video footage closest to the time requested.

20.2.5.4 The API must allow for a field in the request which will make the session transmit as fast as the client/connection will allow.

20.2.5.5 The following streaming transports shall be supported:

20.2.5.5.1 RTP over UDP.

20.2.5.5.2 RTP over TCP.

20.2.6 The system shall include the following regarding Audio Call/Listen:

20.2.6.1 The API shall allow for the streaming of independent audio inputs and outputs to and from the audio inputs and outputs on the server.

20.2.6.2 'Independent' here means that the audio shall not be tied to video.

20.2.6.3 This shall be done over SIP protocol.

20.2.7 The API shall allow the following control over PTZ cameras:

20.2.7.1 Move

20.2.7.2 Go to preset

20.2.7.3 Save preset

20.2.7.4 Focus/iris control

20.2.7.5 Run preset pattern (tour)

20.2.7.6 The control of the PTZ shall be via HTTP.

20.2.8 The system shall include the following regarding Input/Output Resource Management (HTTP; monitor I/O resource state changes, control outputs):

20.2.8.1 The API shall support monitoring of all site I/O's.

20.2.8.2 On request the API will provide all current site I/O's.

20.2.8.3 The API will also maintain an open connection, for as long as the client wishes, and update I/O resources via this connection. These updates will be:

20.2.8.3.1 Resource state changes

20.2.8.3.2 Resource added

20.2.8.3.3 Resource removed

20.2.8.3.4 Resource modified (name changed)

20.2.8.3.5 Output controls shall be Set, Clear, and Pulse.

20.2.9 The system shall include the following regarding Event/Technical Alarm Reception:

20.2.9.1 The API shall allow for the reception of alarms from the server. Both Technical Alarms (alarms related to the functioning of the site), and Event alarms (alarms triggered by VMS and I/O events).

20.2.9.2 The server shall deliver the following alarm information:

20.2.9.2.1 Source site ID

20.2.9.2.2 Source site name

20.2.9.2.3 Alarm type (technical/event)

20.2.9.2.4 Alarm name

20.2.9.2.5 Associated camera resources.