



**SLOVENSKI STANDARD**  
**oSIST prEN IEC 62676-4:2024**  
**01-december-2024**

---

**Video nadzorni sistemi za varnostne aplikacije - 4. del: Smernice za uporabo**

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

Videoüberwachungsanlagen für Sicherheitsanwendungen - Teil 4: Anwendungsregeln

Systèmes de vidéosurveillance destinés à être utilisés dans les applications de sécurité -  
Partie 4: Directives d'application

**Ta slovenski standard je istoveten z: prEN IEC 62676-4:2024**

---

[oSIST prEN IEC 62676-4:2024](https://standards.iteh.ai/catalog/standards/sist/8644647b-a836-4411-838b-6fd8dddcc705/osist-pren-iec-62676-4-2024)

<https://standards.iteh.ai/catalog/standards/sist/8644647b-a836-4411-838b-6fd8dddcc705/osist-pren-iec-62676-4-2024>

**ICS:**

13.320	Alarmni in opozorilni sistemi	Alarm and warning systems
33.160.40	Video sistemi	Video systems

**oSIST prEN IEC 62676-4:2024**

**en**





PROJECT NUMBER: <b>IEC 62676-4 ED2</b>	
DATE OF CIRCULATION: <b>2024-10-25</b>	CLOSING DATE FOR VOTING: <b>2025-01-17</b>
SUPERSEDES DOCUMENTS: <b>79/701/CD, 79/705A/CC</b>	

IEC TC 79 : ALARM AND ELECTRONIC SECURITY SYSTEMS	
SECRETARIAT: France	SECRETARY: Mr Jean-François LIGNEREUX
OF INTEREST TO THE FOLLOWING COMMITTEES:	HORIZONTAL FUNCTION(S):
ASPECTS CONCERNED: Information security and data privacy	
<input checked="" type="checkbox"/> SUBMITTED FOR CENELEC PARALLEL VOTING <b>Attention IEC-CENELEC parallel voting</b> The attention of IEC National Committees, members of CENELEC, is drawn to the fact that this Committee Draft for Vote (CDV) is submitted for parallel voting. The CENELEC members are invited to vote through the CENELEC online voting system.	<input type="checkbox"/> NOT SUBMITTED FOR CENELEC PARALLEL VOTING

<https://standards.iteh.ai/catalog/standards/sist/8644647b-a836-4411-838b-6fd8dddcc705/osist-pren-iec-62676-4-2024>

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 relevant "In Some Countries" clauses to be included should this proposal proceed. Recipients are reminded that the CDV stage is the final stage for submitting ISC clauses. (SEE [AC/22/2007](#) OR [NEW GUIDANCE DOC](#)).

TITLE:

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

PROPOSED STABILITY DATE: 2029

NOTE FROM TC/SC OFFICERS:

**Copyright © 2024 International Electrotechnical Commission, IEC.** All rights reserved. It is permitted to download this electronic file, to make a copy and to print out the content for the sole purpose of preparing National Committee positions. You may not copy or "mirror" the file or printed version of the document, or any part of it, for any other purpose without permission in writing from IEC.

# CONTENTS

1		
2		
3	FOREWORD.....	7
4	1 Scope.....	9
5	2 Normative references .....	9
6	3 Terms, definitions and abbreviations .....	10
7	3.1 Terms and definitions.....	10
8	3.2 Abbreviations .....	18
9	4 Planning considerations.....	19
10	4.1 General considerations .....	19
11	4.2 Security concept .....	20
12	4.2.1 General .....	20
13	4.2.2 Risk assessment .....	21
14	4.2.3 Selection of security grades.....	22
15	4.3 Developing the operational requirements .....	23
16	4.4 Site survey.....	23
17	4.5 Security of the VSCC room .....	23
18	4.6 System design including site plan .....	24
19	4.7 Developing the test plan .....	24
20	4.8 Installation, commissioning and hand over.....	24
21	4.9 Documenting the system.....	24
22	5 Operational requirements specifications .....	25
23	5.1 General.....	25
24	5.2 Purpose of the operational requirements .....	25
25	5.3 Content of the operational requirements .....	25
26	5.3.1 General .....	25
27	5.3.2 Basic objective/functionalities .....	25
28	5.3.3 Definition of surveillance limitations .....	25
29	5.3.4 Definition of the site(s) under surveillance .....	26
30	5.3.5 Definition of activity to be captured .....	26
31	5.3.6 System/picture performance .....	26
32	5.3.7 Period of operation .....	26
33	5.3.8 Conditions at the location .....	26
34	5.3.9 Resilience.....	26
35	5.3.10 Monitoring and image storage.....	26
36	5.3.11 Exporting images .....	27
37	5.3.12 Routine actions.....	27
38	5.3.13 Operational response .....	27
39	5.3.14 Operator workload .....	27
40	5.3.15 Training .....	27
41	5.3.16 Expansions.....	27
42	5.3.17 List of any other special factors not covered by the above .....	27
43	5.4 System operational criteria .....	28
44	5.4.1 General .....	28
45	5.4.2 Automation .....	28
46	5.4.3 Alarm response .....	28

47	5.4.4	System response times.....	28
48	6	Technical considerations (equipment selection and performance).....	29
49	6.1	General.....	29
50	6.2	Camera equipment.....	30
51	6.3	Camera and lens selection criteria .....	30
52	6.4	Camera selection .....	30
53	6.4.1	General .....	30
54	6.4.2	PTZ .....	31
55	6.5	Lens and housing selection .....	31
56	6.6	Site coverage/numbers of cameras .....	32
57	6.7	Object sizes and Pixel Density .....	32
58	6.7.1	General .....	32
59	6.7.2	Object size definitions and Required Pixel Density in IP VSS.....	33
60	6.8	Field of view – Other considerations .....	36
61	6.9	Illumination .....	36
62	6.10	IP Video equipment.....	38
63	6.11	Tamper protection/detection.....	38
64	6.11.1	Camera tamper protection/detection .....	38
65	6.11.2	System tamper protection/detection .....	39
66	6.12	System integration .....	39
67	7	Video signal presentation .....	39
68	7.1	Display types .....	39
69	7.2	Resolution .....	41
70	8	Transmission .....	42
71	8.1	Principles.....	42
72	8.1.1	General .....	42
73	8.1.2	Selection of IP video performance classes.....	42
74	8.1.3	Interoperability.....	43
75	8.1.4	Interoperability with voice communication .....	44
76	8.2	Wired transmission links .....	44
77	8.3	Wireless transmission links .....	44
78	8.4	Key considerations for IP based transmission systems .....	45
79	9	Video performance characteristics .....	46
80	9.1	Image compression.....	46
81	9.2	Frame rate .....	47
82	9.3	Resolution .....	47
83	10	Storage requirements .....	47
84	11	Image storage and export .....	48
85	11.1	Format of the compressed video data .....	48
86	11.2	Encryption .....	49
87	11.3	Basic metadata (time, date, camera identifier) .....	49
88	11.4	Multiplexing format.....	49
89	11.5	Image enhancements.....	50
90	11.6	Image export.....	50
91	11.7	Replay of exported images.....	50
92	12	VSCC control room configuration.....	51
93	12.1	Control rooms or Secure Viewing Area.....	51
94	12.2	Number, size and positioning of VSS video displays .....	51

95	12.3	Displays and screens mounted on or off the workstation .....	51
96	12.4	Recommended display sizes .....	52
97	12.5	Number of camera images per operator .....	52
98	12.6	Number of work stations .....	52
99	12.7	Equipment siting .....	53
100	12.8	Backup power supply provision .....	53
101	12.9	Operating temperature .....	53
102	12.10	Lightning and surge protection .....	53
103	13	Defining the test plan.....	53
104	13.1	Purpose of the test plan .....	53
105	13.2	User acceptance testing/inspection .....	54
106	13.3	Technical acceptance testing .....	54
107	13.3.1	Imaging chain consistency .....	54
108	13.3.2	Image quality .....	54
109	14	Documentational considerations (Pre-installation) .....	56
110	14.1	General.....	56
111	14.2	Risk assessment.....	56
112	14.3	Operational requirements.....	56
113	14.4	Design specification .....	56
114	14.5	Site plan .....	56
115	14.6	Test plan.....	57
116	15	System installation and commissioning .....	57
117	15.1	Factory acceptance testing .....	57
118	15.2	Installation process .....	57
119	15.3	User acceptance testing, commissioning and handover .....	58
120	15.4	Declaration of conformance to standards .....	58
121	16	Final documentation .....	58
122	16.1	General.....	58
123	16.2	Complete system drawings .....	59
124	16.3	System commission (with camera specific audits) .....	59
125	16.4	Interface descriptions.....	59
126	16.5	Operating logbook VSS.....	59
127	16.6	Compliance with legislation (for information) .....	59
128	17	Operation of VSS.....	60
129	17.1	General.....	60
130	17.2	Behaviour in the event of malfunctions .....	61
131	17.3	At-site visual check .....	61
132	17.4	Deviation of requirements for at-site visual checks and maintenance .....	62
133	17.5	Maintenance .....	62
134	17.6	Inspection (part of preventive maintenance) .....	62
135	17.7	Service Checks (part of preventive maintenance).....	64
136	17.8	Repair (corrective maintenance) .....	64
137	17.9	Improvement.....	64
138	Annex A	(informative) Video standard formats .....	65
139	A.1	Current video standard format.....	65
140	A.2	Pixel densities for recognition of other objects of interest .....	65
141	Annex B	(normative) Test protocol for VSS target .....	66
142	B.1	Scope of the test.....	66

143	B.2	Test prerequisites .....	66
144	B.3	Preconditions .....	66
145	B.4	Face selection .....	66
146	B.5	Live view methodology (faces) .....	67
147	B.6	Live view methodology (VRN) .....	67
148	B.7	Recorded view methodology (faces).....	67
149	B.8	Recorded view methodology (VRN).....	68
150	B.9	Motion.....	68
151	B.10	Faces: scoring criteria.....	68
152	B.11	VRN: scoring criteria.....	69
153	B.12	Heads control sheet (for example only) .....	71
154	B.13	VRN control sheet (for example only).....	72
155	Annex C (normative) Test method of image quality Guidance for the use of the video		
156		test target.....	73
157	Annex D (informative) Guide to specifying VSS parameters and security gradings .....		79
158	D.1	VSS parameters.....	79
159	D.2	Suggested building blocks .....	79
160	D.3	Security gradings .....	80
161	D.4	Security grading by system view: .....	80
162	D.5	Security grading by size view:.....	80
163	D.6	Security grading by application view .....	81
164	D.7	Number of frames depending on the object speed in a scene width.....	83
165	Annex E (normative) Detection response testing and acceptability criteria .....		85
166	E.1	General.....	85
167	E.2	False and nuisance alarms .....	85
168	E.3	Setting the response time .....	86
169	E.4	PTZ response time test procedure .....	86
170	E.5	Observer cueing and prompting .....	86
171	E.6	Detection test locations.....	87
172	E.7	Target camouflage .....	87
173	E.8	Tests with moving targets .....	87
174	E.9	Test conditions .....	87
175	E.10	Testing a 'live' system.....	88
176	E.11	Detection test results tables.....	88
177	Bibliography.....		89
178			
179	Figure 1 – structure of a security concept .....		21
180	Figure 2 – HD and UHD screen percentages occupied by various categories .....		35
181	Figure 3 – Pixel Density formula .....		35
182	Figure 4 – Operation of a VSS .....		60
183	Figure B.1 – Heads control sheet.....		71
184	Figure B.2 – VRN control sheet example.....		72
185	Figure C.1 – Test charts .....		75
186	Figure C.2 – Key to Figure C.1.....		77
187	Figure C.3 – Avoiding optical distortion .....		78
188			
189	Table 1 – Measures depending on Security Grades .....		24

190	Table 2 – Example System feedback – PTZ Control Responding time, performance and	
191	operator .....	29
192	Table 3 – Typical Lux level .....	37
193	Table 4 – Examples of display technologies .....	40
194	Table 5 – Example Resolutions .....	41
195	Table 6 – Wireless transmission options .....	45
196	Table 7 – Inspection cycles versus security grading .....	60
197	Table A.1 – Recommendations for recognition of some “non-human” objects .....	65
198	Table B.1 – Example auditor log sheet .....	69
199	Table B.2 – Example control room observer log sheet .....	69
200	Table B.3 – Example camera audit sheet .....	69
201	Table B.4 – Blank auditor log sheet .....	70
202	Table B.5 – Blank control room observer log sheet .....	70
203	Table B.6 – Blank camera audit sheet .....	70
204	Table C.1 – Test targets .....	73
205	Table D.1 – Suggested VSS building blocks .....	79
206	Table D.2 – Security grading by size view .....	81
207	Table D.3 – Security grading by application .....	82
208	Table D.4 – Security grading by critical infrastructure .....	83
209	Table D.5 – Number of frames depending of object speed - Low Pixel Density Objects .....	84
210	Table D.6 – Number of frames depending of object speed - High Pixel Density Objects .....	84
211	Table E.1 – Detection test results .....	88

212

oSIST prEN IEC 62676-4:2024

213 <https://standards.iteh.ai/catalog/standards/sist/8644647b-a836-4411-838b-6fd8dddcc705/osist-pren-iec-62676-4-2024>

214

215



## 216 INTERNATIONAL ELECTROTECHNICAL COMMISSION

217

218

219

**VIDEO SURVEILLANCE SYSTEMS FOR  
USE IN SECURITY APPLICATIONS –**

220

221

222

**Part 4: Application guidelines**

223

224

**FOREWORD**

225 1) The International Electrotechnical Commission (IEC) is a worldwide organization for standardization comprising  
226 all national electrotechnical committees (IEC National Committees). The object of IEC is to promote international  
227 co-operation on all questions concerning standardization in the electrical and electronic fields. To this end and  
228 in addition to other activities, IEC publishes International Standards, Technical Specifications, Technical Reports,  
229 Publicly Available Specifications (PAS) and Guides (hereafter referred to as "IEC Publication(s)"). Their  
230 preparation is entrusted to technical committees; any IEC National Committee interested in the subject dealt with  
231 may participate in this preparatory work. International, governmental and non-governmental organizations liaising  
232 with the IEC also participate in this preparation. IEC collaborates closely with the International Organization for  
233 Standardization (ISO) in accordance with conditions determined by agreement between the two organizations.

234 2) The formal decisions or agreements of IEC on technical matters express, as nearly as possible, an international  
235 consensus of opinion on the relevant subjects since each technical committee has representation from all  
236 interested IEC National Committees.

237 3) IEC Publications have the form of recommendations for international use and are accepted by IEC National  
238 Committees in that sense. While all reasonable efforts are made to ensure that the technical content of IEC  
239 Publications is accurate, IEC cannot be held responsible for the way in which they are used or for any  
240 misinterpretation by any end user.

241 4) In order to promote international uniformity, IEC National Committees undertake to apply IEC Publications  
242 transparently to the maximum extent possible in their national and regional publications. Any divergence between  
243 any IEC Publication and the corresponding national or regional publication shall be clearly indicated in the latter.

244 5) IEC itself does not provide any attestation of conformity. Independent certification bodies provide conformity  
245 assessment services and, in some areas, access to IEC marks of conformity. IEC is not responsible for any  
246 services carried out by independent certification bodies.

247 6) All users should ensure that they have the latest edition of this publication.

248 7) No liability shall attach to IEC or its directors, employees, servants or agents including individual experts and  
249 members of its technical committees and IEC National Committees for any personal injury, property damage or  
250 other damage of any nature whatsoever, whether direct or indirect, or for costs (including legal fees) and  
251 expenses arising out of the publication, use of, or reliance upon, this IEC Publication or any other IEC  
252 Publications.

253 8) Attention is drawn to the Normative references cited in this publication. Use of the referenced publications is  
254 indispensable for the correct application of this publication.

255 9) IEC draws attention to the possibility that the implementation of this document may involve the use of (a)  
256 patent(s). IEC takes no position concerning the evidence, validity or applicability of any claimed patent rights in  
257 respect thereof. As of the date of publication of this document, IEC [had/had not] received notice of (a) patent(s),  
258 which may be required to implement this document. However, implementers are cautioned that this may not  
259 represent the latest information, which may be obtained from the patent database available at  
260 <https://patents.iec.ch>. IEC shall not be held responsible for identifying any or all such patent rights.

261 IEC 62676-4 has been prepared by Technical Committee 79: ALARM AND ELECTRONIC  
262 SECURITY SYSTEMS. It is an International Standard.

263 This 2nd edition cancels and replaces the 1st edition published in 2014. This edition constitutes  
264 a technical revision.

265 **This edition includes the following significant technical changes with respect to the previous**  
266 **edition:**

267 a) ...;

268

269 The text of this International Standard is based on the following documents:

Draft	Report on voting
XX/XX/FDIS	XX/XX/RVD

270  
271 Full information on the voting for its approval can be found in the report on voting indicated in  
272 the above table.

273 The language used for the development of this International Standard is **English [change**  
274 **language if necessary]**.

275 This document was drafted in accordance with ISO/IEC Directives, Part 2, and developed in  
276 accordance with ISO/IEC Directives, Part 1 and ISO/IEC Directives, IEC Supplement, available  
277 at [www.iec.ch/members\\_experts/refdocs](http://www.iec.ch/members_experts/refdocs). The main document types developed by IEC are  
278 described in greater detail at [www.iec.ch/publications](http://www.iec.ch/publications).

279 The committee has decided that the contents of this document will remain unchanged until the  
280 stability date indicated on the IEC website under [webstore.iec.ch](http://webstore.iec.ch) in the data related to the  
281 specific document. At this date, the document will be

- 282 • reconfirmed,
- 283 • withdrawn, or
- 284 • revised.

285

iTeh Standards  
(<https://standards.iteh.ai>)  
Document Preview

[oSIST prEN IEC 62676-4:2024](https://standards.iteh.ai/catalog/standards/sist/8644647b-a836-4411-838b-6fd8dddcc705/osist-pren-iec-62676-4-2024)

<https://standards.iteh.ai/catalog/standards/sist/8644647b-a836-4411-838b-6fd8dddcc705/osist-pren-iec-62676-4-2024>

# VIDEO SURVEILLANCE SYSTEMS FOR USE IN SECURITY APPLICATIONS –

## Part 4: Application guidelines

286  
287  
288  
289  
290  
291  
292

### 293 1 Scope

294 This part of IEC 62676 gives recommendations and requirements for the, planning, design,  
295 installation, testing, commissioning, and maintaining of Video Surveillance Systems (VSS)  
296 comprising of image capture device(s), interconnection(s) and image handling device(s), for  
297 use in security applications within private or public spaces.

298 The objectives of this part of IEC 62676 are to:

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

### 303 2 Normative references iTeh Standards

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

308 IEC 31010, *Risk management - Risk assessment techniques* <sup>24</sup>

309 IEC 62305 (series), *Protection against lightning*

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

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

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

316  
317 IEC 62676-1-2: *Video surveillance systems for use in security applications – Part 1-2: General Video*  
318 *Transmission Requirements*

319  
320 IEC 62676-2-1: *Alarm systems – Video surveillance systems for use in security applications – Part 2-*  
321 *1: Video Transmission Protocols – General Requirements*

322  
323 IEC 62676-2-31: *Video surveillance systems for use in security applications - Part 2-31: Live*  
324 *streaming and control based on web services*

325 IEC 62676-2-32: *Video surveillance systems for use in security applications - Part 2-32:*  
326 *Recording control and replay based on web services*

327 IEC 62676-2-33: *Video surveillance systems for use in security applications - Part 2-33: Video*  
328 *transmission protocols – Cloud uplink and remote management system access*

- 329 IEC 62676-3: *Video surveillance systems for use in security applications– Part 3: Analog and digital*  
330 *video interfaces*  
331
- 332 IEC 62676-5: *Video surveillance systems for use in security applications - Part 5: Data*  
333 *Specifications and Image Quality Performance for Camera devices*  
334
- 335 IEC 62820-2: *Building intercom systems – Part 2: Requirements for advanced security*  
336 *building intercom systems (ASBIS)*  
337
- 338 IEC 62820-3-2: *Building intercom systems – Part 3-2: Application Guidelines – Advanced*  
339 *security building intercom systems (ASBIS)*  
340
- 341 ISO 31000: *Risk management - Guidelines*
- 342 ISO/IEC 11801 (series), *Information technology - Generic cabling for customer premises*
- 343 ISO/IEC 13818-1, *Information technology — Generic coding of moving pictures and associated*  
344 *audio information — Part 1: Systems*
- 345 ISO/IEC 14496-2, *Information technology — Coding of audio-visual objects — Part 2: Visual*
- 346 ISO/IEC 14496-10, *Information technology — Coding of audio-visual objects — Part 10:*  
347 *Advanced video coding*
- 348 ISO/IEC 15444-1, *Information technology — JPEG 2000 image coding system — Part 1: Core*  
349 *coding system*
- 350 ISO/IEC 19794-5, *Information technology — Biometric data interchange formats — Part 5: Face*  
351 *image data*
- 352 ITU-T Rec. T.81 / ISO/IEC 10918-1, *Information technology — Digital compression and coding*  
353 *of continuous-tone still images: Requirements and guidelines — Part 1: Requirements and*  
354 *guidelines*
- 355 ITU-T Rec. H.263, *Video coding for low bit rate communication*
- 356 ITU-T Rec. H.264, *Advanced video coding for generic audiovisual services*
- 357 ITU-T Rec. H.265, *High efficiency video coding*
- 358 ITU-R BT601, Standard to define how digital interlaced video signals to be coded (also formerly  
359 known as CCIR 601)

360

### 361 **3 Terms, definitions and abbreviations**

#### 362 **3.1 Terms and definitions**

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

##### 364 **3.1.1**

##### 365 **4K (UHD)**

366 The standard for Ultra High-Definition television (UHDTV) defined by SMPTE2036 to be with  
367 3.840 x 2.160 pixels at 25 or 30 fps.

368 **3.1.2**  
369 **8K (UHD)**  
370 The standard for Ultra High-Definition television (UHDTV) defined by SMPTE2036 to be with  
371 7.680 x 4.320 pixels at 25 or 30 fps.

372 **3.1.3**  
373 **At-site visual check**  
374 Activity to determine and assess the feasibility of implementing the safety concept per camera  
375 location to be monitored as well as checks of visible disturbances and defects - in particular for  
376 influences occurring outside of VSS system parts - on the monitoring tasks of a VSS that are  
377 not evaluated operationally and whether there are deviations from the function of the VSS  
378 required in the safety concept. The at-site visual check is the responsibility of the operator, who  
379 may, however, hand over the inspection to a competent person VSS or to a competent system  
380 engineer VSS.

381 **3.1.4**  
382 **camera housing**  
383 enclosure to provide physical and/or environmental protection of the camera, lens and ancillary  
384 equipment

385 **3.1.5**  
386 **camera sensitivity**  
387 Image capturing device capability to produce an image in certain light conditions

388 **3.1.6**  
389 **characterise**  
390 Minimum requirement of a VSS camera to characterise a target, e.g. persons (type of person,  
391 gait and actions can be characterised) and vehicles (vehicle brands can be characterised) with  
392 a display of > 250 pixel/metre

393 **3.1.7**  
394 **competent person VSS**  
395 Person who has been instructed by a competent system engineer VSS about the assigned tasks  
396 within the scope of the on-site check and the possible dangers and consequences of improper  
397 behaviour

398 Note 1 to the term: This includes the necessary knowledge for the assessment of the object requirements, with regard  
399 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  
400 the instruction about the security concept of the video surveillance system, about existing requirements as well as  
401 legal requirements or requirements of the operator from safety aspects as personal and property protection measures  
402 or to avoid personal injury.

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

409 **3.1.8**  
410 **Competent system engineer VSS**  
411 Person who, on the basis of professional technical training, knowledge and experience as well  
412 as knowledge of the relevant standards, regulations and directives, is able to assess the work  
413 to be carried out and recognise possible hazards.  
414 A competent system engineer VSS can be employed by either an installation company/system  
415 integrator company, project planning company or at owner or at user of the VSS.

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

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

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

### 432 **3.1.9**

#### 433 **Constant bit rate**

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

### 436 **3.1.10**

#### 437 **Corrective maintenance**

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

### 441 **3.1.11**

#### 442 **discern**

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

### 445 **3.1.12**

#### 446 **electronic iris**

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

### 449 **3.1.13**

#### 450 **electronic shutter**

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

### 453 **3.1.14**

#### 454 **event recording**

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

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

### 457 **3.1.15**

#### 458 **external synchronisation**

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

### 461 **3.1.16**

#### 462 **focal length (f)**

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

### 465 **3.1.17**

#### 466 **geo data**

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