BOSCH
Invented for life

BVMS 10.0.1 - A&E Specification

Author: Verhaeg Mario (BT-VS/PAS4-MKP)
Date: 3 August, 2020

1 Document information 3
1.1 Version history 3
1.2 Extensions 3
2 Summary 4
3 Technical specifications 5
3.1 Video management system 5
3.2 Storage Management System 16
4 Cameras 18
5 Monitor walls 19
6 Bosch specific hardware 20
6.1 Allegiant video matrix switchers 20
6.2 Audio Intercom 20
6.3 Video surveillance keyboards 20
6.4 Intrusion panels 21
6.5 Access control 21
6.6 Bosch Recording Station and DiBos 22
6.7 Digital Video Recorders 22
7 Standards 23

1 Document information

Project	BVMS 10.0.1
Reference	n/a
Version	7
Last modified	03 August 2020

1.1 Version history

Version	Date	Author	Comment
7	2020-08-03	Verhaeg Mario (BT-VS/PAS4-MKP)	

1.2 Extensions

The adjustments made for BVMS 10.0.1 are marked in blue.

2 Summary

This summary includes a generalized description of special functionality of the BVMS.

Topic	Requirement
Scripting	The video management system shall provide a built-in command script editor that allows customized command scripts to be written to control virtually all the system functions. Command scripts may be activated by system operators or automatically in response to alarms or system events. The built-in command script editor shall support C# and VB.NET.
Resilience	The video management system shall be highly resilient to failure. Even in a concurrent failure of all management server(s), video recording manager(s) and iSCSI storage device(s), the operators shall still be able to view & control cameras as well as playing back the video from cameras with a memory card or other form of fail-over recording.
Alarm Management	The video management system's alarm image pane rows shall be displayed in order of their priority, with rows for higher priority alarms always displayed above lower priority alarm rows. The display order for equal priority alarms shall be selectable between new alarms displayed above existing alarms, or new alarms displayed below existing alarms.
Alarm Management	The video management system shall support the association of workflows with alarms. Workflows shall consist of action plans and comment boxes. An action plan shall display a text document, HTML page, or web site that typically contains instructions for handling the alarm. Comments entered in the comment boxes shall be logged in the system logbook.
Forensic Search	All generated metadata shall be stored side-by-side to the video surveillance footage to enable operator to search through previous events without any pre-configuration of video analytic events.
Video Recording Manager	The storage management system shall support encoders and cameras which are using an edge network video recorder to directly stream video surveillance footage to an iSCSI storage device.
Video Recording Manager	The storage management system shall manage all disk arrays in the system as a single or multiple virtual common pool(s) of storage. It shall dynamically assign portions of that pool to the connected encoders, cameras, and server-based network video recorders.
Camera recording	Cameras utilize an on-board network video recorder, and are able to write directly to the storage device without using a server-based network video recorder.
Camera recording	Cameras utilize an on-board caching mechanism, which allows them to mitigate short network outages and continue recording without any loss of frames.
Intelligent tracking	It shall be possible for the operator to pick an object in a live stream and trigger a pan-tilt-zoom camera to focus and follow that particular object automatically.
Aviotec	The video management system shall support the detection of fire using edge-based intelligent video analysis.
Languages	The video management system specified shall support the following languages: English, German, Dutch, Italian, Portuguese, French, Spanish, Simplified Chinese, Traditional Chinese, Russian, Hungarian, Czech, Danish, Finnish, Greek, Norwegian, Polish, Swedish, Thai, Turkish, Japanese, Korean, Arabic and Vietnamese.
Security	The video management system shall be able to encrypt recorded video data using AES-256 without reducing the performance (number of cameras and throughput) of the recorder.
Person identification	The video management system shall offer an embedded person identification solution.

3 Technical specifications

3.1 Video management system

3.1.1 Client software

1. The video management system workstations may be connected to up to 4 monitors where each monitor may be configured to display live streaming video, playback video, site maps, or alarms.
2. The video management system client application software shall provide the user interface for system monitoring and operation. The video management software client application maintains live monitoring, storage retrieval, and alarm handling.
3. The user shall be able to search the logical tree for item (for example, camera) names.
4. The video management system shall provide a user-dependent bookmark tree.
    a. The bookmark tree shall allow saving a time period or a single point in time for later investigation and export.
    b. Bookmarks shall be available both for live mode and for playback mode.
5. The video management system shall provide a user-dependent favourites tree.
    a. The favourites tree shall allow maps, folders, and devices and complete views (image pane patterns with camera assignments) to be configured by each user in a user-defined structure.
    b. The user's favourite tree shall be available irrespective of the computer with which he logs on to the system.
    c. It shall be possible to adapt the different views per image pane using e-pan-tilt-zoom and to save the multi-view as a favourite.
    d. When selecting the favourite, the customized live view of the same camera(s) are called up on screen.
6. The video management system shall provide an image window that displays a collection of image panes. The layout shall be optimized for standard (4:3) and wide-screen (16:9) monitors.
    a. With standard monitors the number of image panes per image window shall be variable between 1 (a single full-window video) and 25, arranged in a 5x5 grid. A slider shall be available allowing the grid size to be changed from 1x1, 2x2, 3x3, 4x4, and 5x5.
    b. With wide-screen monitors the number of image panes per image windows shall be variable between 1 and 30, arranged in grids of 1x1, 3x2, 4x3, 5x4, and 6x5.
    c. The number of image-panes available for the operator can be restricted based on user-group configuration.
    d. The video management system shall allow image panes to be enlarged or decreased in size within the grid. E.g., in a 5x5 grid, a single image pane can be enlarged to use 4 of the grid elements, creating a larger image within the grid. This allows an operator to view video in any pattern created within the grid structure.
        i. The operator shall not be restricted to pre-configured layouts, but shall be able to resize the image panes by clicking and dragging on the border of an image pane to drag the border horizontally or vertically or by clicking on a corner of an image pane to drag the corner diagonally to the desired size.
    e. The video management shall implement the concept of a selected image pane. The selected image pane shall be highlighted.
        i. There shall always be a selected image pane in the video management software client application application.
        ii. The selected image pane is always used for control commands, e.g. pan-tilt-zoom control, instant playback control, and audio replay.
7. The video management system shall support the audio sources of the connected encoders and IP cameras. It shall be possible to assign audio sources to cameras.
    a. In the video management software client application it shall be possible to turn on/off the replay of the audio per camera.
    b. The video management system shall support two different audio modes, single source audio and multi-source audio.
        i. In single source audio mode only the audio source assigned to the camera in the selected image pane is replayed.
        ii. In multi-source audio mode all audio sources of the cameras displayed in the client application are replayed.
8. The video management software client application shall support de-warped panoramic views for displaying 360° cameras.
9. The video management software client application shall provide de-warped playback for video recorded with a 360° camera.

10. The video management software client application shall be able to show a pre-configured de-warped scene for a 360° or 180° camera in an alarm scenario.
11. The video management system shall support automatic sequencing.
    a. It shall be possible for users to multiple-select cameras (control-click or shift click), and drag the multiple-selection to an image pane or a graphic representing an analog monitor connected to a decoder.
    b. All of the cameras in the selection shall then sequence in the image pane or monitor at a user-selectable rate.
    c. It shall also be possible to drag a folder to an image pane or analogue monitor. In this case, all of the cameras contained within the folder shall sequence.
12. The video management system shall support digital zoom of any image pane.
    a. A dedicated graphical control shall be provided in the user interface for this purpose.
    b. The mouse wheel shall control digital zoom when the mouse cursor is hovering over a selected image pane.
13. The video management system shall optionally display the information of the video analytics such as cells with detected motion, object masks, and trajectories in live and playback.
14. The video management system shall graphically display device states on its icons in the logical tree structure and on sitemaps.
    a. For cameras, the states shown shall include: loss of the analogue video signal, network connection loss, video recording, video signal too noisy, video signal too bright, video signal too dark, video de-adjusted, and video includes associated audio.
    b. For relays and contact inputs, the open or close state shall be indicated.
15. The video management software client application shall be able to host Windows based applications, providing the video surveillance operator with a single interface to run multiple applications.

Playback operations

1. The video management system shall support a time-line that provides a graphical overview of video stored on the disk.
    a. The time-line shall display a time scale that can be adjusted flexibly.
    b. For each camera displayed in playback mode, the time-line shall provide a line that depicts the video storage for that camera.
    c. The line shall be colour-coded to show if video is recorded for the displayed time period.
    d. The line shall be cross-hatched if the video is protected from deletion.
2. The video management system shall support simultaneous time-synchronous playback.
    a. Playback shall support single-step forward and backwards; play normal speed forward and backwards; play high-speed forward and backwards; and play slow-speed forward and backwards.
    b. When a playback speed above 4x, or below -4 times, is selected, the playback behaviour will be adjusted to enable smooth high-speed playback.
3. The video management system shall support search of recorded video for motion in user-specified areas of a camera image.
4. The video management system shall support search of recorded video with at least the following criteria: object size, object colour, direction, and speed as well as detecting objects entering or leaving designated areas.
5. The video management system shall support searching based on any combination of time/date-rage, event type(s), alarm priority, alarm state, and device(s).
    a. It shall be possible to save and recall search parameters.
6. The video management system shall support search for text data retrieved from ATMs, point of sales, bar-code readers or other applications. The search shall be performed in the logbook using a wildcard search.
    a. The search results shall appear in a list and selection of a result shall directly call up the exact video images recorded with the text data.
    b. The text data shall be displayed in the image pane of the corresponding camera in playback. It shall thus be possible to simultaneously display text data of multiple cameras.
    c. The operator shall be able to choose whether the text data is displayed on the right side or below the image pane.

Pan-tilt-zoom operations

1. The video management system shall support pan-tilt-zoom control with a dedicated graphical joystick control.
    a. The graphical joystick control shall support pan, tilt, zoom, iris, focus and aux command operations.
    b. It shall also support pan-tilt-zoom control via clicking the mouse in the image panes.

2. It shall be possible for the operator to pick an object in a live stream and trigger a pan-tilt-zoom camera to focus and follow that particular object automatically.

Performance

1. The video management software client application shall support the display of the live stream of multiple ultra HD cameras in without the impact on the smoothness of the displayed video by using Nvidia-based or Intel-based GPU decoding.
2. The video management software client application shall be able to decode the IP, IBP and IBBP GOP structures.
3. The video management software client application shall be able to decode video structures with an i-frame distance of 250 frames.
4. All video management software components shall be based on a 64-bit software architecture.
5. The video management system shall provide the user of the video management software client application to be able to select the video stream offered by a camera displayed on an image pane.
    a. For cameras configured to use two different streams for live view and for recording, operator shall be able to manually switch between the higher resolution stream and the lower resolution stream for a particular camera.
    b. The video management system shall provide the user of the video management software client application an option to enable an automatic switching between a high and a low resolution stream.
        i. The video management system shall automatically switch to a low resolution stream, if the user of the video management software client application opens multiple cameras on a monitor.
        ii. The video management system shall automatically switch to a high resolution stream, when the user of the video management software client application maximizes a camera on the monitor or if he user of the video management software client application zooms in to see more details.

Maps

1. The video management system shall support site maps with hot-spot icons for devices (cameras, relays, inputs but also the system management components), command script initiation, camera sequence initiation, and links to other site maps.
    a. The site maps shall be capable of being zoomed.
    b. The DWF, PNG, and PDF formats shall be supported.
2. The hot-spot icons shall be configurable to optionally display the device name or link title.
3. The status of the devices is visually shown on the corresponding hot-spot icon on the map.
4. It shall be possible to configure, that the importance of the occurrence of a certain event of a device is especially highlighted.
    a. When the selected event occurs, a defined background colour will appear at the corresponding hot-spot icon on the map.
    b. In addition to the background colour, it shall be possible to configure, that the background colour is blinking to further highlight the importance of the occurring event.
5. It shall be possible to configure the priority of the events of devices to ensure, that only one event per hot-spot icon is visualized on the map when several events occur simultaneously.
6. The video management system shall provide a thumbnail of the live video, when the mouse is hovered over the camera icon on the map.
7. It shall be possible to select the pre-positions of a pan-tilt-zoom camera from the context menu of a hot-spot icon of a camera on the map.
8. It shall be possible to accept and clear alarms of triggered by a certain camera from the context menu of the hot-spot icon of that camera on the map.

Remote connectivity

1. The video management system shall provide a bandwidth transcoding service for all supported client devices.
    a. The transcoding service shall be able to assess the network link quality and speed and provide the most usable image according to the available network link quality.
    b. The video quality/bandwidth shall be adapter very quickly to link quality changes, which can occur on, for example, 3G/4G or WiFi networks.
    c. The transcoding service can be used to view for live and playback streams.
    d. When the operator digitally zooms inside an image managed by the transcoding service, the image source should send only the area covered by the zoom, using the whole bandwidth available. This should enable

operators with a low bandwidth to view details coming from a high definition or ultra-high definition video camera.
    e. During video replay, when the playback is paused, the transcoding service shall send a single, full quality image, to the client, allowing the operator to see all details.

Workstation clients

1. The video management system shall be capable to be deployed in a wide area network, such as the internet.
2. When the video management system is deployed in an open wide area network, the client components shall be able to use an SSH tunnel to communicate to central system components, such as the management server, cameras and the video recording system.
    a. Alternatively it shall be possible to setup a port mapping table within the configuration manager in order to map the public port to a private IP and port of the devices. The video management system shall provide a routing and remote access configuration tool to transfer the port mapping table to a routing and remote access service.
3. The video management system shall provide the possibility to the operator to view video streams (live and playback) transcoded by a transcoding service, in order view high quality images. There shall be an indication in the image pane of the video management software client application to indicate, that the stream is being transcoded.

Mobile clients

1. Mobile clients shall be able to access live and recording data of all IP cameras in the video management system.
2. The mobile video client shall be able to send pan-tilt-zoom commands and provide an option for the user to digitally zoom in.
3. The mobile video client shall be able to choose between high quality and smooth motion.
4. It shall be possible to access the video management system from mobile video clients with the user accounts configured in the video management system.

3.1.2 Alarm management

1. The video management system shall provide the capability to allow alarms to be schedule-dependent.
2. The video management system shall allow alarms to be individually allocated to specific user groups for processing.
3. The video management system shall support replication of events such that a single physical event causes multiple system events. These multiple events shall be independently configurable to allow independent handling of the alarms by multiple operator groups, or to be handled differently according to different schedules.
4. The video management system shall be programmable to selectively, per alarm and per user group, automatically pop-up the alarm video.
5. The video management system shall support display of alarm video in a special alarm image window so users do not have to search their display screens to find the alarm images.
    a. The video management system shall display alarm video in rows of alarm image panes, with 1 row per alarm, and with up to 5 image panes per row.
    b. The video management system's alarm image panes shall be configurable to display live video, playback video, text documents, site maps, HTML files, or web sites (URLs). Per alarm one playback video and one site map can be configured.
    c. The video management system's alarm image pane rows shall be displayed in order of their priority, with rows for higher priority alarms always displayed above lower priority alarm rows. The display order for equal priority alarms shall be selectable between new alarms displayed above existing alarms, or new alarms displayed below existing alarms.
6. The video management system shall provide an alarm reaction time of maximum 2 seconds when sufficient network bandwidth is available.
7. The video management system shall distribute alarm notifications, via entries in the alarm list of the operator user interface, to all members of the user groups to which the alarm is assigned. The alarms shall appear in all said users' alarm lists.
    a. The video management system shall operate as follows: when an alarm is accepted by a user, it shall be removed from the other users' alarm lists.
    b. The video management system shall allow a user to un-accept an alarm he has previously accepted. In this case, the alarm shall re-appear in the alarm lists of all members of the user groups assigned to this alarm.

8. The video management system shall support the association of work-flows with alarms.
    a. Work-flows shall consist of action plans and comment boxes. An action plan shall display a text document, HTML page, or web site that typically contains instructions for handling the alarm. Comments entered in the comment boxes shall be logged in the system logbook.
    b. The video management system shall be configurable to force an alarm work-flow. In this case, the alarm cannot be cleared until the workflow is processed.
9. The video management system shall offer the possibility to automatically clear alarms when the originating event condition is no longer true.
10. The video management system shall allow alarms to be configured to send pan-tilt-zoom cameras to prepositions or to execute camera aux commands on occurrence.
11. The video management system shall be configurable to put any IP-connected camera into alarm recording mode on alarm occurrence.
12. The video management system shall be configurable to send an e-mail or SMS message in response to an alarm.
13. The video management system shall be capable of displaying video on monitors connected to video decoders in response to alarms.
14. The video management system alarm response shall take advantage of the row and column arrangement of analogue monitor groups by associating a row of analogue monitors with each active alarm.
    a. Each alarm may display video on multiple monitors, limited by the number of columns in the analogue monitor group.
    b. As new alarms are received, alarm rows shall stack in priority order on the monitors.
    c. The video management system shall support for alarms to display video on multiple monitor groups, with configurable assignment of individual assignment of alarms to monitor groups.
15. The management server of the subsystem which triggered the alarm shall be indicated.
16. The video management system shall provide an instant playback function that displays recorded images on one or multiple image panes.
    a. Recorded images from a single camera may also be played back on multiple panes.
    b. Instant playback supports pause, play forward, play reverse, single step forward, single step reverse, fast-forward, and fast-reverse.
17. The video management system shall be capable of deactivating a camera in the configuration, stopping recording and event generation.
18. The video management system shall be able to automatically stop alarm-based recording after a configurable time-out.

3.1.3 IT infrastructure

1. Video from other sites may be viewed from single or numerous workstations simultaneously at any time. Cameras, recorders, and viewing stations may be placed anywhere in the IP network.
2. The video management system server components shall run as one or multiple services on Windows Server 2016, Windows Server 2012 R2, Windows 8.1 (64-bit) or Windows 10 (64-bit).
3. The video management system client components shall run as one or multiple applications on Windows Server 2016, Windows Server 2012 R2, Windows 8.1 (64-bit) or Windows 10 (64-bit).
4. The video management system shall support Lightweight Directory Access Protocol (LDAP) that allows integration with enterprise user management systems such as Microsoft Active Directory.
    a. LDAP shall also be available when sub-systems are used.
5. Software updates to the video management software client application and configuration software shall be automatically deployed from the management server.
6. The management server software shall provide management, monitoring, and control of the entire system.
7. The management server should be tested with 3rd party high availability and/or virtualization solutions, such as VMware vSphere, Microsoft HyperV and Stratus Everrun.
8. The video management system shall be capable of monitoring third-party equipment SNMP protocol.
9. The video management system shall provide a Management Information Base (MIB) to enable other Physical Security Information Management Systems (PSIM) to monitor the video management system by means of SNMP traps.
    a. The video management system shall support at least SNMPv2.

3.1.4 Camera sequences

1. The video management system shall support pre-programmed camera sequences. These sequences will allow cameras to be automatically displayed on the computer image panes and/or analogue monitors connected to decoders.
2. The sequences shall support simultaneous display on multiple image panes or monitors.
3. The sequences shall also support camera prepositions for each pan-tilt-zoom camera on each sequence step.
4. The system shall be configurable such that operators can select these sequences from the logical tree or a site map.
5. Pre-programmed camera sequences can be displayed in video management software client application and on monitor groups.

3.1.5 Resilience

1. The video management system shall support automated network replenishment.
    a. The recording is buffered within the memory of the IP camera to cover network outages. The video management system shall receive an event and be able to issue an alarm, when the storage in the camera reaches a critical buffer state as well as when recording is deleted due to the local storage capacity being used up. When an outage is resolved, the camera shall automatically replenish the gaps in the storage. This should be automated and should not require and user input.
2. The video management system shall ensure, that recording is not affected in any way by server failure.
3. The video management system shall ensure continues operation during management server down-times as live viewing, playback of recording and export of video data.
4. The video management software client application shall indicate its connection status to the management server.
    a. The client shall be able to continue to operate when the management server is not available.
    b. This shall include connected, disconnected, and configuration out-of-sync between management server and video management software client application.
    c. The connection state of the management server shall be indicated on the icon of the device tree.
5. The video management system shall be designed in such a way that configuration changes to any part of the system shall not interrupt operational tasks, until the operator decides to update re-fresh the workstation configuration.
6. The video management system shall be highly resilient to failure. Even in a concurrent failure of all management server(s), video recording manager(s) and iSCSI storage device(s), the operators shall still be able to view & control cameras as well as playing back the video from cameras with a memory card or other form of fail-over recording.
    a. The video management system shall be designed in such a way the management server downtime does not affect the functionality of the recording services (video recording manager, local storage, direct-to-iSCSI-recording), and digital video recorders.
    b. Continues recording and motion recording shall continue during the management server downtime; alarm recording will not be activated.
    c. During management server downtime the recording services shall still be able to change the recording parameters schedule dependent.
    d. When the failed system components are back on-line, no special user or administrator action shall be required for the system to be back to a normal working mode.
    e. If the video management software client application loses its connection to the management server, the user shall be able to continue working with the connected devices, accessing live and playback and be able to pan-tilt-zoom cameras.
7. A video surveillance operator shall be able to login to the video management system software client even when the management server is unavailable.
8. The video management system shall ensure that alarms are persistent after a graceful management server restart.

3.1.6 Scalability

1. The software components of the video management system can be deployed together on a single computer for small system applications or on separate computers and servers to meet large systems requirements.
2. The video management system client software is able to connect to multiple sub-systems (or sites) simultaneously:
    a. The video management system client software is able to connect to different sites simultaneously using a persistent connection, maintained and monitored by the video management system.

i. Each video management sub-system will act as an independent video management system, containing its own recording system(s), video management software client application(s) and server application(s).
ii. When a user accesses a subsystem, this user shall see all device states and all the user actions on the subsystem shall be logged.
iii. The video management system shall automatically detect when management servers are located in different time zones by means of the local time settings in the servers. The operator shall see from the server list in device tree, which management servers' time zone is currently displayed in the operator's User Interface. The operator shall be given the possibility to set his own operation time to a dedicated time zone of one of the management servers. Selected time zone shall be applied to live view, playback, the alarm list and the logbook. Operator shall also be able to select UTC time.
iv. The video management software client components user logging on to multiple sub-systems shall be able to simultaneously access the devices of up to 100 subsystems and a total number of 10000 encoders/cameras consolidated in all sub-systems.
v. The logical tree of an video management software client application displays the available devices for each configured management server of a subsystem and their connection status.

b. The video management system client software is able to connect to up to 20 sites simultaneously using a non-persistent connection, initiated manually by the video surveillance system operator. Although it is only possible to connect up to 20 sites simultaneously, it shall be possible to configure 9.999 sites in the system.
i. When connecting to a site, the operator shall receive feed-back, whether the connection to the site was successful, partially successful or whether it failed.
ii. It shall be possible to view live and recorded images from multiple cameras within a site using a single site license.

3. The video management system shall provide an easy and comfortable way to the operator to select and connect to a management server from a list of servers during logon. The tool shall provide a search function to quickly find the server by searching for content appearing in the name or description of the servers. This tool to connect to servers shall be capable of listing up to 9.999 servers in its list.

3.1.7 Scripting

1. The video management system shall provide a built-in command script editor that allows customized command scripts to be written to control virtually all the system functions. Command scripts may be activated by system operators or automatically in response to alarms or system events. The built-in command script editor shall support C# and VB.NET.
2. The system shall be configurable such that operators can execute the created scripts by double-clicking on representative icons in a logical tree or site map.
3. The system shall be configurable such that the created scripts can be executed automatically in response to a system event. The automatic event-driven execution shall optionally be schedule-dependent.
4. The system shall be configurable to execute a user-group dependent command script on user logon.
5. The system shall be configurable to execute an alarm-dependent command script on user acceptance of the alarm.

3.1.8 Eco system

1. The video management system shall offer connectivity to:
   a. face recognition systems.
   b. ground radar detection systems.
   c. perimeter detection systems.
   d. physical security management systems.
   e. license plate recognition systems.
2. The video management system shall be able to trigger alarms based on information received by these systems.
   a. The video management system shall be able to show an alarm object which is tracked by a ground radar system simultaneously from multiple angles, using multiple cameras.
3. The video management system shall be able to show and record:
   a. license plates which are send by a license plate recognition system.
   b. personal information which is send by a face recognition system.
   c. zone information which is send by a perimeter detection system.
   d. zone information which is send by a radar detection system.
4. The video management system shall be able to be modified using an SDK to:

a. verify alarm an alarm with other (databased) systems before presenting an alarm to an operator.
b. send information to other systems using customized protocols.

Interfaces with other systems

1. The video management system shall provide a documented Software Development Kit (SDK) to allow integration to and integration from third-party software.
2. SDK functionality shall require authentication to the system.
3. The SDK shall be accessible from all .Net programming languages.
4. A remote client SDK shall be available which allows for (remotely) customizing the actions of the video management system client software.
5. A remote server SDK shall be available which allows for (remotely) customizing the actions of the video management system management software.

Virtual inputs

1. The video management system shall provide a software interface that allows third-party software to generate events in the video management system.
    a. The software shall support any Microsoft .Net programming language (e.g. C#).
2. The video management system shall allow third-party software to include up to 10 data fields and an Alarm ID along with the virtual input event.
    a. These fields shall be searchable in the system logbook.
    b. The virtual input data shall be optionally displayed in the video management software client application playback mode synchronously with the associated video.

OPC

1. The video management system shall provide an OPC Server for integration into third-party software systems, such as building-management systems.
2. The OPC interface shall follow the OPC Alarms and Events standard.

Relays and digital inputs

1. The open/close states of inputs and relays from devices connected to the system shall be indicated on the video management system video management software client application user interface and can be queried via the video management system SDK.
2. Relays from devices connected to the system shall be controllable from command scripts, the video management system SDK, and icons on the video management software client application user interface.
3. Input and relay state changes from devices connected to the system shall be recognizable as events in the video management system.
4. It shall be possible to configure one malfunction relay used to indicate an occurrence with special severity. It shall be possible to configure compound events to trigger the malfunction relay.
5. The video management system shall interface to the Advantech ADAM 6000 family of digital I/O devices.
6. The digital inputs and relay outputs from the ADAM devices shall provide all of the features and functionality described in the Relays and Digital Inputs section of this document.
7. ADAM 6000 family of devices attached to the network shall be automatically discoverable via a network scan.

3.1.9 Video analytics

Edge analytics

1. The video management system shall support the detection of fire using edge-based intelligent video analysis.
    a. The video-based fire detection shall detect uncovered flames with minimum 1.6% of the picture width.
    b. Uncovered uprising smoke shall be detected with minimum 2.3% of the picture width.
    c. The detection shall detect test fires TF1 to TF8 according to EN54.
    d. For the detection of flames and smoke a minimum illumination level of 7 Lux shall be sufficient.
    e. In the occurrence of an event triggered by the camera due to fire or smoke detection, the specific alarm shall appear in the video management software client application, indicating, that this alarm is triggered by a fire or smoke detection.

   f. Results of the video-based fire detection and intelligent video analysis have to be available as metadata in addition to the video data transmitted for alerting, storage and forensic search.
2. The video management system shall support configuring the edge-based intelligent video analysis parameters from the configuration software.
3. The video management system shall react to events triggered by the edge-based intelligent video analysis of encoders or IP cameras.
4. All events shall be stored in the logbook of the video management system to allow to search through these events.
5. All generated metadata shall be stored side-by-side to the video surveillance footage to enable operator to search through previous events without any pre-configuration of video analytic events.
6. The video management system software client shall be able to show the alarm rules to the operator configured in edge-based the intelligent video analytics.

Server-based analytics

1. The video management system shall provide an integration with several server based analytics platforms.
2. All events shall be stored in the logbook of the video management system to allow to search through these events.

Person identification

1. The video management system shall offer an embedded person identification solution.
2. The person identification solution shall be configurable to operate in a GDPR compliant organization.
3. The person identification solution shall be able to recognize persons which are known by the system.
   a. The person identification solution shall be limited to store 5000 persons in order to prevent it being used in mass-surveillance applications.
   b. An operator is able to add and remove persons to the system, depending on the operators' system permissions.
   c. A system administrator is able to add and remove suspect lists to the system, depending on the administrators' system permissions.

3.1.10 Security functionality

1. The video management system shall allow the establishment of user groups that have access rights to specific cameras, priority for pan/tilt/zoom control, rights for exporting video, and access rights to system event log files. Access to live, playback, audio, pan-tilt-zoom control, pre-position control, and auxiliary commands shall be programmable on an individual camera basis.
   a. It shall be possible for one user group to access several sub-systems. Access rights for specific cameras, priority for pan/tilt/zoom control, rights for exporting video, and access rights to system event log files. Access to live, playback, audio, pan-tilt-zoom control, pre-position control, and auxiliary commands shall be programmable on an individual camera basis.
2. To reduce the chance of a successful brute-force-attack, the system shall not have a non-changable administrative account.
3. The video management system shall support dual authorization logon. It shall function as follows:
   a. Dual authorization user groups may be created.
   b. Logon pairs, consisting of any two normal user groups, may be assigned to each dual authorization user group.
   c. A separate set of privileges and priorities can be assigned for each dual authorization user group.
   d. For each user group assigned as part of a logon pair, it shall be configurable whether the group can- log on either individually or as part of the logon pair- or log on only as part of the logon pair.
   e. If a user that is part of logon pair logs on individually, then he shall receive the privileges and priorities of his assigned user group. If the same user logs in as part of a logon pair, i.e. being authorized by the second user, then the user shall receive the privileges and priorities assigned to the dual authorization group to which the pair is assigned.
   f. The logbook shall log the log on procedure to identify a single user or a dual authorization log on. Subsequent user actions shall be logged as the actions of the first user.
   g. Dual authorization shall also be available for systems utilizing sub-systems.
4. The video management system shall support to confirm the authenticity of recorded video data. The video management system shall support to check hash values against recorded video data of cameras, which provide a recording stream with hash values signed by its certificates.
5. Each user group shall only see items in the system's logical tree for which the administrator has granted access.

6. The video management software client application shall support a configurable inactivity logoff for security reasons.
    a. The video management software client application will logoff automatically when no activity is detected from the operator in a configured period of time.
7. It shall be possible to configure that the concurrent logon of the same user on different video management software client applications is being omitted.
8. It shall be possible to enforce a secure password policies for the password user define to log on to the video management software client applications.
    a. When secure password policies are enforced, the video management software client application will only accept passwords with:
        i. A minimum length of 8 digits
        ii. At least one capital letter
        iii. At least one capital letter
10. It shall be possible to lock an account after a configurable amount of log-in attempts.
11. It shall be possible to configure a maximum password age.
12. It shall be possible to de-activate a user-account.
13. It shall be possible to enforce an user to change the password on the next logon.
14. The video management system shall allow the establishment of user groups that have access rights to specific parts of the configuration, which shall at least be split into: devices; maps and logical structure; schedules; recording parameters; events; alarms; and usergroups.
15. The video management system shall be able to configure credentials for web-resources in order to prevent the operator logging into these resources manually.
16. The video management system shall support to enable an encrypted communication between the management server and a camera, between the video management software client application and the cameras and between the video recording manager and the cameras.
    a. The video management system client shall be able to decode video from a secured (AES-128) multi-cast stream.
    a. The video management system client shall be able to decode video from a secured (AES-256) uni-cast stream.
17. The video management system shall be able to encrypt recorded video data using AES-256 without reducing the performance (number of cameras and throughput) of the recorder.
18. The video management system shall be able to replay video data which is encrypted using AES-256.
19. The video management system shall support to enable an encrypted communication between the management server and camera and between the video management software client application and camera
    a. The video management system client shall be able to decode video from an encrypted (AES-128) multi-cast stream.
    b. The video management system client shall be able to decode video from an encrypted (AES-256) uni-cast stream.
20. The video management system shall automatically configure the Windows firewall during the installation of the system, depending on the installed system components.

3.1.11 Languages

1. The video management system specified shall support the following languages: English, German, Dutch, Italian, Portuguese, French, Spanish, Simplified Chinese, Traditional Chinese, Russian, Hungarian, Czech, Danish, Finnish, Greek, Norwegian, Polish, Swedish, Thai, Turkish, Japanese, Korean, Arabic and Vietnamese.
2. The video management system shall allow specifying the language per user group in order to enable multiple languages for different operators in one system. The video management system shall allow specifying the language for configuration software. If "Default System language" is specified, the system shall use the same language as the Operating System language.

3.1.12 Interoperability

ONVIF Profile-S

1. The video management system is listed as an ONVIF Profile-S conformant product on the ONVIF website.
    a. The software manufacturer will offer a service which certifies non ONVIF Profile-S camera with the video management system.
2. A scan functionality will allow the discovery of ONVIF Profile-S cameras.

3. It shall be possible to provide basic configuration of ONVIF Profile-S cameras from within the video management system, such as general camera settings (e.g. multicast streaming), recording profiles (including codec, resolution, frames per second) and audio profiles.
4. It shall be possible to use the events provided by an ONVIF Profile-S camera to trigger events and alarms in the video management system. When the events of a specific ONVIF Profile-S camera model are mapped to the camera events in the video management system, it shall be possible to apply this mapping to all cameras of the same camera model in the system.
5. It shall be possible to export and import the event mapping of ONVIF Profile-S cameras for the purpose of using the same event mapping on other installed systems.
6. It shall be possible for operator to access live streams and to control pan-tilt-zoom functionality of ONVIF Profile-S cameras.
7. It shall be possible to record ONVIF Profile-S compliant cameras.
8. It shall be possible to view the connection status of ONVIF Profile-S compliant cameras in the video management software client application.
9. It shall be possible to display ONVIF Profile-S compliant cameras in live view on a digital monitor wall connected to a workstation or a video decoder.

RTSP

1. It shall be possible to connect cameras and/or other video sources via a RTSP stream to the video management system.
2. It shall be possible to record the RTSP stream of cameras and/or other video sources that are connected to the video management system.

3.1.13 Configuration

1. Configuration software software shall provide the user interface for system configuration and management.
2. The video management system shall auto-discover encoders, decoders, Bosch VRM devices and Bosch DVRs. Device detection shall support devices in different subnets.
3. The video management system shall auto-discover Bosch IP devices with their default IP addresses, and allow auto-assignment of unique IP addresses.
4. The video management system shall be able to simultaneously configure multiple Bosch encoders or decoders, even of different types. When devices of different types are being configured, only the parameters available in all devices are available for configuration.
5. The video management system shall provide an administrator-configured logical tree. The logical tree shall be freely configurable with any tree structure, with nodes consisting of folders or maps, and leaves consisting of devices (cameras, inputs, and relays), sequences, documents, URLs, or command scripts.
6. It shall be possible to configure per workstation and individually per camera which encoding stream (stream 1 or stream 2) of these devices shall be displayed by default.
7. The video management system shall support a centrally stored user profile to store settings individual for each operator.
    a. These settings shall include but are not limited to sequence dwell times, instant playback replay time and image pane ratio settings (16:9 or 4:3) individually per monitor.
    b. These settings shall be available independently of the physical workstation to the operator.

Configuration changes

1. Configuration changes made in the video management system configuration software shall modify a working copy of the configuration, and shall not affect the active operating configuration.
2. It shall be possible to activate the working copy through a user action in the configuration software, at which point the working becomes the new active operating configuration.
3. It shall be possible to set a date and time in the future at which the working copy becomes active.
4. It shall be possible to view a list of all configuration activations that have been applied to the system. It shall be possible to select any of the activated configurations, and have the system "roll back" to an earlier configuration.
5. It shall be possible to activate a configuration and leave it to the operator to refresh the configuration locally instantly or at a later point in time. It shall be possible to enforce a configuration activation for every video management software client application connected to the management server.
6. It shall be possible to create and export a reports of the current configuration in CSV-format for the purpose of documentation. There shall be reports for the following configurations:

a. Recording schedules
b. Task schedules
c. Cameras and Recording Parameters
d. Stream and Quality Settings
e. Event Settings
f. Compound Event Settings
g. Alarm Settings
h. Configured Users
i. User Groups and Accounts
j. Device Permissions
k. Operating Permissions

3.1.14 Scheduling

1. The video management system shall provide up to 10 different and independent programmable recording schedules. The schedules may be programmed to provide different record frames rates for day, night, and weekend periods as well as special days. Advanced task schedules may also be programmed that could specify allowed logon times for user groups, when events may trigger alarms, and when video exports should occur.

3.1.15 Logbook

1. The system shall protocol every event and alarm in an SQL database. The alarm entry shall contain the camera titles that have been recorded due to this alarm.
2. The logbook shall be able to store at least 500,000 entries per hour. If the capacity of the logbook is filled up the oldest entries will be deleted to create space.
3. The user shall be able to search the logbook for events and alarms. The user shall be able to export the search results into a comma separated value list (CSV).
4. The system shall include and install a ready-to-use SQL database. The system shall optionally allow the usage of a separately installed SQL database.
5. The retention time of the system's logbook shall be configurable.

3.1.16 Exporting of video footage

1. The video management system shall export video and audio data optionally in its native recording format to a CD/DVD drive, a network drive, or a direct attached drive. The exported data in native recording format shall include all associated metadata. Viewer software shall be included with the export. Once installed, the viewer software allows playback of the streams on any compatible Windows PC.
2. The video management system shall export video and audio data optionally in MP4 or MOV format to a CD/DVD drive, a network drive, or a USB drive. The exported data in MP4 or MOV format may be played back using standard software, for example VLC.
3. It shall be possible to password protect the video export. The export can then only be opened and viewed when the corresponding password is entered.
4. The video management system shall write a digital signature to the exported video. This shall allow the viewing client to verify, that the imported and opened video has not been tampered. The video management system shall provide a warning in case that the video has been tampered. This shall be done by means of the checksum of the digital signature.
5. The video management system shall offer a way to replay native exported video footage without having to install software on the client workstation.

3.2 Storage Management System

1. The video management system shall support to configure an alarm whenever video recording is manually deleted.
2. The video management system shall be capable of managing multiple storage management systems simultaneously.
    a. The operator will not see which camera is connected to which storage management system.
3. The storage management system, such as storage devices and fail-over settings, shall be configured from the video management system configuration software.
4. When devices are using a network video recorder on the edge:

   a. The recording parameters, such as stream quality settings, shall be configured in the recording tables of the video management system configuration software. These settings will be replicated into the devices connected to the encoders and camera connected to the video management system.
   b. A server-based network video recorder, writing the streams to a storage environment, is not needed.
5. When devices are using a server-based network video recorder:
   a. The recording parameters, such as stream quality settings, shall be configured in the configuration of the camera itself.
6. The storage management system shall support encoders and cameras which are using an edge network video recorder to directly stream video surveillance footage to an iSCSI storage device.
   a. The storage management system shall not be involved in the processing of the data.
7. The storage management system shall support ONVIF Profile-S cameras and encoders to stream video surveillance footage via a server-based network video recorder to an iSCSI storage device.
8. The storage management system shall manage all disk arrays in the system as a single or multiple virtual common pool(s) of storage.
   a. It shall dynamically assign portions of that pool to the connected encoders, cameras, and server-based network video recorders.
   b. The transfer rate of the data from the encoder, camera or server-based network video recorder is limited by network speed and the performance of the iSCSI storage device.
9. When a camera breaks, the recording-track of the broken camera can be re-attached to the recording-track of the new camera.

3.2.1 Pre-alarm recording

1. The pre-alarm shall be recorded in the local storage of IP cameras supporting automatic network replenishment and only be transferred to the central storage in the event of an alarm in order to reduce network strain caused by pre-alarms.
2. It shall be possible to configure up to 7 different pre-alarms for each IP camera supporting Automatic Network Replenishment for different events or compound events.

3.2.2 Storage devices

1. The storage management system is designed to work with iSCSI based recording devices.
2. The storage management system is designed to work with Microsoft Windows (Storage) Server based recording devices.

3.2.3 Cameras

1. Cameras utilize an on-board network video recorder, and are able to write directly to the storage device without using a server-based network video recorder.
2. Cameras utilize an on-board caching mechanism, which allows them to mitigate short network outages and continue recording without any loss of frames.

4 Cameras

1. It shall be possible to configure for fixed cameras and moving-cameras, that the camera automatically focuses and follows an object which is detected by edge-based video analytics.
2. The video management system shall support all Bosch Security Systems H.264 encoders and H.265 encoders, decoders, IP fixed cameras, and IP moving cameras.

5 Monitor walls

1. The video management system shall support monitors connected to IP decoders.
2. It shall be possible to configure monitors in flexible lay-outs, depending on the decoders' capabilities.
3. It shall be possible to group monitors into logical monitor groups, representing a physical installation (such as a wall with 2 rows and 4 columns of monitors).
    a. The video management system shall be able to control up to 50 monitor groups and up to 128 decoders in total.
4. It shall be possible to restrict access to monitor groups to specified video management software user groups.
5. The video management system shall support the display of IP cameras on the Barco Transform N series with up to 64 cameras.
6. The video management system shall support switching of cameras to monitors connected to decoders. The cameras shall be selectable via drag and drop from the logical tree.
7. The video management system shall be able to automatically assign a camera to a decoder and set it to full-screen when an alarm is accepted.
8. The video management system shall be able to assign a camera to a decoder using scripting.
9. The video management system shall be able to change the lay-out of the decoder using scripting.
10. The video management system shall be able to show a preconfigured de-warped scene (from a 360° or 180° camera) on a decoder in an alarm scenario.

6 Bosch specific hardware

6.1 Allegiant video matrix switchers

1. The video management system shall interface with the Bosch Allegiant family of video matrix switches. Video Encoders shall be connected to one or more monitor outputs of the matrix switcher to provide the video interface.
2. The video management system shall automatically import the camera names from the matrix switch.
3. Matrix switch cameras shall behave the same as IP cameras in the video management system video management software client application, with the following exceptions:
4. The video management system shall receive and process events from the matrix switch, including alarm events and video loss events.
5. The video management system shall support switching of cameras on the matrix switch monitors via context menus on the Allegiant cameras in the video management system logical tree.
6. It shall be possible to configure the system to use the Matrix Switch pan-tilt-zoom connections to control pan-tilt-zoom cameras when the video is looped from the Matrix Switch inputs to video encoders. The configuration interface shall allow specification of the logical camera numbers in the Matrix Switch, then the video management system shall route pan-tilt-zoom commands for corresponding cameras to the Matrix Switch.

6.1.1 CCL Interface

1. The video management system shall emulate the Allegiant Command Console Language (CCL). It shall be possible to select the Allegiant model that shall be emulated.
2. CCL commands shall control:
3. The video management system shall receive the CCL commands on a freely definable serial port on the management server.

6.2 Audio Intercom

1. The video management system shall support bidirectional audio intercom functionality. Audio intercom streams audio data from an video management software client application to the audio output of Bosch encoders.
2. The audio intercom function shall be activated by a button in the video management software client application Workstation.
    a. When the button is pressed the operator shall be able to speak into a microphone on the client computer. The audio shall be transmitted to the audio source which is assigned to the currently selected camera.

6.3 Video surveillance keyboards

1. The system shall allow system control via the Bosch IntuiKey family of keyboards, including the KBD-DIGITAL and KBD-UNIVERSAL
2. The Bosch IntuiKey keyboards shall support the control of devices within subsystems, i.e. with a keyboard connected to a video management software client application the desired subsystem's management server shall be selectable.
3. Physical keyboard connections shall be possible to both Bosch VIP-XD Decoders and to video management software client application Workstations.
4. When video surveillance Keyboards are connected to VIP-XD decoders, it shall be possible to:
    a. control the analogue monitor groups in the system via the video surveillance keyboard.
    b. control pan-tilt-zoom operation of the selected camera using the video surveillance keyboard joystick.
    c. control set and call-up pan-tilt-zoom prepositions of the selected camera using the video surveillance keyboard.
    d. execute pan-tilt-zoom and aux-commands of pan-tilt-zoom cameras on the selected camera using the video surveillance keyboard.
5. When video surveillance keyboards are connected to video management software client application, it shall be possible to:
    a. control the current Image Pane selection using the keyboard joystick.
    b. control the analogue monitor groups in the system or control any Image Pane on the connected video management software client application workstation, using the video surveillance keyboard.

c. control pan-tilt-zoom operation of the selected cameras using the video surveillance keyboard joystick.
d. control set and call-up pan-tilt-zoom prepositions of the selected camera using the video surveillance keyboard.
e. execute pan-tilt-zoom and aux commands of the selected pan-tilt-zoom camera using the video surveillance keyboard.
f. control playback of video, including both Instant Playback and Playback-mode synchronous playback, using the video surveillance keyboard.
g. include jog-shuttle emulation using the video surveillance keyboard joystick. When in jog-shuttle emulation mode:
    i. Rotating the Keyboard joystick will control forward and reverse playback, with playback speed proportional to the amount of joystick rotation.
    ii. Moving the joystick up shall set the video into slow forward playback mode. Additional upward movements shall incrementally increase forward playback speed
    iii. Moving the joystick down shall set the video into slow backward playback mode. Additional downward movements shall incrementally increase backward playback speed.
    iv. Moving the joystick right shall set the video into pause mode. Additional rightward movements shall step the video one frame forward.
    v. Moving the joystick left shall set the video into pause mode. Additional leftward movements shall step the video one frame backward.

6.4 Intrusion panels

1. The video management system shall be able to connect to Bosch UL-approved intrusion panels and browse the areas and devices configured in the panel in the configuration software.
2. The video management system shall be able to connect to 40 intrusion panels.
3. The video management system shall be able to map the events of the intrusion panel to events in the video management system in order to use these events in the event and alarm engine of the video management system.
4. The video management system shall be able to use the events of the intrusion panel to create compound events to trigger actions.
5. The video management software client application shall indicate the connection and authentication state of the intrusion panels by means of icons.
6. The video management system shall support the following devices from the intrusion panel:
    a. Areas
    b. Doors
    c. Outputs
    d. Points
7. The states of these intrusion devices shall be shown on the icons in the device tree of the video management software client application as well as on the hot-spot icons of the map. The states that should show are:
    a. Arm, force arm and disarm areas of an intrusion panels
8. The user of an video management software client application shall be able to execute the following operations from the context menu of the intrusion device icons in the device tree as well as from the context menu on the corresponding hot-spot icons on the map:
    a. Silence areas of the intrusion panel
    b. Open and close outputs
    c. Unlock, secure and cycle doors
    d. Bypass and un-bypass points
9. All the user actions of the operator with regards to the intrusion devices in the video management system shall be logged.
10. The video management system shall provide separate user permissions for the above mentioned operations per user group.

6.5 ~~Access control~~

The access control integration is temporarily disabled and will be re-enabled in BVMS 10.1.

1. ~~The video management system client shall be able to provide an access-control based video-verification functionality. This functionality will enable an operator to manually grant or deny access to persons requesting access using the access control system.~~
2. ~~The video management system client shall provide a search mechanism to list the access control related events of a person, with a direct link to the surveillance video.~~
3. ~~The video management system client shall provide a search mechanism to list the access control related events of an entry point, with a direct link to the recorded surveillance video.~~
4. ~~The video management system shall be able to connect up to 5 access control systems.~~
5. ~~The communication between the video management system and access control system shall be encrypted using HTTPS (TLS).~~

6.6 Bosch Recording Station and DiBos

This functionality will be removed as of 2021-03-31

1. The video management system shall interface with the Bosch Recording Station (BRS)/DiBos v8 family
2. The video management system shall be capable of managing up to 100 BRS per Management Server and 500 in an Enterprise Management System.
3. The video management system's BRS-connected cameras shall behave the same as IP cameras in the video management system video management software client application, with the following exceptions:
4. In the playback mode of the video management system video management software client application, BVR-connected cameras shall appear in the graphical timeline, and can be operated identically to IP cameras.
5. Changing the configuration of a BRS/DiBos shall require the BRS/DiBos configuration software which is not integrated into the video management system.

6.6.1 Replay

1. The video management system shall have one video management software client application that can playback recordings stored on iSCSI devices, Bosch Recording Station/DiBos recordings simultaneously.
2. The video management system shall have one video management software client application that can export all recording to one single archive.

6.7 Digital Video Recorders

1. The video management system shall interface with the Bosch DVR 400, 600 and 700 series as well as DIVAR AN 3000/5000, DIVAR Network, and DIVAR Hybrid recorders.
2. The video management system shall be capable of managing up to 50 DVRs per Management Server.
3. The video management shall support live view, playback and pan-tilt-zoom of the cameras connected to the DVRs.
4. It shall be possible to switch controllable relays of the DVRs in the device tree of the video management software client application.

7 Standards

1. This product shall be manufactured by a firm whose quality system is in compliance with the I.S. /ISO 9001/EN 29001, QUALITY SYSTEM
2. The video management system shall be configurable to operate in a IEC 62676 conformant video surveillance environment.
3. The person identification solution shall be configurable to operate in a GDPR compliant organization.
4. The video management system shall be configurable to operate in a GDPR compliant organization.