



DPC: 24 / 30485530 DC

BSI Group Headquarters

389 Chiswick High Road London W4 4AL

Tel: +44 (0)20 8996 9000

Fax: +44 (0)20 8996 7400

www.bsigroup.com

Date: 09 January 2024

Origin: International

Latest date for receipt of comments: 7 February 2024

Project No. 2024/00047

Responsible committee: GW/1/10 Video Surveillance Systems (VSS), commonly known as CCTV

Interested committees:

Title: BS EN IEC 62676-4 Video surveillance systems for use in security applications

Part 4: Application guidelines

Please notify the secretary if you are aware of any keywords that might assist in classifying or identifying the standard or if the content of this standard

- i) has any issues related to 3rd party IPR, patent or copyright
- ii) affects other national standard(s)
- iii) requires additional national guidance or information

**WARNING: THIS IS A DRAFT AND MUST NOT BE REGARDED OR USED AS A BRITISH STANDARD.
THIS DRAFT IS NOT CURRENT BEYOND 7 February 2024**

This draft is issued to allow comments from interested parties; all comments will be given consideration prior to publication. No acknowledgement will normally be sent. **See overleaf for information on the submission of comments.**

No copying is allowed, in any form, without prior written permission from BSI except as permitted under the Copyright, Designs and Patent Act 1988 or for circulation within a nominating organization for briefing purposes. Electronic circulation is limited to dissemination by e-mail within such an organization by committee members.

Further copies of this draft may be purchased from BSI Shop <http://shop.bsigroup.com> or from BSI Customer Services, Tel: +44(0) 20 8996 9001 or email cservices@bsigroup.com. British, International and foreign standards are also available from BSI Customer Services.

Information on the co-operating organizations represented on the committees referenced above may be obtained from <http://standardsdevelopment.bsigroup.com>

Responsible Committee Secretary: **Miss Beverley Webb (BSI)**Direct tel: **0208 996 7061**E-mail: beverley.webb@bsigroup.com

Introduction

This draft standard is based on national and international discussions. Your comments on this draft are invited and will assist in the preparation of the consequent standard.

For international standards, comments will be reviewed by the relevant UK national committee before sending the consensus UK vote and comments to the international committee, which will then decide appropriate action. If the international standard is approved, it is usual for the text to be published as a British Standard.

For national standards, comments will be reviewed by the relevant UK national committee and the resulting standards published as a British Standard.

UK Vote

Please indicate whether you consider the UK should submit a negative (with supporting technical reasons) or positive vote on this draft. Please indicate if you are aware of any reason why this draft standard should not be published as a British Standard.

Submission of Comments

- **Annotated drafts are not acceptable and will be rejected.**
- All comments should be submitted online at <https://standardsdevelopment.bsigroup.com/>. You will need to register in order to comment.

Template for comments and secretariat observations

Date: xx/xx/20xx	Document: ISO/DIS xxxx
------------------	------------------------

1	2	(3)	4	5	(6)	7
MB	Clause No./ Subclause No./Annex (e.g. 3.1)	Paragraph/Figure/ Table/Note	Type of comment	Commend (justification for change) by the MB	Proposed change by the MB	Secretariat observations on each comment submitted
	3.1	Definition 1	ed	Definition is ambiguous and needs clarifying.	Amend to read '...so that the mains connector to which no connection...'	
	6.4	Paragraph 2	te	The use of the UV photometer as an alternative cannot be supported as serious problems have been encountered in its use in the UK.	Delete reference to UV photometer.	

PROJECT NUMBER: IEC 62676-4 ED2	
DATE OF CIRCULATION: 2023-12-15	CLOSING DATE FOR COMMENTS: 2024-03-08
SUPERSEDES DOCUMENTS: 79/693/RR	

IEC TC 79 : ALARM AND ELECTRONIC SECURITY SYSTEMS	
SECRETARIAT: France	SECRETARY: Mr Jean-François LIGNEREUX
OF INTEREST TO THE FOLLOWING COMMITTEES:	PROPOSED HORIZONTAL STANDARD: ☐ Other TC/SCs are requested to indicate their interest, if any, in this CD to the secretary.
FUNCTIONS CONCERNED: ☐ EMC ☐ ENVIRONMENT ☐ QUALITY ASSURANCE ☐ SAFETY	

This document is still under study and subject to change. It should not be used for reference purposes.

Recipients of this document are invited to submit, with their comments, notification of any relevant patent rights of which they are aware and to provide supporting documentation.

Recipients of this document are invited to submit, with their comments, notification of any local regulations or technical reasons that may exist and should be considered should this proposal proceed, recognizing that failure to address such requirements could result in the need for new or existing "In Some Countries" clauses. (SEE [AC/22/2007](#) OR [NEW GUIDANCE DOC](#)).

TITLE:

Video surveillance systems for use in security applications – Part 4: Application guidelines

NOTE FROM TC/SC OFFICERS:

CONTENTS

1	Scope	7
2	Normative references	7
3	Terms, definitions and abbreviations	8
3.1	Terms and definitions.....	8
3.2	Abbreviations.....	16
4	Planning considerations.....	17
4.1	General considerations	17
4.2	Security concept	17
4.2.1	General	17
4.2.2	Selection of security grades.....	19
4.3	Developing the operational requirements	20
4.4	Site survey.....	20
4.5	Security of the VSCC room	20
4.6	System design including site plan	21
4.7	Developing the test plan	21
4.8	Installation, commission and hand over.....	21
4.9	Documenting the system.....	22
5	Operational requirements specifications	22
5.1	General.....	22
5.2	Purpose of the operational requirements.....	22
5.3	Content of the operational requirements	22
5.3.1	General	22
5.3.2	Basic objective/functionalities	22
5.3.3	Definition of surveillance limitations	22
5.3.4	Definition of the site(s) under surveillance	23
5.3.5	Definition of activity to be captured	23
5.3.6	System/picture performance	23
5.3.7	Period of operation	23
5.3.8	Conditions at the location	23
5.3.9	Resilience.....	23
5.3.10	Monitoring and image storage.....	23
5.3.11	Exporting images.....	24
5.3.12	Routine actions.....	24
5.3.13	Operational response	24
5.3.14	Operator workload	24
5.3.15	Training	24
5.3.16	Expansions.....	24
5.3.17	List of any other special factors not covered by the above	25
5.4	System operational criteria	25
5.4.1	General	25
5.4.2	Automation	25
5.4.3	Alarm response	25
5.4.4	System response times.....	26
6	Technical considerations (equipment selection and performance).....	27
6.1	General.....	27

6.2	Camera equipment.....	27
6.3	Camera and lens selection criteria	27
6.4	Camera selection	27
6.4.1	General	27
6.4.2	PTZ	28
6.5	Lens and housing selection.....	28
6.6	Site coverage/numbers of cameras	29
6.7	Object sizes and Pixel Density	29
6.7.1	General	29
6.7.2	Object size definitions and Required Pixel Density in IP VSS.....	30
6.8	Field of view – Other considerations	33
6.9	Illumination	33
6.10	IP Video equipment.....	35
6.11	Tamper protection/detection.....	35
6.11.1	Camera tamper protection/detection	35
6.11.2	System tamper protection/detection	36
6.12	System integration	36
7	Video signal presentation	36
7.1	Display types	36
7.2	Resolution	38
8	Transmission	39
8.1	Principles.....	39
8.1.1	General	39
8.1.2	Selection of IP video performance classes.....	39
8.1.3	Interoperability.....	40
8.2	Wired transmission links	41
8.3	Wireless transmission links	41
8.4	Key considerations for IP based transmission systems	42
9	Video performance characteristics	43
9.1	Image compression.....	43
9.2	Frame rate	44
9.3	Resolution	44
10	Storage requirements	44
11	Image storage and export.....	45
11.1	Format of the compressed video data	45
11.2	Encryption	46
11.3	Basic metadata (time, date, camera identifier)	46
11.4	Multiplexing format.....	46
11.5	Image enhancements.....	46
11.6	Image export.....	47
11.7	Replay of exported images.....	47
12	VSCC control room configuration.....	48
12.1	Control rooms or Secure Viewing Area.....	48
12.2	Number, size and positioning of VSS video displays	48
12.3	Displays and screens mounted on or off the workstation	48
12.4	Recommended display sizes	49
12.5	Number of camera images per operator	49

12.6	Number of work stations	49
12.7	Equipment siting	50
12.8	Backup power supply provision	50
12.9	Operating temperature	50
12.10	Lightning and surge protection	50
13	Defining the test plan	51
13.1	Purpose of the test plan	51
13.2	User acceptance testing/inspection	51
13.3	Technical acceptance testing	51
13.3.1	Imaging chain consistency	51
13.3.2	Image quality	51
14	Documentational considerations (Pre-installation)	53
14.1	General	53
14.2	Risk assessment	54
14.3	Operational requirements	54
14.4	Design specification	54
14.5	Site plan	54
14.6	Test plan	54
15	System installation and commissioning	54
15.1	Factory acceptance testing	54
15.2	Installation process	55
15.3	User acceptance testing, commissioning and handover	55
15.4	Declaration of conformance to standards	56
16	Final documentation	56
16.1	General	56
16.2	Complete system drawings	56
16.3	System commission (with camera specific audits)	56
16.4	Interface descriptions	57
16.5	Operating logbook VSS	57
16.6	Compliance with legislation (for information)	57
17	Operation of VSS	57
17.1	General	57
17.2	Behaviour in the event of malfunctions	58
17.3	At-site visual check	59
17.4	Deviation of requirements for at-site visual checks and maintenance	60
17.5	Maintenance	60
17.6	Inspection (part of preventive maintenance)	60
17.7	Service Checks (part of preventive maintenance)	62
17.8	Repair (corrective maintenance)	62
17.9	Improvement	62
17.10	Deviations from requirements during at-site visual checks and maintenance	62
Annex A (informative)	Video standard formats	63
A.1	Current video standard format	63
A.2	Pixel densities for recognition of other objects of interest	63
Annex B (normative)	Test protocol for VSS target	64
B.1	Scope of the test	64
B.2	Test prerequisites	64

B.3	Preconditions	64
B.4	Face selection	64
B.5	Live view methodology (faces)	65
B.6	Live view methodology (VRN)	65
B.7	Recorded view methodology (faces).....	65
B.8	Recorded view methodology (VRN).....	66
B.9	Motion.....	66
B.10	Faces: scoring criteria.....	66
B.11	VRN: scoring criteria.....	67
B.12	Heads control sheet (for example only)	69
B.13	VRN control sheet (for example only).....	70
Annex C (normative) Test method of image quality Guidance for the use of the video test target		71
Annex D (informative) Guide to specifying VSS parameters and security gradings		77
D.1	VSS parameters.....	77
D.2	Suggested building blocks	77
D.3	Security gradings	78
D.4	Security grading by system view:	78
D.5	Security grading by size view:	79
D.6	Security grading by application view	79
D.7	Number of frames depending on the object speed in a scene width.....	81
Annex E (normative) Detection response testing and acceptability criteria		83
E.1	General.....	83
E.2	False and nuisance alarms	83
E.3	Setting the response time	84
E.4	PTZ response time test procedure	84
E.5	Observer cueing and prompting	84
E.6	Detection test locations.....	85
E.7	Target camouflage	85
E.8	Tests with moving targets	85
E.9	Test conditions	85
E.10	Testing a 'live' system.....	86
E.11	Detection test results tables	86
Bibliography.....		87
Figure 1 – structure of a security concept		18
Figure 2 – HD and UHD screen percentages occupied by various categories.....		32
Figure 3 – Pixel Density formula		33
Figure 4 – Operation of a VSS		58
Figure B.1 – Heads control sheet.....		69
Figure B.2 – VRN control sheet example.....		70
Figure C.1 – Test charts		72
Figure C.2 – Key to Figure C.1.....		75
Figure C.3 – Avoiding optical distortion.....		76
Table 1 – Measures depending on Security Grades		21

Table 2 – Example System feedback – PTZ Control Responding time, performance and operator	26
Table 3 – Typical Lux level	34
Table 4 – Examples of display technologies	37
Table 5 – Example Resolutions	38
Table 6 – Wireless transmission options	42
Table 7 – Inspection cycles versus security grading	58
Table A.1 – Recommendations for recognition of some “non-human” objects	63
Table B.1 – Example auditor log sheet	67
Table B.2 – Example control room observer log sheet	67
Table B.3 – Example camera audit sheet	67
Table B.4 – Blank auditor log sheet	68
Table B.5 – Blank control room observer log sheet	68
Table B.6 – Blank camera audit sheet	68
Table C.1 – Test targets	71
Table D.1 – Suggested VSS building blocks	77
Table D.2 – Security grading by size view	79
Table D.3 – Security grading by application	80
Table D.4 – Security grading by critical infrastructure	81
Table D.5 – Number of frames depending of object speed - Low Pixel Density Objects	82
Table D.6 – Number of frames depending of object speed - High Pixel Density Objects	82
Table E.1 – Detection test results	86

VIDEO SURVEILLANCE SYSTEMS FOR USE IN SECURITY APPLICATIONS –

Part 4: Application guidelines

1 Scope

This part of IEC 62676 gives recommendations and requirements for the design, planning installation, commissioning, maintaining and testing of Video Surveillance Systems – VSS comprising of image capture device(s), interconnection(s) and image handling device(s), for use in security applications.

The objectives of this part of IEC 62676 are to:

- a) provide a framework to assist all interested parties in establishing their requirements,
- b) assist specifiers and users in determining the appropriate equipment required for a given application,
- c) provide means of evaluating objectively the performance of the VSS.

2 Normative references

The following documents, in whole or in part, are normatively referenced in this document and are indispensable for its application. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

IEC 31010, *Risk management - Risk assessment techniques*

IEC 62305 (series), *Protection against lightning*

IEC 62305-3, *Protection against lightning – Part 3: Physical damage to structures and life hazard*

IEC 62305-4, *Protection against lightning – Part 4: Electrical and electronic systems within structures*

IEC 62676-1-1: *Video surveillance systems for use in security applications – Part 1-1: System Requirements*

IEC 62676-1-2: *Video surveillance systems for use in security applications – Part 1-2: General Video Transmission Requirements*

IEC 62676-2-1: *Alarm systems – Video surveillance systems for use in security applications – Part 2-1: Video Transmission Protocols – General Requirements*

IEC 62676-2-2: *Alarm systems – Video surveillance systems for use in security applications – Part 2-2: Video Transmission Protocols – IP interoperability implementation based on HTTP and REST services*

IEC 62676-2-3: *Alarm systems – Video surveillance systems for use in security applications – Part 2-3: Video Transmission Protocols – IP interoperability implementation based on web Services*

IEC 62676-3: *Video surveillance systems for use in security applications– Part 3: Analog and digital video interfaces*

IEC 62676-5 - Data Specifications and Image Quality Performance for Camera devices

ISO 31000, *Risk management - Guidelines*

ISO/IEC 11801 (series), *Information technology - Generic cabling for customer premises*

ISO/IEC 13818-1, *Information technology — Generic coding of moving pictures and associated audio information — Part 1: Systems*

ISO/IEC 14496-2, *Information technology — Coding of audio-visual objects — Part 2: Visual*

ISO/IEC 14496-10, *Information technology — Coding of audio-visual objects — Part 10: Advanced video coding*

ISO/IEC 15444-1, *Information technology — JPEG 2000 image coding system — Part 1: Core coding system*

ISO/IEC 19794-5, *Information technology — Biometric data interchange formats — Part 5: Face image data*

ITU-T Rec. T.81 / ISO/IEC 10918-1, *Information technology — Digital compression and coding of continuous-tone still images: Requirements and guidelines — Part 1: Requirements and guidelines*

ITU-T Rec. H.263, *Video coding for low bit rate communication*

ITU-T Rec. H.264, *Advanced video coding for generic audiovisual services*

ITU-T Rec. H.265, *High efficiency video coding*

ITU-R BT601, Standard to define how digital interlaced video signals to be coded (also formerly known as CCIR 601)

3 Terms, definitions and abbreviations

3.1 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

3.1.1

4K (UHD)

The standard for Ultra High-Definition television (UHDTV) defined by SMPTE2036 to be with 3.840 x 2.160 pixels at 25 or 30 fps.

3.1.2

8K (UHD)

The standard for Ultra High-Definition television (UHDTV) defined by SMPTE2036 to be with 7.680 x 4.320 pixels at 25 or 30 fps.

3.1.3**camera housing**

enclosure to provide physical and/or environmental protection of the camera, lens and ancillary equipment

3.1.4**camera sensitivity**

Image capturing device capability to produce an image in certain light conditions

3.1.5**Constant bit rate**

Where the bit rate of a camera stream is kept constant regardless of the image quality or movement in the scene

3.1.6**VSS surveillance installation**

installation consisting of the hardware and software components of a VSS, fully installed and operational for monitoring a defined security zone

3.1.7**VSS camera**

unit containing an imaging device producing a video signal from an optical image

3.1.8**VSS camera equipment**

unit containing a CCTV camera plus appropriate lens and necessary ancillary equipment

3.1.9**VSS control unit**

equipment for controlling and monitoring the required operational functions of the VSS

3.1.10**VSS**

Video Surveillance System; system consisting of camera equipment, monitoring and associated equipment for transmission and controlling purposes, which may be necessary for the surveillance of a protected area, previously referred to as CCTV

3.1.11**outline**

Minimum requirement of a VSS camera to outline a target, e.g. objects and their movements with a display of > 40 pixel/metre

3.1.12**electronic iris**

automatic electronic shutter which changes the camera sensitivity in relation to the varying light conditions in order to maintain the video output signal within defined limits

3.1.13**electronic shutter**

arrangement in the camera changing its sensitivity by electronically controlling its exposure time

3.1.14**event recording**

event controlled recording or storing of image signals for a pre-determined time

NOTE: refers to video recording not to system log of events

3.1.15**external synchronisation**

method of feeding reference timing signals to all connected devices to ensure that their video output signals are synchronous

3.1.16**focal length (f)**

measurement of the converging power of a lens, normally expressed in mm, which can be used to determine the angle of view for a given sensor size

3.1.17**geo data**

digital information assigning a certain spatial location to the earth's surface

3.1.18**High Definition (HD)**

A contemporary television standard with 1920 x 1080 pixels, interlaced (1080i) or progressive (1080p), as defined by SMPTE274, and with 1280 x 720 pixels, progressive (720p), as defined by SMPTE296

3.1.19**imaging device**

device that converts an optical image into an electrical signal

3.1.20**imaging device illumination**

level of illumination at the photosensitive surface of the imaging device

3.1.21**iris**

variable aperture mechanism which regulates the amount of light passing through the lens onto the imaging device of the CCTV camera

3.1.22**lens**

optical device for projecting an image of a desired scene onto the photo sensitive surface of the imaging device

3.1.23**overview**

Minimum requirement of a VSS camera to overview a target, e.g. objects and their movements with a display of > 20 pixel/metre

3.1.24**NTSC**

National Television Systems Committee, a US standardisation for analogue television

3.1.25**NTSC resolution**

A US standard resolution for analogue television produced by a 525 interlaced scanning system at 29.97 TV frames per second. When digitised, using the ITU-R BT601 recommendation, the NTSC analogue video signal is converted to 720 x 480 pixels at 30 TV frames per second

3.1.26**video signal presentation device**

device for converting video signals into pictures on a display screen

3.1.27**discern**

Minimum requirement of a VSS camera to discern a target, e.g. objects and their movements with a display of > 80 pixel/metre

3.1.28**ONVIF**

ONVIF is an open industry forum that provides and promotes standardized interfaces for effective interoperability of IP-based physical security products

3.1.29**Operational Requirements (OR)**

A formal written statement of need, justifications and purpose of the proposed VSS

3.1.30**pan and tilt unit**

motorised unit permitting the horizontal and vertical positioning of the camera equipment

3.1.31**PAL**

Phase Alternating Line, a European based standardisation for analogue television

3.1.32**PAL resolution**

A European standard resolution for analogue television produced by a 625 interlaced scanning system at 25 TV frames per second. When digitised, using the ITU-R BT601 recommendation, the PAL analogue video signal is represented with 720 x 576 pixels at 25 TV frames per second

3.1.33**pan, tilt, zoom (PTZ)**

function of a camera control permitting the horizontal, vertical positioning of the camera together with the variation of the focal length of the lens

3.1.34**picture storage**

storing of still or video images

3.1.35**pixel density**

a parameter that refers to the number of pixels clearly visible (in focus), per metre width, at the observed object distance

3.1.36**scene illumination**

level of illumination on the area to be kept under surveillance, measured in lux.

3.1.37**site plan**

a map or pictorial representation of the protected area showing the intended views of the CCTV cameras and their locations.

3.1.38**system design proposal (SDP)**

a design proposal that shows the elements of a video surveillance system, equipment installation location, physical interconnection and networking, suggested visual coverage, storage calculation and control room layout design.

- 216 **3.1.39**
217 **service level agreement (SLA)**
218 An agreement between the end user and installer covering the operation and maintenance of
219 the installation
- 220 **3.1.40**
221 **Variable bit rate (VBR)**
222 Where the bit rate for the camera stream is constantly changing during the encoding process,
223 due to changes in the scene
- 224 **3.1.41**
225 **video signal**
226 electronic representation of the motion video captured on an imaging sensor
- 227 **3.1.42**
228 **video signal amplitude**
229 magnitude of the video signal expressed in Volts
- 230 **3.1.43**
231 **zoom lens**
232 lens with variable focal length and therefore variable angle of view
- 233 **3.1.44**
234 **perceive**
235 Minimum requirement of a VSS camera to perceive a target, e.g. objects and their movements
236 with a display of > 125 pixel/metre
- 237 **3.1.45**
238 **characterise**
239 Minimum requirement of a VSS camera to characterise a target, e.g. persons (type of person,
240 gait and actions can be characterised) and vehicles (vehicle brands can be characterised) with
241 a display of > 250 pixel/metre
- 242 **3.1.46**
243 **validate**
244 Minimum requirement of a VSS camera to validate a target, e.g. recognition of known persons,
245 actions can be reconstructed, vehicle registration numbers can be partially reconstructed with
246 a display of > 500 pixel/metre
- 247 **3.1.47**
248 **scrutinise**
249 Minimum requirement of a VSS camera to scrutinise a target, e.g. persons identifiable with a
250 probability bordering on certainty, vehicle recognition according to model/year of construction,
251 undoubted vehicle number plate recognition with a display of > 1500 pixel/metre
- 252 **3.1.48**
253 **Pixel density**
254 Parameter which refers to the number of pixels at the object location (focused area), per unit
255 length (pix/m). the parameter is universal as it includes the variables of the sensor size, pixel
256 count, lens focal length and the distance to the object.
- 257 **3.1.49**
258 **Reaction time**
259 The reaction time is the time span between the recognition of a certain reaction cause and the
260 start of the (defensive) action directed towards it

3.1.50**VSCC**

Device for receiving, processing, controlling, displaying, storing, export and forwarding all video signals and information.

3.1.51**VSCC room**

Room or enclosure containing the VSCC within a room in a building. This covers a small office to a full-scale control room environment

3.1.52**Security concept**

Entirety of identified risks and hazards in connection with the specified organisational, personnel, technical and structural measures to secure a installation and/or to avert hazards

3.1.53**Risk assessment**

Determination and evaluation of the identified risks for the object or the relevant assets, such as theft of material assets and know-how, personal protection, vandalism, sabotage, interruption of operations, etc.

3.1.54**Security Grade**

Grade of security on the basis of the risk assessment carried out

3.1.55**Operator**

The operator is the person responsible for the operation of the VSS and for the effectiveness of the VSS as well as for scheduled, fault-free functioning during the lifecycle of the VSS. Furthermore, the operator is responsible for regular at-site visual check and maintenance of the VSS. The term operator is used because the owner of the building/property does not have to be the user of the VSS at the same time

3.1.56**Competent system engineer VSS**

Person who, on the basis of professional technical training, knowledge and experience as well as knowledge of the relevant standards, regulations and directives, is able to assess the work to be carried out and recognise possible hazards.

A competent system engineer VSS can be employed by either an installation company/system integrator company, planning company or at owner or at user of the VSS.

Note 1 to the term: For the field of video surveillance systems, training from the spectrum of electrical engineering in the field of communications, information, microprocessor, measurement and control or general electrical engineering is required, and experience in the respective other fields as well as system knowledge of video security technology must be demonstrated. Qualification of competence for VSS knowledge can be proven by training certificates of e.g., local security associations or vendors of VSS.

Note 2 to the term: Several years of activity in the relevant fields of work can also be used to assess the professional training.

Note 3 to the term: The activity requires the ability to independently plan and process comprehensive technical tasks in a complex, specialised, changing environment. Integrated technical knowledge and in-depth theoretical knowledge of the subject must be available. The scope and limits of the possible applications of a video surveillance system must be known. A very broad spectrum of specialised cognitive and practical skills is required. Work processes are to be planned in a comprehensive manner and assessed with comprehensive consideration of handling alternatives and interactions with neighbouring areas. The competence to guide others and to support them with well-founded learning guidance must be given. Interdisciplinary complex issues must be presented in a structured, target-oriented and addressee-related manner. Own and externally set learning and working goals must be reflected upon, evaluated, pursued in a self-directed manner and answered.

3.1.57**competent person VSS**

Person who has been instructed by a competent system engineer VSS about the assigned tasks within the scope of the on-site check and the possible dangers and consequences of improper behaviour

Note 1 to the term: This includes the necessary knowledge for the assessment of the object requirements, with regard to the type of danger and the required function of the VSS, the influence of the use as well as the limits of use and the instruction about the security concept of the video surveillance system, about existing requirements as well as legal requirements or requirements of the operator from safety aspects as personal and property protection measures or to avoid personal injury.

Note 2 to the term: The task requires competences for independent planning and processing of the requirements from the at-site visual check as well as in-depth general knowledge and specialist theoretical knowledge in order to be able to assess to what extent environmental or object changes can influence the effectiveness of a video surveillance system. The recognition of possible interactions from other requirements as well as the development of alternative actions is necessary. Detected deviations must be securely justified, responsibly communicated and, if necessary, retracted if no other problem solutions can be found.

3.1.58**Instructed person**

Person who has been instructed in the tasks required for the operation of a VSS by a competent system engineer VSS and is capable of independently operating the VSS.

Note 1 to the term: These tasks include the implementation or initiation of protective measures and other measures to avert danger in the event of shutdown or malfunction of plant components as well as the initiation of fault rectification or maintenance in the event of impairments.

Note 2 to the term: The tasks presuppose the competences to independently fulfil technical requirements in a still manageable field of activity, as well as extended general knowledge and extended expert knowledge with regard to the function of VSS and the organizational measures associated with their operation. Furthermore, it is necessary to always keep the level of knowledge about VSS up to date through independent and responsible learning.

3.1.59**At-site visual check**

Activity to determine and assess the feasibility of implementing the safety concept per camera location to be monitored as well as checks of visible disturbances and defects - in particular for influences occurring outside of VSS system parts - on the monitoring tasks of a VSS that are not evaluated operationally and whether there are deviations from the function of the VSS required in the safety concept. The at-site visual check is the responsibility of the operator, who may, however, hand over the inspection to a competent person VSS or to a competent system engineer VSS.

3.1.60**Maintenance company**

Company, who employs competent system engineer VSS that can carry out all maintenance measures, at-site visual checks as well as system extensions and modifications and that has a 24/7 on-call service, the necessary spare parts and the required equipment.

3.1.61**Maintenance**

Combination of all technical and administrative measures during the life cycle of a VSS that serves to maintain or restore it to a functional state so that it can fulfil the required function. Maintenance includes the preventive measures of inspection and service checks as well as the corrective measures of repair and improvement. Maintenance is usually carried out on site; certain maintenance measures can also take place as "remote maintenance" by means of remote access with the consent of the operator. Remote maintenance must be documented in the operating logbook VSS. Maintenance measures must be carried out by a competent system engineer VSS.

3.1.62**Preventive maintenance**

Maintenance to assess and reduce the probability of failure of a VSS. Preventive maintenance includes inspection and service checks of a VSS and serves as preventive measures before a failure is detected.

3.1.63**Corrective maintenance**

Maintenance carried out after failure detection to restore a VSS to a condition in which it can perform its required function. Corrective maintenance corresponds to repair and serves as a corrective measure after a failure has been detected.

3.1.64**Inspection (part of preventive maintenance)**

Testing for conformity of the relevant characteristics of a VSS by measurement, observation and testing. Checking of all system parts for technical functionality of the VSS according to general manufacturer-independent criteria. An inspection must be carried out by a competent system engineer VSS and must be documented in the operating logbook VSS.

3.1.65**Service checks (part of preventive maintenance)**

General care, adjustments, cleaning and replacement of system parts of a VSS according to the manufacturer's instructions, i.e. primarily implementation of manufacturer-specific measures and activities taking into account the special operating environment conditions. Service checks must be carried out by a competent system engineer VSS and must be documented in the operating logbook VSS.

3.1.66**Repair (corrective maintenance)**

Physical measure carried out to restore the function of a faulty VSS through fault location, fault diagnosis and repair. If it is determined during an inspection or service checks that the required function of the VSS or individual system parts is no longer ensured until the next inspection or that the required function cannot be fulfilled due to a malfunction, a repair must be carried out immediately and coordinated with the operator. Repairs must be carried out by a competent system engineer VSS and must be documented in the operating logbook VSS.

3.1.67**Improvement**

An improvement comprises additions or changes to a VSS that improve the reliability or functional safety of a VSS during operation without changing its original function. An improvement must be carried out by a competent system engineer VSS and must be documented in the operating logbook VSS. An improvement can be, for example, a firmware or software update.

3.1.68**Operating logbook VSS**

At the time of commissioning, the competent system engineer VSS must hand over an operating logbook VSS to the operator, in which all activities on the VSS during the entire lifecycle of the VSS must be continuously recorded. This includes, among other things, all briefings, the handover of the VSS, all operating events such as malfunctions, hazard alarms and false alarms as well as their causes, all maintenance carried out (preventive: inspections and service checks as well as corrective: repair) and all modifications and improvements to the VSS.

In the operating logbook VSS, the competent system engineer VSS must refer to the required at-site visual checks and maintenance as well as to the operator's obligation to keep the logbook. The operating logbook VSS must be kept by the operator or by an instructed person.

3.1.69**Resistance value**

Resistance class or measure given in an abstract unit for the resistance of a security product or also of a building element, such as window, door, a wall, ceiling or floor.

3.1.70**Resistance time**

Value, given in units of time, for which a security product or a building element, such as window, door, a wall, ceiling or floor, resists a defined attack, depending on the respective resistance value

3.2 Abbreviations

For the purposes of this document, the following abbreviations apply.

4K	Acronym for Ultra High Definition TV (UHDTV) with 3.840 x 2.160 pixel
8K	Acronym for Ultra High Definition TV (UHDTV) with 7.680 x 4.320 pixel
ASB	Anti-social behaviour
BNC	Bayonet Neill–Concelmann (connector)
CCIR	Consultative Committee on International Radio
CCTV	Closed circuit television, old term for VSS
DVR	Digital video recorder
CEM	Electro-magnetic compatibility
CRT	Cathode ray tube
FAT	Factory acceptance test
FPS	Frames per second
Gbps	Gigabits per second
H.26x	Covers both H.264 and H.265 advanced video coding format
HD	High definition
HDD	Hard disk drive
HPDO	High Pixel Density Object – reflects to HPDO test chart
NVR	Network video recorder
LCD	Liquid crystal display
LPDO	Low Pixel Density Object – reflects to LPDO test chart
IP	Internet protocol
IPD	Image presentation device
IR	Infrared
Mbps	Megabits per second
MPEG	Motion Picture Experts Group
OODPCVS	Acronym for overview/outline/discern/perceive/characterise/validate/scrutinise
ONVIF	Standard interface of IP-based physical security products
OR	Operational requirement
PTZ	Pan tilt zoom
SD	Standard Definition (576i for PAL; 480i for NTSC)
SDP	System Design Proposal
REST	Restful State Transfer (Webservice)

RTSP	Real time stream control protocol
SSD	Solid state drive
SXGA	Super eXtended Graphics Adapter
TCP/IP	Transmission Control Protocol / Internet Protocol
VRN	Vehicle registration number
UAT	User acceptance testing
UDP	User Datagram Protocol
UHD	Ultra High Definition
UPS	Uninterruptible power supply
UTC	Universal time coordinated
UV	Ultraviolet
VCA	Video content analysis
VMS	Video management system
VMD	Video motion detection
WORM	write once read many
VSCC	Video Surveillance Control Centre
VSS	Video Surveillance System

4 Planning considerations

4.1 General considerations

A VSS is the combination of image capture devices, lighting, interconnections, image handling devices, etc. selected and installed to meet the Operational Requirements (OR).

VSS shall only be planned, installed, extended, modified and maintained by a competent system engineer VSS.

The recommended procedure for implementing a VSS is detailed in the following clauses.

4.2 Security concept

4.2.1 General

The basis for planning of a VSS is a security concept, which must be documented in a suitable form and updated as part of the system documentation.

The operator is responsible for the security concept and defines the measures together with the responsible bodies and project participants, e.g. planners, authorities, insurers, competent system engineers VSS, etc. A prerequisite for the creation of a security concept is a threat analysis and definition of protection goals carried out by the operator or a commissioned body, e.g. specialist planners, experts, etc. This is necessary for the definition of the operating requirements. This is to be used for the determination of the operational requirements (OR).

The security concept must include the VSS as part of a three-pronged security strategy. The strategy consists of:

- structural-mechanical measures to achieve a sufficient resistance time value
- electronic measures, including the VSS and e.g. lightning protection

- organisational measures to support safe and, if necessary, false-alarm-free operation and to react appropriately to the situation in the event of certain occurrences, such as alarms and malfunctions, but also substitute measures in the event of shutdowns and malfunctions

The security concept must describe the interaction of the three strategic components in relation to the specific circumstances and measures.

The structure of a security concept should follow the sequence in Figure 1.

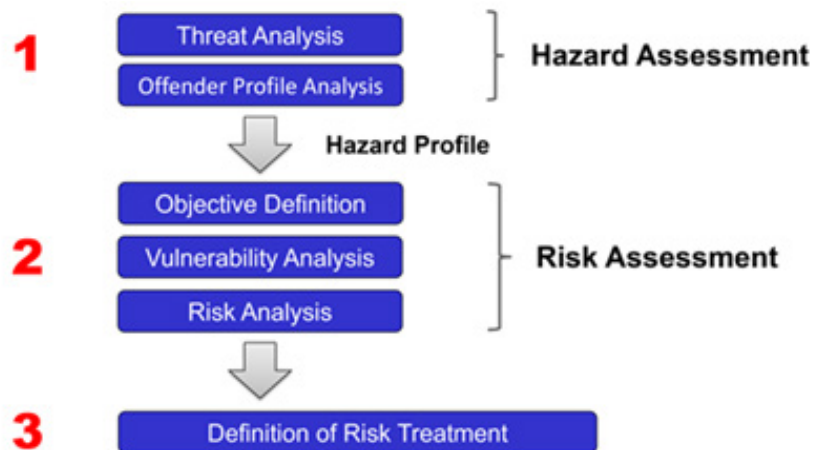


Figure 1 – structure of a security concept

Note: Further detailed information on the preparation of security concepts and risk management can be found in ISO 31000 (Risk Management Guidelines) and IEC 31010 (Risk Management – Risk assessment techniques)

Risk assessment

Prior to the VSS design and to support the understanding of its purpose, a threat analysis and a risk analysis (see Figure 1) should be carried out as part of the preparation of a security concept. The threats and risks to the object should be identified and assessed in terms of their likelihood and impact. These represent the risk to the object or organisation.

A risk assessment should be carried out and the VSS should be designed to mitigate the assessed risks. VSS designs should be carried out in accordance with this standard.

There is no single model design for a VSS. The design should be based on the individual site and object, the threats and content of those sites and the expected threats and damage.

Examples of issues to be considered are listed below:

a) Cost of loss:

- 1) What is the value, e.g. financially, intellectually, etc. of the assets at site?
- 2) What is the consequence of interruption of work/business at site?

b) Location:

- 1) What is the quality and extent of any existing physical security?
- 2) Is the site located in a high crime area?
- 3) Are there any adverse environmental conditions?
- 4) How long does it take to get intervention forces to the site?
- 5) Does the public have access to the site/location?

c) Staffing:

1) Is the site unoccupied for extended periods?

2) Are there security staff?

d) Theft, robbery and threat history:

1) Is there a history of theft, robbery or threats at site?

2) If so, what were the methods of attack of the previous threat?

Results of this assessment will be used to contribute to decisions regarding the type of VSS to be specified and then subsequently installed.

4.2.2 Selection of security grades

The results of the risk assessment (see 4.2.1) should be used to determine the requirements of the VSS and its components. Where appropriate a security grade should be assigned.

The security gradings may be defined by different methods as shown below:

1. Security grade definition applied to the entire VSS (same grade) or different gradings to sub-systems (system view)
2. Security grade definition applied to the size of VSS (size view)
3. Security grade definition applied to the application/vertical within the VSS is being used (application view)
4. Security grade definition applied to the functions within the VSS (function view)

The identified security grade requirements should be specified in the operational requirement (OR) or system design proposal (SDP) and agreed by the customer and system designer.

IEC 62676-1-1 defined the following functions within VSS

Depending on the level of risk, the security grade needs to be defined for the following VSS functions:

- a) common interconnections
- b) storage
- c) archiving and backup
- d) alarm related information
- e) system logs
- f) backup and restore of system data
- g) repetitive failure notification
- h) image handling device PSU monitoring
- i) image buffer holding time
- j) essential function device failure notification time
- k) monitoring of interconnections
- l) tamper detection
- m) authorisation code requirements
- n) time synchronisation
- o) data authentication
- p) export/copy authentication

514 q) data labelling

515 r) data (manipulation) protection

516 Individual functions of the VSS may be specified at different security grades: for example, a
517 system generally specified at grade 1 with grade 4 storage including fail-safe image storage.

518 Any additional functions which are required above the security level may be defined individually
519 in the OR or SDP

520 Further information for security grading examples refer to Annex D.

521 **4.3 Developing the operational requirements**

522 The OR document shall be produced. This is a formal written statement of need, justifications
523 and purpose of the proposed VSS. The installer should assess and determine whether
524 production of the OR is to be completed before or after the site survey. See 5.2 & 5.3 for more
525 details.

526 **4.4 Site survey**

527 Once a location has been chosen for a VSS installation a site survey should be undertaken. This
528 is to familiarise the system designer with the specifics of the intended site, such as access
529 constraints, siting of key components (cameras, controls, power supplies, etc.) and
530 environmental factors including illumination in day and night mode (see Clause 6 for more
531 details).

532 This should be completed by visiting the location to assess its suitability, and to note any issues
533 for the system design phase.

534 If the location where the VSS is to be installed has not yet been constructed then the site survey
535 may be carried out after a preliminary design has been created.

536 **4.5 Security of the VSCC room**

537 The VSCC must be protected by means of structural, mechanical, electronic, organisational
538 and, if necessary, personnel security measures, depending on the security concept, the risk
539 assessment and the resulting security grading.

540 The identified risks and requirements should be specified in the operational requirements (OR)
541 and discussed with the bodies involved. Accordingly, suitable security measures should be
542 selected to protect the VSCC from unauthorised access, sabotage, vandalism and manipulation.

543 The enclosure components of the VSCC room or the housing in which the central components
544 of the VSS are located must have sufficient structural or mechanical resistance in accordance
545 with the results of the risk assessment. In addition, breakthrough monitoring with suitable
546 sensors or detectors (e.g. area monitoring) may be required.

547 Depending on the security grading, the VSCC room or the enclosure should also have an
548 opening and closing contact monitoring system for the doors (access door, openings as side
549 panels of the enclosure, etc.) with logging.

550 At grade 4, the VSCC room should be equipped with an intrusion alarm system that ensures
551 monitoring of opening, closure and breakthrough as well as monitoring of the interior.

In this regard, suitable organisational security measures, such as alarm transmission and intervention by security staff, must be defined. In particular, the failure and sabotage protection of the transmission paths must be taken into account.

Furthermore, a mechanical, mechatronic or electronic access control system may be required for the VSC room. The individual measures depending on the security grades can be found in Table 1.

Table 1 – Measures depending on Security Grades

Measures	SG 1	SG 2	SG 3	SG 4
Structural, mechanical resistance	O	O	X	X
Constructional elements* with a high resistance value	O	O	X	-
Constructional elements* with a very high resistance value	O	O	O	X
electronic burglar alarm system	O	O	X	X
Opening and closure monitoring with logging	O	X	X	X
Breakthrough monitoring	O	O	O	X
External triggering, e.g. motion detectors (spatial monitoring)	O	O	X	X
Transmission device to a permanently manned AMC**	O	R	X	X
Access control system	O	R	X	X

*) Windows, Doors, Walls, Ceilings, Floors

**) Alarm Monitoring Centre

- = not permitted

X = required

O = optional

R = Recommendation

Remark:

The term "resistance or resistance value" refers to "breakthrough".

4.6 System design including site plan

Once the site survey and OR is completed the VSS can be designed, and a System Design Proposal and Specification needs to be prepared. The design shall take into account the various requirements and location factors identified in the previous stages. At this stage a site plan should be drawn up, including locations for the various key components such as cameras (including field of view), detectors (including range and coverage), control rooms, power supplies, interconnections, etc. See Clause 6 for more details.

4.7 Developing the test plan

Having designed the VSS, a test plan shall be produced to allow any installed system to be suitably proven. This test plan should include all the critical aspects of the VSS, such as image quality, system interconnectivity, coverage, camera view, etc. The purpose is to ensure that the system can be measured against its OR and proved to be fit for its intended purpose. See Clause 13 for more information and 6.10.2 for tamper protection testing.

4.8 Installation, commission and hand over

The risk assessment, OR and system design (including a site plan) should all be used to help facilitate the VSS installation.

Having completed the installation, commissioning tests as specified in the test plan should be completed according to the OR.

Once this has been successfully completed the system can be formally handed from the installer to the operator. See Clause 15 for more details.

4.9 Documenting the system

Documentation should be completed supporting the design, installing and commissioning phases of the VSS. These should be collated and held by the operator as the system references. The risk assessment, OR, testing plan, site survey, system design and site plan (see Clauses 14 and 16) should be included, along with the following documents:

- testing results, as built plans/drawings, data interface descriptions;
- training, manuals, support documentation, etc.;
- maintenance plan including routine inspection cleaning, etc. (see Clause 17 for more details).

5 Operational requirements specifications

5.1 General

The purpose of the VSS installation shall be summarized in a document called "Operational Requirements" (OR) or "System Design Proposal" (SDP).

5.2 Purpose of the operational requirements

The operational requirements clearly state what the customer expects the functions of the system to do. If there is an agreement between the system designer and the customer, the OR could be defined within the system design proposal and specification. If so, this should be clearly stated within the document. The development/design process encourages clear thinking about who will use the VSS, where and when it will be used and, in particular, the purpose of the VSS. It is produced by VSS owners, operators and anyone who intends to use information from the VSS. The later stages of development of the OR shall involve those with the necessary skills to convert statements into a technical specification and test procedures.

At appropriate stages checks shall be made to ensure that the proposed implementation will meet the OR. Without an OR and a matching test procedure there is no practical methodology to assess whether the system can meet its required purpose.

5.3 Content of the operational requirements

5.3.1 General

The Operational Requirements shall consist of the following parts:

Note: Depending on size of object or size of system or application, parts of this clause may be irrelevant.

5.3.2 Basic objective/functionalities

Following basic functions shall be included where applicable :

- Intended purpose(s) of the system (e.g. site monitoring, detection and/or monitoring and/or recording of attacks against individual and property, thefts, robberies or damage).
- Risk assessment, which informs the selection of the required security grade of the system according to IEC 62676-1-1.

5.3.3 Definition of surveillance limitations

Following limitations shall be included where applicable :

- Country-specific data protection laws (e.g. GDPR in Europe) must be complied with for the planning and operation of VSS. It is advisable to take the country-specific regulations into account already during the planning of the VSS

- Limitations imposed by legislation, city rules or similar orders.
- Limitations such as privacy areas required by the operator or by the proximity of neighbours.

5.3.4 Definition of the site(s) under surveillance

Buildings, internal, external or separate areas, small, medium or large private or public spaces, etc. which are covered by the VSS.

5.3.5 Definition of activity to be captured

Following activity definitions shall be covered:

- The intended targets of the system in each part of the site (e.g. unauthorized persons within an area bounded by a perimeter fence; vehicles entering the access driveway, etc.).
- The expected speed of the intended target.
- The intended observation category of the targets from the perspective of the operator (e.g. overview, outline, discern, perceive, characterise, validate, scrutinise of a person).
- Whether external detection is required.

5.3.6 System/picture performance

Following performance parameters shall be included where applicable :

- The key performance characteristics of the system and its displayed images (e.g. timescale for operator to view persons and track their movements throughout the scene).
- The degree of image detail required for the purpose which is to be observed in each of the live, recorded and exported views (i.e. it may be desirable or appropriate for a different resolution to be used in the live view than in the recorded view).
- Definition of any image analysis functionality, together with expected accuracy and whether this is to be achieved by the operator or automatically by the system.

5.3.7 Period of operation

Following operation parameters shall be included where applicable :

- Definition of the operating hours for the system (e.g. daily between 21:00 and 08:00 and all day on Sundays and public holidays).

5.3.8 Conditions at the location

Definition of environmental conditions, which will apply and/or vary during the monitoring period and are significant in terms of system design (e.g. illumination of the site, potential obstacles in camera view, maximum and minimum temperatures, on-board).

5.3.9 Resilience

Definition of the ability of the system to continue operating despite the existence of adverse circumstances (e.g. ability to continue operating during sudden or unexpected loss of power for a significant or defined length of time, absence of single interconnection paths, whether all or parts of the system have the same requirement).

5.3.10 Monitoring and image storage

Following monitoring and storage parameters shall be included where applicable :

- Definition of how, and by whom, the system shall be monitored and operated.
- Definition of what is to be recorded (e.g. all images for 10 min before and after an event; all camera views at all times).

- Definition of the retention period for recordings and circumstances in which this will change (e.g. all recorded images to be kept for, and erased after, 28 days except where they relate to a criminal event).
- Definition of additional (remote) sites where the images shall be available.
- Definition of procedures to be followed when extracting, storing and handling images and data from the system. Including those that may be stored off-site e.g, Cloud

5.3.11 Exporting images

Following export parameters shall be included where applicable :

- Definition of how images will be exported for short sequences (e.g. a 10 min clip to be exported to WORM media; individual image snapshots exported to USB/IP storage device).
- Definition of how images will be exported for long sequences (e.g. network download for full system archive).
- Definition of required compatibility of exported video footages (e.g. sequences should be re-playable without the need for any software/codec/hardware that is not considered part of a standard desktop operating system). In case exported video footage is playable on a standard player, it must be possible to identify, if the video footage is untampered.

5.3.12 Routine actions

Definition of actions that are required as a matter of normal routine (e.g. the monitoring service shall carry out routine video patrols at 2 h intervals throughout the monitoring period).

5.3.13 Operational response

Following response actions shall be included where applicable :

- Definition of the person responsible for the response (e.g. key holder, guarding service and/or police).
- Definition of the type of response needed for each potential event (e.g. when a trespasser is observed the local law enforcement agency is contacted).
- Definition of target times for each response (e.g. security personnel to attend scene within 3 min of event detection).

5.3.14 Operator workload

Following operator parameters shall be included where applicable :

- Definition of the number of display screens an operator is expected to monitor.
- Definition of the number of alarm events the operator is expected to manage.
- Definition of the number of live cameras the operator is expected to manage.

5.3.15 Training

Definition of required training for each role involved in the management and operation of the system.

5.3.16 Expansions

Following system expansions shall be included where applicable :

- Definition of any planned future extensions of the system, indicating any compatibility requirements.
- Definition of method used to connect with other systems.

5.3.17 List of any other special factors not covered by the above

If the operational requirement (OR) cannot be met with current technology or resources it will be noted in the system design document.

5.4 System operational criteria

5.4.1 General

The system's operational criteria involve the determination of:

- the operational procedures;
- the alarm response;
- the system response times.

5.4.2 Automation

The VSS shall be designed to enable the operator to analyse the content of the displayed images and take all necessary actions as defined by the OR.

Automatic processing can assist operators allowing them to concentrate on essential tasks.

Automation of the following functions shall be included where applicable :

- video image switching;
- pre-position of image capture devices;
- equipment monitoring, health check and recording process;
- video content analysis;
- lighting control;
- image storage.

Some of the above functions can be controlled from:

- alarm conditions,
- externally triggered events,
- time related events,
- operator manual activations.

5.4.3 Alarm response

The signalling indication of an alarm condition to the VSS shall have priority over other events.

It should be defined in the OR whether or not the operator shall be able to take manual control of the system, following an alarm condition, regardless of the degree of automation.

Automation of image selection shall consider the following requirements:

- specification for the selection of the significant images/sequences in each area where an alarm condition occurs;
- allocation of displays to view the significant images/sequences from the selected image capture devices; on-screen displays with image source identification or animated diagrams of the system can be useful;
- presentation of alarm images on designated displays;
- handling of simultaneous alarm conditions;