



Technischer Leitfaden für Netzwerk-Video

Juni 2026

Einführung

Der vorliegende *Technische Leitfaden zu Netzwerk-Video* soll Sie bei Ihrer Arbeit mit Netzwerk-basierter Videosicherheit von Axis unterstützen und über aktuelle Technologieveränderungen informieren. Unser Leitfaden ist als umfassendes Informationsmaterial für alle Mitarbeiter gedacht, die sich mit der Entwicklung, Implementierung und Wartung von Axis Videosicherheitssystemen beschäftigen. Er bietet einen umfassenden Überblick zum Thema netzwerkbasierte Videosicherheit und behandelt die neuesten Entwicklungen bei Umgebungssensoren, Wärmebildkameras, Thermometern und Standards für Cybersicherheit.

Wir hoffen, dass unser *Technischer Leitfaden für Netzwerk-Video* Sie bei Ihrer Arbeit unterstützt!

Inhalt

1.	Netzwerkvideo: Überblick, Vorteile und Anwendungsbereiche	10
1.1	Überblick über ein Netzwerk-Videosystem	10
1.2	Vorteile	11
1.3	Anwendungen	13
2.	Netzwerk-Kameras	15
2.1	Was ist eine Netzwerk-Kamera?	15
2.1.1	AXIS Camera Application Platform (ACAP)	18
2.1.2	API (Application Programming Interface)	18
2.1.3	Über ONVIF	18
2.2	Kamerafunktionen für optimale Bildverwertbarkeit	19
2.2.1	WDR	20
2.2.2	Lightfinder-Technologie	20
2.2.3	Tag/Nacht-Funktionalität	21
2.2.4	Integrierte Infrarot-Beleuchtung	22
2.2.5	OptimizedIR	23
2.2.6	Objektive mit geringer Blendenzahl	23
2.2.7	Automatische Blendensteuerung	23
2.2.8	Die richtige Auflösung	23
2.2.9	Wärmebildtechnologie	24
2.2.10	Bildstabilisierung	25
2.3	Kamerafunktionen für einfache Installation	25
2.3.1	Geeignet für den Außeneinsatz	25
2.3.2	Fabrikseitige Fokussierung	26
2.3.3	Fernsteuerbare Fokussier- und Zoomfunktionen	26
2.3.4	Ferneinstellung des Auflagemaßes	26
2.3.5	3-Achsen-Kamerawinkelanpassung	26
2.3.6	Korridor-Format	27
2.3.7	Bild ausrichten	27
2.3.8	Pixelzähler	27
2.4	Verschiedene Typen von Netzwerk-Kameras	28
2.4.1	Bullet-Kameras	28
2.4.2	Box-Kameras	29
2.4.3	Blockkameras	29
2.4.4	Dome-Kameras	30
2.4.4.1	Onboard-Kameras	30
2.4.4.2	Panorama-Kameras	31

2.4.5	Modulare Kameras	33
2.4.6	PTZ-Kameras	36
2.4.6.1	Sharpdome-Technologie	38
2.4.7	Wärmebildkameras	40
2.4.7.1	Temperaturmesskameras	43
2.4.8	Explosionsgeschützte Kameras	44
3.	Kameraelemente	47
3.1	Lichtempfindlichkeit	47
3.2	Objektive	48
3.2.1	Objektivtypen	49
3.2.2	Sichtfeld	49
3.2.3	Blendenzahl und Belichtung	51
3.2.4	Blendentypen	51
3.2.5	Schärfentiefe	52
3.2.6	Abstimmung von Objektiv und Sensor	53
3.2.7	Objektivtypen für die Überwachung	54
3.2.8	Fokussieren	55
3.2.9	PTZ-Präzision	57
3.3	Abnehmbarer Infrarot-Sperrfilter (Tag-/Nacht-Funktion)	57
3.4	Bildsensoren	60
3.5	Belichtungssteuerung	61
3.5.1	Belichtungspriorität	61
3.5.2	Belichtungszone	62
3.5.3	Gegenlichtausgleich	62
3.5.4	Dynamischer Aufnahmebereich	62
3.5.5	WDR-Bilder	63
3.6	Aktiver Manipulationsalarm	64
3.7	Audioerfassung	64
4.	Video-Encoder	65
4.1	Was ist ein Video-Encoder?	65
4.1.1	Kriterien für Video-Encoder-Komponenten	66
4.1.2	Ereignisverwaltung und Analyse	66
4.2	Video-Encoder für analoge PTZ-Kameras	67
4.3	Deinterlacing-Techniken	67
4.4	Video-Decoder	68
5.	Bildaufösungen	70
5.1	Auflösungen im Megapixel-Bereich	70
5.2	HDTV-Auflösungen (High-Definition Television)	70

5.3	Ultra-HD-Auflösungen	71
5.4	Seitenverhältnisse	72
6.	Videokomprimierung	75
6.1	Grundlagen der Komprimierung	75
6.1.1	Video-Codec	75
6.1.2	Vergleich zwischen Bild- und Videokomprimierung	76
6.2	Komprimierungsformate	79
6.2.1	H.264	79
6.2.2	H.265	79
6.2.3	AV1	80
6.2.4	Zipstream für H.264, H.265 und AV1	80
6.2.5	Motion JPEG	81
6.2.6	JPEG	82
6.3	Durchschnittliche, variable und maximale Bitraten	82
6.4	Standards im Vergleich	83
7.	Audio	86
7.1	Audioerfassung	86
7.1.1	Geräte und Technologien für audiobasierte Konnektivität	86
7.1.2	Verbesserungen bei der Audioerfassung	88
7.1.3	Audioanalyse	88
7.2	Audio-Ausgang	89
7.2.1	Audioausgang zur Videosicherheit	89
7.2.2	Netzwerk basierte Audiosysteme für Durchsagen	90
7.3	Audio-Kommunikationsmodi	91
7.4	Audiocodecs	91
7.5	Audio- und Videosynchronisierung	92
8.	Radar	93
8.1	Eine nicht-visuelle Technologie als Ergänzung der Videosicherheit	93
8.2	Radargeräte	94
8.3	Radargeräte in einem Sicherheitssystem	95
9.	Zutrittskontrolle	97
9.1	Was ist die Zutrittskontrolle?	97
9.2	Wozu braucht man IP bei der Zutrittskontrolle?	98
9.3	Komponenten der Zutrittskontrolle	99
9.3.1	Netzwerk-Tür-Controller	100
9.3.2	Leser	100
9.3.3	Netzwerk-I/O-Relaismodule	100

9.3.4	Zutrittsverwaltungssysteme	101
10.	Netzwerk-Gegensprechanlagen	102
10.1	Multifunktionale Kommunikationsgeräte für mehr Sicherheit	102
11.	Body Worn	104
11.1	Der Zweck von Body Worn-Kameras	104
11.2	Am Körper getragene Kameras	105
11.3	Axis Body Worn Solution	106
11.4	Bordeigene Lösung	108
12.	Umgebungssensoren	109
12.1	Luftqualitätssensoren	109
12.1.1	Überwachung der Raumluftqualität	109
12.1.2	Luftqualitätsparameter	111
12.1.3	Axis Luftqualitätssensoren	113
12.1.3.1	Freistehender Luftqualitätssensor	113
12.1.3.2	Luftqualitätssensor mit Hostgerät	113
13.	Analyse	114
13.1	Analysefunktionen für eine smarte, sicherere Welt	114
13.2	Welche Vorteile bieten Analysefunktionen?	115
13.2.1	Echtzeitüberwachung	115
13.2.2	Effiziente Suche	117
13.2.3	Erkennen von Trends und Mustern	117
13.2.4	Datenschutz	118
13.3	Systemarchitektur – wo wird das Video analysiert?	118
13.4	Bildqualität und Edge-basierte KI – die Grundlage für hervorragende Analysefunktionen	119
13.5	Künstliche Intelligenz	120
13.6	AXIS Camera Application Platform	121
14.	Netzwerktechnologien	122
14.1	LAN und Ethernet	122
14.1.1	Arten von Ethernet-Netzwerken	123
14.1.2	Anschließen von Netzwerk-Geräten und -Switches	123
14.1.3	Power over Ethernet	125
14.2	Senden von Daten über das Internet	128
14.2.1	IP-Adressierung	129
14.2.1.1	IPv4-Adressen	129
14.2.1.2	IPv6-Adressen	130

14.2.2	Datenübertragungsprotokolle für Netzwerk-Video	131
14.2.3	SIP	133
14.3	VLANs	134
14.4	Quality of Service	135
14.5	Edge-to-Edge	136
14.6	Portcast	137
15.	Systemschutz	139
15.1	Netzwerk-Schutz	139
15.1.1	IEEE 802.1X	139
15.1.2	HTTPS (HTTP over TLS)	140
15.1.3	MACsec	141
15.1.4	Vertrauenswürdige Infrastruktur für öffentliche Schlüssel (PKI)	141
15.1.5	Anmeldung über sicheren Transport	141
15.1.6	NTS Network Time Protocol	142
15.1.7	Netzwerk-Isolierung	142
15.2	Cybersicherheitsstandards	142
15.2.1	ISO 27001	142
15.2.2	SOC 2	142
15.2.3	ETSI EN 303 645	143
15.2.4	FIPS 140 (Federal Information Processing Standard)	143
15.2.5	Common Criteria (CC)	143
15.3	Geräteschutz	144
15.3.1	Integrierte Cybersicherheitsplattform	144
15.3.2	Benutzerkontenverwaltung	145
15.3.3	Hostbasierte Firewall	145
15.3.4	Immer aktuelle Gerätesoftware	145
15.3.5	Protokollierung von Audits	146
15.4	Schutz der VMS	146
15.5	Physischer Schutz	147
16.	Drahtlose Netzwerktechnologien	148
16.1	802.11-WLAN-Standards	148
16.2	WLAN-Sicherheit	149
16.2.1	WPA2™ ¹	149
16.3	Wireless-Bridges	150
16.4	Drahtloses Mesh-Netzwerk	150
16.5	4G- und 5G-Netzwerke	150
16.6	Z-Wave®	151
16.7	Zigbee®	151

17.	Videoverwaltungssysteme	152
17.1	Arten von Videoverwaltungssystemen	152
17.1.1	Cloudbasierte Systeme	153
17.1.1.1	AXIS Camera Station Edge	153
17.1.2	Private Netzwerke	154
17.1.2.1	AXIS Camera Station Pro	155
17.1.3	Maßgeschneiderte Lösungen der Axis-Partner	157
17.2	Systemmerkmale	157
17.3	Integrierte Systeme	158
17.3.1	Zutrittskontrolle	158
17.3.2	Kassenterminal	159
17.3.3	Gebäudeverwaltung	159
17.3.4	Industrielle Kontrollsysteme	160
17.3.5	RFID	160
18.	Cloud-Technologien	161
18.1	Verschiebung in die Cloud	161
18.2	Cloud-Setups	161
18.3	Axis Cloud Connect	162
19.	Überlegungen für das Systemdesign	164
19.1	Auswahl einer Kamera	164
19.1.1	Kameratypen	164
19.1.2	Bildqualität	166
19.1.3	Auflösung	166
19.1.4	Komprimierung	169
19.1.5	Netzwerkfunktionalität	169
19.1.6	Weitere Funktionen	170
19.2	Installation einer Netzwerk-Kamera	172
19.2.1	Überwachungsziel	172
19.2.2	Umgang mit schwierigen Lichtverhältnissen	172
19.2.3	Objektivauswahl	173
19.3	Physischer Schutz der Kamera	173
19.3.1	Schutz und Standards	173
19.3.2	Externe Gehäuse	175
19.3.2.1	Unbewegliche Kameras in Gehäusen positionieren	175
19.3.3	Transparente Dome-Kameras	175
19.3.4	Schutz vor Vandalismus und Manipulation	176
19.3.5	Arten von Befestigungsätzen	178
19.4	Kriterien für die Bandbreite und den Speicher	181

19.4.1	Bits oder Bytes?	181
19.4.2	Bandbreitenanforderungen	183
19.4.3	Speichieranforderungen	184
19.4.4	Systemkonfigurationen	184
19.4.5	Edge Storage	187
19.4.6	Server-basierter Speicher	189
19.4.7	NAS und SAN	189
19.4.8	Redundanter Speicher	191
20.	Tools und Ressourcen	193
20.1	Produkte finden und vergleichen	193
20.2	Standorte planen und gestalten	193
20.3	Systeme installieren und verwalten	194
21.	Axis Communications Academy	195
21.1	Aufbau von Fachwissen für intelligentere Geschäftsprozesse	195

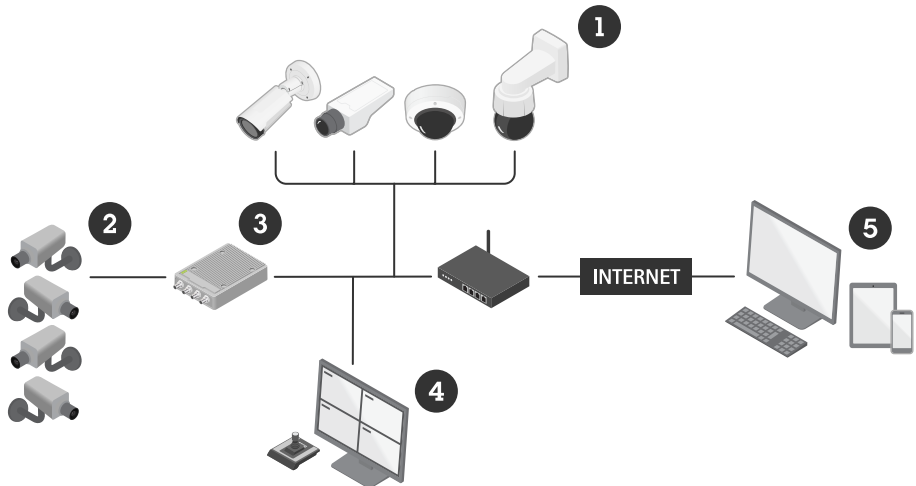
1. Netzwerkvideo: Überblick, Vorteile und Anwendungsbereiche

Ein Netzwerk-Videosystem verwendet IP-basierte Standardnetzwerke für die Übertragung von Video- und Audiodaten. Digitalisierte Video- und Audiostreams werden über kabelgebundene oder kabellose IP-Netzwerke übertragen. Das ermöglicht die Videoüberwachung und -aufzeichnung im gesamten Netzwerk. Mit einer Vielzahl von erweiterten Funktionen bietet Netzwerk-Video eine Menge an Sicherheitsüberwachung. Die hohe Videoqualität, die Skalierbarkeit und die integrierte Intelligenz von Netzwerk-Video ermöglichen es dem Sicherheitspersonal, Menschen, Eigentum und Vermögenswerte besser zu schützen.

1.1 Überblick über ein Netzwerk-Videosystem

Netzwerk-Video wird oft auch als *IP-basierte Videosicherheit* oder *IP-Videoüberwachung* bezeichnet, da die Anwendung vor allem in der Sicherheitsbranche erfolgt und eine kabelgebundene oder drahtlose IP-Netzwerkinfrastruktur zur Übertragung digitaler Video-, Audio- und anderer Daten genutzt wird. Das Netzwerk versorgt die Netzwerk-Videogeräte auch über Power over Ethernet (PoE)-Technologie mit Strom.

Ein Netzwerk-Videosystem ermöglicht die Überwachung und Aufzeichnung im gesamten Netzwerk, egal ob es sich dabei um ein LAN oder Wide Area Network (WAN) wie das Internet handelt.



Ein Netzwerk-Videosystem mit Netzwerk-Kameras (1), analogen Kameras (2), die über Video-Encoder (3) verbunden sind, und Video Management Software (4). Bei den anderen Komponenten wie Netzwerk-Infrastruktur, Speicher und Server handelt es sich um Standard-IT-Ausstattung. Der Fernzugriff ist über einen Computer oder ein Mobilgerät (5) möglich.

Die wichtigsten Komponenten eines Netzwerk-Videosystems sind die Netzwerk-Kamera, der Video-Encoder (zum Anschließen analoger Kameras an ein IP-Netzwerk), das Netzwerk, der Server und Speicher sowie die Video Management Software (VMS). Netzwerk-Kameras und Video-Encoder sind computerbasiert und bieten Funktionen, die mit analogen Videoüberwachungs-Kameras nicht bereit gestellt werden können.

Einer der wichtigsten Vorteile von Netzwerk-Video ist, dass die Komponenten Netzwerk, Server und Speicher leicht zu beschaffende Standardgeräte sind. Weitere Komponenten sind Zubehör wie Halterungen, PoE Midspans oder Joysticks. Die Netzwerk-Videokomponenten werden in den jeweiligen Kapiteln eingehender beschrieben.

1.2 Vorteile

Ein vollständig digitales IP-Videosicherheitssystem verfügt über eine Vielzahl moderner Funktionen. Netzwerk-Video bietet eine hohe Bildqualität, Fernzugriff, Analysefunktionen, einfache Integrationsmöglichkeiten, Skalierbarkeit, Flexibilität, ein gutes Preis-Leistungsverhältnis und sichere Kommunikation.

- > **Hohe Bildqualität.** Bei der Videosicherheit ist eine hohe Bildqualität unverzichtbar, um Vorfälle klar erfassen und beteiligte Personen oder Objekte identifizieren zu können. Dank

Vollbildverfahren und HDTV-/Megapixel-Technologie liefert eine Netzwerk-Kamera eine hohe Bildqualität und eine hohe Auflösung. Weitere Informationen zur Bildqualität siehe Kapitel , und .

- > **Fernzugriff.** Netzwerk-Kameras und Video-Encoder sind per Fernzugriff zugänglich und konfigurierbar, sodass mehrere autorisierte Benutzer jederzeit und von jedem Ort, der mit dem Netzwerk verbunden ist, Live-Videobilder und Videoaufzeichnungen abrufen können. So lässt sich externen Benutzern, z. B. einer Alarmüberwachungszentrale oder der Polizei, Zugriff auf die Videobilder gewähren.
- > **Analyse.** In Netzwerk-Video kann eine Kamera viel mehr als nur eine Videoquelle sein. Analysefunktionen in der Kamera werden verwendet, um aus riesigen Mengen an Video die nützlichen Informationen zu extrahieren und bei Bedarf sofortige, automatische Aktionen auszulösen. Diese können das Sicherheitspersonal benachrichtigen oder eine Videoaufzeichnung starten, wenn bestimmte Ereignisse erkannt werden. Analysefunktionen, die Deep-Learning-Algorithmen für die Objekterfassung und -klassifizierung verwenden, können sehr detaillierte Informationen über Personen und Fahrzeuge in einer Szene extrahieren und so äußerst genaue und effiziente Suchanfragen ermöglichen. Weitere Informationen zur Analysefunktionen finden Sie in Kapitel .
- > **Einfache, zukunftsichere Integration.** Netzwerk-Videoprodukte, die auf offenen Standards basieren, können problemlos in eine Vielzahl von Video Management Systemen integriert werden. Die Videofunktionen einer Netzwerk-Kamera lassen sich auch in andere Systeme integrieren, wie zum Beispiel Kassenterminals, Zutrittskontroll- oder Gebäudeverwaltungssysteme. Weitere Informationen zu integrierten Systemen siehe Kapitel .
- > **Skalierbarkeit und Flexibilität.** Ein Netzwerk-Videosystem kann den Anforderungen des Benutzers angepasst werden. Videoprodukte und andere Arten von Anwendungen nutzen dasselbe drahtgebundene oder drahtlose IP-Netz für die Datenübertragung. Video, Audio, PTZ und I/O-Befehle, andere Daten und Stromversorgung können über das gleiche Kabel übertragen werden. Es lässt sich eine beliebige Anzahl von Geräten zum System hinzufügen, ohne dass aufwendige oder teure Änderungen an der Netzwerkinfrastruktur erforderlich sind. Geräte können an praktisch jedem Ort eingesetzt und von einem beliebigen anderen Ort gesteuert werden. Das System kann sowohl offen als auch geschlossen konfiguriert werden. Da ein Netzwerk-Videosystem auf Standard-IT-Ausrüstung und -Protokollen basiert, kann es bei Systemerweiterungen genau von diesen Technologien profitieren. Die Videoaufnahmen können zum Beispiel in redundanten Servern an verschiedenen Orten gespeichert werden, um die Zuverlässigkeit und Sicherheit zu erhöhen. Es lassen sich Tools zur automatischen Lastverteilung, Netzwerkverwaltung und Systemwartung nutzen.
- > **Kosteneffektivität.** Die Gesamtbetriebskosten von IP-Sicherheitssystemen sind in der Regel gering. Oft ist bereits eine Netzwerkinfrastruktur vorhanden, die für andere Anwendungen

innerhalb einer Organisation genutzt wird. Eine Netzwerk-Video-Anwendung lässt sich so problemlos innerhalb der bestehenden Infrastruktur installieren. Die Verwaltungs- und Gerätekosten fallen ebenfalls geringer aus, da Back-End-Anwendungen und Speichersysteme auf branchenüblichen, auf offenen Systemen basierenden Standardservern ausgeführt werden und nicht auf herstellerspezifischer Hardware, wie z. B. einem DVRs bei einem analogen Videoüberwachungssystem. Viele Netzwerk-Videogeräte werden über die Power over Ethernet (PoE)-Technologie mit Strom versorgt, die das System über das gleiche Ethernet-Kabel mit Strom versorgt, über das auch die Daten (Video) übertragen werden. PoE hält die Installationskosten niedrig und erleichtert die Datensicherung. Weitere Informationen zu PoE siehe Kapitel .

- > **Sichere Übertragung.** Netzwerk-Videogeräte und ihre Videostreams können auf viele verschiedene Arten gesichert werden. Dazu gehören die Authentifizierung mit Benutzername und Kennwort, IP-Adressen-Filterung, Authentifizierung mithilfe von IEEE 802.1X, die Datenverschlüsselung mithilfe von HTTPS (SSL/TLS) sowie die Verwendung mehrerer Benutzerzugriffsebenen. Weitere Informationen zur Netzwerksicherheit finden Sie in Kapitel .
- > **Höhere Sicherheit.** Axis Geräte werden durch die hardwarebasierte Cybersicherheitsplattform Axis Edge Vault abgesichert, die das Cybersecurity-Risiko für Geräte minimiert und es ihm ermöglicht, ein vertrauenswürdiges und zuverlässiges Gerät innerhalb des Netzwerks zu sein. Axis Edge Vault ermöglicht Cybersicherheitsfunktionen wie signiertes Betriebssystem (gewährleistet, dass AXIS OS nicht gefährdet ist), sicheres Booten (gewährleistet, dass beim Hochfahren nicht authentifizierter oder veränderter Code verworfen wird) und signiertes Video (Überprüfung der Authentizität von Videos durch eine Signatur im Videostream).

Bereits bestehende analoge Videoinstallationen können in ein Netzwerk basiertes Videosystem eingebunden werden und so mithilfe von Video-Encodern und Geräten wie Ethernet-over-Coax-Adaptern von einigen Vorteilen der digitalen Funktionen profitieren. Vorhandene Koaxialkabel lassen sich so weiterverwenden. Weitere Informationen zu Video-Encodern und Decodern, siehe Kapitel .

1.3 Anwendungen

Den Anwendungsmöglichkeiten von Netzwerk-Video sind fast keine Grenzen gesetzt. Am häufigsten wird es für die Sicherheits- und Fernüberwachung von Personen, Standorten, Immobilien und Arbeitsprozessen verwendet. Die steigende Zahl der Analyseanwendungen führt jedoch dazu, dass Netzwerk-Video zunehmend zur Optimierung der Wirtschaftlichkeit verwendet wird. Folgende Beispiele sind typische Anwendungsmöglichkeiten in wichtigen Branchen.

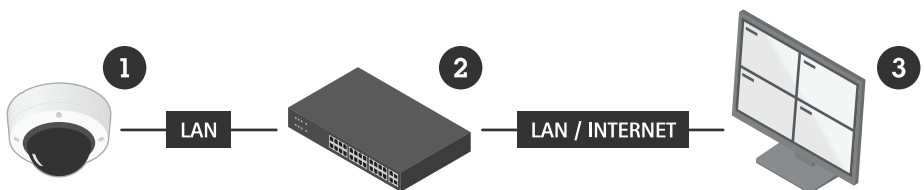
- > **Einzelhandel.** Netzwerk-Videosysteme in Einzelhandelsgeschäften können zu einer deutlichen Senkung der Diebstahlrate beitragen, die Sicherheit der Mitarbeiter erhöhen und die Verwaltung der Ladengeschäfte optimieren.
- > **Verkehr.** Netzwerk-Video trägt zum Schutz von Fahrgästen, Personal und Vermögenswerten in allen Arten von Verkehrsmitteln bei.
- > **Banken und Finanzwesen.** Mithilfe von Netzwerk-Videosystemen können Banken ihre Hauptsitze, Filialen und Geldautomaten zentral und effizient überwachen.
- > **Städteüberwachung.** Netzwerk-Video ist eines der wirkungsvollsten Instrumente zur Verbrechensbekämpfung und für den Schutz der Bevölkerung. Es kann sowohl zur Erkennung als auch zur Abschreckung eingesetzt werden.
- > **Bildungswesen.** Von Kindertagesstätten bis zu Universitäten tragen Netzwerk-Videosysteme dazu bei, Vandalismus zu verhindern und die Sicherheit von Mitarbeitern und Schülern und Studenten zu erhöhen.
- > **Ämter und Behörden.** Netzwerk-Video eignet sich für Polizei, Militär und Zoll. Es lässt sich auch effizient zur Sicherung aller Arten von öffentlichen Gebäuden einsetzen.
- > **Gesundheitswesen.** Mit Netzwerk-Video können Krankenhäuser und andere Einrichtungen des Gesundheitswesens die allgemeine Sicherheit und den Schutz der Mitarbeiter, Patienten und Besucher erhöhen.
- > **Industrie.** Netzwerk-Video ist nicht nur ein effektives Werkzeug zur Sicherung von Umgrenzungen und Grundstücken: Es kann auch eingesetzt werden, um Fertigungsanlagen, Verarbeitungsprozesse und Logistiksysteme zu überwachen und deren Effizienz zu steigern.
- > **Kritische Infrastrukturen.** Ob Solaranlage, Umspannwerk oder Abfalldeponie: Netzwerk-Video hilft dabei, den sicheren und unterbrechungsfreien Betrieb zu gewährleisten. Die Produktionsdaten aus entfernten Betriebsstätten können um visuelle Informationen ergänzt werden.

2. Netzwerk-Kameras

Netzwerk- oder IP-Kameras verfügen über eine große Vielfalt von Funktionen und Merkmalen und erfüllen die Anforderungen fast jedes Sicherheitssystems. In diesem Kapitel wird beschrieben, was eine Netzwerk-Kamera ist, welche Optionen und Funktionen sie haben kann und welche Kamerateypen es gibt: Unbewegliche Kameras, PTZ-Kameras (mit Schwenk-/Neige-/Zoomfunktion), modulare Kameras, Wärmebildkameras und explosionsgeschützte Kameras.

2.1 Was ist eine Netzwerk-Kamera?

Eine Netzwerk-Kamera, auch IP-Kamera genannt, wird in erster Linie zum Senden von Video/Audio über ein IP-Netzwerk, etwa ein lokales Netzwerk (LAN) oder das Internet, eingesetzt. Netzwerk-Kameras ermöglichen Live-Ansicht und/oder Aufzeichnungen – entweder kontinuierlich, zu festgelegten Zeiten, auf Anforderung oder bei Auslösung durch ein Ereignis. Die Speicherung von Video kann im Gerät und/oder an einem Remote-Standort erfolgen. Der autorisierte Zugriff auf Video ist von jedem Ort mit Zugang zu einem IP-Netzwerk möglich.



Eine Netzwerk-Kamera (1) wird mit einem Netzwerk-Switch (2) verbunden, und über das Netzwerk kann auf Video (3) zugegriffen werden.

Eine Netzwerk-Kamera lässt sich als Kombination von Kamera und Computer in einem Gerät beschreiben. Hauptkomponenten sind ein Objektiv, ein Bildsensor, mindestens ein Prozessor und ein Datenspeicher. Die Prozessoren dienen zur Bildverarbeitung, Komprimierung, Videoanalyse sowie

für Netzwerkfunktionen. Der Speicher dient in erster Linie zum Speichern der Gerätesoftware, aber auch zum Speichern von Videodaten.

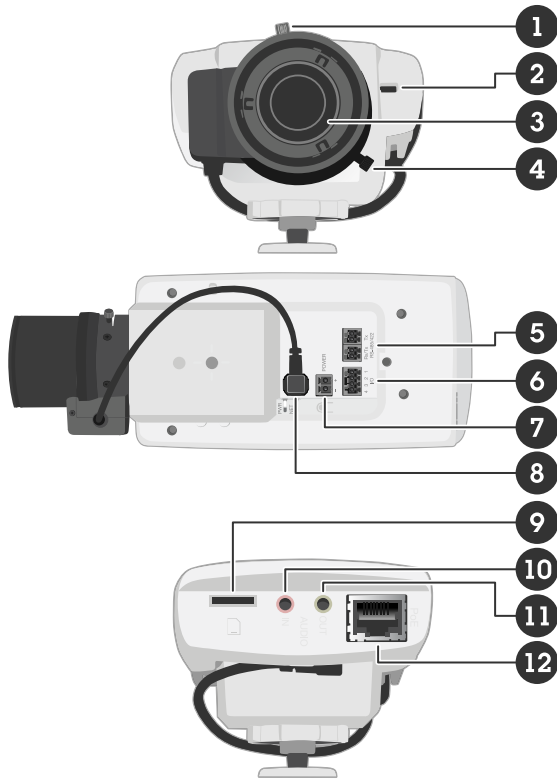
Wie ein Computer verfügt die Kamera über eine eigene IP-Adresse, ist direkt mit einem kabelgebundenen oder drahtlosen Netzwerk verbunden und kann an jedem Ort mit Netzwerk-Verbindung installiert werden. Das unterscheidet sie von einer Web-Kamera, die nur funktioniert, wenn sie an einen PC angeschlossen ist.

Netzwerk-Kameras erfassen nicht nur Videos, sondern ermöglichen auch die Verwaltung von Ereignissen, mit denen Sie automatische Reaktionen auf vordefinierte Ereignisse programmieren können. Zu den typischen Reaktionen zählen das Senden von Live-Video- und E-Mail-Benachrichtigungen, das Aktivieren von Geräten wie Türen und Leuchten sowie das Initiieren von Videoaufzeichnungen. Indem Sie nur dann aufzeichnen, wenn etwas Bestimmtes in der Szene passiert, können Sie die Netzwerkbandbreite und den Speicherplatz effizienter nutzen.

Netzwerk-Kameras unterstützen Analysefunktionen, die automatisch die für den Videostream wichtigen Informationen extrahieren und diese für wertvolle Einblicke nutzen. Analysefunktionen, die in die Kamera eingebettet sind (Edge Analytics), bieten mehrere Vorteile, z. B. einen reduzierten Bedarf an Netzwerkübertragung und geringe Latenz in Szenarien, die eine schnelle Reaktion erfordern. Die Axis Scene Intelligence-Technologie kombiniert fortschrittliche Bildverarbeitungstechnologie mit Analysefunktionen und Deep Learning direkt auf dem Endgerät (der Kamera), um eine überragende Grundlage für eine konsistente Analyseleistung zu schaffen. Sie ermöglicht es der Kamera auch, sich automatisch anzupassen, wenn sich die Umstände ändern.

Viele Netzwerk-Kameras unterstützen Audio. Sie verfügen möglicherweise über Audio-Ein- und -Ausgangs-Ports oder können Audiogeräte über Portcast-Technologie oder Edge-to-Edge-Technologie anschließen (beide bieten vollständig in die Kamera integriertes Audio). Netzwerk-Kameras verfügen häufig über Eingabe-/Ausgabe(E/A)-Ports, die den Anschluss von anderen externen Geräten wie Bewegungssensoren, Türverriegelungsrelais und Audio- und visuellen Alarmmeldern ermöglichen.

Die Stromversorgung der meisten Netzwerk-Videokameras erfolgt über die Power over Ethernet (PoE)-Technologie, d. h. die Stromversorgung erfolgt über das Netzkabel. Außerdem verfügen sie über einen Speicherkartensteckplatz für die lokale Speicherung von Aufzeichnungen.



Vorder-, Unter- und Rückseite einer typischen Netzwerk-Kamera.

1. Zoomregler
2. Internes Mikrofon
3. Objektiv mit P-Iris
4. Fokusregler
5. Serieller Port
6. E/A-Klemmleiste
7. Stromanschluss
8. Blendenanschluss
9. Speicherkarteneinschub
10. Audio-Eingang
11. Audio-Ausgang
12. Netzwerk-Anschluss

Axis Kameras werden über die Video Management Software (VMS) AXIS Camera Station Edge oder AXIS Camera Station Pro, die die Kamera automatisch erkennt und konfiguriert, in einem Netzwerk installiert. Kunden mit großen Systemen können die Kameras mithilfe von AXIS Device Manager konfigurieren. Sie können auch direkt über die integrierten Webseiten auf die Kamera zugreifen, indem sie ihre IP-Adresse in einen Browser eingeben. Konfigurationsbelange wie z. B. Benutzerzugriff, Kameraeinstellungen, Auflösung, Bildrate, Komprimierungsformat (H.264/H.265/AV1) sowie Regeln für Ereignisse.

Axis Kameras unterstützen eine Vielzahl von Zubehörprodukten, mit denen sich die Fähigkeiten der Kameras erweitern lassen. Beispielsweise können Netzwerk-Kameras über einen Media Converter-Switch an ein Glasfasernetzwerk oder über einen Coax-Adapter an Koaxialkabel angeschlossen werden und dabei PoE nutzen.

2.1.1 AXIS Camera Application Platform (ACAP)

Die meisten Axis Kameras (sowie Lautsprecher, Türsprechanlagen und Radarprodukte) werden von der AXIS Camera Application Platform (ACAP) unterstützt. ACAP ist eine offene Plattform für eine breite Palette von Industrien und Einsatzzwecken und aktiviert Analysefunktionen, die über die Website von Axis oder von Drittanbietern aufgerufen werden können. Diese Anwendungen können heruntergeladen und auf den Geräten installiert werden. ACAP ermöglicht auch die Entwicklung kundenspezifischer Anwendungen und die (vollständige oder teilweise) Ausführung von Anwendungen auf dem Gerät durch die Kombination von fortschrittlichen Analysefunktionen und cloudbasierten oder serverbasierten Technologien. Weitere Informationen zu ACAP finden Sie unter www.axis.com/for-developers/acap

2.1.2 API (Application Programming Interface)

Alle Netzwerk-Videoprodukte von Axis verfügen über eine Schnittstelle für die Anwendungsprogrammierung (API) namens VAPIX®. VAPIX ermöglicht Entwicklern die einfache Integration von Netzwerk-Videoprodukten von Axis und ihrer integrierten Funktionen in andere Software-Lösungen.

2.1.3 Über ONVIF

Die meisten Netzwerk-Videoprodukte von Axis sind ONVIF-konform. ONVIF®¹ ist ein globales, offenes Industrieforum, das 2008 von Axis, Bosch und Sony mit dem Ziel gegründet wurde, die Interoperabilität der Netzwerk-Videoprodukte verschiedener Hersteller zu standardisieren und damit zu erhöhen. Es gibt den Benutzern die Flexibilität, ONVIF-konforme Produkte unterschiedlicher Hersteller in einem herstellerübergreifenden, IP-basierten physischen Sicherheitssystem zu verwenden. ONVIF wird heute von den meisten der weltweit größten

Hersteller von IP-basierten physischen Sicherheitsprodukten unterstützt und hat mehr als 500 Mitgliedsunternehmen. Weitere Informationen finden Sie unter www.onvif.org.

¹ONVIF ist eine eingetragene Marke von ONVIF, Inc.

2.2 Kamerafunktionen für optimale Bildverwertbarkeit

Klare und detailreiche Bilder sind die Grundlage einer zuverlässigen Videoüberwachung. Doch anspruchsvolle Licht- und Umgebungsbedingungen erschweren die Bildaufnahme erheblich.

Schwache oder fehlende Beleuchtung stellt eine dauerhafte Herausforderung dar. Wenn das natürliche Licht nachlässt oder Bereiche nur schwach beleuchtet sind, können Bilder dunkel und verrauscht wirken, sodass wichtige Details im Bildrauschen verloren gehen. Für eine zuverlässige Videoüberwachung bei völliger Dunkelheit ist eine zusätzliche IR-Beleuchtung erforderlich. Auch Szenen mit sehr hellen und sehr dunklen Bildbereichen können eine Herausforderung darstellen. Treten gleichzeitig extreme Helligkeitsunterschiede auf – etwa durch grelles Sonnenlicht und tiefe Schatten –, können Bilder überbelichtete helle oder unterbelichtete dunkle Bereiche aufweisen, wodurch wichtige Details verloren gehen.

Das Streben nach Detailtreue erfordert eine angemessene Auflösung. Eine höhere Pixelzahl kann zwar für mehr Bilddetails sorgen, doch für die Identifikation von Personen oder Objekten und die forensische Auswertung ist vor allem die Qualität der Pixel unter schwierigen Lichtverhältnissen entscheidend.

Für flüssige Videoaufnahmen ist zudem eine ausreichend hohe Bildrate erforderlich. Dies erfordert jedoch häufig kürzere Belichtungszeiten. Kurze Belichtungszeiten frieren Bewegungen ein und reduzieren Bewegungsunschärfe. Gleichzeitig gelangt jedoch weniger Licht auf den Bildsensor, wodurch sich die Herausforderungen bei schlechten Lichtverhältnissen verschärfen. Längere Belichtungszeiten erfassen hingegen mehr Licht, erhöhen jedoch das Risiko von Bewegungsunschärfe. Die richtige Balance zwischen Bildhelligkeit und Bildschärfe ist dabei entscheidend.

Neben diesen zentralen Herausforderungen bei der Bildaufnahme können auch Umwelteinflüsse wie Vibrationen oder Sichtbehinderungen durch Nebel die Qualität des Videomaterials beeinträchtigen.

Axis bietet eine Reihe fortschrittlicher Technologien, die speziell entwickelt wurden, um diese Herausforderungen zu meistern. Axis Kameras sind zudem für einen vollautomatischen Betrieb ausgelegt. Das bedeutet, dass sich die Bildverarbeitungsparameter automatisch an wechselnde Lichtverhältnisse anpassen – ganz ohne manuelle Einstellungen. Diese Kombination aus

Kamerafunktionen und automatischen Anpassungen gewährleistet eine hohe Bildqualität und zuverlässige Bildverwertbarkeit – selbst unter anspruchsvollen und wechselnden Bedingungen.

2.2.1 WDR

Wenn sich die Lichtstärke der Szene ändert, passt sich für eine optimale Beleuchtung eine Axis Kamera automatisch an die neuen Lichtverhältnisse an. Für Szenen, die sowohl helle als auch dunkle Bereiche umfassen, wird die WDR-Option (großer Dynamikbereich) empfohlen. Diese Funktion ist standardmäßig aktiviert und eignet sich am besten für Axis Kameras, da sie im Laufe der Zeit nicht angepasst werden muss. Mit WDR kann die Kamera in vielen Fällen kurze Belichtungszeiten in den hellen Teilen der Szene mit langen Belichtungszeiten in den dunklen Bereichen kombinieren. Das daraus resultierende Bild wird in allen Bereichen korrekt belichtet.

Axis bietet mehrere Lösungen für die WDR-Bildtechnologie an:

- > **Forensic WDR** ist eine Kombination aus einer Methode für duale Belichtung und einer Methode zur lokalen Kontrastverstärkung. Es liefert Bilder, die für maximale forensische Verwertbarkeit optimiert sind. Die Technologie nutzt die neueste Generation von Algorithmen zur Bildverarbeitung und verringert effizient Bildrauschen und Artefakte. Forensic WDR eignet sich auch für bewegte Szenen und für Kameras mit extrem hoher Auflösung.
- > **WDR – Dynamic Contrast** nutzt ein Verfahren zur Kontrastverstärkung mit einem relativ begrenzten Dynamikbereich, erzeugt dabei jedoch nur sehr wenige Artefakte. Da nur eine Belichtung verwendet wird, liefert diese Lösung auch dann gute Ergebnisse, wenn sich Objekte schnell durch die Szene bewegen.
- > **WDR** setzt eine Methode für die duale Belichtung ein, um Bilder mit unterschiedlicher Belichtungszeit zusammenzuführen.

Der Dynamikbereich einer Kamera wird in der Regel als dB-Wert angegeben. Die tatsächliche WDR-Leistung lässt sich jedoch nicht so einfach messen, da sie von vielen Faktoren wie der Szenenkomplexität, Bewegungen in der Szene und den Bildverarbeitungskapazitäten der Kamera abhängt. Für Axis hat die Eignung für den forensischen Einsatz und eine hohe Bildqualität eine höhere Priorität als ein hoher dB-Wert. Deshalb kann eine Axis-Kamera mit einem bestimmten Dynamikbereich durchaus eine bessere Leistung aufweisen als eine andere Kamera mit einem höheren dB-Wert laut Datenblatt.

Weitere Informationen zur Belichtungssteuerung und zur WDR-Bildgebung finden Sie im Kapitel .

2.2.2 Lightfinder-Technologie

Durch Überwachungsvideos in Farbe können Personen, Fahrzeuge und Vorfälle deutlich besser identifiziert werden. Kameras mit der Axis Lightfinder-Technologie sind extrem lichtempfindlich.

Sie können auch bei einer Lichtstärke von 0,08 Lux oder weniger noch Farbbilder im Tagmodus erzeugen. Dies wird erreicht durch eine optimale Zusammenstellung von Bildsensor und Objektiv, das Know-how von Axis hinsichtlich der Bildverarbeitung sowie die betriebseigene ASIC-Chip-Entwicklung. Da diese Lightfinder-Bausteine regelmäßig verbessert werden, entwickelt sich auch Lightfinder ständig weiter. Lightfinder 2.0, der auch für Kameras mit einer Auflösung von bis zu 4K geeignet ist, stellt eine schrittweise Änderung dieser Entwicklung dar – mit erhöhter Lichtempfindlichkeit, einer naturgetreueren Farbwiedergabe und individuellen Einstellungen für erfahrene Benutzer.



Links: Scharfes, helles Farbbild von einer Lightfinder 2.0-Kamera, obwohl die Lichtstärke unter der Brücke nur 0,05 Lux betrug. Rechts: Ein Schnappschuss derselben Szene, der manipuliert wurde, um zu visualisieren, wie das menschliche Auge die Szene sehen würde.

2.2.3 Tag/Nacht-Funktionalität

Eine Netzwerk-Kamera mit Tag- und Nachtfunktionalität ist mit einem automatisch schwenkbaren Infrarot-Sperrfilter ausgestattet. Am Tag ist der Filter aktiv, damit die Kamera Farben originalgetreu wiedergeben kann. In der Nacht wird der Filter entfernt, damit die Kamera Nah-Infrarotlicht nutzen und Graustufenbilder in guter Qualität liefern kann. Dies ist eine Möglichkeit, den Anwendungsnutzen einer Netzwerk-Kamera unter schlechten Lichtbedingungen zu erweitern.



Links: Tag-Modus. Rechts: Nacht-Modus.

2.2.4 Integrierte Infrarot-Beleuchtung

Bei schwachem Licht oder völliger Dunkelheit unterstützen die in die Kamera eingebauten Infrarot-LEDs (oder ein separater Infrarotstrahler) die Fähigkeit der Kamera, Graustufenbilder in guter Qualität mit Nah-Infrarotlicht zu liefern. Nah-Infrarotlicht des Mondes, von Straßenlaternen oder Infrarotstrahlern ist für das menschliche Auge nicht sichtbar, der Bildsensor einer Kamera kann es jedoch erkennen.

Die in Axis Kameras eingebauten Infrarot-LEDs können an einen bestimmten Blickwinkel angepasst werden und bei Dunkelheit, einem Ereignis oder bei Bedarf automatisch aktiviert werden.



Links: Schnappschuss im Nacht-Modus ohne Infrarotstrahler (ein wenig Licht fiel durch eine Spalte unter einer Tür in der linken Ecke in den Raum ein). Rechts: Schnappschuss im Nacht-Modus mit Infrarotstrahlern.

2.2.5 OptimizedIR

Axis Kameras mit OptimizedIR sind eine einzigartige und leistungsstarke Kombination aus Kameraintelligenz und ausgereifter LED-Technologie unter Verwendung der modernsten in die Kamera integrierten Infrarotlösungen von Axis. Eine patentierte, auf die Kamera abgestimmte Technologie gewährleistet eine gleichbleibende Beleuchtung im variablen Sichtfeld der Kamera, ein äußerst effizientes Wärmemanagement sowie die Verwendung hochwertiger LEDs mit großer Reichweite. Und dies ist nur ein Beispiel. OptimizedIR wird ständig weiterentwickelt, wobei regelmäßig neue Funktionen hinzugefügt werden.

2.2.6 Objektive mit geringer Blendenzahl

Kameraobjektive mit kürzerer Brennweite haben eine höhere Lichtstärke. Im Allgemeinen ist eine niedrigere Blendenzahl besser für Umgebungen mit schwachem Licht. Dem stehen allerdings eine geringere Schärfentiefe, größere und schwerere Objektive sowie höhere Kosten gegenüber. In bestimmten Beleuchtungssituationen kann eine höhere Blendenzahl von Vorteil sein. Die Lichtempfindlichkeit einer Kamera beruht nicht nur auf ihrem Objektiv, sondern auch auf dem Bildsensor und der Bildverarbeitung. Weitere Einzelheiten zu Objektiven und Bildsensoren entnehmen Sie Kapitel .

2.2.7 Automatische Blendensteuerung

Für Szenen mit wechselnder Lichtstärke wird eine automatisch verstellbare Blende (DC-Blende, P-Blende oder i-CS-Objektiv) empfohlen, um für korrekte Belichtungszeiten zu sorgen. Kameras mit einem P-Blendenobjektiv oder i-CS-Objektiv ermöglichen eine bessere Blendensteuerung für optimale Bildqualität bei allen Lichtbedingungen. Einzelheiten hierzu entnehmen Sie Kapitel .

2.2.8 Die richtige Auflösung

Die Auflösung einer Kamera ergibt sich aus der Anzahl von Pixeln auf dem Bildsensor. Eine Kamera mit einem *Megapixel*-Sensor liefert einen Videostream mit einer Million Pixeln pro Bild oder mehr.

Eine hohe Auflösung ist in der Regel erwünscht. Bei Verwendung eines Weitwinkels bietet eine Kamera mit höherer Auflösung einen größeren Erfassungsbereich. Bei einem engeren Bildwinkel liefert eine Kamera mit höherer Auflösung detailliertere Bilder, sodass Personen und Objekte besser erkannt werden können.

Aber während des anhaltenden Trends der Überwachungsbranche hin zu höheren Auflösungen haben Hersteller in der Regel versucht, die Sensorgröße beizubehalten, um die höheren Kosten eines größeren Sensors zu vermeiden. Dies bedeutet, dass jedes Pixel kleiner sein muss und kleinere Pixel weniger Licht erfassen können. Wenn einfach die Pixelanzahl eines Sensors gleicher Größe

erhöht wird, wird eine bessere Auflösung erzielt, aber das Bild weist möglicherweise auch eine geringere Qualität auf, besonders bei schwachem Licht. Eine Kamera mit einem Sensor von etwa 4 Megapixeln bietet in der Regel ein ausgewogenes Verhältnis zwischen Auflösung und Lichtempfindlichkeit, da die Pixelgröße ausreicht, ohne dass ein größerer, teurerer Sensor verwendet werden muss.

Kameras mit der Unterstützung für HDTV 720p (1280 x 720 Pixel) und HDTV 1080p (1920 x 1080 Pixel), WQHD (2560 x 1440 Pixel) sowie 4K Ultra HD (3840 x 2160 Pixel) und 8K Ultra HD (7680 x 4320 Pixel), mit jeweils etwa 1, 2, 4, 8,5 und 33 Megapixel entsprechen Standards, die eine volle Bildrate, hohe Farbtreue und ein Seitenverhältnis von 16:9 gewährleisten. Weitere Informationen zu Video-Auflösungen finden Sie im Kapitel .

2.2.9 Wärmebildtechnologie

Neben Sonnenlicht, künstlichem Licht und Nah-Infrarotlicht können auch mit Wärmestrahlung Bilder erzeugt werden. Eine Wärmebildkamera benötigt keine Lichtquelle. Stattdessen wird die von jedem Objekt ausgehende Wärmestrahlung über Null Grad Kelvin erfasst.

Mit Wärmebildkameras können Objekte in völliger Dunkelheit, in Rauch oder Nebel oder völlig verdeckt durch Schatten oder einen komplexen Hintergrund erkannt werden. Solche Kameras werden auch durch starken Lichteinfall nicht geblendet. Wärmebild-Netzwerk-Kameras sind ideal für Erkennungsaufgaben geeignet und können als Ergänzung zu konventionellen Kameras die Effizienz eines Überwachungssystems verbessern. Weitere Informationen zu Wärmebildkameras finden Sie im Abschnitt .



Links: Bild einer herkömmlichen Kamera in einer nebligen Szene. Rechts: Bild einer Wärmebildkamera in der gleichen nebligen Szene.

2.2.10 Bildstabilisierung

Eine an einer exponierten Stelle montierte Überwachungskamera, z. B. an einem hohen Masten oder einem Straßenschild in der Nähe einer belebten Straße, kann durch Wind oder Straßenverkehr geschüttelt werden. Dadurch kann das Video unscharf werden, insbesondere dann, wenn ein leistungsstarkes Zoom-Objektiv verwendet wird.

Echtzeit-Bildstabilisierungsverfahren verbessern die Videoqualität, indem sie das Videosignal weniger anfällig für Kameravibrationen machen. Diese Flexibilität ermöglicht vielseitigere Installations- und Montagemöglichkeiten für Kameras, auch wenn Kameravibrationen nach Möglichkeit vermieden werden sollten. Da das stabilisierte Video verhältnismäßig weniger Bewegung enthält, sind auch weniger Bandbreite und Speicherressourcen erforderlich als bei wackeligen Aufnahmen.

- > **Optische Bildstabilisierung** (OIS) arbeitet meist mit Gyroskopen oder Beschleunigungsmessern, die die Kameravibrationen erkennen und messen. Dieses Verfahren ist besonders hilfreich bei großen Brennweiten. Es funktioniert auch bei schlechten Lichtverhältnissen gut. Der größte Nachteil einer optischen Lösung ist der Preis.
- > **Elektronische Bildstabilisierung** (EIS) basiert auf Algorithmen zur Modellierung der Kamerabewegung, die danach zur Korrektur der Bilder verwendet werden. Dieses Verfahren ist kostengünstig, kann aber nicht immer zwischen physikalischen Bewegungen durch Vibrationen und wahrgenommenen Bewegungen durch bewegte Objekte vor der Kamera unterscheiden.
- > **Die elektronische Bildstabilisierung mit Gyro**, eine Axis Funktion, umfasst fortschrittliche Gyroskope und optimierte Algorithmen, die zusammenarbeiten, um ein robustes, zuverlässiges System zu gewährleisten. Sie deckt ein breites Band an Vibrationsfrequenzen ab und kommt mit hohen und niedrigen Amplituden zurecht. Das System funktioniert selbst bei schlechten Lichtverhältnissen sehr gut, da es für seine Bewegungsberechnungen Gyroskopinformationen und keine Videoinhalte verwendet. Aus demselben Grund kann das System zwischen wahrgenommener Bewegung und physisch verursachten Vibrationen unterscheiden.

2.3 Kamerafunktionen für einfache Installation

Axis Kameras sind mit Funktionen ausgestattet, die die Installation und Nutzung erleichtern. Weniger Installationsfehler sorgen für mehr Zuverlässigkeit.

2.3.1 Geeignet für den Außeneinsatz

Für den Außenbereich geeignete Produkte stehen sofort für die Installation zum Außeneinsatz bereit. Es ist kein separates Gehäuse erforderlich, und die Produkte werden mit unverlierbaren Schrauben geliefert, die nicht aus den Schraublöchern herausfallen können. Die Produkte sind so konzipiert, dass sie trotz großer Temperaturunterschiede funktionieren und gegen Staub, Regen und

Schnee geschützt sind. Einige davon erfüllen sogar militärische Betriebsanforderungen für raue Witterungsbedingungen.

2.3.2 Fabrikseitige Fokussierung

Um die Installation schneller und einfacher zu machen, werden Axis Kameras mit fester Brennweite bereits in der Fabrik fokussiert, sodass während der Installation nicht mehr manuell fokussiert werden muss. Dies ist möglich, weil Kameras mit fester Brennweite und weitem oder mittlerem Sichtfeld in der Regel eine große Tiefenschärfe haben (der Bereich, in dem sowohl nahe als auch ferne Objekte scharf abgebildet werden). Weitere Einzelheiten zu Brennweite, Blendenzahlen und Schärfentiefe finden Sie in Kapitel .

2.3.3 Fernsteuerbare Fokussier- und Zoomfunktionen

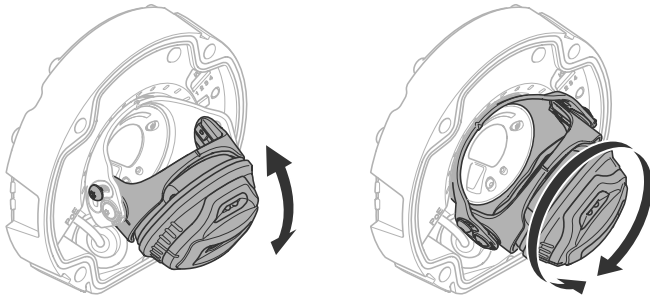
Eine Variofokus-Kamera mit Remote-Fokus und -Zoom macht eine manuelle Fokussierung und Sichtfeldeinstellung vor Ort überflüssig, wenn die Kamera installiert wird. Dank des Objektivmotors der Kamera ist dies über einen an das Netzwerk angeschlossenen Rechner per Ferneinstellung möglich.

2.3.4 Feineinstellung des Auflagemaßes

Eine Variofokus-Kamera mit CS-Anschluss und Feineinstellung des Auflagemaßes gestattet die Feineinstellung der Fokussierung über einen Rechner, indem kleine Anpassungen an der Position des Bildsensors vorgenommen werden. Diese Funktion gibt es auch für optionale Objektive.

2.3.5 3-Achsen-Kamerawinkelanpassung

Eine Dome-Kamera von Axis verfügt über eine 3-Achsen-Kamerawinkeleinstellung, mit der die Objektivereinheit (bestehend aus Objektiv und Bildsensor) geschwenkt, geneigt und gedreht werden kann. Dadurch ist eine Kameramontage an der Wand oder Decke möglich. Die Benutzer können dann problemlos Kamerarichtung und Bildausrichtung einstellen. Dank der flexiblen Kameraeinstellung und der Möglichkeit zum Drehen des Bildes über die Weboberfläche der Kamera können die Benutzer vertikal ausgerichtete Videostreams beziehen (Corridor Format).



3-Achsen-Kamerawinkelanpassung

2.3.6 Korridor-Format

Das Korridor-Format ermöglicht vertikal ausgerichtete Videoaufnahmen von unbeweglichen Kameras. Das vertikale Format optimiert die Abdeckung von Bereichen wie Korridoren, Fluren und Gängen und maximiert die Bildqualität bei gleichzeitiger Minimierung von Bandbreiten- und Speicheranforderungen. Dadurch können beispielsweise HDTV-Netzwerk-Kameras Bilder im Seitenverhältnis 9:16 liefern. Mit einer Dome-Kamera wird dies erreicht, indem zunächst das Objektiv um 90° gedreht wird (bei Bullet- oder Box-Kameras wird die gesamte Kamera gedreht) und dann das Videobild über die Webseite der Kamera wieder um 90° zurückgedreht wird.

2.3.7 Bild ausrichten

„Bild ausrichten“ ist ein Werkzeug zur Bildverarbeitung, das die digitale Korrektur der Bilddrehung bei einer leichten mechanischen Abweichung von der Längsachse des Bildes ermöglicht. Ziel ist es, das Bild am Horizont auszurichten.

2.3.8 Pixelzähler

Der Axis Pixelzähler ist ein visuelles Hilfsmittel in Form eines Rahmens mit entsprechendem Zähler zur Anzeige der Rahmenbreite und -höhe. Mit dem Pixelzähler können Sie sicherstellen, dass die Videoauflösung hoch genug ist, um zum Beispiel eine Gesichtsidentifizierung zu ermöglichen. Mit ihm kann auch geprüft werden, ob die Auflösung eines Objekts behördlichen Vorgaben oder den Kundenanforderungen entspricht. Weitere Informationen zu empfohlenen Pixeldichten für unterschiedliche Überwachungszwecke finden Sie in Kapitel .



Axis Pixelzähler, der die Pixelauflösung einer Fläche anzeigt.

2.4 Verschiedene Typen von Netzwerk-Kameras

Netzwerk-Kameras können für den reinen Einsatz in Innenräumen oder für den Innen- und Außeneinsatz geeignet sein. Eine für den Außenbereich geeignete Kamera wird mit einem äußeren Schutzgehäuse geliefert. Weitere Informationen zum Schutz finden Sie im Abschnitt .

2.4.1 Bullet-Kameras



Eine Bullet-Kamera ist eine Überwachungskamera mit einem langgestreckten, zylindrischen Gehäuse, das an die Form einer Patrone erinnert. Dank ihrer Bauform bietet sie Platz für ein größeres Zoomobjektiv und eignet sich dadurch ideal für die Überwachung über große Entfernungen sowie für hochauflösende Videoaufnahmen. Ein größeres Objektiv ermöglicht zudem den Einsatz von Kameras, die selbst bei extrem schlechten Lichtverhältnissen hochwertige Bilder liefern.

Bullet-Kameras eignen sich sowohl für den Außen- als auch für den Innenbereich. Zu den gängigen Anwendungsfällen zählen Verkehrsüberwachung, Parkplätze, Flughäfen, Einzelhandelsflächen und Lagerhallen. Sie lassen sich einfach mit einer Wandhalterung oder Deckenhalterung installieren und können schnell ausgerichtet werden. Bullet-Kameras verfügen meist über IR-Strahler für die Nachtsicht. Dank ihrer auffälligen Bauform können Bullet-Kameras bereits durch ihre sichtbare Präsenz zur Abschreckung potenzieller Straftäter beitragen.

2.4.2 Box-Kameras



Eine Box-Kamera ist eine Überwachungskamera mit einem quadratischen oder rechteckigen Gehäuse. Im Vergleich zu Bullet-Kameras wirken Box-Kameras klassischer und auffälliger. Dadurch können sie potenzielle Straftäter zusätzlich abschrecken. Box-Kameras sind als Modelle für den Innen- und Außenbereich erhältlich. Viele Innenraummodelle können jedoch mit einem zusätzlichen Schutzgehäuse auch im Außenbereich eingesetzt werden.

Typische Einsatzbereiche sind die Städteüberwachung, der Verkehr, der Einzelhandel, kritische Infrastrukturen, Flughäfen und Behörden. Ihre hochauflösenden Videoaufnahmen, fortschrittlichen Analysefunktionen und die hohe Leistungsfähigkeit bei schlechten Lichtverhältnissen machen sie zur idealen Wahl für die Überwachung weitläufiger Bereiche und den Perimeterschutz.

Box-Kameras werden in der Regel an Halterungen, Auslegern oder kundenspezifischen Gehäusen montiert. Dadurch lassen sie sich einfach positionieren und ausrichten, um den gewünschten Überwachungsbereich optimal abzudecken. Viele Box-Kameras sind mit Wechselobjektiven kompatibel und bieten Ihnen dadurch die Flexibilität, das passende Objektiv für Ihre Anwendung auszuwählen.

2.4.3 Blockkameras



Eine Blockkamera ist eine kompakte Sicherheitskamera, die in der Regel aus einem integrierten Objektiv und einem hochwertigen Bildsensor besteht, die in einem quadratischen oder rechteckigen, blockförmigen Gerät untergebracht sind. Diese Kameras sind für den Einbau in

Standard- oder kundenspezifische Gehäuse konzipiert und bieten eine hohe Vielseitigkeit. Dank ihrer fernsteuerbaren Zoom- und Fokussierfunktionen, ihrer ausgezeichneten Bildqualität und ihrer Flexibilität beim Einbau in beengte Räume oder maßgeschneiderte Gehäuse eignen sie sich ideal für verschiedene Umgebungen, in denen eine leistungsstarke Kamera erforderlich ist.

2.4.4 Dome-Kameras



Dome-Kameras bestehen aus einer unbeweglichen Kamera, die in einem kleinen, kuppelförmigen Gehäuse vorinstalliert ist. Der Hauptvorteil dieser Kamera ist das diskrete, unauffällige Design. Darüber hinaus können Personen im Sichtfeld der Kamera nur schwer erkennen, in welche Richtung die Kamera ausgerichtet ist. Es gibt eine große Auswahl an Zubehör, das eine noch unauffälligere Installation ermöglicht, z. B. schwarze Gehäuse, Einbaumontagen und rauchfarbene Kuppeln. Die Dome-Kamera ist außerdem besser gegen Manipulation geschützt als andere unbeweglichen Kameras. Sie ist mit einem unbeweglichen, Vario-Fokus- oder motorbetriebenen Zoom-Objektiv ausgestattet.

Dome-Kameras bieten verschiedene Schutztypen und -stufen, zum Beispiel Vandalismus- und Staubschutz sowie IP66, IP67 und NEMA 4X für die Installation im Außenbereich. Ein externes Gehäuse ist nicht erforderlich. Diese Kameras werden in der Regel an einer Wand, einer Decke oder einem Mast befestigt.

2.4.4.1 Onboard-Kameras



Onboard-Kameras sind für die Videosicherheit im Straßen- und Schienenverkehr konzipiert, einschließlich Schienenfahrzeugen und Bussen. Sie sind vibrationsfest und verfügen über spezielle Bildprofile für Datenaustausch-Szenarien, die eine hohe Bildqualität in anspruchsvollen Umgebungen erfordern. Die Onboard-Kameras von Axis erfüllen strenge Industriestandards und sind für den Einsatz in Fahrzeugen zertifiziert. Sie sind so konstruiert, dass sie

Temperaturschwankungen standhalten und unter unterschiedlichsten Bedingungen zuverlässig funktionieren.

Das Kameraangebot von Axis enthält eine Reihe robuster Kameras für diverse Onboard-Umgebungen. Zu den verfügbaren Optionen gehören Panorama-Fischaugenkameras für eine breite Abdeckung, vielseitige Fixed-Dome-Kameras sowie flexible modulare Kameras.



Eine Onboard-Dome-Kamera, die in der Decke eines Busses montiert ist.

2.4.4.2 Panorama-Kameras

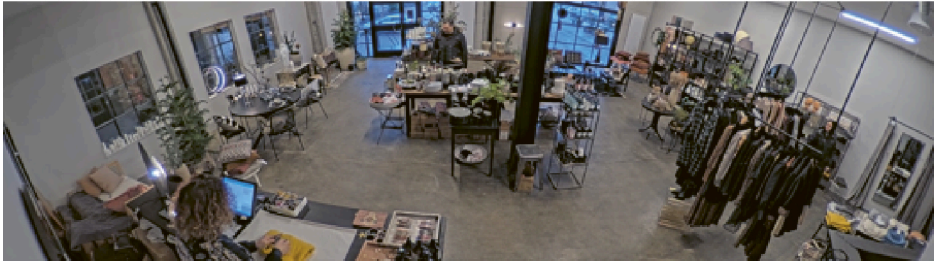


Panorama-Kameras: Einzelsensor-, Multisensor-, Mehrrichtungskamera und eine Lösung, die eine Mehrrichtungskamera mit einer PTZ-Kamera kombiniert.

Eine Panorama-Kamera ist eine Dome Kamera, die einen großen Bereich abdeckt und gleichzeitig eine ausgezeichnete Bilddetailgenauigkeit ermöglicht – alles in einer effizienten Ein-Kamera-Installation. Die Kamera kann eine Einzelsensor-, Multisensor- oder eine multidirektionale Panorama-Kamera sein.

Eine Einzelsensor-Panorama-Kamera verfügt über ein Weitwinkelobjektiv mit 360° im Fischaugenformat. Das Format kann – in der Live-Ansicht oder auf aufgezeichnetem Material – in

verschiedene Rechteckansichten umgewandelt werden, darunter in das Panorama-, das Doppelpanorama- oder das Vierfach-Format (mit einer Simulation vier verschiedener Kameras).



Eine Einzelsensor-Panorama-Kamera bietet mehrere Formate wie 360°-Übersicht, Vierfach-Ansicht und Panorama.

Eine Multisensor-Kamera bietet nahtlose 180°-Abdeckung mit großartiger Detailschärfe und minimaler Verzerrung. Sie verfügt über mehrere Sensoren und verbindet große Abdeckung mit hoher Bildqualität und hoher Pixeldichte. Sie verwendet eine universale Weißabgleichseinstellung und eine synchronisierte Belichtung für alle Sensoren. Durch das nahtlos geheftete Bild eliminiert eine Multisensor-Kamera auch tote Winkel.



180°-Ansicht mit Multisensorkamera.

Eine Mehrrichtungs-Kamera mit 360°-Abdeckung ist eine Panorama-Kamera mit einzeln einstellbaren Kameraköpfen. Sie eignet sich ideal für z. B. Einzelhandelsgeschäfte, Flure und Lagerhäuser.

Eine Lösung, die eine Mehrrichtungs-Panoramakamera mit einer PTZ-Kamera kombiniert, ist z. B. bei Kreuzungen besonders nützlich.

2.4.5 Modulare Kameras



Modulare Kameras enthalten Hauptgeräte, Sensoreinheiten und Kabel.

Modulare Kameras von Axis sind auf Flexibilität, Skalierbarkeit und Effizienz ausgelegt. Dank austauschbarer Komponenten, flexibler Designs und nachhaltiger Lösungen fügen sie sich harmonisch in die Umgebung ein und können praktisch überall eingesetzt werden. Die Sensoreinheiten eignen sich für die Installation in engen Räumen. Sie können in Busse und Polizeifahrzeuge eingebaut oder in Geräte wie Geldautomaten integriert werden und ermöglichen, in Ausgangsbereichen auf Augenhöhe platziert, eine optimale Gesichtserfassung. Sie eignen sich hervorragend für äußerst diskrete Videosicherheit und Analysefunktionen. Diese Kameras sind vielseitig und eignen sich für eine Vielzahl von Anforderungen an die Videosicherheit.

Modulare Kameras sind kostengünstig, wenn Sie mehrere Kameras in einem Bereich installieren müssen. Haupteinheiten sind mit einem oder vier Kanälen sowie eine Haupteinheit mit vier Kanälen für bis zu vier Sensoreinheiten verfügbar. Dank der maximalen Kabellängen von bis zu 30 m kann eine Haupteinheit mit vier Sensoreinheiten größere und kleinere Bereiche abdecken. Vier

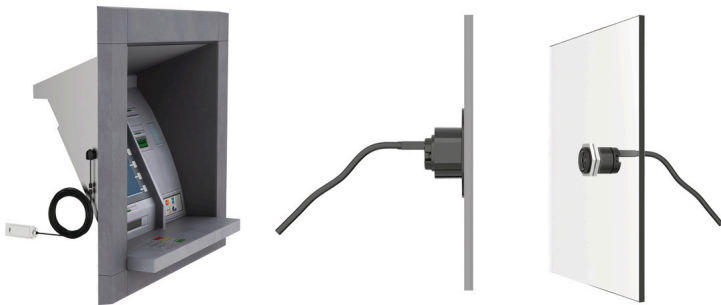
angeschlossene Sensoreinheiten ermöglichen zudem gleichzeitiges, multiples Videostreaming und Streaming in der Vierfachansicht mit nur einer IP-Adresse. Eine Haupteinheit benötigt unabhängig davon, ob sie einen oder vier Videokanäle unterstützt, VMS-Einzellizenz und einen Switch-Port.



Die AXIS F Modular Camera Series bietet eine Reihe von modularen Hochleistungskameras für den Innen- und Außenbereich sowie Onboard-Umgebungen. Die Serie umfasst robuste Haupteinheiten, UL-zertifizierte Barebone-Haupteinheiten, mehrere Kabeloptionen und Sensoreinheiten für eine breite Palette von Anwendungen.



Videostream in der Vierfachansicht von einer in einem Bus installierten modularen Kamera mit vier Kanälen.



Links: eine modulare Kamera mit Pinhole-Objektiv in einem Geldautomaten. Rechts: ein an einer Wand montierter und ein an einer Glasscheibe montierter Sensor.

Sensoreinheiten sind in unterschiedlichen Formvarianten und mit verschiedenen Objektivarten erhältlich, z. B. in der Standardausführung, mit Vario-Fokus oder als Pinhole-Objektiv.



Das für die Montage in der Nähe von Gebäudeausgängen konzipierte Gehäuse mit Höhenleiste ermöglicht eine äußerst diskrete Installation der Pinhole-Sensoren. Die Kamera ist so positioniert, dass sie direkt in das Gesicht einer Person gerichtet ist und so eine zuverlässige Identifizierung bietet.

2.4.6 PTZ-Kameras

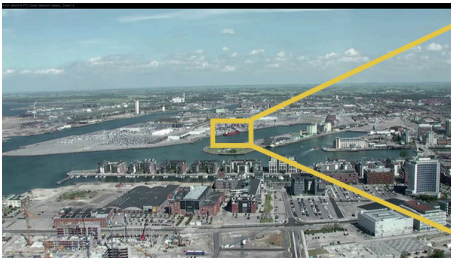


PTZ-Kameramodelle (von links nach rechts): mit HDTV 1080p-Auflösung mit Sharpdome-Technologie, aktiver Kühlung, einer kombinierten Lösung aus Multisensor- und PTZ-Kamera und (ganz rechts) einer Kombination einer visuellen und einer Wärmebildkamera in einem Gerät.

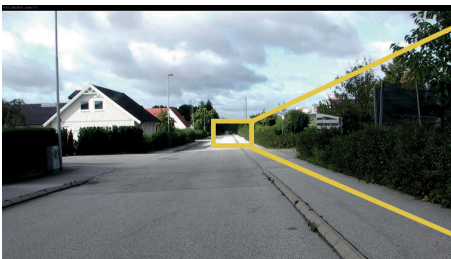
Eine PTZ-Kamera verfügt über Funktionen zum Schwenken, Neigen und Zoomen (mit manueller oder automatischer Steuerung), die einen großen Überwachungsbereich und eine hohe Detailgenauigkeit beim Zoomen ermöglichen. Axis PTZ-Kameras lassen sich in der Regel um 360°

schwenken, um 180° oder 220° neigen und sind häufig mit einem Zoom-Objektiv ausgestattet. Ein echtes Zoomobjektiv bietet einen optischen Zoom, der die Bildauflösung beibehält – im Gegensatz zu einem digitalen Zoom, der bei der Vergrößerung des Bildes zu Qualitätsverlusten führt.

Im Rahmen der Live-Überwachung können PTZ-Kameras zum Verfolgen von Objekten eingesetzt werden und zur weiteren Objektprüfung heranzoomen. Beim Betrieb ohne Personal können PTZ-Kameras dank automatischer Rundgangüberwachung verschiedene Bereiche einer Szene überwachen. Im Guard-Tour-Modus lässt sich mit einer PTZ-Kamera ein Bereich abdecken, für den sonst viele unbewegliche Kameras erforderlich wären.



Die Weitwinkelansicht (links) und die herangezoomte Ansicht (rechts) mit einer HDTV 1080p PTZ-Kamera: Der Text auf dem Frachtschiff ist noch aus 1,6 km Entfernung lesbar.



Die Weitwinkelansicht (links) und die herangezoomte Ansicht (rechts) mit einer HDTV 1080p PTZ-Kamera: Das Kennzeichen ist noch in einer Entfernung von 275 m lesbar.

Axis PTZ-Kameras können mit einer Vielzahl intelligenter Funktionen ausgestattet werden, z. B.:

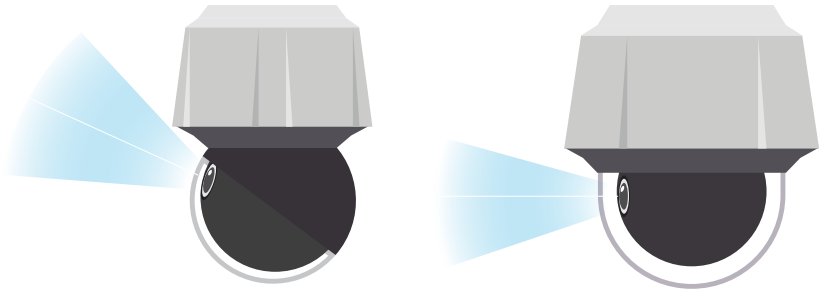
- > **Guard-Tour (voreingestellte Positionen).** Bei PTZ-Kameras können in der Regel bis zu 100 voreingestellte Positionen programmiert werden. Sind diese Positionen in der Kamera eingestellt, kann der Bediener durch einfaches Auswählen schnell von einer Position zur anderen schalten. Im Guard-Tour-Modus kann die Kamera so programmiert werden, dass sie automatisch in einer bestimmten oder zufälligen Reihenfolge von einer voreingestellten Position zur nächsten fährt. Normalerweise können bis zu 20 Überwachungsrundgänge konfiguriert und zu verschiedenen Tageszeiten aktiviert werden.

- > **Guard-Tour (aufgezeichnet).** Die Funktion von PTZ-Kameras zum Konfigurieren und automatischen Abspeichern der Rundgangüberwachung ermöglicht das einfache Einrichten eines automatischen Kamerarundgangs mit einem Joystick oder einem ähnlichen Gerät. Dabei werden die Schwenk-/Neige-/Zoombewegungen des Bedieners sowie die Verweildauer an den einzelnen Positionen aufgezeichnet. Der aufgezeichnete Rundgang kann dann per Knopfdruck oder zu festgelegten Zeitpunkten gestartet werden.
- > **Autotracking.** Diese Analyseanwendung kann eine Person oder ein Fahrzeug in Bewegung automatisch erfassen und in dem von der Kamera abgedeckten Bereich verfolgen. Auto-Tracking ist besonders bei unbemannter Videosicherheit in Situationen hilfreich, in denen die Anwesenheit von Personen oder Fahrzeugen besondere Aufmerksamkeit erfordert. Diese Funktion senkt die Kosten für ein Überwachungssystem deutlich, da für die Abdeckung einer Szene weniger Kameras erforderlich sind. Sie steigert auch die Effektivität der Lösung, da die PTZ-Kamera die Bereiche einer Szene aufzuzeichnen kann, in denen Aktivität verzeichnet wird.
- > **AXIS Radar Autotracking for PTZ.** Diese Softwareanwendung erkennt anhand der Bewegungsdaten von Axis Radargeräten an einem Standort Objekte von Interesse und steuert automatisch die Richtung und den Zoom von einer oder mehreren PTZ-Kameras. Das Radargerät dient als Gegenstück der PTZ-Kamera. Die Anwendung ermöglicht die visuelle Bestätigung erfasster Objekte auch außerhalb des aktuellen Sichtfelds der Kamera. AXIS Radar Autotracking for PTZ minimiert außerdem den Bedarf an manueller Kamerasteuerung mittels Joystick.
- > **AXIS Perimeter Defender PTZ Autotracking.** Auf einer PTZ-Kamera installiert, wird diese von einer fest ausgerichteten Wärmebild- oder Lichtbildkamera, auf der AXIS Perimeter Defender ausgeführt wird, gesteuert. Sobald diese in ihrem fest definierten Erfassungsfeld ein alarmauslösendes Objekt erfasst, lenkt sie die PTZ-Kamera für automatische Nahaufnahmen auf das Objekt. Die PTZ-Kamera passt die Zoomstufe automatisch so an, dass alle Alarmobjekte im Blickfeld bleiben, einschließlich neuer Objekte, die im Erfassungsbereich der festen Kamera auftauchen.
- > **Advanced/Active Gatekeeper** Mit Advanced Gatekeeper kann die PTZ-Kamera bei Erkennung von Bewegung in einem vorab definierten Bereich an eine voreingestellte Position schwenken und dann nach einem festgelegten Zeitraum wieder in die Ausgangsposition zurückkehren. Wenn diese Funktion mit der Möglichkeit zur weiteren Verfolgung des erfassten Objekts kombiniert wird, heißt sie Active Gatekeeper.

2.4.6.1 Sharpdome-Technologie

Mit der Sharpdome-Technologie von Axis ausgestattete PTZ-Kameras können Bereiche oberhalb ihres Horizonts erfassen. Aufgrund der innovativen Mechanik der Sharpdome-Kameras rotiert die

gesamte Kuppel, während sich das Objektiv einer herkömmlichen Dome-Kamera nur innerhalb der Kuppel dreht. Dank dieser Mechanik, der Platzierung des Kameramoduls und dem einzigartigen Design der Dome-Kamera für den Außenbereich sind in sämtlichen Schwenk- und Neigepositionen die gleiche optimale Bildschärfe und absolute Szenentreue gewährleistet. Auf diese Weise werden Objekte erkannt, die sich um bis zu 20° über dem Kamerahorizont befinden.



Eine Kamera mit Sharpdome (links) und eine herkömmliche Dome-Kamera (rechts)

Die Sharpdome-Technologie beinhaltet die Speed-Dry-Funktion, die auch bei Regen scharfe Bilder liefert. Mit der Speed-Dry-Funktion wird die Kuppel mit raschen Bewegungen in verschiedene Richtungen gedreht. So lassen sich Wassertropfen von der Außenseite der Kuppel entfernen, die die Bilderfassung beeinträchtigen.



Zwei Momentaufnahmen derselben Szene bei Regen: vor der Rotationsbewegung (links) und nach Entfernen des Wassers (rechts) mithilfe der Speed-Dry-Funktion

2.4.7 Wärmebildkameras



Wärmebildkameras als Bullet (links) und als festes Gehäuse auf einer Positionierungseinheit (Mitte). Die bispektrale PTZ-Kamera (rechts), die eine visuelle und eine Wärmebildkamera in einem Gerät kombiniert.

Wärmebildkameras erfassen die von allen Objekten aufgrund ihrer Temperatur ausgesandte Infrarotstrahlung. Mit der Fähigkeit, kleine Temperaturunterschiede zu erfassen und in ein visuelles Bild umzuwandeln, können diese Kameras Personen und Fahrzeuge auf große Entfernungen erkennen. Sie funktionieren selbst bei völliger Dunkelheit und unabhängig von den Lichtverhältnissen, Tarnung, Vegetation, widrigen Wetterbedingungen oder anderen Umständen, unter denen eine herkömmliche Kamera an ihre Grenzen stößt.

Wärmebildkameras werden im Perimeterschutz eingesetzt, um potenzielle Aktivitäten bereits in einem frühen Stadium zu erkennen – deutlich bevor optische Kameras eine zuverlässige Erfassung ermöglichen. Durch den Einsatz von Edge-basierter Videoanalyse löst die Kamera automatisch definierte Reaktionsprotokolle aus: Sie aktiviert Lautsprecher zur aktiven Abschreckung, sendet Alarmer an das Sicherheitspersonal und steuert PTZ-Kameras, um identifizierbare Aufnahmen zu erfassen. Da die Wärmebildtechnik eine kontrastreiche Erkennung ermöglicht, ohne personenbezogene Identitäten aufzulösen, eignet sie sich besonders für die Überwachung in datenschutzsensiblen Bereichen. Wärmebildkameras können zudem Temperaturen in der Industrie überwachen und Wärmeverluste an Gebäuden erkennen oder feststellen, ob ein Fahrzeug kürzlich genutzt wurde.

Bispektralkameras vereinen Wärmebildtechnik und hochauflösende visuelle Bildgebung in einem einzigen Gerät. Sie erkennen Wärmequellen und ermöglichen eine zuverlässige visuelle Erfassung auch bei schlechten Lichtverhältnissen, widrigen Wetterbedingungen, Rauch und Nebel. Dadurch können die Einsatzkräfte Vorfälle genauer einschätzen, Fehlalarme reduzieren und effizienter reagieren.

Einige Bispektralkameras bieten eine Fusion von Wärmebildern und visuellen Bildern – eine fortschrittliche Technologie, bei der der Wärmebild-Stream der Kamera mit dem visuellen Bild-Stream der Kamera integriert wird, wodurch ein fusioniertes visuelles Ergebnis entsteht. Dieser

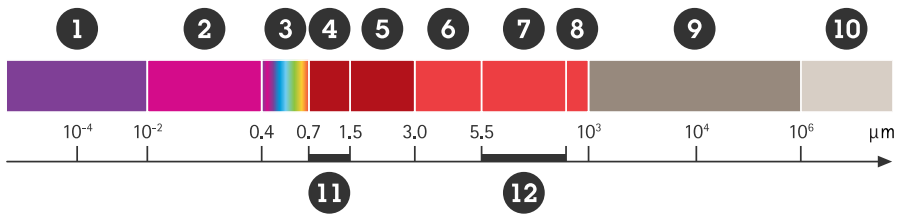
Vorgang umfasst die präzise Ausrichtung der beiden Videostreams, wodurch sichergestellt wird, dass die im Infrarotspektrum detektierten Objekte genau mit denen im sichtbaren Lichtspektrum übereinstimmen. Durch die Zusammenführung dieser Streams entsteht eine einheitliche visuelle Ansicht, die individuell angepasst werden kann, um bestimmte Elemente oder Datenpunkte hervorzuheben.



Zusammengeführtes Bild einer bispektralen Kamera mit Fusion von Wärmebild- und optischem Bild.

Eine Wärmebildkamera benötigt eine Spezialoptik, da normales Glas die Wärmestrahlung behindern würde. Wie viel oder aus welcher Entfernung eine Wärmebildkamera „sehen“ oder erkennen kann, ist abhängig vom Objektiv. Ein Weitwinkelobjektiv bietet ein größeres Sichtfeld, jedoch eine kürzere Erkennungsreichweite als ein Teleobjektiv. Dieses ermöglicht eine größere Erkennungsreichweite, allerdings bei einem kleineren Sichtfeld.

Eine Wärmebildkamera benötigt auch einen speziellen Bildsensor. Bildsensoren lassen sich in zwei Typen unterteilen: gekühlte und ungekühlte. Gekühlte Wärmebildsensoren liefern zwar eine außergewöhnlich hohe Bildqualität, sind jedoch groß, kostspielig sowie energie- und wartungsintensiv. Daher kommen sie hauptsächlich in spezialisierten militärischen Anwendungen zum Einsatz. Ungekühlte Wärmebildsensoren hingegen sind kompakt, kostengünstig und ideal für den Einsatz im Sicherheitsbereich. Sie basieren häufig auf der Mikrobolometer-Technologie. Die Wärmebildkameras von Axis verwenden ungekühlte Sensoren, die im langwelligen Infrarotbereich von 8 bis 14 Mikrometer (μm) betrieben werden.



Das Spektrum der elektromagnetischen Strahlung, einschließlich des langwelligen Infrarot-Bereichs (7).

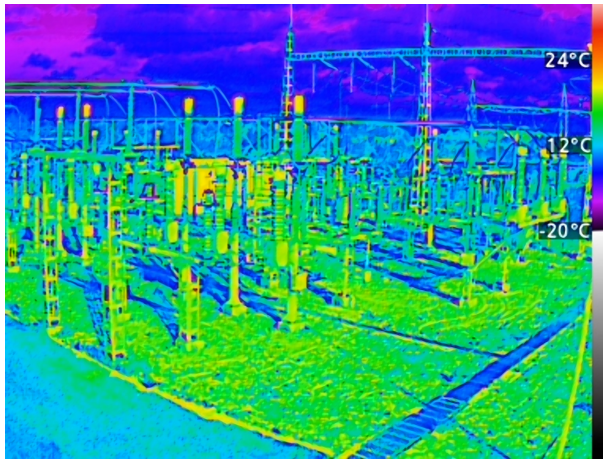
1. Röntgenstrahlen
2. UV-Licht
3. Sichtbares Licht
4. Nah-Infrarotstrahlung (NIR) (ca. 0,75 bis 1,4 μm)
5. Kurzwellige Infrarotstrahlung (SWIR) (1,4 bis 3 μm)
6. Mittlere Infrarotstrahlung (MWIR) (3 bis 5 μm)
7. Langwellige Infrarotstrahlung (LWIR) (8 bis 14 μm) – von Axis Wärmebildkameras verwendet
8. Fernes Infrarot (FIR) (ca. 15 bis 1.000 μm)
9. Mikrowellenstrahlung
10. Radio-/TV-Wellenlängen
11. IR-Beleuchtung
12. Axis Wärmebildkameras

Die Fähigkeit eines Wärmebildsensors, sehr kleine Unterschiede in der Wärmestrahlung zu erfassen, kann durch seinen NETD-Wert (Noise Equivalent Temperature Difference) gekennzeichnet sein. Je kleiner der NETD-Wert, desto besser ist der Sensor. Kameras sollten aber nicht nur durch einen Vergleich ihrer NETD-Spezifikationen bewertet werden, da es kein standardisiertes Messprotokoll gibt.

Produkte und Technologien, die sowohl für militärische als auch für kommerzielle Zwecke verwendet werden können, werden als doppelverwendungsfähige Güter bezeichnet. Der Export solcher Gegenstände ist im internationalen Wassenaar-Abkommen von 1996 geregelt. Mit diesem Abkommen soll unter anderem die Transparenz und die größere Verantwortung für den Vertrieb konventioneller Produkte und Technologien sowie von Gebrauchsartikeln und -technologien gefördert werden. Eine für den Export freigegebene Wärmebildkamera darf die maximale Bildrate von 9 Bildern pro Sekunde (Bilder/s) nicht überschreiten. Wärmebildkameras mit einer Bildrate von bis zu 60 Bildern pro Sekunde können in den meisten der 42 Länder des Wassenaar-Arrangement verkauft werden, unter der Bedingung, dass der Käufer registriert und rückverfolgbar ist und dass der Händler alle landesspezifischen Exportanforderungen einschließlich der Lizenz oder der

LizenzAusnahmeregelung erfüllt. Wärmebildkameras dürfen nicht in Länder verkauft werden, gegen die ein Embargo oder Sanktionen verhängt wurden.

2.4.7.1 Temperaturmesskameras



Aufnahme einer Wärmebildkamera, bei der unterschiedliche Temperaturen mithilfe einer Farbpalette dargestellt werden.

Eine thermometrische Kamera ist eine Wärmebildkamera, mit der sich durch Überwachung von Objekten oder Vorgängen feststellen lässt, ob die Temperatur einen benutzerdefinierten Grenzwert über- oder unterschreitet. Wärmebildkameras werden zur Temperaturüberwachung in Kraftwerken, der Energieinfrastruktur, brandgefährdeten Bereichen und industriellen Anlagen eingesetzt. Die Wärmebildtechnik hilft, potenzielle Ausfälle frühzeitig zu erkennen, Problemstellen zu lokalisieren und die Wirksamkeit von Isolierungen zu beurteilen – noch bevor Schäden sichtbar werden oder zu einem Ausfall von Anlagen führen. Dazu gehört es, überhitzte Bauteile, verstopfte Rohrleitungen oder lockere elektrische Verbindungen zu erkennen, bevor diese zu Schäden, Betriebsausfällen oder Bränden führen.

2.4.8 Explosionsgeschützte Kameras



Kameras mit Explosionsschutz.

Links und Mitte: Für die Gefahrenbereiche der Zone/Division 1 entwickelte und zertifizierte unbewegliche und PTZ-Kameras.

Rechts: Für die weniger brennbaren Bereiche der Zone/Division 2 in Gefahrenbereichen ausgelegte und zertifizierte unbewegliche Kameras.

Kameras mit Explosionsschutz eignen sich ideal für Einsätze in den Bereichen Gesundheit und Sicherheit sowie für einen effizienten Betrieb. Damit lassen sich Abläufe und Prozesse per Fernzugriff auf die Messgeräte und Sensoren des Standorts überwachen und die Lage bei Bedarf visuell überprüfen. Sie können zur Effizienzsteigerung, Aufrechterhaltung der maximale Betriebsfähigkeit und Maximierung der Betriebszeit beitragen. Kameras, die in Gefahrengeländen eingesetzt werden, können in ein bereits vorhandenes System von Sensoren und Kameras für sichere Bereiche in einem bestehenden Netzwerk integriert werden. Thermografische Kameras können potenzielle Überhitzungen von Geräten überwachen. Damit können fundierte Entscheidungen über den laufenden Prozess getroffen werden, um die Produktion so effizient wie möglich in Betrieb zu halten.

Mithilfe von Kameras mit Explosionsschutz können Sie die Sicherheit von Mitarbeitenden erhöhen und die unnötige Gefährdung von Menschen in Gefahrenbereichen auf ein Minimum reduzieren. Analysefunktionen können zur Überwachung der Verwendung von persönlicher Schutzausrüstung wie z. B. Schutzhelmen, oder zur Erkennung von Rauch oder Feuer in potenziell brennbaren Umgebungen eingesetzt werden.



Typische Branchen für den Einsatz explosionsgeschützter Geräte sind die verarbeitende Industrie, Öl- und -Gasindustrie und Getreideumschlag und -lagerung. Gefahrenbereiche sind jedoch auch in einer Vielzahl anderer Branchen wie in der chemischen und pharmazeutischen Produktion, im Bergbau sowie in der Wasser- und Abfallindustrie zu finden.

Explosionsgeschützte Netzwerk-Kameras bieten gegenüber Analogmodellen viele Vorteile. Die wichtigsten sind integrierte Intelligenz, Analysefunktionen, Möglichkeiten zur Aufzeichnung und Datenspeicherung, ausgezeichnete Bildqualität und eine moderne, zukunftssichere Kameratechnologie.

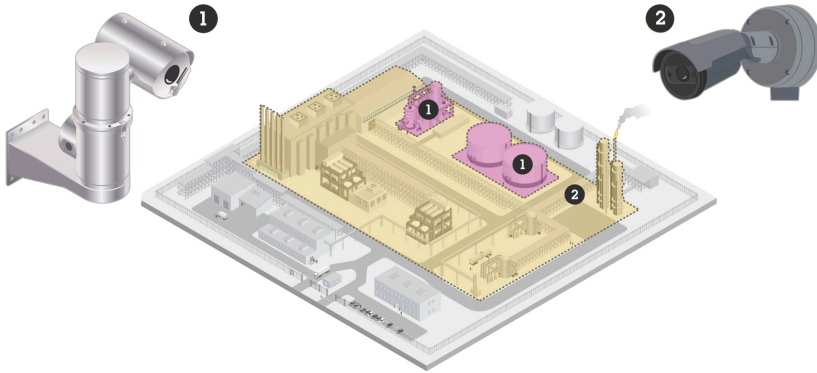
Nur elektrische Geräte, die ganz bestimmte Sicherheitsstandards erfüllen, dürfen in einer potenziell brennbaren Umgebung z. B. in einem Chemiewerk oder in der Nähe von Gasventilen oder Abluftleitungen, installiert werden. Dabei gilt es, die potenziell brennbare Umgebung vor Entzündung zu schützen.

Kameras mit Explosionsschutz sind für den Einsatz in Gefahrenbereichen zertifiziert, da die Kameras so konzipiert sind, dass sie über Mechanismen zum Schutz vor Explosionen verfügen, wie zum Beispiel Eindämmung oder Vorbeugung. Der Begriff explosionsgeschützt **bedeutet nicht**, dass die Kamera selbst einer externen Explosion standhalten würde.

- > **Eindämmung:** Das Gehäuse der Kameras ist so stark belastbar, dass die Energie eines potenziellen internen Brands eingedämmt wird. Bei Explosionen, die durch Funken oder hohe Temperaturen in diesen Kameras verursacht werden, beschränkt sich die Explosion auf das Gehäuse und breitet sich nicht auf die möglicherweise entflammbare Atmosphäre außerhalb des Gehäuses aus. Dieser Typ von explosionsgeschützten Kameras kann für den Einsatz in Gefahrenbereichen der *Zone/Division 1* zertifiziert werden, in denen die Atmosphäre aufgrund der Konzentration von explosiven Dämpfen, Gasen, Staub oder Fasern relativ leicht entflammbar ist.
- > **Prävention:** Diese Kameras sind so konzipiert, dass sie nicht genügend Energie freisetzen können, um eine entflammbare Atmosphäre zu entzünden. Sie können für den Einsatz in Gefahrenbereichen der *Zone/Division 2* zertifiziert werden, bei denen es sich um weniger potenziell brennbare Bereiche in Gefahrenorten handelt.

Die Bereiche der *Zone/Division 2* in explosionsgefährdeten Bereichen sind in der Regel erheblich größer als die Bereiche der *Zone/Division 1*. Für Bereiche der *Zone/Division 1* zertifizierte Kameras

können auch in Bereichen der Zone/Division 2 eingesetzt werden, wobei speziell für Bereiche der Zone/Division 2 entwickelte und zertifizierte Kameras kostengünstigere Alternativen bieten.



Die richtige Kamera für den richtigen Gefahrenbereich.

- 1. In Bereichen der Zone/Division 1 müssen Kameras eingesetzt werden, die speziell für Zone/Division 1 zertifiziert sind.*
- 2. In den großen, potenziell nicht brennbaren Bereichen (Zone/Division 2) eines Gefahrenortes dürfen auch wesentlich kostengünstigere, für Bereiche der Zone/Division 2 zertifizierte Kameras eingesetzt werden.*

Kameras mit Explosionsschutz müssen entsprechend den Branchenstandards des Landes zertifiziert sein, in dem sie eingesetzt werden.

3. Kameraelemente

Bildqualität und Sichtfeld sind wahrscheinlich die wichtigsten Merkmale jeder Kamera. Sie werden durch eine Reihe von Kameraelementen beeinflusst. Dazu zählen unter anderem die Lichtempfindlichkeit der Kamera, das verwendete Objektiv, der Bildsensor und die Bildverarbeitungsfunktionen.

3.1 Lichtempfindlichkeit

Die oft in Lux angegebene Lichtempfindlichkeit einer Kamera entspricht dem niedrigsten Lichtstärkeniveau, bei dem die Kamera noch ein akzeptables Bild erzeugen kann. Helligkeit ist ein Maß dafür, wie stark das einfallende Licht eine Oberfläche je Flächeneinheit beleuchtet. Die Lichtempfindlichkeit hängt in erster Linie vom Objektiv und dem Bildsensor ab. Je niedriger der angegebene Lux-Wert ist, desto größer ist die Lichtempfindlichkeit der Kamera.

Helligkeit (Lux)	Lichtbedingung
100.000	Starkes Sonnenlicht
10.000	Helles Tageslicht
500	Bürobeleuchtung
100	Wohnzimmer
10	Kerze bei 30 cm Abstand
0,1	Vollmond in klarer Nacht
0.01	Halbmond

Tabelle 3.1a *Beispiellichtstärken bei unterschiedlichen Lichtverhältnissen.*

Natürliche Szenen weisen häufig sehr komplexe Lichtverhältnisse auf. Sie enthalten sowohl Schatten als auch Schlaglichter, sodass in verschiedenen Bereichen einer Szene unterschiedliche

Lux-Werte zu verzeichnen sind. Es ist daher zu berücksichtigen, dass ein einzelner Lux-Wert nicht die Lichtverhältnisse der gesamten Szene angibt.

Viele Hersteller geben an, wie viel Helligkeit mindestens erforderlich ist, damit die Netzwerk-Kamera ein akzeptables Bild erzeugt. Diese Spezifikationen sind zwar hilfreich, um die Lichtempfindlichkeit von Kameras desselben Herstellers zu vergleichen. Für Vergleiche von Kameras verschiedener Hersteller sind sie nicht geeignet. Der Grund dafür ist, dass die Hersteller die Spezifikationen mit verschiedenen Methoden messen und unterschiedliche Kriterien dafür anlegen, was unter einem akzeptablen Bild zu verstehen ist. Es empfiehlt sich, die Leistung zweier verschiedener Kameras bei schlechten Lichtverhältnissen zu vergleichen, indem die Kameras nebeneinander platziert und auf ein sich bewegendes Objekt unter schlechten Lichtverhältnissen gerichtet werden.

Axis bietet eine Reihe von Lösungen an, mit denen man bei schlechtem Licht oder in der Nacht Bilder guter Qualität aufnehmen kann. Dazu zählen z. B. Kameras mit Tag-und-Nacht-Funktionalität oder Tag-und-Nacht-Kameras mit Axis Lightfinder-Technologie oder mit integrierter Infrarot-LED. Kameras mit Tag-Nacht-Funktionalität erzeugen mithilfe von Nah-Infrarot-Licht qualitativ hochwertige Videos in Schwarzweiß, Tag-und-Nacht-Kameras mit Lightfinder ermöglichen Farbvideos bei sehr schwachem Licht. Bei schlechten Lichtverhältnissen oder in völliger Dunkelheit verbessern externe Infrarotstrahler die Qualität von Schwarzweiß-Videobildern. Wärmebildkameras, welche die von Objekten ausgehende Infrarotstrahlung (mit längeren Wellenlängen als das sichtbare Licht) nutzen, sind für die Erfassung von Vorfällen rund um die Uhr am zuverlässigsten.

Weitere Informationen zur Axis Lightfinder-Technologie, Kameras mit eingebauter IR-LED und Wärmebildkameras siehe Kapitel . Weitere Informationen zur Tag- und Nachtfunktionalität und Strahlern finden Sie im Abschnitt .

3.2 Objektive

Das Objektiv (oder die Objektiv-Baugruppe) einer Kamera übernimmt verschiedene Aufgaben.

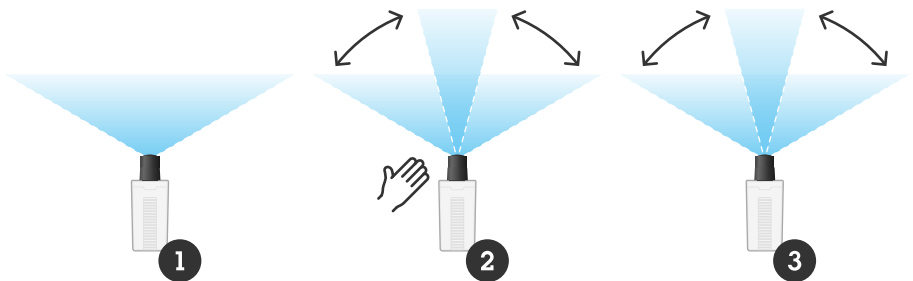
- > Es definiert das Sichtfeld, mit dem festgelegt wird, wie viel einer Szene im Bild zu sehen ist.
- > Durch Anpassung der Objektivauflösung an die Sensorauflösung bleiben die Szenendetails erhalten.
- > Es steuert die Lichtmenge, die durch das Objektiv auf den Bildsensor fällt, sodass das Bild korrekt belichtet wird.
- > Es fokussiert das Bild, indem es entweder die Linsen in der Objektiv-Baugruppe selbst bewegt oder den Abstand zwischen Objektiv-Baugruppe und Bildsensor ändert.

Das Objektiv ist das Auge der Kamera und daher sind seine Fähigkeiten und Funktionen sehr wichtig. Sichtfeld, Auflösung, Lichtempfindlichkeit und Schärfentiefe sollten bei der Kamerawahl sorgfältig bedacht und auf Ihre Bedürfnisse abgestimmt werden.

3.2.1 Objektivtypen

Je nach Verwendungsarten stehen verschiedene Objektive zur Auswahl:

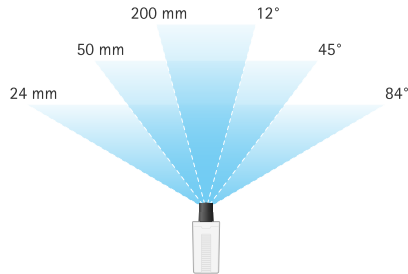
- > **Objektive mit fester Brennweite.** Auch als festes Objektiv bezeichnet. Die Brennweite ist fest und bietet ein einziges Sichtfeld.
- > **Vario-Fokus-Objektiv.** Bietet eine variable Brennweite und damit unterschiedliche Sichtfelder. Das Sichtfeld kann am Objektiv oder über die Weboberfläche der Kamera eingestellt werden. Wenn Sie die Brennweite eines Vario-Fokus-Objektivs einstellen, muss das Objektiv erneut fokussieren.
- > **Das Zoom-Objektiv.** Ist wie ein Vario-Fokus-Objektiv, da es ein einstellbares Sichtfeld bietet, aber hier muss der Fokus nicht neu ausgerichtet werden, wenn das Sichtfeld geändert wird. Der Fokus wird bei wechselnder Brennweite beibehalten. Dieser Objektivtyp ist in der Sicherheitsbranche sehr unüblich, kann jedoch mit motorisierten Objektiven nachgeahmt werden.



Kamera mit festem Objektiv (1), Vario-Objektiv (2) und Zoomobjektiv (3).

3.2.2 Sichtfeld

Das Sichtfeld beschreibt den Winkel, den die Kamera erfassen kann. Es ergibt sich aus der Brennweite des Objektivs sowie der Größe des Bildsensors. Je größer die Brennweite, desto kleiner das Sichtfeld. Das Sichtfeld wird gelegentlich mit HFoV, VFoV oder DFoV gekennzeichnet. Dies entspricht dem horizontalen, vertikalen oder diagonalen Sichtfeld.



Eine größere Brennweite (in mm) ermöglicht ein engeres Sichtfeld (in Grad).

Ein Objektiv kann in eine von drei Kategorien eingeteilt werden, je nachdem, welche Winkel das Objektiv wiedergeben kann.

- > **Weitwinkelobjektiv.** Ergibt ein viel größeres Sichtfeld als das normale Sichtfeld des menschlichen Auges. Bietet in der Regel auch eine große Schärfentiefe.
- > **Normalsichtobjektiv.** Ergibt ein ähnliches Sichtfeld wie das zentrale Sichtfeld des menschlichen Auges.
- > **Teleobjektiv.** Ergibt ein engeres Sichtfeld und eine Vergrößerungswirkung im Vergleich zum menschlichen Sichtfeld. Kann manchmal zu einer geringen Schärfentiefe führen.



Sichtfeld mit Weitwinkelobjektiv (1), Normalsichtobjektiv (2) und Teleobjektiv (3).

Die einfachste Möglichkeit, die erforderliche Brennweite für ein bestimmtes Sichtfeld zu finden, besteht in der Verwendung der Axis Online-Tools *Objektivrechner* oder *Product Selector*, beide unter www.axis.com/tools verfügbar.

3.2.3 Blendenzahl und Belichtung

Die Lichterfassung einer Kamera wird durch die Blendenzahl (auch als Blende bezeichnet) des Objektivs angegeben. Mit der Blendenzahl wird definiert, wie viel Licht das Objektiv passieren und den Bildsensor erreichen kann. Es ist das Verhältnis zwischen der Brennweite des Objektivs und dem Durchmesser des Eingangsbereichs des Objektivs.

Je kleiner die Blendenzahl, desto größer ist die Lichtstärke, d. h. desto mehr Licht kann zum Bildsensor gelangen. In Szenen mit geringer Beleuchtung wird mit einer kleinen Brennweite eine höhere Bildqualität erzielt, während eine größere Brennweite für mehr Schärfentiefe sorgt. Ein Objektiv mit kleiner Brennweite ist in der Regel teurer als eines mit einer großen Brennweite.

Bei einigen Objektiven kann die Blendenöffnungsgröße geändert werden. Dies erfolgt über die Blende, die manuell oder von der Kamera gesteuert werden kann. Bei einem Vario-Fokus- oder Zoom-Objektiv steigt die Brennweite in der Regel mit zunehmender Brennweite an. Die auf dem Objektiv aufgedruckte Blendenzahl ist normalerweise nur für die breite Einstellung gültig. Bei einigen Vario-Fokus- oder Zoom-Objektiven bleibt die Brennweite unabhängig von der Zoom-Einstellung gleich. Diese werden als Objektive mit konstanter Blendenöffnung oder konstanter Blendenzahl bezeichnet.



Die Lichtstärke einer Kamera ist bei niedriger Blendenzahl höher.

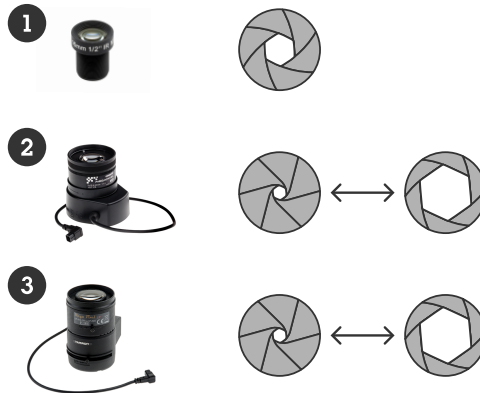
3.2.4 Blendentypen

Die Blende eines Objektivs funktioniert auf ähnliche Weise wie die Blende des menschlichen Auges. Sie steuert die Lichtmenge, die durchgelassen wird, damit das Kamerabild richtig belichtet wird. Sie kann auch zur Optimierung von Bildqualitätsaspekten wie Auflösung, Kontrast und Schärfentiefe verwendet werden.

In der Sicherheitsbranche sind drei Blendentypen üblich:

- > Bei Objektiven mit **fester Blende** kann die Größe der Blendenöffnung nicht geändert werden. Dies wird vom M12-Objektiv (S-Mount) genutzt. Objektive mit dieser Blendenart werden hauptsächlich in Umgebungen mit kontrollierten Lichtverhältnissen eingesetzt, in der Regel im Innenbereich.

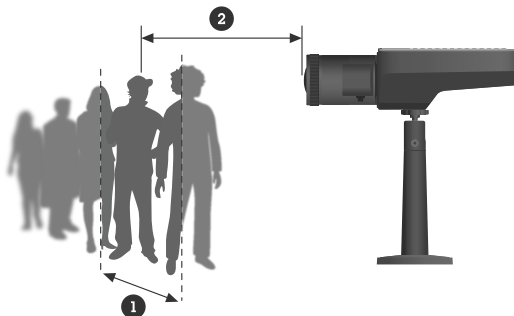
- > Bei Objektiven mit **DC-Blende** kann die Kamera die Blendenöffnung als Reaktion auf die Lichtmenge automatisch ändern und dadurch die Lichtmenge steuern, die den Bildsensor erreicht. Objektive mit dieser Art von Blende können in Umgebungen mit schwierigeren Lichtverhältnissen, in der Regel im Außenbereich, eingesetzt werden.
- > Bei einem **P-Blendenobjektiv** kann die Kamera die Blendenöffnung viel präziser steuern als mit dem DC-Blendenobjektiv. Die Kamera kann nicht nur die Lichtmenge optimieren, die den Bildsensor erreicht, sondern auch die Schärfe, den Kontrast und die Tiefenschärfe verbessern.



In der Sicherheitsbranche übliche Blendentypen: feste Blende (1), DC-Blende (2), P-Blende (3).

3.2.5 Schärfentiefe

Die Schärfentiefe bezieht sich auf den Abstand zwischen dem nächstgelegenen und dem am weitesten entfernten Objekt, die gleichzeitig scharf erscheinen. Dies ist bei Anwendungen wie der Überwachung von Parkplätzen wichtig, bei denen Nummernschilder in 20, 30 und 50 Metern Entfernung noch lesbar sein müssen.



In dieser Abbildung werden die Schärfentiefe (1) und der Brennpunkt (2) durch den Abstand zwischen Kamera und Brennpunkt dargestellt. Bei größerer Schärfentiefe erscheinen Objekte bei einem größeren Bereich um den Brennpunkt scharf.

Die Schärfentiefe wird von vier Faktoren beeinflusst: Brennweite, Blendenzahl, Abstand zwischen Kamera und Motiv und Art der Betrachtung des Bildes. Der Teil über die Art der Betrachtung des Bildes bezieht sich auf Aspekte wie die Pixelgröße, den Abstand zwischen dem Monitor und dem Betrachter, die Sehkraft des Betrachters und so weiter.

Eine längere Brennweite, eine niedrigere Blendenzahl, ein kürzerer Abstand zwischen Kamera und Objekt sowie ein kürzerer Abstand zwischen Monitor und Beobachter verringern die Schärfentiefe.



Links: Foto mit geringer Schärfentiefe – nur die Stifte vorne befinden sich im Fokus. Rechts: Foto mit größerer Schärfentiefe – alle Stifte sind akzeptabel scharf abgebildet.

3.2.6 Abstimmung von Objektiv und Sensor

Beim Austausch von Objektiven muss das Objektiv auf den Bildsensor der Kamera abgestimmt werden. Wenn das Objektiv für einen kleineren Sensor als den in der Kamera vorgesehen ist, werden schwarze Ecken angezeigt. Wenn das Objektiv für einen größeren Sensor als den in der Kamera vorgesehen ist, ist das Sichtfeld kleiner als das Sichtfeld des Objektivs, da ein Teil der Informationen außerhalb des Bildsensors verloren geht. In diesem Szenario entsteht eine Tele-Darstellung, in der alles vergrößert aussieht.



Die Wirkung verschiedener Objektive auf einen 1/1,8-Zoll-Sensor. Rechts: Ein 1/2,7-Zoll-Objektiv ist für den Sensor zu klein und das Bild hat schwarze Ecken. Mitte: Ein 1/1,8-Zoll-Objektiv entspricht der Sensorgröße. Links: Ein 1/1,2-Zoll-Objektiv ist für den Sensor zu groß, die Informationen außerhalb des Bildsensors gehen verloren.

Auf den Seiten zum Objektivprodukt auf axis.com werden in der Regel Informationen darüber angezeigt, welche Sensorgrößen unterstützt werden und welche Kameras mit jedem Objektiv kompatibel sind.

3.2.7 Objektivtypen für die Überwachung

	Ein Block-Objektiv kann Fokus und Zoom remote über Motoren einstellen. Es bietet einige Möglichkeiten für eine optimale Bildqualität. Es wird häufig in PTZ-, Dome- und Bullet-Kameras verwendet. Dieser Objektivtyp ist in die Kamera integriert und kann nicht ausgetauscht werden.
	Ein M12-Objektiv hat in den meisten Fällen eine feste Brennweite und keine Blendensteuerung. Aufgrund seiner kleinen Bauform wird es in modularen Kameras, einigen Dome-Kameras, Body Worn-Kameras und Gegensprechanlagen eingesetzt. Bei einigen Kameras ist dieses Objektiv austauschbar. Dieses Objektiv wird auch als S-Mount-Objektiv bezeichnet.



Ein C/CS-Objektiv hat ein bestimmtes Montagegewinde, wodurch es sich leicht austauschen lässt. Dieser Objektivtyp wird in Boxkameras verwendet. Es ist in einer Vielzahl von Variofokus-Längen mit DC- oder P-Iris-Steuerung vorhanden. Dieses Objektiv bietet eine große Flexibilität und ist für verschiedene Überwachungsszenarien geeignet.



Ein i-CS-Objektiv verfügt über das gleiche Gewinde wie ein C/CS-Objektiv, wobei es jedoch aufgrund der integrierten Motoren für die Fernsteuerung von Zoom und Fokus zusätzliche Intelligenz bietet. Es bietet ähnliche Vorteile wie das Blockobjektiv, ist jedoch austauschbar. Es ist mit Boxkameras mit i-CS-Unterstützung kompatibel.

3.2.8 Fokussieren

Das Fokussieren mit einer Netzwerk-Kamera erfordert häufig Feineinstellungen am Objektiv. Bei einfachen Objektiven mit automatischer Blende empfiehlt sich das Einstellen des Fokus bei schwachem Licht oder die Verwendung eines verdunkelnden Filters, z. B. eines Neutralschichtfilters. Bei schwachem Licht öffnet sich die Blende automatisch. Dadurch verringert sich die Schärfentiefe und der Fokus lässt sich leichter präzise einstellen.

Autofokus

Eine Kamera mit Autofokus nimmt automatisch eine mechanische Einstellung des Objektivs vor, sodass das Bild scharf ist. Die Autofokus-Funktion ist unerlässlich für Schwenk-/Neigekameras, bei denen sich die Kameraausrichtung kontinuierlich verändert. Einige unbewegliche Kameras verfügen über einen Autofokus. Die zusätzlichen Kosten für diese Funktion sind jedoch kaum zu rechtfertigen, da das Fokussieren einer unbeweglichen Kamera normalerweise nur bei der Installation erforderlich ist.

Einige Kameras verfügen über vollständige Remote-Fokus-Funktionen und müssen somit nicht mehr manuell vor Ort eingestellt werden. Die zugehörige Computersoftware liefert ein Feedback in Echtzeit, das dem Benutzer eine Überprüfung des Fokus ermöglicht. Über einen integrierten Pixelzähler können Benutzer zudem sicherstellen, dass die Pixel der Aufnahme ausreichen, um Objekte – vom Gesicht bis zum Nummernschild – zu identifizieren.

Die Autofokus-Funktion erfordert weder eine gesonderte Einstellung noch eine Programmierung. Sie ist bei den PTZ-Kameras von Axis standardmäßig aktiviert und wird mit dem Einschalten der Kamera ausgeführt.

In Szenen mit schwachem Licht, geringem Kontrast oder starkem Bildrauschen benötigt der Autofokus möglicherweise etwas Zeit, um zu fokussieren. In manchen Fällen wird das falsche Objekt fokussiert. Bei einer Veränderung der Szene muss möglicherweise neu fokussiert werden, wofür der Autofokus etwas Zeit benötigt. Dies kann den Eindruck erwecken, dass die Kamera kontinuierlich fokussiert wird.

Fokusabruf

Mit einem Fokusabrufbereich in der gewünschten Ansicht kann die Bildschärfe schnell und einfach wiederhergestellt werden. Der Hauptunterschied zwischen Autofokus und Fokusabruf liegt darin, dass der Autofokus bei jeder Veränderung der Szene erneut fokussiert. Der Fokusabruf speichert hingegen die genaue Bildschärfe für einen bestimmten Bereich ab, sodass diese nicht erneut eingestellt werden muss.

Zum Festlegen eines Fokusabrufbereichs klickt der Benutzer auf die Schaltfläche für den Fokusabruf in der Benutzeroberfläche der Kamera, sobald die Ansicht die gewünschte Bildschärfe aufweist. Die Kamera speichert die Fokuseinstellung. Der Fokusabruf wird aktiviert, sobald der Benutzer mithilfe des Joysticks eine Schwenk- oder Neigebewegung auf den Fokusabrufbereich ausführt. Die Kamera verwendet dabei automatisch die gespeicherte Einstellung.

Laserfokus

Bei bestimmten Lichtverhältnissen kann der Einsatz der Autofokus-Funktion zu Problemen führen. In Szenen mit schwachem Licht, geringem Kontrast, Reflektionen oder konzentrierten Lichtquellen kann sich das Fokussieren als schwierig erweisen.

Der Laserfokus ermöglicht das Fokussieren heller und reflektierender Objekte wie z. B. Fensterscheiben. Solche Objekte sind für den Autofokus problematisch, weil die zum Fokussieren benötigten scharfen Kanten durch das reflektierte Licht verschwimmen. In Szenen mit beweglichen Objekten und schnellen Veränderungen ermöglicht der Laserfokus ein schnelles Fokussieren. So können etwa Nummernschilder an fahrenden Fahrzeugen scharf erfasst werden.



Laserfokus beim Fokussieren eines Nummernschilds bei schwachem Licht und konzentrierten Lichtquellen

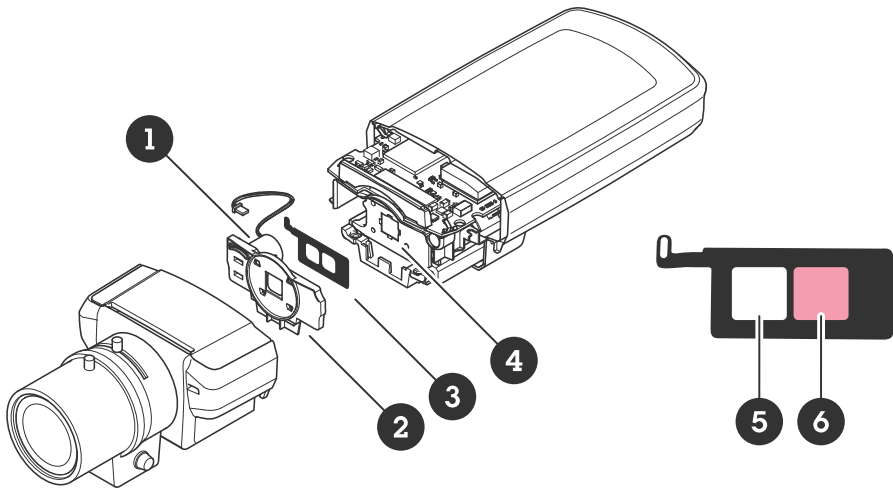
Der Laserfokus ist besonders für PTZ-Kameras geeignet, da sich die Ansicht beim Verwenden der PTZ-Funktion dynamisch verändert.

3.2.9 PTRZ-Präzision

Die PTRZ-Funktion mit Fernzugriff ermöglicht ein Verändern der Kameraeinstellungen aus der Distanz, ohne die Aufnahme zu unterbrechen. Die Kamera kann um ihre vertikale Achse (oben-unten), ihre Quer- (links-rechts) und Längsachse (vorn-hinten) rotieren. Sie kann außerdem ihre Brennweite anpassen, um ein engeres (hineinzoomen) oder weiteres (herauszoomen) Sichtfeld zu erhalten.

3.3 Abnehmbarer Infrarot-Sperrfilter (Tag-/Nacht-Funktion)

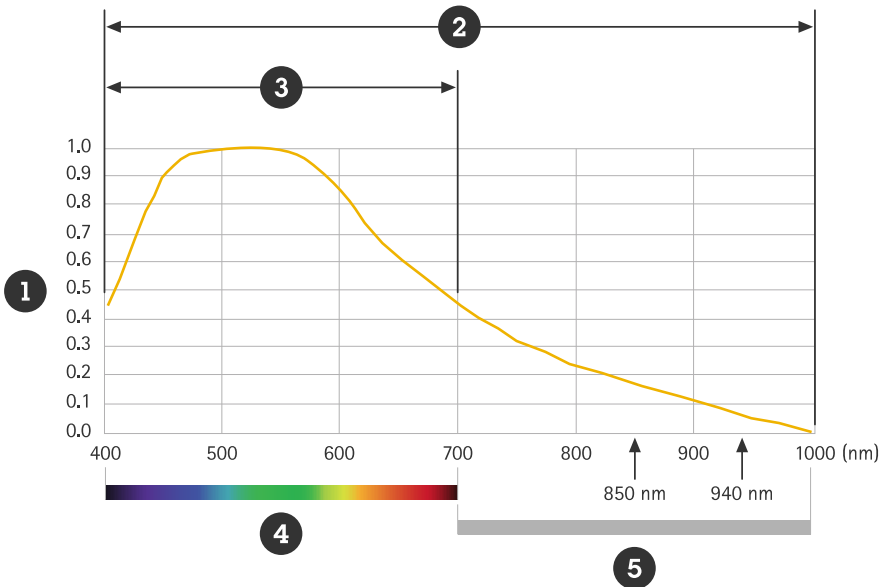
Viele Kameras verfügen zwischen Objektiv und Bildsensor über einen automatisch abnehmbaren Infrarot-Sperrfilter. Dieser Filter blockiert das einfallende Infrarotlicht (IR-Licht), damit die Kamera Farben so wiedergeben kann, wie sie vom menschlichen Auge wahrgenommen werden. Wird dieser Filter jedoch bei schlechten Lichtverhältnissen oder nachts weggeschwenkt, kann der Kamerasensor das Nah-Infrarotlicht (NIR-Licht) der Umgebung nutzen und Schwarzweißbilder von Szenen produzieren, bei denen das sichtbare Licht nicht ausreicht.



IR-Sperrfilter (Tag-/Nacht-Filter) an der optischen Einheit, der bei dieser Kamera seitlich verschoben wird. Der rotgetönte Filter wird tagsüber, der farblose Teil nachts verwendet.

1. Antrieb
2. Frontschutz
3. Optikhalter
4. Bildsensor
5. Nachtfilter
6. Tageslichtfilter

Fotografisches Nah-Infrarotlicht ist mit seiner Wellenlänge von 700–1000 Nanometern (nm) für das menschliche Auge nicht wahrnehmbar. Die meisten Bildsensoren von Kameras können es jedoch erkennen und nutzen.



Das Diagramm zeigt, wie ein Bildsensor auf sichtbares Licht und Nah-Infrarot-Strahlung reagiert.

1. Relative Sensorempfindlichkeit
2. Verwendete Wellenlängen im Nacht-Modus
3. Verwendete Wellenlängen im Tag-Modus
4. Sichtbares Licht
5. Nah-Infrarot-Licht

Kameras mit einem entfernbaren Infrarot-Sperrfilter haben eine Tag/Nacht-Funktion, durch die sie bei Tageslicht farbige und bei Dunkelheit schwarzweiße Videobilder liefern können. Sie sind bei schlechten Lichtverhältnissen, bei verdeckter Überwachung und in Umgebungen nützlich, in denen die Verwendung von Kunstlicht eingeschränkt ist.

Es können Infrarotlicht-Strahler, die Nah-Infrarotlicht erzeugen, in Verbindung mit einer Tag- und Nacht-Kamera verwendet werden. So lässt sich deren Fähigkeit verbessern, auch bei schlechten Lichtverhältnissen oder völliger Dunkelheit qualitativ hochwertige Videobilder zu erzeugen. Einige Tag-Nacht-Kameras verfügen über eine integrierte Infrarotbeleuchtung mit IR-LEDs. Diese liefern normalerweise Infrarotlicht mit einer Wellenlänge von 850 nm oder 940 nm.



Externe Infrarotstrahler und eine Kamera mit eingebauten Infrarotstrahlern.

In Axis Kameras eingebaute Infrarot-LEDs können an einen bestimmten Blickwinkel angepasst werden und bei Dunkelheit, einem Ereignis oder bei Bedarf automatisch aktiviert werden. Axis Kameras mit integrierten Infrarot-LEDs vereinfachen die Installation und stellen im Vergleich zu externen Infrarot-Strahlern eine kostengünstige Option dar. Monteure können externe Infrarotstrahler hingegen den Anforderungen entsprechend auswählen (beispielsweise ein Modell mit großer Reichweite) und an der am besten geeigneten Position montieren. Dies muss nicht unbedingt der Kamerastandort sein.

3.4 Bildsensoren

Der Bildsensor ist eine der Schlüsselkomponenten einer digitalen Kamera. Er erfasst das durch das Objektiv fallende Licht in allen Bereichen einer Szene und wandelt es in elektrische Signale um. Diese Signale liefern nach der zusätzlichen Verstärkung und Verarbeitung die Informationen, die die Kamera zur Wiedergabe eines digitalen Abbilds der Szene benötigt.

Der Bildsensor der Kamera besteht aus Millionen von Photodetektoren (lichtempfindlichen Dioden), die besser als Pixel bekannt sind. Ein Pixel nimmt Licht (Photonen) über einen festgelegten Zeitraum auf, bei dem es sich um die Belichtungszeit oder das Belichtungsintervall der Kamera handelt. Nach Verstreichen des Zeitraums wird das Pixel ausgelesen und seine Ladung gemessen. Anschließend beginnt ein weiteres Belichtungsintervall, in dem das Pixel neue Photonen aufnehmen kann.

Sicherheitskameras verwenden meist Rolling-Shutter-Bildsensoren. Dabei werden die Pixel nicht gleichzeitig, sondern nacheinander Zeile für Zeile belichtet. Zwischen dem Belichtungsbeginn der einzelnen Zeilen besteht ein geringer Zeitversatz. Einige Kameras nutzen stattdessen die Global-Shutter-Technologie, bei der der Sensor jedes Pixel des Bildes gleichzeitig belichtet. Dies eignet sich ideal für die Hochgeschwindigkeitsaufnahme, bei der Sie sich schnell bewegende Objekte verzerrungsfrei erfassen müssen. Global-Shutter ermöglicht zudem den Einsatz von Stroboskop- oder Blitzbeleuchtung mit hoher Spitzenleistung.

Die Qualität von Sensoren hat sich stark verbessert. Megapixel-, HDTV- und 4K-Sensoren sind weitverbreitet. Aber trotz des anhaltenden Trends der Überwachungsbranche hin zu höheren Auflösungen haben Hersteller oft die Sensorgröße beibehalten, um die höheren Kosten eines

größeren Sensors zu vermeiden. Aus diesem Grund sind sie gezwungen, zusätzliche Photodetektoren auf derselben Sensorfläche unterzubringen, wodurch die Pixel schrumpfen und weniger Licht aufnehmen können. Dementsprechend ist die Ladung nach jedem Belichtungsintervall kleiner und die elektrischen Signale für die Pixel erfordern eine größere Verstärkung und weisen ein höheres Rauschen auf.

Durch die reine Erhöhung der Pixelanzahl bei einem Sensor derselben Größe lässt sich also eine höhere Auflösung erreichen; allerdings kann das auch die Bildqualität verringern. Dies gilt vor allem bei schlechten Lichtverhältnissen, wo das Bildrauschen eher störend wirkt. Wird stattdessen die Größe des Sensors erhöht, kann jeder Photodetektor eine größere Anzahl von Photonen aufnehmen und ein stärkeres Signal mit geringerem Rauschen ausgeben.

Das Sortiment von Axis umfasst Kameras mit verschiedenen Sensorgrößen, von denen mehrere eine 4K-Auflösung sowie einen großen Sensor bieten. Mit Pixeln, deren Größe mehr als das Vierfache als bei den meisten anderen 4K-Kameras erreicht, erzeugen diese Kameras mit großen Sensoren mühelos hochauflösendes Bildmaterial, das selbst bei wenig Licht nicht an Klarheit und Schärfe verliert.

3.5 Belichtungssteuerung

Die beiden Hauptfaktoren, die beeinflussen, wie viel Licht ein Bildsensor empfängt, sind die Lichtstärke des Objektivs oder Blendenzahl und die Belichtungszeit. Ein dritter Faktor ist die Verstärkung. Dabei handelt es sich um einen Pegelverstärker zur Aufhellung des Bilds. Mit zunehmender Verstärkung wird jedoch auch das Rauschen („Körnigkeit“) eines Bildes verstärkt. Deshalb sollte in Regel eher die Belichtungszeit oder Blende angepasst werden.

Die Belichtungszeit wirkt sich immer auf Bilder aus, und die Einstellungen zur Belichtung können auf unterschiedliche Arten geändert werden. Die wichtigsten davon – Belichtungspriorität, Belichtungszonen, WDR und Dynamikbereich sowie Gegenlichtkorrektur – werden in diesem Abschnitt erläutert.

3.5.1 Belichtungspriorität

Helle Umgebungen erfordern kürzere Belichtungszeiten. Schlechte Lichtbedingungen erfordern längere Belichtungszeiten, sodass der Bildsensor mehr Licht aufnehmen kann, um die Bildqualität zu verbessern. Mit einer längeren Belichtungszeit werden jedoch auch die Bewegungsunschärfe erhöht und die Bildrate verlangsamt, da für die Belichtung jedes Einzelbilds mehr Zeit erforderlich ist.

Bei schlechten Lichtbedingungen können Benutzer von Axis Kameras die Videoqualität in Bezug auf Bewegung oder geringes Rauschen (Körnigkeit) priorisieren. Bei schnellen Bewegungen oder wenn eine hohe Bildrate erforderlich ist, wird eine kürzere Belichtungszeit bzw. eine schnellere Verschlusszeit empfohlen. Dies kann sich jedoch negativ auf die Bildqualität auswirken.

Wenn ein geringes Rauschen priorisiert wird, sollte die Verstärkung so gering wie möglich gehalten werden, um die Bildqualität zu verbessern, wodurch sich die Bildrate wiederum verlangsamen kann. Beachten Sie, dass eine niedrige Verstärkung bei schlechten Lichtbedingungen zu sehr dunklen Bildern führen kann. Durch eine hohe Verstärkung sind auch dunkle Szenen erkennbar, jedoch mit einem erhöhten Rauschen.

3.5.2 Belichtungszonen

Die automatische Belichtung einer Kamera muss entscheiden, welcher Teil des Bilds den Belichtungswert bestimmen soll. Bei vielen Axis Kameras kann der Benutzer auch Belichtungszonen einstellen, um sicherzustellen, dass der wichtigste Teil der Szene optimal belichtet wird.

3.5.3 Gegenlichtausgleich

Netzwerk-Kameras mit Gegenlichtkorrektur versuchen, abgegrenzte Bereiche mit starker Helligkeit (typischerweise der Himmel) zu ignorieren. Durch den Gegenlichtausgleich werden Objekte im Vordergrund sichtbar. Die hellen Bereiche werden damit allerdings überbelichtet.



Starkes Gegenlicht ohne Gegenlichtkorrektur (links). Bei angewendetem Gegenlichtausgleich wird der Vordergrund besser sichtbar (rechts).

3.5.4 Dynamischer Aufnahmebereich

Der Dynamikbereich ist, im Kontext von Licht, das Verhältnis zwischen der höchsten und der niedrigsten Beleuchtungsstärke in einem Bild. Viele Szenen haben einen großen Dynamikbereich

mit sehr hellen und sehr dunklen Stellen. Für normale Kameras mit einem begrenzten Dynamikbereich stellt dies ein Problem dar. In solchen Szenen oder bei Gegenlicht, wenn z. B. eine Person vor einem hell erleuchteten Fenster steht, erzeugt eine normale Kamera ein Bild, auf dem Objekte in den dunklen Bereichen kaum zu erkennen sind. Um den Dynamikbereich von Kameras zu vergrößern, sodass Objekte in dunklen und hellen Bereichen besser erkennbar sind, können verschiedene Techniken angewendet werden. Die Belichtung kann gesteuert werden, und mittels Tone Mapping lässt sich die Verstärkung in dunklen Bereichen anheben.



Zwei Bilder derselben Szene. Das Bild auf der rechten Seite bietet eine bessere Auswertung des dynamischen Aufnahmebereichs und einen größeren Detailreichtum sowohl in hellen als auch in dunklen Bereichen.

3.5.5 WDR-Bilder

Die WDR-Bildgebung (Wide Dynamic Range) ist eine Möglichkeit, den gesamten Dynamikbereich einer WDR-Szene in einem einzigen Bild wiederzugeben. Betrachten Sie als Beispiel im Folgenden die Parkhausszene. Eine herkömmliche Kamera kann nicht den vollen Dynamikbereich erfassen, und die Bildqualität ist entweder in den dunklen oder in den hellen Bereichen beeinträchtigt.



Parkhaus mit einer herausfordernden Lichtsituation. Auf der linken Seite ist das Bild überbelichtet. Auf der rechten Seite ist das Bild unterbelichtet.

Mit einer WDR-fähigen Kamera können alle Bereiche in einem einzigen Bild sichtbar gemacht werden.



Mit einer WDR-fähigen Überwachungskamera erfasstes Parkhaus mit nachteiligen Lichtverhältnissen.

Informationen zu den WDR-Lösungen von Axis finden Sie im Abschnitt .

3.6 Aktiver Manipulationsalarm

Der aktive Manipulationsalarm benachrichtigt den Bediener automatisch, wenn eine Kamera manipuliert wird. Dadurch kann das Personal eine Verschlechterung der Bildqualität schnell erkennen. Die Anwendung ist besonders nützlich, wenn das Risiko von Vandalismus besteht, z. B. in Schulen, Gefängnissen oder öffentlichen Verkehrsmitteln sowie bei schwierigen äußeren Umweltbedingungen, wo die Kameralistung durch Witterung, Vibrationen oder Schmutz beeinträchtigt werden kann. Der aktive Manipulationsalarm erkennt Ereignisse wie das Verstellen, Blockieren oder Defokussieren des Kamerabilds. Er reagiert auch, wenn die Kamera beschädigt, mit Farbe besprüht oder absichtlich abgedeckt wird.

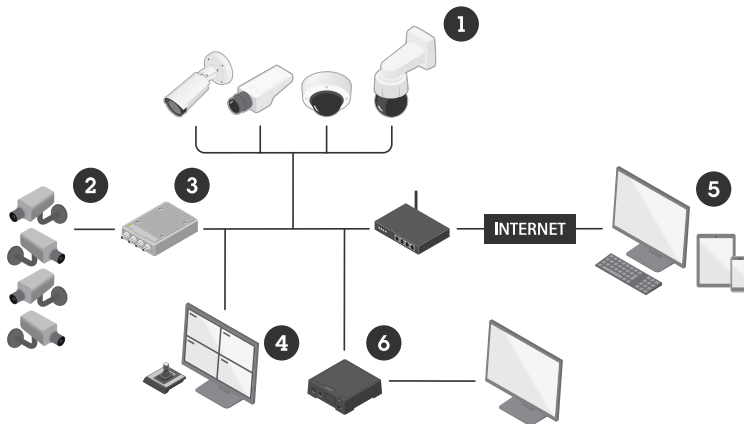
3.7 Audioerfassung

Audioerfassung kann eingesetzt werden, um relevante Geräusche wie Schreie oder Glasbruch zu erkennen und automatische Alarme zu senden, die Mitarbeiter auf verdächtige Aktivitäten aufmerksam machen. Die Audioerfassung ist eine leistungsstarke Ergänzung zur Videotechnik, da sie Aktivitäten auch außerhalb des Sichtfelds der Kamera oder in schlecht beleuchteten Bereichen erkennen kann. Für eine funktionierende Audioerfassung muss die Kamera Audiofunktionen unterstützen und benötigt ein eingebautes oder ein externes Mikrofon.

4. Video-Encoder

Mithilfe von Video-Encodern können vorhandene analoge CCTV-Videosicherheitssysteme in Netzwerk-Videosysteme integriert werden. Video-Encoder spielen bei Installationen mit vielen analogen Kameras eine wichtige Rolle.

4.1 Was ist ein Video-Encoder?



Video-Encoder und -Decoder können zur Integration von analogen Videokameras und Live-Ansichten in ein Netzwerk-Videosystem verwendet werden. Netzwerk-Kameras (1) werden hier durch analoge Kameras (2) und einen Video-Encoder (3) ergänzt. Das System wird über ein Videoverwaltungssystem (4) verwaltet und kann über einen Computer oder ein Mobilgerät (5) per Fernzugriff erreicht werden. Mit einem Decoder (6) können Monitore für die Wiedergabe von Live-Video ohne Computer verwendet werden.

Mithilfe von Video-Encodern können Sicherheitsmanager ihre analogen CCTV-Kameras weiterhin nutzen, während sie ein Sicherheitssystem mit den Vorteilen von Netzwerk-Video aufbauen. Wenn ein Video-Encoder in das System integriert wird, können analoge Kameras über ein IP-Netzwerk,

z. B. ein LAN oder das Internet, gesteuert und aufgerufen werden. Außerdem können so ältere Geräte zur Videoaufzeichnung wie DVRs und Monitore durch Standardcomputermonitore und -server ersetzt werden.

4.1.1 Kriterien für Video-Encoder-Komponenten

Video-Encoder von Axis bieten viele der Funktionen, die auch bei Netzwerk-Kameras zur Verfügung stehen. Bei der Auswahl eines Video-Encoders für professionelle Systeme sollte besonders auf Zuverlässigkeit und Qualität geachtet werden. Weitere Aspekte sind die Anzahl der unterstützten analogen Kanäle, die Bildqualität, Komprimierungsformate, die Bildrate und die Auflösung. Einige Encoder unterstützen analoge HD-Kameras sowie analoge Kameras mit Standardauflösung. Außerdem können Funktionen wie PTZ-Unterstützung, Audio, Ereignisverwaltung, Analysen, Power over Ethernet und Sicherheitsfunktionen entscheidend sein.

Wenn der Video-Encoder Vibrationen, Stößen und extremen Temperaturen standhalten muss, sollte ein Schutzgehäuse oder ein robuster Video-Encoder in Betracht gezogen werden.



Videoencoder unterstützen vier Kanäle und 16 Kanäle.

Über einen Mehrkanal-Video-Encoder werden die Videosignale der einzelnen Remote-Kameras über dieselben Netzkabel übertragen, wodurch Verkabelungskosten eingespart werden können. Wenn bereits Investitionen in analoge Kameras getätigt, jedoch noch keine Koaxialkabel verlegt wurden, ist der Einsatz von Video-Encodern empfehlenswert. Diese sollten in der Nähe der analogen Kameras positioniert werden. Auf diese Weise werden die Installationskosten gesenkt, da die Videodaten über das Ethernet-Netzwerk übertragen werden können und keine neuen Koaxialkabel zu einem zentralen Standort verlegt werden müssen.

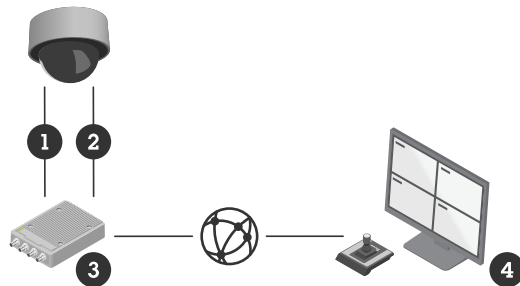
4.1.2 Ereignisverwaltung und Analyse

Ein Hauptvorteil der Axis Video-Encoder ist die Möglichkeit, Ereignisverwaltungs- und Analyseanwendungen bereitzustellen, über die analoge Videosysteme nicht verfügen. Dank integrierter Analysefunktionen wie z. B. videobasierter Bewegungserkennung in mehreren Fenstern, Audioerfassung und aktivem Manipulationsalarm sowie Eingangsanschlüssen für externe Sensoren kann das IP-Videosicherheitssystem jederzeit sofort auf Ereignisse reagieren. Wenn ein Ereignis

erkannt wurde, kann das System automatisch mit Aktionen reagieren. Hierzu zählen Videoaufzeichnungen, das Senden von Warnmeldungen per E-Mail, das Einschalten von Beleuchtungen, das Öffnen bzw. Schließen von Türen sowie akustische Alarmer.

4.2 Video-Encoder für analoge PTZ-Kameras

In einem Netzwerk-Videosystem werden PTZ-Befehle von einer Steuerungseinheit über dasselbe IP-Netzwerk wie die Videodaten gesendet und dann über den seriellen Anschluss (RS-422/RS-485) des Video-Encoders an die analoge PTZ-Kamera weitergeleitet. Mithilfe von Video-Encodern können analoge PTZ-Kameras somit selbst über das Internet über große Entfernungen gesteuert werden.

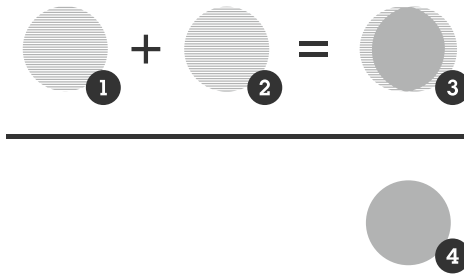


Eine analoge PTZ-Dome-Kamera wird über den seriellen Anschluss (z. B. RS-485) des Video-Encoders angeschlossen und kann dadurch per Fernzugriff über das IP-Netzwerk gesteuert werden.

1. Twisted-Pair-Koaxialkabel RS-485
2. Koaxialkabel
3. Video-Encoder
4. Arbeitsplatz mit Joystick

4.3 Deinterlacing-Techniken

Analoge Kameras stellen mithilfe des Zeilensprungverfahrens ein Bild zusammen. Dabei werden zwei Zeilenfelder erzeugt: ein Feld mit den ungeraden Zeilen und ein zweites Feld mit den geraden Zeilen. Beim Übertragen eines Zeilensprungbildes wird immer nur die Hälfte der Zeilen (gerade oder ungerade) eines Bildes gesendet, sodass auch die Bandbreitennutzung halbiert wird. Netzwerk-Kameras verwenden stattdessen die progressive Abtastung, bei der alle Zeilen des Bildes aufgezeichnet, übertragen und in einem Einzelbild angezeigt werden.



Oben: Ein per Zeilensprungverfahren erzeugtes Bild, wobei immer nur die Hälfte der Zeilen (gerade oder ungerade) gesendet wird, mit Enddarstellung auf einem Computermonitor. Unten: Darstellung eines mit progressiver Abtastung erstellten Bilds auf demselben Monitor.

1. Erstes Feld: ungerade Zeilen.
2. Zweites Feld: gerade Zeilen, 17/20 ms später (NTSC/PAL).
3. Standbild eines sich bewegenden Objekts beim Zeilensprungverfahren.
4. Standbild eines sich bewegenden Objekts bei progressiver Abtastung.

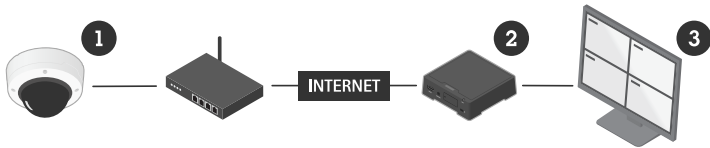
Videobilder von analogen Kameras sind für analoge Monitore wie herkömmliche Fernsehgeräte vorgesehen, die das Zeilensprungverfahren verwenden. Wenn solche Videobilder stattdessen auf Computerbildschirmen angezeigt werden, die die progressive Abtastung verwenden, treten bei sich bewegenden Objekten Zeilensprüngeffekte (d. h. Reißen oder Kammeffekt) auf. Um diese unerwünschten Zeilensprüngeffekte zu reduzieren, können verschiedene Deinterlacing-Verfahren angewendet werden. Bei erweiterten Video-Encodern von Axis können Benutzer zwischen zwei Deinterlacing-Verfahren wählen: Adaptive Interpolation oder Blending.

Die adaptive Interpolation bietet die beste Bildqualität. Dabei wird nur eines der beiden aufeinanderfolgenden Halbbilder verwendet und das andere Halbbild durch Interpolation zu einem Vollbild zusammengesetzt. Beim Blending werden zwei aufeinander folgende Halbbilder verschmolzen und als ein Bild angezeigt, so dass alle Halbbilder vorhanden sind. Anschließend wird das Bild gefiltert, um unerwünschte Bewegungsartefakte bzw. Kammeffekte zu entfernen, die dadurch entstanden sind, dass die beiden Halbbilder zu unterschiedlichen Zeiten aufgenommen wurden. Das Blending-Verfahren beansprucht den Prozessor nicht so sehr wie die adaptive Interpolation.

4.4 Video-Decoder

Mit den Video-Decodern von Axis können digitale Monitore an Axis Kameras angeschlossen werden und Live-Video von ihnen anzeigen. Dies ist eine kostengünstige Lösung für die Videoüberwachung,

bei der mehrere Live-Videostreams auf einem öffentlichen Überwachungsmonitor oder Sicherheitsmonitor ohne PC-Verbindung angezeigt werden können.



Ein Video-Decoder (2) ermöglicht die Anzeige von Live-Video von einer Axis Kamera (1) auf einem Monitor (3), ohne einen Computer zu verwenden.

5. Bildauflösungen

Je mehr Pixel ein Sensor umfasst, desto feinere Details können aufgezeichnet werden und desto besser ist die Bildqualität. Mehrere neue, weltweit genormte Auflösungen wurden eingeführt, die aus der Computer- und Digitalfernsehindustrie stammen.

5.1 Auflösungen im Megapixel-Bereich

Ein Megapixel-Sensor liefert ein Bild mit Millionen von Pixeln (eine Million oder mehr). Megapixel-Kameras kommen bei der Überwachung zum Einsatz, wenn es auf Details ankommt, z. B. wenn Menschen und Objekte identifiziert oder größere Bereiche überwacht werden müssen.

Gemäß bewährten Verfahren für die Videosicherheit benötigt ein Übersichtsbild etwa 70–100 Pixel, um 1 m (20–30 Pixel pro Fuß) darstellen zu können. In Situationen, die detaillierte Bilder erfordern, z. B. bei der Identifizierung von Personen, können bis zu 250 Pixel pro Meter erforderlich sein. Müssen beispielsweise Personen identifiziert werden, die einen Bereich von 4 m Breite und 4 m Höhe durchlaufen, muss die Kamera eine Auflösung von mindestens einem Megapixel (1000 × 1000 Pixel) liefern können. Weitere Informationen zur empfohlenen Pixeldichten finden Sie in Kapitel .

5.2 HDTV-Auflösungen (High-Definition Television)

Die beiden wichtigsten HDTV-Standards sind SMPTE 296M, mit dem das HDTV 720p-Format, und SMPTE 274M, mit dem das HDTV 1080p-Format definiert wird.

Eine Kamera, die den SMPTE-Standard erfüllt, liefert HDTV-Qualität und sollte alle Vorteile von HDTV bezüglich Auflösung, Farbtreue und Bildrate bieten. Der HDTV-Standard basiert auf quadratischen Pixeln, ähnlich wie bei Computerbildschirmen. Daher kann HDTV-Video von Netzwerk-Videoprodukten entweder auf HDTV-Bildschirmen oder auf Standardcomputermonitoren angezeigt werden. Bei einem HDTV-Video mit progressiver Abtastung muss keine Umwandlung oder

Deinterlacing-Technik angewendet werden, wenn das Video auf einem Computer verarbeitet oder auf einem Computerbildschirm angezeigt werden soll.

Größe	Seitenverhältnis	Scannen	Bildrate (Bilder pro Sekunde/Hz)	Etikett
1280 × 720	16:9	Vollbild	50	720p50
1920 × 1080	16:9	Zeilensprungverfahren	25 ^a	1080i50
1920 × 1080	16:9	Vollbild	25	1080p25
1920 × 1080	16:9	Vollbild	50	1080p50

Tabelle 5.2a *Normale HDTV-Bildgrößen in der Europäischen Rundfunkunion. Bildrate 50 Hz. Beachten Sie, dass auch andere Bildraten verwendet werden können. Die gängigsten sind 24, 25, 30, 50 und 60 Bilder pro Sekunde.*

Größe	Seitenverhältnis	Scannen	Bildrate (Bilder pro Sekunde/Hz)	Etikett
1280 × 720	16:9	Vollbild	60	720p60
1920 × 1080	16:9	Zeilensprungverfahren	30 ^a	1080i60
1920 × 1080	16:9	Vollbild	30	1080p30
1920 × 1080	16:9	Vollbild	60	1080p60

Tabelle 5.2b *Normale HDTV-Bildgrößen in Ländern des National Television System Committee. 60 Hz. Beachten Sie, dass auch andere Bildraten verwendet werden können. Die gängigsten sind 24, 25, 30, 50 und 60 Bilder pro Sekunde.*

5.3 Ultra-HD-Auflösungen

Wie HDTV ist auch Ultra-HD ein Standard, der eine bestimmte Videoqualität garantiert, wobei die Megapixel lediglich die Kamerauflösung angeben. Ultra-HD-Auflösungen (UHDTV) umfassen zwei digitale Videoformate:

- > Ultra-HD 2160p wird im Allgemeinen als 4K bezeichnet und bietet eine Auflösung von 3840 x 2160 Pixeln, wodurch sich 8,3 Megapixel ergeben, das Vierfache von HDTV 1080p.

- > Ultra-HD 4320p wird im Allgemeinen als 8K bezeichnet und bietet eine Auflösung von 7680 x 4320 Pixeln, wodurch sich 33,2 Megapixel ergeben, das 16-fache von HDTV 1080p.

Beide Formate bieten eine überragende Farbtreue, eine progressive Abtastung mit bis zu 100/120 Bildern pro Sekunde sowie H.265-Komprimierung.

Bei der Videosicherheit ermöglichen solch hohe Auflösungen von Ultra-HD eine außerordentliche Zoomfähigkeit sowie ein erweitertes Sichtfeld. Dadurch können Ultra-HD-Kameras ideal zum Aufzeichnen von Gesichtsmerkmalen und anderen Details eingesetzt werden. Ultra-HD erfordert jedoch qualitativ hochwertige Objektive, viele Pixel, große Sensoren, die genügend Licht aufzeichnen können, sowie eine deutliche Erweiterung der Bandbreite und Speicherkapazität. Mit anderen Worten: Die erhöhte Auflösung kann mit sehr hohen Kosten verbunden sein.

HDTV 1080p			
Ultra HD 2160p (4K)			
		Ultra HD 4320p (8K)	

Ultra-HD 4320p (8K) bietet die 16-fache Auflösung von HDTV 1080p. Ultra-HD 2160p (4K) bietet die vierfache Auflösung von HDTV 1080p.

5.4 Seitenverhältnisse

Das Seitenverhältnis ist das Verhältnis zwischen der Breite und Höhe eines Bildes. Altmodische TV-Monitore, die traditionell zur Anzeige von analogen Überwachungsvideos eingesetzt werden, zeigen Bilder mit einem Seitenverhältnis von 4:3 an. Netzwerk-Video kann das gleiche Verhältnis, aber auch andere Verhältnisse wie 16:9 anzeigen.

Der Vorteil eines Seitenverhältnisses von 16:9 besteht darin, dass unwichtige Details, die sich meist im oberen oder unteren Szenenbereich befinden, nicht Teil des Bilds sind. Anforderungen an Bandbreite und Speicherplatz können so reduziert werden.

Das Seitenverhältnis 9:16 ist einfach ein 16:9-Bild, das um 90° gedreht wurde. 9:16 wird häufig in der Videosicherheit eingesetzt, da das gesamte Sichtfeld der Kamera zur Überwachung schmaler Szenen wie z. B. von Ladengängen, Straßen, Schulfluren und Bahnsteigen genutzt werden kann. Dieses Seitenverhältnis wird mitunter als Corridor Format bezeichnet.



Seitenverhältnisse 4:3 und 16:9



Das Corridor Format wird häufig in Einzelhandelsbetrieben eingesetzt.

6. Videokomprimierung

Die meisten Anbieter von Netzwerk-Video verwenden heute standardisierte Komprimierungsverfahren, die Kompatibilität und Interoperabilität gewährleisten. Industriestandards sind vor allem für die Videosicherheit bedeutend, da das Videomaterial oft für viele unterschiedliche Zwecke genutzt wird und in einigen Fällen auch noch viele Jahre nach der Aufzeichnung verwendbar sein muss. Dank Technologien wie Axis Zipstream kann ein Überwachungssystem die Verwendung hochauflösender Kameras mit günstigen Systemkosten kombinieren und gleichzeitig den forensischen Wert des Videos erhalten. Dies liegt daran, dass unnötige Daten entfernt werden, wodurch die Speicheranforderungen niedrig gehalten werden, während die wichtigen Details und Bewegungen erhalten bleiben.

6.1 Grundlagen der Komprimierung

Bei der Videokomprimierung werden redundante Videodaten reduziert und entfernt, sodass digitale Videodaten effizient über ein Netzwerk übertragen und auf Computerfestplatten gespeichert werden können. Mit effizienten Komprimierungsverfahren kann eine deutliche Verkleinerung des Datenvolumens erzielt werden, ohne dass dabei die Bildqualität merklich beeinträchtigt wird. Wenn jedoch der Komprimierungsgrad eines bestimmten Komprimierungsverfahren zu stark erhöht wird, kann dies negative Auswirkungen auf die Qualität haben.

6.1.1 Video-Codec

Bei der Komprimierung wird das Quellvideo mit einem Algorithmus in eine komprimierte Datei umgewandelt, die übertragen oder gespeichert wird. Um die komprimierte Datei wiedergeben zu können, wird das Video mit dem umgekehrten Algorithmus dekomprimiert, um die Inhalte des ursprünglichen Quellvideos wiederherzustellen. Die zum Komprimieren, Übertragen, Dekomprimieren und Anzeigen der Datei erforderliche Zeit wird als Verzögerung bezeichnet. Je ausgereifter der Komprimierungsalgorithmus ist, desto länger dauert die Verzögerung. Ein zusammengehöriges Algorithmenpaar wird als Video-Codec (Encoder/Decoder) bezeichnet.

Video-Codecs unterschiedlicher Standards sind normalerweise nicht miteinander kompatibel, d. h. zur Komprimierung und Dekomprimierung der Videoinhalte muss der gleiche Standard verwendet werden. So funktioniert z. B. ein MPEG-4 Part 2-Decoder nicht in Kombination mit einem H.264-Encoder. Dies liegt einfach daran, dass ein Algorithmus nicht das Ergebnis eines anderen Algorithmus dekomprimieren kann. Es ist jedoch möglich, viele verschiedene Algorithmen in derselben Software oder Hardware zu implementieren, sodass verschiedene Formate parallel verwendet werden können.

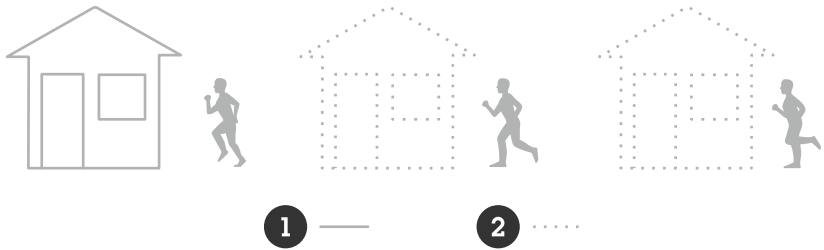
6.1.2 Vergleich zwischen Bild- und Videokomprimierung

Die verschiedenen Komprimierungsstandards nutzen unterschiedliche Methoden zur Datenreduzierung. Komprimierungsalgorithmen lassen sich in zwei Typen unterteilen: Bildkomprimierung und Videokomprimierung. Für die Bildkomprimierung wird die Intra-Frame-Codierung verwendet. Die Daten werden innerhalb eines Bildes reduziert, indem unnötige Informationen, die vom menschlichen Auge nicht wahrnehmbar sind, einfach entfernt werden. Motion JPEG ist ein Beispiel für einen solchen Komprimierungsstandard. Bilder in einer Motion JPEG-Sequenz werden als einzelne JPEG-Bilder codiert oder komprimiert.



Im Motion JPEG-Format werden die drei Bilder in der oben dargestellten Reihenfolge codiert und als separate, eigenständige und voneinander unabhängige Bilder übertragen.

Videokomprimierungsalgorithmen wie z. B. H.264, H.265 und AV1 verwenden eine Interframe-Vorhersage, um die Videodaten zwischen mehreren Bildern zu reduzieren. Dies umfasst Techniken wie die Differenzcodierung, bei der ein Bild mit einem zuvor gesendeten Referenzbild verglichen wird und nur die Pixel codiert werden, die sich im Vergleich zum Referenzbild geändert haben. Auf diese Weise wird die Anzahl der codierten und übertragenen Pixelwerte reduziert. Wenn eine solche codierte Sequenz angezeigt wird, erscheinen die Bilder wie in der Original-Videosequenz.



Bei der Differenzcodierung wird nur das erste Bild (I-Frame) vollständig codiert. In den beiden folgenden Bildern (P-Frames) wird auf statische Elemente im ersten Bild verwiesen, hier z. B. auf das Haus. Nur die beweglichen Teile, hier z. B. die laufende Person, werden codiert, so dass die Menge der zu übertragenden und zu speichernden Informationen reduziert wird.

1. Übertragen
2. Nicht übertragen

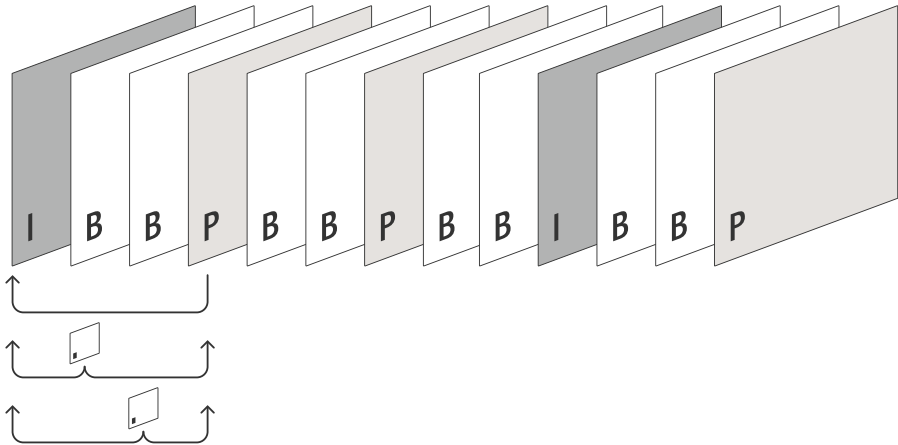
Es können weitere Techniken angewendet werden, um die Daten zusätzlich zu reduzieren. Beim blockbasierten Bewegungsausgleich wird z. B. berücksichtigt, dass ein großer Teil des neuen Bilds der Videosequenz möglicherweise in einem früheren Bild vorhanden ist, wenn auch an einer anderen Stelle. Bei dieser Methode wird ein Bild in mehrere Makroblöcke (Pixelblöcke) aufgeteilt. Ein neues Bild kann dann Block für Block zusammengesetzt oder durch die Suche nach einem übereinstimmenden Block in einem Referenzbild 'vorhergesagt' werden. Wenn eine Übereinstimmung gefunden wird, codiert der Encoder die Position des passenden Blocks im Referenzbild. Für das Codieren dieses sogenannten Bewegungsvektors sind weniger Bits erforderlich, als für das Codieren des tatsächlichen Blockinhalts.

Bei der Interframe-Vorhersage wird jedes Bild in einer Reihe von Bildern als ein bestimmter Bildtyp klassifiziert, z. B. als I-Frame, P-Frame oder B-Frame.

Ein I-Frame oder Intra-Frame ist ein unabhängiges Bild, das separat und ohne Verweis auf andere Bilder decodiert werden kann. Das erste Bild in einer Videosequenz ist immer ein I-Frame, der als Startpunkt für neue Viewer oder als Re-Synchronisationspunkt benötigt wird, falls der Bit-Stream beschädigt werden sollte. I-Frames können für Schnellvorlauf, Rücklauf und andere Zufallszugriffsfunktionen verwendet werden. Encoder fügen in regelmäßigen Abständen automatisch I-Frames ein. Dies gilt auch, wenn ein neuer Client die Wiedergabe des Streams beginnt. Der Nachteil der I-Frames besteht im größeren Bedarf an Bits. Andererseits generieren sie weniger Artefakte, die durch fehlende Daten entstehen.

P-Frames („Predictive Interframes“) verweisen auf Bildinformationen vorausgehender I- und/oder P-Frames. P-Frames erfordern ein geringeres Datenvolumen als I-Frames, sind jedoch aufgrund der Abhängigkeit von vorausgehenden P- und/oder I-Frames anfälliger gegen Übertragungsfehler.

B-Frames („Bi-predictive Interframes“) haben einen bidirektionalen Bezug und verweisen zugleich auf ein vorausgehendes und ein nachfolgendes Referenzbild. B-Frames erhöhen die Latenzzeit.



Typische Sequenz von I-, B- und P-Frames. P-Frames verweisen nur auf vorausgehende I- oder P-Frames, B-Frames ggf. auch auf nachfolgende I- oder P-Frames.

Wenn ein Decoder ein Video wiederherstellt, indem er den Bitstream Bild für Bild decodiert, muss er stets bei einem I-Frame beginnen. P- und B-Frames müssen ggf. zusammen mit ihren Referenzbildern decodiert werden.

Für die Videoprodukte von Axis können Benutzer über die GOP-Länge (Group of Pictures) festlegen, wie viele P-Frames vor einem weiteren I-Frame gesendet werden sollen. Durch das Verringern der I-Frame-Frequenz (größere GOP) kann die erforderliche Bitrate reduziert werden. Allerdings kann sich die Videoqualität durch verloren gegangene Netzwerkpakete verschlechtern, wenn das Netzwerk stark ausgelastet ist.

Neben der Differenzcodierung und dem Bewegungsausgleich können noch andere fortschrittliche Methoden eingesetzt werden, um die Datenmenge weiter zu reduzieren und die Videoqualität zu verbessern. H.264 und andere Videokomprimierungsstandards unterstützen fortschrittliche Techniken wie Vorhersageverfahren für die Codierung von I-Frames, einen verbesserten

Bewegungsausgleich bis hin zu einer Genauigkeit im Sub-Pixel-Bereich und einen In-Loop-Deblocking-Filter zur Glättung von Blockrändern (Artefakten).

6.2 Komprimierungsformate

Axis verwendet vier Videokomprimierungsstandards: H.264, H.265, AV1 und Motion JPEG. AV1 ist der neueste und fortschrittlichste Videokomprimierungsstandard mit einer sehr attraktiven Bitrate. MPEG-4 Teil 2 (einfach als MPEG-4 bezeichnet) wurde abgeschafft.

6.2.1 H.264

H.264, auch bekannt als MPEG-4 Part 10 oder ISO/IEC 14496-10 Advanced Video Coding, ist der MPEG-Standard für Video-Encoder. Es wurde gemeinsam von Standardisierungsunternehmen der Telekommunikationsbranche (Video Coding Experts Group der ITU-T) und der IT-Branche (ISO/IEC Moving Picture Experts Group) entwickelt.

H.264 ist der am weitesten verbreitete Standard und mit einer Vielzahl von Betriebssystemen, Software und mobilen Clients kompatibel. H.264 hat dazu beigetragen, die Einführung von Megapixel-/HDTV-Kameras zu beschleunigen, da die hocheffiziente Komprimierungstechnologie die großen Dateigrößen und Bitraten reduzieren kann, ohne die Bildqualität zu beeinträchtigen.

H.264 ist zwar immer noch eine verlässliche Wahl für die Komprimierung von Videos, wurde aber vor über zwei Jahrzehnten eingeführt und ist nicht mehr der Standard mit der besten Bitrate. Die veraltete Technologie kann den wachsenden Anforderungen an die Videoübertragung und -speicherung in hoher Auflösung nicht gerecht werden, und H.264 unterstützt keine Videos, die breiter als 8K sind.

Das Baseline-Profil für H.264 verwendet nur I- und P-Frames, während das Main-Profil zusätzlich auch B-Frames verwenden kann. Ohne B-Frames ist die Latenz geringer. Die Videoprodukte von Axis verwenden das H.264 Baseline- oder Main-Profil. Für Videoprodukte mit leistungsfähigeren Prozessoren verwendet Axis das Main-Profil ohne B-Frames, um eine höhere Komprimierung und gleichzeitig eine geringere Verzögerung bei gleichbleibender Videoqualität zu erzielen.

6.2.2 H.265

H.265 ist der von der ITU genehmigte Standard für hocheffiziente Videokodierung, ISO/IEC 23008-5. Im Vergleich zu H.264 verbessert H.265 die Komprimierung um 15–40 % bei gleicher Videoqualität. Der Standard ist für höhere Videoauflösungen, größere Bildraten und mehr Bewegung ausgelegt.

Die H.265-Kodierung erfüllt noch nicht vollständig die Anforderungen der Videosicherheit. Die meisten Überwachungsgeräte unterstützen H.265, jedoch sind die Unterstützung für Decoder und den Browser eingeschränkt. Viele Benutzer müssen weiterhin H.264 verwenden, um Videos auf ihren bevorzugten Clients ansehen zu können, aber das sollte kein Problem sein, da Zipstream mit H.264 sehr bitrateneffizient ist. Der neuere Standard AV1 wird wahrscheinlich H.265 als bevorzugten Nachfolger von H.264 herausfordern, da AV1 im Vergleich zu H.265 eine bessere Leistung aufweist und von der Industrie breit unterstützt wird.

6.2.3 AV1

AV1 ist ein moderner Video-Encoder-Standard, der für die Videoübertragung über das Internet optimiert ist. AV1 bietet hochauflösende, problemlose und kosteneffiziente Videostreams und Speicher.

AV1 dürfte dank seiner niedrigen Bitrate, neuer Merkmale und breiter Client-Decoder-Unterstützung der dominierende Codec in der Videosicherheitsbranche werden. Es wird bereits von den wichtigsten Browsern, Betriebssystemen, Cloud-Plattformen und mobilen Geräten unterstützt.

AV1 wurde in der Alliance for Open Media (AOM) als *AOMedia Video 1 Videocodierung* gemäß *AV1 Bitstream & Decoding Process Specification v1.0.0* von aomedia.org standardisiert. Die AOM wurde von den wichtigsten IT-Unternehmen der Welt gegründet und AV1 ist frei und ohne Lizenzgebühren an AOM zugänglich.

AV1 hat in der gesamten IT-Industrie breite Unterstützung gefunden. Es wird häufig in Cloud-Streaming-Technologien wie WebRTC verwendet, die eine effiziente Echtzeitkommunikation und Videostreams aktivieren. Die nahtlose Integration in die Cloud ermöglicht es Entwicklern, Sicherheitsvideos direkt in IT-Anwendungen, z. B. in Logistiksystemen, einzusetzen, um die Geschäftsentelligenz und die Betriebseffizienz zu verbessern.

6.2.4 Zipstream für H.264, H.265 und AV1

Die Standards H.264, H.265 und AV1 definieren zwar eindeutig die Bitstream-Syntax und den Dekodierungsprozess, schreiben jedoch keinen bestimmten Komprimierungsalgorithmus vor. Diese Flexibilität ermöglicht die Entwicklung fortschrittlicher, standardkonformer Encoder wie der Axis Zipstream-Technologie. Sie steigert die Effizienz deutlich und gewährleistet gleichzeitig eine reibungslose Wiedergabe mit jedem standardkonformen Decoder.

Zipstream ist speziell für die Videoüberwachung optimiert und arbeitet mit dem zugrunde liegenden Videocodec zusammen, um den Bandbreiten- und Speicherbedarf im Durchschnitt um 50 % oder mehr zu reduzieren. Wichtige Bilddetails bleiben im Videostream in voller Auflösung

erhalten, während nicht relevante Daten weggelassen werden. Zipstream wird ständig um weitere dynamische Funktionen erweitert.

Zipstream ist eine Sammlung verschiedener Algorithmen zur Reduzierung der Bandbreite:

- > **Algorithmus für veränderlichen Beobachtungsbereich (RIO).** Automatisches Verfahren mit voller Bildfrequenz, um wichtige Bereiche auszuwählen und die Größe aller Bilder zu reduzieren.
- > **Algorithmus für veränderliche Bilder/s (FPS).** Zusätzliche Methode zur Reduzierung der Bildrate, um den für P-Frames benötigten Speicherplatz zu reduzieren.
- > **Algorithmus für Dynamic Group of Pictures (GOP).** Zusätzliche Methode zur Änderung der GOP-Länge, um die für I-Frames benötigte Speichermenge zu reduzieren.

Zipstream passt den komprimierten Videostream dynamisch an die Bewegung und den Inhalt der Szene, die Umgebungshelligkeit sowie an Konfigurationseinstellungen wie Komprimierungsparameter, Bildrate und den eingestellten Zipstream-Stärkegrad an.

Die einzelnen Komponenten des Zipstream-Algorithmus lassen sich individuell konfigurieren. Alternativ können Sie das Speicherprofil verwenden, das Zipstream automatisch für eine speicheroptimierte Videokomprimierung konfiguriert.

- > **Klassisches Profil:** Das Standardprofil, mit dem Sie einen Großteil des Zipstream-Algorithmus gezielt steuern können. Ab Werk ist die Stärke auf „niedrig“ festgelegt, und die dynamische GOP und die dynamischen FPS sind deaktiviert. Diese Einstellung ist mit allen Anwendungen kompatibel. Die Bitrate wird dabei weiterhin reduziert. Für eine weitere Reduzierung der Bitrate können Sie eine höhere Zipstream-Stufe wählen und Dynamic GOP und/oder Dynamic FPS aktivieren.
- > **Speicherprofil:** Mit diesem Profil wird Zipstream so konfiguriert, dass das Video für die Speicherung und den späteren Zugriff optimiert wird, wofür Axis Videoprodukten hauptsächlich eingesetzt werden. Das Speicherprofil minimiert die Bitrate, aber maximiert den Wert als Beweismittel für den betreffenden Einsatzzweck. Im Speicherprofil ruft die Kamera automatisch den Zipstream-Algorithmus auf, der sich für die betreffende Kamera am besten eignet, und nutzt fortschrittlichere Tools zur Videocodierung. Das Profil unterscheidet sich je nach Kamera, abhängig der jeweiligen Funktionen. Ebenso kann auch das Ergebnis bei unterschiedlichen Kamertypen anders ausfallen.

6.2.5 Motion JPEG

Motion JPEG oder MJPEG ist eine digitale Videosequenz, die aus einer Reihe von einzelnen JPEG-Bildern erstellt wird. Da es keine Abhängigkeit zwischen den Bildern gibt, ist ein Motion JPEG-Video weniger anfällig gegen Übertragungsfehler, d. h. wenn ein Bild während der Übertragung verloren

geht, wird der Rest des Videos davon nicht beeinträchtigt. Motion JPEG ist ein lizenzfreier Standard. Dank seiner breiten Kompatibilität eignet sich das Format auch für die Integration in Systeme, die ausschließlich Motion JPEG unterstützen. Darüber hinaus wird es häufig in Anwendungen eingesetzt, bei denen einzelne Bilder einer Videosequenz benötigt werden – beispielsweise für Videoanalysen – sowie in Anwendungen mit niedrigen Bildraten, etwa in der Übersichtsansicht eines Video-Management-Systems (VMS).

Motion JPEG kann keine Videokomprimierungsverfahren verwenden, um Daten zu reduzieren, da es sich um eine Reihe vollständiger Einzelbilder handelt. Dies führt im Vergleich zu anderen Videokomprimierungsstandards zu einer relativ hohen Bitrate oder einem niedrigen Komprimierungsverhältnis für die gelieferte Qualität.

Für Videoprodukte mit einer Auflösung von mehr als 1080p kann Motion JPEG möglicherweise nicht verwendet werden, da die Bilder zu groß für eine Übertragung bei vollständiger Bildrate in einem 100 Mbit/s-Netzwerk werden können. Ein Upgrade auf ein Gigabit-Netzwerk verlagert den Engpass lediglich auf die Bildverarbeitungsschritte in der Kamera vor und nach der Übertragung im Netzwerk. Zudem ist die Nutzbarkeit stark eingeschränkt. Wenn JPEG-Bilder erforderlich sind, muss die Bildrate des Systems entsprechend verringert werden.

6.2.6 JPEG

Standbilder folgen dem JPEG-Standard, der von allen Kameras unterstützt wird. Standbilder werden gelegentlich in Videokameras als Symbole oder für die Übersicht verwendet.

6.3 Durchschnittliche, variable und maximale Bitraten

H.264, H.265 und AV1 können so konfiguriert werden, dass codierte Videostreams mit einer durchschnittlichen, variablen oder maximalen Bitrate verwendet werden. Welche Auswahl am besten geeignet ist hängt von der Anwendung und der Netzwerkinfrastruktur ab.

Mit ABR (Average Bitrate, durchschnittliche Bitrate) wird über einen bestimmten Zeitraum eine bestimmte Menge an Speicherplatz verwendet. Einem Videostream wird eine bestimmte Menge an Speicher zugewiesen, und der ABR-Controller der Kamera passt die Videoqualität an, um sicherzustellen, dass das Video aus dem gesamten Zeitraum in das Bitrate-Budget passt. Ungenutzter Speicher aus früheren, inaktiveren Zeiträumen kann für die Aufrechterhaltung einer hohen Videoqualität in späteren, aktiveren Zeiträumen verwendet werden, und das Bitrate-Budget wird eingehalten. Damit soll die Videoqualität verbessert und gleichzeitig ein Überschreiten der Speichergrenzen des Systems vermieden werden. ABR ist optimal für kontinuierlich aufgezeichnete Videostreams ohne geplante Pausenzeiten.

Bei einer variablen Bitrate (VBR) lässt sich unabhängig davon, ob eine Szene Bewegungen enthält, ein vordefinierter Grad an Bildqualität aufrechterhalten. Dies bedeutet, dass mehr Bandbreite benötigt wird, wenn eine Szene viele Aktivitäten aufweist, und weniger Bandbreite, wenn keine Bewegung stattfindet. Dies ist häufig für Videosicherheit mit hohem Qualitätsbedarf wünschenswert, besonders bei bewegten Szenen. Da sich die Bitrate ändern kann, muss die Netzwerkinfrastruktur (verfügbare Bandbreite) selbst dann für einen hohen Durchsatz ausgelegt sein, wenn eine durchschnittlich zu erzielende Bitrate definiert wurde.

Wenn die zur Verfügung stehende Bandbreite begrenzt ist, bietet sich eine maximale Bitrate (MBR) an. Hierbei wird ein Grenzwert für die maximal zulässige Bitrate definiert. Es besteht jedoch der Nachteil, dass beispielsweise bei vermehrter Aktivität in einer Szene, die zu einer Bitrate oberhalb des zulässigen Werts führt, aufgrund der begrenzten Bitrate Bildqualität und Bildrate beeinträchtigt werden. Mit Videoprodukten von Axis kann der Benutzer die Priorität auf Bildqualität oder Bildrate legen, wenn die Bitrate den festgelegten Grenzwert überschreitet.

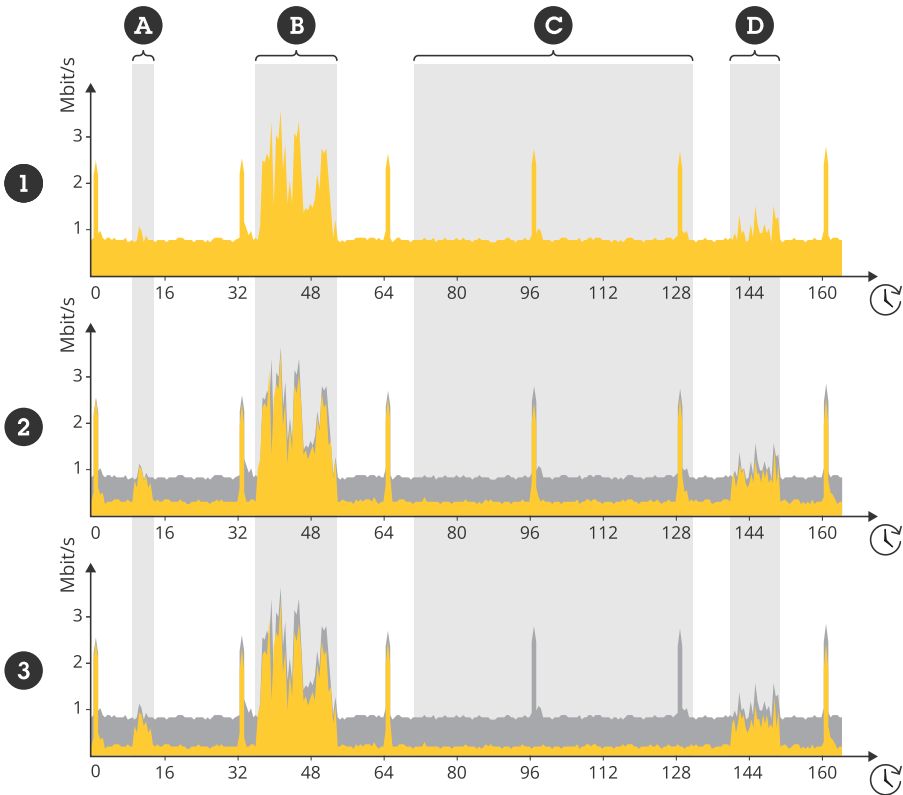
6.4 Standards im Vergleich

Beim Vergleich der Leistung von Videokomprimierungsstandards muss beachtet werden, dass die Ergebnisse für verschiedene Encoder variieren können, auch wenn sie denselben Standard verwenden. Dies liegt daran, dass jeweils verschiedene Teile der Standards implementiert werden können. Solange die Ausgabe eines Encoders mit dem Standardformat und dem Decoder übereinstimmt, können unterschiedliche Implementierungen umgesetzt werden. Dies trägt zur Optimierung der Technologie und zu weniger komplexen Implementierungen bei.

Es bedeutet jedoch auch, dass ein Standard keine bestimmte Bitrate oder Bildqualität gewährleisten kann. Zudem können Vergleiche erst dann durchgeführt werden, wenn zuvor definiert wurde, wie die Standards in einem Encoder implementiert werden.

Anders als beim Encoder müssen im Decoder alle erforderlichen Bestandteile eines Standards implementiert sein, damit ein konformer Bitstream decodiert werden kann. Daher ist letztlich nur der Decoder standardisiert. Ein Standard legt genau fest, auf welche Weise ein Dekomprimierungsalgorithmus die einzelnen Bits des komprimierten Videos wiederherstellt. Wenn die Videoqualität von Bedeutung ist, sollten verschiedene Produkte getestet werden, um sicherzustellen, dass die Qualität für den Zweck geeignet ist.

Ausgehend von einer identischen Bildqualität werden in der folgenden Abbildung die Bitrate von H.264 und dem verbesserten H.264 von Axis (Axis Zipstream) bei geringer und hoher Leistung verglichen.



Momentane Bitrate (gelb) und Reduzierung der Bitrate (dunkelgrau).

1. Zipstream ausgeschaltet.
2. Zipstream-Stärke: niedrig. Die Bitrate (gelb) ist deutlich gesunken.
3. Zipstream-Stärke: hoch. Die Bitrate (gelb) ist sogar noch geringer.

Alle Streams sind Streams mit variabler Bitrate (VBR) und einer GOP-Länge von 32. Jede Aktualisierung eines I-Frames ist deutlich als Ausschlag in der Bitrate zu erkennen.

Die Buchstaben A–D in der Abbildung kennzeichnen Zeitabschnitte im Video, in denen unterschiedliche Typen von Bewegungen auftreten. Zipstream funktioniert je nach den Bedingungen im jeweiligen Zeitintervall unterschiedlich.

- > *A. Zeitintervall mit geringer und kurzzeitiger Bewegung im Video. Der dynamische ROI-Algorithmus erkennt Bereiche im Bild mit Bewegung, sodass auf diese Region von Interesse eine geringere Komprimierung angewendet wird.*
- > *B. Zeitabschnitt mit ausgeprägter und länger anhaltender Bewegung. Für diese Video-Sequenz ist eine höhere Bitrate erforderlich. Dennoch wird die Bitrate weiterhin reduziert, da mithilfe des dynamischen ROI-Algorithmus nicht priorisierte Bildinformationen weggelassen werden können.*
- > *C. Zeitintervall ohne Bewegung. Der Dynamic Group of Pictures-Algorithmus kann hier eine höhere Anzahl von P-Frames zulassen und dadurch unnötige I-Frame-Aktualisierungen verhindern.*
- > *D. Zeitabschnitt mit leichter, aber lang anhaltender Bewegung. Die Aufzeichnung der Bewegung erfolgt wie erwartet, und die Anzahl der P-Frames normalisiert sich wieder.*

Mit AXIS Site Designer können Bitraten für verschiedene Szenentypen geschätzt werden.

7. Audio

Die Nutzung der Audiofunktionen in Verbindung mit einem Videoüberwachungssystem eröffnet wertvolle Möglichkeiten zur Erkennung und Interpretation von Ereignissen und Notfällen. Die Audioanalyse kann den Audioeingang überwachen und auf relevante Geräusche reagieren. Wenn Sie das System mit Netzwerk-Lautsprechern kombinieren können Sie einfach mit Besuchern kommunizieren oder Eindringlinge warnen.

7.1 Audioerfassung

Die Audioerfassung kann als eigenständige Technologie eingesetzt werden, die ein direktes Eingreifen des Bedieners ermöglicht, wie zum Beispiel Abspielen einer Audionachricht oder Entsenden von Sicherheitspersonal zur Überprüfung eines Ereignisses. In einem Krankenhaus oder einer Pflegeeinrichtung kann die Audioerfassung dazu beitragen, dass jemand aufmerksam wird, wenn ein Patient sich unwohl fühlt und eine Krankenschwester benötigt. Die Audioerfassung kann auch erkennen, ob das Geräusch von links oder rechts kam, und eine PTZ-Kamera auf das betreffende Ereignis ausrichten.

In Verbindung mit der Videosicherheit bietet Audio eine weitere Dimension von Informationen für die Entscheidungsfindung und kann bestehende Videosicherheitsanlagen sinnvoll ergänzen. Beispielsweise können Mitarbeitende Situationen deutlich besser einschätzen, wenn der Videostream um zusätzliche Audioinformationen ergänzt wird.

7.1.1 Geräte und Technologien für audiobasierte Konnektivität

Es gibt verschiedene Möglichkeiten zur Implementierung der Audioerfassung in einer Kamera.



Eine Kamera mit integrierten Mikrofonen und Lautsprecher, ein eigenständiges digitales Mikrofon sowie eine Audio- und I/O-Schnittstelle mit Portcast-Technologie.

Integriertes Mikrofon: Mit integrierten Mikrofonen können Audiofunktionen wie z. B. der Sprachoptimierer auf das jeweilige Kameramodell und dem beabsichtigten Einsatz zugeschnitten werden. Mit zwei integrierten Mikrofonen kann eine Kamera Stereosound liefern, wodurch erkennbar wird, aus welcher Richtung die Töne kommen. Mit drei oder mehr integrierten Mikrofonen erhält die Kamera noch detailliertere räumliche Informationen. Dies kann für die automatische Lokalisierung von Audioquellen oder für das Beamforming verwendet werden, eine Methode zum „Heranzoomen“ von Audio, das aus einer bestimmten Richtung kommt.

Integrierte Audiounterstützung und eigenständiges Mikrofon: Kameras verfügen häufig über eine 3,5-mm-Buchse z. B. zum Anschließen eines separaten Mikrofons. Separate Mikrofone können an strategisch günstigen Positionen angeordnet werden, um klare und relevante Geräusche zu erkennen. Wenn für eine gute Übersicht eine Kamera oben an einer Wand oder an einer Decke angebracht werden muss, kann ein kleines, separates Mikrofon unauffällig auf der Höhe, auf der sich Personen befinden, platziert werden. Bei Anschluss mithilfe eines digitalen Audioerweiterungssets kann ein digitales Mikrofon das Audiosignal ohne Verlust über ein Netzkabel bis zu 100 m weit übertragen.

Edge-to-Edge-Technologie: Ein Mikrofon kann mithilfe der Edge-to-Edge-Technologie gekoppelt werden, wenn sich beide Geräte im selben Netzwerk befinden und deren Software Edge-to-Edge unterstützt. Nach der Koppelung können die Audioeinstellungen des Mikrofons über die Benutzeroberfläche der Kamera gesteuert werden, selbst wenn die Kamera ursprünglich kein Audio unterstützt.

Audio- und E/A-Schnittstelle mit Portcast: Bei der Portcast-Technologie handelt es sich um ein einzigartiges Konzept von Axis, bei dem Audio- und E/A-Schnittstellengeräte über ein Netzkabel direkt an die Kamera angeschlossen werden. Damit kann Kameras, die selbst kein Audio unterstützen, die Fähigkeit zur Zwei-Wege-Kommunikation hinzufügen. Das Portcast-Gerät nutzt die IP-Adresse der Kamera, wird über die Kamera gesteuert und ermöglicht der Kamera die

Bereitstellung von Anschlussmöglichkeiten über Audio und E/A mit Video in einem Stream über das Netzwerk. Einige Portcast-Geräte verfügen über ein integriertes Mikrofon.

Anschlusshub: Dieses Gerät erweitert Ihr System um audiobasierte Funktionen, darunter Zwei-Wege-Kommunikation und eine hohe Mikrofonkompatibilität. Der Anschlusshub verfügt über eine eigene IP-Adresse und über mehrere Ein-/Ausgänge sowie Ports zur Integration verschiedener nicht visueller Sensoren.

7.1.2 Verbesserungen bei der Audioerfassung

Geräte mit Audioerfassungsfunktionen verbessern mithilfe verschiedener Erweiterungen den Ton.

- > **Sprachoptimierer:** Verstärkt Sprachinhalte gegenüber anderen Tönen, um Sprache besser wahrnehmbar zu machen.
- > **Automatische Verstärkungsregelung:** Passt die Verstärkung dynamisch an Klangänderungen an.
- > **Echounterdrückung:** Erkennt und entfernt Töne, die durch den integrierten Lautsprecher erzeugt werden.
- > **Grafik-Equalizer:** Damit können fortgeschrittene Benutzer bestimmte Audiofrequenzen herausfiltern.

7.1.3 Audioanalyse

Genauso wie verschiedene Typen der Videoanalyse für automatische Alarmmeldungen auf Basis visueller Erkennung eingesetzt werden können, kann die Audioanalyse auf relevante Geräusche reagieren. Auf der Grundlage der Audioerfassung und KI-basierten Klassifizierung kann die Audioanalyse spezifische Geräusche wie Schreie oder Glasbruch erkennen und sofort wertvolle Informationen liefern. Das ermöglicht eine frühzeitige Warnung und eine schnellere Reaktion. Mithilfe der Audioanalyse kann eine PTZ-Kamera (Schwenken/Neigen/Zoomen) automatisch auf ein hörbares Ereignis ausgerichtet oder die Lärmbelastung gemessen werden, um eine Umgebung mit ungefährlichen Geräuschpegeln zu gewährleisten und die Einhaltung von Vorschriften sicherzustellen.

In der Regel erfolgt bei der Audioanalyse keine dauerhafte Übertragung oder Aufzeichnung von Ton. Stattdessen puffern und analysieren sie kurze Audio-Segmente auf Muster oder Frequenzänderungen und präsentieren das Ergebnis als Metadaten. Außerdem können Systeme so konfiguriert werden, dass sie zur Überprüfung oder für forensische Zwecke einen kurzen Abschnitt vor und nach einem erkannten Ereignis speichern.

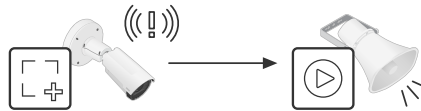
7.2 Audio-Ausgang

Durch die Erweiterung eines Videosicherheitssystems um IP-basierte Lautsprecher können Sie Verbrecher proaktiv abschrecken, indem Sie sofort per Fernzugriff mit aufgezeichneten oder Live-Meldungen reagieren. Die Lautsprecher können auch in einem Mehrzweckaudiosystem eingesetzt werden, das Abschreckung, Informationen, Sicherheitsmeldungen und Hintergrundmusik in einer einzigen Installation ermöglicht.

7.2.1 Audioausgang zur Videosicherheit

Viele Kameras verfügen über eine integrierte Audiofunktion und einen Audioausgangsanschluss zum Anschließen eines Lautsprechers. Eine Kamera, die Edge-to-Edge-Technologie unterstützt, kann jedoch auch mit einem Lautsprecher gekoppelt werden, wenn die Kamera über keine Audio- oder Audioausgangsfunktion verfügt. Nach der Koppelung können die Audioeinstellungen über die Benutzeroberfläche der Kamera gesteuert werden. Viele Kameras können auch über einen Anschlusshub oder eine Audio- und E/A-Schnittstelle an Lautsprecher angeschlossen werden.

Eine Sicherheitslösung mit Audio und Video ist sowohl mit als auch ohne Überwachung möglich und bietet verschiedene Grade der Kameraintegration.



Unüberwachte Lösung: Eine Kamera mit Analysefunktionen erkennt unbefugtes Betreten oder andere Ereignisse in einem eingeschränkten Bereich und sendet den Befehl an einen Lautsprecher, eine zuvor aufgezeichnete Durchsage wiederzugeben.



Überwachte Lösung: Eine Kamera mit Analysefunktionen erkennt unbefugtes Betreten oder andere Ereignisse und sendet eine Benachrichtigung an einen Bediener. Der Bediener kann live sprechen oder eine voraufgezeichnete Audio-Nachricht abspielen.

Die Kameras können auch mit Audio- und visuellen Alarmen wie z. B. einer Sirene verbunden werden. Es handelt sich um ein voll vernetztes Gerät, das zur Abschreckung von Eindringlingen oder zur Verbesserung der Betriebseffizienz mithilfe von Blitzlicht und Sirenenalarms verwendet werden kann. Es lässt sich mit unterschiedlichen Weiß- und RGBA-Lichtmustern sowie

vorkonfigurierten Tönen anpassen. Eine Blitzsirene ist besonders wertvoll, wenn sie an eine Kamera mit Perimeterschutz oder Nummernschilderkennungs(LPR)-Analyse angeschlossen ist.

7.2.2 Netzwerk basierte Audiosysteme für Durchsagen

Netzwerk basierte Lautsprecher und andere Audiogeräte können zu einem IP-basierten System für Live- und aufgezeichnete Durchsagen, Sicherheitsansagen und Hintergrundmusik kombiniert werden. Durch den Einsatz von IP-Technologie ist das System flexibel und skalierbar. Zudem wird damit die Integration in andere Systeme vereinfacht, da die Lautsprecher direkt in eine VMS- oder VoIP(Voice over IP)-Telefonanlage integriert werden können.

Axis Netzwerk-Lautsprecher sind vollständige, hochwertige Audiosysteme mit integriertem Verstärker und digitalem Signalprozessor für vorkonfigurierte Töne. Zur Gewährleistung einer optimalen Klangqualität verfügen sie über ein integriertes Mikrofon für Zwei-Wege-Kommunikation und automatische Selbstüberprüfungen.



Die Lautsprecher von Axis sind in verschiedenen Größen, Schalldruck und Montagemöglichkeiten für verschiedene Einsatzmöglichkeiten erhältlich.

Audioinhalte und Geräte werden mithilfe der Audio Management Software verwaltet. Die gesamte Audiohardware von Axis verfügt über integrierte Software für den Basiseinsatz in kleinen und mittelgroßen Systemen. Axis verfügt zudem über Softwareoptionen für größere und erweiterte Systeme, einschließlich standortübergreifender Systeme mit Tausenden von Standorten. Mit einer Audio Management Software kann jeder Lautsprecher einzeln adressiert werden. Die Lautsprecher können zudem in Zonen gruppiert werden, damit Sie Durchsagen an ein bestimmtes Publikum in den entsprechenden Bereichen des Standorts richten können, ohne die Meldung im gesamten

Lautsprechernetz durchgeben zu müssen. Die Zonen können ebenso schnell wie mühelos und ohne erneutes Verkabeln neu konfiguriert werden. Aufgezeichnete Nachrichten und Hintergrundmusik können geplant, und die Funktionen des Systems werden automatisch überwacht.

Mehr zu netzwerkbasierten Audiosystemen erfahren Sie im technischen Leitfaden zu netzwerkbasierendem Audio, der auf axis.com/learning/technical-guides heruntergeladen werden kann.

7.3 Audio-Kommunikationsmodi

Je nach Anwendung müssen Audiosignale nur in eine Richtung oder in beide Richtungen gesendet werden. Dies bezieht sich auf drei grundlegende Modi für die Audiokommunikation:

- > **Simplex** bedeutet, dass die Audiodaten nur in eine Richtung übertragen werden können. Beim Netzwerk-Audio werden Audiodaten in der Regel vom Bediener an einen Lautsprecher gesendet, z. B. um Warnungen oder Durchsagen über den Lautsprecher zu kommunizieren. Im Simplex-Modus können die Audiodaten jedoch stattdessen vom Lautsprecher an den Bediener gesendet werden, z. B. in Fernüberwachungssituationen, in denen Live-Audio von einem überwachten Standort über ein Netzwerk gesendet wird.
- > **Halbduplex** bedeutet, dass die Audiodaten in beiden Richtungen übertragen und empfangen werden können, jedoch immer nur in jeweils eine Richtung gleichzeitig. Die Richtung wird entweder über eine physische Sprachtaste oder durch eine Spracherkennungssoftware gesteuert. Dieser Kommunikationsmodus ist mit einem Walkie-Talkie-Gespräch vergleichbar. Da Lautsprecher und Mikrofon nie gleichzeitig aktiv sind, bestehen beim Halbduplex-Betrieb keine Echoprobleme.
- > **Vollduplex** bedeutet, dass die Benutzer Audiodaten gleichzeitig senden und empfangen (zuhören und sprechen) können. Dieser Kommunikationsmodus ist mit einem Telefongespräch vergleichbar. Für Vollduplex müssen sowohl der Client (PC, SIP-Mikrofon oder VoIP-Telefon) als auch der Lautsprecher Vollduplex-Audio verarbeiten können. Um Echoeffekte zu vermeiden, muss die Implementierung auch die akustische Echounterdrückung (AEC) unterstützen.

Die Audiogeräte von Axis sind für 2-Wege-Audio mit Halb- oder Vollduplex-Betrieb geeignet.

7.4 Audiocodecs

Ein Audio-Codec (Encoder-Decoder) ist ein Softwaresystem, mit dem Daten für die Übertragung digitalisiert und komprimiert und die empfangenen Daten dekomprimiert werden können. Axis Produkte unterstützen verschiedene Audio-Codecs, zum Beispiel:

AAC-LC (Advanced Audio Coding – Low Complexity), auch bekannt als MPEG-4 AAC, für das eine Lizenz erforderlich ist. AAC-LC, insbesondere bei einer Abtastrate von 16 kHz oder höher und einer Bitrate von 64 KBit/s oder mehr, ist der empfohlene Codec, wenn es auf die bestmögliche Audioqualität ankommt.

G.711 und **G.726** sind lizenzfreie ITU-T-Standards. Sie haben eine geringere Verzögerung und benötigen weniger Rechenleistung als AAC-LC. G.711 und G.726 sind Sprachcodecs mit einer geringen Audioqualität, die hauptsächlich in der Telefonie eingesetzt werden. Beide haben eine Abtastrate von 8 kHz. G.711 hat eine Bitrate von 64 KBit/s. Die G.726-Implementierung von Axis unterstützt 24 und 32 KBit/s. Bei G.711 unterstützen die Axis Produkte nur μ -law, einen der beiden Komprimierungsalgorithmen des G.711-Standards. Bei der Verwendung von G.711 muss auch der Client die μ -law-Komprimierung verwenden.

Axis Kameras unterstützen außerdem LPCM. Axis Produkte, die SIP unterstützen, können zusätzlich auch Opus, L16/16000, L16/8000, speex/8000, speex/16000 und G.726-32 verwenden.

7.5 Audio- und Videosynchronisierung

Die Synchronisierung der Audio- und Videodaten erfolgt über einen Mediaplayer oder ein Multimedia-Framework wie WebRTC.

Die Audio- und Videodaten werden als zwei separate Paketstreams über das Netzwerk übertragen. Damit ein Client oder Player die Audio- und Videostreams perfekt synchronisieren kann, müssen die Audio- und Videopakete mit einem Zeitstempel versehen sein. Das Versehen von Videopaketen mit Zeitstempeln mithilfe der Motion JPEG-Komprimierung wird nicht von allen Netzwerk-Kameras unterstützt. Wenn dies der Fall ist, jedoch synchronisierte Video- und Audiodaten benötigt werden, muss als Videoformat H.264, H.265 oder AV1 ausgewählt werden, da die Videostreams zusammen mit den Audiostreams mit RTP (Real-time Transport Protocol) gesendet werden. Dieses Protokoll versieht die Video- und Audiodaten mit einem Zeitstempel. Es gibt jedoch viele Situationen, in denen eine Audiosynchronisierung nicht wichtig oder sogar unerwünscht ist (z. B. wenn der Ton überwacht aber nicht aufgezeichnet werden soll).

8. Radar

Radargeräte sind ideal für die Überwachung großer Flächen oder den Einsatz in der Verkehrsüberwachung. Sie können eigenständig eingesetzt werden, beispielsweise wenn eine Kamera aus Datenschutzgründen nur eingeschränkt einsetzbar ist, aber sie lassen sich auch leicht in ein Überwachungssystem integrieren. Einige Radargeräte unterstützen die Radar-Video-Fusion. Diese liefert umfangreichere Daten, ermöglicht eine erweiterte automatische Objektverfolgung und sorgt für zuverlässigere Alarme.

8.1 Eine nicht-visuelle Technologie als Ergänzung der Videosicherheit

Radar ist eine nicht visuelle Technologie, die sich in vielen Situationen zuverlässig zeigt, in denen andere Überwachungstechnologien unzureichend sind. Radar erfasst Bewegungen mit elektromagnetischen Wellen und ist gegenüber Objekten, die üblicherweise Fehlalarme auslösen, wie etwa sich bewegende Schatten oder Lichtkegel, Regentropfen oder Insekten, unempfindlich. Die von Axis Radargeräten ausgesendeten elektromagnetischen Wellen sind selbst bei kontinuierlicher Exposition ungefährlich, sodass Sie sich ohne Bedenken in ihrer Nähe aufhalten können¹. Radargeräte funktionieren zuverlässig bei allen Lichtverhältnissen und rund um die Uhr.

Darüber hinaus liefern Radargeräte wichtige Informationen über erkannte Objekte, die mit Videokameras nicht ermittelt werden können – etwa die exakte Position sowie die Geschwindigkeit und Bewegungsrichtung. Analysefunktionen zur Erkennung, Verfolgung und Klassifizierung von Objekten sind in das Radargerät integriert.

¹ Nach Berechnungen gemäß den ICNIRP-Richtlinien zur Begrenzung der Exposition durch elektromagnetische Felder liegt die Sendeleistung von Axis Radargeräten selbst in einem Zentimeter Abstand vom Radar unter dem medizinisch schädlichen Wert.

8.2 Radargeräte



Radargeräte für die Flächen- und Verkehrsüberwachung, eine Kamera mit integrierter Radar-Video-Fusion sowie ein Radargerät, das sich mit einer ausgewählten PTZ-Kamera kombinieren lässt, um eine Radar-Video-Fusion zu realisieren.

Dank der integrierten Analysefunktionen kann ein Axis Radargerät Personen und Fahrzeuge präzise erfassen, klassifizieren und verfolgen. Seine Erfassungsprofile sind für verschiedene Szenarien optimiert.

Das Profil zur Bereichsüberwachung erfasst Personen und Fahrzeuge mit geringer Geschwindigkeit. Mit aktiviertem Profil bietet das Radargerät einen zuverlässigen Rund-um-die-Uhr-Schutz für weitläufige Bereiche bei einer geringen Fehlalarmrate. Es eignet sich ideal für offene Außenbereiche mit Aktivität, wie z. B. Industrieanlagen oder die Überwachung von Parkplätzen und Laderampen nach Geschäftszeiten.

Das Profil zur Straßenüberwachung erfasst Fahrzeuge mit höheren Geschwindigkeiten. Mit diesem Profil wird die Geschwindigkeit von Fahrzeugen für die Überwachung des Verkehrsflusses erfasst und gemessen. Wenn AXIS Speed Monitor im Radargerät oder in einer angeschlossenen Kamera installiert ist, können Sie ganz einfach Statistiken extrahieren, die fundiertere Entscheidungen ermöglichen. Geschwindigkeiten werden in der Live-Ansicht des Radargeräts oder der Kamera visualisiert.

Eine Radar-Video-Fusionskamera vereint zwei Technologien in einem Gerät: eine Kamera mit hervorragender Bildqualität und ein vollständig integriertes Radarsystem. Das integrierte Radarsystem erkennt Objekte zuverlässig auch bei Dunkelheit oder schlechten Lichtverhältnissen und zeigt Geschwindigkeit sowie Entfernung bewegter Objekte direkt in der Anwendungsansicht an. Die Kombination von Video- und Radaranalyse liefert vollständigere Daten mit einer verbesserten Szenenerkennung in Verbindung mit dem forensischen Wert von Videos. Je nach Bedarf können Sie Aktionen auslösen, die nur auf der Erkennung durch Radar, nur durch die Kamera oder durch beides basieren.

Die neuesten Radargeräte von Axis bieten einen großen Erfassungsbereich und lassen sich flexibel als eigenständige Lösung oder in Kombination mit weiteren Geräten einsetzen. Die Integration ausgewählter PTZ-Kameras ermöglicht eine Fusion der nächsten Generation aus Radar und Video, bei der KI-gestützte Radaranalysefunktionen mit Videoanalyse kombiniert werden. Sie erhalten diese umfassende Integration über *Radar-Kopplung* in der Weboberfläche der PTZ-Kamera. Dies ermöglicht einen reibungslosen Betrieb mit präziser visueller Überprüfung und modernsten Funktionen zur Objektverfolgung.

8.3 Radargeräte in einem Sicherheitssystem

Axis Radargeräte werden über PoE versorgt und lassen sich einfach in andere Geräte und Video Management Systeme integrieren.

Das Radargerät kann beim Erfassen eines Eindringlings nicht nur einen Alarm auslösen, sondern dazu auch noch die Videoaufzeichnung für die Sichtüberprüfung aktivieren. Die Kombination von Radargeräten und Kameras ist besonders effektiv bei PTZ-Kameras (Pan-Tilt-Zoom). Mithilfe dieser Kameras können Personen oder Fahrzeuge anhand ihrer genauen geografischen Position, die vom Radargerät bereitgestellt wird, verfolgt und identifiziert werden. Die Integration ausgewählter Geräte ermöglicht eine Kombination aus Radar und Video, was eine optimierte visuelle Überprüfung und eine verbesserte Objektverfolgung ermöglicht.

Im Perimeterschutz ergänzen sich Radargerät und Wärmebildkamera ideal: Das Radargerät deckt große Bereiche ab, während die Wärmebildkamera weit entfernte Bereiche präzise erfasst. Außerhalb eines Zauns installiert, schafft das Radargerät eine Pufferzone und erkennt potenzielle Eindringlinge, bevor sie den Zaun erreichen. Radargeräte können auch zusammen mit Lautsprechern in Szenarien eingesetzt werden, in denen die visuelle Identifizierung nicht erlaubt oder nicht priorisiert wird. Ein vom Radargerät erfasster Eindringling kann durch eine Durchsage effektiv abgeschreckt werden.

Ein Radargerät erkennt Objekte auch bei Dunkelheit zuverlässig und trägt so zu einem energieeffizienten Betrieb des Sicherheitssystems bei. Sie können beispielsweise Auslöser festlegen, die das Infrarotlicht oder Flutlicht einschalten, sobald ein Radargerät ein Objekt erfasst. Dies ist für Standorte mit geringer Aktivität nach den Geschäftszeiten nützlich. Sie können auch Speicherplatz sparen, wenn Sie Aufzeichnungen nur in bestimmten Situationen auslösen lassen. Darüber hinaus hat die geringe Anzahl falscher Benachrichtigungen zur Folge, dass das Sicherheitspersonal nur bei echten Bedrohungen eingreift und so mehr Kameras bedienen kann, was Zeit und Geld spart.

Dank der intelligenten Koexistenzfunktion können mehrere Radargeräte problemlos in unmittelbarer Nähe zueinander betrieben werden. Das Datenblatt jedes Radarmodells gibt die Größe des Koexistenzbereichs und die maximale Anzahl von Radargeräten in diesem Bereich an.

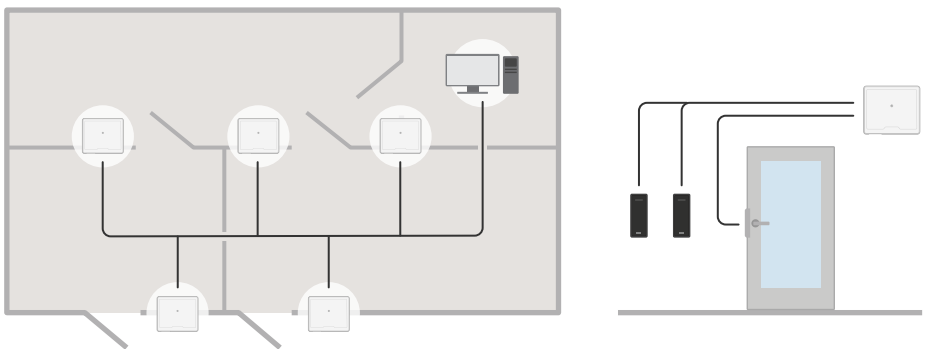
Innerhalb der Koexistenz-Zone kann das Radargerät andere Radargeräte stören. Der integrierte Koexistenz-Algorithmus erkennt jedoch andere Radargeräte und wählt eine geeignete Konfiguration für das Radarsignal, um mögliche Störungen auszuräumen.

9. Zutrittskontrolle

Physische Zutrittskontrollsysteme sind überall auf der Welt in Fabriken, Krankenhäusern, Einzelhandelsgeschäften und vielen anderen Branchen zu finden. Aktuell verlagert sich die Zutrittskontrolle von traditionellen, proprietären (geschlossenen) Lösungen auf die offene IP-Technologie, die erhebliche Verbesserungen der Produktleistung und Verwaltung mit sich bringt. Die IP-Zutrittskontrolle kann als eigenständiges Sicherheitssystem eingesetzt werden, aber auch als Ergänzung zur IP-Videosicherheit oder integriert in andere Systemtypen.

9.1 Was ist die Zutrittskontrolle?

In einem System für die physische Zutrittskontrolle werden Geräte wie Türcontroller, Kartenleser und I/O-Relaismodule an Türen und Zugangspunkten installiert. In Kombination mit der Zutrittsmanagement-Software helfen sie bei der Verwaltung des Zutritts von Personal und Besuchern zu bestimmten Bereichen.



Zutrittskontrollsystem mit Türcontrollern, Zutrittsmanagement-Software und Kartenleser.

Ein Beispiel: Was geschieht, wenn ein Mitarbeiter seine Zutrittskarte neben den Leser des Büroeingangs hält? Der Leser sendet die Informationen der Karte an den Türcontroller (der mit dem elektronischen Schloss der Tür verbunden ist). Dieser überprüft anhand einer Zutrittsliste (in einem Zutrittsverwaltungssystem, das im Türcontroller oder auf einem Server integriert ist), ob der Karte der Zutritt gewährt werden soll. Wenn die Zugangsdaten mit einem Element in der Liste identisch sind, sendet der Türcontroller ein Signal an das elektronische Schloss, wodurch die Tür entsperrt wird.

Die Zutrittskontrolle kann auch in Netzwerk-Gegensprechanlagen integriert werden, um Besuchern einen kontrollierten und sicheren Zutritt zu ermöglichen, einschließlich Videoidentifizierung und Zweiwegekommunikation. Die Integration von Zutrittssystemen in die Videosicherheit fügt der Sicherheitslösung eine neue Komponente hinzu, die Funktionen wie Überwachung, Recherche und Unterstützung ermöglicht.

9.2 Wozu braucht man IP bei der Zutrittskontrolle?

Eine herkömmliche Zutrittskontrolle ist ein geschlossenes System, das von Anbietern konzipiert wird, die das gesamte Produkt – von den Controllern und Zugangsdaten bis zur Software – entwickeln. Dadurch wird der Systembetrieb gewährleistet, jedoch fehlt die Flexibilität für den Benutzer. Wenn eine Organisation wächst oder sich die Anforderungen an die Zutrittskontrolle ändern, muss möglicherweise ein vollständig neues System installiert und das alte komplett entfernt werden. Und möglicherweise muss der Prozess einige Jahre später wiederholt werden, falls sich die Anforderungen erneut ändern.

Ein auf IP basierendes Zutrittssystem ist von Anfang an flexibel und lässt sich einfach erweitern oder um neue Funktionen ergänzen. Sogar die Tür bietet intelligente Funktionen, sodass Zutrittsentscheidungen sowohl zentral als auch lokal getroffen werden können. Der Türcontroller verwendet Regeln, die über das IP-Netzwerk verteilt und aktualisiert werden. Sie können mit PoE-Kabeln verbunden und versorgt werden.

Die Hauptvorteile können wie folgt zusammengefasst werden:

- > **Verbesserte Sicherheit durch Verschlüsselung.** Ein intelligenter, Edge-basierter Tür-Controller kann mithilfe eines integrierten EAL6+-zertifizierten Rechenmoduls die sichere Speicherung kryptografischer Schlüssel gewährleisten. Eine OSDP Secure Channel-Zertifizierung gewährleistet, dass die Kommunikation mit dem Leser vollständig verschlüsselt und geschützt ist. Ein solches System kann auch eine sichere Kommunikation mit der Software für das Zutrittskontrollmanagement gewährleisten.
- > **Einfache, zukunftssichere Integration.** Die IP-Zutrittskontrolle lässt sich mit offenen Standards und Schnittstellen in andere Systeme integrieren, darunter Überwachung,

Analysefunktionen, Gegensprechanlagen, Audio oder Zeit- und Anwesenheitssysteme. Die Möglichkeiten sind endlos, wenn die Technologie als IoT-Lösung (Internet der Dinge) angesehen wird, anstatt nur als Zutrittskontrolle.

- > **Kosteneffizienz.** IP-Lösungen für die Zutrittskontrolle können problemlos ohne spezielle Kabel an ein bestehendes IP-Netzwerk angeschlossen und über dieses mit Strom versorgt werden. IP aktiviert auch die Fernverwaltung und die Überwachung des Systemzustands, was zur Senkung der Gesamtbetriebskosten beiträgt.
- > **Skalierbarkeit.** Mit IP können Sie zunächst die Lösung implementieren, die Sie heute benötigen – und sie dann entsprechend den sich ändernden Geschäftsanforderungen erweitern.
- > **Flexibilität.** Die IP-Zutrittskontrollprodukte von Axis beruhen auf einer offenen API-Architektur und sind nicht proprietär. Dies bedeutet, dass es möglich ist, offene Standardkomponenten von jedem Anbieter zu verwenden und zu kombinieren.

9.3 Komponenten der Zutrittskontrolle

Die Komponenten eines Zutrittsystems beinhalten alles, von der grundlegendsten Software und Hardware für das Zutrittskontrollmanagement bis hin zu erweiterten Optionen.



Produkte zur Zutrittskontrolle (von links): eine IP-Türsprechanlage, ein Kartenleser, eine Tür-Steuerung, ein E/A-Relaismodul und Zugangsdaten: Funkschlüssel, Zugangskarten und mobile Zugangsdaten.

9.3.1 Netzwerk-Tür-Controller

Ein Netzwerk-Türcontroller ist so etwas wie das Gehirn eines Zutrittsystems. Er entriegelt die Tür, speichert jedoch auch die Zutrittskontrollsoftware.

Unabhängig von der Systemgröße kann für jede Tür ein Netzwerk-Türcontroller installiert werden. Für Installationen mit grundlegenden Zutrittsanforderungen kann die Verwaltung mit integrierter Software erfolgen, während ein komplexeres System eine Software von Drittanbietern erfordert.

Eine Türsteuerung lässt sich einfach in andere Systeme wie etwa die Videosicherheit, Eindringdetektion sowie Zeit- und Anwesenheitserfassung integrieren. So kann die Türsteuerung z. B. die Aufzeichnung durch eine Kamera auslösen, wenn eine Person durch eine Tür ein- oder austritt. Wenn eine Verbindung zu Heizungs-, Lüftungs- und Klimaanlage besteht, können die Informationen eines Türcontrollers über die Belegung eines Gebäudes zur Einstellung der Heizungen und Klimaanlage des Standorts verwendet werden. Für die Video- und Audiokommunikation können die Tür-Controller auch in Netzwerk-Gegensprechanlagen integriert werden.

9.3.2 Leser

Kartenlesegeräte sind die gängigste Methode, mit der sich Benutzer in einem Zutrittskontrollsystem identifizieren müssen. Die Berechtigungsarten müssen jedoch nicht auf Karten beschränkt werden, besonders dann nicht, wenn Sie Kameras und Netzwerkvideo-Türstationen in eine Zutrittskontrolllösung integrieren. Der Zutritt kann basierend auf verschiedenen Faktoren gewährt werden:

- > **Der Benutzer hat** beispielsweise eine Smartcard, einen QR-Code, einen Schlüsselanhänger oder ein Mobiltelefon.
- > **Der Benutzer kennt** beispielsweise eine PIN oder die Antwort auf eine Sicherheitsfrage.
- > **Biometrische Faktoren** wie Fingerabdrücke oder Gesichtszüge.
- > **Eine Person überprüft den Benutzer**, beispielsweise ein Empfangsmitarbeiter, der das Kamerabild des Benutzers erkennt.

Die Sicherheit ist am höchsten, wenn mindestens zwei Faktortypen kombiniert werden müssen, um Zutritt zu gewähren.

9.3.3 Netzwerk-I/O-Relaismodule

Ein Netzwerk-I/O-Relaismodul ist eine einfache und kostengünstige Möglichkeit, den Funktionsumfang beliebiger Axis Produkte zu erweitern. Sie eignen sich besonders für die

Integration eines Netzwerk-Türcontrollers in andere Systeme in einem Gebäude. Sie können jedoch auch für andere Gebäudesysteme eingesetzt werden. Das Modul löst anhand von Eingangssignalen, beispielsweise von PIR-Bewegungsmeldern oder Türpositionsschaltern, Aktionen aus. Das Modul können zudem eigenständig und im Rahmen eines Zeitplans betrieben werden, z. B. wenn ein Tor täglich um eine bestimmte Uhrzeit entriegelt werden soll. Es ist außerdem möglich, bestimmte Regeln für Zugangsdaten festzulegen, um den Zugang zu einem Aufzug für bestimmte Etagen eines Gebäudes zu regeln.

9.3.4 Zutrittsverwaltungssysteme

Für die Überwachung eines Zutrittssystems gibt es verschiedene Softwarelösungen. AXIS Camera Station Secure Entry bietet eine intuitive Zugriffsverwaltung für jeden Bedarf. Für eine Lösung, die auf der Fahrzeugzufahrt basiert, gibt es den AXIS License Plate Verifier zur automatischen Erfassung und Validierung von Kennzeichen, um die Zufahrtsverwaltung zu rationalisieren. Auch für die Verwaltung der Zutrittskontrolle steht Software unterschiedlichen Typs von Drittanbietern zur Auswahl.

10. Netzwerk-Gegensprechanlagen

Netzwerk-Gegensprechanlagen werden als Kommunikationstools für Benutzer an Eingängen, aber auch als Infopoints oder lokale Notruftelefone eingesetzt. Sie sind zuverlässige, leicht zu installierende Geräte, die die allgemeine Sicherheit erhöhen. Netzwerk-Gegensprechanlagen basieren auf einer offenen, standardisierten IP-Technologie, die eine einfache Integration in andere Systeme zulässt, z. B. Zutrittskontrolle, Videosicherheit und IP-basierte Kommunikationssysteme (VoIP).

10.1 Multifunktionale Kommunikationsgeräte für mehr Sicherheit

Netzwerk-Video-Gegensprechanlagen vereinen Videosicherheit, Zwei-Wege-Kommunikation sowie die Zutrittsfernkontrolle in nur einem Gerät. Sie können an Ein- und Ausgängen für bekannte und unbekannte Besucher platziert werden, wo sie Videoanrufe ermöglichen und es Ihnen erlauben, den Zugang über einen Computer, ein Festnetztelefon, ein mobiles Gerät oder einen bestimmten Anrufbeantworter aus der Ferne zu kontrollieren. Gegensprechanlagen werden auch in größeren Gebieten wie Städten, Parks oder Universitätsgeländen häufig als Help-Point oder Notruftelefone eingesetzt. Die IP-Türsprechanlagen können einfach an ein bestehendes IP-Netzwerk angeschlossen und darüber mit Strom versorgt werden. Besondere Kabel sind nicht erforderlich.



Netzwerk-Video-Gegensprechanlagen.

Zu den Leistungsmerkmalen von Netzwerk-Video-Gegensprechanlagen von Axis gehören:

- > **Ausgezeichnete Videoqualität.** Eine integrierte, hochwertige Netzwerk-Videokamera bietet ein Bild des Anrufers mit guter Auflösung auf Augenhöhe. Mit fortschrittlichen Kamerafunktionen wie WDR (Wide Dynamic Range) ist der Anrufer selbst bei schwierigen Lichtverhältnissen gut erkennbar. Videobasierte Bewegungserkennung kann je nach Setup unterschiedliche Alarme sowie Videoaufzeichnungen auslösen. AXIS Camera Application Platform (ACAP) ermöglicht die Installation weiterer Anwendungen.
- > **Deutliches Zweiwege-Audio.** Dank des Full-Duplex Audio-Streams mit Geräusch- und Echounterdrückung ist die Kommunikation klar, unterbrechungsfrei und ohne Echo. Türsprechanlagen können auch Zugriffsmöglichkeiten für hörgeschädigte Personen bieten, wie z. B. eine Induktionsschleife für Hörgeräte. Dank der Audioanalyse können IP-Türsprechanlagen akustische Warnungen oder Aufzeichnungen auslösen, zum Beispiel wenn sich jemand nähert oder wenn Schüsse oder aggressives Verhalten erkannt werden.
- > **Zutrittskontrolle.** Einige IP-Türsprechanlagen können als Karten- und PIN-Code-Leser fungieren, um Mitarbeitern und anderen autorisierten Personen ohne weiteren Eingriff Zutritt zu gewähren. Unbekannte Besucher können die Tastatur der IP-Türsprechanlage verwenden, um den Empfang, die Person, die sie besuchen, oder das Sicherheitspersonal anzurufen und um Zutritt zu bitten. Die Empfänger können dann direkt oder per Fernzugriff über ein Mobiltelefon, ein IP-Telefon oder ein Videoverwaltungssystem den Besucher sehen, mit ihm sprechen oder die Tür zu öffnen.
- > **Integration.** Als IP-Geräte können Netzwerk-Türsprechanlagen problemlos in andere Systeme integriert werden. Die SIP-Unterstützung ermöglicht die Integration mit IP-Telefonie, so dass Video und Audio von der IP-Türsprechanlage übertragen und Anrufe von einem Tischtelefon oder einem mobilen Gerät entgegengenommen werden können. Anrufe lassen sich auch über die meisten IP-basierten Video Management Systeme empfangen, sodass der Kunde die von ihm bevorzugte Systemlösung nutzen kann. In komplexeren Systemen z. B. von Logistikzentren oder Flughäfen sind Gegensprechanlagen eine sinnvolle Ergänzung für integrierte Lösungen mit Netzwerk-Kameras, Zutrittskontrollsystemen, Einbruchalarmen und weiteren Sicherheitsanwendungen. IP-Türsprechanlagen verfügen über eine Vielzahl an Ports, Relais und unterstützten Protokollen, mit denen Sie externe Sensoren anschließen, Lampen einschalten, Türen öffnen, externe Kameras oder akustische Alarme auslösen können.

11.Body Worn

Am Körper getragene Kameras dokumentieren Ereignisse und halten wertvolle Beweise fest. Sie sind auch ein wirksames Mittel, um von schlechtem Verhalten abzuschrecken und die Handlungen der Kameraträger und der Öffentlichkeit positiv zu beeinflussen. Axis Body Worn-Kameras bieten eine überragende Video- und Audioqualität und ermöglichen so eine leicht verständliche und interpretierbare Beweisführung, die auch vor Gericht Bestand hat. Das am Körper getragene System von Axis basiert auf offenen Standards, die Flexibilität und Skalierbarkeit gewährleisten. Es kann mit verschiedenen Inhaltszielen verwendet werden und verwendet eine End-to-End-Verschlüsselung für die Cybersicherheit. Und mit AXIS Body Worn Live ist es möglich, Live-Video, Audio und Metadaten von den Axis Body Worn-Kameras zu übertragen. Die sichere und zuverlässige Anwendung ermöglicht fundierte Entscheidungen der Bediener und gibt den Kameraträgern ein zusätzliches Sicherheitsgefühl.

11.1 Der Zweck von Body Worn-Kameras

Eine Body Worn-Kamera ermöglicht die Aufzeichnung von Vorfällen an jedem beliebigen Ort. Die Kamera wird beispielsweise am Körper eines Zustellers, eines Zugführers, eines Angestellten oder eines Sicherheitsbeamten befestigt. Sie wird dorthin mitgenommen, wo sie gebraucht wird, und kann Ereignisse aufzeichnen, die von fest installierten Kameras nie erfasst worden wären.

Eine von einer Body Worn-Kamera produzierte Aufnahme ist ein vertrauenswürdiges und sicheres Beweismittel, das objektiv zeigt, was am Schauplatz eines Vorfalls passiert ist. Das Filmmaterial kann bei internen Ermittlungen und vor Gericht verwendet werden, aber auch für Diskussionen und Analysen, um den Mitarbeitern beizubringen, wie sie auf Situationen reagieren sollen, denen sie wahrscheinlich begegnen werden. Mit Body Worn-Kameras lässt sich auch leicht dokumentieren, dass Lieferungen oder andere Aufgaben in Übereinstimmung mit den zugehörigen Verfahren durchgeführt wurden.

Der Einsatz von am Körper getragenen Kameras beeinflusst das Verhalten sowohl der Kameraträger als auch der Personen, mit denen diese interagieren. Das Bewusstsein, aufgezeichnet zu werden, scheint den Menschen das Gefühl zu geben, dass es einen digitalen Zeugen für ihre Handlungen gibt. Sie neigen weniger zu Fehlverhalten und die Kameraträger neigen eher dazu, sich ruhig zu verhalten und die Vorschriften einzuhalten.



Die Verwendung von Body Worn-Kameras kann dazu beitragen, die Situation zu beruhigen, wenn sowohl der Kameraträger als auch die Öffentlichkeit wissen, dass ihr Verhalten und ihre Entscheidungen von einer anderen Partei beobachtet werden können.

11.2 Am Körper getragene Kameras



Axis Body Worn-Kameras sind in Schwarz, Weiß oder Grau erhältlich, damit sie sich von der Kleidung abheben oder mit dieser farblich verschmelzen. Diese Modelle sind für den Einsatz in jeder Branche geeignet.

Body Worn-Kameras von Axis liefern scharfe Bilder und klaren Ton. Sie sind leicht, robust und wasserbeständig. Sie starten und stoppen auf Knopfdruck und puffern bis zu 120 Sekunden, bevor

eine Aufnahme beginnt. Lange Akkulaufzeit, USB-Ladung und schnelles Herunterladen machen die Nutzung noch einfacher.

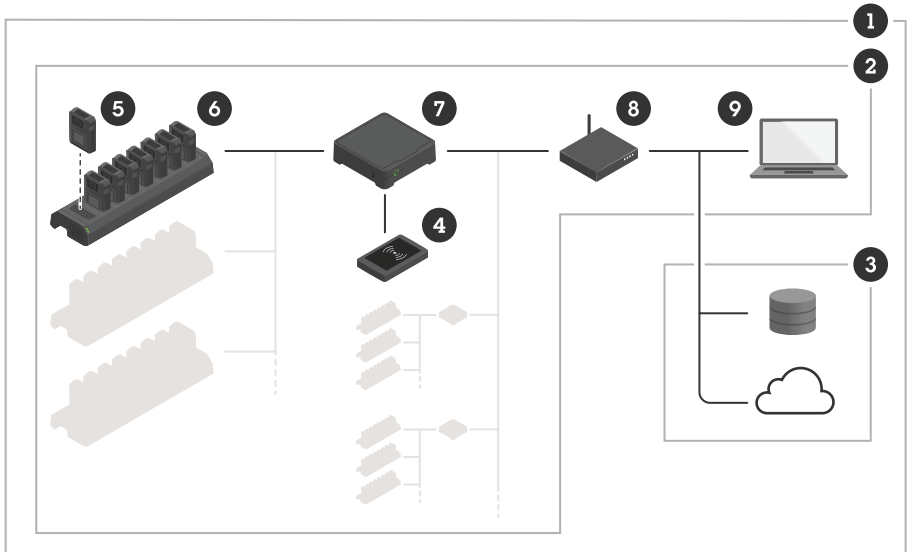
Wählen Sie ein schwarzes oder weißes Modell aus, je nachdem, ob Sie möchten, dass die Kamera unauffällig ist oder sich von der Kleidung abhebt. Mini-Sensoren können an der Kamera befestigt und mithilfe von Standardhalterungen an einer Kopfhalterung angebracht werden, um komfortable und unauffällige Aufnahmen zu ermöglichen.

Body Worn Kameras speichern in ihren Aufzeichnungen Standortdaten, die von Navigationssatelliten bestimmt wurden. Durch die Verknüpfung des Videomaterials mit den geografischen Koordinaten, an denen es gefilmt wurde, wird eine Standortverfolgung ermöglicht und die Beweiskraft der Aufnahmen deutlich erhöht. Die Body Worn-Kameras von Axis sind außerdem mit der Zipstream-Technologie von Axis ausgestattet. Damit können Sie eine große Menge an Videomaterial speichern, ohne Kompromisse bei der Videoqualität eingehen zu müssen.

Wenn der Träger einer Bodycam eine Aufzeichnung startet, kann er mit AXIS Body Worn Live auch sofort einen Live-Audio- und Videostream von der Kamera zum Bediener aktivieren, welcher dann Ereignisse in Echtzeit verfolgen kann. Unternehmen können sich für die cloudbasierte, von Axis gehostete Version entscheiden, wenn sie eine Hands-off-Lösung benötigen. Oder sie können AXIS Body Worn Live selbst hosten, wenn die Regeln ein cloudbasiertes Hosting ausschließen. Der Bediener kann fundierte Entscheidungen treffen, beispielsweise über die Bedingungen für das Senden von Verstärkung, und die GPS-Koordinaten geben an, wohin die Verstärkung gesendet werden soll. Der Bediener kann eine Benachrichtigung an den Träger senden, der dann weiß, dass er mit Unterstützung rechnen und sich auf den Vorfall konzentrieren kann, anstatt mit der Zentrale zu kommunizieren. Benachrichtigungen können als Signalton oder – bei einigen Modellen – als Symbol auf dem LCD-Bildschirm der Kamera empfangen werden.

11.3 Axis Body Worn Solution

Nachdem die Body Worn-Kamera verwendet wurde, platzieren Sie sie in der Dockingstation. Der Systemcontroller überträgt sofort die Daten von der Kamera an das Ziel Ihrer Wahl und die Batterie der Kamera lädt sich auf. Der Systemcontroller hält die Kameras außerdem mit der neuesten AXIS OS-Version und anderen Einstellungen auf dem neuesten Stand und überwacht den allgemeinen Zustand der am Körper getragenen Axis Lösung.



Komponente der Axis Body Worn-Lösung.

Bei der Body Worn-Lösung von Axis (1) handelt es sich um eine oder mehrere Axis Body Worn-Systeme (2), die mit einem Inhaltsziel (3) verbunden sind. Das Body Worn-System funktioniert nur, wenn es mit einem Inhaltsziel verbunden ist.

Das Axis Body Worn-System (2) besteht aus Axis Body Worn-Kameras (5), Axis Dockingstationen (6), Axis Systemcontrollern (7) und aus einem AXIS Body Worn Manager (9).

An den System-Controller kann ein optionaler RFID-Leser (4) angeschlossen werden. Damit kann der Benutzer mithilfe des Selbstzuweisungs-Tags sich selbst jede verfügbare Body Worn-Kamera zuweisen.

AXIS Body Worn Manager (9) ist die Webanwendung, mit der Sie Ihr Body Worn-System konfigurieren und verwalten können.

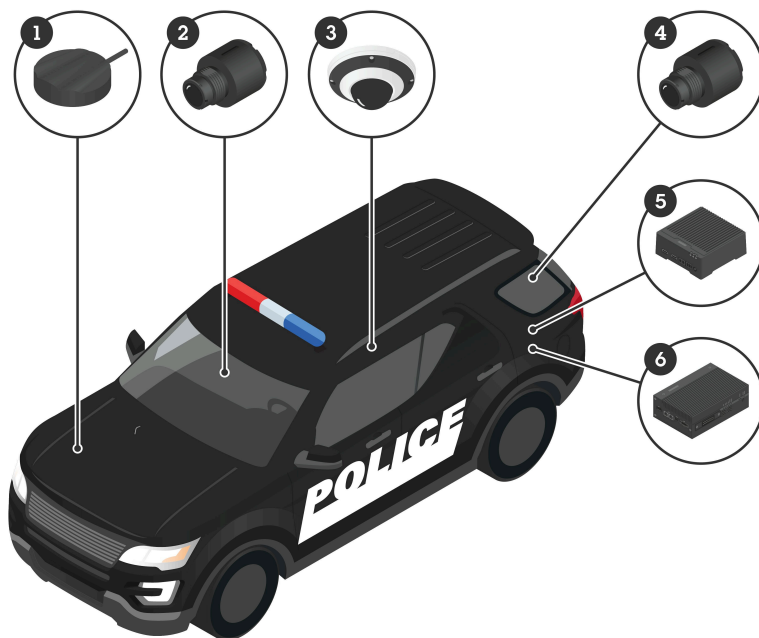
Offene Standards und die kostengünstigen Dockingstationen mit einem separaten Systemcontroller machen es einfach und kostengünstig, dem System bei Bedarf weitere Kameras und Benutzer hinzuzufügen. AXIS Body Worn Assistant ist die Anwendung für mobile Geräte, die direkt an die Body Worn-Kamera angeschlossen wird und die unter anderem beispielsweise die Anzeige aufgezeichneter Videos ermöglicht.

Die Axis Body Worn-Lösung wird von verschiedenen Typen von Inhaltszielen unterstützt: Evidence Management Systemen (EMS) zur Beweissicherung, Video Management Systemen (VMS) und Medienservern. Sie können eine End-to-End-Axis Lösung verwenden, die AXIS Camera Station oder Axis Case Insight umfasst, oder ein VMS oder EMS von Drittanbietern, entweder vor Ort oder in der Cloud.

Die Body Worn-Kameras von Axis unterstützen die offiziellen FBI-Standards für Cybersicherheit mit End-to-End-Verschlüsselung.

11.4 Bordeigene Lösung

Die bordeigene Lösung von Axis für Strafverfolgungsbehörden verbindet die robuste und zuverlässige Videosicherheit im Fahrzeug mit den tragbaren Kameras von Axis. Die Kameras und Mikrofone dieser Lösung liefern Video und Audio für die forensische Nutzung und sorgen für ein umfassendes Situationsbewusstsein innerhalb und außerhalb von Fahrzeugen. Alle aufgezeichneten Materialien und Informationen sind durch integrierte Cybersicherheitsfunktionen geschützt.



Eine typische Installation in einem Fahrzeug, mit folgenden Bestandteilen: 1) Antenne, 2) Windschutzscheibenkamera, 3) unbewegliche Kamera, 4) Rückfahrkamera, 5) Hauptgerät, 6) robuster Computer.

12. Umgebungssensoren

Umweltsensoren detektieren und messen verschiedene Parameter in der Umgebung, typischerweise Temperatur, Feuchtigkeit, Geräusch- / Rauschlevel und verschiedene Arten von Verschmutzung. Umweltsensoren von Axis sind netzwerkbasierte Geräte, die über ihre bestehende IP-Infrastruktur verbunden werden. Sie können sie zusammen mit Ihren Kameras in ein Netzwerkvideosystem integrieren oder sie eigenständig nutzen.

12.1 Luftqualitätssensoren

Ein Luftqualitätssensor ist ein Typ von Umweltsensor, der speziell die Messung von Luftqualitätsparametern wie Gas- und Partikelgehalt ermöglicht.

Die Aufrechterhaltung eines gesunden Raumklimas ist von Bedeutung für Gesundheit und Sicherheit, den Betrieb und die Geschäftsanalyse. Durch das Überwachen der Luftqualität können Sie Abweichungen erfassen, Anpassungen vornehmen, Nachhaltigkeitsziele verfolgen und die Einhaltung der einschlägigen Vorschriften nachweisen.

12.1.1 Überwachung der Raumluftqualität

Luftqualitätssensoren tragen in zahlreichen Szenarien und Branchen zur Gesundheit und Sicherheit, zur betrieblichen Effizienz sowie zur Geschäftsanalyse bei.

- > **Erfassen von Vapen und Rauchen.** Wenn Rauchverbote nicht eingehalten werden, können Sie frühzeitig eingreifen und automatische oder manuelle Reaktionen auslösen. Dazu zählen beispielsweise Audio-Alarme, Videoaufzeichnungen oder Benachrichtigungen an das Personal. Zu den typischen Einsatzorten zählen Toiletten, Treppenhäuser und andere Gemeinschaftsbereiche.
- > **Sorgen Sie für eine gesunde Raumluftqualität.** Durch die Überwachung von CO₂ und anderen wichtigen Kennzahlen können Sie Warnmeldungen auslösen, sobald die Messwerte Ihre Schwellenwerte überschreiten, sodass Sie die Belüftung anpassen oder die Bewohner informieren können, bevor sich Probleme verschlimmern. Dies ist besonders wertvoll in Büros,

Schulen, Einkaufszentren und öffentlichen Räumen, wo eine schlechte Luftqualität die Konzentration, Produktivität und das Wohlbefinden von Kunden und Besuchern beeinträchtigen kann.

- > **Angenehmes Raumklima gewährleisten.** Durch das Überwachen von Temperatur und Luftfeuchtigkeit können Sie Anomalien erfassen, die die Lebensdauer Ihrer Geräte verkürzen könnten. In Serverräumen und Rechenzentren trägt dies dazu bei, die Lebensdauer der Geräte zu verlängern und kostspielige Ausfälle zu vermeiden.
- > **Die Sicherheit der Arbeitnehmer verbessern.** Wenn Sie die Innentemperaturen kennen, können Sie gesundheitsgefährdende Hitzebelastungen frühzeitig erkennen und Zeitpläne entsprechend anpassen, um das Risiko hitzebedingter Erkrankungen zu verringern. In industriellen Umgebungen trägt die Überwachung prozessbedingter Luftverschmutzung dazu bei, die Gesundheit der Beschäftigten zu schützen und eine gleichbleibend hohe Produktqualität sicherzustellen.
- > **Unterstützung von Einrichtungen im Gesundheitswesen.** Eine genaue Überwachung der Luftqualität in Operationssälen, Patientenbereichen und auf Intensivstationen ist entscheidend, um saubere Luftverhältnisse für die Patientensicherheit aufrechtzuerhalten – auch während Renovierungs- oder Bauarbeiten.
- > **Trends analysieren.** Anhand historischer Daten und Metadaten können Sie nachvollziehen, wie sich die Luftqualität im Laufe der Zeit verändert, und fundierte Entscheidungen hinsichtlich der Belüftung und der Raumgestaltung treffen.
- > **Erreichen von Nachhaltigkeitszielen.** Mit Luftqualitätsdaten machen Sie Ihre Nachhaltigkeitsmaßnahmen messbar, unterstützen Gebäudezertifizierungen und kommunizieren Ihr Engagement für Umwelt und Gesundheit glaubwürdig.
- > **Halten Sie die Vorschriften ein.** Durch die Installation von Luftqualitätssensoren können Sie die Regelung der Raumluftqualität angemessen dokumentieren und nachweisen.



Luftqualitätssensoren können das Rauchen oder Dampfen in Toiletten und Treppenhäusern erfassen und die Parameter der Raumluftqualität sowie Temperatur und Luftfeuchtigkeit in Büros, öffentlichen Bereichen und Serverräumen überwachen.

12.1.2 Luftqualitätsparameter

Luftqualitätssensoren messen in der Regel die folgenden Parameter.

- > **Feinstaub (PM).** Die Belastung durch Feinstaub kann zu Reizungen der Augen, der Nase und des Rachens führen, die Lungenfunktion beeinträchtigen und Erkrankungen wie Asthma und Herzerkrankungen verschlimmern. Die Luftqualitätssensoren von Axis messen Feinstaub mithilfe eines optischen Partikelzählers (OPC), der einen Laserstrahl auf die durch den Sensor strömende Luft richtet und misst, wie viel Licht von den Partikeln gestreut wird.
- > **Flüchtige organische Verbindungen (VOC – Volatile Organic Compounds).** Viele VOC sind gesundheits- oder umweltschädlich, und einige unterliegen gesetzlichen Vorschriften. Zu den Quellen zählen Farben, Lösungsmittel, Desinfektionsmittel und gelagerte Kraftstoffe. VOC lassen sich mit einem Metalloxid-Sensor (MOX) messen, der durch die Reaktion der VOC an der Sensoroberfläche den Sauerstoffgehalt ändert.

- > **Stickoxide (NO_x).** Selbst geringe Langzeitkonzentrationen können schädlich sein. Zu den Quellen in Innenräumen zählen Gasherde, Kerzen und das Rauchen. Auch äußere Einflüsse wie Autoabgase können die Raumluftqualität beeinträchtigen. Genau wie VOC werden auch NO_x -Werte mit einem MOX-Sensor gemessen, der zwischen oxidierenden und reduzierenden Gasen unterscheidet.
- > **Kohlendioxid (CO_2).** Hohe Konzentrationen führen zu Kopfschmerzen und Atembeschwerden. In Schulen und Büros kann ein erhöhter CO_2 -Gehalt die Konzentrationsfähigkeit beeinträchtigen und die Produktivität verringern. CO_2 lässt sich mithilfe einer gepulsten IR-Lichtquelle messen, die CO_2 -Moleküle in Schwingung versetzt und so eine Schallwelle erzeugt, die von einem Mikrofon erfasst wird, um die Konzentration zu berechnen.
- > **Vapen und Rauchen.** E-Zigaretten erzeugen Feinstaubpartikel, die sich in den Atemwegen ausbreiten. Rauchen steht im Zusammenhang mit Atemwegserkrankungen, chronischer Bronchitis, Herzerkrankungen und Lungenkrebs.
- > **Relative Luftfeuchtigkeit.** Eine zu hohe Luftfeuchtigkeit kann Schimmelbildung begünstigen, während eine zu niedrige Luftfeuchtigkeit zu Haut- und Augenreizungen führt. Auch in Serverräumen ist die Regulierung der Luftfeuchtigkeit wichtig, um die Lebensdauer der Geräte zu verlängern.
- > **Temperatur.** Extreme Temperaturen wirken sich sowohl auf das Wohlbefinden der Menschen als auch auf die Lebensdauer der Geräte aus.
- > **Luftqualitätsindex (LQI).** Ein weit verbreiteter Messwert, der die Konzentration von Luftschadstoffen quantifiziert. Die NowCast-Methode nutzt einen gewichteten Durchschnitt der letzten 12 Stundenmessungen, um eine Echtzeit-Schätzung des AQI zu liefern.
- > **Hitzeindex und Humidex.** Beschreibt die gefühlte Temperatur unter Berücksichtigung der Lufttemperatur und der relativen Luftfeuchtigkeit. Eine zu hohe gefühlte Temperatur kann zu einem Hitzschlag und zu einer Hitzeerschöpfung führen.

12.1.3 Axis Luftqualitätssensoren



Axis bietet zwei Typen von Luftqualitätssensoren an: ein eigenständiges IP-Netzwerk-Gerät und einen Sensor, der an ein übergeordnetes IP-Netzwerk-Gerät angeschlossen wird.

Beide Typen messen Parameter der Raumluftqualität und erfassen das Dampfen sowie das Rauchen. Sie können diese so konfigurieren, dass automatische Ereignisse ausgelöst werden, sobald die Werte der Parameter die von Ihnen festgelegten Grenzwerte überschreiten.

12.1.3.1 Freistehender Luftqualitätssensor

Der eigenständige Sensor erfasst sowohl das Dampfen und Rauchen als auch die gesamte Bandbreite der Luftqualitätsparameter. Darüber hinaus verfügt das Gerät über einen PIR-Sensor zur Erfassung der Anwesenheit, mehrfarbige LEDs zur optischen Alarmierung sowie eine Zwei-Wege-Audiofunktion für Sprachmitteilungen und Analysefunktionen für Audio. Die Messergebnisse sind in der Weboberfläche des Sensors verfügbar und lassen sich über ein Dashboard direkt im VMS anzeigen.

12.1.3.2 Luftqualitätssensor mit Hostgerät

Der auf Portcast basierende Luftqualitätssensor ist eine kostengünstige Lösung, für die ein kompatibles Axis Hostgerät, wie beispielsweise eine Netzwerkkamera oder eine Blitzsirene, erforderlich ist. Dank der Axis Portcast-Technologie lässt sich der Sensor einfach anschließen und erweitert das Host-Gerät um eine Luftqualitätsmessung – ganz ohne zusätzliche IP-Adresse. Sie steuern den Sensor über die Weboberfläche des Host-Geräts, und die Ergebnisse der Messungen sind über MQTT-Overlays auch im Kamerastream verfügbar.

13. Analyse

Eine Kamera kann viel mehr als nur eine Videoquelle sein. Analysefunktionen ermöglichen Einblicke in Video, Audio und andere Daten. Dank künstlicher Intelligenz (KI) ist die Analytik inzwischen zu einem zentralen Unterscheidungsmerkmal in der Videoüberwachung geworden und trägt maßgeblich zur Verbesserung von Sicherheit und betrieblicher Effizienz bei.

13.1 Analysefunktionen für eine smarte, sicherere Welt

Analysefunktionen erhöhen die Sicherheit und verbessern das Echtzeit-Situationsbewusstsein. Darüber hinaus steigern sie die Betriebs- und Ressourceneffizienz und ermöglichen eine smartere, datengestützte Verwaltung und Entscheidungsfindung. Sie können zum aktiven Schutz der Privatsphäre von Personen entwickelt werden.

Der Zugriff auf strukturierte, gekennzeichnete Daten, die die entscheidenden Details und Aktivitäten einer Szene aufzeigen, ermöglicht es Organisationen und Unternehmen, Aktionen zu automatisieren, Entscheidungen zu lenken und den Ressourcenaufwand für die Analyse von Informationen oder die Erkennung von Trends zu reduzieren. Regelbasierte Ereignisse und Alarme, wie das Auslösen eines Alarms beim Überschreiten einer virtuellen Linie in einem Sicherheitsbereich oder das automatische Öffnen eines Tors für autorisierte Fahrzeuge, verbessern die betriebliche Effizienz und das Situationsbewusstsein.

Analysefunktionen können auch Objekte in der Szene und deren Eigenschaften beschreiben, wie etwa Personen mit einer Einkaufstasche oder Kopfbedeckung, sowie ihre Farbe, Form, Geschwindigkeit und Bewegungsrichtung. Ereignis- und szenenbezogene Metadaten werden zu Analyse-Metadaten zusammengeführt, die eine effiziente Suche in großen Videodatenmengen ermöglichen und zugleich Echtzeitanalysen, forensische Auswertungen sowie prädiktive Erkenntnisse im großen Maßstab unterstützen.

Die Anwendungsfälle von Analysefunktionen entwickeln sich ständig weiter, und die künftigen Möglichkeiten sind praktisch endlos. In diesem Kapitel werden einige der wichtigsten aktuellen Anwendungsmöglichkeiten behandelt.

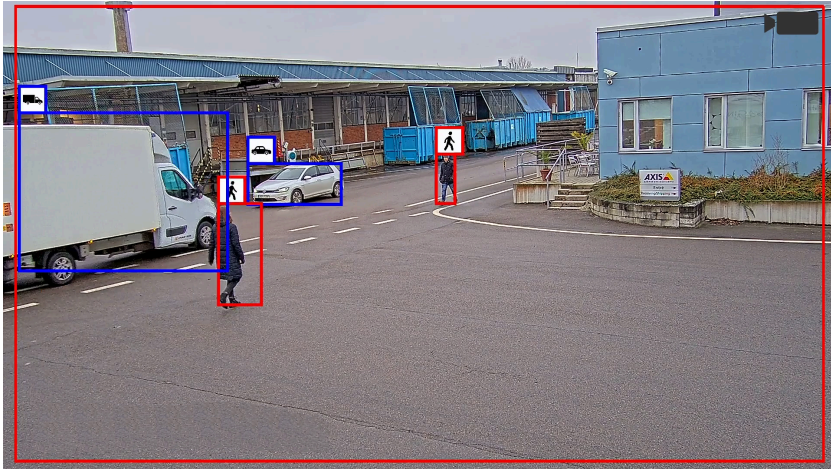
13.2 Welche Vorteile bieten Analysefunktionen?

Analysen erhöhen die Sicherheit und die Betriebseffizienz und können wertvolle Geschäftsinformationen liefern. Sie können Ihnen bei Folgendem helfen:

- > **Schnelleres Reagieren auf kritische Vorfälle.** Echtzeit-Ereignisse, Benachrichtigungen und ein verbessertes Szenenverständnis helfen Ihnen, in zeitkritischen Situationen schnell zu handeln. Sie können sogar Reaktionen automatisieren.
- > **Treffen fundiertere Entscheidungen.** Die Analysefunktionen optimieren Betriebsabläufe, beseitigen Engpässe und unterstützen datengestützte Entscheidungen. All dies trägt dazu bei, die Effizienz zu steigern und die allgemeinen Geschäftsergebnisse zu verbessern.
- > **Bessere Nutzung von Ressourcen.** Durch die Automatisierung von Aufgaben, die Maschinen genauso gut oder sogar besser als Menschen erledigen können, können sich die Bediener auf anspruchsvollere Aufgaben konzentrieren.
- > **Auffindung dessen, was Sie suchen.** Analysefunktionen beschleunigen Untersuchungen, indem sie eine effiziente Suche nach Objekten, deren Eigenschaften oder relevanten Vorfällen in mehreren Video-Streams ermöglichen.
- > **Proaktive Verhinderung unerwünschte Ereignisse.** Frühzeitige Warnungen vor Sicherheitsrisiken – wie herumlungernenden Personen oder einem gestohlenen Fahrzeug im überwachten Bereich – sowie vor betrieblichen Engpässen wie Warteschlangen ermöglichen ein rechtzeitiges Eingreifen, bevor sich Probleme verschärfen.

13.2.1 Echtzeitüberwachung

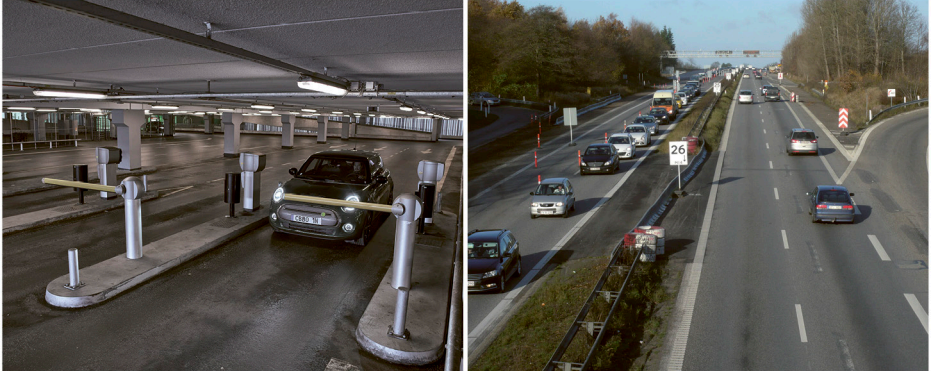
Mithilfe von Analysefunktionen können große Mengen an Videomaterial automatisiert überprüft werden, um relevante Informationen zu extrahieren und bei Bedarf zeitnah eingreifen zu können. Objekte wie Personen und Fahrzeuge in der Szene können erkannt werden, um bestimmte Ereignisse zu identifizieren oder vordefinierte Reaktionen auszulösen. Die automatischen Aktionen können zum Beispiel Mitarbeiter benachrichtigen, eine Videoaufzeichnung starten, ein Tor öffnen oder eine vorab aufgezeichnete Durchsage wiedergeben.



AXIS Object Analytics bietet KI-basierte Objekterkennung und -klassifizierung.

Im Einzelhandel oder ähnlichen Umgebungen kann mit Hilfe von Analysefunktionen die Verwaltung des Personals effizienter gestaltet werden. Eine lange Warteschlange könnte zum Beispiel die Durchsage "Bitte mehr Personal an die Kassen" auslösen. Personenzählung und Fahrzeugzählung liefern wertvolle Informationen, die Ihnen helfen, Einblicke in Besuchertrends und Kundenverhalten zu gewinnen. Mithilfe dieser Daten können Sie die Geschäftsperformance des Standorts bewerten, das Kundenverhalten überwachen, die Parkplatzkapazität maximieren und letztendlich Ihren Betrieb optimieren.

Analysefunktionen können auch zur Kennzeichenerkennung eingesetzt werden, womit sie die optimale Lösung für die Zutrittskontrolle, die Verwaltung von Parkplätzen, die Verkehrsleitung und vieles mehr darstellen. Diese Lösungen helfen bei der Verfolgung von Fahrzeugen, die in kriminelle Handlungen, Geschwindigkeitsübertretungen oder Diebstähle verwickelt sind, und unterstützen gleichzeitig alltägliche Aufgaben wie die Automatisierung der Mauterhebung, die Überwachung des Verkehrsflusses, die nahtlose Einfahrt in Parkeinrichtungen und eine proaktive Verkehrsplanung durch datengestützte Erkenntnisse.



AXIS License Plate Verifier verfügt über eine KI-gestützte Kennzeichenerkennung in Echtzeit für eine Reihe von Anwendungen im Verkehrsbereich.

13.2.2 Effiziente Suche

Der Einsatz von Analysefunktionen zur Verbesserung der Suche ist einer der häufigsten und wertvollsten Anwendungsfälle, da er viel Zeit und Ressourcen sparen kann. Analysefunktionen optimieren Suchanfragen nach bestimmten Objekten, Attributen und Aktivitäten, sodass relevante Momente in mehreren Video-Streams schneller gefunden werden können. In Logistikumgebungen können sie helfen, fehlende Container oder Pakete zu lokalisieren, was die manuelle Suchzeit erheblich verkürzt. In Sicherheits- und Betriebsabläufen unterstützen sie die Suche nach Fahrzeugen, Objekten oder Personen, die mit einem Ereignis in Verbindung stehen, und helfen, den Zeitpunkt und Ort eines Vorfalls genau zu bestimmen.

Diese Lösungen extrahieren mithilfe künstlicher Intelligenz detaillierte Informationen, die eine schnelle, genaue und effiziente Suche ermöglichen. Analysefunktionen können für eine weitere Suche und Analyse auch in bestehende Systeme und Arbeitsabläufe integriert werden, beispielsweise in Video Management Software (VMS), Ermittlungswerkzeuge oder Datenbanken mit Informationen über vermisste Fahrzeuge.

13.2.3 Erkennen von Trends und Mustern

Analysefunktionen können wertvolle und verwaltbare Einsichten und Statistiken liefern, um den Betriebsablauf zu verbessern und fundiertere Entscheidungen zum Verwalten von Datenverkehr oder Besucherbewegungen zu treffen. Da Analysefunktionen Metadaten zur Beschreibung des Inhalts einer Szene nutzen, können sie Daten über einen bestimmten Zeitraum hinweg effektiv sammeln, um Trends und Muster zu erkennen.

13.2.4 Datenschutz

Mit der KI-basierten dynamischen Maskierung können Sie zum Schutz der Privatsphäre Gesichter, ganze Körper, Fahrzeugkennzeichen und Hintergründe in einer Szene unkenntlich machen. Dabei werden sensible Daten mit einer Überblendung versehen, sodass sie nicht mehr erkennbar sind. Die Bewegungsabläufe können jedoch weiterhin verfolgt werden. Die dynamische Maskierung kann sowohl auf Live- als auch auf aufgezeichnete Videos angewendet werden, so dass Sie Aktivitäten überwachen können, ohne personenbezogene Daten zu erfassen.

13.3 Systemarchitektur – wo wird das Video analysiert?

Bei der Entwicklung eines Videoanalysesystems ist die Frage, wo die Analysedaten verarbeitet werden sollen, von entscheidender Bedeutung. Es gibt vier Optionen: in der Kamera, auf einem Server, in der Cloud oder in einer Hybridlösung.

> **Auf der Kamera.** Die Analyse von Video in Edge ist aus vielen Gründen von Vorteil:

- **Höhere Genauigkeit:** Das Ausführen von Analysen nicht komprimierter Videos führt zu einer höheren Genauigkeit, da die Videoqualität nicht beeinträchtigt wird.
- **Schnelle Reaktion und Aktion:** Edge-basierte Lösungen minimieren die Verzögerung durch die Verarbeitung von Daten in der Nähe ihrer Quelle und vermeiden so Verzögerungen, die durch die Übertragung an entfernte Server oder cloudbasierte Plattformen entstehen. Dabei werden Warnmeldungen in Echtzeit aktiviert, die zusammen mit automatischen Auslösern kurze Reaktionszeiten und sofortige Aktionen ermöglichen.
- **Einfach zu skalieren:** Die Ausführung von Analysen am Rande des Netzwerks erleichtert die Skalierbarkeit, da die Verarbeitungslast auf zentralen Systemen reduziert wird. Dies ist besonders vorteilhaft, da die Verarbeitung aller Videodaten in der Cloud sehr teuer sein kann. Außerdem senkt es die Serverkosten und den Wartungsbedarf.
- **Verringerte Netzwerklast und Anforderungen an die Infrastruktur:** Durch den Verzicht auf unnötige Datenübertragungen werden Sie einen geringeren Datenaustausch im Netzwerk, geringeren Bandbreitenanforderungen und geringeren Bedarf an Hardware erleben, was letztendlich zu erheblichen Kosteneinsparungen führt.
- **Verbesserter Datenschutz:** Wenn Analysen in am Rande des Netzwerks ausgeführt werden, können nur anonymisierte Daten und/oder Warnmeldungen über das Netzwerk gesendet werden, was mehr Datenschutz gewährleisten kann.

- > **Auf einem Server.** Wenn Sie viel Rechenleistung benötigen, ist oft die Analyse von Video auf dedizierten Servern erforderlich. Außerdem können die Server mehrere Videostreams aus vielen verschiedenen Quellen gleichzeitig analysieren und in großen Datenmengen Datenbankabfragen durchführen.
- > **In der Cloud.** Eine weitere Option ist das Senden von Video direkt von Kameras in die Cloud zur Verarbeitung. Die Verarbeitung sämtlicher Videodaten in der Cloud kann jedoch aufgrund von Gebühren für Datenspeicherung, -übertragung und -verarbeitung erhebliche Kosten verursachen, was ihre Eignung für bestimmte Anwendungen einschränken kann. Cloud Computing erfordert häufig eine robuste und zuverlässige Internetverbindung, die nicht in jeder Situation verfügbar ist. Andererseits können Sie mit Cloud-Computing mehrere Videostreams auf einmal verarbeiten. Außerdem lässt sie sich einfach skalieren. Einige Unternehmen müssen aufgrund von Vorschriften alle Daten in ihren Räumlichkeiten aufbewahren und werden daher eher keine Cloud-Lösung in Erwägung ziehen.
- > **Hybridlösung.** Ein hybrides System, das die Verarbeitung am Rande des Netzwerks, in der Cloud und auf Servern vor Ort kombiniert, ist oft der beste Ansatz, da es die Stärken jeder Technologie nutzt. Bei Hybridsystemen kann die Objektklassifizierung in den Kameras erfolgen, während Algorithmen, die mehr Leistung benötigen, auf Servern oder in der Cloud ausgeführt werden. Durch die Aufteilung der Rechenlast zwischen Edge und Server werden Systeme viel besser skalierbar, weil beim Hinzufügen einer neuen Kamera mit Edge-Analysefunktionen die Server-Rechenleistung nicht erhöht werden muss.

13.4 Bildqualität und Edge-basierte KI – die Grundlage für hervorragende Analysefunktionen

Wir haben ein paar wichtige Faktoren identifiziert, die eine genaue Analyse von Videos ermöglichen.

- > **Spezialgefertigte Hardware.** Die von uns verwendeten Geräte sind robust und für die Aufzeichnung hochwertiger Videobilder unter allen Bedingungen ausgelegt. Dies gilt nicht nur für Kameras, sondern auch für andere Geräte wie Radargeräte.
- > **Verbesserte Bildqualität.** Dies wird durch unsere Bildverarbeitungsalgorithmen wie Lightfinder, Forensic WDR und OptimizedIR erreicht. Ein proaktiver Ansatz umfasst jedoch auch die Auswahl des optimalen Geräts und dessen sorgfältige Platzierung für Ihr spezielles Schutzziel und Ihre Szene. Damit bereits vor Beginn der Analyse jedes einzelne Bild optimiert ist, überwacht und analysiert AXIS Image Health Analytics kontinuierlich das Videomaterial auf Probleme, die sich auf die Analyseleistung auswirken könnten. Wird ein Problem erfasst, z. B. ein blockiertes, unscharfes, unterbelichtetes oder umgeleitetes Bild, sendet das System eine Benachrichtigung, so dass sofortige Korrekturmaßnahmen ergriffen werden können.

- > **KI-Fähigkeiten.** Unsere KI läuft auf dem proprietären ARTPEC SoC. Sie erkennt und klassifiziert wichtige Szenen-Details in umfangreichen Metadaten, die für die Verwendung durch die Analysefunktionen, von Dashboards, AXIS Camera Station und VMS von Drittanbietern bereit sind.

Diese Elemente bilden gemeinsam Axis Scene Intelligence: eine offene Plattform, auf der speziell entwickelte Hardware, optimierte Bildqualität und Edge-basierte KI im Zusammenspiel eine überragende Analysegenauigkeit und hochwertige Metadaten liefern.

13.5 Künstliche Intelligenz

Künstliche Intelligenz (KI) ist ein weitgefächertes Konzept, das auf Maschinen angewendet wird, die komplexe Aufgaben lösen und dabei scheinbar intelligente Merkmale aufzeigen können. Im Gegensatz zur traditionellen Programmierung, die auf expliziten Anweisungen und von Menschen definierten Regeln beruht, können Maschinen mit KI riesige Datenmengen verarbeiten und sich selbstständig an neue Situationen anpassen. Der Vorteil von KI gegenüber herkömmlichen Programmieren besteht in der Möglichkeit, viel mehr Daten zu verarbeiten, als der Mensch kann. Dies führt zu genaueren Anwendungen. Maschinelles Lernen und Deep Learning sind Teil der KI.

Maschinelles Lernen verwendet statistische Lernalgorithmen, um Systeme zu erstellen, die während des Trainings lernen und sich verbessern können, ohne dass sie neu programmiert werden, z. B. um zu bestimmen, was in Bildern oder Videostreams vor sich geht (Computer Vision). Computer Vision beruht üblicherweise auf manueller Merkmalsextraktion, bei der Menschen die zu erfassenden Merkmale in Bildern oder Video definieren. Der Algorithmus lernt, diese Merkmale zu kombinieren, indem er große Mengen an durch Menschen erfassten und mit Anmerkungen versehenen Schulungsdaten betrachtet. Die Daten werden in das System eingespeist, bis das Programm genug gelernt hat, um zu erkennen, was erforderlich ist. Wenn dies beendet ist, wird das Programm nichts Neues lernen.

Deep Learning ist das datengetriebene Lernen von Funktionen und deren Kombination. Ähnlich wie das menschliche Gehirn kann der Algorithmus sehr tiefe Strukturen aus verketteten Merkmalskombinationen erlernen, die in künstlichen neuronalen Netzen simuliert werden, dem häufigsten Algorithmientyp beim Deep Learning. Deep-Learning-Algorithmen können eine größere Anzahl von Merkmalskombinationen nutzen und so kompliziertere Aufgaben in Angriff nehmen und höhere Genauigkeit erzielen.

Kameras mit einer DLPU (Deep Learning Processing Unit) bieten eine feinere Klassifizierung der erfassten Objekte. Dies kann bei Zeitdruck sehr nützlich sein, da die Klassifizierung direkt auf der Kamera stattfinden kann. Deep Learning-basierte Analysefunktionen eignen sich ideal für anspruchsvollere Anforderungen und komplexere Szenen. Außerdem verfügen sie über bessere

Erkennungs- und Klassifizierungsmöglichkeiten für Personen in ungewöhnlichen Positionen (z. B. gebückt) und für Objekte, die nur teilweise sichtbar sind. Bei ausreichenden Trainingsdaten können Deep-Learning-Algorithmen Objektattribute genau detektieren, z. B. die Farbe der Kleidung, das Vorhandensein eines Hutes, die Erfassung von Taschen und vieles mehr.

13.6 AXIS Camera Application Platform

Die meisten Axis Geräte unterstützen unsere offene Anwendungsplattform AXIS Camera Application Platform (ACAP). Diese leistungsstarke Plattform nutzt bekannte Toolchains, Open-Source-APIs nach Industriestandard und höhere Programmiersprachen. Sie ermöglicht die Entwicklung, Bereitstellung und Integration von Anwendungen direkt in der Kamera (Edge-basiert), maßgeschneidert für spezifische Kundenanforderungen. Damit können Anwendungen direkt auf dem Gerät ausgeführt werden, was erhebliche Vorteile wie geringere Latenzzeiten, minimierte Netzwerkbandbreite und besseren Datenschutz mit sich bringt. Die Maximierung der Verarbeitungseffizienz und der Systemgesamtleistung kommt sowohl den Endbenutzern als auch den Entwicklern zugute. Die Endbenutzer erhalten ein leistungsstarkes, optimiertes System. Entwickler können sich hingegen auf die Logik der Anwendung statt auf Plattformbeschränkungen konzentrieren. Dies reduziert die Barrieren für die Entwicklung und ermöglicht bedeutende Innovationen auf Axis Geräten.

14. Netzwerktechnologien

Für die Unterstützung und Bereitstellung der vielen Vorteile eines Netzwerk-Videosystems werden unterschiedliche Netzwerk-Technologien verwendet. In diesem Kapitel werden zuerst die lokalen Netzwerke (LAN) und insbesondere das Ethernet-Netzwerk und die Komponenten, die es unterstützen, behandelt. Auch die Verwendung von Power over Ethernet wird behandelt.

Anschließend wird die Internetkommunikation mit Themen wie IP-Adressierung (Internet Protocol) behandelt, einschließlich der Frage, wie auf Netzwerk-Videoprodukte über das Internet zugegriffen werden kann. Wir behandeln auch virtuelle lokale Netzwerke, Quality of Service und einen Überblick über die für Netzwerk-Video verwendeten Datenübertragungsprotokolle.

14.1 LAN und Ethernet

Bei einem lokalen Netzwerk (LAN) handelt es sich um eine Gruppe von Computern, die lokal verbunden sind, um miteinander zu kommunizieren und Ressourcen wie z. B. Drucker gemeinsam zu nutzen. Daten werden in Form von Paketen gesendet und für die Übertragung dieser Pakete können verschiedene Technologien eingesetzt werden. Die am weitesten verbreitete LAN-Technologie ist Ethernet, das in der Norm IEEE 802.3 spezifiziert ist. Andere Typen von Netzwerktechnologien für LANs sind Token Ring und FDDI (Fiber Distributed Data Interface).

Heute verfügt Ethernet über eine Sterntopologie, in der einzelne Knoten (Geräte) über aktive Netzwerkgeräte wie beispielsweise Switches miteinander verbunden sind. Ein LAN kann mehrere tausend vernetzte Geräte umfassen.

Es gilt die Faustregel, stets ein Netzwerk einzurichten, das eine größere Kapazität hat, als gegenwärtig erforderlich ist. Für ein zukunftssicheres Netzwerk können Sie ein Netzwerk einrichten, von dem anfänglich nur 30 % der Gesamtkapazität genutzt werden. Da heute mehr und mehr Anwendungen über Netzwerke ausgeführt werden, wird eine immer höhere Netzwerkleistung erforderlich sein. Während Netzwerk-Switches sich nach einigen Jahren leicht aktualisieren lassen, ist der Austausch von Kabeln meist ein aufwendigeres Unterfangen.

14.1.1 Arten von Ethernet-Netzwerken

Im Folgenden finden Sie die gebräuchlichsten Arten von Ethernet-Netzwerken für die Videosicherheitsbranche. Es können Twisted Pair- oder Glasfaserkabel verwendet werden.

Fast Ethernet. Kann Daten mit einer Geschwindigkeit von 100 Mbit/s übertragen. Das ältere Ethernet mit 10 Mbit/s wird immer noch installiert und verwendet, aber solche Netzwerke bieten für manche Netzwerk-Video Anwendungen nicht genug Bandbreite. Die meisten Geräte sind mit einer 10BASE-T/100BASE-TX-Ethernet-Schnittstelle oder kurz „10/100-Schnittstelle“ ausgestattet, die sowohl 10-Mbit/s- als auch Fast Ethernet unterstützt. Der Twisted Pair-Kabeltyp, der Fast Ethernet unterstützt, wird als Cat-5-Kabel bezeichnet.

Gigabit Ethernet Unterstützt eine Datenrate von 1.000 Mbit/s (1 Gbit/s) und wird heute häufiger verwendet als Fast Ethernet. Für das Backbone-Netzwerk, das viele Netzwerk-Kameras miteinander verbindet, kann 1 oder 10 Gbit/s Ethernet erforderlich sein. Der für das Gigabit-Ethernet erforderliche Twisted Pair-Kabeltyp ist das Cat-5e-Kabel, in dem alle vier verdrehten Drahtpaare verwendet werden, um die hohen Datenraten zu erzielen. Für Netzwerk-Videosysteme werden Kabel ab Cat-5e empfohlen. Die meisten Schnittstellen sind abwärtskompatibel mit 10- und 100-Mbit/s-Ethernet und werden in der Regel als „10/100/1000-Schnittstellen“ bezeichnet. Für Übertragungen über größere Entfernungen können Glasfaserkabel verwendet werden, z. B. 1000BASE-SX (bis zu 550 m) und 1000BASE-LX (bis zu 550 m mit Multimode-Glasfasern und 5.000 m mit Monomode-Fasern).

Ethernet 10 Gigabit. Unterstützt eine Datenrate von 10 GBit/s (10.000 Mbit/s). 10GBASE-LX4, 10GBASE-ER und 10GBASE-SR können mit Glasfaserkabeln Entfernungen von bis zu 10 km abdecken. Für eine Twisted Pair-Lösung ist ein qualitativ äußerst hochwertiges Kabel (Cat-6a oder Cat-7) erforderlich. 10 Gbit/s-Ethernet wird hauptsächlich als Backbone für Anwendungen mit hohen Datenraten verwendet.

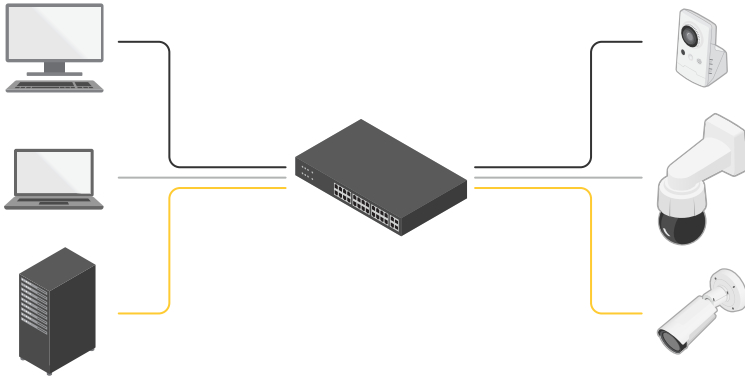
14.1.2 Anschließen von Netzwerk-Geräten und -Switches

Für die Netzwerkverbindung mehrerer Geräte in einem LAN sind Geräte wie z. B. Netzwerk-Switches erforderlich. Die Hauptfunktion eines Switches besteht im Übertragen von Daten von einem Gerät zu einem anderen im selben Netzwerk. Die Daten werden effizient von einem Gerät direkt an das Zielgerät weitergeleitet, ohne dass andere Geräte im selben Netzwerk davon beeinflusst werden.

Ein Netzwerk-Switch registriert die MAC-Adressen (Media Access Control) aller Geräte, die mit ihm verbunden sind. Jedes Netzwerkgerät verfügt über eine eindeutige MAC-Adresse, die aus einer Reihe von vom Hersteller vorgegebenen Ziffern und Buchstaben im Hexadezimalformat besteht. Die Adresse steht häufig auf dem Typenschild des Produktes. Wenn ein Netzwerk-Switch Daten

empfängt, leitet er diese nur an den Port weiter, der mit dem Gerät verbunden ist, das die richtige MAC-Zieladresse aufweist.

Die Leistung von Netzwerk-Switches wird in der Regel in Raten pro Port sowie als Backplane-Kapazität oder interne Rate angegeben (sowohl in Bitraten als auch in Paketen pro Sekunde). Die Port-Raten weisen die maximale Kapazität bestimmter Ports aus. Dies bedeutet, dass die Geschwindigkeit eines Switches (z. B. 100 Mbit/s) häufig auch der Leistung des Ports entspricht.



Bei einem Netzwerk-Switch werden Daten sehr effizient übertragen, da der Datenverkehr direkt von einem Gerät zu einem anderen geleitet werden kann, ohne dass andere Ports am Switch davon betroffen sind.

Ein Netzwerk-Switch unterstützt in der Regel verschiedene Datenraten gleichzeitig. Die gebräuchlichsten Datenraten waren 10/100 Mbit/s mit Unterstützung von 10 Mbit/s und Fast Ethernet. Heute verfügen die meisten Netzwerk-Switches jedoch über 10/100/1000-Schnittstellen und unterstützen daher gleichzeitig 10 Mbit/s, Fast-Ethernet und Gigabit-Ethernet. Die Datenrate und der Übertragungsmodus zwischen dem Port eines Switch und einem verbundenen Gerät werden üblicherweise automatisch verhandelt, wobei die höchste gemeinsame Datenrate und der optimale Übertragungsmodus verwendet werden. Ein Netzwerk-Switch ermöglicht es einem verbundenen Gerät zudem, im Vollduplex-Modus ausgeführt zu werden, d. h. dass es Daten gleichzeitig senden und empfangen kann, was zu einer höheren Leistung führt.

Netzwerk-Switches können zudem mit verschiedenen Features oder Funktionen ausgestattet sein. So sind zum Beispiel einige mit Routerfunktionen ausgestattet und viele unterstützen Power over Ethernet. Ein Switch mit Quality of Service kann steuern, wie viel Bandbreite von verschiedenen Anwendungen genutzt wird.

14.1.3 Power over Ethernet

Mit Power over Ethernet (PoE) können die an das Ethernet-LAN angeschlossenen Geräte über das gleiche Kabel, das auch für die Datenübertragung verwendet wird, mit Strom zu versorgt werden. Power over Ethernet wird überwiegend für die Stromversorgung von IP-Telefonen, drahtlosen Zugriffspunkten und Geräten wie Kameras verwendet.

Der Hauptvorteil von PoE sind die Kosteneinsparungen. Die Installation durch einen zertifizierten Elektriker oder eine separate Stromleitung sind bei der Installation von PoE nicht erforderlich, was vor allem in schwer zugänglichen Bereichen von Vorteil ist. Da keine Stromkabel verlegt werden müssen, können pro Kamera potenziell Hunderte von Euro eingespart werden. PoE erleichtert zudem die Verlegung des Standorts einer Kamera oder das Hinzufügen weiterer Kameras zu einem bestehenden Videosicherheitssystem.

Darüber hinaus kann PoE ein Überwachungssystem sicherer machen. Ein System mit PoE kann vom Server-Raum aus mit Strom versorgt werden, der häufig mit einer USV (Unterbrechungsfreie Stromversorgung) abgesichert ist. Dadurch bleibt das System auch bei einem Stromausfall funktionsfähig.

Aufgrund seiner Vorteile wird die Verwendung von PoE bei möglichst vielen Geräten empfohlen. Der vom PoE-fähigen Switch oder Midspan gelieferte Strom muss für die angeschlossenen Geräte ausreichen, und die Geräte müssen die Spannungsklassifizierung unterstützen.

802.3af-Standard, PoE+ und High-PoE

Die meisten derzeit erhältlichen PoE-Geräte erfüllen die Anforderungen des IEEE 802.3af-Standards, der im Jahr 2003 veröffentlicht wurde. Im Rahmen des Standards wird das Gerät, das den Strom liefert, als „Power Sourcing Equipment“ (PSE) bezeichnet. Hierbei kann es sich um einen PoE-fähigen Switch oder Midspan handeln. Das Gerät, das mit Strom versorgt wird, wird als „Powered Device“ (PD) bezeichnet. Diese Funktion ist häufig in das Netzwerkgerät integriert. Alternativ kann sie über einen eigenständigen Splitter bereitgestellt werden.

Abwärtskompatibilität mit Netzwerk-Geräten, die nicht mit PoE kompatibel sind, ist gewährleistet. Der Standard umfasst eine Methode, mit der automatisch geprüft wird, ob ein Gerät PoE unterstützt. Nur wenn dies der Fall ist, wird es mit Strom versorgt. Dies bedeutet auch, dass das an einen PoE-Switch angeschlossene Ethernetkabel nur zur Stromversorgung verwendet werden kann, wenn es an einem PoE-fähigen Gerät angeschlossen ist. Dadurch wird bei der Installation oder Neuverkabelung eines Netzwerks die Gefahr eines Stromschlags vermieden.

Ein Twisted Pair-Kabel enthält vier Adernpaare. PoE kann entweder die beiden nicht genutzten oder die Adernpaare verwenden, über die auch die Datenübertragung erfolgt. Bei Switches mit

integriertem PoE erfolgt die Stromversorgung häufig über die Adernpaare für die Datenübertragung, während Midspans in der Regel die beiden ungenutzten Adernpaare verwenden. Ein PD unterstützt beide Optionen.

Gemäß IEEE 802.3af liefert ein PSE pro Anschluss bei einer Spannung von 48V DC eine maximale Leistung von 15,4 W pro Port. Da bei einem Twisted-Pair-Kabel ein gewisser Leistungsverlust auftritt, werden dem PD nur 12,95 W garantiert. Der IEEE 802.3af-Standard legt verschiedene Leistungskategorien für PDs fest.

PSE wie Switches und Midspans liefern normalerweise eine bestimmte Menge an Strom, in der Regel 300 – 500 W. Bei einem Switch mit 48 Ports würde dies 6 – 10 W pro Port bedeuten, wenn alle Ports mit Geräten verbunden sind, die PoE verwenden. Sofern die PDs keine Stromklassifizierung unterstützen, müssen für jeden PoE-Port ganze 15,4 W reserviert werden, so dass ein Switch mit 300 W nur 20 der 48 Ports mit Strom versorgen kann. Wenn jedoch alle Geräte dem Switch melden, dass es sich um Geräte der Klasse 1 handelt, kann der 300-W-Switch alle 48 Ports mit Spannung versorgen.

Class	Typ	Mindeststromstärke bei PSE	Maximale Stromstärke bei PD
0	Typ 1, 802.3af	15,4 W	0,44 W bis 12,95 W
1	Typ 1, 802.3af	4,0 W	0,44 W bis 3,84 W
2	Typ 1, 802.3af	7,0 W	3,84 W bis 6,49 W
3	Typ 1, 802.3af	15,4 W	6,49 W bis 12,95 W
4	Typ 2, 802.3at	30 W	12,95 W bis 25,5 W
6	Typ 3, 802.3bt	60 W	51 W
8	Typ 4, 802.3bt	90 W	71,3 W

Tabelle 14.1a *Stromklassifizierungen gemäß IEEE 802.3af, IEEE 802.3at und IEEE 802.3bt.*

Die meisten unbeweglichen Netzwerk-Kameras können über PoE gemäß dem IEEE-802.3af-Standard mit Strom versorgt werden und entsprechen in der Regel Geräteklasse 1 oder 2.

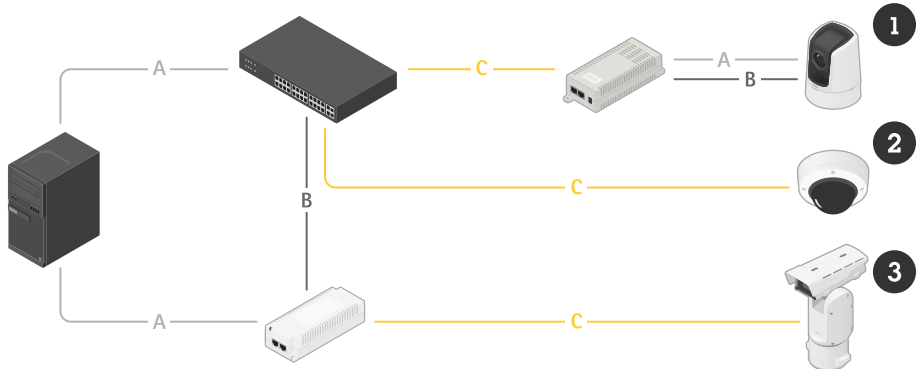
Weitere PoE-Standards sind IEEE 802.3at, auch bekannt als PoE+, und IEEE 802.3bt. Bei PoE+ wurde die Leistungsgrenze auf mindestens 30 W über zwei Adernpaare von einem PSE erhöht. Bei einem Strombedarf, der über den PoE+ Standard hinausgeht, verwendet Axis den Begriff High PoE,

wobei die Leistungsgrenze über die vier Adernpaare auf mindestens 60 W erhöht wird. Damit sind 51 W für PoE garantiert.

PoE+ und High PoE Midspans und Splitter können für Geräte wie z. B. PTZ-Kameras mit Motorsteuerung sowie für Kameras mit Heizelementen und Lüftern verwendet werden, die mehr Leistung benötigen, als im Rahmen des IEEE-802.3af-Standards verfügbar ist. Für PoE+ und High PoE wird ein Kabel mit Cat-5e- oder höher empfohlen.

Der Midspan, der Strom über ein Ethernet-Kabel leitet, wird zwischen den Netzwerk-Switch und die versorgten Geräte geschaltet. Damit der Datentransfer nicht beeinträchtigt wird, sollte bedacht werden, dass die maximale Entfernung zwischen der Datenquelle (z. B. dem Switch) und dem Gerät nicht mehr als 100 m betragen darf. Daher sollten der Midspan und die aktiven Splitter innerhalb einer Entfernung von 100 m platziert werden.

Ein Splitter trennt den Strom- und Datenpfad in einem Ethernetkabel auf und leitet ihn zu zwei separaten Anschlüssen. Diese können dann an ein Endgerät angeschlossen werden, das keine integrierte Unterstützung für PoE bietet. Da PoE oder PoE+ nur 48 V DC liefert, besteht eine andere Funktion des Splitters darin, die Spannung auf eine für das Endgerät geeignete Versorgungsspannung zu reduzieren, beispielsweise 12 V oder 5 V.



Mit Splitttern und Midspans lassen sich Kameras ohne PoE-Unterstützung (1), PoE-fähige Kameras (2) und Kameras kombinieren, die mehr Strom benötigen, als PoE im selben System bereitstellen kann (3).

- A. Strom (von der USV)
- B. Ethernet (vom Netzwerk-Switch)
- C. Power over Ethernet

1. Eine Kamera ohne PoE-Unterstützung kann über einen Splitter angeschlossen werden.
2. Eine PoE-fähige Kamera erhält über ein Ethernet-Kabel des Switchs sowohl Strom als auch Ethernet-Konnektivität.
3. Eine Kamera, die mehr Strom benötigt, als ein normaler PoE-Switch bereitstellen kann, kann über einen Midspan angeschlossen werden, der die Kamera zusätzlich mit Strom versorgen kann. Der Midspan empfängt und gibt Daten vom Switch weiter, während die PoE-Leistung zur Kamera von der Stromversorgung stammt – in diesem Beispiel über die USV.

14.2 Senden von Daten über das Internet

Die grundlegenden Komponenten der Internetkommunikation umfassen:

Router Um Datenpakete über das Internet von einem LAN zu einem anderen weiterzuleiten, müssen Netzwerk-Router verwendet werden. Diese Geräte leiten basierend auf IP-Adressen Informationen von einem Netzwerk zu einem anderen weiter. Ein Router leitet nur Datenpakete weiter, die an ein anderes Netzwerk adressiert sind. Er wird zumeist für Verbindungen eines lokalen Netzwerks mit dem Internet verwendet. Router werden mitunter als Gateways bezeichnet.

Firewalls Mit einer Firewall soll der unbefugte Zugriff auf ein privates Netzwerk verhindert werden. Firewalls können in Hardware und/oder in Software implementiert werden. Sie werden in der Regel verwendet, um nicht autorisierte Internet-Benutzer am Zugriff auf private, mit dem Internet verbundene Netzwerke zu hindern. Nachrichten in oder aus dem Internet passieren die Firewall, die jede einzelne Nachricht prüft und gegebenenfalls blockiert, wenn sie nicht den festgelegten Sicherheitskriterien entspricht.

Internetverbindungen. Bei Verbindungen mit dem Internet beschreibt der Begriff „Upstream“ die Übertragungsrate (Bandbreite), mit der Daten von dem Gerät in das Internet hochgeladen werden, beispielsweise wenn Videos von einer Netzwerk-Kamera gesendet werden. Downstream ist die Übertragungsgeschwindigkeit beim Herunterladen von Dateien, z. B. beim Empfang von Videos auf einem PC. In den meisten Szenarien ist die Download-Geschwindigkeit das wichtigste Kriterium. Bei einer Netzwerk-Videoanwendung mit einer Netzwerk-Kamera an einem entfernten Standort ist jedoch die Upstream-Geschwindigkeit am wichtigsten, da die Videos von der Netzwerk-Kamera in das Internet hochgeladen werden. Ältere Internettechnologien mit asymmetrischen Bandbreiten wie ADSL (Asymmetric Digital Subscriber Line) sind für eine Netzwerk-Videoanwendung möglicherweise nicht geeignet, da die Upstream-Kapazität zu gering ist.

Um Daten von einem Gerät in einem LAN an ein Gerät in einem anderen LAN zu senden, ist eine Standardkommunikationsmethode erforderlich, da die lokalen Netzwerke möglicherweise unterschiedliche Technologien verwenden. Diese Anforderung führte zur Entwicklung von IP-Adressen und den vielen IP-basierten Protokollen für die Kommunikation im Internet.

14.2.1 IP-Adressierung

Geräte, die über das Internet mit anderen Geräten kommunizieren möchten, müssen über eine eindeutige und geeignete IP-Adresse verfügen, um die sendenden und empfangenden Geräte zu identifizieren. Aktuell gibt es zwei IP-Versionen: IP Version 4 (IPv4) und IP Version 6 (IPv6). Der Hauptunterschied zwischen den beiden besteht darin, dass eine IPv6-Adresse länger ist als eine IPv4-Adresse (128 Bits gegenüber 32 Bits). IPv4-Adressen werden heute am häufigsten verwendet.

14.2.1.1 IPv4-Adressen

IPv4-Adressen sind in vier Blöcken gruppiert, die jeweils durch einen Punkt voneinander getrennt sind. Jeder Block ist eine Zahl zwischen 0 und 255, z. B.: 192.168.12.23.

Einige Blöcke von IPv4-Adressen sind ausschließlich für die private Nutzung reserviert. Diese privaten IP-Adressen sind 10.0.0.0 bis 10.255.255.255, 172.16.0.0 bis 172.31.255.255 und 192.168.0.0 bis 192.168.255.255. Diese Adressen können nur in privaten Netzwerken verwendet werden und dürfen nicht über einen Router an das Internet weitergeleitet werden. Alle Geräte, die über das Internet kommunizieren möchten, müssen über eine eigene öffentliche IP-Adressen verfügen, die von einem Internetdienstanbieter zugeordnet wird. Die Adresse kann entweder eine dynamische IP-Adresse, die sich während einer Sitzung ändern kann, oder eine statische Adresse sein, für die in der Regel eine zusätzliche monatliche Gebühr anfällt.

Ports

Eine Portnummer definiert einen bestimmten Dienst oder eine Anwendung, damit der empfangende Server (z. B. eine Netzwerk-Kamera) weiß, wie die eingehenden Daten verarbeitet werden müssen. Wenn ein Computer Daten sendet, die an eine bestimmte Anwendung gebunden sind, fügt er in der Regel automatisch die Portnummer einer IP-Adresse hinzu.

Portnummern liegen zwischen 0 und 65535. Einige Anwendungen verwenden Portnummern, die ihnen von der Internet Assigned Numbers Authority (IANA) vorab zugewiesen wurden. So wird z. B. bei einer Netzwerk-Kamera der Webdienst über HTTP in der Regel Port 80 zugeordnet.

IPv4-Adressen festlegen

Damit ein Gerät in einem IP-Netzwerk betrieben werden kann, muss dem Gerät eine IP-Adresse zugewiesen werden. Eine IPv4-Adresse für ein Gerät von Axis kann automatisch über DHCP (Dynamic Host Configuration Protocol) eingerichtet werden. Hierfür ist im Netzwerk ein DHCP-Server erforderlich. Außerdem kann die IP-Adresse mithilfe einer Verwaltungssoftware wie zum Beispiel AXIS Device Manager eingerichtet werden. Die Adresse kann zudem manuell eingerichtet werden. Dies kann erfolgen, indem auf der Webseite des Geräts die statische IP-Adresse, die

Subnetzmaske sowie die IP-Adressen von Standardrouter, DNS-Server (Domain Name System) und NTP-Server (Network Time Protocol) eingegeben werden.

Ein DHCP-Server verwaltet einen IP-Adressen-Pool, den er dynamisch Netzwerkgeräten zuweisen kann. Diese Funktion wird häufig von einem Breitbandrouter ausgeführt, der wiederum in der Regel mit dem Internet verbunden ist und eine eigene öffentliche IP-Adresse von einem Internetdienstanbieter erhält. Bei der Verwendung einer dynamischen IP-Adresse kann sich die IP-Adresse eines Netzwerkgeräts täglich ändern. Bei dynamischen IP-Adressen wird empfohlen, dass der Benutzer einen Domainnamen für das Gerät auf einem dynamischen DNS-Server registriert (zum Beispiel *www.mycamera.com*), wodurch der Domainname des Geräts mit einer beliebigen, aktuell zugewiesenen IP-Adresse verknüpft werden kann. Ein Domainname kann über einige der bekannten Dynamic-DNS-Sites wie zum Beispiel *www.dyndns.org* registriert werden.

IPv4-Adressen werden mit DHCP folgendermaßen festgelegt: Wenn ein Netzwerkgerät (wie z. B. eine Netzwerk-Kamera) online geht, fordert es die Konfiguration von einem DHCP-Server an. Der DHCP-Server antwortet mit der vom Gerät angeforderten Konfiguration. Dies beinhaltet in der Regel die IP-Adresse, die Subnetzmaske und die IP-Adressen für den Router sowie den DNS- und NTP-Server. Das Gerät prüft zuerst, ob die angebotene IP-Adresse nicht bereits im lokalen Netzwerk verwendet wird, weist die Adresse dann sich selbst zu und kann anschließend einen dynamischen DNS-Server mit seiner aktuellen IP-Adresse aktualisieren, sodass die Benutzer über den Domain-Namen auf das Gerät zugreifen können.

AXIS Device Manager ist eine Software, die automatisch IP-Adressen finden und einstellen und den Verbindungsstatus anzeigen kann. Mit ihr können statische und private IP-Adressen für alle Axis Netzwerk-Video-Produkte zugewiesen werden. Dies wird empfohlen, wenn eine Video Management Software für den Zugriff auf die Netzwerk-Videoprodukte verwendet wird. In einem Netzwerk-Videosystem mit möglicherweise Hunderten von Kameras ist ein Softwareprogramm wie AXIS Device Manager für die effiziente Verwaltung des Systems hilfreich.

NAT (Network Address Translation)

Wenn ein Netzwerkgerät mit einer privaten IP-Adresse Informationen über das Internet senden möchte, muss es hierfür einen Router verwenden, der NAT unterstützt. Mit dieser Technik wandelt der Router für die Offenlegung im Internet die private in eine öffentliche IP-Adresse um.

14.2.1.2 IPv6-Adressen

Eine IPv6-Adresse wird in Hexadezimalnotation mit Doppelpunkten angegeben. Letztere teilen die Adresse in acht Blöcke zu je 16 Bit auf, z. B. 2001:0da8:65b4:05d3:1315:7c1f:0461:7847.

Ein Hauptvorteil von IPv6 ist neben der Verfügbarkeit einer großen Anzahl von IP-Adressen die Möglichkeit, dass ein Gerät seine IP-Adresse automatisch anhand seiner MAC-Adresse konfigurieren kann. Für die Kommunikation über das Internet fordert der Host vom Router das erforderliche Präfix des öffentlichen Adressblocks und weitere Informationen an. Daraufhin werden das Präfix und das Suffix des Hosts verwendet, so dass IP-Adressen bei IPv6 nicht mehr per DHCP zugewiesen oder manuell eingestellt werden müssen. Zu den weiteren Vorteilen von IPv6 gehören die Neunummerierung zur Vereinfachung des Wechsels ganzer Unternehmensnetzwerke zwischen Providern, schnelleres Routing, Punkt-zu-Punkt-Verschlüsselung gemäß IPsec und Konnektivität unter Verwendung derselben Adresse in wechselnden Netzwerken (Mobile IPv6).

IPv6-Adressen werden in URLs in eckigen Klammern angegeben. Ein bestimmter Port kann wie folgt adressiert werden: `http://[2001:0da8:65b4:05d3:1315:7c1f:0461:7847]:8081/`

Eine IPv6-Adresse lässt sich ganz einfach durch das Aktivieren des entsprechenden Kontrollkästchens im Gerät für ein Axis Netzwerkgerät einrichten. Das Gerät erhält daraufhin eine IPv6-Adresse gemäß der Konfiguration im Netzwerk-Router.

14.2.2 Datenübertragungsprotokolle für Netzwerk-Video

Das Transmission Control Protocol (TCP) und das User Datagram Protocol (UDP) sind IP-basierte Protokolle zum Senden von Daten. Diese Übertragungsprotokolle agieren als Träger für viele andere Protokolle. So erfolgt z. B. HTTP (Hyper Text Transfer Protocol), das zum Browsen von Webseiten verwendet wird, über TCP.

TCP bietet einen zuverlässigen, verbindungsbasierten Datenübertragungskanal. Es stellt sicher, dass die von einem Punkt gesendeten Daten am anderen Punkt ankommen. Die hohe Zuverlässigkeit von TCP durch erneute Übertragung kann unter Umständen zu erheblichen Verzögerungen führen, aber im Allgemeinen verwendet man TCP, wenn zuverlässige Kommunikation wichtiger ist als eine geringere Verzögerung.

UDP ist ein verbindungsloses Protokoll, bei dem die Zustellung der übertragenen Daten nicht garantiert wird, so dass der gesamte Kontrollmechanismus und die Fehlerprüfung der Anwendung selbst überlassen werden. UDP überträgt verlorene Daten nicht erneut und verursacht daher keine zusätzliche Verzögerung.

Protokoll	Übertra- gungsproto- koll	Port	Allgemeine Verwendung	Netzwerkvideoverwendung
FTP (File Transfer Protocol)	TCP	21	Dateiübertragung	Übertragung von Bildern oder Video an FTP-Server oder Anwendungen
SMTP (Simple Mail Transfer Protocol)	TCP	25	Protokoll zum Senden von E-Mails	Das Netzwerk-Videoprodukt sendet über den integrierten E-Mail-Client Alarmbenachrichtigungen.
HTTP (Hyper Text Transfer Protocol)	TCP	80	Browsen im Internet, d. h. Abrufen von Webseiten von Webservern	Das Videogerät fungiert als Webserver, sodass die Videos für den Benutzer- oder Anwendungsserver verfügbar sind.
HTTPS (Hypertext Transfer Protocol over Transport Layer Security)	TCP	443	Sicherer Zugriff auf Webseiten mithilfe von Verschlüsselung	Sichere Übertragung von Videos von Netzwerk-Videoprodukten.
RTP (Real Time Protocol)	UDP/TCP	Nicht definiert	RTP-standardisiertes Paketformat für die Übertragung von Audio- und Videodaten über das Internet. Wird häufig in Streaming-Mediansystemen oder für Videokonferenzen verwendet.	Übertragung von Video und Synchronisierung von Video und Audio. RTP bietet eine fortlaufende Nummerierung und Zeitstempelung von Datenpaketen, was eine korrekte Wiederausammensetzung ermöglicht. Unicast oder Multicast.
RTSP (Real Time Streaming Protocol)	TCP	554	Einrichten und Steuern von Multimedia-Sitzungen über RTP	

Tabelle 14.2a *Gängige TCP/IP-Protokolle und Ports, die für Netzwerk-Videos verwendet werden.*

Weitere Informationen zur Axis Dokumentation zu häufig verwendeten Ports finden Sie unter <https://help.axis.com/axis-os-knowledge-base#commonly-used-network-ports>

14.2.3 SIP

SIP (Session Initiation Protocol) ist ähnlich wie HTTP und SMTP ein textbasiertes Protokoll für die Kommunikation über IP-Netzwerke. Es wird zum Starten, Ändern und Beenden von Mediastream-Sitzungen verwendet, die Sprach- und Videoelemente enthalten können. SIP ist das Standardprotokoll für Voice-over-IP-Anwendungen (VoIP) und einheitliche Kommunikationsplattformen für Videokonferenzen, Anrufsteuerung und Instant Messaging. SIP ermöglicht die Verbindung, Integration und Steuerung von Axis Netzwerkprodukten.

SIP-Anrufe können auf verschiedene Art und Weise eingerichtet werden, es gibt jedoch drei Haupttypen:

Peer-to-Peer-Anrufe (auch als lokale Anrufe bezeichnet). Dabei handelt es sich um Anrufe zwischen zwei Geräten (z. B. Computern, Netzwerk-Lautsprechern, Softphones, Tüstationen, Kameras oder IP-Festnetztelefonen) im selben Netzwerk. Der Anruf erfolgt an die SIP-Adresse des Geräts.

SIP-Server-Anrufe (auch als PBX-Anrufe (Telefonanlage) bezeichnet). Für SIP-Server-Anrufe muss das Gerät mit einem SIP-Server verbunden sein, der die Anrufverbindungen verarbeitet. Ein SIP-Server oder eine Nebenstellenanlage ist ein Hub, der wie eine traditionelle Telefonzentrale funktioniert. Er kann im Intranet oder von einem Drittanbieter gehostet werden. SIP-fähige Geräte werden beim SIP-Server registriert und können sich anhand ihrer SIP-Adressen kontaktieren. Eine Nebenstellenanlage kann u. a. den Anrufstatus anzeigen, Rufweiterleitungen zulassen, Voicemail verarbeiten und Anrufe weiterleiten.

Anhand der SIP-Adressen (auch als SIP-URIs [Uniform Resource Identifiers] oder SIP-Nummern bezeichnet) werden die Benutzer ähnlich wie mit Telefonnummern oder E-Mail-Adressen in einem Netzwerk identifiziert. Wie E-Mail-Adressen sind auch SIP-Adressen ein URI-Typ, der zwei benutzerspezifische Teile umfasst: eine Benutzer-ID oder Durchwahl sowie den Domain-Namen oder die IP-Adresse. Zusammen mit einem Präfix und dem @-Symbol bilden sie eine eindeutige Adresse. Bei einem Peer-to-Peer-Anruf enthält die SIP-Adresse eher die IP-Adresse als den Domain-Namen.

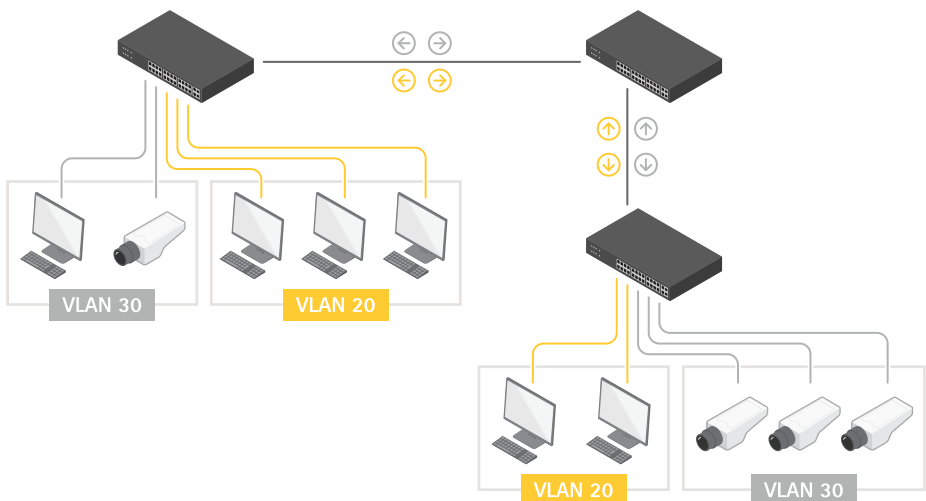
SIP-Ferngespräche. Bei Diensteanbietern, die ein SIP-Trunking anbieten, können über das herkömmliche Telefonnetz Anrufe getätigt und SIP-Geräten althergebrachte Telefonnummern

zugewiesen werden. Auf diese Weise können Anrufe von einem Netzwerk-Lautsprecher oder einer IP-Türstation zu einem Handy oder umgekehrt getätigt werden.

14.3 VLANs

Wenn ein Netzwerk-Videosystem umgesetzt wird, besteht häufig der Wunsch, das Netzwerk von anderen Netzwerken getrennt zu halten – sowohl aus Sicherheits- als auch aus Leistungsgründen. Auf den ersten Blick wäre es daher das Beste, ein separates Netzwerk einzurichten. Das Design würde zwar vereinfacht, die Kosten für den Kauf der Geräte, die Installation und die Verwaltung des Netzwerks wären jedoch häufig höher als bei der Verwendung eines virtuellen lokalen Netzwerks, dem sogenannten VLAN (Virtual Local Area Network).

VLAN ist eine Technologie zur virtuellen Segmentierung von Netzwerken, einer Funktion, die von den meisten Netzwerk-Switches unterstützt wird. Die Segmentierung erfolgt durch eine Aufteilung in logische Gruppen. Nur Benutzer in bestimmten Gruppen können Daten austauschen oder auf bestimmte Ressourcen im Netzwerk zugreifen. Wenn ein Netzwerk-Videosystem in ein VLAN segmentiert wird, können nur die Server in diesem VLAN auf die Netzwerk-Kameras zugreifen. VLANs bieten eine flexible und kostengünstigere Lösung als ein separates Netzwerk. Das primäre Protokoll für das Konfigurieren von VLANs ist IEEE 802.1Q. Es kennzeichnet jedes Einzelbild oder Paket mit zusätzlichen Bytes, um anzugeben, zu welchem virtuellen Netzwerk das Paket gehört.

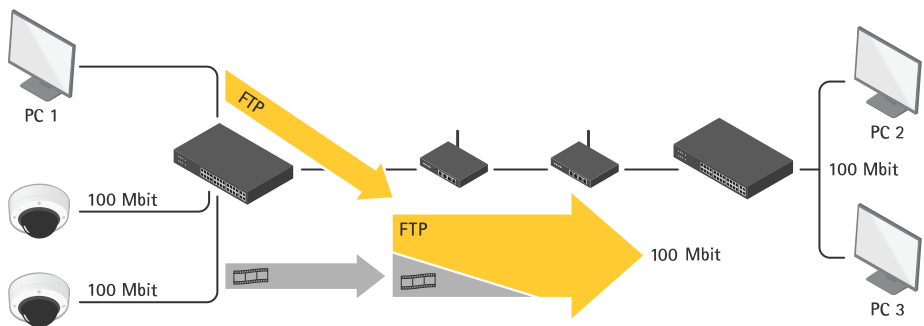


In dieser Abbildung sind die VLANs über mehrere Switches verteilt. Die beiden unterschiedlichen LANs werden in VLAN 20 und VLAN 30 segmentiert. Nur Mitglieder desselben VLAN können Daten im selben Netzwerk oder über verschiedene Netzwerke austauschen.

14.4 Quality of Service

Da verschiedene Anwendungen wie Telefon, E-Mail und Videosicherheit möglicherweise über ein IP-Netzwerk laufen, muss häufig die gemeinsame Nutzung der Netzwerkressourcen geregelt werden, um die Anforderungen der einzelnen Dienste zu erfüllen. Eine Lösung besteht darin, beim Datenverkehr im Netzwerk ein unterschiedliches Verhalten von Routern und Switches für unterschiedliche Dienstarten (Sprache, Daten, Video) zuzulassen. Mithilfe von Quality of Service (QoS) können verschiedene Netzwerkanwendungen in einem Netzwerk nebeneinander existieren, ohne bei der Bandbreitennutzung in Konflikt zu geraten.

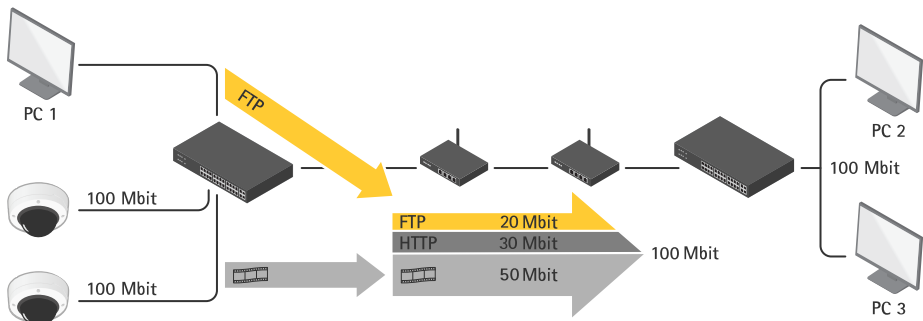
„Quality of Service“ bezieht sich auf eine Reihe von Technologien, z. B. DSCP (Differentiated Service Codepoint), die den Datentyp eines Datenpakets identifizieren und die Pakete in Datenverkehrsklassen einteilen können. Somit können die Datenverkehrsklassen für die Weiterleitung priorisiert werden. Ein Hauptvorteil eines QoS-Netzwerks ist die Möglichkeit der Priorisierung von Datenverkehr, damit wichtige Daten vor weniger wichtigen übertragen werden. Ein weiterer Vorteil ist die größere Zuverlässigkeit des Netzwerks, da die von einer Anwendung genutzte Bandbreite und damit die Verteilung der Bandbreite auf die Anwendungen gesteuert werden kann. Ein Beispiel für den Einsatz von QoS sind PTZ-Befehle, mit denen eine schnelle Kamerareaktion auf Bewegungsanforderungen gewährleistet wird. Damit QoS in einem Videonetzwerk verwendet werden kann, müssen alle Switches, Router und Netzwerk-Videogeräte QoS unterstützen.



Standardnetzwerk (nicht QoS-fähig). In diesem Beispiel teilen FTP- und Videostreaming 100 Mbit/s untereinander und die Videobandbreite kann nicht garantiert werden.

In dieser Illustration verfolgt PC 2 zwei Videostreams (von zwei Kameras). Jede Kamera überträgt mit 25 MBit/s. Plötzlich startet PC 3 eine Dateiübertragung von PC 1. In diesem Szenario versucht das File Transfer Protocol (FTP), die gesamte Bandbreite von 100 Mbit/s zwischen den beiden Routern zu nutzen, während die Videostreams versuchen, ihre Bildrate von 50 Mbit/s beizubehalten. Die verfügbare Bandbreite des Sicherheitssystems kann nicht mehr garantiert

werden und die Bildrate der Videos wird wahrscheinlich reduziert. Im schlimmsten Fall beansprucht der FTP-Datenverkehr die gesamte verfügbare Bandbreite.

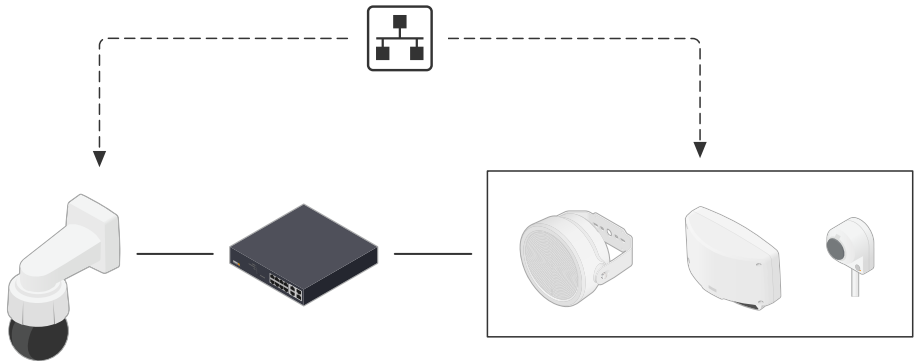


QoS-fähiges Netzwerk. Das Videostreaming verfügt über eine garantierte Bandbreite von bis zu 50 Mbit/s.

In dieser Abbildung wurde der erste Router so konfiguriert, dass er bis zu 50 Mbit/s der verfügbaren 100 Mbit/s für Video-Streaming nutzen kann. FTP-Datenverkehr darf 20 Mbit/s nutzen, HTTP und alle anderen Datenströme maximal 30 Mbit/s. Dadurch haben Videostreams immer die erforderliche Bandbreite zur Verfügung. Dateiübertragungen werden als weniger wichtig betrachtet und erhalten somit weniger Bandbreite, wobei dennoch Bandbreite zum Surfen im Internet und für weiteren Datenverkehr verfügbar ist. Beachten Sie, dass diese Einschränkungen nur gelten, wenn das Netzwerk stark ausgelastet ist. Ungenutzte Bandbreite kann von jeder Art von Datenverkehr genutzt werden.

14.5 Edge-to-Edge

„Edge-to-Edge“ ist eine Technologie, die es IP-Geräten ermöglicht, direkt miteinander zu kommunizieren, ohne den Kern des Systems durchlaufen zu müssen. Es ermöglicht die intelligente und automatische Kopplung von Axis Geräten.



Die Kamera ist über „Edge-to-Edge“ mit einem anderen Gerät (in diesem Fall einem Lautsprecher, einem Radargerät oder einem Mikrofon) gekoppelt.

Wenn Sie beispielsweise eine Kamera ohne Audiofunktion mit einem Lautsprecher koppeln, können Sie die Audio-Einstellungen des Lautsprechers direkt über die Weboberfläche der Kamera steuern. Die Kamera identifiziert sich zur VMS als Kamera mit integriertem Audioausgang und leitet alle abgespielten Audiosignale an den Lautsprecher weiter.

Wenn Sie eine reine Audio-Gegensprechanlage (als Hauptgerät) mit einer Kamera koppeln, können Sie die Video-Funktionen der Kamera über die Gegensprechanlage steuern, als wäre die Kamera fest integriert. Die Türsprechanlage kann den Videostream der Kamera abrufen und sendet ihn an Empfänger in VMS- oder SIP-Anrufen. Ebenso können Sie, wenn Sie ein Radargerät (als Hauptgerät) mit einem Lautsprecher koppeln, Audioinhalte über die Weboberfläche des Radargeräts abspielen.

Damit „Edge-to-Edge“ funktioniert, müssen beide Geräte im Netzwerk verbunden sein und das Hauptgerät muss „Edge-to-Edge“-Unterstützung bieten. Sie können ein Gerät direkt in der Weboberfläche des Hauptgeräts koppeln, indem Sie dessen IP-Adresse, Benutzernamen und Passwort wählen oder eingeben.

14.6 Portcast

Portcast ist eine einzigartige Technologie von Axis, mit der Sie einem angeschlossenen Host-Gerät Ports oder Sensoren hinzufügen können, ohne dass dafür eine zusätzliche Lizenz oder IP-Adresse erforderlich ist. Sie können beispielsweise eine Kamera, die über kein integriertes Mikrofon verfügt, mit Audio-Anschlüssen ausstatten oder I/O-Ports für die Überwachung des Zugangs hinzufügen. Sie können einen Sensor genau dort anbringen, wo er am nützlichsten ist, selbst wenn das Host-

Gerät an einer schwer zugänglichen Stelle mit einer Halterung montiert ist. Ein Luftqualitätssensor kann beispielsweise in Atemhöhe angebracht werden, während die damit verbundene Kamera an der Decke mit einer Halterung montiert ist.

Ein Portcast-Gerät wird zwischen dem Host-Gerät und dessen Stromquelle angeschlossen, wobei das Host-Gerät als Gateway fungiert. Die Funktionen des Portcast-Geräts werden direkt in der Schnittstelle des Host-Geräts angezeigt, als wären sie fest integriert. Es sind keine zusätzlichen Schritte der Konfiguration und keine separate Schnittstelle für die Verwaltung erforderlich.

Das Portcast-Gerät wird über die bestehende PoE-Verbindung zwischen dem Host-Gerät und der Stromquelle mit Strom versorgt, sodass kein zusätzliches Netzteil erforderlich ist. Da die Stromversorgung gemeinsam mit dem Host-Gerät erfolgt, ist dies bei energieintensiven Produkten eine Überlegung wert. In diesen Fällen können Sie einen Midspan verwenden, um zusätzliche Energie bereitzustellen. Die maximale Kabellänge zwischen der Stromquelle und dem Host-Gerät beträgt gemäß dem PoE-Protokoll 100 Meter.

Portcast bietet eine kabelgebundene Alternative zu drahtlosen Protokollen wie Bluetooth® oder Z-Wave®. Sie profitieren von denselben Vorteilen hinsichtlich der Erweiterung der Gerätefunktionen, ohne dabei auf drahtlose Kommunikation angewiesen zu sein. Dies eignet sich besonders für Umgebungen, in denen die drahtlose Konnektivität eingeschränkt ist oder in denen eine sicherere, störungsfreie Verbindung bevorzugt wird.

15.Systemschutz

Cyberbedrohungen werden häufig mit Hackern und Schadenknaben in Verbindung gebracht. Allerdings kann sich auch unbeabsichtigter Missbrauch negativ auswirken. Bei der Bereitstellung eines Systems sollten die bewährten Verfahren der Branche befolgt werden. Zu dessen Schutz muss ein System sowohl gut konfiguriert als auch gut gewartet werden.

15.1 Netzwerk-Schutz

Ein Netzwerk muss vor Cyberattacken geschützt werden. Alle Pakete, die im Netzwerk gesendet werden, können von anderen Computern im selben Netzwerk erfasst werden. Wenn die Nutzlast der Pakete im Klartext versendet wird, können die Daten durch sogenannte Netzwerk-Sniffer ganz leicht kompromittiert werden. Eine andere Gefahr geht vom Netzwerk-Spoofing aus. Dabei versucht ein angreifender Computer, einen legitimen Server, einen Computer oder ein Netzwerkgerät zu imitieren, um Zugang zum Netzwerk zu erhalten. Verschlüsselte Verbindungen und CA-signierte Zertifikate gewährleisten Schutz.

Anleitungen zur Verringerung mit dem Netzwerk verbundenen Risiken finden Sie im *Härtungsleitfaden für Axis Netzwerk-Switches* auf <https://help.axis.com/axis-network-switches-hardening-guide>.

Bewährte Vorgehensweisen für das Onboarding und den Betrieb von Axis Geräten in Netzwerken von HPE Aruba Networking finden Sie im Integrationsleitfaden *HPE Aruba Networking – Integration Guide* unter help.axis.com/axis-aruba-secure-network-integration. Die bewährte Konfiguration verwendet moderne Sicherheitsstandards und -protokolle wie IEEE 802.1X, IEEE 802.1AR und HTTPS.

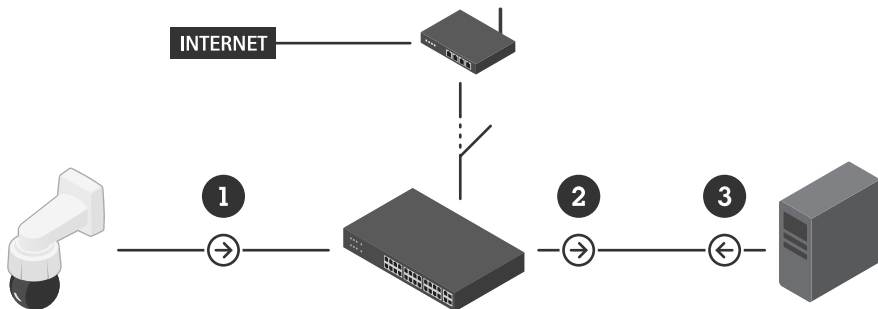
15.1.1 IEEE 802.1X

Die meisten Produkte von Axis unterstützen IEEE 802.1X, einen Standard, der Netzwerke vor dem Zugriff durch nicht autorisierte Geräte schützt. IEEE 802.1X stellt eine Punkt-zu-Punkt-Verbindung her oder verhindert den Zugriff vom LAN-Port, wenn die Authentifizierung fehlschlägt. IEEE 802.1X

verhindert das sogenannte „Port-Hijacking“, also den Zugriff eines unbefugten Geräts auf ein Netzwerk durch physischen Zugang zu einer Netzwerkbuchse. IEEE 802.1X ist bei Netzwerk-Videoanwendungen hilfreich, da sich Kameras häufig in öffentlichen Bereichen befinden und eine zugängliche Netzwerkbuchse gegebenenfalls ein Sicherheitsrisiko darstellen kann. In modernen Unternehmensnetzwerken ist IEEE 802.1X eine grundlegende Anforderung für alle Geräte, die mit dem Netzwerk verbunden werden.

In einem Netzwerk basierten Videosystem kann IEEE 802.1X wie folgt eingesetzt werden:

- 1 Eine Kamera, die für IEEE 802.1X konfiguriert ist, sendet eine Anfrage auf Netzwerkzugriff auf einen Switch.
- 2 Durch den Switch wird die Anforderung an einen Authentifizierungsserver weitergeleitet, z. B. an einen RADIUS-Server (Remote Authentication Dial-In User Service) wie den Microsoft Internet Authentication Service-Server.
- 3 Wenn die Authentifizierung erfolgreich ist, weist der Server den Switch an, seinen Port zu öffnen, damit die Daten der Netzwerk-Kamera durchgelassen und über das Netzwerk gesendet werden können.



IEEE 802.1X ermöglicht eine portbasierte Sicherheit.

15.1.2 HTTPS (HTTP over TLS)

HTTPS (Hypertext Transfer Protocol Secure) ist ein sicheres Kommunikationsprotokoll, das HTTP innerhalb einer abgesicherten Transport-Layer-Security-Verbindung (TLS) sendet. Dies bedeutet, dass HTTP und die Daten selbst verschlüsselt werden.

Viele Axis Produkte unterstützen HTTPS, wodurch eine sichere Kommunikation von Daten möglich ist. Damit ein Axis Gerät über HTTPS kommunizieren kann, müssen ein digitales Zertifikat und ein asymmetrisches Schlüsselpaar auf dem Gerät installiert sein. Das Schlüsselpaar wird vom Axis Gerät generiert. Das Zertifikat kann entweder vom Axis Gerät generiert und selbst signiert oder von einer

Zertifizierungsstelle ausgegeben werden. HTTPS verwendet das Zertifikat zur Authentifizierung und Verschlüsselung, sodass ein Client mithilfe des Zertifikats die Identität des Axis Geräts überprüfen kann. Die Datenkommunikation wird mithilfe von kryptographischen Public-Key-Schlüsseln verschlüsselt.

15.1.3 MACsec

Die meisten Axis Geräte unterstützen den Sicherheitsstandard IEEE 802.1AE MACsec. MACsec ist standardmäßig aktiviert und verschlüsselt automatisch Daten auf der Ebene Ethernet Layer 2 in den Verbindungen zwischen Axis Geräten und MACsec-fähigen Ethernet Switches. Da es auf dieser grundlegenden Ebene arbeitet, kann MACsec Daten verschlüsseln und schützen, die bisher nicht verschlüsselt werden konnten, wie z. B. NTP, DHCP für den allgemeinen Gerätebetrieb und RTP/RTSP für Videostreaming.

15.1.4 Vertrauenswürdige Infrastruktur für öffentliche Schlüssel (PKI)

Eine vertrauenswürdige Infrastruktur für öffentliche Schlüssel (PKI) besteht aus einer privaten oder öffentlichen Zertifizierungsstelle (CA), einem Dienst, der Zertifikate ausstellt (signiert), die in vernetzten Geräten installiert werden sollen. Zertifikate werden für die End-to-End-Verschlüsselung TLS-basierter Verbindungen zwischen Hosts in einem Netzwerk verwendet. Mithilfe eines CA-signierten Zertifikats mit validierter Trust Chain können Anwendungen, wie z. B. VMS oder Webbrowser, die Identität des Axis Netzwerk-Geräts validieren. In der Regel signiert ein CA-Zertifikat (Root-Zertifikat) ein CA-Zwischenzertifikat, das wiederum Clientzertifikate für Endgeräte signiert. Für eine erfolgreiche Prüfung muss das öffentlich bekannte CA-Zertifikat (Root- und/oder Zwischenzertifikat) von der Anwendung zum Überprüfen von Clientzertifikaten von Axis Netzwerk-Geräten installiert sein und verwendet werden. AXIS Device Manager verfügt über einen integrierten CA-Dienst, der kostengünstig Server-Zertifikate für die Geräte ausgeben und bereitstellen kann.

15.1.5 Anmeldung über sicheren Transport

Die Gerätesoftwareversionen AXIS OS 12.10 und höher unterstützen den Netzwerkstandard „Anmeldung über sicheren Transport“ (EST) (RFC 7030). Es optimiert den automatischen Lebenszyklus und die Verlängerung von X.509-Zertifikaten, beispielsweise für HTTPS, 802.1X und andere Dienste. Axis Geräte fordern X.509-Zertifikate automatisch an und erneuern diese fortlaufend, indem sie mit einer zentralisierten IT-Infrastruktur und Anwendungen wie KeyFactor EJBCA, HPE Aruba ClearPass Policy Manager oder Cisco Identity Service Engine (ISE)® kommunizieren.

15.1.6 NTS Network Time Protocol

NTS bietet kryptografische Sicherheit für den Client-Server-Modus des Network Time Protocol (NTP), so dass die Benutzer die Zeit auf authentifizierte Weise abrufen können. Axis Geräte unterstützen NTS ab AXIS OS 11.1.

Die Zeitsynchronisierung erfolgt traditionell nach dem NTP (Network Time Protocol). NTS stellt sicher, dass das Gerät die Zeit nur von vertrauenswürdigen Quellen erhält. Dabei wird jede Synchronisierung authentifiziert und validiert und die Zeitsynchronisierungsfunktionen des NTP-Protokolls bleiben erhalten.

15.1.7 Netzwerk-Isolierung

Die Netzwerk-Isolierung oder Netzwerksegmentierung ist ein Weg, um kritische Netzwerkressourcen voneinander zu trennen, um das Risiko zu verringern, dass sie sich negativ aufeinander auswirken. Dies ist eine besonders relevante Taktik, wenn verschiedene Ressourcen nicht miteinander interagieren müssen oder sollen. Die Netzwerksegmentierung kann virtuell sein (VLAN) und eine Infrastruktur mit verwalteten Switches erfordern. Die Netzwerke können auch mit unterschiedlichen Kabeln und Netzwerk-Geräten getrennt werden.

15.2 Cybersicherheitsstandards

Die Produkte von Axis erfüllen eine Reihe von Vorschriften und Standards im Bereich Cybersicherheit. Weitere Informationen zu Cybersicherheit, Zertifikaten, Übersichten und Berichten finden Sie im Axis Trust Center unter trust.axis.com.

15.2.1 ISO 27001

ISO/IEC 27001 ist die weltweit bekannteste Norm für Informationssicherheits-Verwaltungssysteme (ISMS). Es legt die Anforderungen fest, die ein ISMS erfüllen muss. Das ISMS bei Axis entspricht der Norm ISO/IEC 27001:2023 und gewährleistet einen systematischen und risikobasierten Ansatz für die Informationssicherheit.

15.2.2 SOC 2

Die SOC 2® (System and Organization Controls) Typ 2-Bescheinigung, die als Branchenstandard für Datenschutz und Betriebsintegrität bei Cloud-Diensten anerkannt ist, gewährleistet, dass Axis Cloud Connect, AXIS Device Manager Edge, AXIS Device Manager Extend und AXIS Body Worn Live so ausgelegt sind, dass sie die Standards für Sicherheit und Risikomanagement erfüllen und übertreffen. Die Bescheinigung bewertet sowohl das Design als auch die Wirksamkeit der Kontrollmechanismen eines Unternehmens über einen bestimmten Zeitraum hinweg und prüft

insbesondere die Einhaltung der vom American Institute of Certified Public Accountants (AICPA) festgelegten Trust Services Criteria. Dazu gehören Sicherheit, Verfügbarkeit und Vertraulichkeit. So entsteht ein ganzheitlicher Blick auf die Fähigkeit einer Organisation, Vertrauen, Zuverlässigkeit und Integrität ihrer Systeme dauerhaft zu gewährleisten.

15.2.3 ETSI EN 303 645

ETSI EN 303 645 ist ein Cybersicherheitsstandard, nach dem Axis Geräte mit AXIS OS 11 oder höher zertifiziert sind. Er legt ein Baseline-Profil für Verbrauchsgüter fest, die mit dem Internet verbunden sind, und trägt dazu bei, dass Geräte die DSGVO-Vorschriften besser erfüllen.

15.2.4 FIPS 140 (Federal Information Processing Standard)

FIPS 140 gilt als ein moderner Sicherheitsstandard, den US-amerikanische und kanadische Bundesbehörden sowie kritische Infrastrukturen erfüllen müssen. FIPS 140-2 und FIPS 140-3 sind Informationssicherheitsstandards für kryptografische Computermodule, die in den USA vom NIST (National Institute of Standards and Technology) (nationales Normungs- und Technologieinstitut) herausgegeben werden. FIPS 140-3 hat FIPS 140-2 im Jahr 2019 als aktualisierte Fassung abgelöst. FIPS 140-2 wird ab September 2026 nicht mehr gültig sein.

Axis verlangt, dass seine integrierten, hardwarebasierten kryptografischen Computermodule mindestens gemäß den Common Criteria EAL4 und/oder dem FIPS-Standard 140-2/3 Stufe 2 zertifiziert sind. Der FIPS-140-Standard sieht vier Sicherheitsstufen vor. Mit jeder Stufe gelten höhere und restriktivere Anforderungen. Entsprechend stellt Stufe 1 die geringsten und Stufe 4, die für militärische und unternehmenskritische Anwendungen erforderlich ist, die höchsten Anforderungen.

Im Juli 2024 begann Axis mit der Aufrüstung seines Produkt-Portfolios mit Geräten, deren sichere Elemente (Secure Elements) gemäß Stufe 3 des Standards FIPS 140-3 validiert wurden. Mit der Einführung von AXIS OS 12.4 im April 2025 erfüllen alle Axis Geräte, auf denen AXIS OS 12.4 oder spätere Versionen installiert sind, die Anforderungen von FIPS 140-2 Level 1. In der zweiten Jahreshälfte 2026 wird im Rahmen von AXIS OS eine neue Softwareversion eingeführt, die die Konformität mit FIPS 140-3 Level 1 ermöglicht. Informationen zur Zertifizierung eines Axis Geräts finden Sie im Datenblatt des Geräts oder im Axis Product Selector.

15.2.5 Common Criteria (CC)

Common Criteria (CC) ist ein internationaler Standard (ISO/IEC 15408) für die Sicherheitszertifizierung von IT-Produkten. Axis verlangt für die in seine Hardware integrierten kryptografischen Berechnungsmodule eine Zertifizierung mindestens nach Common Criteria EAL4 und/oder FIPS 140-2/3 Level 2.

15.3 Geräteschutz

Ein vernetztes Gerät und dessen Ressourcen müssen geschützt werden. Der Schutz kann sich in diesem Fall sowohl auf den physischen Schutz beziehen, z. B. indem die Kameras unerreichbar platziert werden, als auch auf den Schutz der Software der Kamera. Das *AXIS OS Hardening Guide* liefert weitere Informationen zum Schutz von Geräten.

15.3.1 Integrierte Cybersicherheitsplattform

Axis Geräte werden von der hardwarebasierten Cybersicherheitsplattform Axis Edge Vault geschützt. Es sorgt für eine starke Grundlage kryptografischer Berechnungsmodule (Sicherheitselement und TPM) und SoC-Sicherheit (TEE und Secure Boot), die wir mit Expertise in Edge-Gerätesicherheit kombinieren.

Mit Axis Edge Vault ist das Gerät weniger Cybersicherheitsrisiken ausgesetzt, sodass es zu einer vertrauenswürdigen und zuverlässigen Einheit im Netzwerk wird.

- > **Vertrauenswürdige Geräteidentität.** Den Ursprung eines Gerätes überprüfen zu können, ist der Schlüssel zum Vertrauen in die Geräteidentität. In der Produktion wird Geräten mit Axis Edge Vault ein eindeutiges, von der Fabrik bereitgestelltes und IEEE 802.1AR-kompatibles Zertifikat für die Axis Geräte-ID zugewiesen. Dieses wird sicher und dauerhaft im sicheren Schlüsselspeicher gespeichert und kann für die automatisierte, sichere Integration von Geräten und zur sicheren Geräteidentifizierung genutzt werden.
- > **Sichere Speicherung der Schlüssel.** Der sichere Schlüsselspeicher speichert kryptografische Daten Hardware-basiert und manipulationsgeschützt. Es schützt die Axis Geräte-ID sowie vom Kunden hochgeladenen kryptografischen Informationen und verhindert im Fall einer Sicherheitsverletzung unbefugten Zugriff und böswillige Extraktion.
- > **Videomanipulationserkennung.** *Signiertes Video* ermöglicht es, das Video bis zur Ursprungskamera zurück zu verfolgen und zu überprüfen, ob das Video nach dem Verlassen der Kamera nicht manipuliert wurde. Jede Kamera hat ihren eigenen, eindeutigen Videosignierschlüssel, der im sicheren Schlüsselspeicher aufbewahrt wird und eine Signatur zum Videostream hinzufügt. Beim Abspielen des Videos zeigt der Datei-Player an, ob das Video intakt ist.
- > **Schutz der Lieferkette.** Die Cybersicherheitsfunktionen *sicheres Hochfahren* und *signiertes OS* schaffen eine sichere Grundlage für Axis Edge Vault durch Bereitstellung einer ununterbrochenen Kette kryptografisch validierter Software. *Secure Boot* verhindert Manipulationen der physischen Lieferkette, indem es sicherstellt, dass ein Gerät nur mit einem von Axis signierten Betriebssystem booten kann. *Signed OS* garantiert, dass das installierte Betriebssystem (AXIS OS) wirklich von Axis stammt, und stellt sicher, dass jede neue

Gerätesoftware, die auf das Gerät heruntergeladen und auf ihm installiert wird, ebenfalls von Axis signiert ist. Erkennt das Gerät, dass die Integrität der Software verletzt oder diese nicht von Axis signiert wurde, wird das Upgrade zurückgewiesen.

15.3.2 Benutzerkontenverwaltung

Gerätekennwörter werden tendenziell innerhalb einer Organisation verbreitet. Beispielsweise fordert eine Person bei der Gerätwartung das Kennwort an, um etwas anzupassen. Ein paar Tage oder Wochen später stellt eine neue Person dieselbe Anfrage. Innerhalb kurzer Zeit kennen viele neue (oder temporäre) Benutzer das Kennwort für alle Geräte – und Sie haben die Kontrolle darüber verloren, wer auf sie zugreifen kann. Die Stärke des Kennworts spielt in diesem Szenario keine Rolle. Das Verwalten von Geräten sollte über mehrere Konten (je nach Funktion) erfolgen, und es müssen temporäre Konten für die gelegentliche Wartung und Fehlerbehebung erstellt werden.

Verwenden Sie bei Kontozugängen das Prinzip der Konten mit den geringsten Berechtigungen. Dies bedeutet, dass die Zugriffsrechte des Benutzers auf die Ressourcen beschränkt sind, die er für die Durchführung seiner spezifischen Aufgaben benötigt. AXIS Device Manager oder AXIS Device Manager Extend verwaltet auf einfache und effiziente Weise mehrere Konten und Kennwörter auf Betrachter-, Bediener- oder Administratorebene. Produkte von Axis mit AXIS OS 11.6 oder höher unterstützen außerdem OAuth 2.0, das branchenübliche Autorisierungsprotokoll.

15.3.3 Hostbasierte Firewall

Die Produkte von Axis bieten leistungsfähige Layer-2/3-Firewall-Schutzfunktionen. Damit lässt sich der Zugriff auf definierte IP- oder MAC-Adressen sowie die Protokoll- und Portfilterung zulassen oder verweigern. In einem typischen Setup erlauben vernetzte Geräte nur den notwendigen Servern und Clients, auf das Produkt zuzugreifen. Auf diesen wird die Audio-Management-Software gehostet. Die Firewall verringert Risiken, wenn das Kennwort des Geräts von ungepatchten Geräten und von Brute-Force-Attacken kompromittiert wird.

15.3.4 Immer aktuelle Gerätesoftware

Durch den Betrieb von Geräten mit einer aktuellen Version von AXIS OS werden die üblichen Risiken verringert. Dies liegt daran, dass die aktuelle Version in der Regel Sicherheitspatches für alle bekannten Sicherheitslücken enthält, einschließlich neu entdeckter. Damit können die Sicherheitslücken nicht ausgenutzt und das System, die Anwendung oder die Geräte beeinträchtigt werden. Die Software für das Gerätemanagement von Axis unterstützt Sie bei der Verwaltung von Upgrades für mehrere Geräte und Standorte und benachrichtigt Sie automatisch, wenn es neuere Versionen gibt.

Als CVE Numbering Authority (CNA) folgt Axis bewährten Verfahren der Branche bei der Verwaltung und Reaktion auf Sicherheitslücken, die in unseren Produkten entdeckt wurden.

Sicherheitslücken werden mithilfe des weit verbreiteten CVSS-Rating-Systems ermittelt und je nach NS-Wert innerhalb einer vorgegebenen Zeitspanne gepatcht. Mehr lesen auf www.axis.com/support/cybersecurity/vulnerability-management

15.3.5 Protokollierung von Audits

AXIS OS unterstützt eine rund um die Uhr verfügbare Protokollierung von Audit-Ereignissen über Remote-Syslog für SIEM- und SNMP-Überwachungsanwendungen. Mit mehr als 10 Ereignisklassen, darunter verdächtige Netzwerkaktivitäten und die Erkennung von Eindringversuchen, bietet sie:

- > Rückverfolgbarkeit: Erfasst das Verhalten der Benutzer und die Systemaktivitäten rund um die Uhr
- > Cybersicherheit: Erfasst unbefugte Zugriffe und verdächtiges Verhalten
- > Compliance: Eine Anforderung in vielen Vorschriften und Cybersicherheitsstandards im Internet der Dinge

Die Audit-Protokolle lassen sich problemlos integrieren und können zur zentralen Speicherung und Analyse an verschiedene IT-Überwachungsplattformen weitergeleitet werden. Zudem entsprechen sie den Standards der Industrie (OCSE).

15.4 Schutz der VMS

Viele der Prinzipien, die für Geräte- und Netzwerkschutz gelten, gelten auch für den Schutz der VMS. Beim Definieren von Systemkonten sollten Sie zum Beispiel das Prinzip der wenigsten Berechtigungen befolgen und sicherstellen, dass die aktuelle Softwareversion der VMS mit Sicherheitspatches für alle neu entdeckten Sicherheitslücken verwendet wird. Außerdem sollte auf allen mit dem VMS-Server verbundenen Servern und Computern eine Antiviren-Software installiert sein. Zudem sollten Sie nur die VMS-Server-Software und vertrauenswürdige Integrationen von Drittanbietern auf der Host-Hardware ausführen.

Weitere Informationen finden Sie im AXIS Camera Station System Hardening Guide unter <https://help.axis.com/axis-camera-station-system-hardening-guide>. Darin werden Cybersicherheitsrichtlinien und -verfahren zur Unterstützung der sicheren Bereitstellung und Wartung von AXIS Camera Station-Systemen beschrieben.

15.5 Physischer Schutz

Obwohl ein vernetztes Gerät niemals zu 100 % physisch geschützt werden kann, müssen verschiedene physische Aspekte berücksichtigt werden. Für viele Gerätetypen wie Kameras und Lautsprecher können Sie ein Design und eine Farbe wählen, die sich in die Umgebung einfügen, das Gerät außer Reichweite anbringen und das Kabel immer direkt durch die Wand oder Decke hinter dem Gerät ziehen. Diesen Maßnahmen bieten einen erheblichen Schutz sowohl vor spontanem Vandalismus als auch vor geplanten Angriffen. Bei Geräten, die leicht zugänglich sein müssen, z. B. Gegensprechanlage oder Türsteuerungen, sollten vandalismussichere Modelle mit einer Manipulationserkennung gewählt werden. Wichtige Netzwerk basierte Geräte wie Router und Switches sowie der Host, auf dem die VMS-Serversoftware ausgeführt wird, sollten in einer Umgebung mit eingeschränktem Zutritt installiert werden.

16. Drahtlose Netzwerktechnologien

Drahtlose Netzwerktechnologien für Videosicherheitsanwendungen ermöglichen eine flexible, kostengünstige und schnelle Installation von Sicherheitskameras, insbesondere in ausgedehnten Bereichen wie auf Parkplätzen oder in Innenstädten. In älteren, unter Denkmalschutz stehenden Gebäuden ist die drahtlose Technologie möglicherweise die einzige Alternative, wenn Kabel nicht in Frage kommen.

Axis bietet Kameras mit integrierter WLAN-Unterstützung. Auch Kameras ohne diese Unterstützung können über eine Wireless-Bridge in ein drahtloses Netzwerk integriert werden.

16.1 802.11-WLAN-Standards

Der häufigste Standard für drahtlose lokale Netzwerke (WLANs) ist IEEE 802.11. Der Vorteil dieses Standards gegenüber anderen Standards und proprietären Technologien ist, dass er lizenzfrei ist, d. h. für das Einrichten und den Betrieb des Netzwerks fällt keine Lizenzgebühr an. Die wichtigsten Änderungen der Standards für Axis Produkte sind:

- > 802.11ac (auch als Wi-Fi 5 bezeichnet) wurde 2014 genehmigt. Er entspricht dem 802.11n-Standard, jedoch ausschließlich im 5 GHz-Band. Je nach Betriebsbedingungen kann der Datendurchsatz 1,7 bis 2,5 Gbit/s erreichen.
- > 802.11n (auch als Wi-Fi 4 bezeichnet), den die meisten drahtlosen Produkte unterstützen. Er wurde 2009 genehmigt und arbeitet im 2,4-GHz- oder 5-GHz-Band. Je nachdem, welche Eigenschaften für den Standard implementiert sind, ermöglicht 802.11n eine maximale Datenrate von 600 Mbit/s.
- > 802.11g wurde 2003 genehmigt und nutzt das 2,4-GHz-Band, mit Datenraten von bis zu 54 Mbit/s.
- > 802.11b wurde 1999 veröffentlicht und nutzt das 2,4-GHz-Band, wobei Datenraten von bis zu 11 Mbit/s erzielt werden.

Produkte, die als 802.11b/g/n/ac bezeichnet werden, sind mit allen vier Erweiterungen kompatibel.

Bei der Einrichtung eines drahtlosen Netzwerks müssen die Bandbreitenkapazität des Access Points sowie die Bandbreitenanforderungen der Netzwerk-Geräte berücksichtigt werden. Im Allgemeinen liegt der tatsächliche Datendurchsatz, der von einem WLAN-Standard unterstützt wird, bei etwa 50 Prozent der Bitrate, die ein Standard brutto liefert. Ursachen hierfür sind der Overhead bei der Signalisierung und der Protokollierung.

16.2 WLAN-Sicherheit

Beim Übertragen von Daten über eine drahtlose Verbindung sollte unbedingt berücksichtigt werden, dass die feste Grenze eines drahtgebundenen LAN bei der drahtlosen Alternative wegfällt. Theoretisch kann jede Person innerhalb der Reichweite eines WLAN das Netzwerk angreifen und Daten abfangen. Daher wird die Sicherheit noch wichtiger, wenn es darum geht, den nicht autorisierten Zugriff auf Daten und das Netzwerk zu verhindern.

Einige Sicherheitsrichtlinien:

- > Aktivieren Sie die Anmeldung mit Benutzername und Kennwort in den Kameras.
- > Aktivieren Sie Verschlüsselung (HTTPS) im Wireless-Router/in den Kameras. Dies sollte vor dem Einrichten der Schlüssel oder Anmeldedaten für das WLAN erfolgen, damit niemand die Schlüssel auf dem Weg zur oder bei der Konfiguration in der Kamera einsehen kann.
- > Verwenden Sie WPA2-PSK und eine Passphrase mit mindestens 20 zufälligen Zeichen in einer Kombination aus Klein- und Großbuchstaben, Sonderzeichen und Zahlen. WPA2-PSK kann zur Sicherung kleiner Netzwerke verwendet werden, die keinen Authentifizierungsserver verwenden können.
- > WPA2-Enterprise mit EAP-TLS bietet die höchste Sicherheitsstufe und wird für Unternehmensumgebungen empfohlen, die eine zuverlässige Authentifizierung und Verschlüsselung erfordern.

16.2.1 WPA2™¹

WPA2™ basiert auf dem Standard IEEE 802.11i. Beachten Sie, dass das ältere WPA™ nicht mehr für die Sicherung von Drahtlosnetzwerken empfohlen wird.

WPA2-Personal oder WPA2-PSK (Pre-shared key) wurde für kleinere Netzwerke entwickelt und erfordert keinen Authentifizierungsserver. Mit dieser Technologie authentifizieren sich Drahtloskameras von Axis mit dem PSK am Access Point. Der Schlüssel kann entweder als 256-Bit-Zahl in 64 Hexadezimalziffern (0 bis 9, A bis F) oder als Kennwort mit 8 bis 63 ASCII-Zeichen

eingegeben werden. Um Schwachstellen bei dieser Sicherheitsmethode zu umgehen, müssen lange Kennwörter verwendet werden.

WPA-/WPA2-Enterprise wurde für große Netzwerke entwickelt und benötigt einen Authentifizierungsserver mit Unterstützung für IEEE 802.1X. Weitere Informationen über IEEE 802.1X finden Sie in Abschnitt .

¹ WPA und WPA2 sind Marken der Wi-Fi Alliance.

16.3 Wireless-Bridges

Es sind Lösungen möglich, die nicht auf dem dominierenden Standard IEEE 802.11 beruhen, die jedoch neben einer höheren Leistung und größeren Entfernungen ein sehr hohes Maß an Sicherheit bieten. Zwei häufig verwendete Technologien sind Mikrowellen und Laser, mit denen Gebäude oder Standorte über eine Hochgeschwindigkeits-Datenverbindung Punkt-zu-Punkt verbunden werden.

16.4 Drahtloses Mesh-Netzwerk

Ein drahtloses Mesh-Netzwerk ist eine weitverbreitete Lösung für Videosicherheitsanwendungen in Innenstädten. Es kann Hunderte von Kameras, Mesh-Routern und Gateways umfassen. Ein solches Netzwerk verfügt über mehrere Verbindungsknoten zum Empfangen, Senden und Weiterleiten von Daten, die individuelle und redundante Verbindungspfade zueinander bieten. Bei Anwendungen, die Videos live übertragen, und insbesondere wenn PTZ-Kameras verwendet werden, ist eine möglichst kurze Verzögerung von großer Bedeutung.

16.5 4G- und 5G-Netzwerke

Das Universal Mobile Telecommunications System (UMTS) ist ein Mobilfunkstandard, der eine Reihe von Technologien umfasst. 3G war die erste Technologiegeneration, die ausreichend hohe Bitraten für die Datenübertragung bereitstellte und ist heute weit verbreitet, auch wenn sie schnell durch spätere Standards ersetzt wird.

Der 4G-Standard bietet Spitzen-Bitraten von bis zu 100 Mbit/s für mobile Anwendungen (z. B. in fahrenden Fahrzeugen) und bis zu 1 Gbit/s für mehr oder weniger stationäre Anwendungen. 4G ist in seinen verschiedenen Formen ebenfalls weit verbreitet.

Der Nachfolger der 4G-Netze, der derzeit in vielen Ländern eingeführt wird, wird allgemein als 5G bezeichnet. 5G bietet nicht nur höhere Durchsatzgeschwindigkeiten, sondern auch eine höhere Kapazität und kann daher viel mehr Geräte in demselben geografischen Gebiet verbinden. Die jetzt

und in naher Zukunft verfügbaren Datenraten machen 5G-Netzwerke für Videosicherheitsanwendungen sehr interessant. Einige Geräte, z. B. Body Worn Kameras, verfügen über die integrierte 4G- oder 5G-Technologie zum Streamen von Live-Video über das mobile Netzwerk.

16.6 Z-Wave®

Z-Wave wurde zuerst als Steuerungssystem für die Beleuchtung auf Verbraucherebene eingeführt. Es ist mittlerweile in ein vollständiges Mesh-Protokoll und System für die Hausautomatik integriert, das es bis zu 232 intelligenten Geräten ermöglicht, sich in einem einzigen Netzwerk miteinander zu verbinden. Obwohl Z-Wave nicht für Video verwendet wird, können verschiedene Z-Wave-Geräte wie IR-Sensoren, Tür-/Fenstersensoren und drahtlose Alarmtasten bei der Verwendung in einem Videosicherheitssystem nützlich sein. Ein Z-Wave-Netzwerk verfügt zudem über einen Controller oder Smart Hub, der in der Regel das einzige direkt mit dem Internet verbundene Gerät ist. Es bietet bei kleinen Datenpaketen Übertragungsraten von bis zu 100 kBit/s. Z-Wave arbeitet in den USA im Niederfrequenzband von 908,42 MHz und in Europa im 868,42-MHz-Band. Wenn Z-Wave bei diesen niedrigeren Frequenzen verwendet wird, ist die Signalreichweite größer und Innenwände können besser durchdrungen werden.

16.7 Zigbee®

Wie Z-Wave ist auch Zigbee ein Netzwerkprotokoll mit geringer Leistung und geringer Datenrate in unmittelbarer Nähe. Ein Zigbee-Netzwerk unterstützt jedoch mehr als 65.000 Geräte mit unbegrenzten Hops zwischen den Geräten. Zigbee verwendet mehrere Protokolle und offene Standards und ist lizenzfrei. Es arbeitet hauptsächlich mit der höheren Frequenz von 2,4 GHz.

17. Videoverwaltungssysteme

Ein wichtiger Aspekt bei Videosicherheitssystemen ist neben der Verwaltung der Netzwerk-Video-Produkte die Verwaltung von Live-Ansichten, Aufzeichnung, Wiedergabe, Suche und Speicher. Dies alles erfolgt über ein Video Management System (VMS).

Axis bietet VMS für Windows-basierte Vor-Ort-Systeme sowie Edge-basierte Hybrid-Cloud-Lösungen mit Fernzugriff und Live-Überwachung von Standorten, Wiedergabe und Speicherung von Videos, Export von Videos und Nutzung von Analysen. Die Systeme können auch eine Zutrittsverwaltung und andere Funktionen wie Audio für die Sicherheit umfassen. Der Zugriff auf die Systeme kann über einen PC oder Laptop oder über Apps auf einem mobilen Endgerät erfolgen. Darüber hinaus bietet das Axis Netzwerk von Technologie-Integrationspartnern Lösungen für jeden Systemtyp, jede Größe und jede Komplexität.

17.1 Arten von Videoverwaltungssystemen

Videoverwaltungssysteme umfassen eine Kombination aus Hardware und Softwareplattformen, die auf unterschiedliche Arten eingerichtet werden können. Die Aufzeichnung kann z. B. lokal am Standort der Kamera erfolgen, sie kann gehostet werden, oder alles kann an einem zentralen Standort erfolgen. PC-basierte Lösungen bieten Flexibilität und maximale Leistung für das jeweilige Systemdesign, mit der Möglichkeit, Funktionen wie erweiterten oder externen Speicher, Firewalls, Analysefunktionen und andere IP-Geräte hinzuzufügen.

Das eingesetzte System sollte von Ihren Anforderungen und davon abhängen, wie Sie das System verwalten möchten. Für ein kleines System mit bescheidenen Anforderungen an die Videoverwaltung kann ein cloudbasiertes System ideal sein. Größere Systeme mit umfangreichen Aufzeichnungen, die mehr Speicherkapazität benötigen, könnten vom Betrieb in einem privaten Netzwerk profitieren.

17.1.1 Cloubasierte Systeme

Cloubasiertes Video Management bedeutet, dass der Großteil des Dienstes und der Software gehostet wird und der Zugriff über das Internet erfolgt. Die einzigen Teile des Systems, die vor Ort sein müssen, sind die Geräte.

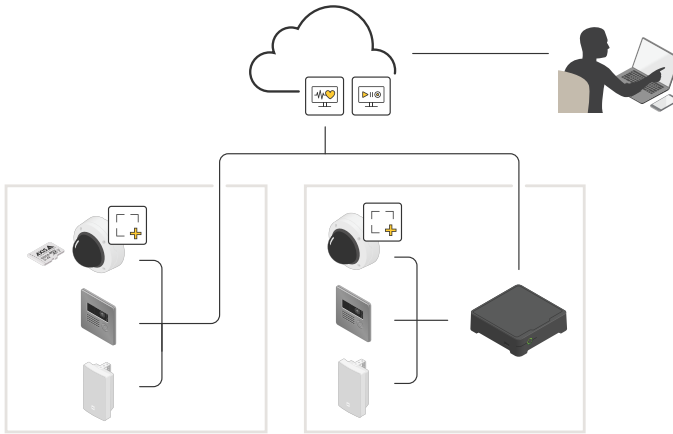
17.1.1.1 AXIS Camera Station Edge

AXIS Camera Station Edge ist ein cloubasiertes Video Management System (VMS), das minimale Wartung und keinen Server erfordert. Es ermöglicht die direkte Verbindung zwischen Kameras und der Cloud und macht lokale Server überflüssig. Über eine benutzerfreundliche Schnittstelle haben Sie Zugriff auf wichtige Funktionen wie Live-Ansicht, Suche in der Zeitleiste und Videoexport. Sie ist skalierbar und Sie können problemlos neue Standorte oder Geräte zu bestehenden Installationen hinzufügen.

AXIS Camera Station Edge ist mit den Kameras und Geräten von Axis kompatibel. Das System unterstützt redundanten Cloud-Speicher mit der AXIS Camera Station Cloud Storage und stellt so sicher, dass das aufgezeichnete Bildmaterial jederzeit abrufbar ist. Echtzeit-Alarm-Benachrichtigungen können mithilfe von KI-basierten Analysefunktionen angepasst werden, so dass Sie verdächtige Aktivitäten sofort erkennen können. Die Konfiguration der Geräte und die Aktualisierung der Software erfolgen automatisch, so dass weniger manuelle Eingriffe erforderlich sind.

Sie können auch die Berechtigungen für die Verwaltung des Zugriffs auf die Systemfunktionen anpassen und selbst bestimmen, wer bestimmte Aktionen durchführen darf (Viewer, Operator, Administrator). Die Aufbewahrungsdauer der Aufzeichnungen ist leicht zu verwalten und die Geräte können bei Bedarf per Fernzugriff neu gestartet werden. Dank der Live-Audioaufnahme können Sie auf Alarme reagieren und mit Personen vor Ort kommunizieren.

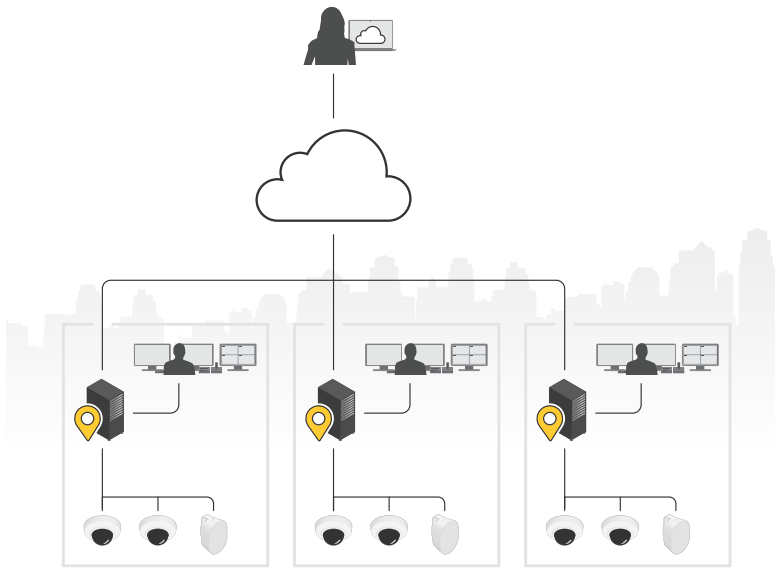
Es gibt mehrere Möglichkeiten, auf das AXIS Camera Station Edge-System zuzugreifen und es zu überwachen. Eine spezielle mobile Anwendung ermöglicht den Zugriff auf die Systemfunktionen von unterwegs aus, eine Desktop-Client-Anwendung bietet eine umfassende Schnittstelle für die Verwaltung. Für die Überwachung der Systemfunktionen von jedem beliebigen Ort aus steht auch eine webbasierte Schnittstelle zur Verfügung.



Links: AXIS Camera Station Edge mit SD-Kartenspeicher. Rechts: AXIS Camera Station Edge mit einem Netzwerk-Videorekorder von Axis.

17.1.2 Private Netzwerke

Wenn Sie höhere Ansprüche an die Kapazität oder strengere Anforderungen an Ihr Video Management System haben, dann ist es sehr wahrscheinlich, dass Sie ein Setup in Ihrem eigenen privaten Netzwerk in Betracht ziehen müssen. Dies bietet unter anderem folgende Vorteile: bessere Kontrolle über die Sicherheitsmaßnahmen, die Erfüllung von Vorschriften, nach denen Sie Ihre Daten in Ihren eigenen Räumlichkeiten speichern müssen, und Einsparungen bei den Speicherkosten bei großen Mengen an aufgezeichneten Videos. Eine private Netzwerk-Lösung kann durch optionale Cloud-Funktionen ergänzt werden.

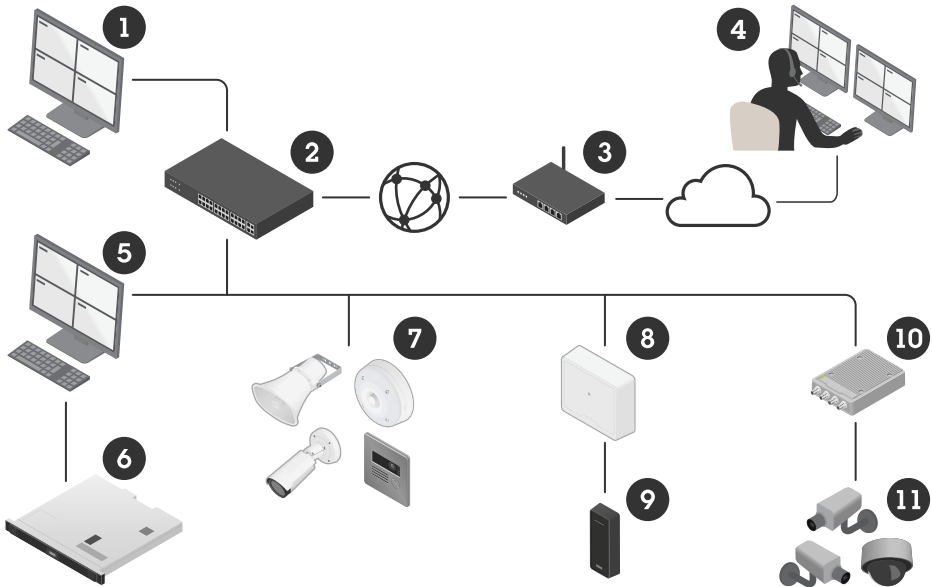


Ein Beispiel für eine private Netzwerk-Lösung mit optionalem Zugriff auf die Cloud.

17.1.2.1 AXIS Camera Station Pro

AXIS Camera Station Pro bietet erweiterte Video Management Funktionalität und ermöglicht ein komplettes Überwachungs- und Aufzeichnungssystem einschließlich Verwaltung der Zutrittskontrolle. Die Software kann auf validierten AXIS Camera Station Netzwerk-Videorekorden, Hardware von Drittanbietern und virtuellen Maschinen ausgeführt werden. Sie ermöglicht eine einfache Installation und effiziente Verwaltung von Axis Kameras und anderen Geräten. Die Software enthält eine Reihe von Funktionen zur Unterstützung bei der Handhabung von Vorfällen und beim Export von Beweismaterial. Dazu gehören das flexible Einrichten der Live-Ansicht, eine leistungsstarke Aktionsregel-Engine zum Einrichten automatisierter Auslöser, die intelligente Suche zum schnellen Finden von Videoinhalten, Video-Nachbearbeitung zum Schutz der Privatsphäre von Drittanbietern sowie Vorfalloberichte zum einfachen Erstellen eines Falls.

Zusammen mit einer Client-Server-Anwendung von Windows ist AXIS Camera Station Pro eine zentralisierte Lösung, bei der die Video Management Software für die Verwaltungs- und Aufzeichnungsfunktionen durchgehend auf einem Server vor Ort ausgeführt werden muss. Die Aufzeichnungen erfolgen über das Privatnetz, entweder auf dem gleichen Computer, auf dem AXIS Camera Station Pro installiert ist, oder auf separaten Speichergeräten.



Sicherheitssystem auf Basis einer offenen PC-Server-Plattform mit der Video Management Software AXIS Camera Station Pro.

1. AXIS Camera Station Pro Client-Software:
2. Netzwerk-Switch
3. Router
4. Fernzugriff über AXIS Camera Station Pro Client-Software
5. AXIS Camera Station Pro Software
6. Aufzeichnungsserver
7. Netzwerk-Video- und Audio-Produkte von Axis
8. Zutrittskontrolle: Türsteuerung
9. Zutrittskontrolle: Lesegerät
10. Video-Encoder
11. Analogkameras

Es gibt mehrere Möglichkeiten, eine Verbindung zu Ihrem AXIS Camera Station Pro-System herzustellen. Eine Client-Anwendung zur Anzeige, Wiedergabe und Verwaltung kann auf jedem beliebigen Computer installiert werden. Dies kann vor Ort oder über das Internet erfolgen. Durch die Unterstützung mehrerer Standorte können Benutzer über den Client auf Kameras zugreifen, die mit verschiedenen AXIS Camera Station Pro-Servern verbunden sind. Dies ermöglicht die Videoverwaltung an mehreren entfernten Standorten oder in einem großen System, einschließlich

erweiterter Videofunktionen, Zugangskontrolle, Alarmbenachrichtigung, Systemkonfiguration, Geräteverwaltung und Systemüberwachung.

Ein mobiler App-Client ermöglicht den Zugriff auf mehrere Systeme, den Empfang von Benachrichtigungen, die Verwaltung von Videos und die Durchführung von Aktionen, wie z. B. das Öffnen einer Tür über eine IP-Türsprechanlage. Darüber hinaus können Sie über einen Webbrowser in Ihrem privaten Netzwerk oder über die Cloud auf das System zugreifen, um Live-Videos von Kameras anzuzeigen, PTZ-Kameras zu steuern, Aufzeichnungen zu suchen, wiederzugeben und zu exportieren, Benutzer und Geräte zu verwalten und den Systemstatus zu überwachen.

AXIS Camera Station Pro bildet die Grundlage für die Erstellung einer Lösung mit Produkten aus dem gesamten Axis Portfolio, wie z. B. Audio, Zutrittskontrolle, Radarzielverfolgung und Analysefunktionen. Mithilfe von API- und E/A-Modulen lässt sich auch die Integration in andere Systeme wie Gebäudeverwaltung, Industrielle Steuerung und andere externe Systeme ermöglichen.

17.1.3 Maßgeschneiderte Lösungen der Axis-Partner

Axis arbeitet weltweit mit mehr als 800 Technologieintegrationspartnern zusammen, um nahtlos integrierte Softwarelösungen zu gewährleisten, die die Videoprodukte von Axis unterstützen. Diese Partner stellen eine Palette maßgeschneiderter Softwarelösungen bereit. Viele bieten zudem optimierte, erweiterte oder kundenspezifische Funktionen für bestimmte Branchen sowie Lösungen für bestimmte Länder an. Zudem sind Lösungen verfügbar, die mehr als 1.000 Kameras und Videoprodukte verschiedener Marken unterstützen. Kompatible Anwendungen finden Sie unter www.axis.com/partner.

17.2 Systemmerkmale

Einige der häufigsten Merkmale von Videoverwaltungssystemen sind:

- > **Aufzeichnen.** Das Aufzeichnen von Video und Audio ist eine Hauptfunktion eines Video Management Systems. Dies beinhaltet das Einrichten von Aufzeichnungsregeln, die Smart Search in Aufzeichnungen sowie den Export in andere Systeme.
- > **Anzeige.** Mit den meisten Video Management Software Lösungen können verschiedene Benutzer mehrere Kameras gleichzeitig anzeigen und simultane Aufzeichnungen durchführen. Zu den weiteren Funktionen zählen das Anzeigen auf mehreren Bildschirmen und Mapping. Mapping heißt, dass eine Karte des Gebäudes oder Bereichs mit Kamerasymbolen überlagert werden kann, die der tatsächlichen Kameraposition entsprechen. Es besteht auch die Möglichkeit, externe Webseiten einzuschließen, um eine Integration in externe Systeme zu ermöglichen. Dies kann u. a. zur Darstellung von Switch-Oberflächen, Personenzählungen und sogar Wetterberichten verwendet werden.

- > **Suche läuft.** Video Management Software sollte über eine intelligente Suchfunktion verfügen, die es den Benutzern ermöglicht, das Videomaterial schnell zu durchsuchen, um Personen und Fahrzeuge von Interesse zu finden. AXIS Camera Station verfügt über eine intelligente Suchfunktion, die auf den Bewegungsobjektdaten der Kamera basiert. Die Daten werden mit Machine Learning und Deep-Learning-Algorithmen weiterverarbeitet, um Objekte wie Personen, Autos, Lastwagen und Fahrräder schnell zu klassifizieren. Dies funktioniert mit den meisten Kameras von Axis. Es wird keine zusätzliche Hardware und Software benötigt. Die Leistung lässt sich einfach verbessern, indem zusätzliche Serverkapazität hinzugefügt und Axis Kameras mit Funktionen zum Machine oder Deep-Learning verwendet werden.
- > **Ereignisverwaltung und Analyse.** Video Management Software kann Ereignisbenachrichtigungen verschiedener Quellen empfangen, verarbeiten und zuordnen. Bei den Quellen kann es sich um Zutrittskontrollpunkte, Kassenterminals (POS), Analysefunktionen und die Videoprodukte selbst handeln. Wenn eine Ereignisbenachrichtigung ausgelöst wurde, kann das VMS diese erfassen, den Videoclip einer nahegelegenen Kamera zuordnen und einen Bediener oder Ermittler über ein Pop-Up-Fenster auf dem Bildschirm oder eine Nachricht auf das Smartphone benachrichtigen.
- > **Verwaltung.** Dies umfasst die Installation, Gerätesoftware-Upgrades, die Sicherheit, das Prüfprotokoll sowie die Parameterkonfigurationen der Kameras und weiterer Komponenten wie Registrierkassen, Türsteuerungen und Türstationen. Je größer das System, desto wichtiger ist eine effiziente Verwaltung der Geräte. Die Überwachung des Systemzustands bietet eine Systemübersicht einschließlich der Aufzeichnungshardware und erzeugt Benachrichtigungen, wenn ein Gerät oder System offline geht. Eine Video Management Software sollte auch über Optionen für die Verwaltung von autorisierten Benutzern, Kennwörtern, Benutzerzugriffsebenen sowie des jeweiligen Zugriffs auf bestimmte Geräte verfügen. Manche Video Management Softwareprogramme können Windows-Benutzerdatenbanken übernehmen, so dass keine separate Benutzerdatenbank eingerichtet und gepflegt werden muss.

17.3 Integrierte Systeme

Wenn Video mit anderen Systemen wie Zutrittskontroll-, Point-of-Sale-, Gebäudeverwaltungs-, Patienteninformations- oder Logistiksystemen kombiniert wird, können die Informationen des anderen Systems zum Auslösen von Funktionen, z. B. ereignisgesteuerten Aufzeichnungen im Netzwerk-Videosystem, verwendet werden und umgekehrt. Darüber hinaus bietet dies den Vorteil einer gemeinsamen Schnittstelle für die Verwaltung unterschiedlicher Systeme.

17.3.1 Zutrittskontrolle

Die Zutrittskontrolle ist eine der am häufigsten verwendeten VMS-Integrationen. AXIS Camera Station Secure Entry ist Teil der Software AXIS Camera Station Pro und bietet eine vereinheitlichte

Lösung, die Überwachungs- und Zutrittskontrollfunktionen in sich vereint. Mehr zur Zutrittskontrolle erfahren Sie im Kapitel .

17.3.2 Kassenterminal

Die Einführung von Netzwerkvideo im Einzelhandel hat die Integration von Video- mit Kassenterminalsystemen (POS) vereinfacht.

Durch diese Integration können alle Registrierkassentransaktionen mit der Videoaufzeichnung der Transaktionen verknüpft werden. Sie hilft, Betrug und Diebstahl durch Mitarbeiter und Kunden zu erkennen und zu verhindern. POS-Ausnahmen wie Retouren, manuell eingegebene Werte, Zeilenkorrekturen, Transaktionsabbrüche, Einkäufe von Mitarbeitern, Rabatte, speziell gekennzeichnete Artikel, Umtausch und Rückerstattungen können visuell überprüft werden, indem man bei diesen Ereignissen ereignisgesteuerte Aufzeichnungen aktiviert. Die Szene vor und nach einem Ereignis kann mithilfe von Pufferspeichern für die Aufzeichnung vor und nach dem Ereignis erfasst werden. Ereignisbasierte Aufzeichnungen erhöhen die Qualität des aufgezeichneten Materials und verringern die Speicheranforderungen sowie die Zeit, die zum Suchen von Vorkommnissen erforderlich ist.

17.3.3 Gebäudeverwaltung

Videos können in ein Gebäudeverwaltungssystem (GVS) integriert werden, das verschiedene Systeme von der Heizung, Belüftung und Klimaanlage bis hin zu Sicherheits-, Energie- und Feueralarmsystemen verwaltet. Im Folgenden finden Sie einige Anwendungsbeispiele:

- > Bei einem Geräteausfallalarm kann nicht nur ein Alarm, sondern auch die Anzeige von Videos für den Bediener ausgelöst werden.
- > Ein Feueralarmsystem kann die Überwachung von Gebäudeausgängen durch eine Kamera sowie die Aufzeichnung zu Sicherheitszwecken auslösen. Dadurch können die Ersthelfer und Gebäudeverwalter die Lage an sämtlichen Notausgängen in Echtzeit mitverfolgen und einschätzen, wo sie am dringendsten benötigt werden.
- > Mit Analysefunktionen kann z. B. im Anschluss an eine Evakuierung die Rückkehr von Personen in ein Gebäude durch offene oder ungesicherte Türen erfasst werden.
- > Ein automatischer Videoalarm kann gesendet werden, wenn eine Person einen Sperrbereich oder Raum betritt.
- > Die videobasierte Bewegungserkennung einer Kamera in einem Besprechungsraum kann für Beleuchtungs- und Heizungssysteme verwendet werden, um zum Energiesparen Licht und Heizung automatisch auszuschalten, sobald alle Personen den Raum verlassen haben.

17.3.4 Industrielle Kontrollsysteme

In komplexen automatisierten Industrieanlagen ist eine externe Sichtkontrolle oftmals von Vorteil oder gar erforderlich. Durch die Möglichkeit, über dieselbe Schnittstelle sowohl auf die Netzwerk-Videofunktionalität als auch auf die Überwachung eines Vorgangs zuzugreifen, muss ein Bediener nicht die Steuerkonsole verlassen, um einen Vorgang visuell zu überprüfen. Darüber hinaus kann eine Betriebsstörung das Senden von Bildern von der Netzwerk-Kamera auslösen. Für einige empfindliche Reinraumprozesse oder in Einrichtungen mit gefährlichen Chemikalien ist die Videosicherheit oft die einzige Möglichkeit einer Sichtkontrolle. Dies gilt auch für abgelegene Energieverteilungssysteme mit Umspannwerken.

17.3.5 RFID

Verfolgungssysteme mit RFID (Funkerkennung) oder ähnlichen Verfahren werden in vielen Anwendungen zur Verfolgung von Objekten eingesetzt. Zum Beispiel können in einem Ladengeschäft speziell gekennzeichnete Artikel zusammen mit dem Videomaterial zur Verfolgung dienen, um Diebstähle zu vermeiden oder Beweise zu sichern. Ein anderes Beispiel ist die Gepäckabfertigung in Flughäfen, bei der das Gepäck mit RFID erfasst und an das korrekte Ziel geleitet werden kann. Bei einer Integration in die Videosicherheit liegen visuelle Beweise vor, wenn ein Gepäckstück verloren gegangen ist oder beschädigt wurde. Auch Suchroutinen können auf diese Weise optimiert werden.

18. Cloud-Technologien

18.1 Verschiebung in die Cloud

Cloud-Technologien haben die Art und Weise, wie wir Netzwerk-Videosicherheit angehen, revolutioniert. Mit cloudbasierten Diensten und Lösungen können die Benutzer nun jederzeit und von überall aus auf ihre Videos zugreifen. Diese erhöhte Flexibilität ermöglicht eine effizientere Überwachung und Reaktion auf Sicherheitsvorfälle.

Die Nutzung cloudbasierter Dienste und Lösungen bietet viele Vorteile. Cloudbasierte Managed Services können beispielsweise auch automatische Software-Updates durchführen, was eine manuelle Wartung erübrigt und das Risiko von Systemschwachstellen verringert. Ein weiterer wichtiger Vorteil ist die Skalierbarkeit, die es den Benutzern ermöglicht, Kameras und Speicher je nach Bedarf einfach hinzuzufügen oder zu entfernen. Der Cloud-Speicher bietet eine sichere und skalierbare Lösung für die Speicherung großer Mengen an Videodaten. Durch die externe Speicherung von Filmmaterial können Organisationen das Risiko von Datenverlusten aufgrund von Hardware-Ausfällen oder physischen Schäden verringern.

Darüber hinaus sind mit cloudbasierten Analysefunktionen fortschrittliche Funktionen wie die Erfassung von Objekten, Personenzählung und Kennzeichenerkennung möglich, die die Sicherheit und die geschäftliche Effizienz erhöhen. Die effektivste Lösung ist oft eine hybride Konfiguration, die kamerabasierte Objektklassifizierung mit serverbasierten oder cloudbasierten Algorithmen für Aufgaben kombiniert, die mehr Rechenleistung erfordern.

Grundsätzlich bietet die Integration von Cloud-Technologien in Netzwerk-Videosicherheitssysteme mehr Flexibilität, Skalierbarkeit und Sicherheit, was sie zu einer attraktiven Option für Unternehmen und Organisationen macht, die ihre Netzwerkinfrastruktur modernisieren möchten.

18.2 Cloud-Setups

Die Cloud-Video- und Geräteverwaltung besteht häufig aus einem Dienst, der über das Internet gehostet und aufgerufen wird. Über ein Abonnement können Sie so viel (oder so wenig) des

bezahlten Dienstes nutzen, wie Sie möchten. Bei jeder Definition eines Cloud-basierten Systems handelt es sich um eine Kombination der Systemfunktionen mit dem Standort dieser Funktionen. Im Folgenden finden Sie einige gebräuchliche Definitionen:

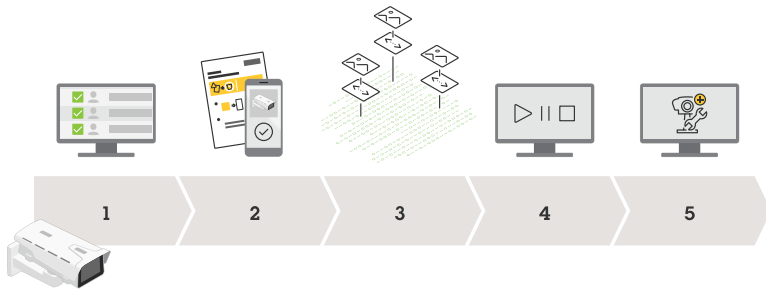
- > **Direkte Cloud-Verbindung:** Diese Lösungen werden auch als „Cam-to-Cloud“ oder „pure Cloud“ bezeichnet und haben in der Regel drei Hauptfunktionen in der Cloud – Betrachten, Verwalten und Speichern. Einige führen Analysefunktionen möglicherweise als Cloud-Anwendungen aus, obwohl es oft kostengünstiger ist, die Edge zu nutzen.
- > **Hybride Cloud:** Dies beschreibt häufig ein System, in dem einige Funktionen in der Cloud und einige lokal sind. Ein Beispiel hierfür ist eine On-Demand-Cloud, bei der die meisten Funktionen in der Cloud ausgeführt werden können, in der Praxis aber einige oder alle Funktionen am Rande der Cloud ausgeführt werden, um die Latenz zu verringern.
- > **Relais-Cloud:** Eine Lösung, die nur Cloud-Ansicht und möglicherweise einige grundlegende Verwaltungsfunktionen bietet. Alle anderen Funktionen sind entweder lokal oder über andere Lösungen verfügbar.

Die optimale Lösung hängt von den jeweiligen Bedürfnissen, Anforderungen und der Systemkonstellation ab. Für Unternehmen mit mehreren kleineren Standorten kann eine reine Cloud-Lösung am sinnvollsten sein, während für eine Organisation mit einem größeren Standort eine reine On-Premise-Lösung die richtige Option sein kann. Für die meisten Unternehmen ist eine Kombination aus leistungsstarken, angeschlossenen Edge-Geräten mit Cloud und privatem Netzwerk die ideale Lösung.

18.3 Axis Cloud Connect

Axis Cloud Connect ist eine offene, hybride Cloud-Plattform, die in Verbindung mit Axis Geräten Managed Services wie System- und Geräteverwaltung, Videobetrieb und Datenbereitstellung sowie Sicherheit und Support ermöglicht. Welche Dienste Sie erhalten, hängt von den in der Plattform enthaltenen Technologien ab.

Mit Lösungen, die Axis-Geräte verwenden und mit Axis Cloud Connect aufgebaut sind, wie AXIS Camera Station, AXIS Device Manager Edge oder AXIS Device Manager Extend werden Videobetrieb, Verwaltung des Gerätelebenszyklus und Datenzugriff flexibler und effizienter. Sie bieten auch neue Möglichkeiten in den Bereichen Sicherheit, Schutz, Betriebseffizienz und Business Intelligence.



Beispiele für Dienste über Axis Cloud Connect: 1) Benutzer- und Zugriffsverwaltung, 2) Sicheres Onboarding von Geräten, 3) Medien in der Cloud, 4) Live-Betrieb, 5) Geräteverwaltung.

19. Überlegungen für das Systemdesign

Einer der Hauptvorteile eines Netzwerk-Video-Systems ist seine Flexibilität und Skalierbarkeit: die Freiheit, die geeignetsten Komponenten von verschiedenen Anbietern miteinander zu kombinieren und die Möglichkeit, das System zu optimieren oder beliebig zu erweitern.

Dabei ist es entscheidend, die richtige Kamera auszuwählen, sie ordnungsgemäß zu installieren und zu schützen sowie sie entsprechend der Szenen-Komplexität zu konfigurieren. Zudem sollte die Kamera zum richtigen Zeitpunkt, im richtigen Format und in der richtigen Qualität Live-Bilder streamen oder Videos aufzeichnen. Auch die geeigneten Netzwerk- und Speicherlösungen sind von den ausgewählten Kameras und deren Einstellungen (z. B. Auflösung, Komprimierung und Bildrate) sowie von der Anzahl der Kameras abhängig.

Mit AXIS Site Designer können Sie für jedes Überwachungsszenario die richtige Kamera auswählen, sowie Zubehör hinzufügen und die Aufzeichnungsauflösung ermitteln. Wenn Sie den Entwurf Ihres Projekts abgeschlossen haben, können Sie mit AXIS Site Designer eine vollständige Bestellliste ausdrucken, die alles enthält, was Sie für Ihre Installation benötigen.

19.1 Auswahl einer Kamera

In diesem Abschnitt werden die Aspekte für die Auswahl einer Kamera aufgeführt.

19.1.1 Kameratypen

Um festzulegen, welche Kameratypen sich eignen, und wie viele Kameras zum Abdecken eines Bereichs erforderlich sind, müssen zunächst die Szene und ihre Bedingungen ermittelt werden. Sie müssen auch über den Zweck Ihrer Überwachungsmaßnahme nachdenken.

- > **Innen- oder Außenbereich.** Wenn die Kamera im Außenbereich angebracht werden soll, muss sie hierfür geeignet sein oder über ein geeignetes Schutzgehäuse verfügen. Beachten Sie die

IP-Einstufung (ab IP66) oder die NEMA (National Electrical Manufacturers Association)-Einstufung (ab 4X). Die Kamera sollte zudem über eine automatische Blendenfunktion verfügen.

- > **Schwenken/Neigen/Zoomen (PTZ) oder unbewegliche Kamera.** PTZ-Kameras mit einem großen optischen Zoom-Faktor können detailreiche Bilder liefern und einen großen Bereich überwachen. Beachten Sie, dass der Bediener die Bewegungen steuern muss, wenn die Möglichkeiten einer PTZ-Kamera vollständig ausgeschöpft werden sollen. Hierzu kann auch eine automatische Kameratour eingerichtet werden. Für Überwachungsaufzeichnungen ohne Live-Überwachung sind unbewegliche Kameras in der Regel die kostengünstigere Lösung.
- > **Lichtempfindlichkeit und Beleuchtungsanforderungen.** Die Lichtempfindlichkeit ist einer der wichtigsten Faktoren einer Kamera. Die Tag- und Nachtfunktionalität ermöglicht Bilder auch bei schlechten Lichtbedingungen. Einige Kameras sind mit integrierten LED-Infrarotleuchten ausgestattet, die eine energieeffiziente, unauffällige Beleuchtung ermöglichen, die für das Auge unsichtbar ist, aber auch bei Dunkelheit scharfe Bilder ermöglicht.
- > **Völlige Dunkelheit und Perimeterschutz.** Wärmebildkameras können selbst in völliger Dunkelheit oder anderen schwierigen Bedingungen Bewegungen erkennen. Sie können zudem Bewegungen in größerer Entfernung als herkömmliche Kameras wahrnehmen.
- > **Vor Manipulation oder Vandalismus geschützte Kameras und weitere Spezialgehäuse.** Ein ausreichender Schutz vor Wasser, Staub, Temperatur und Vandalismus ist entscheidend.
- > **Verdeckte oder äußerst unauffällige Überwachung.** Dies hilft bei der Auswahl von Kameras, die offen abschreckend wirken oder weniger offensichtlich installiert sind.
- > **Abdeckung.** Ermitteln Sie für einen bestimmten Ort, welche Bereiche für die Überwachung relevant sind, wie viele dieser Bereiche abgedeckt sein sollen, und ob die Bereiche sich relativ nah beieinander oder weiter voneinander entfernt befinden. Wenn beispielsweise zwei relativ kleine, nah beieinander liegende Bereiche zu überwachen sind, können Sie potenziell anstelle von zwei niedriger auflösenden Kameras eine HD-Kamera mit Weitwinkelobjektiv verwendet werden.
- > **Übersicht oder Detailgenauigkeit.** Bestimmen Sie das Sichtfeld oder die Art des zu erfassenden Bildes: eine Übersicht oder Bilder mit hoher Detailgenauigkeit zur Identifizierung von Personen oder Objekten, z. B. Gesichts- oder Kennzeichenerkennung oder Überwachung von Kassenterminals (POS).
- > **Edge- oder Server-basierte Analysefunktionen.** Analysefunktionen ermöglichen effizientes Überwachen und Suchen, und sie können wertvolle Einblicke liefern. Edge-basierte Analysefunktionen bieten viele Vorteile (wenn die Kamera über genügend Rechenleistung verfügt), aber leistungsintensive Analysefunktionen können einen eigenen Analyseserver voraussetzen. Erwägen Sie, Ihre Investition zukunftssicher zu machen, indem Sie Kameras mit

Analyseunterstützung und der Leistung kaufen, die für die Art der Analyse erforderlich ist, die Sie später benötigen.

19.1.2 Bildqualität

Die Bildqualität ist eines der wichtigsten Kriterien einer Kamera. Trotzdem fällt die Auswahl der richtigen Kamera nicht immer leicht. Tatsächlich können nicht alle Aspekte der Bildqualität quantifiziert oder gemessen werden. Am besten lässt sich die Bildqualität möglicherweise ermitteln, indem verschiedene Kameras installiert und deren Bilder verglichen werden. Denken Sie daran, dass sich die Bildqualität auch bei qualitativ hochwertigen Standbildern verschlechtern kann, wenn sich die Szene stark bewegt oder wenn wenig Licht vorhanden ist.

Viele Faktoren wirken sich auf die Bildqualität aus. So sind z. B. der Weißabgleich und die Anpassungsfähigkeit der Kamera unter verschiedenen Lichtbedingungen (fluoreszierende, Natriumdampf-Hochdruck- und LED-Lampen) für die Farbtreue entscheidend. Schwaches Licht, Gegenlicht, dynamisches Licht und andere extreme Lichtverhältnisse stellen Herausforderungen dar, die die Kamera meistern muss. In der Regel ist eine Kamera, die hochauflösendes Videomaterial aufzeichnet, weniger lichtempfindlich als eine, die mit geringerer Auflösung aufzeichnet. In anderen Worten: Möglicherweise müssen Sie Einbußen bei der Auflösung hinnehmen, um eine bessere Leistung bei dunklen Lichtbedingungen zu erzielen, oder gar Kameras mit Sensoren und Verarbeitungsalgorithmen verwenden, die speziell für diese Herausforderungen ausgelegt sind.

19.1.3 Auflösung

Beim Entwurf eines Überwachungssystems ist der Zweck des Systems zu berücksichtigen. Mithilfe der technischen Daten können Sie herausfinden, welche Kamera die beste Auflösung hat. Um Kosten und Aufwand zu optimieren, sollten Sie sich darauf konzentrieren, welche Kamera und welches Setup Ihren Betriebsvoraussetzungen entsprechen. Möchten Sie zum Beispiel Personen aus dem Videomaterial identifizieren können oder müssen Sie nur erkennen, ob eine Person anwesend ist?

Wir unterscheiden zwischen **Erfassung**, **Beobachtung**, **Erkennung** und **Identifizierung**. Diese Anforderungen werden mitunter als DORI bezeichnet.

Technische Anforderungen	Detailgenauigkeit
Erfassung	Es kann festgestellt werden, ob eine Person anwesend ist.
Beobachtung	Es ist möglich, die Anzahl der Personen zu ermitteln und Details, wie etwa einzigartige Kleidung, zu erkennen.

Technische Anforderungen	Detailgenauigkeit
Erkennung	Ein Betrachter kann ermitteln, ob eine Einzelperson mit einer zuvor gesehenen Person identisch ist oder nicht.
Identifizierung	Es ist möglich, eine Person zu identifizieren.

Tabelle 19.1a *Allgemeine technische Anforderungen bei der Videosicherheit*

Die Spezifikationen für diese Anforderungen (für visuelle Kameras) sind in der internationalen Norm IEC 62676-4 (Video Surveillance Systems for Use in Security Applications – Part 4: Application guidelines) niedergelegt.

Die Spezifikationen für diese technischen Anforderungen gelten in Situationen, in denen visuelle Videobilder von menschlichen Bedienern interpretiert werden. Für Analysefunktionen oder andere Systeme, in denen die Bildanalyse von Software durchgeführt wird, gelten andere Definitionen für die Betriebsanforderungen. In der Wärmebildtechnologie (mit Wärmebildkameras) gelten wieder andere Spezifikationen bei den technischen Anforderungen.

Die von Ihnen ausgewählte Kamera muss in der Lage sein, das passende Sichtfeld sowie eine adäquate Pixeldichte für die von Ihnen priorisierten Objekte zu bieten, z. B. das Gesicht einer Person.

Die Grundlage der empfohlenen Pixeldichte ist die Pixelanzahl, die erforderlich ist, um die Breite eines menschlichen Gesichts mit seinen einzigartigen Erkennungsmerkmalen der gewünschten Detailgenauigkeit wiederzugeben. Um eine standardisierte Pixeldichte zu erhalten, kann die Pixeldichte des Gesichts auf Grundlage der durchschnittlichen Breite eines menschlichen Gesichts von 16 cm auf die entsprechende Pixelanzahl pro Meter berechnet werden. Die Tabelle listet die resultierenden Pixeldichten für unterschiedliche Kategorien von technischen Anforderungen auf.

Technische Anforderungen	Erforderliche Pixeldichte		
Erfassung	4 px/Gesicht	25 px/m	8 px/ft
Beobachtung	10 px/Gesicht	63 px/m	20 px/ft
Erkennung	20 px/Gesicht	125 px/m	40 px/ft
Identifizierung	40 px/Gesicht	250 px/m	80 px/ft

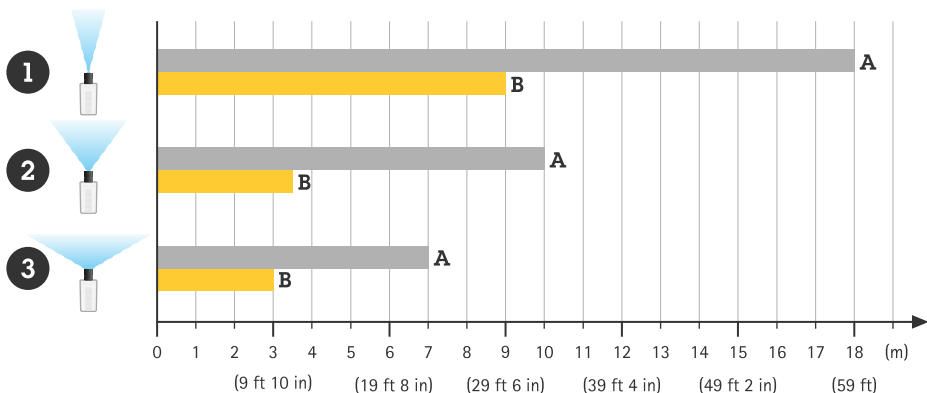
Tabelle 19.1b *Pixeldichten für unterschiedliche technische Anforderungen*

Üblicherweise wird empfohlen (zum Beispiel in IEC 62676-4), dass ein menschliches Gesicht mindestens 40 Pixel breit sein sollte, um eine Identifizierung zu ermöglichen. Sogar eine noch höhere Pixeldichte kann vorteilhaft sein und eine Sicherheitsspanne für schwierige Bedingungen bieten, wie z. B. suboptimale Beleuchtung und Personen, die nicht direkt in die Kamera schauen. Wenn eine Installation nicht den Vorgaben in Bezug auf die Pixeldichte entspricht, muss dies nicht unbedingt bedeuten, dass die Betriebsvoraussetzungen nicht erfüllt werden. In der Realität wird das Ergebnis immer noch durch weitere Faktoren wie Lichteinfall, Qualität der Optik und Bildkomprimierung beeinflusst.

Auch ist zu bedenken, dass bei der Überwachung einer Szene durch einen externen Bildschirm die Möglichkeit zur Erfassung, Beobachtung, Erkennung und Identifizierung von Personen stark von der Auflösung dieses Bildschirms abhängt.

Kameras von Axis verfügen über eine Pixelzählerfunktion, mit der sich die Pixeldichte in einem Bild mühelos überprüfen lässt. Es handelt sich hier um eine visuelle Hilfe in Form eines Rahmens. Die Breite und Höhe des Rahmens (in Pixeln gemessen) wird deutlich angezeigt.

Die Pixeldichte eines zu überwachenden Objekts hängt von der Auflösung des Kamerasensors, der Entfernung des Objekts von der Kamera und der Art des verwendeten Objektivs ab. Die Wahl der Optik ist besonders wichtig und eine Wissenschaft für sich. Deshalb ist es ratsam, mit Anbietern zusammenzuarbeiten, die Kameras liefern, die durchgängig mit dem mitgelieferten Objektiv getestet wurden. Die Abbildung zeigt ein allgemeines Beispiel dafür, wie sich die maximale Entfernung für die Erkennung und Identifizierung bei unterschiedlichen Objekttypen (d. h. unterschiedlichen Sichtfeldern) ändern kann.



Beispiele dafür, wie sich die maximalen Entfernungen für die Erkennung (A) und Identifizierung (B) je nach Objekttyp ändern: Tele (1), normal (2), Weitwinkel (3).

Axis bietet mehrere Online-Tools für die Projektierung eines Sicherheitsstandorts, die neben der Pixeldichte noch viele weitere Faktoren berücksichtigen. AXIS Site Designer hilft bei der Berechnung der Bildauflösung und des Sichtfelds basierend auf dem Kameramodell und der Position. Mit diesem Tool können Sie die gewünschte Pixeldichte festlegen und dann die Montagehöhe und das Sichtfeld der Kamera anpassen, um zu ermitteln, ob die Kamera den Anforderungen des Anwendungsfalls entspricht oder nicht.

19.1.4 Komprimierung

Kameras, die mehrere Videokomprimierungsstandards unterstützen, bieten eine größere Flexibilität in Bezug auf die Anzeige- und Aufzeichnungsanforderungen.

Das Entwerfen des Netzwerk- und Speichersystems ist in hohem Maße vom gewählten Komprimierungsstandard abhängig. Im Folgenden finden Sie einige grundlegende Empfehlungen:

- > **AV1.** Dieser neue Standard ist die empfohlene Option, wenn Ihr System ihn unterstützt. AV1 ist für die Videoübertragung über das Internet optimiert und bietet hochauflösendes und kosteneffizientes Videostreaming und Speicher.
- > **H.264.** Der mittlerweile vorherrschende Videokomprimierungsstandard für die Videosicherheit. Im Vergleich zu AV1 benötigen H.264-Videos etwa doppelt so viel Speicherplatz.
- > **H.265.** Die H.265-Kodierung erfüllt noch nicht vollständig die Anforderungen der Videosicherheit. Die meisten Überwachungsgeräte unterstützen H.265, jedoch sind die Unterstützung für Decoder und den Browser eingeschränkt. Viele Benutzer müssen weiterhin H.264 verwenden, um Videos auf ihren bevorzugten Clients anzusehen, aber das sollte kein Problem sein, da Zipstream mit H.264 sehr bitrateneffizient ist.
- > **Axis Zipstream.** Filtert weniger interessante Bereiche heraus und komprimiert sie stärker, während die relevanten Details und Bewegungen mit höherer Qualität aufgezeichnet werden. Der Wechsel zwischen einem maximalen und einem niedrigeren GOP-Wert verringert die Bitrate sowie die Anforderungen an Bandbreite und Speicher erheblich.

19.1.5 Netzwerkfunktionalität

Nicht nur qualitativ hochwertige Bilder, sondern auch die Netzwerkfunktionen sind von großer Bedeutung. Neben der Ethernet-Verbindung sollte eine Netzwerk-Kamera folgende Funktionen unterstützen:

- > **Power over Ethernet (PoE)** bedeutet, dass die Stromversorgung der Kamera über dasselbe Kabel wie die Datenübertragung erfolgt, sodass keine zusätzlichen Netzkabel verlegt werden

müssen. PTZ-Kameras im Außenbereich erfordern möglicherweise mehr Strom, der über einen Midspan geliefert werden kann.

- > Mit **Dynamic Host Configuration Protocol (DHCP)** werden IP-Adressen verwaltet. Ein DHCP-fähiger Switch oder Router vergibt automatisch an jedes angeschlossene Gerät eine IP-Adresse. Möglicherweise sind jedoch statische IP-Adressen aufgrund ihrer Vorhersagbarkeit und der Möglichkeit, den ID-Nummern der Kameras bestimmte IP-Adressen zuzuordnen, vorzuziehen.
- > **HTTPS** ist eine Verschlüsselung für die sichere Kommunikation.
- > Mit **SNMP** können IT-Administratoren den Zustand des Netzwerks überwachen und ermitteln, ob für die angeschlossenen Geräte eine Wartung erforderlich ist.
- > Mit der **IP-Adressen-Filterung** ist nur definierten IP-Adressen der Zugriff auf die Kamera möglich.
- > **Cybersicherheitsfunktionen** sind entscheidend für den Schutz der Kamera und des Netzwerks, mit dem sie verbunden ist. Integrierte Cybersicherheitsfunktionen wehren verschiedene Arten von Cyberangriffen ab, eliminieren zuverlässig Schwachstellen und verhindern unberechtigte Zugriffe auf Ihr System. *Sicheres Booten* beispielsweise stellt sicher, dass ein nicht authentifizierter, veränderter Code während des Bootvorgangs blockiert und zurückgewiesen wird, bevor er das System angreifen oder infizieren kann. Mit einem *signierten Betriebssystem* können Sie die Integrität der Gerätesoftware überprüfen, bevor Sie neue Geräte installieren oder bestehende Geräte verbessern.
- > **Drahtlostechnologie** ist eine sinnvolle Option, wenn das Verlegen eines Kabels zu Netzwerk-Kamera unpraktisch, schwierig oder teuer ist. Für Standard-Netzwerk-Kameras kann auch ein drahtloser Zugriff bereitgestellt werden, indem diese mit einer WLAN-Brücke oder einem WLAN-Dongle versehen werden.

19.1.6 Weitere Funktionen

Netzwerk-Kameras bieten über Videostreams hinaus viele weitere Funktionen. Bei der Auswahl einer Kamera müssen diese Funktionen berücksichtigt werden. Einige Beispiele für zusätzliche Funktionen sind:

- > **Audio für Kommunikation und Erfassung.** Die Benutzer können verschiedene Arten von Geräuschen erfassen und klassifizieren sowie Anweisungen, Befehle oder Anfragen an Besucher oder Eindringlinge übermitteln. Die Mikrofone können Alarmer oder die Kameraaufzeichnung auslösen, wenn Töne über einer bestimmten Lautstärke erkannt werden. Ermitteln Sie, ob Sie Ein- oder Zwei-Wege-Audio benötigen.

- > **Integrierte Analysefunktionen.** Mit integrierter Intelligenz ist das System skalierbarer, so dass eine geringere Bandbreite und weniger Speicher erforderlich sind, da die Kamera entscheiden kann, wann Videodaten gesendet und verarbeitet werden sollen.
- > **Ein-/Ausgangsanschlüsse (E/A).** Wenn Sie externe Eingabegeräte (z. B. Türkontakte, Infrarot-Bewegungsmelder, Radarmelder, Glasbruchsensoren oder Stoßsensoren) an eine Kamera anschließen, kann die Kamera auf externe Ereignisse reagieren, indem sie z. B. ein Video aufnimmt und sendet. Über die Ausgänge können die Kamera oder der Bediener externe Geräte wie z. B. Alarmgeräte, Schlösser oder Lampen steuern.
- > **Audio-/visuelle Alarme.** Ein Audio-/visueller Alarmmelder kann zur Abschreckung von Eindringlingen oder zur Verbesserung der Betriebseffizienz mithilfe von Blitzlicht und Sirenenalarms verwendet werden. Dieses voll vernetzte Gerät ist besonders wertvoll, wenn es an eine Kamera mit Perimeterschutz oder Kennzeichenerkennungs(LPR)-Analyse angeschlossen ist.
- > **Edge-to-Edge-Konnektivität.** Edge-to-Edge ist eine Technologie, mit der IP-Geräte direkt miteinander kommunizieren. Sie bietet eine intelligente Koppelungsfunktion z. B. zwischen Axis Kameras und Axis Audio- oder Radarprodukten.
- > **Radar.** Die Bewegungserkennung auf Radarbasis ist eine wertvolle Ergänzung für Videosicherheitssysteme. Das Gerät kann beim Erfassen eines Eindringlings nicht nur einen Alarm auslösen, sondern dazu auch noch die Videoaufzeichnung für die Sichtüberprüfung aktivieren. Wenn Radar mit einer PTZ-Kamera kombiniert wird, kann das Radar die Kamera automatisch steuern. Es gibt auch Kameras, die mit einem vollständig integrierten Radar kombiniert werden. Diese können Objekte unabhängig von der Sichtbarkeit über weite Bereiche erfassen und dann die Geschwindigkeit und Entfernung von sich bewegenden Objekten direkt in der Anwendungsansicht visualisieren.
- > **Alarmverwaltungsfunktionen.** Erweiterte Kameras können Alarmverwaltungsaufgaben wie z. B. das Verarbeiten und Verknüpfen von Ein- und Ausgängen sowie weitere Ereignisse übernehmen. Mit entsprechenden Puffern können Kameras vor oder nach einem Alarm Video aufzeichnen.
- > **Weitere Geräte für die physische Sicherheit.** Bei der Bewertung eines Videosicherheitssystems sollten Sie auch andere Systemkomponenten wie Zutrittskontrolle, IP-Türsprechanlagen, Audiolösungen und Eindringfänger berücksichtigen. So können Sie feststellen, ob sich ein integriertes System erstellen lässt, das alle physischen Sicherheitsanforderungen abdeckt.
- > **Unterstützung für mehrere Anwendungen und einfache Integration.** Stellen Sie sicher, dass Ihre Kameras über offene APIs (Application Programming Interfaces) verfügen und daher in verschiedene Video Management Software Anwendungen integriert werden können. Alle Axis

Kameras sind ONVIF-konform, sodass sie unabhängig vom Hersteller gemeinsam mit anderen Netzwerk-Videoprodukten eingesetzt werden können.

19.2 Installation einer Netzwerk-Kamera

Die Installationsmethode einer Netzwerk-Kamera ist genauso wichtig wie die Auswahl der passenden Kamera. Im Folgenden finden Sie einige Empfehlungen in Bezug auf die Kamerapositionierung, damit Sie erstklassige Videosicherheit erzielen.

19.2.1 Überwachungsziel

Um eine Kamera optimal zu positionieren, müssen Sie wissen, welches Bild erfasst werden soll. Wenn Sie z. B. Menschen oder Objekte erfassen möchten, die sich in verschiedene Richtungen auf unterschiedliche Positionen zu- oder von diesen wegbewegen, benötigen Sie ein Übersichtsbild, auf dem Sie derartige Ereignisse am besten erkennen können. Im Anschluss an die Auswahl einer geeigneten Übersichtskamera können Sie diese in einer sinnvollen Position installieren.

Mit AXIS Site Designer können Sie die optimale Position einer Kamera ermitteln. Zudem verfügt das Programm über Plug-Ins für verschiedene Diagramm- und 3D-Softwarelösungen. Mit diesen Tools können Sie Kameras platzieren, Sichtwinkel und Erfassung berechnen sowie tote Winkel und die Sicht versperrende Objekte finden.

19.2.2 Umgang mit schwierigen Lichtverhältnissen

Szenen mit sehr wenig Licht, direktem Sonneneinfall in die Kamera oder anderen Gegenlichtproblemen können für herkömmliche Kameras eine Herausforderung darstellen. Die Kameras von Axis sind mit verschiedenen Lösungen ausgestattet, die auch bei widrigen Bedingungen für gute Bilder sorgen. Beispiele hierfür sind Lightfinder, IR-LEDs und Forensic WDR. Wenn es die Szene und der Einsatzort zulassen, können Sie eine externe Beleuchtung hinzufügen. Einige Kameras verfügen über einen Sonnenschutz, der die Auswirkungen von direktem Sonnenlicht reduziert und das Platzieren der Kamera vereinfacht.

Obwohl auch die automatischen Einstellungen der Kameras von Axis in der Regel für optimale Bilder sorgen, können Einstellungen wie Helligkeit, Schärfe, Weißabgleich und WDR manuell geändert werden.

Alternativ zu visuellen Kameras können auch Wärmebildkameras eingesetzt werden, um schwierige Lichtbedingungen zu bewältigen.

19.2.3 Objektivauswahl

Für die Auswahl des Objektivs muss das Sichtfeld definiert werden. Das Sichtfeld ergibt sich aus der Brennweite des Objektivs sowie der Größe des Bildsensors. Die Brennweite eines Objektivs wird durch den Abstand zwischen dem Eingangsobjektiv (oder bei einer komplexen Objektivanordnung einem bestimmten Punkt) und dem Punkt, an dem alle Lichtstrahlen genau zusammentreffen (normalerweise der Bildsensor der Kamera), definiert. Je länger die Brennweite, desto enger das Sichtfeld.

Das Sichtfeld kann in drei Typen eingeteilt werden:

- > Normale Ansicht: Entspricht dem Sichtfeld des menschlichen Auges.
- > Tele-Darstellung: Ein engeres Sichtfeld, das in der Regel mehr Details enthält, als das menschliche Auge wahrnehmen kann. Ein Objektiv für die Tele-Darstellung kann in der Regel weniger Licht erfassen als ein gewöhnliches Objektiv.
- > Weitwinkel: ein größeres Sichtfeld mit weniger Details als in Normalansicht. Ein Weitwinkelobjektiv bietet in der Regel eine gute Schärfentiefe und eine ordentliche Leistung bei schwachem Licht.

AXIS Site Designer und das Produktauswahl-Tool sind bei der Auswahl von Kamera und Linse hilfreich. Weitere Informationen finden Sie im Axis Tool-Portal, www.axis.com/support/tools.

19.3 Physischer Schutz der Kamera

Überwachungskameras werden häufig in Umgebungen eingesetzt, in denen sie stark beansprucht werden. Bei Installationen im Außenbereich müssen sie vor witterungsbedingten Einflüssen geschützt werden. Im Industriebereich müssen die Kameras oft vor Gefahren wie Staub, Säuren oder ätzenden Stoffen geschützt werden. In Fahrzeugen wie Bussen und Zügen müssen die Kameras hohe Luftfeuchtigkeit, Staub und Vibrationen aushalten. Manche Kameras müssen auch gegen Vandalismus und Manipulation geschützt werden.

In den folgenden Abschnitten finden Sie Informationen zu folgenden Themen: Schutzarten, Gehäuse, Positionieren von unbeweglichen Kameras in Gehäusen, Dome-Kameras, Schutz gegen Vandalismus und Manipulation sowie Befestigungsarten.

19.3.1 Schutz und Standards

Die größten Umweltrisiken für Videoprodukte bilden – speziell im Außenbereich – Kälte, Hitze, Wasser, Staub und Schnee. Mittlerweile sind viele Geräte von Axis für den Innen- und Außenbereich so konstruiert, dass sie bereits standardmäßig gegen diese Umweltbedingungen

geschützt sind und keine separaten Gehäuse benötigen. Dies ermöglicht kompaktere Geräte und eine einfachere Installation. Beispielsweise sind Axis Kameras, die für den Betrieb bei Temperaturen bis 75 °C (167 °F) konzipiert wurden, selbst dann sehr kompakt, wenn sie über ein integriertes aktives Kühlsystem verfügen.

Das Kameradesign kann zudem die Zuverlässigkeit und Wartungsfreundlichkeit während der gesamten Lebensdauer der Kamera gewährleisten, insbesondere bei extremen Betriebsbedingungen. Beispielsweise sind einige der unbeweglichen und PTZ-Kameras von Axis mit Arctic Temperature Control ausgestattet, was einen Einsatz der Kameras ohne zusätzlichen Verschleiß der mechanischen Teile bei Minustemperaturen bis -40 °C (-40 °F) ermöglicht. Manche Dome-Kameras von Axis können auch ohne Arctic Temperature Control bei -40 °C/-40 °F in Betrieb genommen werden und sofort Videos senden.

Der Schutzgrad von Gehäusen, ob eingebaut oder als separates Gehäuse, wird häufig durch Klassifizierungen angegeben, die durch Normen wie IP, NEMA und IK festgelegt sind. IP steht für Ingress Protection und ist weltweit gültig. NEMA steht für National Electrical Manufacturers Association und gilt in den Vereinigten Staaten. IK-Bewertungen beziehen sich auf äußere mechanische Einwirkungen und gelten international.

Die gebräuchlichsten Schutzklassen für Axis Geräte für den Innenbereich sind IP42, IP51 und IP52, die Schutz vor Staub und Feuchtigkeit/Wasser bieten. Axis Geräte für den Außenbereich haben in der Regel die Schutzklassen IP66 und NEMA 4X. IP66 bietet Schutz vor Staub, Regen und starkem Strahlwasser. NEMA 4X bietet nicht nur Schutz gegen Staub, Regen und starkes Strahlwasser, sondern auch gegen Schnee, Korrosion und Schäden durch Eisbildung von außen. Einige Axis Kameras, die für extreme Umgebungsbedingungen entwickelt wurden, entsprechen auch dem US-amerikanischen Militärstandard MIL-STD-810G, der sich auf hohe Temperaturen, Temperaturschocks, Strahlung, Salzsprühnebel und Sand bezieht. Für vor Vandalismus geschützte Produkte werden die Klassen IK08 und IK10 am häufigsten verwendet, um die Widerstandsfähigkeit gegen äußere Einwirkungen zu definieren.

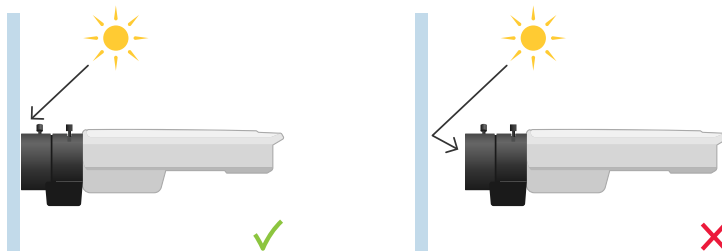
Wenn Kameras z. B. in der Lebensmittelindustrie Säuren ausgesetzt sind, sind Gehäuse aus rostfreiem Stahl erforderlich. Spezialgehäuse können auch aus ästhetischen Gesichtspunkten sinnvoll sein. Zudem gibt es spezielle druckdichte, wasserdichte oder kugelsichere Gehäuse. Wenn Kameras in explosionsgefährdeten Umgebungen installiert werden sollen, kommen andere Standards zur Geltung. Beispiele: IECEx, eine globale Zertifizierung, und ATEX, eine europäische Zertifizierung.

19.3.2 Externe Gehäuse

Wenn die durch die Umgebung bedingten Anforderungen zu hoch für die Betriebsbedingungen eines Netzwerk-Video-Produkts sind, sind externe Gehäuse erforderlich. Die Gehäuse sind in verschiedenen Größen und Ausführungen mit unterschiedlichen Eigenschaften erhältlich. Es gibt Gehäuse mit Heizung und Belüftung (Gebläse), um schwankenden Temperaturbedingungen gerecht zu werden. Einige verfügen über Peripheriegeräte wie Antennen für drahtlose Anwendungen. Eine externe Antenne ist jedoch nur erforderlich, wenn das Gehäuse aus Metall gefertigt ist.

Installationen im Außenbereich machen unter Umständen den Einsatz spezieller Gehäuse für Video-Encoder und Zubehör wie E/A-Audiomodule und Video-Decoder erforderlich. Wichtige Systemkomponenten wie Netzteil, Midspan und Switch müssen möglicherweise zudem vor Witterung und Vandalismus geschützt werden.

19.3.2.1 Unbewegliche Kameras in Gehäusen positionieren



Wenn die Kamera hinter Fensterglas montiert wird, ist eine korrekte Positionierung wichtig, um Spiegeleffekte zu vermeiden.

Beim Installieren einer unbeweglichen Kamera in einem Gehäuse ist es wichtig, dass das Kameraobjektiv im rechten Winkel zum Fensterglas montiert ist, um Spiegelungen im Bild zu verhindern. Zur Verringerung von Spiegeleffekten sind auch spezielle Beschichtungen erhältlich, die auf dem Glas vor dem Objektiv aufgebracht werden können. Unbewegliche Außenkameras von Axis werden in für den Außenbereich geeigneten Gehäusen geliefert. Dies spart Zeit bei der Installation und verhindert Fehler.

19.3.3 Transparente Dome-Kameras

Die transparente Kuppel ist das „Sichtfenster“ des Gehäuses und besteht in der Regel aus Acryl (PMMA) oder Polycarbonatkunststoff. Da die Fenster als optische Linsen fungieren, müssen sie von hoher Qualität sein, damit die Bildqualität nicht beeinträchtigt wird. Mängel des Materials beeinträchtigen die Transparenz.

Noch höhere Anforderungen gelten für die Domes von Gehäusen von PTZ-Kameras. Sie müssen nicht nur speziell geformt (kuppelförmig) sondern auch äußerst klar sein, da bei hohen Auflösungen und Vergrößerungsfaktoren der Kameras auch Mängel wie z. B. Schmutzpartikel vergrößert dargestellt werden. Wenn zudem die Dicke des Domes uneinheitlich ist, wird im resultierenden Bild eine Gerade möglicherweise gekrümmt angezeigt. Qualitativ hochwertige Dome-Gehäuse dürfen die Bildqualität unabhängig von Zoom-Stärke und Objektivposition nur geringfügig beeinträchtigen.

Es ist möglich, die Dicke des Dome-Gehäuses zum Schutz gegen starke Erschütterungen zu erhöhen. Dadurch wird jedoch auch das Risiko von Mängeln größer. Dickere Abdeckungen können außerdem unerwünschte Spiegelungen und Lichtbrechungen hervorrufen. Dickere Dome-Abdeckungen müssen daher höhere Anforderungen erfüllen, um die Gefahr einer Beeinträchtigung der Bildqualität zu minimieren.

Es gibt eine Vielzahl von Dome-Abdeckungen in durchsichtiger und getönter Ausfertigung. Getönte Abdeckungen ermöglichen zwar eine verdeckte Montage, sie reduzieren jedoch – vergleichbar mit einer Sonnenbrille – die der Kamera zur Verfügung stehende Lichtmenge. Dies wirkt sich wiederum auf die Lichtempfindlichkeit der Kamera aus.



Durchsichtige, getönte und teilweise getönte Dome-Abdeckungen für PTZ und Dome-Kameras.

19.3.4 Schutz vor Vandalismus und Manipulation

In bestimmten Überwachungsszenarien sind die Kameras zuweilen dem Risiko von Vandalismus ausgesetzt. Die Stoßfestigkeit kann durch die IK-Schutzart einer Kamera oder eines Gehäuses angezeigt werden. Die IK-Schutzart gibt an, wie gut die Gehäuse von elektrischen Anlagen und Maschinenteilen gegen äußere mechanische Einwirkungen geschützt sind. Ein IK10-Stoßfestigkeitsgrad bedeutet zum Beispiel, dass das Produkt einem Schlag von 20 Joules standhält, was dem Aufprall eines 5 kg schweren Objekts aus einer Höhe von 40 cm entspricht. Unabhängig von der tatsächlichen technischen Umsetzung sind die Ziele des Vandalismusschutzes folgende:

- > **Verhindern durch Erschweren.** Manipulationen an Sicherheitskameras sollten möglichst erschwert werden. Noch wichtiger ist möglicherweise, dass Design und Anbringungsort eine Manipulation schwer erscheinen lassen.
- > **Schaffen von Unsicherheit.** Wenn Täter die Kamera angreifen, sollten sie im Unklaren darüber bleiben, ob sie die Kamera erfolgreich zerstört oder die Aufzeichnung unterbrochen haben.

- > **Verlängern und Verzögern.** Auch wenn eine Kamera vor einem entschlossenen Angriff nicht geschützt werden kann, lohnt es sich, das Zerstören oder Umlenken der Kamera für die Täter möglichst zeitraubend zu gestalten. Jede gewonnene Sekunde erhöht die Chance, dass der Täter entdeckt wird oder aufgibt.
- > **Erkennung und Alarme.** Eine Kamera mit integrierter Analyse kann Manipulationsversuche erkennen und die Betreiber benachrichtigen.

Es gibt keine Kameras bzw. Gehäuse, bei denen in jeder Situation ein 100%-iger Schutz vor zerstörerischem Verhalten gewährleistet ist, dennoch kann der Schutz vor Vandalismus anhand folgender Aspekte verstärkt werden:

Design von Kamera/Gehäuse. Ein Gehäuse oder eine herkömmliche unbewegliche Kamera, die von einer Wand absteht oder von der Decke herabhängt, ist empfindlicher für Angriffe (zum Beispiel Schläge) als Gehäuse, die etwas verdeckter verbaut sind, wie etwa bei einer Dome-Kamera oder PTZ-Kamera. Durch die glatte, abgerundete Form einer Dome-Kamera oder einer an der Decke befestigten PTZ-Dome-Kamera ist es zudem schwieriger, das Sichtfeld der Kamera einzuschränken, etwa durch Vorhängen mit Stoff. Je besser das Gehäuse oder die Kamera in die Umgebung eingebunden ist oder als etwas anderes getarnt wird, z. B. als Außenbeleuchtung, um so besser ist der Schutz gegen Vandalismus.

Halterungen. Eine versenkt montierte Kamera, bei der nur die transparenten Teile der Kamera oder des Gehäuses sichtbar sind, ist besser gegen Angriffe geschützt, als eine von außen vollständig zugängliche Kamera. Berücksichtigen Sie beim Planen der Kameramontage sowie des Schutzes vor Vandalismus stets die Kabelführungen. Ein optimaler Schutz ist gegeben, wenn das Kabel hinter der Kamera direkt durch die Wand oder Decke geführt wird. Auch Installationsrohre aus Metall schützen Kabel vor Angriffen.

Kamerapositionierung. Eine hoch an einer Wand oder der Decke montierte Kamera wird seltener spontanen Angriffen ausgesetzt sein. Hierdurch können sich Nachteile beim Sichtfeld ergeben, die jedoch durch ein anderes Objektiv ausgeglichen werden können.

Manipulationsschalter. Durch das Hinzufügen von Manipulationsschaltern zu Kameragehäusen und -kästen wird der Schutz verbessert. Wenn dieses Zubehör ausgelöst wird, kann ein Alarm oder eine Benachrichtigung an ausgewählte Clients gesendet werden.

Analyse. Intelligente Algorithmen können auch erkennen, ob eine Kamera umgelenkt, verdeckt oder manipuliert wurde. Zudem können Alarmmeldungen an Bediener in zentralen Kontrollräumen oder an Mitarbeiter vor Ort gesendet werden. Es gibt Algorithmen zur Erkennung von: veränderter Ansicht (Manipulation), ungewöhnlichen Geräuschen (Audio), wenn die Kamera Gewalt ausgesetzt ist (Schock), wenn das Gehäuse geöffnet oder manipuliert wird (offenes Gehäuse) und wenn Kabel

durchtrennt werden (überwachte Ein-/Ausgänge). Insbesondere benachrichtigt Sie AXIS Image Health Analytics, wenn das Bild blockiert, unscharf, unterbelichtet oder umgeleitet ist.

19.3.5 Arten von Befestigungssätzen

Da nicht nur bestimmte Arten von Räumen überwacht werden müssen, ist eine Vielzahl von Befestigungsoptionen erforderlich. Mit der Wahlhilfe für Zubehör von Axis können Benutzer das richtige Gehäuse und das dazugehörige Montagezubehör ermitteln. Weitere Informationen finden Sie im Axis Tool-Portal, www.axis.com/support/tools

Um Erschütterungen zu vermeiden, sollte stets eine stabile Kamerahalterung verwendet werden. Da PTZ-Kameras innerhalb ihres Gehäuses beweglich sind, können nicht ordnungsgemäß befestigte Kamerahalterungen zu Bildstörungen führen. Im Außenbereich ist eine robuste Befestigungs-ausrüstung erforderlich, um Erschütterungen durch starken Wind zu vermeiden. Wenn die Halterung nicht stark oder stabil genug ist, kann die Kamera fallen und Personen- oder Sachschäden verursachen.

Deckenhalterungen. Kameras können mithilfe folgender Elemente an der Decke angebracht werden:

- > Flächenhalterung: Vollständig sichtbare direkte Befestigung an der Deckenoberfläche.
- > Versenkte Montage: Innerhalb der Decke montiert, wobei nur Teile der Kamera und des Gehäuses sichtbar sind (in der Regel der Dome). Diese Befestigung wird auch als bündige oder abgehängte Montage bezeichnet.
- > Hängemontage-Satz: Ermöglicht eine hängende Befestigung der Kamera an einer Decke.
- > Lichtschienenhalterung: Damit kann die Kamera ohne zusätzliche Bohrung an einer vorhandenen Lichtschiene befestigt werden.



Beispiele für Oberflächenmontage und versenkte Montage (oben); Hängemontage-Satz und Lichtschienenhalterung (unten).

Wandhalterungen. Wandhalterungen werden häufig zur Befestigung von Kameras in oder außerhalb von Gebäuden verwendet. Das Gehäuse ist an einer Halterung befestigt, die an der Wand montiert wird. Anspruchsvollere Halterungen verfügen zum Schutz der Kabel über innere Kabelverschraubungen. Wenn ein Gehäuse an der Ecke eines Gebäudes angebracht werden soll, wird eine herkömmliche Wandhalterung und zusätzlich ein Eckadapter benötigt.

Masthalterungen. Masthalterungen werden häufig für PTZ-Kameras in großflächigen Außenbereichen wie z. B. Parkplätzen, Straßen und Plätzen eingesetzt. Mit dieser Befestigungsart werden gewöhnlich die Auswirkungen von Wind und Bodenvibrationen auf die Kamera ausgeglichen. Beim Berechnen der Schwingung müssen sowohl die Höhe und der Durchmesser des Mastes als auch das Material berücksichtigt werden. Betonmasten schwanken weniger als Holz- oder Metallmasten. Berücksichtigen Sie zudem das Gewicht und die Abmessungen der Ausrüstung, die der Mast tragen soll. Dies ist besonders wichtig für PTZ-Kameras und Kameras mit hohem optischem Zoom – wenn der Mast unterdimensioniert ist, besteht ein größeres Risiko von Bewegungsunschärfe auf den Bildern. Anspruchsvollere PTZ-Kameras verfügen über eine integrierte elektronische Bildstabilisierung, um die Auswirkungen von Wind und Erschütterungen zu verringern. Schwere Kameras können beim Fallen jedoch zu gefährlichen Verletzungen führen. Wie

bei der Wandmontage werden die Kabel häufig im Inneren des Mastes geführt, sodass die Öffnungen ordnungsgemäß abgedichtet werden müssen.



Beispiele für Wand- und Masthalterung.

Brüstungshalterungen. Brüstungshalterungen werden zur Befestigung von Kameras auf Dächern sowie zum Erhöhen der Kamera eingesetzt, um einen besseren Sichtwinkel zu erzielen. Ein Vorteil der Brüstungshalterung besteht darin, dass die Kamera kostengünstiger und einfacher gewartet werden kann als bei einer Wandmontage. Da die Halterung nach innen schwingen kann, ist der Wartungszugang über das Dach möglich, sodass keine Kräne oder Hebebühnen eingesetzt werden müssen.

Äußerst unauffällige Montage. Eine äußerst unauffällige Montage erfolgt in der Regel dort, wo winzige modulare Kameras an Orten angebracht werden, an denen Diskretion oberstes Gebot ist. Diese Befestigung kann vollständig unauffällig und kaum sichtbar (Pinhole-Halterung), teilweise sichtbar (bündige Montage) oder vollständig sichtbar (Oberflächenmontage) erfolgen.



Beispiele für die Brüstungshalterung und eine äußerst unauffällige Montage (eine modulare Kamera in einer Höhenleiste verborgen).

19.4 Kriterien für die Bandbreite und den Speicher

Bei der Planung eines Videosicherheitssystems sind die Anforderungen an die Netzwerkbandbreite und den Speicherplatz wichtige Faktoren. Mit AXIS Site Designer können Sie den Bedarf Ihres Systems effektiv abschätzen. Die Anforderungen an Bandbreite und Speicherplatz hängen von den folgenden Faktoren ab:

- > Anzahl Kameras
- > Kontinuierliche oder durch Ereignisse ausgelöste Aufzeichnung
- > Edge-Aufzeichnung in der Kamera oder im Video-Encoder, serverbasierte Aufzeichnung oder eine Kombination
- > Länge der täglichen Aufzeichnungsdauer der Kamera
- > Bilder pro Sekunde
- > Bildauflösung
- > Typ der Videokomprimierung: H.264, H.265, AV1 und ob Zipstream verwendet wird
- > Szenen-Komplexität: Bildkomplexität, Lichtverhältnisse und Ausmaß der Bewegung
- > Aufbewahrungsdauer der aufgezeichneten Daten.

19.4.1 Bits oder Bytes?

Was unter verschiedenen Begriffen wie Bits, Bytes, Mbit/s, Gigabytes usw. verstanden wird, ist häufig verwirrend. Welcher Begriff steht für Kapazität? Welcher für Geschwindigkeit?

Datengrößen

Die kleinste Einheit mit digitalen Informationen ist eine Binärziffer, besser bekannt als Bit (b), die einen von zwei möglichen Werten haben kann. Diese werden oft als 1 oder 0 dargestellt, manchmal jedoch als Ein/Aus, true/false, ja/nein, +/-.

Da Bits so kleine Inkrementschritte an Daten sind, verwenden wir Vielfache davon, um von größeren Werten zu sprechen:

- > 1.000 Bits = 1 Kilobit (kBit)
- > 1 Million Bits = 1 Megabit (Mbit)

Bits können auch in Gruppen dargestellt werden, so genannten Bytes. 1 Byte (B) = 8 Bits (b). Diese acht Bits sind die erforderliche Mindestmenge für die Darstellung eines einzelnen Zeichens in einem Text.

Die gleichen Präfixe für Bits werden auch für Bytes verwendet:

> 1 Million Bytes = 1 Megabyte (MB)

> 1 Milliarde Bytes = 1 Gigabyte (GB)

Gut zu wissen ist, dass Computer Binärsysteme und nicht Dezimalsysteme sind – das heißt, sie arbeiten mit Basis zwei anstelle von Basis zehn. Dies bedeutet, dass sich die genauen Gesamtsummen in den beiden Systemen unterscheiden, selbst wenn die verschiedenen Präfixe (Kilo, Mega, Giga usw.) häufig sowohl für Dezimal- als auch für Binärwerte verwendet werden.

Zum Beispiel, um 1 Byte mit 1.000 zu multiplizieren:

> Bei Basis zehn (Dezimal) wären dies $10^3 = 1.000$

> Bei Basis zwei (binär) beträgt der entsprechende Wert $2^{10} = 1.024$

Obwohl sich beide Werte leicht unterscheiden, werden sie in der Regel als „1 Kilobyte“ angegeben, weil die meisten Menschen es viel einfacher finden, in Dezimalzahlen zu zählen als in Binärzahlen. Festplattengrößen werden in der Regel in Dezimalwerten angegeben. 1 GB wird beispielsweise als genau eine Milliarden Byte definiert.

Da der mit dem Laufwerk genutzte Computer jedoch ein Binärsystem ist, wird ein Laufwerk mit 10 GB vom Computer als nur mit 9,31 GB bezeichnet, da in einem Binärsystem 10 GB = 10.737.418.240 Bytes sind.

Da jedes Byte acht Bits enthält, folgt daraus:

> 1 Mb = 0,125 MB

> 8 Mb = 1 MB

Weitere Vergleiche der Datengrößen finden Sie in der folgenden Tabelle.

Gerät	Größe (binär)	Größe (dezimal)
Kilobyte (KB)	1.024 Bytes	1.000 Bytes
Megabyte (MB)	1.024 Kilobytes	1.000.000 Bytes
Gigabyte (GB)	1.024 Megabytes	1.000.000.000 Bytes
Terabyte (TB)	1.024 Gigabytes	1.000.000.000.000 Bytes

Petabyte (PB)	1.024 Terabytes	1.000.000.000.000.000 Bytes
Exabyte (EB)	1.024 Petabytes	1.000.000.000.000.000.000 Bytes

Tabelle 19.4a *Vergleich von Datengrößen.*

Datenübertragungsraten

Netzwerk- oder Internetverbindungen werden in Megabit pro Sekunde (Mbit/s) angegeben. Obwohl dies ein Maß für die Kapazität (Anzahl der bewegten Bits pro Sekunde) ist, werden Werte in Mbit/s im Allgemeinen als Geschwindigkeiten bezeichnet, d. h. Verbindungen mit hoher Kapazität werden oft als schnell wahrgenommen.

Beachten Sie bei Netzwerk-Videos, dass die Daten „Bit für Bit“ und nicht in Bytes über das Netzwerk gesendet werden. Dies bedeutet, dass Mbit/s hilfreich sein können, um eine Verbindung zu beschreiben, über die ein Live-Videostream angezeigt werden kann, also wenn das Video nicht heruntergeladen und gespeichert wird. Eine „schnelle“ Verbindung ermöglicht ein ruckelfreies Ansehen (durch Verringerung der Verzögerung) und das Anzeigen hochauflösender Videos. Wenn Sie stattdessen einfach das Video herunterladen und speichern möchten, ist die Verbindungsgeschwindigkeit weniger wichtig. Eine langsamere Verbindung braucht möglicherweise etwas länger als eine schnelle Verbindung, um das Video herunterzuladen. Aber ist das wirklich wichtig?

Auch hier ist relevant, dass Bits, die über ein Netzwerk übertragen werden, nicht immer in der richtigen Reihenfolge ankommen und nicht unbedingt von derselben Quelle stammen. Dies ist kein Problem, da die Anwendungen Bits in der richtigen Reihenfolge ordnen. Es wird jedoch deutlich, warum Netzwerkgeschwindigkeiten in der Regel in Mbit/s und nicht in Bytes angegeben werden.

Obwohl Mbit/s die gebräuchlichste Methode zur Definition von Datengeschwindigkeiten sind, können MB/s auch verwendet werden, z. B. beim Speichern eines Videos auf einer Festplatte. Das Herunterladen/Übertragen einer 100 MB-Videodatei über eine 100 Mbit/s-Verbindung würde 8 Sekunden dauern, da die in MB/s konvertierte Schreibgeschwindigkeit 12,5 MB/s (d. h. 100 Megabyte = 800 Megabit) beträgt.

19.4.2 Bandbreitenanforderungen

In einem kleinen Überwachungssystem mit höchstens zehn Kameras kann ein 100 Megabit-Netzwerk-Switch verwendet werden, ohne Einschränkungen der Bandbreite berücksichtigen zu müssen. Die meisten Unternehmen können ein Überwachungssystem dieser Größe im Rahmen ihrer

vorhandenen Netzinfrastruktur implementieren. Bei mehr als 10 Kameras lässt sich die Netzwerk-Last anhand folgender Faustregel schätzen:

- > Eine Kamera, die so konfiguriert ist, dass sie hochwertige Bilder bei hohen Bildraten liefert, beansprucht etwa 2 bis 8 Mbit/s der verfügbaren Netzwerkbandbreite.
- > Bei mehr als 12 bis 15 Kameras sollten Sie einen Switch mit einem Gigabit-Backbone in Erwägung ziehen. Wird ein Gigabit-Switch verwendet, sollte auf dem Server mit der Video Management Software ein Gigabit-Netzwerkadapter installiert sein.

Zu den Technologien, die die Verwaltung der genutzten Bandbreite ermöglichen, gehören die Verwendung von VLANs in einem Switch-Netzwerk, Quality of Service und ereignisbasierte Aufzeichnungen.

19.4.3 Speichieranforderungen

Einer der Faktoren, die sich auf den Speicherbedarf auswirken, ist die Art der verwendeten Videokomprimierung. H.264 ist derzeit der vorherrschende Standard für die Videokomprimierung in der Videosicherheit, auch wenn die Formate AV1 und H.265 wesentlich effizienter sind.

Neue Systeme unterstützen AV1, das den Speicherbedarf im Vergleich zu H.264 um 50 % reduziert. H.264 wird noch viele Jahre lang parallel zu AV1 unterstützt werden.

H.265 erfüllt noch nicht vollständig die Anforderungen der Videosicherheit.

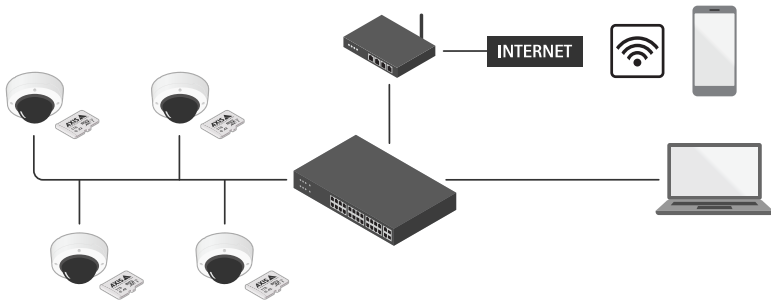
Es wird empfohlen, Zipstream zu aktivieren, da es den Speicherumfang des Systems erheblich verringern kann, ohne den forensischen Wert der Videos zu beeinträchtigen.

AXIS Site Designer ist die optimale Möglichkeit, den Speicherbedarf ohne Vor-Ort-Messungen einzuschätzen. Mit diesem Tool können Sie die richtigen Kameras und Zubehörteile für Ihre Überwachungsszenarien und -zwecke auswählen und automatisch den Speicher- und Bandbreitenbedarf einschätzen. Dabei müssen im Tool alle Kameras mit Szenentyp, Auflösung, Bildrate, Qualitätsauswahl und Aufzeichnungseinstellungen konfiguriert werden.

19.4.4 Systemkonfigurationen

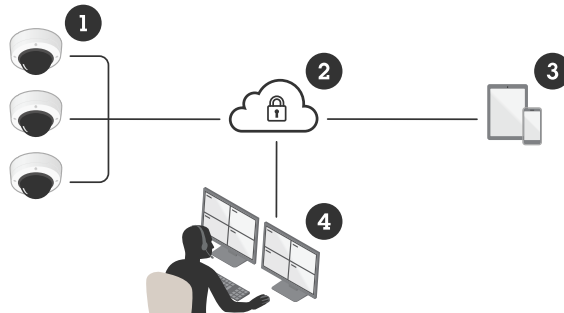
Edge-Lösung. Eine Kamera kann mit einer SD-Speicherkarte ausgestattet sein, um Videos und Metadaten zu speichern. Axis hat besonders hoch belastbare SD-Speicherkarten speziell für die Videosicherheit entwickelt. Bei Edge Storage oder Cloud Storage ist weder ein Netzwerk-Video-Videorecorder noch ein Dateiserver erforderlich. Auch Analysen, die das Videomaterial und/oder Metadaten verarbeiten, können direkt in der Kamera ausgeführt werden. Bei einem hybriden Setup profitieren die Systeme von einer Kombination aus Edge-, Cloud- und Vor-Ort-Komponenten.

Cloud-basierte Komponenten bieten Remote-Ansicht, Cloud-Speicherung, Remote-Systemüberwachung und Remote-Verwaltung.



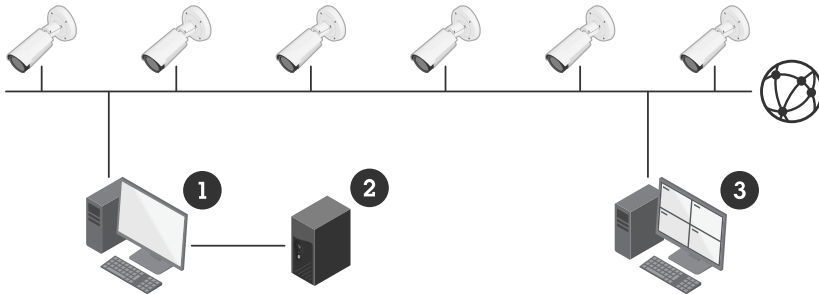
Eine Lösung mit Edge Storage und einem VMS für die Videoverwaltung.

Cloud-Lösung. Bei einem Cloud-Video-Setup werden die meisten Systemkomponenten von einem Dienstanbieter verwaltet, der den Benutzern über das Internet den Zugriff auf Live-Videos und Aufzeichnungen ermöglicht. Axis Cloud Connect ist eine offene Hybrid-Cloud-Plattform, die zusammen mit Axis Geräten Managed Services ermöglicht.



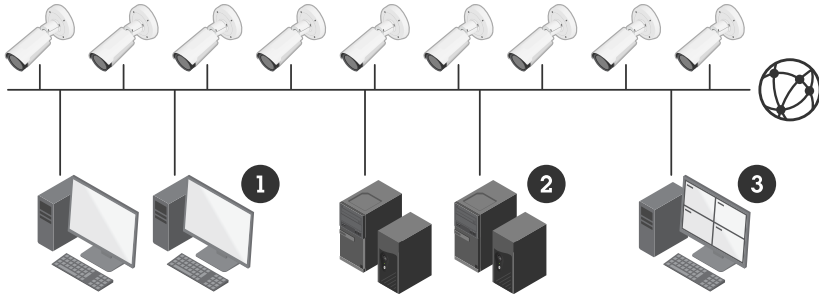
Bei einer Cloud-Lösung wird das Video (1) in der Cloud (2) gespeichert und verwaltet. Autorisierte Benutzer können über mobile Geräte (3) oder einen beliebigen Browser (4) auf Live- und aufgezeichnete Videos zugreifen.

Vor-Ort-Lösung. Bei einer typischen Installation vor Ort wird der Speicher, die Verwaltung und die Wartung des Systems über einen Server erledigt, während das Anzeigen und der Betrieb von Video- und Ereignisbenachrichtigungen über einen Client verwaltet wird. Der Speicher wird üblicherweise mit RAID konfiguriert, um die Leistung und Zuverlässigkeit zu optimieren. Analysefunktionen können auf Edge, aber auch auf einem Server basieren.



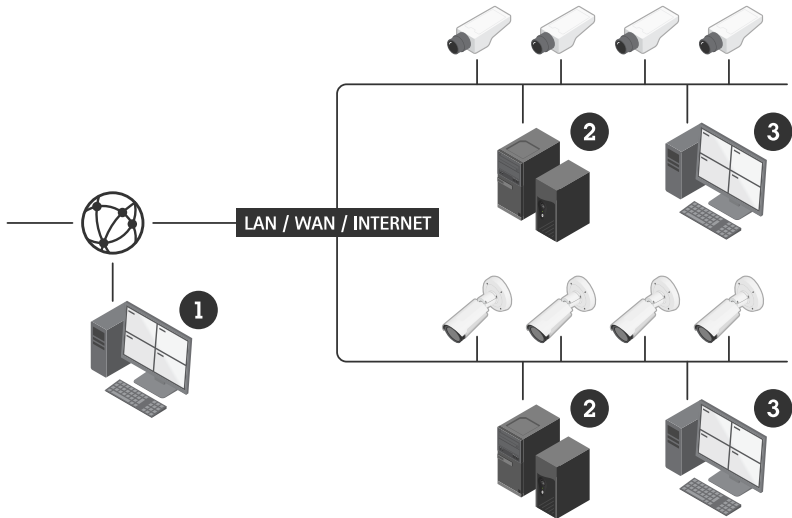
Eine Lösung vor Ort mit einem Server (1), optionalem RAID-Speicher (2) und einem Workstation-Client.

Großes zentralisiertes System. Für eine große Installation ist hohe Leistung und Zuverlässigkeit erforderlich, um die großen Datenmengen und Bandbreiten zu verwalten. Hierfür werden mehrere Server benötigt, denen bestimmte Aufgaben zugewiesen sind. Ein Hauptserver steuert das System und entscheidet, welche Videos auf welchem Speicherserver gespeichert werden. Mithilfe dedizierter Speicherserver ist ein Lastausgleich möglich. In einem solchen Setup lässt sich das System auch vergrößern, indem bei Bedarf weitere Speicherserver hinzugefügt und Wartungen durchgeführt werden, ohne das gesamte System abschalten zu müssen.



Ein großes zentralisiertes System mit Hauptservern (1), Speicherservern (2) und einer Workstation für die Überwachung (3).

Großes verteiltes System. Für die Überwachung mehrerer Standorte, die zentral verwaltet werden sollen, können verteilte Aufzeichnungssysteme verwendet werden. An jedem Standort werden Videoaufnahmen über lokale Kameras aufgezeichnet und gespeichert. Der Haupt-Controller kann die Aufzeichnungen an allen Standorten anzeigen und verwalten.



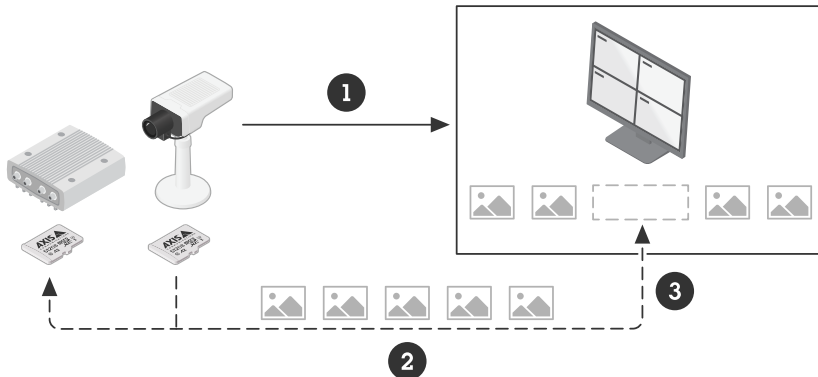
Ein großes verteiltes System mit Überwachungsstationen (1, 3) und Speicherservern mit RAID (2).

19.4.5 Edge Storage

Edge-Storage, manchmal auch als lokaler Speicher oder Onboard-Aufzeichnung bezeichnet, ermöglicht es Kameras und Video-Encodern, Aufzeichnungen lokal auf einer SD-Speicherkarte (Secure Digital), einem Netzwerk-Speicher (NAS) oder auf einem Dateiserver zu erstellen, zu steuern und zu verwalten. Edge Storage kann als der Hauptspeicher in einer hybriden Cloud-Lösung verwendet werden.

Edge Storage ermöglicht flexible und zuverlässige Speicherlösungen. Zu den Vorteilen zählen eine höhere Systemzuverlässigkeit, qualitativ hochwertige Videos bei Installationen mit niedriger Bandbreite, Aufzeichnungen für die mobile und Fernüberwachung sowie eine Integration in die Video Management Software. Der Einsatz von SD-Speicherkarten als einziges Speichermedium für Aufzeichnungen ist eine äußerst kostengünstige Lösung.

Edge Storage kann die zentrale Speicherung ergänzen. Videos können fortlaufend parallel oder bei Ausfall des zentralen Systems lokal aufgezeichnet werden. Wenn diese Lösung mit einer Video Management Software wie AXIS Camera Station eingesetzt wird, sind zudem ausfallsichere Aufzeichnungen möglich. Hierbei werden durch Störungen im Netzwerk oder zentrale Systemwartungsarbeiten verursachte fehlende Videosequenzen später von der Kamera abgerufen und mit dem Material im zentralen Speicher zusammengeführt, um sicherzustellen, dass die Videoaufzeichnungen unterbrechungsfrei sind.



Edge Storage als Redundanz (unterbrechungsfreie Aufzeichnung).

- 1 Im Normalbetrieb überträgt die Kamera Videomaterial zum Speichern zur VMS.
- 2 Bei einem Netzausfall werden Videoclips vorübergehend auf der SD-Karte in der Kamera gespeichert.
- 3 Wenn die Netzwerkverbindung wieder hergestellt ist, ruft die VMS die fehlenden Videoclips ab und fügt sie in die Aufzeichnung ein.

Außerdem kann Edge Storage die Videoforensik bei Systemen verbessern, die über niedrige Netzwerkbandbreiten verfügen, so dass der Videostream nicht in der höchsten Qualität erfolgen kann. Durch die Verwendung einer Überwachung bei niedriger Bandbreite und gleichzeitiger lokaler Aufzeichnung mit hoher Qualität können die Benutzer ihre jeweilige Bandbreite optimal ausnutzen und trotzdem qualitativ hochwertige Videoaufzeichnungen von Vorfällen erhalten, die genauer untersucht werden müssen.

Edge Storage kann auch verwendet werden, um Aufzeichnungen an entfernten Standorten oder anderen Installationen zu verwalten, zu denen nur vorübergehend oder niemals eine Netzwerkverbindung besteht. In Zügen und anderen Schienenfahrzeugen kann Edge Storage dazu dienen, zunächst Onboard-Videoaufnahmen aufzuzeichnen und diese dann an das zentrale System zu übertragen, sobald das Fahrzeug an einer Station anhält.

Axis bietet Überwachungskarten, d. h. SD-Karten, die speziell für eine optimale Leistung bei der Videosicherheit entwickelt wurden. Diese sind für den industriellen Einsatz geeignet und damit widerstandsfähig gegen die Auswirkungen extremer Temperaturen und Umgebungen. Sie haben auch eine höhere Ausdauer, um dem typischen Aufzeichnungsverhalten einer Überwachungskamera zu entsprechen. Dies bedeutet, dass sie viel häufiger beschrieben und überschrieben werden können als eine herkömmliche SD-Karte. Daher kann dieselbe Karte ohne Verschleiß länger verwendet werden.

Mit Sicherheitskarten wird Videomaterial unter optimaler Ausnutzung jedes Speicherblocks aufgezeichnet. Dies spart nicht nur Speicher, sondern verringert auch die Anzahl der Zyklen zum Schreiben/Löschen, um die Lebensdauer der Karte effektiv zu erhöhen.

Edge Storage mit SD-Speicherkarten oder NAS. Die folgenden Vor- und Nachteile der Verwendung von SD-Speicherkarten oder NAS für Edge Storage müssen berücksichtigt werden:

- > SD-Speicherkarten sind einfacher zu installieren und zu konfigurieren als ein NAS.
- > SD-Speicherkarten können manipuliert werden, wenn sie physisch zugänglich sind. NAS kann an einem sicheren Standort platziert werden.
- > Bei einem Ausfall ist immer nur die jeweilige SD-Karte betroffen. Wenn ein NAS oder seine Anbindung ausfällt, sind viele Kameras betroffen.
- > Ein NAS kann über eine RAID-Konfiguration verfügen.
- > Das Auswechseln von SD-Speicherkarten kann kostspielig sein, wenn die Kamera an schwer zugänglichen Orten montiert wurde (z. B. an einem Mast oder einer Wand in einer Höhe über 4,5 m).

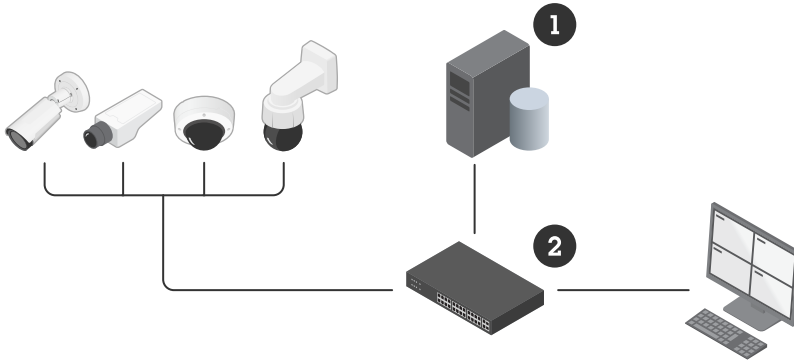
19.4.6 Server-basierter Speicher

Für die serverbasierte Speicherung ist ein Server erforderlich, der lokal an die Netzwerk-Videogeräte für die Videoverwaltung und Aufzeichnung angeschlossen ist. Auf dem Server läuft eine Video Management Software, die Videos entweder auf der lokalen Festplatte (Direct Attached Storage) oder auf NAS aufzeichnet. Abhängig von seiner Zentraleinheit (CPU), Netzwerkkarte und dem internen RAM (Random Access Memory) kann der Server eine bestimmte Anzahl von Kameras, Bilder pro Sekunde und Bildgrößen verarbeiten. Die meisten Server haben Platz für mehrere Festplatten.

19.4.7 NAS und SAN

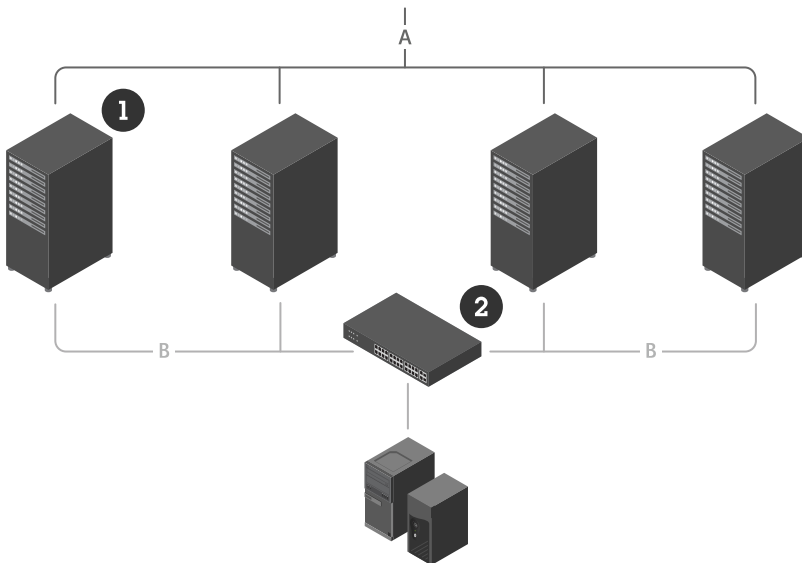
Wenn die Anforderungen an Speicherplatz und Speicherverwaltung größer sind als die verfügbare Kapazität der angeschlossenen Festplatten, sorgt ein NAS-Speicher bzw. ein Speichernetzwerk (SAN) für mehr Speicherplatz, Flexibilität und Wiederherstellbarkeit.

NAS ist ein einzelnes, direkt mit dem LAN verknüpftes Speichergerät und bietet eine gemeinsame Speichermöglichkeit für alle Clients im Netzwerk. Ein NAS-Gerät ist eine kostengünstige Speicherlösung, die sich einfach installieren und verwalten lässt.



Network-Attached Storage (1) wird über den Netzwerk-Switch (2), einen Breitbandrouter oder eine Unternehmens-Firewall mit einem Netzwerk-Videosystem verbunden.

Ein SAN ist ein Hochgeschwindigkeitsnetzwerk für Speichergeräte. Es wird über einen Glasfaserkanal mit einem oder mehreren Servern verbunden. Die Benutzer können über die Server auf alle Speichergeräte des SAN zugreifen, wobei der Speicher auf mehrere Hundert Terabyte erweitert werden kann. Der zentrale Speicher senkt den Verwaltungsaufwand und stellt ein flexibles Hochleistungs-Speichersystem für Umgebungen mit mehreren Servern zur Verfügung. Glasfasertechnologie wird häufig eingesetzt, um Datenübertragungsraten von bis zu 16 GBit/s zu erreichen und große Datenmengen mit einem hohen Maß an Redundanz zu speichern.



SAN-Architektur, in der Speichergeräte miteinander kombiniert werden und die Speicherkapazität gemeinsam nutzen. Benutzer können über die Server (1) und einen Glasfaserkanal-Switch (2) auf jedes Speichergerät zugreifen.

A. TCP/IP LAN

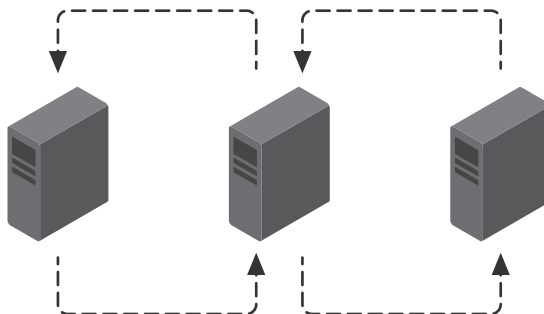
B. Glasfaserkanal

19.4.8 Redundanter Speicher

Durch Redundanz in einem Speichersystem können Videos oder andere Daten gleichzeitig an mehreren Orten gespeichert werden. Dadurch wird ein Backup für die Wiederherstellung von Videomaterial erstellt, falls ein Teil des Speichersystems unlesbar wird. Diese zusätzliche Speicherstufe kann in einem IP-Sicherheitssystem auf verschiedene Weise bereitgestellt werden, zum Beispiel als redundante Anordnung unabhängiger Festplatten („Redundant Array of Independent Disks“, RAID), durch Datenduplizierung, Server-Cluster, mehrere Video-Empfänger, Cloud-Redundanzspeicher und SD Karten.

RAID. Ein RAID ist eine Anordnung von Standard-Festplatten zu einem Gesamtsystem, das vom Betriebssystem als eine einzige große Festplatte betrachtet wird. Ein RAID-Setup verteilt die Daten mit ausreichender Redundanz auf mehreren Festplattenlaufwerken, damit die Daten wiederhergestellt werden können, falls eine Festplatte ausfällt. Es gibt verschiedene RAID-Stufen, von einer praktisch redundanzfreien Lösung bis hin zu einer Lösung mit vollständiger Datenspiegelung, bei der es bei einem Festplattenausfall zu keinen Unterbrechungen oder Datenverlusten kommt.

Datenduplizierung. Die Datenduplizierung ist ein Merkmal vieler Netzwerk-Betriebssysteme. Die Netzwerk-Dateiserver sind so konfiguriert, dass sie die Daten untereinander duplizieren, damit eine Sicherung vorhanden ist, wenn ein Server ausfällt.



Datenduplizierung.

Server-Cluster. Eine typische Server-Clustering-Methode besteht darin, für zwei Server dasselbe Speichergerät auszuführen, beispielsweise ein RAID-System. Wenn ein Server ausfällt, übernimmt der andere, identisch konfigurierte Server. Diese Server können sogar über dieselbe IP-Adresse verfügen, sodass das sogenannte „Failover“ für die Benutzer vollständig transparent wird.

Mehrere Video-Empfänger. Eine gängige Methode für die Notfallwiederherstellung und externe Speicherung von Netzwerk-Videos ist die gleichzeitige Übertragung des Videos an zwei verschiedene Server an verschiedenen Standorten. Diese Server können mit RAID ausgestattet sein, als Cluster konfiguriert werden oder ihre Daten mit noch weiter entfernten Servern duplizieren. Dies ist ein besonders nützlicher Ansatz, wenn sich die Überwachungssysteme in gefährlichen oder schwer zugänglichen Bereichen befinden, wie beispielsweise in Massentransportmitteln oder in Industrieanlagen.

SD-Karte. Edge Storage mit SD-Karten kann die zentrale Speicherung ergänzen. Videos können fortlaufend parallel oder bei Ausfall des zentralen Systems lokal aufgezeichnet werden. Wenn diese Lösung zusammen mit einem VMS verwendet wird, können Failover-Aufzeichnungen verarbeitet werden. Hierbei werden durch Störungen im Netzwerk oder zentrale Systemwartungsarbeiten verursachte fehlende Videosequenzen später von der Kamera abgerufen und mit dem Material im zentralen Speicher zusammengeführt, um sicherzustellen, dass die Videoaufzeichnungen unterbrechungsfrei sind.

Cloud-Speicher. Cloudspeicher sind Daten, die in Remotesystemen gespeichert werden, wo sie verwaltet und den Benutzern über ein Netzwerk zur Verfügung gestellt werden. Cloudspeicher können von Drittanbietern angeboten werden, bei denen die Benutzer in der Regel ein Abonnement bezahlen. Private Cloudspeicher werden von der Benutzerorganisation verwaltet (und gehören ihr in der Regel), zum Beispiel wenn erhöhte Sicherheitsanforderungen gelten. Hybride Lösungen sind nützlich, wenn Organisationen unterschiedliche Arten von gespeicherten Daten trennen oder ihren Speicher erweitern müssen.

20. Tools und Ressourcen

Axis bietet eine Vielzahl praktischer Tools und Informationsressourcen für den Entwurf eines IP-Überwachungssystems. Wir bieten Ihnen Tools, mit denen Sie Produkte finden und vergleichen, Standorte planen und entwerfen, Systeme installieren und verwalten sowie Downloads und Plugins hinzufügen können. Viele Tools sind über www.axis.com/support/tools abrufbar. In diesem Kapitel werden einige unserer am häufigsten verwendeten Tools aufgeführt.

20.1 Produkte finden und vergleichen

Produktauswahl-Tool. Mit diesem Tool können Sie anhand der benötigten Merkmale und Funktionen die richtigen Kameras, Lautsprecher, Gegensprechanlage und andere Netzwerkgeräte für Ihr Projekt auswählen.

Wahlhilfe für Zubehör. Dieses Tool hilft Ihnen bei der Auswahl der richtigen Halterungen, Gehäuse, Befestigungen sowie der Stromversorgung für die Kameras Ihres Projekts.

Objektivrechner. Mithilfe des Objektivrechners können Sie verfügbare Objektive für eine bestimmte Kamera anzeigen sowie die optimale Kameraplatzierung und erforderliche Brennweite für eine bestimmte Szenengröße und Auflösung ermitteln.

Kameraauswahl für AXIS People Counter. Mit diesem Tool finden Sie vorkalibrierte Kameramodelle, mit der Sie bei der Personenzählung eine optimale Genauigkeit erzielen.

20.2 Standorte planen und gestalten

AXIS Site Designer. Mit AXIS Site Designer können Sie das Design des Überwachungssystems mithilfe von bestimmten Installationsvorgehensweisen optimieren. Egal, ob Sie ein System mit Tausenden von Axis Produkten oder nur wenigen Produkten erstellen müssen – mit AXIS Site Designer können Sie Sicherheitssysteme entwerfen, genehmigen und installieren, die genau Ihren Arbeitsbedingungen und Anforderungen entsprechen. Dank der intuitiven Produktauswahl können

Sie die idealen Kameras und Produkte für jede Situation einfach identifizieren und die passenden Halterungen und Zubehörteile sowie ihre Platzierung auswählen. Auch Systemspeicher und Bandbreite können effektiv geschätzt werden. Mit AXIS Site Designer lassen sich Sicherheitssysteme mit End-to-End-Produkten von Axis sowie Produkte von ausgewählten Drittanbieter-VMS-Partnern für größere Systeme entwerfen.

Mit dem **AXIS Plugin for Autodesk® Revit®** können Sie interaktive Axis Produkte direkt auswählen, in den Gebäudeplan einfügen und Sicherheitsfunktionen in das Design integrieren. Das Plugin verfügt über ein integriertes Produktauswahl-Tool, mit dem Sie die Abdeckung überprüfen und die Einstellungen an die Szene anpassen können.

20.3 Systeme installieren und verwalten

AXIS Installer. Vereinfacht die Installation von Axis Geräten. Mit dieser App können Sie Geräte im Netzwerk erkennen, die Konfiguration vornehmen, auf die Live-Ansicht zugreifen, um die genaue Positionierung und Fokussierung vorzunehmen, sowie Geräte sowohl in lokale Netzwerke als auch in die Cloud integrieren. Über die App können Sie zudem schnell auf die Installationsanleitung und das Benutzerhandbuch eines Geräts zugreifen, indem Sie den QR-Code® auf dem mit dem Axis-Gerät gelieferten OAK-Zettel (Owner Authentication Key) scannen.

AXIS Device Manager.. Ermöglicht eine effiziente Verwaltung der Installation, Sicherheit und Wartung wichtiger Geräte. Zu den Schlüsselfunktionen gehören das Zuweisen von IP-Adressen, das Verwalten von Gerätelisten, das Verwalten von Benutzern und Kennwörtern, das Aktualisieren der Gerätesoftware, das Erneuern und Verwalten von Zertifikaten sowie das Einrichten von Cybersicherheitsmaßnahmen zum Schutz Ihrer Netzwerk-Geräte und zur Ausrichtung an einer Sicherheitsinfrastruktur.

AXIS Device Manager Edge. Bietet eine standortbezogene Übersicht, die es Ihnen ermöglicht, den Geräteverbindungsstatus aus der Ferne zu überwachen und einfache Verwaltungsaufgaben wahrzunehmen. Er liefert eine sofortige Übersicht über den Status aller Geräte im System und ermöglicht automatische Aktualisierungen sowie einen sicheren Fernzugriff. So lassen sich Schutzmaßnahmen während des gesamten Lebenszyklus eines Geräts einfach anwenden und instand halten.

AXIS Device Manager Extend.. AXIS Device Manager Extend ist ideal für den Betrieb an mehreren Standorten geeignet und bietet eine vereinheitlichte, benutzerfreundliche Benutzeroberfläche, über die Sie Ihre Axis Geräte und Standorte proaktiv von jedem Ort aus verwalten können.

21. Axis Communications Academy

21.1 Aufbau von Fachwissen für intelligenteren Geschäftsprozesse

Wir bei Axis Communications verstehen, dass Ihr Geschäftserfolg darauf beruht, Ihre Stärken kontinuierlich weiter auszubauen und stets die neuesten Lösungen und Technologien zu haben, um Ihren Kunden das absolut Beste zu liefern.

Die Axis Communications Academy deckt alle Facetten Ihres Unternehmens ab und bietet Schulungen für alles, was Ihre Kunden von Ihnen erwarten – und alles, was Ihre Kunden noch gar nicht kennen, aber dennoch benötigen.

Wenn Sie immer über Axis Lösungen, Technologie, Branchentrends und branchenspezifische Fragen informiert sind, können Sie Ihren Kunden fachliche Kompetenz bieten. Vom Vertrieb über die Geschäfts- und Systemplanung bis hin zur Installation und Konfiguration.

Wählen Sie aus einer Reihe von Lernformaten – in persona oder online – je nach Ihrem Lernstil, Ihren Vorlieben und individuellen Bedarf.

- > Lernvideos
- > Wissenschaftliche Artikel
- > Interaktive Apps
- > E-Learning
- > Online-Training mit Schulungsleiter
- > Präsenztraining mit Schulungsleiter
- > Blended Learning (Mischung der Formate)
- > Webinare

Axis Zertifizierungsprogramm

Verschaffen Sie sich einen Wettbewerbsvorteil mit international und branchenweit anerkannten Zertifikaten.

Weitere Informationen finden Sie auf dem Portal zum Lernen unter <https://www.axis.com/learning>

Über Axis Communications

Axis ermöglicht eine smartere und sichere Welt durch die Verbesserung von Sicherheit, Schutz, betrieblicher Effizienz und Geschäftsanalytik. Als Technologieführer im Bereich Netzwerk-Video bietet Axis Videosicherheits-, Zutrittskontroll-, Intercom- und Audiolösungen. Die branchenweit anerkannten Schulungen der Axis Communications Academy vermitteln fundiertes Expertenwissen zu den neuesten Technologien.

Das 1984 gegründete schwedische Unternehmen beschäftigt etwa 5.000 engagierte Mitarbeiter in über 50 Ländern und bietet mit Technologie- und Systemintegrationspartnern auf der ganzen Welt kundenspezifische Lösungen an. Der Hauptsitz ist in Lund, Schweden.