BOSCH

Invented for life

BVMS - IEC62676-1

Author: Verhaeg Mario (BT-SC/PAS4-MKP)

Date: 5 July, 2019

1 Document information 3
1.1 Version history 3
2 Introduction 4
2.1 Summary 4
2.2 Standard 4
3 IEC62676-1 5
3.1 System requirements 5
4 Grading 23
4.1 Grading 24
5 IEC62676-1-2 33
5.1 System requirements 34
5.2 Grading 37
5.3 Transport level Security Requirements for Transmission 40

1 Document information

Project	BVMS 10.0
Reference	IEC62676
Version	40
Last modified	19 June 2019

1.1 Version history

Version	Date	Author	Comment
40	2019-06-19	Verhaeg Mario (BT-SC/PAS4-MKP)	

2 Introduction

2.1 Summary

Based on the evaluation described in this document a video surveillance system can be compliant to IE62676-1 section 1 and section 2 when BVMS is used as a video management system. A video surveillance system using BVMS as a video management system can be configured to match security grade 4.

2.2 Standard

IEC 62676 is a series of standards on video surveillance systems for use in security applications.

IEC 62676-1 consists out of 2 parts:

1. Video surveillance systems requirements
2. Video transmission - general video transmissions - requirements

IEC 62676-2 consists out of 3 parts:

1. Video transmission protocols - general requirements
2. Video transmission protocols - IP interoperability implementation based on HTTP and REST services
3. Video transmission protocols - IP interoperability implementation based on web services

IEC 62676-3 consists out of 1 part, describing analog and digital video interfaces.

IEC 62676-4 consists out of 1 part, describing application guidelines.

This document describes the conformance of BVMS to IEC 62676 part 1, section 1 and section 2. When BVMS is matching a specific requirement, the related item in the "Security grade" part of the table it marked **bold green**. The other parts of the IEC 62676 are not applicable on video management systems but relate to camera functionality.

3 IEC62676-1

3.1 System requirements

Section	Name	Requirements	Comments	Evaluation
6.1.1	Image capture	The captured images of the area of interest shall have sufficient accuracy and detail to enable users to extract the appropriate information defined in the image quality requirements.	Part of camera selection and system configuration.	**n/a**
6.1.1	Image capture	The capturing of images shall fulfil the customer objectives for image handling e.g. presentation and recording (concerning fps, resolution, colour depth and latency time) defined in the image quality requirements.	Part of camera selection and system configuration.	**X**
6.1.2.1	General	Any interconnections shall be designed to minimise the possibility of signals or messages being delayed, modified, substituted or lost in accordance with the requirements defined in 6.3.2.3.1.	Part of network and system design.	**X**
6.1.2.1	General	Monitoring of interconnections shall be provided in accordance with the requirements defined in 6.3.2.2.4 of the system security requirements.	Connections are monitored and connection loss is reported by default.	**X**
6.1.2.2	Common Interconnections	Image streams sharing common interconnection shall be designed and configured in a way that they do not adversely affect each other or any message transfer in any normal operation mode.	Part of network and system design.	**n/a**
6.1.2.2	Common Interconnections	For security grades 3 and 4, if a VSS is designed and configured in a way that single or multiple operators request video images via common interconnections, the design of the system shall ensure that the available capacity is sufficient for the anticipated operation of the VSS. This may be achieved by configuring the maximum throughput of image streams on the VSS. NOTE: Consideration should be given to prioritization of image streams, e.g. for recordings.	Part of network and system design.	**n/a**

Section	Name	Requirements	Comments	Evaluation
6.1.3.1	Presentation	If the VSS is able to present information, the following properties shall be declared by the manufacturer in the documentation: • maximum number of simultaneously displayed image sources; • resolution of displayed image(s); • size(s) of displayed image(s); • display rate (number of images displayed per s); • response time; • colour / B/W.	Information available in camera and VMS documentation.	X
6.1.3.1	Presentation	When displaying images, whether they consist of the entire image source or a part of it, the proportions of the displayed image shall be the same as in the original image source. Any superimposed information e.g. timestamps, camera names produced by the system shall not affect the recorded image.	Camera names and timestamps are recorded in the image as part of the evidence chain, but this is configurable.	X
6.1.3.2	Analysis	Any superimposed information e.g. object masks, trajectory lines, and classification information, produced by the system shall be processed as meta data and shall not affect the image itself (see 6.3.3). Only a privacy mask is allowed to affect the field of view of an image for privacy reasons, in order to block out sensitive areas from view.	Metadata is recorded as a separate stream of which the overlays can be enabled or disabled.	X
6.1.3.3	Storage	Most systems modify the video images before they are stored (conversion between analogue and digital format, resolution changes, compression, watermarking, or encryption). In the documentation, all processes that might cause loss of information shall be clearly stated.		X
6.1.3.3	Storage	If redundant storage is not provided, images shall be stored on the storage medium in a manner that will enable the data to be displayed and copied using alternative devices.	Images can be exported manually or automatically in open formats.	X

Section	**Name**	**Requirements**	**Comments**	**Evaluation**
6.1.3.3	Storage	The following properties of the storage device(s) shall be declared by the manufacturer in the system documentation: • type(s) and number of video input channels or image streams; • type(s) and number of video output channels or image streams; • type(s) and number of other input channels or data streams; • maximum number of images stored per second for each channel or stream at the specified resolution; • maximum total number of images stored per second at the specified resolution when all channels or streams are connected; • maximum number of images displayed locally and/or at a remote workstation when storing at maximum rate; • maximum number of images stored when displaying at maximum rate locally and/or remotely; • resolution and size of stored images; • maximum bit rate per storage device and per stream; • storage capacity in hours at the chosen number of input channels or streams, images per second, resolution and quality; • compression (methods available, settings, compression rates); • time to recommence image storage after a system restart (e.g. on power loss).	Part of this information is available from Bosch, parts of this information needs to be generated and calculated by the system integrator as part of the system design.	X
6.1.3.3	Storage	The storing of video images shall not be influenced by any live image display and requests or image backup and export. The configured recording rate shall always be granted in every normal operation mode.		X
6.1.3.3	Storage	If a constant frame rate is specified the sequences of pictures shall provide images at equal time intervals.		X
6.1.3.3	Storage	The system shall be configurable such that a maximum storage time can be set. The VSS shall be capable of automatically deleting images once they have been stored for the set period of time. Recorded images marked as protected from being deleted, may be stored for a longer period of time. The maximum storage time allowable by the applicable national legislation should not be exceeded.		X

Section	Name	Requirements	Comments	Evaluation
6.1.3.3	Storage	The VSS shall offer information about: • the video input channels or streams being recorded; • the image storage usage in capacity and recording time; • remaining storage capacity.	This information is available in the VRM monitor.	X
6.1.3.3	Storage	The system shall be capable of indicating as specified in the system documentation, if the storage capacity is running low.	This information is available in the VRM monitor, including a prediction on the required and consumed storage space.	X
6.1.3.4	Image data backup / archiving	It shall be possible to extract and preserve the image data for evidential or other purpose. It shall be possible to extract or move the stored data so that it can be viewed or replayed in an alternative location. A means of playing back the extracted image data (e.g. archive viewer system) shall be available without compromising the ability of the system to continue to function as designed.		X
6.1.3.4	Image data backup / archiving	If digital data is transferred to a secondary storage medium then it shall be an identical copy of the original data and shall be called ´exact copy´.	Naming of exports is set by the script or the operator manually.	X
6.1.3.4	Image data backup / archiving	This data shall be viewable with an archive viewer system including all additional meta data (ATM, POS, VCA info, location identifying data etc.) or shall be recoverable into the primary system storage without any loss of information.	When the export is made in one of the Bosch native formats.	X
6.1.3.5	Image export	the image export shall not alter the original recording in the primary storage. The system shall be able to offer the selection of time range and image source to be exported or copied.		X
6.1.3.5	Image export	the exported data shall have an image source identifier and time stamp ´identifying´ images to guarantee order and completeness of image sequences.		X
6.1.3.5	Image export	the system shall be able to export or copy a single image as well.		X

Section	Name	Requirements	Comments	Evaluation
6.1.3.5	Image export	The system documentation shall specify the export formats supported		X
6.1.3.5	Image export	Printing of images onto paper shall not be considered as image export and does not satisfy requirements for image export.		X
6.1.3.6	Data format	Compression algorithms that require the use of proprietary software to obtain direct access to VSS data shall not be used unless the information to achieve this is made available (e.g. by a Software Development Kit). NOTE: Special or modified compression algorithms prevent direct access to the VSS data without the use of proprietary software, which makes replay of Images by third parties difficult.	Standard compression algorithms are used.	X
6.1.3.6	Data format	The methods of storage and/or transmission for video, audio and metadata shall use standard formats, codec's and containers. The data shall comply strictly with the standards and contain the full information required to decode the content.	Storage method: iSCSI; transmission for video, audio and metadata based on UDP or TCP using standard codecs and contains. Metadata structure is proprietary.	X
6.1.3.6	Data format	The format and the means of locating the data within the VSS files shall be available as international published standards IEC, ISO or ITU.	The data within the VSS files is based on H.264 and H.265 coding standards.	X
6.1.3.6	Data format	The system shall be able to export the image sequences in a standard format at an equivalent quality to the original and still displaying time and date information with no significant increase in file size.	ASF, MOV.	X
6.1.3.6	Data format	The format of the VSS files shall permit the size and aspect ratio of each image to be determined.	This is configurable in the camera.	X

Section	Name	Requirements	Comments	Evaluation
6.1.3.7	Encryption and watermark	The VSS format may contain checksums or other methods for ensuring that changes to the data may be detected but, where used, they shall not alter the compressed image information.	Video authenticity is available.	X
6.1.3.7	Encryption and watermark	If images are encrypted the encryption should not alter the image information. The methodology for encryption and decryption should be readily available to authorised users	Encryption of images available from BVMS 10 onwards.	X
6.1.3.8	Minimum metadata	The data contained within the VSS files shall, as a minimum, permit a UTC time stamp and camera identifier to be associated with each image and audio sample. For VSS without audio, the time stamp shall have a resolution of no less that one second. Where both video and audio are present, the time stamps shall have sufficient resolution to permit synchronised playback of the audio-visual streams.		X
6.1.3.8	Minimum metadata	The means for determining the time stamps and camera identifier on each image and audio sample shall be made public. There are many way of encoding time stamps, but whichever is used shall be stated.	The timestamps are exposed in the video as well as retrievable via publicly available SDKs.	X
6.1.3.8	Minimum metadata	The VSS format shall specify any time offsets that are applied to time stamps and give the method for converting each time stamp into a local time that is local to a time zone and which includes any applicable daylight-saving adjustment.		X
6.1.3.8	Minimum metadata	Time should auto update for changes between any daylight saving offsets and UTC		X
6.1.3.9	Multiplexing format	Where a VSS recording contains multiple steams of video (and audio) the VSS files shall incorporate metadata which permit the streams to be de-multiplexed. The method for demultiplexing shall be made public.	Video and audio streams from separate devices are stored in separate containers.	X

Section	Name	Requirements	Comments	Evaluation
6.1.3.9	Multiplexing format	It is permissible for the VSS format to contain other streams of data which are not essential for extracting the images and audio samples with their time stamps. The additional data streams may remain proprietary although it is recommended that their format is published so that they can be decoded independently of the manufacturer’s software.		X
6.1.3.9	Multiplexing format	It is recommended that each video and audio stream has a name which may be meaningful to the user of the VSS. Where names are present, the method for associating streams and their names shall be made public.	Configurable in the system (by names of system objects).	X
6.1.3.10	Image enhancements	If the system provides enhancement tools such as image sharpening, brightening or zooming in on a particular part of the image then any applied enhancements should not change the original recording. If an enhanced image is exported, an audit trail documenting these changes should exist.		X
6.1.3.11	Image export	VSS data exported from a recorder shall have no loss of individual frame quality, change of image rate or audio quality. There should be no duplication or loss of frames in the export process. The system should not apply any format conversion or further compression to the exported images, as this can reduce the usefulness of the content.		X
6.1.3.11	Image export	Minimum metadata (see 6.1.3.8) and authentication signatures, where they exist, should be exported with the images.	Only in native format.	X
6.1.3.11	Image export	The system should be capable of exporting images, and audio where applicable, from selected cameras (and microphones) within user-defined time periods.		X
6.1.3.11	Image export	The system should not lose functionality or performance during the export of data		X
6.1.3.11	Image export	The export method of the system should be appropriate to the capacity of the system and its expected use.	Mass export is available via separate tools.	X

Section	Name	Requirements	Comments	Evaluation
6.1.3.11	Image export	The system should display an estimated time to complete the export of the requested data The software application needed to replay the exported images should be included on the media used for export, otherwise viewing by authorized third parties can be hindered.	A progress bar indicates the remaining time for the export. The archive player can be included on the media.	X
6.1.3.12	Replay of exported images	If the export format meets a common non-proprietary standard then a proprietary export player may not be necessary. If the manufacturer chooses to produce proprietary replay software then the exported images shall be capable of being replayed on a computer via the exported software.	A proprietary export player is available. Additionally common standards can be used.	X
6.1.3.12	Replay of exported images	The replay application should: • have variable speed control including real time play, stop, pause, fast forward, rewind, and frame-by-frame forward and reverse viewing; • display single and multiple cameras and maintain aspect ratio i.e. the same relative height and width; • display a single camera at the maximum recorded resolution; • permit the recordings from each camera to be searched by time and date; • allow printing and/or saving (e.g. bitmap or JPEG) of still images with time and date of recording; • allow for time synchronized multi-screen replay; • allow for time synchronized switching between cameras upon replay; • allow replay of associated audio and other metadata; • be able to export the image sequences in a standard format (see 6.1.3.6) at an equivalent quality to the original and still displaying time and date information with no significant increase in file size; • clearly show the time and date, and any other information associated with each displayed image, without obscuring the image.		X
6.1.3.12	Replay of exported images	If removable hard drives are used as a primary export option (dependent on download scale) then the drive should be capable of being replayed using a standard computer, for example, on a Windows based operating system. This functionality is also desirable for any hard drive used in a VSS where this is not the primary means of export.	Hard-drives should not be removed from the system. Other efficient export tools are available.	X

Section	Name	Requirements	Comments	Evaluation
6.2.1	Operation	Operation of the user interface shall be self-explanatory, simple and fast for an operator. The system status shall be detected, processed and displayed automatically. Alarm situations shall be identifiable and accessible immediately with a consistent documentation of the event.		X
6.2.2.1	General	The system shall clearly distinguish between user requested and event-driven data. Alarm data may be given priority over continuously displayed data.	Alarm priorities can be configured overruling other activities.	X
6.2.2.1	General	Images presented to an operator shall be clearly labelled as live or replayed video. In addition event driven video shall be clearly labelled as such to differentiate it from user requested video.	Event-driven video will appear in the alarm images panes. Live, recorded or instant-replay state is clearly indicated.	X
6.2.2.2	Status of system functions	The VSS shall always be able to offer information about the status of the essential functions.	Status is visible in the logical and alarms can be generated.	X
6.2.2.3	Events and event driven activities	Triggers or messages shall be retrieved from a queue in the order of their arrival except when a means to prioritise these inputs is provided.		X
6.2.2.3	Events and event driven activities	Where the system provides the facility to prioritize alarms then the priority level shall also be indicated. In this case messages or triggers shall be retrieved according to the priority levels. Where a number of messages or triggers of equal priority are in the queue they shall be retrieved in the order of their arrival.		X
6.2.2.3	Events and event driven activities	General requirements for the indication of the priority are as follows: • the system shall indicate when more alarms exist than are currently being displayed; • In addition to the information actually displayed, additional information may be available on demand. The visibility of the prioritised information shall be preserved; • any normal operation of the VSS shall not prevent the indication of an alarm.		X

Section	Name	Requirements	Comments	Evaluation
6.2.2.3	Events and event driven activities	It shall be possible to distinguish between different system conditions that may have triggered the activity and between an alarm, a fault or tamper.	Using the alarm priority.	X
6.2.2.3	Events and event driven activities	The VSS shall offer means to indicate an alarm visually and audibly in order to get the attention of an operator.		X
6.2.2.3	Events and event driven activities	The VSS shall offer means to acknowledge alarms.		X
6.2.2.3	Events and event driven activities	For systems of security grades 3 and 4, on alarm the VSS shall be able to display alarm related information. The information presented for each alarm message shall include: • the origin or source of alarm; • the type of alarm; • the time and date of alarm.		X
6.2.2.4	System logs	Accurate and complete system logs shall be maintained for a period of time as defined in the OR. Data in the system log shall be organized and presented in chronological order. The system shall prevent unauthorised editing or deletion of system logs. A log shall be available for each operator's workstation.	The operating system is in charge of preventing editing or deletion of system logs. Some information is logged in the system logbook as well. This cannot only be edited by authorized users.	X
6.2.3	Interfacing to other systems	All system security requirements as defined in 6.3 shall be fulfilled even in cases where thee VSS is accessed or controlled by another system. The other system shall be seen as a system user with defined access rights.	An external system will not influence the security behaviour of the system itself.	X
6.2.3	Interfacing to other systems	Access levels to another system shall be consistent with the levels required by that system standard and shall not give unauthorised access to the VSS and vice versa.		X

Section	Name	Requirements	Comments	Evaluation
6.3.1	General	VSS security consists of system integrity and data integrity. System integrity includes physical security of all system components and control of access to the VSS. Data integrity will include prevention of loss or manipulation of data.	Physical security of system components is part of the system design. The prevention of loss and manipulation can be configured (for example, CHAP passwords on the iSCSI drives).	X
6.2.1	System integrity	VSS of security grades 3 and 4 shall be capable of backup and restore of all system data.	System data can be backed-up and restored. Video data can be exported, replayed, but not restored.	X
6.3.2.2.1	Failure notifications	For VSSs with a user interface which is normally manned by an operator (either remote or local), alarm conditions from the components and functions, where specified in this standard, shall cause an alert. The failure shall be notified at any time a new user logs in or the system restarts.		X
6.3.2.2.1	Failure notifications	The information to be presented shall include: • time and date; • origin and type of failure; In addition, where the system provides for the facility to prioritize messages then the priority level shall also be indicated.		X
6.3.2.2.1	Failure notifications	Notification of failures shall never cover or hide any important information display such as the area of interest in live images.		X
6.3.2.2.1	Failure notifications	For security grades 3 and 4, the system shall be able to detect repetitive failures from a component and shall be configurable to generate a single message which shall only be repeated each time a new user logs in or the system restarts.	Alarm suppression or the debounce time mechanisms can be configured.	X

Section	Name	Requirements	Comments	Evaluation
6.3.2.2.2	Monitoring of power supply	For security grade 4, failure of the primary and, if available alternative, power supplies to the system shall be monitored, with notification according to clause 6.3.2.2.1. In any case power supply failure shall always be indicated locally. The VSS shall attempt to resume normal operation after recovering from power loss. If the system is unable to resume after power has been restored, with the settings which existed before the power failure, this shall be logged and also indicated to an operator.	Power supply monitoring can be achieved using SNMP or based on connection loss messages.	X
6.3.2.2.2	Monitoring of power supply	The VSS shall be able to shutdown regular operation in a defined procedure without loss of stored data. For security grades 3 and 4 images shall not be held in a buffer for longer than 5 s without being written into the storage medium.	ANR should not be used to meet this requirement. System shutdown possible without losing data, but recording will (naturally) stop.	X
6.3.2.2.3	Monitoring of system functions and components	For security grades 3 and 4 the VSS shall manage device failure by indicating any failure of the essential functions within 100 s of the failure.		X
6.3.2.3.1	Tamper detection	If tamper is detected a tamper condition shall be set and a tamper alarm generated. The tamper alarm shall be logged and clearly separated from other conditions e.g. failure, alarm or normal operation.		X
6.3.2.3.2	Tamper protection of camera housings	The image capturing devices shall be protected against tamper in systems of security grade 3 and 4. Cameras should be placed out of reach and the fixing screws shall be tamper proof, to prevent un-authorised repositioning.	Camera requirement.	X
6.3.2.4.1	Protection against unauthorized access	For each VSS access to operation and data shall be governed by an authorisation scheme. This also includes access through a remote workstation or through an external system integrated with the VSS.	BVMS usergroup permissions can be set as needed.	X

Section	Name	Requirements	Comments	Evaluation
6.3.2.4.2	Access levels	For all grades of the VSS, there shall be several user access levels to the functions of the VSS or part(s) thereof. The user accessing the system can be either an operator or another system: 1. Access by any person 2. Access by any user 3. Access by system administrators 4. Access by service personnel or manufacturer	BVMS usergroup permissions can be set as needed. In this case at least four user-groups need to be configured.	X
6.3.2.4.3	Authorization	The VSSs shall provide logical **or** physical means to restrict access to the system or system part(s) with a key, password, code or similar access-limiting means or device.	BVMS provides logical means to restrict access.	X
6.3.2.4.3	Authorization	The passwords of users shall never be displayed or stored in clear text.		X
6.3.2.4.3	Authorization	A valid change of a password by the user itself shall always require a valid user login with the old one and the entry of the new password plus validation in an identical way.		X
6.3.2.5	Time synchronisation	For security grades 3 and 4 the time settings of various components of a VSS shall always be within ± 10 s of UTC	With the default BVMS embedded time server this is easily achievable. If more accuracy is needed (ms) a dedicated NTP server is recommended.	X
6.3.3.2	Data authentication	To verify the integrity of images and other data, VSSs of security grades 3 and 4 shall provide a method (e.g. watermarking, checksums, fingerprinting) to authenticate image and meta data and their identity.	Video authenticity check functionality	X

Section	Name	Requirements	Comments	Evaluation
6.3.3.2	Data authentication	The authentication method shall be applied at the time the data is recorded and shall notify the user if any of the following has occurred: • any of the images has been changed or altered; • one or more images have been removed from a sequence; • one or more images have been added to a sequence; • the data label has been changed or altered.	The authenticity hashes are added as metadata. Data can be manually checked or can be checked when it is exported from the system. Any modifications to the data will notify the user of possible modifications during the export or manual checking process.	X
6.3.3.2	Data authentication	VSSs of security grades 3 and 4 shall also provide a method by which the authenticity of copied and exported data is verified.	This is possible when a native export is done using the VRM eXport wizard.	X
6.3.3.2	Data authentication	The authentication method used shall be specified in the system documentation.		X
6.3.3.3	Data (manipulation) protection	VSSs of security grade 4 shall provide a method (e.g. encryption) to prevent unauthorized persons viewing the images and other data without permission.	Before BVMS 10.0 this was achieved using internal system permissions only. From BVMS 10.0 onwards encryption is available.	X
6.3.3.3	Data (manipulation) protection	VSSs of security grade 4 shall also provide a method to protect the confidentiality of copied and exported data.	Exported data can be encrypted.	X
6.3.3.3	Data (manipulation) protection	The method used to protect the data confidentiality shall be specified in the system documentation.		X

Section	Name	Requirements	Comments	Evaluation
6.4.1	VSS as primary mitigation of risk	IEC 62599-2 shall be applied to VSSs, where VSS is identified as the primary mitigation of the risk. These VSSs may be used for relevant security and safety applications e.g. as intruder or fire detection systems. The environmental stability of the VSS shall be of the same level in all grades. The VSS shall operate correctly in the environmental class specified in Clause 7 it is designed for and exposed to EMC conditions described in IEC 61000-6-3, IEC 61000-6-4 and IEC 62599-1:2010 ´Environmental test methods´. A VSS shall neither change state, suffer damage to components nor substantially change in performance. IEC 62599-1 describes environmental test methods which shall be applied to VSS components. In IEC 62599-2 sub clause 8.3.4 Conditioning, the requirement of Table 2 ´Voltage reduction of 100% for a ´Duration of reduction´ of 250 ´no. of periods´ or ´cycles of the voltage wave´ can be covered by VSSs in relevant security applications by the use of UPS. Functional tests to be applied for component evaluation shall be at least a test or measurement of the essential functions of the component. Acceptance criteria shall be that there is no change in the functioning of the component and no significant change in any measurement, during the environmental testing. A VSS component shall provide protection against electrical shock and consequential hazards by achieving compliance with the requirements of IEC 60950-1 or IEC 60065.	BVMS can run in an environment that meets these requirements. The requirements are not related to the software functionality.	X

Section	Name	Requirements	Comments	Evaluation
6.4.2	VSSs as secondary mitigation of the risk	If VSSs or parts thereof are not used for relevant security or safety applications e.g. not as intruder or fire detection systems, they shall be compliant to IEC 61000-6-1 or IEC 61000-6-2 and do not need to be compliant to IEC 62599-2. NOTE 1 The security family standard IEC 62599-2 needs only to be applied to relevant security applications, but not to video systems as auxiliary equipment. In these applications VSS is not identified as the primary mitigation of the risk. NOTE 2 Both standards include a lower degree of severity concerning voltage interruptions and a loss of functionality (e.g. image quality reduction) whilst conditioning (details see clause 4 in both standards) The IEC 62599-2 sub clause 8.3.4 Conditioning, requirement of Table 2 ´Voltage reduction of 100% for a ´Duration of reduction´ of 250 ´no. of periods´ or ´cycles of the voltage wave´ is only applicable to VSS components, parts or systems in security applications, which are essential for the detection of an intruder, e.g. as part of an intruder detection system. This does not include image display, observation, monitoring, identification or recording of intruders.	BVMS can run in an environment that meets these requirements. The requirements are not related to the software functionality.	X
6.5	Image quality	The imaging chain – consisting of image capturing, codec, transmission, handling, storage and display – shall be tested according to ISO 12233 clause 6.1 'Visual Resolution' (see Figure 5). The results shall be documented and reported according to ISO 12233, Clause 7.	This depends on the camera. BVMS will display the stream as it is served by the camera without modifications but no camera specific tests are made.	X
7	Environmental classes		BVMS can run in an environment that meets these requirements. The requirements are not related to the software functionality.	X
8.1	System documentation	Documentation relating to the components of a VSS shall be concise, complete and unambiguous. Information shall be provided sufficient to install, put into operation, operate and maintain a VSS. System specification and block diagram incl. specification of configuration: • installation details for operation and service; • inspection and maintenance procedures/routines.		X

Section	Name	Requirements	Comments	Evaluation
8.2	Instruction relating to operation	Instructions relating to the operation of the components of a VSS shall be designed to minimise the possibility of incorrect operation and be structured to reflect the access level of the user.		X
8.3	System component documentation	Documentation relating to VSS components shall be concise, complete and unambiguous. The documentation shall be sufficient to ensure the correct installation, putting into operation and maintenance of VSS components. Component documentation may be provided by the manufacturer on paper or an alternative medium. Sufficient information shall be provided to ensure the integration of each component with other VSS components. Component documentation shall include the following: • installation guide / manual; • technical system data specification: • performance specification; • min. requirements of equipment; • min. requirements of the environment; • standard to which component claims compliance; • inspection & maintenance procedures/routines; • name of manufacturer or supplier; • name of system integrator or installer, if appropriate; • description of equipment; • name or mark of the certification body (for components which are required to be certified); • environmental class.	The information is available and needs to be gathered and tailored for the specific system by the system integrator.	X

Section	Name	Requirements	Comments	Evaluation
8.3	System component documentation	Documentation shall be supplied to the user regarding the retention period of the system. The documentation should also provide the approximate times and methods to export each of the following, where available: • up to 15 min of recorded data per camera; • up to 24 h of recorded data per camera; • all of the data on the system. The latency time of the system reaction to a trigger shall be specified in the system documentation The method of defining the input priorities of alarm triggers shall be provided by the manufacturer in its documentation.	The information is available and needs to be gathered and tailored for the specific system by the system integrator.	X

4 Grading

4.1 Grading

It is the functions of the system rather than the VSS system components that are graded. Due to the wide range of the surveillance tasks functions of a VSS may have different security grades within one system. The system shall be given an overall grade for which the grade dependent requirements of this standard shall apply. When identified by the OR, or system design proposal, the functions of the VSS may use a different grade but this shall be applied consistently throughout the system. The tamper protection and detection requirements of 6.3.2.3 may be applied with different grades in various locations within the system as appropriate to the risk at that location. This shall be recorded in the OR or system design proposal and. This shall be determined by a risk assessment and be explicitly defined in the OR. The security grades shall be applied, where VSS is identified as the primary mitigation of the risk. It shall be noted that the risks identified may be best mitigated by other means than VSS.
Sections of grading or the grading of individual functions may only apply, if determined to be relevant in the risk assessment, OR, or system design proposal. Where not specified the default security grade is 1.

Source: 62676-1-1/CDV

Grade	Risk	Description
1	Low	A VSS intended for surveillance of low risk situations. The VSS has no protection level and no restriction of access.
2	Low-Medium	A VSS intended for surveillance of low to medium risk situations. The VSS has low protection level and low restriction of access.
3	Medium-High	A VSS intended for surveillance of medium to high risk situations. The VSS has high protection level and high restriction of access.
4	High	A VSS intended for surveillance of high risk situations. The VSS has very high protection level and very high restriction of access.

4.1.1 Requirements

Section 6.1.3.3, table 1: Storage

The VSS shall be capable of:	Comments	Security grade			
		1	2	3	4
data backup and/or redundant recording				X	X
operating a fail-safe storage (e.g. RAID 5, continuous mirror) or switching automatically over from one storage media to another in case of storage failure					X
reacting to a trigger with a maximum latency time of			1 s	500 ms	**250 ms**
replaying an image from storage with a maximum time after the incident or actual recording of	In general this depends on resolution, bitrate, network, type of storage, size of storage, and the performance of the client.			2 s	**1 s**

Section 6.1.3.4, table 2: Archiving and backup

The archiving shall offer:	Comments	Security grade			
		1	2	3	4
authentication of every single image and image sequence	Related functionality: video authenticity.				X
an automatically scheduled backup of alarm image data	Using the SDKs automated exports can be created.				X
a backup of alarm image data by manual request				X	X

The archiving shall offer:	**Comments**	**Security grade**			
		1	**2**	**3**	**4**
verify the successful image backup	Only for native exports.			X	X

Section 6.2.2.4, table 3, system logs.

The system shall log with time stamp (date and time), event, source:	**Comments**	**Security grade**			
		1	**2**	**3**	**4**
Alarms			X	X	X
Tamper				X	X
video loss and recovery from video loss				X	X
power loss			X	X	X
essential function failure and recovery from failure				X	X
fault messages displayed to the user					X
system reset, start, stop			X	X	X
diagnostic actions (health check)					X
export, print/ hardcopy incl. the image source identifier, time range			X	X	X

The system shall log with time stamp (date and time), event, source:	**Comments**	**Security grade**			
		1	**2**	**3**	**4**
user log in and log out at workstation with time stamp, successful and denied logins (local/ remote) including reason of denial (wrong password, unknown user, exceeded account)	In logbook as well as system logs.		X	X	X
changes in authorisation codes	logged in operator client system logs.			X	X
control of functional cameras					X
search for images and replay of images				X	X
manual changes of recording parameters	If manual recording is started by the operator this is logged.			X	X
alarm acknowledge /restore				X	X
system configuration change	no details on the change, only that something has been changed.			X	X
date and time set and change with current time and new time	Based on Windows event log functionality.			X	X

Section 6.3.2.2.4, table 4: monitoring of interconnections.

The system shall:	**Comments**	**Security grade**			
		1	**2**	**3**	**4**
repeatedly verify the interconnection at regular intervals with a maximum of	The debounce time can be configured to prevent repetitive events. Alarm duplicates can be suppressed as well.			30 s	10 s

The system shall:	Comments	Security grade			
		1	2	3	4
try to re-establish a interconnection with following number of retries before notification	The debounce time can be configured to prevent repetitive events. Alarm duplicates can be suppressed as well.			5	2
maximum time permitted before notification to an operator of an interconnection failure	In BVMS an alarm message notification can be configured either with the help of the ´debounce time´ configured to 180000ms inSG3, 30000ms in SG4. Alternatively you could use an Event Script			180 s	30 s

Section 6.3.2.3.1, table 5: Tamper detection

The system shall detect:	Comments	Security grade			
		1	2	3	4
video loss	BVMS supports video loss detection and notification in default configurations		X	X	X
if an image capturing device with a fixed field of view no longer includes the entire specified field of view				X	X
deliberately obscuring or blinding of the imaging device range				X	X
the substitution of any video data at image source, interconnection or handling	using the video authenticity functionality recorded video can be authenticated manually.				X
significant reduction of the contrast of the image					X

Section 6.3.2.4.3, table 7: Authorisation code requirements.

Authorisation code requirement:	Comments	Security grade			
		1	2	3	4
Number of possible logical authorisation keys	No limitation in password length.		> 10 000	> 100 000	> 1 000 000
Number of possible physical authorisation keys	The system itself does not provide a physical authorization method. This could be implemented on the operating system level.		> 3 000	> 15 000	> 50 000

Section 6.3.2.4.2, table 6: level of access

Function:	Comments	Access levels			
		1	2	3	4
System configuration	BVMS user groups	NP	NP	P	P
Change individual authorisation codes	BVMS user groups	NP	P	P	P
Assign and delete level 2 users and authorisation codes	BVMS user groups	NP	NP	P	P
Restoration to factory defaults	Operating system	NP	NP	P	P
upgrading of the system	Operating system	NP	NP	P	P
Start / Stop VSS or component	Operating system	NP	NP	P	P

Function:	**Comments**	**Access levels**			
		1	**2**	**3**	**4**
Key P Permitted NP Not Permitted.					

Section 6.3.2.4.4, table 8: data access

Function:	**Comments**	**Access Levels**			
		1	**2**	**3**	**4**
View live images and data	BVMS user groups	P	P	P	P
View stored images and data, if recordings are available	BVMS user groups	NP	P	P	P
View information about storage, if storage is part of the VSS	BVMS user groups	NP	P	P	P
Print and save video data	BVMS user groups	NP	P	P	P
Exporting of images and data	BVMS user groups	NP	P	P	P
Deletion of images and data (only with confirmation)	BVMS user groups	NP	NP	P	P
Key P Permitted NP Not Permitted.					

Section 6.3.2.4.5, table 9: access to system logs

Function:	**Comments**	**Access Levels**			
		1	**2**	**3**	**4**
View system logs	BVMS user groups	NP	P	P	P
Exporting from logs	BVMS user groups	NP	NP	P	P
Deletion of logs	Operating system	NP	NP	NP	NP
Key P Permitted NP Not Permitted.					

Section 6.3.2.4.6, table 10: access to system set-up

Protection of access to system set-up:	**Comments**	**Access Levels**			
		1	**2**	**3**	**4**
Configuration & set-up		NP	NP	P	P
Recovery from system failure		NP	P	P	P
Recovery from tampering		NP	P	P	P

Protection of access to system set-up:	**Comments**	**Access Levels**			
		1	**2**	**3**	**4**
Key P Permitted NP Not Permitted.					

Section 6.3.3.1, table 11: Data labelling

The VSS shall uniquely label data by:	**Comments**	**Security grade**			
		1	**2**	**3**	**4**
location (e.g. name of site)	Name of the system		X	X	X
source (e.g. capturing device labelled by camera number)	Name of the device in the system		X	X	X
date and time		X	X	X	X
date and time in UTC including offset for local time					X

5 IEC62676-1-2

The second part of IEC62676-1 is split into the following subjects:

Section	Description	Applicable to BVMS
4	Performance requirements	Yes
5	IP Video Transmissions Network Design requirements	No, related to the design of the IT network.
6	General IP requirements	No, specifies basic network requirements and protocols.
7	Video Streaming requirements	No, relates to video streaming of the camera.
8	Video Stream Control requirements	No, relates to video streaming of the camera.
9	Device Discovery and description requirements	No, relates to functionality of the camera.
10	Eventing requirements	No, relates to video streaming of the camera.
11	Network device management requirements (recommendation)	No, relates to network management protocols.
12	Network security requirements	Yes

> *Therefore this standard introduces different performance classes. For each application the requirements shall be specified and include classes for: time service accuracy (Table 1), interconnection timing (Table 2), throughput sharing (Table 3 and 4), streaming (Table 5), network jitter (Table 6) and monitoring (Table 7). Different functions of the system can have different performance classes.*
>
> ...
>
> *These requirements do not apply to mobile cell based interconnections, but shall be applied to fixed wireless network connections and transport applications, such as on-board systems.*

5.1 System requirements

Section	Name	Requirements	Comments	Evaluation
4.2.1	Network time services	The VTD shall never start streaming video for recording purposes, if the requirements below on the accuracy of the time stamping of the video frames cannot be granted.	The device itself cannot know the accuracy of it's time if it is not synchronized with an external time source.	X
4.2.2	Real-Time clock	The real time clock in the Video Transmission device should be synchronized with a time normal using RFC 2030, Simple Network Time Protocol (SNTP) Version 4 for IPv4, IPv6 and OSI. The addresses of the SNTP servers should come from the Time Server DHCP opt ion (4). The more accurate system time shall be used as default: the SNTP best accuracy is 0,25 µs, whereas the usage of the ´Time Server´ according to RFC 868 offers only a best accuracy of 1 s.	SNTP is used by default.	X
4.2.3	Accurate time services for the transport stream	As an option, Network Time Protocol (NTP) (Version 3) as detailed in RFC 1305 should be implemented when time services with an accuracy of 1 ms to 50 ms according to the requirements of table 1 are needed. The IP addresses of the time servers should come from the Network Time Server DHCP option (42). The Network Time Protocol should be tried first and only on failure shall Simple Network Time Protocol be used. A null Network Time Server DHCP option (42) means no server is available and Simple Network Time Protocol should be used.	NTP is used optionally.	X
4.3.1	Video transmission timing requirements	Video Transmission devices and their interconnections shall be designed in accordance with the system requirements IEC62676-1-1 as part of the VSS.		X
4.3.3	Connection capabilities	At no time the video transmission receiver shall allow the opening and initializing of connections to new video stream sources on cost of the video streams already displayed or recorded in order to avoid frame loss.	The users can be restricted in the amount of streams they can open on a workstation.	X

Section	Name	Requirements	Comments	Evaluation
4.3.3	Connection capabilities	At no time the video transmission receiver shall allow the display of live streams on cost of the video streams recorded, in order to avoid frame loss.	Viewing live streams will not impact the recording. When an all-in-one unit is used it is important to stay within the specific performance parameters.	X
4.3.3	Connection capabilities	If the qualities of video for live viewing by an operator and for recording needs to be different, the video transmission device shall offer a minimum of 2 streams of different quality settings.	This is a camera requirement which can be managed by BVMS for Bosch cameras.	X
4.3.3	Connection capabilities	If the quality of video for continuous recording and for event based alarm recording needs to be different, the video transmission device shall offer an additional stream, if the quality setting is different from the other 2.	This is a camera requirement which can be managed by BVMS for Bosch cameras.	X
4.4.2	Requirements on network jitter	The overall need is that even when video traffic has a jitter, the operator watching the video images shall not be destructed. For that reason, video security networks shall use techniques to minimize jitter for live and replay streams.	The BVMS decoders optimize this depending on the type of camera. Jitter increases the latency, so the jitter buffer is decreased for PTZ cameras to offer a smoother control experience.	X
4.4.3	Packet loss	The VTD shall be capable to detect packet loss and compensate the effects.	Bosch recording is based on TCP: packet loss is detected and packets are retransmitted by nature of the TCP. For live the decoder will, on best-effort, try to mitigate packet loss.	X
4.4.3	Packet loss	The VTD shall be able to provide an acceptable operator and user experience and video perception during packet loss. The reduction of the visual effects associated with the stream delivery is critical to the end-user retention. At least the visual impression of the packet loss shall be masked or hidden according to the needs to fulfil the surveillance task and objective.		X
4.4.3	Packet loss	A VTD shall offer state-of-the art error and loss concealment techniques.		X

Section	Name	Requirements	Comments	Evaluation
4.4.3	Packet loss	The VTD shall offer any packet loss or error concealment capability e.g. by using packet information of the encoded video from neighbouring macroblocks, prior or future frames, in order to estimate the video content of the current frame.	This is part of the H.264 and H.265 coding standards (usage of I-frames, B-frames and P-frames, for example).	X
4.4.5	Packet jitter	The VTD receiver has to offer a buffer for compensating the specified jitter. This actually means that a VTD has to offer bigger buffers to achieve a proper receiving and decoding of video frames with larger jitter. This delay adds up in the VTD receiver buffer, which shall be large enough to compensate for variation in the inter -arrival times (jitter).	BVMS dynamically compensates for network jitter in the decoder.	X
12.1	Network security requirements	The video transmission device shall have in the higher security grade 4 the ability to provide authentication, integrity checking and encryption on all network interfaces.		X
12.1	Network security requirements	All data communication outside secured technical room areas shall be encrypted in the security grade 4. AES with 128 bit key for symmetric and RSA with 1024 bit key shall be provided. Native encryption shall not be accepted. The VTDs shall not store any form of passwords in clear text. All such passwords either in configuration files or a database shall be encrypted. A VTD according to this standard shall support transport level security for the security grade 4.	From BVMS 10.0 onwards both live and recorded communication between cameras and central devices can be encrypted.	X
12.2	Transport level security requirements for SG4 transmission	Transport level security provides a protection of all video data between a VTD client and a server. Transport Layer Security (TLS) shall be provided by a VTD for encrypted transport. The TLS protocol offers authenticated transport sessions between 2 VTDs and takes care of confidentiality and integrity of the transported data.		X
12.2	Transport level security requirements for SG4 transmission	A VTD compliant to this standard shall support in security grade 4 TLS 1.0 according to the IETF standard RFC 2246 and TLS 1.1 according to RFC 4346. Optionally the VTD may support TLS 1.2 according to RFC 5246.		X

Section	Name	Requirements	Comments	Evaluation
12.2	Transport level security requirements for SG4 transmission	The VTD shall offer protection for the transport of all data and information concerning streaming, stream control and eventing.	From BVMS 10.0 onwards both live and recorded communication between cameras and central devices can be encrypted.	**X**
12.2	Transport level security requirements for SG4 transmission	The VTD client and server shall support the cipher suites TLS_RSA_WITH_AES_128_CBC_SHA and TLS_RSA_WITH_NULL_SHA from RFC 2246 and RFC 3268.		**X**

5.2 Grading

Section 4.2.3, table 1: time service accuracy for video transport stream

Class	Comments	T1	T2	T3	T4
Time Service Accuracy for Transport Stream	time accuracy depends on the stable root time source. BVMS depends on operating system mechanisms described here: Support boundary for high-accuracy time. For high accuracy time services it is recommended to deploy an separate NTP time server.	**80 ms**	**40 ms**	**5 ms**	**1 ms**

Section 4.3.2, table 2: Interconnections - timing requirements

Video transmission devices shall have a maximum	Comments	Class			
		I1	I2	I3	I4
Initial connection time for every new video stream request of	depending on workstation and network performance.	**2 000 ms**	**1 000 ms**	**500 ms**	**250 ms**

Section 4.3.3, table 3: video transmission network requirements

Video transmission devices in a shared network shall offer means to configure:	**Comments**	**Class**			
		C1	**C2**	**C3**	**C4**
the maximum data rate of video streams for every video channel	This is configured in the camera, and can be managed by BVMS.			**X**	**X**
the maximum data rate for all available video streams of a single device	This is configured in the camera, and can be managed by BVMS.			**X**	**X**
the maximum data rate or number of video streams to all client devices in the network	This should be handled in the network. Stream configuration can be managed in BVMS, the maximum expected bandwidth can be calculated.			**X**	**X**

Section 4.3.3, table 4: video transmission network requirements

Video transmission devices in a shared network shall offer means to:	**Comments**	**Class**			
		P1	**P2**	**P3**	**P4**
Prioritize certain streams over others, e.g. streams for recording or alarms over live image streams	This should be handled in the network (by means of Quality of Service)			**X**	**X**
Prioritize certain users over others, e.g. for PTZ control	BVMS has PTZ priority based on usergroups			**X**	**X**

Section 4.4.4, table 5: performance requirements video streaming and stream display

Class	**Comments**	**S1**	**S2**	**S3**	**S4**
Maximum Loss	Depends on network performance.	**240 ppm**	**120 ppm**	**60 ppm**	**30 ppm**

Class	Comments	S1	S2	S3	S4
Maximum one-way latency live stream (incl. encoding, networking, decoding, display)	Depends on network and workstation performance. A low-latency network might be required. It might be required to increase the bandwidth generated by the camera to reduce the encoding time and therefore reduce the end-to-end latency.	**600 ms**	**400 ms**	**200 ms**	**100 ms**
Max Trick Play (Pause, Single Step,,..) Reaction Time	Depends on available system resources.	**400 ms**	**200 ms**	**200 ms**	**100 ms**
Round-trip latency incl. visualisation & control e.g. PTZ	Depends on network and workstation performance. A low-latency network might be required. It might be required to increase the bandwidth generated by the camera to reduce the encoding time and therefore reduce the end-to-end latency.	**700 ms**	**500 ms**	**300 ms**	**200 ms**
Round-trip latency incl. visualisation & control e.g. PTZ, when moving objects need to be monitored and tracked	Depends on network and workstation performance. A low-latency network might be required. It might be required to increase the bandwidth generated by the camera to reduce the encoding time and therefore reduce the end-to-end latency.	**650 ms**	**450 ms**	**250 ms**	**150 ms**

Section 4.4.5, table 6: video stream network packet jitter.

Class	Comments	M0 ms	M1 ms	M2 ms	M3 ms	M4 ms
Maximum peak-to-peak packet jitter	Depends on available system resources.	-	**160**	**80**	**40**	**20**

Section 4.4.6, table 7: monitoring of interconnections.

The system shall offer	Comments	Security Grade			
		1	2	3	4
Maximum permitted duration of device unavailability	BVMS will typically notify within 1seconds that a device is unavailable. Issue needs to be solved by manual intervention.			**180s**	**30 s**
Maximum detection time for live signal loss	BVMS will typically notify within 1seconds that a device is unavailable. Issue needs to be solved by manual intervention.		**8s**	**4s**	**2s**
The requirement above is intended to establish if communication is possible by monitoring the communication video to ascertain if it is available to convey a signal or message. Monitoring may take the form of listening for jamming when a video transmission device communicates via shares interconnections with other devices or other applications.					

- ## 5.3 Transport level Security Requirements for Transmission

The system shall offer	Comments	Security Grade			
		1	2	3	4
TLS 1.0 and TLS 1.1 security	From BVMS 7.0 onwards for unicast streaming. From BVMS 10.0 onwards for multicast configurations.	Op	Op	Op	**M**
TLS 1.2 security	From BVMS 7.0 onwards for unicast streaming. From BVMS 10.0 onwards for multicast configurations.	Op	Op	Op	**Op**
cipher suites TLS_RSA_WITH_AES_128_CBC_ SHA and TLS_RSA_WITH_NULL_SHA		Op	Op	Op	**M**

The system shall offer	Comments	Security Grade			
		1	2	3	4
Transport level security provides a protection of all video data between a VTD client and a server. Transport Layer Security (TLS) shall be provided by a VTD for encrypted transport. The TLS protocol offers authenticated transport sessions between 2 VTDs and takes care of confidentiality and integrity of the transported data. A VTD compliant to this standard shall support in security grade 4 TLS 1.0 according to the IETF standard RFC 2246 and TLS 1.1 according to RFC 4346. Optionally the VTD may support TLS 1.2 according to RFC 5246. The VTD shall offer protection for the transport of all data and information concerning streaming, stream control and eventing. The VTD client and server shall support the cipher suites TLS_RSA_WITH_AES_128_CBC_ SHA and TLS_RSA_WITH_NULL_SHA from RFC 2246 and RFC 3268.					