DIGITAL VIDEO MANAGEMENT SYSTEM SPECIFICATION VERSION 3

1.	**GENERAL**	**4**
1.1	**Database Servers**	**5**
1.2	**Distributed Video System Architecture**	**6**
1.3	**Camera Servers**	**6**
1.4	**Video Analytics Servers**	**9**
1.5	**Security System**	**9**
1.6	**Integrated building management and Control System**	**10**
1.7	**Industrial Control System**	**11**
1.8	**Operator Station**	**12**
1.9	**System Sizing**	**12**
2.	**HARDWARE**	**13**
2.1	**Database Server**	**13**
2.2	**Camera Server (Preferred and Backup)**	**14**
2.3	**Mobile Video Streaming Server**	**15**
2.4	**Video analytics Server**	**15**
2.5	**Multiprocessor Support**	**16**
2.6	**System Fault Tolerance**	**16**
2.7	**Operator Interface**	**16**
2.8	**Device support: network cameras and video encoders**	**19**
2.9	**Network and Video Cabling**	**20**
3.	**SYSTEM SOFTWARE**	**22**
3.1	**Database Server**	**22**
3.2	**Camera Server**	**22**
3.3	**Video analytics Server**	**22**
3.4	**Mobile video streaming server**	**22**
3.5	**Security Server**	**22**
3.6	**integrated Building management and Control Server**	**23**
3.7	**Industrial process control System Server**	**23**
3.8	**Integrated Operator Station**	**23**
3.9	**Network**	**23**
4.	**APPLICATION SOFTWARE FUNCTIONS**	**24**
4.1	**Surveillance client operation**	**24**
4.2	**Alarm and Spot monitors**	**34**
4.3	**Video Loss Alarm**	**35**
4.4	**Camera Tamper Detection**	**35**
4.5	**Camera settings**	**35**
4.6	**Recording video**	**38**

4.7 Device configuration redundancy 49
4.8 Privacy 50
4.9 Digital Zoom and Image Enhancement 50
4.10 System and User Audit Trail 51
4.11 Storage 51
4.12 Integrated Operator Station 52
4.13 Image Blocking 54
4.14 Network 55
4.15 International Language Support 55
4.16 Application Development Interface 55
4.17 System diagnostics 55
4.18 System Maintenance 56
5. SERVICES 57
5.1 Training 57
5.2 Configuration Services 57
5.3 Installation Services 57
5.4 Hardware Maintenance 57
5.5 Software Enhancement & Software Support 57

1. GENERAL

The Digital Video Management System (DVMS) shall be designed and developed to the following standards:

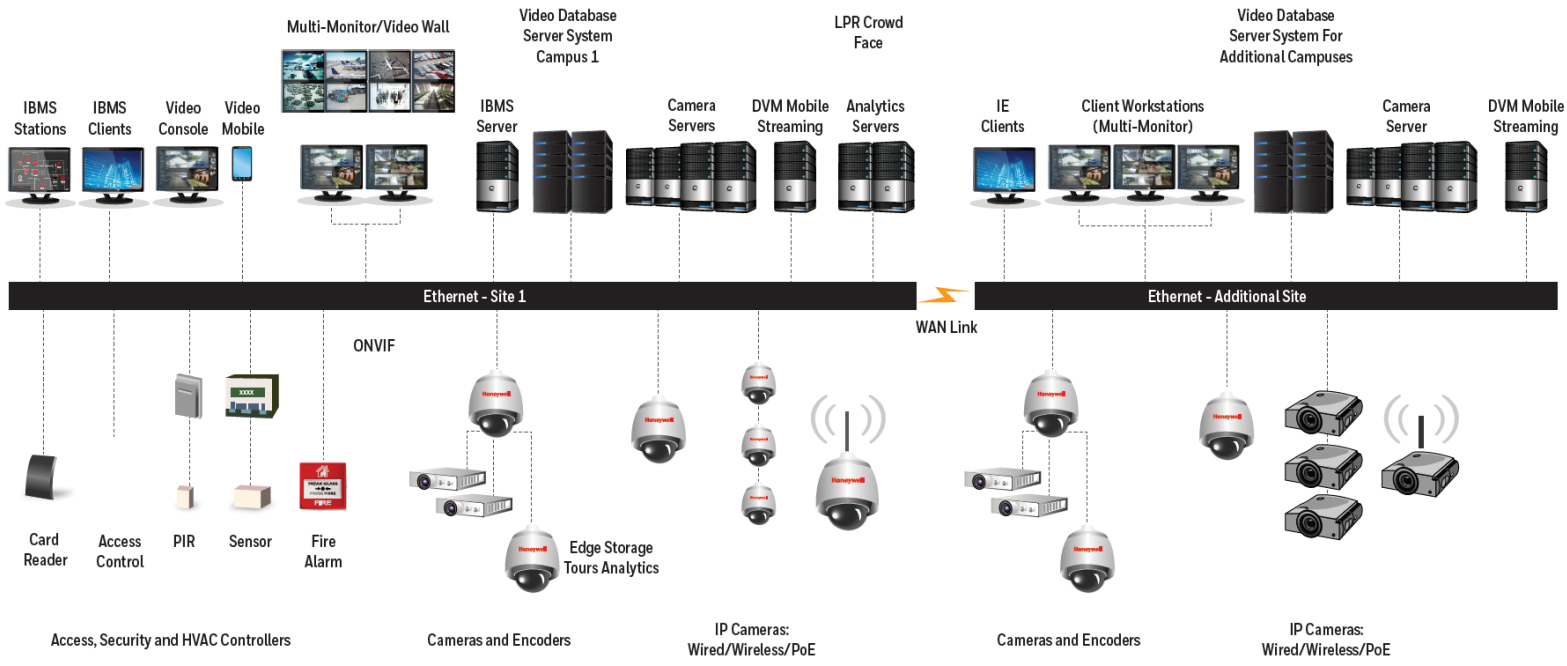
- ISO 9001 (2015)
- ISO/IEC 15504 Level 3 or higher
  (SPICE 2.0 Software Process Improvement and Capability Determination)
- SEI CMM Level 5 or higher
  (American Software Engineering Institute - Capability Maturity Model)

Evidence of at least 10 years of certified adherence to an internationally accepted quality management standard used by the vendor's development organisation shall be provided.

The Digital Video Management System shall include:

- (Redundant) Database Servers
- (Redundant) Camera Servers
- Mobile Client Video Streaming Servers
- Video Analytics Servers
- Security or Control Systems
- Operator Stations
- IP Connected Keyboards
- Network connected cameras and/or network connected video encoders
- Network infrastructure, including network-based storage solutions

The following diagram explains the relationship of these system components:



1.1 DATABASE SERVERS

The database server shall provide a central fault tolerant repository for all configuration and run time information for the complete system.

1.1.1 DATABASE SERVER TASKS

The Database Server shall:

- Manage the system database containing:
    - System configuration
    - System Redundancy configuration for both Database and Camera Servers
    - Distributed system data for connection to remote Digital Video Management Systems
    - Details of IP Camera and/or Encoder functional capabilities
    - Camera configuration and settings
    - Video Encoder and/or IP Camera Input/Output configuration and settings
    - Video stream profile configuration for Live and Recorded video
    - Details of run time information such as recordings and audit logs
    - Configuration of operator views showing multiple camera layouts
    - Schedules for recording, Input monitoring, Output switching and video analytics
    - Operator security details
    - Configuration of Surveillance and Alarm Monitors
    - Configuration of IP CCTV Keyboards
    - Configuration of Video Analytics including:
        - Video Motion Detection
        - Intelligent Video Analytics
        - Camera Tamper Detection
    - Configuration of Video Wall Clients
- Manage communication between the Operator Stations and the Camera Servers
- Allow alarms/events in the Security System or Control System to initiate recordings
- Support connection to multiple Security System or Control System servers simultaneously
- Each connected server shall be able to receive alarms, activate events and view live or recorded video from the DVMS
- Report any camera failures or recording failures to the integrated Control system or Security system
- Provide a full audit log of system activity including system status and operator actions.
- The Database Server shall use Microsoft SQL Server 2017 as the database engine. No other database type shall be permitted.
- Use Microsoft Windows Active Directory to manage access to the system

The Database Server shall be able to be used in a redundant configuration, using two separate Database Servers (being executed on separate computers). The backup Database Server shall be continuously synchronised with the master Database Server to ensure that it is always up-to-date and ready for a fail-over, when required.

1.1.2 REDUNDANT DATABASE SERVER

The DVMS must be capable of running a pair of similarly configured computers in a hot backup configuration where at any point in time, one is the acting Primary and the other is acting as the Hot Backup. An on-line database duplication mechanism must be supported.

Simply having each Database Server scan each Camera Sever or requiring the Camera Servers send all updates to both Database Servers is not acceptable. The database duplication must be performed on a per-transaction basis for two reasons:

- To ensure that the duplicated Backup database is always consistent with the Primary database
- To avoid unnecessary loading of Camera Servers caused by duplicate polling

It must be possible to remove one of the redundant systems for maintenance without interrupting operation, and upon its reinstatement, automatically re-synchronize the databases, again without interruption to system operation.

Deviations to the above method of achieving Database Server Redundancy shall not be acceptable. This includes, but it not limited to:

- Clustering shall not be an acceptable means of achieving Redundancy for the Database Server.
- Redundant hardware platforms will not be an acceptable means of achieving Redundancy.
- Virtualisation shall not be an acceptable means of achieving Redundancy for the Database Server

1.2 DISTRIBUTED VIDEO SYSTEM ARCHITECTURE

It shall be possible to connect multiple database servers together to allow sharing of live and recorded video between systems in a distributed video system architecture.

The link between the systems shall be configurable to allow the transmission of video data and/or system event and status information.

Operators configured on one of the distributed systems (their local system) shall be able to view live and recorded video on the one or more of the other distributed systems (remote systems) based on their security configuration. Operators shall also be allowed to control cameras with Pan/Tilt/Zoom functionality on the remote systems.

Cameras from remote systems shall be presented to the operator in the same User Interface as their local system. Systems requiring a second instance of the Operator User Interface or break in the connection to the existing system to allow display of remote cameras shall not be acceptable.

It shall not be possible for operators to configure cameras on the remote systems. All system configuration and administration must be performed on each local system to maintain system security and integrity.

It shall be possible to connect systems together even when on different releases, up to 2 releases prior to the most recent release of product used in the unified system.

1.3 CAMERA SERVERS

The DVMS shall support two types of Camera Servers:

- Preferred Camera Servers
- Backup Camera Servers

The DVMS shall support Camera Server Redundancy by allowing the configuration of Backup Camera Servers which can assume the role of the Preferred Camera Server if the Preferred Camera Server is no longer operational.

Camera Servers shall rely on the Database Server for all camera database and configuration information.

The system shall support multiple Camera Servers, with no software-imposed limit to the number of Camera Servers used in the DVMS.

1.3.1 PREFERRED CAMERA SERVERS

The Preferred Camera Server(s) manage all camera operations during normal operation of the system. They must be capable of supporting a large amount of disk space for online video storage and access to high capacity archiving mechanisms for the transfer of stored video to off-line media.

1.3.1.1 Preferred Camera Server Tasks

The Camera Server shall:

- Manage live video and/or video and audio from Video Encoders and IP Cameras
- Transmit live and/or recorded video and audio/video to Operator Stations
- Transmit live video to Surveillance Monitors or Alarm Monitors
- Transmit live video to the Analytics Server(s) for processing using video analytics algorithms
- Receive analytics events from the Analytics Server(s) and perform actions on these events based on pre-configured settings
- Receive camera control commands from Operator Stations or Operator Keyboards and then send the commands to cameras
- Store live video and/or video and audio to hard disk
- Transmit previously recorded video and/or audio/video to Operator Stations
- Archive previously stored video and/or audio/video to media storage location for later archiving
- Retrieve archived video and/or audio/video from storage media
- Analyse live video for events of interest using both simple and advanced Video Motion Detection algorithms
- Export recordings in a format supported by standard video players in either transcoded or non-transcoded format. The following encoding file formats shall be supported:
    - Non-transcoded exports: Advanced System Format (asf) or MPEG-4 Part 14 (MP4)
    - Transcoded exports: Windows Media Video (wmv)or Audio Video Interleave (AVI)
- Provide the ability to monitor cameras for tampering including:
    - Changed field of view
    - Blurred image
    - Camera blinded or covered
- Receive input events from the digital input ports of IP cameras or video encoders and react to these events in a pre-configured manner including but not limited to:
    - Start recordings on 1 or more cameras
    - Send alarms to the Security System or Control System
- Transmit output commands to the output port(s) of the IP cameras or video encoders
- Facilitate intercom functionality by routing video and audio from the field to the relevant operator station and routing audio from the operator station to the relevant field device.
- Monitor the video loss status of analogue video feeds connected to IP encoders. The video loss status of an analogue video feed shall be represented on the user interface in a readily accessible manner

The DVMS ability to replay recorded video shall not be affected by the operational status of the Camera Server that performed the original recording. If the original recording Camera Server is not available, any operational Camera Server shall be able to support the replay of the applicable recorded video provided that it has logical access to the video data files.

1.3.2 BACKUP CAMERA SERVERS

The Backup Camera Server(s) provides redundancy at the Camera Server level for the DVMS.

It shall be possible to define pools of Backup Camera Servers containing one (1) or more Backup Camera Servers. The pools of Backup Camera Servers shall be assignable to specific Preferred Camera Servers.

It shall be possible to define and modify the order of Servers in the pool which will define the order in which Backup Camera Server assume control of failed Preferred Camera Servers. The system shall also include a default Backup Camera Server pool that contains all Backup Camera Servers without the need for additional configuration.

Systems that only support a one-to-one relationship between Preferred and Backup Camera Servers will not be acceptable.

The first available Backup Camera Server in the Preferred Camera Servers assigned backup pool shall assume the role of the Preferred Camera Server if the Preferred Camera Server is not available. If the Backup Camera Server fails, the next available Camera Server in the backup pool shall assume the role of the failed server.

All cameras and Input/Output devices managed by the Preferred Camera Server shall be transferred to the Backup Camera Server on failover.

Once a Backup Camera Server has assumed the role of the Preferred Camera Server, it shall no longer be available to back up any other Preferred Camera Servers until the original Preferred Camera Server operation has been restored.

The user interface shall provide a summary of the current status of the overall system indicating the number of primary camera servers, number of backup camera servers and the status of each.

For ease of configuration, Camera Server Redundancy configuration must be performed at the camera server level and not configurable per camera. Systems that require the individual configuration of a Backup Camera Server per camera will not be acceptable.

1.3.2.1 Available Functionality after Failover

The following functionality continues to be available after a Camera Server failover:

- Live video, including PTZ and camera control
- Processing of Video Analytics
- Processing of Camera Tamper Detection
- Video recordings, including scheduled recordings
- Recording playback, including searching for recordings when video was recorded to a network location
- Archive, restore, delete and export of video clips when video was recorded to a network location
- Intercom
- Triggering of input and output devices, including scheduled triggering
- Video Loss Alarms

The failover of cameras between Preferred and Backup Camera Servers shall be transparent to system Operators and shall not require the operator to reconnect their Operator Station to re-establish access to live or recorded video.

1.3.2.2 Failover and Fail Back Mechanism

The failover and fail back mechanism between Preferred and Backup Camera Servers shall be configurable and support both automatic and manual operation.

Automatic failover shall be triggered by the system in the following instances:

- The system detects that the Camera Server does not have an available, healthy storage volume for recordings
- The Camera Server has suffered a deadlock in operation
- The free space for a recording location has reached a minimum predefined threshold

Manual failover and fail back support shall always be available if required via a button on the Operator User Interface, provided the Operator has the correct security level.

It shall be possible to enable or disable the use of automatic failover for each Preferred Camera Server individually. When enabled, it shall also be possible to set the duration of the delay period that the Preferred Camera Server must be in a failed state after which the DVMS shall initiate a failover. It shall also be possible to set the level of alarm associated with a Preferred Camera Server failure event.

It shall be possible to enable or disable the use of automatic fail back for each Preferred Camera Server individually. When enabled, it shall also be possible to set the duration of the delay period that the Preferred Camera Server must be in a healthy state after which the DVMS shall initiate a fail back. It shall also be possible to set the level of alarm associated with a Preferred Camera Server fail back event.

Systems that enforce system-wide settings for failover and fail back operation shall not be acceptable.

1.4 VIDEO ANALYTICS SERVERS

The Video Analytics (VA) Server(s) must be dedicated to analysing video of interest streamed from the Camera Server(s) only. The VA Server(s) shall not be used to record video footage but shall pass event information from the analysis of the video streams back to the Camera Server(s) supplying the video for analysis for further action.

The VA Server shall:

- Receive live video from Camera Servers
- Process the live video using preconfigured rules and Intelligent video content analysis algorithms to determine events of interest
- Transmit Intelligent video content analysis event information to the Camera Servers
- Provide video content analysis including:
    - Video Motion Detection
    - Advanced Intelligent Video Content Analysis
- Provide the ability to monitor cameras for potential tampering including:
    - Changed field of view
    - Blurred image
    - Camera blinded or covered

The VA Server shall not be used to record live video or transmit any video – live or recorded – to any other part of the DVMS.

The system shall support multiple VA Servers, with no limit to the number of VA Servers used in the DVMS.

1.5 SECURITY SYSTEM

The Security System is specified in other project documents. It shall be based on Honeywell Command & Control Suite and Enterprise Buildings Integrator (EBI) or equivalent.

The Security System monitors and controls Security and Access. It provides a real-time view of the status of the security system to operators using dedicated Operator Station machines.

In relation to the DVMS system, the Security System shall:

- Limit and grant operators access to live and recorded video images
- Send requests to record video
- Command PTZ cameras to preset positions based on events within the Security System
- Provide indication of any cameras or recordings which have failed

- Provide a link in its alarm list directly to any associated video recording. Clicking on the link shall call up a pop-up window that allows the operator to replay the video without the need to navigate to the DVMS.
- Provide the ability to develop custom displays with video and video controls integrated within the displays for the display of live and recorded video
- Provides an ability to report on system activity and configuration using customizable reports
- Present all DVMS system alarms to the security system operator

Integration to the Security System shall be provided by the DVMS manufacturer and shall be a standard component of the DVMS software. Solutions that are not yet integrated and require the development of integration – with or without a manufacturer's Software Development Kit (SDK) or Application Programming Interface (API) – for the purpose of the project shall not be acceptable. System integration shall be via a High Level Interface (HLI) and not be based on any of the following: hard-wiring and or so-called "open protocols" such as, but not limited to, BACnet, Modbus or OPC.

The integration between DVMS and Security System must be maintained by the vendor. Any updates to the integration required for future releases of either the Security System or DVMS software shall be managed as part of the respective products development and testing programs.

Proposal of systems that do not have proven examples of integration between both systems operationally available for at minimum 2 years shall result in disqualification of the proposal.

The proposed DVMS and Security System shall have been deployed together as an integrated solution on more than 1,000 customer sites globally.

1.6 INTEGRATED BUILDING MANAGEMENT AND CONTROL SYSTEM

The Building Control System is specified in other project documents. It shall be based on the Honeywell Enterprise Buildings Integrator (EBI) or equivalent.

The Building Control System monitors and controls HVAC, lighting, fire panels[1] and other building assets. It provides a real-time view of the status of the building control system to operators using dedicated Operator Station machines.

- In relation to the DVMS System, the Building Control System shall:
- Limit and grant operator access to live and recorded video images.
- Send requests to record video
- Command PTZ cameras to preset positions based on events within the Security System
- provide indication of any cameras or recordings which have failed
- Provide a link in its alarm list directly to any associated video recording. Clicking on the link shall call up a pop up window that allows the operator to replay the video without the need to navigate to the DVMS.
- provide the ability to develop custom displays with video and video controls integrated within the displays
- Provides an ability to report on system activity and configuration using customizable reports
- Present all DVMS system alarms to the building control system operator

Integration to the Building Management and Control System shall be provided by the DVMS manufacturer and shall be a standard component of the DVMS software. Solutions that are not yet

[1] For Fire Systems, a UL listed LAN device may be used to isolate the DVMS from the Fire System.

integrated and require the development of integration – with or without a manufacturer's Software Development Kit (SDK) or Application Programming Interface (API) – for the purpose of the project shall not be acceptable.

System integration shall be via a High Level Interface (HLI) and not be based on any of the following: hard-wiring and or so-called "open protocols" such as, but not limited to, BACnet, Modbus or OPC.

The integration between DVMS and Building Management and Control System must be maintained by the vendor. Any updates to the integration required for future releases of either the Building Management and Control System or DVMS software shall be managed as part of the respective products development and testing programs.

Proposal of systems that do not have proven examples of integration between both systems operationally available for at minimum 2 years shall result in disqualification of the proposal.

The proposed DVMS and Security System shall have been deployed together as an integrated solution on more than 1,000 customer sites globally.

1.7 INDUSTRIAL CONTROL SYSTEM

The Industrial Control System is specified in other project documents. It shall be based on the Honeywell Experion PKS Control System or equivalent.

The Industrial Control System monitors and controls industrial sites using integrated controllers and Remote Terminal Units (RTUs). It provides a real-time view of the status of the control system to operators using dedicated Operator Station machines.

In relation to the DVMS System, the Industrial Control System shall:

- Limit and grant operator access to live and recorded video images.
- Send requests to record video
- Command PTZ cameras to preset positions based on events within the Security System
- Provide indication of any cameras or recordings which have failed
- Provide a link in its alarm list directly to any associated video recording. Clicking on the link shall call up a pop up window that allows the operator to replay the video without the need to navigate to the DVMS.
- Provide the ability to develop custom displays with video and video controls integrated within the displays
- Provides an ability to report on system activity and configuration using customizable reports
- Present all DVMS system alarms to the industrial control system operator

Integration to the Industrial Control System shall be provided by the DVMS manufacturer and shall be a standard component of the DVMS software. Solutions that are not yet integrated and require the development of integration – with or without a manufacturer's Software Development Kit (SDK) or Application Programming Interface (API) – for the purpose of the project shall not be acceptable.

System integration shall be via a High Level Interface (HLI) and not be based on any of the following: hard-wiring and or so-called "open protocols" such as, but not limited to, BACnet, Modbus or OPC.

The integration between DVMS and Industrial Control System must be maintained by the vendor. Any updates to the integration required for future releases of either the Industrial Control System or DVMS software shall be managed as part of the respective products development and testing programs.

Proposal of systems that do not have proven examples of integration between both systems operationally available for at minimum 2 years shall result in disqualification of the proposal.

The proposed DVMS and Security System shall have been deployed together as an integrated solution on more than 1,000 customer sites globally.

1.8 OPERATOR STATION

Operator view shall be provided using one or more Operator Station machines. These are connected via a TCP/IP network to the Security, Building Control or Industrial Control System. They can view live video and recorded video from the Camera Servers. They also provide levels of operator security.

In addition, the DVMS shall provide a Microsoft Internet Explorer client interface for viewing and recording live video, video search, replaying recorded video, system configuration and system administration.

To aid in software deployment on large systems, the Internet Explorer client shall be able to be installed without the need for external media. The Internet Explorer station shall require no more than a once-off installation of software to the client at the first connection of the client to the DVMS web server.

Both client interfaces shall provide the ability to play live or recorded audio when configured and available with the associated video stream. The clients shall have the ability to manage Intercom calls using bi-directional audio when supported and configured on the system.

The client shall provide the ability to display up to at least 16 simultaneous video streams in various configurations. It must be possible to support both standard 4:3 aspect ratio screens and wide 16:9 aspect ratio video display monitors without distortion of video but also taking advantage of the entire screen viewing area.

1.9 SYSTEM SIZING

The security system or control system for the site/complex requires that operators be able to simultaneously view, record and replay video, as detailed in this specification, for all cameras throughout the site/complex. The vendor must size the Camera Servers to accommodate the live view and recording requirements of the cameras and desired recording settings.

2. HARDWARE

2.1 DATABASE SERVER

The Database Server shall be able to operate with no performance degradation using the following hardware and operating system configuration:

2.1.1 SYSTEMS WITHOUT REDUNDANT DATABASE SERVERS:

- Standard system:
  - Server level hardware specification
  - Quad Core Intel® Xeon® E5-2403 1.8GHz or AMD equivalent
  - 8GB RAM
  - Two separate hard drives or two sets of RAID arrays.
  - Hard Disk storage sized to meet Section 4 requirements
  - DVD Drive
  - 1000 Mbps NIC for network connection to the other components of the DVMS
  - Graphics card supporting 1280x1024 pixel resolution and 24-bit colour – see client PC specifications if Database Server also used as a client machine
  - Windows Server 2016
  - Microsoft SQL Server 2017
  - Microsoft Internet Explorer 11
- Large, high performance system:
  - Server level hardware specification
  - 2 x Quad Core Intel® Xeon® X5570 2.9GHz or AMD equivalent
  - 8GB RAM
  - Two separate hard drives or two sets of RAID arrays.
  - Hard Disk storage sized to meet Section 4 requirements
  - DVD Drive
  - 1000 Mbps NIC for network connection to the other components of the DVMS
  - Graphics card supporting 1280x1024 pixel resolution and 24-bit colour – see client PC specifications if Database Server also used as a client machine
  - Windows Server 2016
  - Microsoft SQL Server 2017
  - Microsoft Internet Explorer 11
  -

2.1.2 SYSTEMS WITH REDUNDANT DATABASE SERVERS:

- Standard system:
  - Server level hardware specification
  - Quad Core Intel® Xeon® E5-2403 1.8GHz or AMD equivalent
  - 8GB RAM
  - Two separate hard drives or two sets of RAID arrays.
  - Hard Disk storage sized to meet Section 4 requirements
  - DVD Drive
  - 1000 Mbps NIC for network connection to the other components of the DVMS
  - Graphics card supporting 1280x1024 pixel resolution and 24-bit colour – see client PC specifications if Database Server also used as a client machine
  - Windows Server 2016
  - Microsoft SQL Server 2017
  - Microsoft Internet Explorer 11
  -

- Large, high performance system:
    - Server level hardware specification
    - 2 x Quad Core Intel® Xeon® X5570 2.9GHz or AMD equivalent
    - 8GB RAM
    - Two separate hard drives or two sets of RAID arrays.
    - Hard Disk storage sized to meet Section 4 requirements
    - DVD Drive
    - 1000 Mbps NIC for network connection to the other components of the DVMS
    - Graphics card supporting 1280x1024 pixel resolution and 24-bit colour – see client PC specifications if Database Server also used as a client machine
    - Windows Server 2016
    - Microsoft SQL Server 2017
    - Microsoft Internet Explorer 11

The supplier shall demonstrate software compatibility as described in Section 4 if equivalent hardware is proposed.

Proprietary hardware platforms are not acceptable.

The DVMS database shall be hosted on Microsoft SQL Server 2017. No other database solution shall be acceptable, including Microsoft SQL Server Express.

The Database Server must provide the following system fault tolerance:

- Support RAID 0+1, 1, 3 or 5 for the Operating System
- Support RAID 0+1 or 1 for the DVMS database (SQL Server 2014)

2.2 CAMERA SERVER (PREFERRED AND BACKUP)

The Camera Server shall be able to operate with no performance degradation using the following hardware and operating system configuration:

- Standard systems:
    - Quad Core Intel® Xeon® E5-2603 v2 1.8GHz or AMD equivalent
    - 4GB RAM + requirements for pre-event recordings
    - Hard Disk storage sized to meet Section 4 requirements
    - DVD Drive
    - It should be possible to support a dual Network Interface Card configured as follows:
        - 1000 Mbps NIC for video transmission to Operator Stations
        - 1000 Mbps NIC for video transmission from camera video encoders
- High performance systems:
    - Quad-Core Intel® Xeon® E5-2637 v2 3.5GHz or AMD equivalent or 2 x Quad-Core Intel® Xeon®E5-2637 v2 3.5GHz or AMD equivalent
    - 8GB RAM + requirements for pre-event recordings
    - Hard Disk storage to meet Section 4 requirements
    - It should be possible to support a dual Network Interface Card configured as follows:
        - 1000 Mbps NIC for video transmission to Operator Stations
        - 1000 Mbps NIC for video transmission from camera video encoders
- Graphics card supporting 1280x1024 pixel resolution and 24-bit colour – see client PC specifications if Camera Server also used as a client machine
- Microsoft Windows Server 2016
- Microsoft Internet Explorer 11

The supplier shall demonstrate software compatibility as described in Section 4 if equivalent hardware is proposed.

Proprietary hardware platforms are not acceptable, and the Camera Server shall not require onboard/embedded Video Capture Cards to encode video for storage and transmission.

The system shall support deployment within a virtual infrastructure supporting at least VMware and Windows Hyper-V.

Camera Servers shall be able to manage up to 100 camera channels per Camera Server depending on system configuration.

2.3 MOBILE VIDEO STREAMING SERVER

The Mobile Video Streaming Server shall be responsible for delivering live and recorded video to the DVMS Mobile clients. Video shall be delivered via RTSP streaming services and shall support secure communications with Mobile clients using HTTPS.

The Mobile Video Streaming Server shall be able to operate with no performance degradation using the following hardware and operating system configuration:

- Standard systems (up to 40 Mobile streams):
  - Quad Core Intel® Xeon® E5-14100 2.8GHz or AMD equivalent
  - 8GB RAM
  - 40GB Hard Disk
  - Networking: minimum 1Gbps NIC
  - DVD Drive
- High performance systems (up to 90 Mobile streams):
  - Dual Quad Core Intel® Xeon® E5-2609 2.4GHz or AMD equivalent
  - 8GB RAM
  - 40GB Hard Disk
  - Networking: minimum 1Gbps NIC
  - DVD Drive
- Graphics card supporting 1280x1024 pixel resolution and 24-bit colour – see client PC specifications if Camera Server also used as a client machine
- Microsoft Windows Server 2016

The supplier shall demonstrate software compatibility as described in Section 4 if equivalent hardware is proposed.

2.3.1 ADAPTIVE VIDEO STREAMING

The Mobile Video Streaming Server shall Support the ability to dynamically adjust the quality of live video delivered to Mobile clients based on the available network bandwidth.

The adaptive streaming calculation shall be performed by the Mobile Video Streaming Server based on feedback from the Mobile device and take into consideration the available bandwidth and client decoding capability. The Server shall adjust video quality by first altering video frame rate and then the video encoding compression level.

The Mobile Video Streaming Server shall support up to 30 different video streams simultaneously in adaptive mode.

2.4 VIDEO ANALYTICS SERVER

The Video Analytics (VA) Server (when required) shall be able to operate with no performance degradation using the hardware and operating system configuration as specified by the video analytics vendor.

The supplier shall demonstrate software compatibility as described in Section 4 if equivalent hardware is proposed.

Proprietary hardware platforms are not acceptable.

2.5 MULTIPROCESSOR SUPPORT

The Database Server, Camera Server and Video Analytics Server software shall be able to run on both multiple and single processor computers. Where a multiple processor system is used the DVMS software shall be able to make optimal use of that configuration.

2.6 SYSTEM FAULT TOLERANCE

A failure of any one of the Database Servers or Camera Servers shall NOT cause the DVMS system to cease operation. As a worst case, only the cameras controlled by the Camera Server will be temporarily unavailable until re-allocated to other Camera Servers using the DVMS software in the event that the Camera Server Redundancy feature is not used. No physical changes to hardware, cabling or connections shall be required.

2.7 OPERATOR INTERFACE

The DVMS shall provide 5 (five) types of Operators Interface:

- Surveillance Console: a dedicated, full feature Surveillance client
- Integrated Operator Station: A client completely hosted within the Operator Station of the Security System, Integrated Building Management and Control System or Industrial Control System
- Browser Client: A lightweight Internet Explorer based client
- Operator Keyboard: A professional CCTV Keyboard interface which allows view and control of cameras without the need for a PC-based Operator Station
- A Mobile Video Client supporting Apple iOS-based and Google Android-based devices

DVMS clients shall make use of hardware acceleration utilising the client PC Graphics Processor Unit (GPU) for video decoding and rendering to improve video rendering performance and quality. The client shall automatically shift a portion of the video decompression load to the PC CPU in the event that the computational limits of the GPU are reached. Not operator interaction shall be required to enable load sharing between the PC CPU and GPU.

PC-based Operator Stations shall provide full control via keyboard and mouse of all parts of the system to which the operator is assigned access.

2.7.1 SURVEILLANCE CONSOLE

The Surveillance Console shall provide a dedicated, professional surveillance client used by Security officers. Other clients may be installed and utilised on the physical machine used by the Surveillance Console as required.

The Surveillance Console shall have as a minimum the following hardware and Operating System components required to support digital video integration:

- Standard Clients:
    - Intel Core i7or AMD equivalent Hyperthreaded
    - 4GB RAM
    - 100/1000 Mbps NIC
    - Microsoft Windows 10
    - Video Graphics Card: NVIDIA Quadro P400 2GB (NVIDIA Graphics Driver R430 U7)
    - Microsoft Internet Explorer 11

- Performance Clients:
    - Quad-Core Intel® Xeon® or AMD equivalent
    - 4GB RAM
    - 1000 Mbps NIC
    - Microsoft Windows 10
    - Video Graphics Card: NVIDIA Quadro P1000 4GB (NVIDIA Graphics Driver R431 U6) Microsoft Internet Explorer 11
- Ultimate Performance Clients:
    - 2 x Quad-Core Intel® Xeon® or AMD equivalent
    - 4GB RAM
    -
    - 1000 Mbps NIC
    - Microsoft Windows 10
    - Video Graphics Card: NVIDIA Quadro P1000 4GB (NVIDIA Graphics Driver R431 U6)
    - Microsoft Internet Explorer 11

Proprietary hardware platforms are not acceptable.

2.7.2 INTEGRATED OPERATOR STATION

The Integrated Operator Station shall as a minimum conform to the Security System, Building Control System or Industrial Control System specifications for hardware requirements.

In addition to the Security System, Building Control System or Industrial Control System requirements, the Integrated Operator Station shall have as a minimum the following hardware and Operating System components required to support digital video integration:

- Standard Clients:
    - Intel Core i7or AMD equivalent Hyperthreaded
    - 4GB RAM
    - 100/1000 Mbps NIC
    - Microsoft Windows 10
    - Video Graphics Card: NVIDIA Quadro P400 2GB (NVIDIA Graphics Driver R430 U7)
    - Microsoft Internet Explorer11
- Performance Clients:
    - Quad-Core Intel® Xeon® or AMD equivalent
    - 4GB RAM
    - 1000 Mbps NIC
    - Microsoft Windows 10
    - Video Graphics Card: NVIDIA Quadro P1000 4GB (NVIDIA Graphics Driver R431 U6)
    - Microsoft Internet Explorer11
- Ultimate Performance Clients:
    - 2 x Quad-Core Intel® Xeon® or AMD equivalent
    - 4GB RAM
    - 1000 Mbps NIC
    - Microsoft Windows 10
    - Video Graphics Card: NVIDIA Quadro P1000 4GB (NVIDIA Graphics Driver R431 U6)
    - Microsoft Internet Explorer 11

Proprietary hardware platforms are not acceptable.

The Integrated Operator Station shall be able to host the user interface for the DVMS within the same user interface used for the Security System, Building Control System or Industrial Control System. It shall not be acceptable for the DVMS to only provide a separate application as user interface thus

necessitating switching between applications to access either video or the Security System, Building Control System or Industrial Control System.

2.7.3 BROWSER CLIENT

The Browser Client shall support system configuration and casual system viewing.

The Browser Client shall have as a minimum the following hardware and Operating System components required to support digital video integration:

- Standard Clients:
  - Intel Core i7or AMD equivalent Hyperthreaded
  - 4GB RAM
  - 100/1000 Mbps NIC
  - Microsoft Windows 10
  - Video Graphics Card: NVIDIA Quadro P400 2GB (NVIDIA Graphics Driver R430 U7)
  - Microsoft Internet Explorer11
- Performance Clients:
  - Quad-Core Intel® Xeon® or AMD equivalent
  - 4GB RAM
  - 1000 Mbps NIC
  - Microsoft Windows 10
  - Video Graphics Card: NVIDIA Quadro P1000 4GB (NVIDIA Graphics Driver R431 U6)
  - Microsoft Internet Explorer11
- Ultimate Performance Clients:
  - 2 x Quad-Core Intel® Xeon® or AMD equivalent
  - 4GB RAM
  - 1000 Mbps NIC
  - Microsoft Windows 10
  - Video Graphics Card: NVIDIA Quadro P1000 4GB (NVIDIA Graphics Driver R431 U6)

Microsoft Internet Explorer 11Proprietary hardware platforms are not acceptable.

The browser client shall utilise HTTPS and TLS1.2 for all internal web server communication

2.7.4 OPERATOR KEYBOARD

The DVMS shall support a professional type CCTV keyboard. The Operator Keyboard shall be Honeywell UltraKey or equivalent and shall be integrated to the system via an Ethernet connection to the system. The Operator Keyboard shall allow operators to view and control live video without the need for a dedicated Operator Station.

The Operator Keyboard shall utilise the DVMS Surveillance Monitor(s) for display of live video and system interaction.

The Operator Keyboard shall provide the operator with a means to:

- Log on to the system
- Select and display cameras on surveillance monitors
- Select and display multiple camera views on surveillance monitors
- Select and control PTZ cameras using the keyboard’s joystick
- Command PTZ cameras to predefined preset positions
- Start and stop recordings
- Log off from the system

It shall be possible to configure connected keyboards and operators from the DVMS.

2.7.5 MOBILE CLIENTS

The DVMS shall support mobile clients based on:

- Apple's iOS devices including iPhone and iPad.
- Google's Android 10 operating system

The app shall be available for download and install from the Apple App Store or Google Play Store. The clients shall support the display of both live and recorded video with the system able to intelligently vary video quality to match the bandwidth available for wireless video transmission.

The mobile client shall support user authentication aligned with the DVMS security permissions. Mobile operators shall only be able to see and control cameras to which they have assigned access.

The mobile client shall display a camera tree for easy camera selection. It shall be possible to display multiple cameras simultaneously in live view with up to a 2x3 display for mobile phones and a 3x3 display for tablets. The application shall include a searchable camera tree and a list of recently accessed cameras.

It shall be possible to control a PTZ camera directly from the mobile applications. The user shall be able to select configured presets or move the camera via finger press directly on the video footage. Touching the screen above or below the centre of the scene shall tilt the camera up or down and touching to the left or right shall pan the image in the same direction. The speed of the pan and tilt shall vary based on the distance from the centre of the image to the touch point.

Recorded video shall display as a single camera only and shall include a timeline for display and easy navigation of recordings as well as a date and time selector to quickly locate video. A control shall be provided to support variable speed playback in both forward and reverse directions. An instant replay button shall be provided and shall provide the ability to instantly jump back by a selectable amount of 30 seconds, 60 seconds or 5 minutes.

The Mobile Clients shall all support Apple's iOS10.x or later and Android 10 or later.

2.7.6 VIDEO WALL CLIENTS

The DVMS shall support integration to video wall control devices from at minimum:

- Barco: Barco Control Room Management Suite (CMS) V3.0
- Matrox: Including the MURA MPX Series

The DVMS shall support video streaming to the video wall controller by both unicast and multicast streaming. The video wall shall support the configuration of multiple monitors as a single workspace and it shall be possible to command a camera to display on a configured tile in the workspace.

It shall be possible to control a PTZ camera displayed on the workspace and direct it to a configured preset, tour or pattern.

It shall be possible to stream video directly from the camera to the Video Wall, without the need for video to pass through a Camera Server.

2.8 DEVICE SUPPORT: NETWORK CAMERAS AND VIDEO ENCODERS

The Digital Video Management System shall be expandable to support a minimum of 6000 cameras per Database Server node. Additional system expansion shall be supported through additional Database Servers connected together into a unified solution with centralised control and management.

The Digital Video Management System shall be capable of supporting up to 300 cameras per Camera Server depending on system configuration.

As a minimum, the system must support network cameras and video encoding devices:

- Network Video Encoders:
    - AXIS Communications M-series, P-series and Q-series video encoders
    - ONVIF conformant video encoders supporting at minimum ONVIF Profile S and Profile G
- Network Cameras:
    - Honeywell network cameras
    - AXIS Communications network cameras
    - Panasonic iPro series network cameras
    - Pelco Sarix series network cameras
    - Sony IPELA Generation 5 and 6 series network cameras
    - ONVIF conformant network cameras supporting at minimum ONVIF Profile S and Profile G

The DVMS shall support at least industry-standard Motion JPEG, H.264 and H.265 video encoding formats.

The DVMS shall support certified ONVIF devices that conform to the ONVIF Profile S and Profile G standards. The DVMS shall be a certified ONVIF Network Video Client with certification for both ONVIF Profile S and Profile G registered on the ONVIF website as a minimum requirement. Systems that do not support ONVIF Profile S and Profile G will not be acceptable.

The DVMS shall support the ability to analyse and upload device capabilities of supported manufacturers as listed above and for ONVIF compliant devices. Once discovered, device details shall be added to the DVMS database and used for further device configuration. Systems that require a software update to add support for new devices from supported manufacturers shall not be acceptable.

2.9 NETWORK AND VIDEO CABLING

A Local Area Network (LAN) shall be provided for communication between the system elements. All interfaces to the LAN shall be a minimum of 1000BaseTX Ethernet. The LAN may use additional technologies within the backbone for greater speed or distance. Acceptable types are:

- FDDI
- 1000BaseSX or 1000BaseLX Gigabit Ethernet
- Asynchronous Transfer Mode (ATM)

The LAN shall use standard network cables. Acceptable cable types are:

- Optical Fiber
- Category 5e or Category 6 Unshielded Twisted Pair (UTP)

The LAN shall be logically and/or physically separate from any existing LAN infrastructure. Interconnection to other LANs shall be through one of the following:

- A router
- A Layer 3 capable network switch
- As an additional VLAN to the existing LAN equipment. Where required to interconnect VLANs, a router or Layer 3 capable switch shall be provided

2.9.1 VIDEO CABLING

Where standard CCTV cameras are used, RG59/RG11/RG6 coaxial cable or optical fiber shall be used to connect the camera to a video encoder. Video encoders shall be located at locations as close as possible to the analog CCTV cameras.

Star topology wiring of video cabling to a central location shall only be permitted for the integration of existing analog CCTV infrastructure. All new equipment shall be integrated via connection to the closest Ethernet network point provided.

It is not acceptable for video cables to be run back to the Camera Server. All communications with the Camera Server shall be via the LAN.

Each network camera or video encoder shall have a single network interface to be used for video and Pan/Tilt/Zoom communications.

3. SYSTEM SOFTWARE

This section describes the required System Software. If other software is proposed, then suppliers must be able to demonstrate full compliance with Section 4.

The proposed solution shall be based on standard Microsoft technology for Server and Client/desktop Operating System and Database solution. Systems that utilise non-Microsoft solutions shall not be acceptable.

3.1 DATABASE SERVER

The Database Server will include the following system software components:

- Microsoft Server 2016
- Microsoft SQL Server 2017 database
- Microsoft Internet Information Server (IIS) (web server)
- Application software with functionality detailed in Section 4.

3.2 CAMERA SERVER

The Camera Server (Preferred and Backup) will include the following system software components:

- Windows Server 2016
- Application software with functionality detailed in Section 4.

It shall be possible to install the Camera Server software for all Camera Servers on the DVMS from a central location.

The Camera Server shall be a native 64-bit application to ensure optimal system performance. A DVMS supporting only 32-bit Camera Server applications shall not be acceptable.

3.3 VIDEO ANALYTICS SERVER

The Video Analytics Server will include the following system software components:

- Windows Server 2016
- Application software with functionality detailed in Section 4.

The DVMS shall support integration to video content analysis solutions from at minimum:

- AllGoVision Technologies
- IPSOTEK Ltd

3.4 MOBILE VIDEO STREAMING SERVER

The Mobile Video Streaming Server will include the following system software components:

- Windows Server 2016
- Application software with functionality detailed in Section 4.

The Mobile Video Streaming Server shall be configurable to allow for video streaming to mobile devices over both local Wi-Fi as well as cellular mobile telephony networks.

3.5 SECURITY SERVER

The Security System will include the following system software components:

- System and Application software detailed in the Security System Specification
- Application software with functionality detailed in Section 4.

3.6 INTEGRATED BUILDING MANAGEMENT AND CONTROL SERVER

The Building Control System will include the following system software components:

- System and Application software detailed in the Building Control System Specification
- Application software with functionality detailed in Section 4.

3.7 INDUSTRIAL PROCESS CONTROL SYSTEM SERVER

The Industrial Control System will include the following system software components:

- System and Application software detailed in the Industrial Control System Specification
- Application software with functionality detailed in Section 4.

3.8 INTEGRATED OPERATOR STATION

The Operator Station will include the following system software components:

- Application software detailed in the Security System or Control System Specification
- Microsoft Windows 10
- Microsoft Internet Explorer 11
- Application software with functionality detailed in Section 4.

3.9 NETWORK

Each Ethernet Switch shall support:

- Simple Network Management Protocol (SNMP)
- IEEE 802.1D bridging capability and loop detection
- IEEE 802.1Q tagged VLANs
- IEEE 802.1p traffic prioritization for multiple Quality of Service levels
- IEEE 802.1w rapid spanning tree with fast link support
- IEEE 802.3ad link aggregation support
- IGMP snooping for IP Multicast support
- Multicast network traffic
- Non-blocking configuration capable of simultaneous wire-speed switching across all ports.

4. APPLICATION SOFTWARE FUNCTIONS

4.1 SURVEILLANCE CLIENT OPERATION

Operators shall utilise one or more of the available DVMS Client interfaces depending on their specific operational role and needs.

4.1.1 SURVEILLANCE CONSOLE

The surveillance Console shall provide a professional level surveillance interface for control room operators. Its primary role shall be to meet the operational requirements related to surveillance. The Surveillance Console client shall be a native 64bit application for optimal performance.

The Surveillance Console shall inherit Security permissions from the Security System, Integrated Building Management and Control System or Industrial Control System. Security shall be managed using Trusted Root Certificates which will allow the Surveillance Console to communicate with the required Database and Camera Servers.

Solutions that do not allow for integration of the Security model between DVMS and the Security System, Integrated Building Management and Control System or Industrial Control System shall not be permitted.

The Surveillance Console user interface shall consist of the following key elements:

- Navigation Pane
- Flexible Video Workspace
- Timeline with video Export capability
- Recently Used Camera List

It shall be possible to minimise each individual element of the Surveillance Console to maximise the use of the screen for video display.

The Surveillance Console Client shall be configurable with both dark and light themes to assist with usability in light or dark control room environments.

The individual elements of the User Interface shall operate as follows:

4.1.1.1 Navigation Pane

The Navigation Pane shall include separate tabs to display available cameras, Views, groups and locations available to the operator based on their security settings. It shall include a Camera Tree as well as a location for defining logical groups of elements.

The Camera Tree shall be a multi-level element up to at least 5 layers deep and shall display cameras, groups and predefined camera views as separate icons.

The Camera tree shall conform to the system security model and only allow operators to see and interact with devices to which they have been provided rights.

It shall be possible to arrange cameras in locations on the Camera Tree, either by via integration with the facility model of the Security System, Integrated Building Management and Control System or Industrial Control System or by manually creating groups and allocating applicable cameras.

The Camera Tree shall provide a location for operators to create their own logical groups of cameras to suit their individual operational surveillance needs. Cameras and Views shall be able to appear in multiple logical groups.

The Camera Tree shall include an automatic filtering facility which allows for dynamic filtering of the items in the tree as text is typed into the filter text box. Searchable items shall include cameras, locations, multi-camera views and bookmark text.

It shall be possible to drag individual cameras, locations, groups or Views to the Video Workspace to display all cameras involved in the operation. Cameras shall also be added to the workspace by a single left mouse click – which will add the camera to the next empty tile – or by double-clicking the left mouse button – which replaces the existing selected Tile's camera with the new camera.

Double left-clicking on a group or location will replace all cameras in the Workspace with the new Group or Location. Single left-clicking on a Group or Location will expand or collapse the Group or Location in the Navigation Pane.

4.1.1.2 Flexible Video Workspace

The Video Workspace shall display cameras in 1 or more tiles, and it shall be possible to arrange the Video Workspace into several different layouts. The layouts shall be selectable from a list of options displayed as icons on the Video Workspace toolbar providing a visual representation of the layout. Separate layouts shall be provided for 4:3 and 16:9 aspect ratio monitors.

Tiles in the Video Workspace shall display either a single camera or cycle through multiple cameras. A header bar shall be provided in the Workspace to indicate information about a current View being displayed or to control the cycling of cameras in the workspace.

Tiles shall display either Live or Recorded video. The Video Workspace shall support the simultaneous display of Live and Recorded video from the same or different cameras. Information describing the camera and associated video shall be shown in the tile including camera name, camera number, camera health status and whether the camera is currently recording, replaying video, paused or playing live video.

The Tiles shall provide a tile toolbar which appears as a popup when the mouse pointer is hovered over the tile. The toolbar shall provide buttons to allow interaction and control of the camera directly. Buttons shall include at least: instant playback, return to live, record, snapshot, playback controls, focus, iris, digital zoom, preset controls and annotation controls.

It shall be possible to control PTZ cameras directly from the Tile in the Workspace. Control shall be either via the controls on the popup overlay menu or by clicking directly on the video in the tile.

It shall be possible to drag one or more selected cameras between tiles to allow rearranging of the cameras in the Workspace as required by the operator.

All cameras dragged from a location on Navigation Pane shall be displayed in the Workspace. If the number of cameras dragged into the Workspace exceeds the number of available tiles, the additional cameras will cycle in tiles on the Workspace.

It shall be possible to clear the workspace via a single operation by clicking a button on the Workspace toolbar.

It shall be possible to maximise the workspace to full screen mode, whereby the Workspace shall expand to fill the entire monitor screen.

The Workspace toolbar shall include a keyboard command box that allows for typed commands to be entered and executed. Keyboard commands shall include:

- Arrows: move selection between tiles
- CTRL+A: Select all cameras in a Workspace
- F11: Switch to Full Screen mode (and ESC to cancel)

- Enter: maximise/minimise the tile with focus
- Delete: remove the selected cameras from the workspace

Integration with the Security System, Integrated Building Management and Control System or Industrial Control System shall provide the ability to create custom display pages within those systems with embedded camera objects from the DVMS. It shall be possible to drag those camera objects to the DVMS Surveillance Client Video Workspace and hence display that camera in a Tile on the Workspace.

The video workspace shall support a “surrounding cameras” functionality that shall operate as follows:

- Selecting the “Surrounding Cameras” option for a displayed camera shall centre that camera in a 3x3 tiled workspace
- The tiles surrounding the centre tile shall be populated with cameras in the geographic direction of those tiles from the central camera
- The cameras shall be automatically determined based on their placement on the site map in the Integrated Operator Station
- It shall not be necessary to manually configure the relationships between cameras. Only systems that automatically determine location based on the camera placement on the site map shall be acceptable.
- Selecting the “Surrounding Cameras” option on another camera in the workspace shall the reconfigure the workspace to place that camera in the central tile and automatically rearrange the cameras displayed on the surrounding tiles based on their geographical map locations.

4.1.1.3 Timeline

The Surveillance Client shall provide a timeline control to display and play back recorded video for one or more cameras. Playback shall be possible on 1 or more cameras simultaneously for all cameras currently displayed in the Video Workspace.

Each camera and its associated recording shall be represented in the timeline by a separate row. Background and Scheduled Recordings shall be represented as thick horizontal rows in the camera row while other recording types shall be represented as thinner, vertical lines

The Timeline shall provide a time ruler indicating the time from which video is sourced. It shall be possible to move the ruler to earlier or later dates and zoom in or out on the time scale for greater accuracy or easier searching for recordings.

The Timeline shall provide a playhead control to indicate the time of the recording currently viewed for all cameras in the timeline. The playhead shall also be used to scrub through video for all recordings in the timeline.

A Timeline toolbar shall be provided to assist with playback of recordings. The toolbar shall include the following standard features as a minimum:

- **Play:** play recorded video
- **Pause:** Pause video currently being played
- **Snapshot:** Captures a single frame of video from the current scene
- **Fast rewind:** rewinds the video at a speed related to the number of times the button is clicked with each click increasing the rewind speed by a factor of 4 from 4 times to 1024 times normal speed. Clicking once rewinds the video at normal speed with subsequent clicks increasing the speed. Video speed shall be slowed by right-clicking one or more times with each right-click reversing the speed by a single factor of 4. Right-clicking when displaying normal speed will slow the replay to 0.75, 0.5 and 0.25 normal speed on respective clicks. The fast rewind operation shall be applicable to all cameras displayed in the timeline.

- **Frame rewind:** Rewinds the video a single frame per click or click and hold to rewind continuously through individual frames
- **Frame Forward:** Advances the video a single frame per click or click and hold to advance continuously through individual frames
- **Fast forward:** plays the video at a speed related to the number of times the button is clicked with each click increasing the speed by a factor of 4 from 4 times to 1024 times normal speed. Video speed shall be slowed by right-clicking one or more times with each right-click reversing the speed by a single factor of 4. Right-clicking when displaying normal speed will slow the replay to 0.75, 0.5 and 0.25 normal speed on respective clicks. The fast forward operation shall be applicable to all cameras displayed in the timeline.
- **Jump Back:** Control containing 3 separate buttons to rewind and start playing video from 30 seconds, 1 minute and 5 minutes prior to that point in time.
- **Motion Search:** Enables the Motion Search operation which allows configuration of the parameters to search for motion in recorded video.
- **Regions of Interest:** This option shall be displayed if live video annotations are enabled. Selecting the option shall show or hide the configured regions of interest.
- **Calendar control:** allows the ability to select a date and time to which to navigate immediately.
- **Video Export:** allows the operator the ability to select export duration on one (1) or more cameras directly from the timeline and export them in a single operation as per section "Video as evidence: Digitally Signed Recordings and Audit Logs"

It shall be possible to add any camera currently displayed in the Video Workspace to the timeline allowing the timeline to contain from 1 up to the total number of cameras displayed in the Video Workspace. It shall be possible to replay 2 or more videos displayed in the timeline in time synchronised playback.

It shall be possible to add any camera visible to the operator to the timeline by a simple drag-&-drop operation from both the camera tree and the video workspace.

The timeline shall provide a Motion Search feature that allows searching for areas of motion in recorded video. The Motion Search feature shall provide the ability to define a region of interest for each camera currently included in the timeline. The region of interest will be displayed on the camera image in the Video Workspace and each shall be separately configurable.

Motion Search shall commence from the position of the playhead on the timeline and an indication shall be provided on the corresponding tiles in the Video Workspace that motion search is in progress.

Motion results shall be indicated on the camera rows in the Timeline as discovered and it shall be possible to navigate to each event via "Next Event" and "Previous Event" buttons. Video can be replayed at these events while motion search is currently active.

It shall be possible to stop or disable motion search as required.

It shall be possible for operators to add bookmarks to video directly from the timeline. A button shall be provided for this purpose and shall allow the operator to insert the bookmark at the point of the playhead position once pressed. Bookmarks must be associated with recorded video and shall be visible to all users.

Bookmarks shall by default be added to all cameras present in the timeline. It shall be possible to deselect bookmarks if not required on specific cameras at the point of creation.

Bookmarks shall be represented on the timeline to allow easy identification. Selecting a bookmark shall display the text entered by the operator.

It shall be possible to modify or delete bookmarks provided the user has the appropriate security permissions.

Bookmark text shall be a searchable item in the DVMS camera tree. Selecting the bookmark found or dragging the bookmark to the video workspace or timeline shall load the camera recording and automatically locate the playhead to the video frame closest to the bookmark location automatically.

It shall be possible to easily navigate between bookmarks on a camera by using a “Jump to Next” feature included on the timeline.

4.1.1.4 Recently Used Camera List

The Surveillance Console shall provide a visual location for cameras that have recently been viewed by the operator. Cameras displayed in this location shall be represented by a live view image from the camera at reduced frame rate for easy reference.

Cameras shall be displayed in the recently used list under the following scenarios:

- They are removed from a tile and are not shown in any other tile in the Video Workspace.
- They are replaced in the Video Workspace by another camera or view.
- The camera no longer fits in the Video Workspace due to a layout change.
- The camera was part of a cycling view or cycling camera tiles when the Video Workspace was altered, and the camera no longer fits on the Video Workspace. A Video Workspace can be altered by selecting a different workspace layout or cameras being added or removed on the Video Workspace.

It shall be possible to select and move a camera from the Recently Used List to the Video Workspace for further viewing

It shall be possible to display a minimum of ten (10) cameras in the Recently Used List

It shall be possible to clear a single camera, or all cameras displayed in the Recently Used List.

4.1.2 INTEGRATED OPERATOR STATION AND BROWSER CLIENTS

For the purposes of this section, Integrated Operator Station Clients and Browser Clients shall be handled together as their operational functionality is equivalent.

The live output from cameras shall be configured and viewed through a series of displays. These shall support:

- Single camera view
- Multiple camera viewing of up to 16 cameras simultaneously, each at 25/30fps and each view port supporting sequencing of cameras and/or cameras presets for PTZ cameras
- Specific viewing options for both standard aspect ratio as well as wide aspect ratio (wide screen) monitors thus preventing distortion of original video aspect ratio while still taking advantage of the entire screen area for image display of multiple video channels.
- Sequence view of camera preset positions
- Modifying settings for a camera
- Modify recording settings for a camera
- Adding and deleting cameras
- Creating schedules for recordings, video analytics and Input/Output monitoring and switching
- Modifying Video Analytics settings and tuning for:
    - Video Motion Detection
    - Object Tracking
    - Object Classification

    - Intelligent Video Analytics
- Modify settings for Inputs and Outputs on IP cameras and video encoders
- Modify settings for camera tamper detection
- View and initiate Intercom calls with cameras configured with bi-directional audio capabilities.

Users shall be able to select a camera from a tree control listing the cameras available to the user.

4.1.3 SINGLE CAMERA

From this display, the user shall be able to:

- View the live output from the selected camera
- Pan, tilt, zoom and focus the camera using a joystick attached to the Operator Station PC
- Pan, tilt, zoom and focus the camera using a pointing device attached to the Operator Station PC. Standard Microsoft Windows supported pointing devices such as a mouse or touch-screen shall be supported.
- For cameras which support continuous pan, tilt, zoom (PTZ), a mouse shall be able to be used for continuous PTZ directly in the live video window. By dragging the mouse up or down, left or right in the video window, the operator shall be able to tilt the camera up or down, or pan the camera left or right. Zooming must also be provided using the mouse in a similar way.
- Manually record live video. Recording will continue for the configured period of time. Once recording has begun, a stop button shall be provided as well as a counter showing the recording time remaining.
- Manually store the current frame of video (snapshot) as a bitmap image file. The file name shall be automatically generated by the DVMS software and include the camera name, date and time of the recording (to millisecond precision).
- Indicate whether video motion detection is currently enabled for the selected camera.
- Initiate an intercom call or accept an incoming intercom call.
- Digitally zoom into a region of the image
- Enhance the image by adjusting brightness, contrast, noise levels or sharpness of the image

4.1.4 MULTIPLE CAMERA VIEWS

The DVMS shall support multiple camera views. A multiple camera view consists of up to sixteen related cameras viewed simultaneously on a single display. Support for multi-camera views with larger camera counts shall be possible via configuration.

The layout for a view shall be configurable from a selection of different layouts templates. There shall be a set of templates for standard aspect ratio (4:3) monitors and another set of templates for wide aspect ratio monitors to properly utilise the entire monitor screen real estate without distorting the original video aspect ratio.

It shall be possible to configure and save individual views for re-use. It shall be possible for the view to be created by dragging and dropping cameras and presets if applicable directly into the view ports from the camera tree.

Standard aspect ratio templates shall include:

Single camera (sequencing – see 4.1.5.1)

- 2 x 2 View
- 3 x 3 View
- 4 x 4 View
- 1 + 5 View
- 2 + 8 View

- 1 + 12 View

Wide aspect ratio templates shall include:

- Single camera (sequencing – see 4.1.5.1)
- 2 x 3 View
- 3 x 4 View
- 1 + 3 View
- 2 + 4 View
- 1 + 8 View

Multiple camera views shall be divided into quadrants. For each quadrant the view shall have a camera or be blank. Within each quadrant the view shall be configured to cycle between any of the cameras accessible to the user on a configurable time basis. Pan-tilt-zoom cameras, which support preset positions, can have these presets cycled on a time basis. In this way, an operator can view a variety of presets on a series of PTZ cameras in a multiple camera view.

It shall be possible to show the camera names of each camera and preset (if applicable) configured in a view on either the operator station or on surveillance monitors. Hovering the mouse pointer over a view port shall trigger a tooltip showing the camera name and preset (if applicable).

There shall be no limit to the number of cameras that can be assigned to a single multiple camera view. There shall also be no limit to the number of available multiple camera views.

The system shall support the ability to intelligently manage video streaming to the alarm and spot display monitors by automatically selecting a lower quality video stream when displaying multiple cameras on a single stream. The quality of the video stream for this purpose shall be configurable on a per-camera basis. The system shall automatically switch between the lower quality stream (if configured) and the normal live video stream when switching from a multi-camera view to a single camera view.

4.1.4.1 Sequence View

The DVMS shall support sequence views. A sequence view consists of a single camera view, which can be cycled on a time basis. Pan-tilt-zoom cameras, which support preset positions, can have these presets cycled on a time basis. In this way an operator can view a variety of presets on a series of PTZ cameras. Fixed cameras can also be included in the sequence and cycled accordingly.

There shall be no limit to the number of cameras that can be assigned to a single Sequence View. There shall also be no limit to the number of available Sequence Views.

4.1.5 VIEWING RECORDINGS

The recorded video shall be available to all users, which have adequate security. Each user shall only be able to view recordings from cameras they have security access to view.

A display shall be provided to view recordings from any Operator Station. From this display, the operator can select the recording he/she wishes to view, which shall be immediately shown in an embedded video player.

The following information and controls shall be provided on this display:

- A navigation panel to allow the user to select the required camera
- A calendar control (similar to Microsoft Outlook) to select the desired date. All days which have recordings for the chosen camera shall be displayed in bold font.

- A table listing all the recordings on the chosen camera for the chosen day. The user shall be able to select the required recording from this table. Each column shall be able to be sorted by selecting the column heading. This table shall display the following information as a minimum:
    - The time each recording was activated
    - The duration of each recording
    - The type of recording (operator, intercom, event, video analytics, camera tamper, input/output scheduled or background)
    - The Operator or user that activated the recording (for operator activated recordings)
    - The Name, Description and Value of the Security System Server or Control System Server which activated the recording (for alarm/event activated recordings)
- An embedded video player with control buttons to control video playback. The information displayed on the video player and the controls provided shall include:
    - The time and date of the frame being displayed
    - A slider control which is used to move backwards and forwards through the recording
    - Play, pause and stop buttons
    - Step forward and step backward buttons, to move through the recording frame by frame
    - Fast forward and rewind buttons, to play the recording at speeds of x2, x4, x8, x16, etc (to a minimum of x1024). Video speed shall be slowed by right-clicking one or more times with each right-click reversing the speed by a single factor of 4. Right-clicking when displaying normal speed will slow the replay to 0.75, 0.5 and 0.25 normal speed on respective clicks.
    - A snapshot button, to allow for the frame being displayed to be stored as a bitmap file (in a similar way to the snapshot button for live video).
    - Buttons to access slider bars for adjusting the brightness, contrast, noise levels and sharpness of the image
    - A mouse-pointer activated overlay allowing for control of digital zoom
- Information about the chosen recording. The following information as a minimum shall be displayed with the chosen recording
    - The type of recording (operator, intercom, event, video analytics, camera tamper, input/output scheduled or background)
    - The Operator or user that activated the recording (for operator activated recordings)
    - The Name, Description and Value of the Security System, Building Control System or Industrial Control System which activated the recording (for alarm/event activated recordings)
    - The sub-priority of the recording (for alarm/event activated recordings)
    - The frame rate that the recording was recorded at
    - The resolution of the recording
    - The compression used
    - The recording start time and date (including pre-record)
    - The recording end time and date
    - The date and time that the recording will be deleted by default (which can be changed as required)
    - Operator comments and notes about the recording (made by the scheduled recording configuration automatically or by an operator)
    - The date and time that the recording will be archived by default (which can be changed as required)
    - The date and time that the recording will be deleted by default (which can be changed as required)

- When a recording is displayed, the exact frame of video when the recording was activated shall be shown. The slider shall be positioned accordingly along with the frame time. It is not appropriate to show the first frame in the recording, as the recording may have pre-event recording.
- Buttons to allow the operator to archive, delete or export the chosen recording
- A button is provided to playback the recording at the recorded resolution. This shall be done using a display that pops up containing the embedded video control with full playback functionality as described above.

4.1.6 SEARCHING FOR RECORDED VIDEO

4.1.6.1 Simple Search

The DVMS shall provide a simple search for all video recorded. The user selects the time indicator which shows a calendar and timeline. The user selects the required search period.

Once the time criterion is entered, the “search” is selected. Video recorded during the selected period will be returned by the search.

The user shall be able to search on combinations of cameras by clicking on an “Advanced Search” icon as described in the next section.

4.1.6.2 Advanced Search

The DVMS shall provide an advanced search of recorded video. The search shall be based on recording time, camera and recording details.

The user shall select from the list of cameras. It shall also include any cameras that have been deleted from the system but still have video stored on a Camera Server or on archived media. If a camera has been deleted and all video associated with the camera has been deleted, the camera name will not appear in this list.

The time criterion shall be selected from a calendar and timeline control. Days containing recorded video shall be shown in bold on the calendar control. Cameras shall be able to be added and removed from the search list.

The user shall be able to choose to filter the search based on the following criteria:

- Alarm or event type for alarm/event activated recordings
- Recording type (operator, intercom, event, video analytics, camera tamper, input/output scheduled or background)
- Area
- Point name
- Event description (urgent, high, low, journal and all)
- Operator name
- Camera name or number
- Any comments entered by users in the comments field of recordings

Wildcards shall be accepted for the Point ID, description, area, priority and value for alarm/event activated recordings.

4.1.6.3 Search Results

The DVMS shall show the results of the basic and advanced searches in a table format, such that the user is able to select columns within the list to sort the output. Functionality shall be provided to allow the

user to see a list of recordings for a camera from the past 24 hours without needing to use one of the searches.

4.1.7 VIDEO AS EVIDENCE: DIGITALLY SIGNED RECORDINGS AND AUDIT LOGS

Export of video for evidentiary purposes shall be possible directly from the Operator Client. Systems that require a separate application to manage video export shall not be acceptable.

The DVMS shall support at minimum 2 means for video authentication:

- **Digital Signature:** A default Digital Certificate shall be provided and installed on Client computers used for Export purposes. It shall be possible to utilise digital certificates purchased from other certificate authorities as required and supported by corporate policy. The digital signature shall be applied to the exported video and the audit log
- **Watermarking:** A default watermark image shall be provided, and it shall also be possible to configure a custom image as a watermark. It shall be possible to configure the size and location of the watermark in the exported video as well as its opacity.

It shall be possible to select the portion of video required and export only that portion.

It shall be possible to select the video to be exported directly from the video timeline in the Operator Client. Manipulation of the export range for each camera shall be performed using the mouse and allow dragging of the export range and its edges to select the desired period for each camera. It shall be possible to configure unique time periods for each camera in the export operation.

It shall be possible to export video from 1 or more cameras in a single operation from the timeline. The maximum number of cameras managed in a single export shall be limited to the number of cameras displayed simultaneously in the operator's video workspace.

Export recordings in a format supported by standard video players in either transcoded or non-transcoded format.

It shall be possible to export in either the native, non-transcoded format or a more compressed, transcoded format as follows:

- Non-transcoded export: Advanced System Format (asf) or MPEG-4 Part 14 (MP4)
- Transcoded exports: Windows Media Video (wmv)or Audio Video Interleave (AVI)

Exporting in non-transcoded format will retain the original, native video format and will keep the original video format unchanged.

Systems that require a proprietary viewer application for viewing exported video shall not be acceptable.

The system shall provide the ability to export the system event log associated to the export range along with the video.

The system shall provide the ability to overlay the camera and recording date and time details on the exported video. It shall be possible to enable and disable this feature at the point of export as required.

It shall be possible to select the export destination location and provide a unique name for the export.

The system shall provide visual feedback as to the progress of each individual camera's export status as well as the overall video export progress and status. This feedback will include estimated remaining duration of the export action and size of the export package. This feedback shall also include any errors or warnings associated with the export operation.

The system shall provide the ability to cancel the entire export or remove individual cameras from the export operation without disrupting the export for the remaining cameras.

The Operator Client shall create a queue of recordings to be exported and shall allow for items to be exported concurrently where possible. Client CPU utilization shall be monitored during the export process and the export load adapted to ensure that the Operator Client PC CPU utilization remains below 90%.

The DVMS shall allow for the protection of the exported video by means of a freely configurable password for each export package.

It is a requirement for all exported recordings and exported audit logs to be digitally signed. This is required to prove authentication (origin of the recording and audit log) and integrity (exported recording and audit log have not been altered or tampered with).

The DVMS system shall provide a default digital certificate for signing the exported recordings and audit logs. Customization shall also be provided to allow for the user to supply his/her own digital certificate.

A utility shall be provided to display the exported recording, view the audit log and verify the digital signatures. A visual indication shall be provided to whether the exported recording and audit log have been altered or tampered with.

4.2 ALARM AND SPOT MONITORS

The system shall also support the display of video on spot and alarm monitors in the following manner:

- **Alarm monitor:** When an alarm occurs in the Security System, Integrated Building Management and Control System or Industrial Control System Server, the live video output associated with that alarm shall be switched directly to an alarm monitor. The system shall support the switching of both live video from single cameras as well as from a collection of cameras associated with the alarm. The user shall be able to acknowledge the alarm to clear the monitor using the numeric keypad. Cameras that are directed to alarm monitors will not be removed from the queue unless explicitly cleared by the operator. It shall be possible to create a queue of alarm monitors to manage multiple alarm views simultaneously.
- **Cyclic Alarm Monitors:** An alarm monitor shall be available at the end of an alarm monitor queue to cycle the camera views from unacknowledged alarms if the number of cameras or groups of cameras to view exceeds the number of alarm monitors. Once the alarm monitor queue is filled, any new alarm will be placed in the queue relative to its priority and then time of occurrence. Existing activated alarm camera views shall reshuffle to accommodate the new alarm. If all the available alarm monitors are used, the oldest active alarm camera or group of cameras shall be added to the cycling alarm monitor. The alarm views shall cycle on this final alarm monitor until acknowledged and cleared by an operator in the event of multiple alarms added to this monitor.
- **Surveillance monitor:** Operators shall be able to call up both single camera views and multiple camera views to a surveillance monitor. It shall be possible to sequence the cameras displayed on the surveillance monitor and the system shall support sequences of single cameras as well as cameras sequencing in individual view ports when a surveillance monitor displays multiple cameras simultaneously. The User shall be able to clear the monitor using the numeric keypad. It shall be possible to call up a camera to an individual tile of a multiple camera view displayed on Surveillance Monitor.

Monitors shall be able to be configured to act as both Alarm and Surveillance monitors. In this case, the monitor behaves as a Surveillance monitor until an alarm occurs, in which case it shall show the alarm video. Once the alarm is acknowledged, the video previously shown (as a surveillance monitor) is displayed again.

In each of these cases, these additional monitors shall be either connected to an Operator Station using a multi-monitor PC card or to other PCs.

The system shall support the ability to intelligently manage video streaming to the display monitors by automatically selecting a lower quality video stream when displaying multiple cameras on a single stream. The quality of the video stream for this purpose shall be configurable on a per-camera basis. The system shall automatically switch between the lower quality stream (if configured) and the normal live video stream when switching from a multi-camera view to a single camera view.

Systems that do not offer this functionality will be disqualified.

4.3 VIDEO LOSS ALARM

The DVMS shall support the video encoder Video Loss Alarm feature. The Video Loss Alarm feature shall provide DVMS operators with a notification when the video signal from the camera to the video encoder is lost. A video loss alarm shall result in an alarm being raised, the change of the camera icon in the camera tree to indicate the alarm condition and an entry in the system audit log for future reference.

4.4 CAMERA TAMPER DETECTION

The DVMS shall provide the ability to detect attempts to tamper with connected cameras. The system will at minimum detect the following:

- Changed field of view: repositioning the camera away from a reference position shall trigger an alarm
- Camera blur: any attempt to defocus or blur the camera shall trigger an alarm
- Camera blind: any attempt to cover or blind the camera (via abnormally high light levels) shall trigger an alarm

Each of the above options shall be individually selectable as required per camera. It shall thus be possible to enable any combination of the above three detection options on each camera connected to the DVMS.

The detection algorithms for tampering shall be run on one or more of the DVMS Camera Servers. It shall be possible to configure and tune the algorithms individually per camera. The configuration screen shall provide:

- The ability to enable any combination of the tamper detection algorithms
- Real time feedback of the percentage of tampering detected
- The ability to set the threshold at which a tamper alarm will be generated
- Real time feedback of when a tamper threshold has been crossed
- How often the detection algorithm should check for a tamper condition
- System response to a tamper alarm including:
    - Starting a recording with the possibility of also configuring the system to record video prior to the event occurring. It must be possible to record video prior to the event occurring where the duration of this pre-record is a pre-configured value.
    - Generating alarms with configurable alarm levels
    - Sending live video to an Integrated Operator Station
    - Trigger an output on a device connected to the DVMS such as a network camera or video encoder.

Once a tamper condition is detected, the system shall provide visual indication to the operator through both a text overlay on the live video and indication on the camera tree. The text overlay shall be for viewing purposes only and shall not be recorded.

Systems that provide the same camera tamper settings for all cameras shall not be acceptable.

4.5 CAMERA SETTINGS

Camera configuration shall be accomplished via the Integrated Operator Station or Browser Clients.

Users shall be able to change important settings for an individual camera from the local system to which that camera is assigned. The details are grouped into several sections:

- Camera Details
- Camera Connection
- Camera PTZ Control
- Security
- Camera Deletion

The parameters listed in the sub-sections below are configurable on a per camera basis and their specific selection on a particular camera(s) will not limit the ability to freely select other options on other cameras as required. It will be easy to change any of these parameters for each camera individually as and when required. Systems that do not allow changes to each camera's parameters on an individual basis will not be acceptable.

Only users with the highest level of security are permitted to modify camera connection details, camera PTZ control or delete cameras.

4.5.1 CAMERA DETAILS

The user shall be able to configure the following parameters for each camera:

- Camera name
- Allocated Camera Server
- Location
- Description
- Camera Number (for fast numeric keypad call-up). It shall be possible to define camera numbers up to 1,000,000,000.

4.5.2 CAMERA CONNECTION

The DVMS shall provide the capability to define the connection parameters for each camera and include the following items:

- Camera Family and Model
- Camera IP address. The DVMS shall support both IPv4 and IPv6 device addressing.
- The frame delivery type; unicast or multicast
- The stream type: video, video and audio or video and bi-directional audio
- The video format: PAL or NTSC

It shall be possible to configure unique video stream profiles for each camera. The system shall support up to 4 unique stream profiles, depending on the capabilities of the IP Camera or video encoder used.

It shall be possible to define the priority of the different video stream profiles configured for each camera.

Each stream profile shall be comprised of the following parameters:

- User-configurable name
- Compression format: H.265, H.264, MPEG4 or Motion JPEG
- Stream limiter type: Stream limited by either frame rate or bandwidth
- Stream limit: Frame Rate or Bandwidth value
- GOP (for differential video encoding formats)
- Video Resolution
- Video Compression ratio

Each stream profile shall be assignable as follows:

- Live video display (all clients except Mobile)
- Mobile Clients
- Low resolution profile (for use with multi-camera views)
- Supported recording types

4.5.3 CAMERA CONTROL

The user shall be able to configure any appropriate camera to be PTZ controllable. The following camera types must be supported as a minimum:

- Video Controls Limited (VCL) Orbiter cameras.
- Honeywell Video RapidDome cameras
- Cameras supporting the Pelco P protocol
- Cameras supporting the Pelco D protocol
- American-Dynamics Speed Dome
- Axis video encoder supported PTZ cameras and devices
- Honeywell HVE video encoder series supported PTZ cameras and devices

The following PTZ characteristics shall be tuneable on a camera-by-camera basis from the camera definition pages:

- Pan speed
- Tilt Speed
- Zoom speed
- Focus speed
- Iris speed
- Increment step size
- Continuous Pan/Tilt speed

The DVMS shall provide the ability support streamer-side camera control for video encoding devices providing this feature. In this case, the video encoding device will be responsible for providing the control mechanism to the associated camera and the communications protocol will not need to be natively supported in the DVMS.

4.5.3.1 Advanced Camera Control

The DVMS shall provide more advanced control capability for cameras supporting the Pelco D camera protocol as well as the features mentioned below. The DVMS shall support the following functions:

- Control of the camera washer and wiper function via dedicated button on the DVMS User Interface. A hardware interface via the output port of a video encoding device shall not be sufficient
- Call up and navigation of the device system menu and setting of device options on this menu via the DVMS User Interface
- The ability to record patterns of motion for a Pan/Tilt/Zoom camera. These patterns will be available as preset positions for Pan/Tilt/Zoom cameras allowing the cameras to “patrol” the facility when not being controlled by operators.

The DVMS shall provide access to the absolute positioning coordinates of Pan/Tilt/Zoom cameras using the Pelco D protocol. The coordinates will be provided via the DVMS Application Programming Interface – see section 4.16

4.5.4 SECURITY

The following parameters shall be configurable for each camera:

- Area: Allows the system to be configured to only allow users to view specified cameras. These areas shall be the defined by the Security System, Building Control System or the Industrial Control System.
- Control Level: Determines if a user has permission to operate the PTZ controls for a camera. Also used to allow higher-level users to take control of cameras. These Control Levels shall be defined by the Security System, Building Control System or Industrial Control System.
- Control Reservation Period: Once a user has controlled the camera no other user can control the camera until this reservation period has expired. Users with a higher security level shall be able to take control of the camera at any time.

User names and passwords for all IP cameras and video encoders shall be stored in the database in encrypted format.

4.5.5 CAMERA DELETION

The “Delete” function shall allow a user with the highest-level security to delete the camera from the system. After deletion name of the camera will no longer appear in the list of cameras. All camera settings will be deleted but the camera record will remain in the database for searching purposes.

Any recordings associated with a deleted camera will remain until their configured deletion date. The recordings will remain on the Camera Server and archive media unless they are later individually deleted. The camera name will also continue to appear in the list of cameras used for searching the video clip database.

4.6 RECORDING VIDEO

Recorded video will be stored by the Camera Server in one of the following locations:

- Internal hard disk drive array
- External, direct attached storage array
- Network storage location

The Operator station shall be able to locate relevant recorded video and to then replay that video at the Operator Station.

The DVMS shall support the replay of recorded video from any location provided that the recording can be accessed by a functioning Camera Server deployed on the system. Recording playback shall not be affected by the availability of the original recording Camera Server.

The system shall provide the ability to use any of the defined video stream profiles – as defined in section 4.5.2 – for the device for recording purposes. All recording types shall use the same video encoding format.

The system shall only record a single video stream from each camera configured in the system so that most efficient use is made of available system storage. If more than one (1) recording type is active simultaneously, the systems shall record the video delivered by the video stream profile with the highest defined priority.

The following methods of recording live video shall be supported:

- User activated
- Intercom activated
- Event-activated by the Security, Building Control or Industrial Control System
- Streamer and/or IP camera Inputs/Outputs
- Scheduled
- Continuous background recording
- Video Analytics

    - Video Motion Detection
    - Intelligent Video Analytics
    - Camera Tamper events
- Snapshot
- PTZ-Activated
- Edge Recording

4.6.1 USER ACTIVATED RECORDING

User activated recording occurs when a user viewing live video chooses to record the currently viewed camera output by selecting the "Record" button on the applicable user interface.

The user shall be able to configure the following parameters uniquely for each camera:

- **Pre-Record Duration:** The amount of pre-recorded video that will be associated with a user request for recorded video. This will allow the Camera Server to capture video prior to the user request, as well as after the request. Shall be selectable from a list of values ranging from No Recording to 5 minutes.
- **Frame Rate:** Video quality required for user activated recording. It shall be possible to have different frame rates for user and event-activated recordings. Shall be selectable from the entire range of frame rates supported for the camera. For MPEG encoding (including H.264 and H.265), support shall also be provided to record only the Index frames, or a subset of the Index frames.
- **Record Duration:** User activated recordings shall terminate after this period. Shall be selectable from a list of values ranging between 0 seconds and 10 minutes
- **Retention Period:** The default period that the Camera Server shall retain user-activated recordings before being deleted. The retention period of individual recordings shall be able to be changed on a per-recording basis. Shall be selectable from a list of values ranging between one hour and forever.
- **Archive After period:** The default period for which user activated recordings are available for playback before they are automatically archived. The Archive After period of individual recordings shall commence at the video clip's end date and time and be able to be changed on a per-recording basis. The period shall be selectable from a list of values to provide a default setting for all recordings of this type per camera but shall also be manually configurable on each individual recording after the recording has occurred.
- **Delete After period:** The default period that the recording will be retained before being automatically deleted by the system. The Delete After period of individual recordings shall commence at the video clip's end date and time and shall be and be able to be changed on a per-recording basis. The period shall be selectable from a list of values to provide a default setting for all recordings of this type per camera but shall also be manually configurable on each individual recording after the recording has occurred.

4.6.2 INTERCOM ACTIVATED RECORDING

Intercom activated recording occurs when an operator starts an intercom call. It shall be possible to configure the system to either start recording automatically or require that the operator press the "Record" button once the call has started. It shall also be possible to disable intercom recordings.

Intercom recordings shall be identified by their own activation type to allow for easier searching and identification.

The user shall be able to configure the following parameters uniquely for each camera:

- **Pre-Record Duration:** The amount of pre-recorded video that will be associated with intercom activated recording. This will allow the Camera Server to capture video prior to the intercom

request, as well as after the request. Shall be selectable from a list of values ranging between 0 seconds and 5 minutes.

- **Frame Rate:** Video quality required for intercom activated recording. It shall be possible to have different frame rates for intercom and event-activated recordings. Shall be selectable from the entire range of frame rates supported for the camera. For MPEG encoding (including H.264 and H.265), support shall also be provided to record only the Index frames, or a subset of the Index frames.
- **Record Duration:** Intercom activated recordings shall terminate after this period. Shall be selectable from a list of values ranging between 0 seconds and 10 minutes
- **Retention Period:** The default period that the Camera Server shall retain user-activated recordings before being deleted. The retention period of individual recordings shall be able to be changed on a per-recording basis. Shall be selectable from a list of values ranging between one hour and forever.
- **Archive After period:** The default period for which intercom activated recordings are available for playback before they are automatically archived. The Archive After period of individual recordings shall commence at the video clip's end date and time and be able to be changed on a per-recording basis. The period shall be selectable from a list of values to provide a default setting for all recordings of this type per camera but shall also be manually configurable on each individual recording after the recording has occurred.
- **Delete After period:** The default period that the recording will be retained before being automatically deleted by the system. The Delete After period of individual recordings shall commence at the video clip's end date and time and shall be and be able to be changed on a per-recording basis. The period shall be selectable from a list of values to provide a default setting for all recordings of this type per camera but shall also be manually configurable on each individual recording after the recording has occurred.

For cameras that support Pan/Tilt/Zoom and Presets, a specified preset location shall be selected automatically when the Intercom call is connected prior to the intercom activated recording commencing.

4.6.3 EVENT ACTIVATED RECORDING

Event activated recording is a process that allows a segment of video or a snapshot to be associated with the Security System, Building Control System or Industrial Control System alarm or event.

There shall be at least four priorities of alarms/events in the Security or Control System:

- Event (journal priority)
- Low priority alarms
- High priority alarms
- Urgent priority alarms

The following settings shall be individually configurable for each alarm and each camera:

- **Pre-Record Duration:** The amount of pre-recorded video that will be associated with an alarm/event. This shall allow the Camera Server to capture video prior to the alarm/event, as well as after the alarm/event. Shall be selectable from a list of values ranging between 0 seconds and 5 minutes.
- **Post Record Duration:** Event activated recordings shall terminate after this period. Shall be selectable from a list of values ranging between 0 seconds and 5 minutes
- **Frame Rate.** Video quality required for event activated recording. It shall be possible to have different frame rates for user, event-activated, scheduled and motion detection activated recordings. Shall be selectable from the entire range of frame rates supported for the

camera/streamer. For MPEG encoding (including H.264 and H.265), support shall also be provided to record only the Index frames, or a subset of the Index frames.

- **Retention period.** The default period the Camera Server will retain event-activated recordings before being deleted. The retention period of individual recordings shall be able to be changed as necessary. Shall be selectable from a list of values ranging between one hour and forever.
- **Archive After period:** The default period for which event activated recordings are available for playback before they are automatically archived. The Archive After period of individual recordings shall commence at the video clip's end date and time and be able to be changed on a per-recording basis. The period shall be selectable from a list of values to provide a default setting for all recordings of this type per camera but shall also be manually configurable on each individual recording after the recording has occurred.
- **Delete After period:** The default period that the recording will be retained before being automatically deleted by the system. The Delete After period of individual recordings shall commence at the video clip's end date and time and shall be and be able to be changed on a per-recording basis. The period shall be selectable from a list of values to provide a default setting for all recordings of this type per camera but shall also be manually configurable on each individual recording after the recording has occurred.

The pre-record and post-record durations in the paragraph above define the maximum allowable limits for each camera. They shall be configured on a camera-by-camera basis. However each alarm or event causing video to be recorded shall also be capable of individual configuration with pre and post alarm periods being selected from a range defined by the maximum settings for the camera.

DVMS systems requiring a single pre and post record event period to be defined for all alarms and events on an individual camera are not acceptable. DVMS systems requiring a single pre and post event period to be defined for all alarms and events on all cameras are also not acceptable.

In the case of multiple alarms/events relating to the same camera, a video clip shall be created for each alarm/event.

For cameras that support Pan/Tilt/Zoom and Presets, a specified preset location shall be selected automatically when the alarm/event occurs prior to the event activated recording commencing. For example, when an alarm is detected on a security door, the alarm shall trigger a PTZ camera to move to a preset position, which is pointing at the door prior to the DVMS commencing recording.

4.6.4 DEVICE INPUT/OUTPUT ACTIVATED RECORDING

Input or output recording activation occurs when an input or an output connected to an IP camera or streamer is activated and then subsequently triggers recording on one or more associated cameras.

It shall be possible for any digital input or output connected to a streamer or IP camera on the system to trigger a recording on one or more cameras simultaneously.

The following settings shall be individually configurable for each alarm and each camera:

- **Pre-Record Duration:** The amount of pre-recorded video that will be associated with a device input/output. This shall allow the Camera Server to capture video prior to the alarm/event, as well as after the alarm/event. Shall be selectable from a list of values ranging between 0 seconds and 5 minutes.
- **Post Record Duration:** Device input/output activated recordings shall terminate after this period. Shall be selectable from a list of values ranging between 0 seconds and 10 minutes or while the device is active.
- **Frame Rate.** Video quality required for device inout/output activated recording. It shall be possible to have different frame rates for user, device input/output activated, event-activated, scheduled and motion detection activated recordings. Shall be selectable from the entire range

of frame rates supported for the camera/streamer. For MPEG encoding (including H.264 and H.265), support shall also be provided to record only the Index frames, or a subset of the Index frames.

- **Retention period.** The default period the Camera Server will retain device input/output activated recordings before being deleted. The retention period of individual recordings shall be able to be changed as necessary. Shall be selectable from a list of values ranging between one hour and forever.
- **Archive After period:** The default period for which device input/output activated recordings are available for playback before they are automatically archived. The Archive After period of individual recordings shall commence at the video clip's end date and time and be able to be changed on a per-recording basis. The period shall be selectable from a list of values to provide a default setting for all recordings of this type per camera but shall also be manually configurable on each individual recording after the recording has occurred.
- **Delete After period:** The default period that the recording will be retained before being automatically deleted by the system. The Delete After period of individual recordings shall commence at the video clip's end date and time and shall be and be able to be changed on a per-recording basis. The period shall be selectable from a list of values to provide a default setting for all recordings of this type per camera but shall also be manually configurable on each individual recording after the recording has occurred.

The pre-record and post-record durations in the paragraph above define the maximum allowable limits for each camera. They shall be configured on a camera-by-camera basis.

For cameras that support Pan/Tilt/Zoom Presets, a specified preset location shall be selected automatically when the input/output event occurs prior to the recording commencing. For example, when an intrusion alarm is detected, the alarm shall trigger a PTZ camera to move to a preset position, which is pointing at the area monitored by the intrusion sensor prior to the DVMS commencing recording.

4.6.5 SCHEDULED RECORDING

Scheduled recording allows video to be recorded between start and stop times on defined days.

The system shall support the ability to schedule recordings for each individual camera for times in the future. For each scheduled recording the user shall be able to configure the following (with descriptions as per User Activated and Event Activated recordings):

- Start time
- Stop time
- Frame rate for the recording
- Retention period before the recording will be deleted
- Recurrence (if this is to be a recurring schedule)
- Description (at least 255 characters)
- Archive After period providing the period after which the recording will automatically be archived
- Delete After period providing the period after which the recording will automatically be deleted
- Whether audio is recorded with the scheduled recording or not (if supported on the camera)

There shall be no limit on the number of schedules that can be entered for the system. There shall be no limit to the number of schedules per camera.

4.6.6 CONTINUOUS BACKGROUND RECORDING

The system shall support the ability to provide continuous background recording from any camera(s) managed by the system. Background recordings will be stored as a discrete series of clips and will continue to operate in the event that communication between the Camera Server and the Database Server is lost. Once communication is restored, all relevant information will be updated to the Database Server.

For each camera the user shall be able to configure the following (with descriptions as per User Activated and Event Activated recordings):

- Enable / disable background recording
- Duration of the recorded clip
- Frame rate for the recording
- Enable / disable archiving of the clip and the period after which to archive
- Retention period before the recording will be deleted
- Enable or disable audio recording (if available)
- Archive After period providing the period after which the recording will automatically be archived
- Delete After period providing the period after which the recording will automatically be deleted

Systems that require the configuration of multiple time periods to manage background recordings will not be accepted.

Continuous background recordings will not be dependent on network communications between the Camera Server and the Database server. Once configured, these recordings will continue to operate in the event that this communication is lost.

4.6.7 VIDEO ANALYTICS RECORDING

The DVMS system must be able to activate recordings automatically based on events generated by the real-time analysis of video from any camera on the system that has Video Analytics enabled. The real time analysis comprises several algorithms as follows:

- Video Motion Detection
- Object Tracking and Object Classification
- Intelligent Video Analytics based on Honeywell Intelligent Video Analytics or equivalent.

4.6.7.1 Video Motion Detection

The DVMS system must be able to support video motion detection algorithms, which can be executed by the video streamer or the Camera Server. The enabling of Video Motion Detection shall be either:

- on a continuous basis
- scheduled for particular times, dates, days, months etc.

The Camera Server-based algorithm must be able to provide the following functionality:

- Detect and track objects
- Learn the scene
- Adapt to a changing outdoor environment
- Ignore environmental changes including rain, hail, wind, swaying trees and gradual light changes

The user shall be able to configure the following parameters for each camera:

- **Detection Type:** Continuous or scheduled

- **Actions to Perform When Motion is Detected:** When motion is detected, the following actions shall be performed automatically:
    - Generate an alarm in the Security System, Building Control System or Industrial Control System of configurable priority (journal, low, medium, high)
    - Start a recording, with the following configurable settings
        - **Pre-Record Duration:** The amount of pre-recorded video, allowing the Camera Server to capture video prior to the detection of motion, as well as after the detection of motion. Shall be selectable from a list of values ranging between 0 seconds and 5 minutes.
        - **Post Record Duration:** Motion detection activated recordings will terminate after this period. Shall be selectable from a list of values ranging between 0 seconds and 10 minutes or until motion has stopped. It shall be possible for the recording to continue until the motion detection algorithm considers motion finished.
        - **Frame Rate.** Video quality required for motion detection activated recordings. Shall be selectable from the entire range of frame rates supported for the camera/streamer. For MPEG encoding (including H.264 and H.265), support shall be provided to record only the Index frames, or a subset of the Index frames.
        - **Retention period.** The default period that motion detection activated recordings will be retained by the Camera Server before being deleted. The retention period of individual recordings shall be able to be changed as necessary. Shall be selectable from a list of values ranging between one hour and forever.
        - **Archive After period:** The default period for which motion detection activated recordings are available for playback before they are automatically archived. The Archive After period of individual recordings shall commence at the video clip's end date and time and be able to be changed on a per-recording basis. The period shall be selectable from a list of values to provide a default setting for all recordings of this type per camera but shall also be manually configurable on each individual recording after the recording has occurred.
        - **Delete After period:** The default period that the recording will be retained before being automatically deleted by the system. The Delete After period of individual recordings shall commence at the video clip's end date and time and shall be and be able to be changed on a per-recording basis. The period shall be selectable from a list of values to provide a default setting for all recordings of this type per camera but shall also be manually configurable on each individual recording after the recording has occurred.
    - Send video to an operator station or alarm monitor: Automatically switch an operator station or alarm monitor to view the camera which has motion detected
    - Trigger an output device on a related network camera or video encoder
- Motion Finished Time: The amount of time where no motion (inactivity) is detected before the previous motion is classified as completed. This shall be used for allowing recordings to continue until motion has finished.

The DVMS must provide a means of automatic and manual tuning of the Video Motion Detection for each camera. Incorporated within this tuning are the following:

- Selection of the frame rate used for detection
- Optimization for directions of movement
- In any direction
- Across the camera view

- Towards and away from the camera
- Sensitivity level to fine tune the motion detection algorithm
- Specification of a minimum object size to allow noise filtering in the system to reduce false detections and alarms.

The DVMS must also provide the ability to only detect motion in particular regions of the camera view. The ability to graphically select these regions using the mouse must be provided, with an unlimited number of regions permitted per camera. The regions of interest will be multi-verticed shapes with a minimum of 6 vertices to allow the region to be properly matched to the scene being detected. It shall be possible to add and remove vertices from the defined region of interest as needed. Solutions providing only rectangular regions of interest will not be accepted.

Each region must be able to be individually tuned and have separate tuning parameters. This method of tuning must also provide a live tuning window whereby these settings and regions can be altered and tested prior to be being used. This live tuning window shall show the live video as well as the regions of interest. During the time that motion is detected within a region, the border of the region shall change to a different colour. In this way, tuning can be performed to achieve the desired performance. Text shall also be provided in the window to alert the user that motion has been detected.

4.6.7.2 Intelligent Video Analytics

The DVMS must provide integration to an Intelligent Video Analytics system. The Intelligent Video Analytics system will be specified separately and will be based on Honeywell Intelligent Video Analytics or equivalent.

Video for analysis will be supplied to the Intelligent Video Analytics system algorithms by the Analytics Server(s) of the DVMS. The Intelligent Video Analytics system will run on the DVMS Camera Servers and shall accept and process the video based on preconfigured conditions of interest.

Events from the Intelligent Video Analytics system will be passed back to the DVMS for further action. It will be possible to automatically perform the following actions from the DVMS based on events detected by the Intelligent Video Analytics system:

- Generate an alarm in the Security System, Building Control System or Industrial Control System of configurable priority (journal, low, medium, high)
- Start a recording, with the following configurable settings
    - **Pre-Record Duration:** The amount of pre-recorded video, allowing the Camera Server to capture video prior to the alarm/event, as well as after the alarm/event, shall be selectable from a list of values ranging between 0 seconds and 5 minutes.
    - **Record Duration:** The period that the recording is active relating to the period of activity in the region of interest. Activated recordings will terminate after this period. Shall be selectable from a list of values ranging between 0 seconds and 10 minutes or the object is no longer in the region of interest.
    - **Frame Rate:** Video quality required for recordings triggered by events from the Intelligent Video Analytics system. Shall be selectable from the entire range of frame rates supported for the camera/streamer. For MPEG encoding (including H.264 and H.265), support shall be provided to record only the Index frames, or a subset of the Index frames.
    - **Retention period:** The default period that recordings generated based on events from the Intelligent Video Analytics system will be retained by the Camera Server before being deleted. The retention period of individual recordings shall be able to be changed as necessary. Shall be selectable from a list of values ranging between one hour and forever.

    - **Archive data:** enable/disable archiving and set the period after which the recording will be automatically archived
    - **Deletion data:** Set the period after which the recording will be automatically deleted
- Send video to an operator station or alarm monitor: Automatically switch an operator station or alarm monitor to view the camera which has motion detected
- Trigger an output device on a related network camera or video encoder

It shall be possible to enable or disable the display of annotations associated with event detection delivered by the Video Content Analysis system on the DVMS Operator Station

4.6.8 SNAPSHOT RECORDING

The DVMS system must provide every operator with the ability to record the current frame of video. This snapshot of video shall be stored as a bitmap file. The file name shall be automatically generated by the DVMS software and include the camera name, date and time of the recording (to millisecond precision). An audible sound shall be produced by the Client computer, to ensure that the operator has feedback when the snapshot is taken.

4.6.9 RECORDED VIDEO

The DVMS shall allow camera output to be recorded for the following conditions:

- Manually activated by a user viewing a live camera
- Activated by or during an intercom call
- Activated by a Security System or Control System alarm or event
- Activated by inputs or outputs on a streamer or IP Camera
- Continuous background recording
- Scheduled recording
- Specialised real-time video analysis including:
    - Video Motion Detection
    - Intelligent Video Analytics
    - Camera Tamper events

User activated recording occurs when a user viewing live video chooses to record the currently viewed camera output by selecting the “Record” button.

Intercom activated recording occurs when an operator either accepts an intercom call from the field or when the operator chooses to start a recording during an intercom call when the system is configured without automatic recording of intercom calls enabled.

Event activated recording is a process that allows a segment of video or a snapshot to be associated with a Security System, Building Control System or Industrial Control System alarm or event.

Input or output recording activation occurs when an input or an output connected to an IP camera or streamer is activated and then subsequently triggers recording on one or more associated cameras.

Scheduled recording allows video to be recorded between start and stop times on defined days.

Real-time video analysis activated recording is a process that allows a segment of video or a snapshot to be recorded when a specific event is detected by a video analysis algorithm used by the DVMS.

Recorded video is stored on the Camera Server. The Operator station shall be able to query the Database Server to locate relevant recorded video and to then replay that video at the Operator Station.

4.6.10 LIVE AND RECORDED AUDIO

The DVMS shall provide the ability to have audio included with the video. Two types of audio support shall be provided:

- Single directional audio from the field (camera or streamer) locations to the DVMS Camera Servers (and Operator Stations)
- Bi-directional audio (intercom) between the field (camera or streamer) locations and the DVMS Camera Servers (and Operator Stations)

4.6.10.1 Single Directional Audio

The DVMS shall provide the following single directional audio support:

- Audio shall be recorded by the streamer using an attached microphone (or similar device)
- Audio shall be streamed along with the video from the camera (or streamer) locations to the DVMS Camera Servers (and Operator Stations) using the same network used for the video stream. This shall require no additional network cabling
- Audio shall be played at the Operator Stations using speakers connected to the Operator Station computer
- Live audio shall be played whenever the live video is displayed
- Audio shall be recorded whenever the video is recorded.
- For scheduled and continuous (background) recordings, the audio shall be optionally disabled
- Audio shall be played when the recording containing audio is played. The audio shall be heard in the same synchronization it was recorded in.
- Wherever the audio is played with the video, a mute button and volume control shall be provided on the video player. It is unacceptable to use the Operating System's volume controls for this purpose.
- Recordings containing audio shall be exported with the audio and video in the same synchronization it was recorded in.

4.6.10.2 Bi-Directional Audio (Intercom)

The DVMS shall provide the following bi-directional audio (intercom) support:

- Audio from camera location (or streamer) to DVMS Camera Server (and Operator Stations)
    - Audio shall be recorded by the streamer using an attached microphone (or similar device)
    - Audio shall be streamed along with the video from the camera (or streamer) locations to the DVMS Camera Servers (and Operator Stations) using the same network used for the video stream. This shall require no additional network cabling
    - Audio shall be played at the Operator Stations using speakers connected to the Operator Station computer
- Audio from Operator Stations to camera location (or streamer)
    - Audio shall be recorded at the Operator Station using a microphone (or similar device) connected to the Operator Station computer
    - Audio shall also be streamed from the Operator Stations to the camera (or streamer) locations using the same network used for the video stream. This shall require no additional network cabling.
    - Audio shall be played at the camera (or streamer) locations using speakers (or similar devices) connected to the streamer
- A intercom call shall be able to be initiated by either the field (camera location) or the Operator Station
    - Initiated from the field using a push-button (or another device) connected to the streamer

    - Initiated from the Operator Station using an intercom button provided within the DVMS Live Video control
- Intercom calls initiated by the field shall be alerted to the Operator Station in all the following ways:
    - An alarm raised in the Security or Control System
    - An intercom button flashing on the Live Video Control of the Operator Station. The Operator shall use this button to answer the intercom call and end the intercom call.
    - An indication in the camera tree that an intercom call is awaiting answering
    - An Intercom call queue above the camera tree shall show all pending Intercom calls
- Intercom calls initiated by an Operator Station shall be alerted to the field through a buzzer (or similar device) connected to the streamer.
- Audio from the field shall be recorded whenever the video is recorded.
- Audio shall be played when the recording containing audio is played. The audio shall be heard in the same synchronization it was recorded in.
- The bi-directional audio shall use full duplex bi-directional audio whereby the audio from the field device shall be carried on a separate channel to the audio from the operator station. This will allow separation of the audio streams for processing and muting of the individual streams if required.

4.6.11 PTZ-ACTIVATED RECORDING

The DVMS shall support the ability to automatically commence recording on a PTZ camera when an operator takes control of the camera. The recording will commence when the user starts to control the camera and will stop after a predefined period

PTZ-Activated recordings shall be identified by their own activation type to allow for easier searching and identification.

The user shall be able to configure the following parameters uniquely for each camera:

- **Pre-Record Duration:** The amount of pre-recorded video that will be associated with intercom activated recording. This will allow the Camera Server to capture video prior to the intercom request, as well as after the request. Shall be selectable from a list of values ranging between 0 seconds and 5 minutes.
- **Frame Rate:** Video quality required for intercom activated recording. It shall be possible to have different frame rates for intercom and event-activated recordings. Shall be selectable from the entire range of frame rates supported for the camera. For MPEG encoding (including H.264 and H.265), support shall also be provided to record only the Index frames, or a subset of the Index frames.
- **Record Duration:** Intercom activated recordings shall terminate after this period. Shall be selectable from a list of values ranging between 0 seconds and 10 minutes
- **Retention Period:** The default period that the Camera Server shall retain user-activated recordings before being deleted. The retention period of individual recordings shall be able to be changed on a per-recording basis. Shall be selectable from a list of values ranging between one hour and forever.
- **Archive After period:** The default period for which intercom activated recordings are available for playback before they are automatically archived. The Archive After period of individual recordings shall commence at the video clip's end date and time and be able to be changed on a per-recording basis. The period shall be selectable from a list of values to provide a default setting for all recordings of this type per camera but shall also be manually configurable on each individual recording after the recording has occurred.

- **Delete After period:** The default period that the recording will be retained before being automatically deleted by the system. The Delete After period of individual recordings shall commence at the video clip's end date and time and shall be and be able to be changed on a per-recording basis. The period shall be selectable from a list of values to provide a default setting for all recordings of this type per camera but shall also be manually configurable on each individual recording after the recording has occurred.

4.6.12 EDGE RECORDING

The DVMS shall support the recording of video to storage on the IP Camera or video encoder. Video stored in this way will be accessible to DVMS Operators for playback and export and to the system as a backup in the event of recording loss.

The DVMS shall be ONVIF Profile G compliant and a certificate of conformance shall be listed on the ONVIF website as evidence.

Edge Recordings shall be configured directly in the device using the device webpage and recordings shall be stored on the Secure Digital (SD) Card installed in the device. Edge recordings shall be stored using H.264 or H.265 video encoding. Access to the edge recording shall be configurable on a per camera basis.

The DVMS shall support the ability to backfill gaps in background recordings by using the recordings stored on the edge device. The DVMS shall monitor for gaps in background recordings, determine whether a recording exists on the edge device for that period and then download the video data and store it as part of the background recording on the DVMS storage subsystem. The backfill operation shall be automatic and not require any user interaction.

The DVMS shall intelligently manage the backfill operation to ensure:

- Recordings that have been deleted from the DVMS are not backfilled.
- The backfill operation shall be prioritised so that gaps in the most recent background recordings are filled first.
- The backfill of a long duration of missing recording is split into smaller time periods with a maximum duration of 30 (thirty) minutes to prevent a single camera monopolising the backfill operation over all other cameras.
- A sliding time window shall be maintained to ensure that the DVMS only monitors for recording gaps that have occurred after the last backfill operation.
- The DVMS shall provide a buffer of up to 6 (six) seconds of time synchronisation difference between the DVMS Servers and the camera. The backfill operation shall not be affected provided the camera time does not differ from the DVMS server time by more than the defined buffer period.
- The DVMS shall provide an alarm notification if the camera time starts to differ from the DVMS Server time by more than the defined buffer period.
- All failures in the video edge backfill operation shall be logged by the system for diagnostic purposes.

4.7 DEVICE CONFIGURATION REDUNDANCY

The DVMS shall support the ability to configure more than a single instance of a camera. Each instance of the camera shall support unique configuration as allowed by the associated physical device.

It shall be possible to manage each instance of the camera by a separate Camera Server and record to a unique location to provide for redundant recording of video.

4.8 PRIVACY

Privacy of video data information is vital to protect the corporation using the DVMS as well as those monitored by the system. The DVMS shall provide the ability to further restrict access to recordings than the simple method of limiting operator access to specific cameras.

The DVMS shall provide additional privacy control by requesting authorization for the review of recordings on cameras that have this feature enabled. The authorisation will must be provided by a management level operator.

Authorization shall be provided by a second, unique user account to prevent any operator from authorising themselves to review video recordings on affected cameras.

Operators authorizing the review of recordings shall be presented with a dialog box requesting their user name and password. They will also set the period for which the authorization is active, after which authorization will need to be obtained again to allow recording review.

Authorization success and failure shall be recorded in the DVMS audit log.

It shall be possible to set a grace period during which recordings can be immediately reviewed without authorization. Once this grace period has expired, operators will need to obtain authorization to review recordings on the affected camera(s).

It shall be possible to configure the need for authorized recording review on a per-camera basis. Systems enabling this feature as a system-wide setting only will not be acceptable.

4.9 DIGITAL ZOOM AND IMAGE ENHANCEMENT

The DVMS User Interface for Integrated Operator Station and Browser Clients shall support the following capability on both live and recorded video:

- The ability to digitally zoom into an area of the image
- The ability to enhance the image viewed by adjusting the levels of brightness, contrast, noise levels and sharpness.

Digital Zooming and Image Enhancement settings shall not be persistent and shall be reset on navigation away from the currently-viewed live or recorded scene.

Digital Zooming and Image Enhancement settings shall only be applied to the image viewed by an operator making the changes on a specific operator workstation. The settings shall not affect other operator stations displaying the same video feed.

4.9.1 DIGITAL ZOOM

Digital zooming will be possible using all of the following methods:

- “Rubber-banding: using the mouse pointer, select the area to zoom in to by clicking and dragging the pointer over the area of interest
- Mouse Scroll Wheel: point to the area of interest and rotate the mouse scroll wheel to zoom in and out
- Using a zoom slider overlay or click on the “+” and “-“ digital zoom buttons on the digital zoom window

It shall be possible to return to the original scene by right-clicking anywhere in the video window or by clicking on a digital zoom overlay icon

Once zoomed into an image, arrows will be overlaid onto the video window at the top, bottom, left and right of the image allowing for digital panning and tilting within the zoomed image.

The system shall provide the ability to switch between digital and analog zoom for cameras that support analog zoom.

4.9.2 IMAGE ENHANCEMENT

It shall be possible to adjust the image brightness, contrast, noise levels and sharpness via slider bars accessed via buttons on the DVMS video window

4.10 SYSTEM AND USER AUDIT TRAIL

It is a requirement that all user actions on the DVMS Operator Station be recorded in a log file. User actions include:

- Interventions such as manual recording and configuration setting changes
- Cameras viewed
- Video replayed
- Video exported
- Cameras pan/tilt/zoomed and preset switching

This log must also contain a history of the status of the DVMS system components. It shall list the status of all cameras, streamers, servers and other system components including when they were disabled, failed or a tamper condition occurred.

The log of user and system actions shall be available in text format and automatically included with any video recordings that are exported.

The DVMS shall provide engineering logs covering all system events. Operator names shall be obfuscated in the logs for privacy reasons.

4.11 STORAGE

4.11.1 ONLINE STORAGE

The system shall hold a configurable amount of video in online storage. The amount of video stored on-line shall only be limited by the Camera Server's disk capacity, the disk capacity of storage solutions attached to the Camera Server or the dedicated network storage allocated to the Camera Server.

For each Camera Server a limit on available storage space for on-line video shall be configurable.

The system shall support RAID 0+1, 1, 3, 5 or 1+0 for video recordings (clips).

The DVMS shall support storage on both NTFS and non-NTFS storage media. Systems that mandate the use of NTFS file systems for storage shall not be acceptable.

4.11.2 STORAGE & DISK ADMINISTRATION

The DVMS shall provide a flexible means to configure storage behaviour within the system administration displays. The system will provide an automated and configurable means to delete those remaining clips closest to their deletion criteria in order to increase available system storage. The disk space configuration will be separately configurable for each drive volume on each Camera Server.

Deletions will commence once the amount of available disk space decreases to below a configurable limit. Alarms will be generated by the system to warn operators of this action. It shall be possible to configure the following parameters for this purpose:

- The Camera Server and volume being configured
- Threshold values for alarm generation (2 alarms: low and very low)
- Enable or disable automatic deletion of clips based on available disk space
- The threshold value used to initiate the automatic deletion of clips

- Inclusion or exclusion of clips marked for archiving in automatic deletions
- Threshold value to stop recordings when available storage is critically low
- Threshold value to restart recordings when more disk space becomes available

The DVMS shall provide a summary showing the available disk space, total disk space and number of recordings for directories used for this purpose on camera servers.

4.11.3 AUTOMATIC ARCHIVING

The DVMS shall provide the ability to automatically archive all recordings. It shall be possible to automatically archive any type of recording at a preconfigured period after the recording has completed.

It shall be possible to modify the automatic archive setting for each recording individually, as required.

In addition, the system shall also support manual archiving of video recordings.

4.11.4 OFF-LINE STORAGE

The Camera Server shall be able to manage several off-line media devices for archiving and restoring video. The Camera Server must use an IT industry standard archiving method that is supported by the Microsoft operating systems specified within this document.

Offline storage shall be possible on non-NTFS storage devices. Systems that mandate the use of NTFS file systems for storage shall not be acceptable.

At least one of the following off-line devices shall be supported:

- Network storage solutions
- USB-connected storage devices
- DVD-RW
- Magnetic tape media

If a user attempts to replay video stored in off-line media then the Camera Server will automatically restore and play the video if it is accessible to an automated data retrieval system, or shall prompt the user the make the media containing the video available to the archive device.

4.12 INTEGRATED OPERATOR STATION

4.12.1 VIDEO INTEGRATION USER TASKS

The following system tasks shall be performed from the Operator Station

- View live video
- Adjust the PTZ position of a camera
- Live video is automatically displayed on a monitor when an event occurs
- Search through the stored video clips of a camera
- An operator records an incident
- An operator records a snapshot of the current viewed video
- Add a new camera to the system
- Delete a camera from the system
- Change the configuration settings for a camera
- Provide alarm/event activated recording from the integrated Security System, Building Control System or Industrial Control System
- Search for video clips from different cameras
- Define and export video evidence
- Create a sequence (camera tour)
- Conduct a sequence (camera tour)

- Create a multiple camera view
- View a multiple camera view
- View live video from a custom schematic
- Add live video to a custom schematic
- Configure, schedule and tune Video Analytics
- Configure, schedule and tune camera tamper alarms
- Add new input or output devices on the streamers or IP cameras
- View the status of input or output devices on the streamers or IP cameras
- Command output devices on the streamers or IP cameras
- Change the configurations settings of input or output devices on the streamers or IP cameras
- Accept an Intercom call
- Initiate an Intercom call
- View the audit log
- Digitally zoom into live or recorded video
- Adjust the brightness, contrast, noise levels and sharpness of live or recorded video
- Control the washer and wiper function on a supported camera
- Manually fail the Preferred Database Server to the Backup Database Server and vice versa
- Manually fail a Preferred Camera Server to the configured Backup Camera Server or Camera Server Pool and vice versa

The following tasks shall also be performed from the Integrated Operator Station

- View the organization's Intranet from within the Operator Station window.

4.12.2 SECURITY, BUILDING CONTROL OR INDUSTRIAL CONTROL SYSTEM INTEGRATION USER TASKS

It shall be possible to perform the following tasks in the Security or Control System from the DVMS Operator Station:

- Acknowledge an alarm
- Reset an acknowledged alarm
- Control a security or control system point
- Run a report containing security information
- Run a report containing process control information
- Respond to a security alarm
- View security and control system information on a process control schematic
- Configure a security report
- Configure a point control schedule
- Change an access level and download it to all affected access controllers
- View Access Controller details

All alarms and events from the DVMS, Security and Control systems shall appear and be able to be managed from the same display on the Operator Station.

All alarms passed from the DVMS to the Security, Building Control or Industrial Control Systems shall have configurable priorities.

The system shall support the display of live video within custom display screens of the Security System, Integrated Building Management and Control System or Industrial Control System. The DVMS system shall support the simultaneous display of dynamic data from the Security System, Integrated Building Management and Control System or Industrial Control System and live or recorded video.

The system shall support the display of dynamic Intranet information on DVMS displays

4.12.3 EVENT RESPONSE ORCHESTRATION

Integration between the DVMS and Security Management System shall provide the following functional support to security operators:

- It shall be possible to call up a camera in the VMS Surveillance Console via selection in the Integrated Operator station
- It shall be possible to navigate to the camera location on the Integrated Operator Station site map via selection in the VMS Surveillance Console
- It shall be possible to call display nearby cameras from an incident triggered in the Integrated Operator Station. Nearby cameras shall be determined by a configurable distance from the event location.

4.12.4 REPORTING

The DVMS shall utilise the reporting infrastructure of the Security System, Integrated Building Management and Control System or Industrial Control System to provide the following standard reports:

- System Bookmark Summary: A report detailing the operator bookmarks added to the system and including camera name, camera number, date, time and bookmark text
- **Comprehensive Audit Report:** A report displaying an audit trail of all DVMS operator and system activities during a defined period
- **System Activity Report:** A report of actions and changes in the DVMS during a defined period
- User Configuration Report: A report providing details of user permissions including their security level and access rights to cameras, keyboards, mobile devices and facility locations
- **User Activity Report:** A report of all DVMS user actions during a defined period
- **Camera Configuration Report:** A report detailing the camera configuration settings within the DVMS
- **Clip Summary Report:** A report detailing the number and type of video clips recorded and which cameras were responsible for the recordings
- **Storage Usage Report:** A report detailing the available and consumed storage for specific Camera Servers in the DVMS
- **Video Analytics Event Report:** A report detailing the video content analysis activity in the system during a defined period
- **Controller Point Status Report:** A report detailing the status of the DVMS controller points within the Security System, Integrated Building Management and Control System or Industrial Control System
- **Process Point Status Report:** A report providing the status of all DVMS process points (cameras, control inputs and control outputs) within the Security System, Integrated Building Management and Control System or Industrial Control System
- **Camera Profile Configuration Report:** A report providing the configuration of video stream profiles allocated to each camera

It shall not be acceptable to require that these reports be created using separate software products such as Crystal Reports or equivalent.

It shall be possible to define the start and end times for the reports listed above where applicable to a defined time period.

4.13 IMAGE BLOCKING

The system shall provide the ability to limit the view of live and recorded video for specifically configured PTZ cameras to a specific group of users.

Images from these cameras will cease to be available to standard operators as soon as a user from the privileged group moves a camera away from its home preset position.

The ability to view live and recorded video from a camera that has had its imaged blocked in this manner shall be returned to normal once the privileged operator has stopped using the camera and the reservation period for that operator has lapsed.

4.14 NETWORK

The Network Management Station shall perform the following functions:

- Provide a graphical display of the network topology
- Provide network traffic statistics for each LAN port
- Configuration of network equipment
- Support standard Management Information Bases (MIBs)

4.15 INTERNATIONAL LANGUAGE SUPPORT

The DVMS Operator Station shall be fully translatable into the local language. This includes languages not supporting the European character set (e.g. Chinese). All text displayed in the DVMS user interface shall be stored in the DVMS database to allow for easy translation to another language. The process of translating a system shall be done by editing the DVMS database and replace all English words with the required local language equivalent.

Language translation packs for the DVMS shall be available in the following languages:

- Dutch
- German
- French
- Spanish
- Italian
- Russian
- Danish
- Finnish
- Simplified Chinese
- Traditional Chinese
- Korean

4.16 APPLICATION DEVELOPMENT INTERFACE

The DVMS shall provide for the ability of custom developed applications to access and control the DVMS system using a complete application development interface. These applications shall be able to be developed without the need to contact the DVMS manufacturer. Complete documentation of this application development interface shall also be provided.

The DVMS shall provide a browser-agnostic, zero install video player component to support integration to third party systems. The video player shall support both H.264 and H.265 video encoding formats.

4.17 SYSTEM DIAGNOSTICS

The DVMS shall provide diagnostic modules to assist with system health assessments and collection of diagnostic information.

The Diagnostics applications shall provide a unified user interface for running tests, recording system activity, collecting diagnostic information and viewing system log files.

It shall be possible to collect diagnostic information on all components of the DVMS application including Database Servers, Camera Servers, Clients and network activities.

4.18 SYSTEM MAINTENANCE

The DVMS shall provide the ability to upgrade to future versions of the software without the loss of recorded video, except for the time taken to move a camera to a Backup Camera Server.

Zero recording loss upgrades shall be accomplished by the combined use of Redundant Database Servers, Redundant Camera Servers and edge recording and backfill.

5. SERVICES

The vendor should be capable of providing supporting services as detailed in the following sections.

5.1 TRAINING

The vendor either at vendor's premises or on site shall provide standard training on all aspects of the system.

5.2 CONFIGURATION SERVICES

The vendor should be able to supply all necessary configuration services if required including controller configuration, database configuration, etc.

5.3 INSTALLATION SERVICES

The vendor should be able to provide installation services for the system including validation services if necessary.

5.4 HARDWARE MAINTENANCE

The vendor should be able to provide hardware maintenance and spare parts support if required.

5.5 SOFTWARE ENHANCEMENT & SOFTWARE SUPPORT

The vendor should be able to provide a comprehensive software maintenance and enhancement program for on-going support of the system