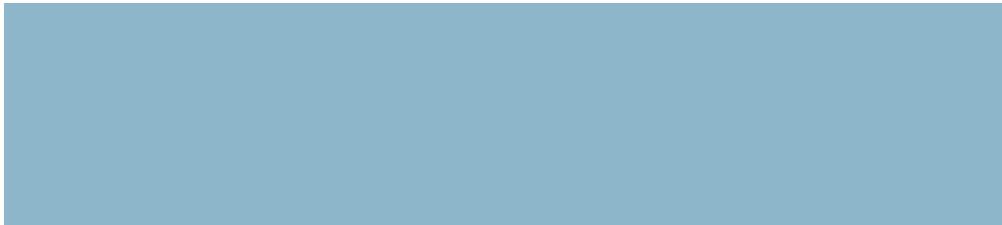


Technischer Leitfaden zur Netzwerk-Videotechnologie.

Anforderungen und Faktoren, die es zu berücksichtigen gilt, um eine IP-basierende Sicherheits- und Fernüberwachungslösung erfolgreich einsetzen zu können.



Willkommen beim technischen Leitfaden von Axis zur Netzwerk-Videotechnologie

Der Trend zu offenen Videosystemen sowie die Vorteile von Netzwerken, digitaler Bildgebung und intelligenten Kamerafunktionen bieten gänzlich neue Überwachungsmöglichkeiten. Die Netzwerk-Videotechnologie weist alle Vorteile von analogem Video sowie eine Vielzahl innovativer Funktionen und Merkmale auf, die nur mit der Digitaltechnologie möglich sind.

Bevor Sie Ihr eigenes System einrichten, müssen Sie festlegen, welche Funktionen Sie benötigen. Leistung, Interoperabilität, Skalierbarkeit, Flexibilität und zukunftssichere Funktionalität sind wichtige Faktoren. In diesem Leitfaden werden diese Faktoren eingehend erläutert, um Ihnen dabei zu helfen, eine Lösung zu entwickeln, die die Möglichkeiten der Netzwerk-Videotechnologie in vollem Umfang ausschöpft.

Das Beste im Bereich Netzwerk-Video

Axis nimmt im Bereich Netzwerk-Video weltweit eine marktführende Position ein. Wir haben als erster Hersteller die Vorteile der Netzwerk-Videotechnologie für professionelle Anwendungen zur Video- und Fernüberwachung nutzbar gemacht und im Jahre 1996 die weltweit erste Netzwerk-Kamera auf den Markt gebracht. Mit mehr als zwei Jahrzehnten Erfahrung auf dem Gebiet der Netzwerktechnologien, der größten Anzahl an installierten Netzwerk-Videoprodukten sowie starken Partnerschaften mit führenden Unternehmen weltweit ist Axis Ihr kompetenter Partner im Bereich Netzwerk-Video.

Flexible, skalierbare Lösungen

Unter Verwendung offener Technologiestandards, die eine einfache Integration und Skalierbarkeit ermöglichen, bietet Axis verschiedenste Netzwerk-Videolösungen für Video- und Fernüberwachungsanwendungen in einem breiten Branchenspektrum. Unser innovatives Sortiment umfasst Netzwerk-Kameras, die neue Maßstäbe in ihrer Klasse setzen, sowie Videoserver/Video-Encoder, die einen kostengünstigen Übergang zu den besten Produkten im Bereich der Netzwerk-Videotechnologie ermöglichen. Unser Angebot beinhaltet außerdem umfassende Softwarelösungen für die Videoverwaltung und ein breit gefächertes Zubehörsortiment.



Inhalt

Netzwerk-Video: Überblick, Vorteile und Einsatzbereiche	7
1.1 Überblick über ein Netzwerk-Videosystem	7
1.2 Vorteile	8
1.3 Anwendungsbereiche	12
1.3.1 Einzelhandel	12
1.3.2 Verkehr	12
1.3.3 Bildungseinrichtungen	12
1.3.4 Industrie	13
1.3.5 Stadtüberwachung	13
1.3.6 Behörden und öffentliche Gebäude	13
1.3.7 Gesundheitswesen	13
1.3.8 Banken und Finanzwesen	14
Netzwerk-Kameras	15
2.1 Was ist eine Netzwerk-Kamera?	15
2.2 Netzwerk-Kameratypen	16
2.2.1 Fest ausgerichtete Netzwerk-Kameras	17
2.2.2 Fest ausgerichtete Dome-Netzwerk-Kameras (Fixed Dome)	17
2.2.3 PTZ-Kameras und PTZ-Dome-Kameras	18
2.3 Tag- und Nacht Netzwerk-Kameras	21
2.4 Megapixel-Netzwerk-Kameras	23
2.5 Richtlinien für die Auswahl einer Netzwerk-Kamera	24
Kameraelemente	27
3.1 Lichtempfindlichkeit	27
3.2 Objektivelemente	28
3.2.1 Sichtfeld	28
3.2.2 Objektiv und Bildsensor aufeinander abstimmen	30
3.2.3 Standards bei den Objektivanschlüssen	31
3.2.4 Öffnungsverhältnis und Belichtung	31
3.2.5 Manuelle oder automatische Blende	32
3.2.6 Tiefenschärfe	33
3.3 Bildsensoren	34
3.3.1 CCD-Technologie	34
3.3.2 CMOS-Technologie	34
3.3.3 Megapixel-Sensoren	35
3.4 Bildabtasttechniken	35
3.4.1 Zeilensprungverfahren	35
3.4.2 Progressive Abtastung	36
3.5 Bildverarbeitung	37
3.5.1 Gegenlichtkompensation	37
3.5.2 Belichtungszonen	37
3.5.3 Großer Dynamikbereich	37
3.6 Installation einer Netzwerk-Kamera	38

Kameraschutz und Gehäuse	39
4.1 Allgemeine Hinweise zu Kameragehäusen	39
4.2 Durchsichtige Abdeckung	40
4.3 Unbewegliche Kameras in Gehäusen positionieren	40
4.4 Schutz vor schwierigen Umgebungsbedingungen	41
4.5 Schutz gegen Vandalismus und Manipulation	41
4.5.1 Design von Kamera/Gehäuse	41
4.5.2 Montage	42
4.5.3 Kamerapositionierung	43
4.5.4 Intelligentes Video	43
4.6 Befestigungsarten	43
4.6.1 Deckenhalterungen	43
4.6.2 Wandhalterungen	44
4.6.3 Masten-Halterungen	44
4.6.4 Brüstungshalterungen	44
Video-Encoder	45
5.1 Was ist ein Video-Encoder?	45
5.1.1 Video-Encoder-Komponenten und Empfehlungen	46
5.1.2 Ereignisverwaltung und intelligentes Video	47
5.2 Eigenständige Video-Encoder	47
5.3 In einem Rack montierte Video-Encoder	48
5.4 Video-Encoder für PTZ-Kameras und PTZ-Dome-Kameras	48
5.5 Deinterlacing-Techniken	49
5.6 Video-Decoder	50
Auflösungen	51
6.1 NTSC- und PAL-Auflösung	51
6.2 VGA-Auflösungen	52
6.3 Megapixelauflösungen	53
6.4 HDTV-Auflösungen (High-Definition Television)	54
Videokomprimierung	55
7.1 Grundlagen der Komprimierung	55
7.1.1 Video-Codec	55
7.1.2 Bild- im Vergleich zu Videokomprimierung	56
7.2 Komprimierungsformate	59
7.2.1 Motion JPEG	59
7.2.2 MPEG-4	60
7.2.3 H.264 oder MPEG-4 Part 10/AVC	60
7.3 Variable und konstante Bitraten	61
7.4 Standards im Vergleich	61
Audio	63
8.1 Audio-Anwendungen	63
8.2 Audio-Unterstützung und Geräte	64
8.3 Audiomodi	65
8.3.1 Simplex	65
8.3.2 Halbduplex	66

8.3.3	Vollduplex	66
8.4	Audioerkennungsalarm	66
8.5	Audiokomprimierung	66
8.5.1	Sampling-Frequenz	67
8.5.2	Bitrate	67
8.5.3	Audio-Codecs	67
8.6	Audio- und Videosynchronisierung	67
Netzwerktechnologien		69
9.1	LAN und Ethernet	69
9.1.1	Ethernet-Netzwerke	70
9.1.2.	Switch	71
9.1.3	Power over Ethernet	73
9.2	Das Internet	75
9.2.1	IPv4-Adressen	76
9.2.2	Datenübertragungsprotokolle für Netzwerk-Video	80
9.3	VLANs	82
9.4	Quality of Service	82
9.5	Netzwerksicherheit	84
9.5.1	Benutzernamen- und Kennwortauthentifizierung	84
9.5.2	IP-Adressfilterung	84
9.5.3	IEEE 802.1X	84
9.5.4	HTTPS oder SSL/TLS	85
9.5.5	VPN (Virtual Private Network)	85
Drahtlose Netzwerktechnologien		87
10.1	WLAN-Standards 802.11	88
10.2	WLAN-Sicherheit	88
10.2.1	WEP (Wired Equivalent Privacy)	89
10.2.2	WPA/WPA2 (WiFi Protected Access)	89
10.2.3	Empfehlungen	89
10.3	Wireless-Bridge	89
Videoverwaltungssysteme		91
11.1	Hardware-Plattformen	91
11.1.1	PC-Server-Plattform	91
11.1.2	NVR-Plattform	92
11.2	Software-Plattformen	93
11.2.1	Integrierte Funktionalität	93
11.2.2	Windows-Client-basierte Software	93
11.2.3	Webbasierte Software	94
11.2.4	Skalierbarkeit von Videoverwaltungssoftware	94
11.2.5	Offene im Vergleich zu herstellerspezifischer Software	94
11.3	Systemmerkmale	94
11.3.1	Anzeigen	95
11.3.2	Multi-streaming	95
11.3.3	Videaufzeichnung	96
11.3.4	Aufzeichnung und Speicherung	97
11.3.5	Ergebnisverwaltung und intelligentes Video	97

11.3.6 Verwaltungsfunktionen	102
11.3.7 Sicherheit	103
11.4 Integrierte Systeme	104
11.4.1 API (Application Programming Interface)	104
11.4.2 Kassenterminals	104
11.4.3 Zugangskontrolle	105
11.4.4 Gebäudeverwaltung	105
11.4.5 Industrielle Kontrollsysteme	106
11.4.6 RFID	106
Kriterien für die Bandbreite und den Speicher	107
12.1 Berechnung der Bandbreite und des Speicherplatzes	107
12.1.1 Erforderliche Bandbreite	107
12.1.2 Berechnung des Speicherbedarfs	108
12.2 Serverbasierter Speicher	110
12.3 NAS und SAN	110
12.4 Redundante Speicherung	112
12.5 Systemkonfigurationen	113
Tools und Ressourcen	115
Axis Communications' Academy	117
Kontaktinformationen	118

Netzwerk-Video: Überblick, Vorteile und Einsatzbereiche

Netzwerk-Video wird wie viele andere Arten der Kommunikation, z. B. E-Mail, Web-Dienste und Computertelefonie, über drahtgebundene oder drahtlose IP-Netzwerke (IP = Internet Protocol) ausgeführt. Digitale Video- und Audio-Datenströme sowie andere Daten werden über dieselbe Netzwerkinfrastruktur übertragen. Netzwerk-Video bietet Anwendern insbesondere in der Sicherheitsüberwachungsbranche viele Vorteile gegenüber herkömmlichen analogen CCTV-Systemen (CCTV = Closed-Circuit Television).

Dieses Kapitel gibt einen Überblick über Netzwerk-Video sowie über dessen Vorteile und Einsatzbereiche in verschiedenen Branchen. Ein Vergleich mit einem analogen Videoüberwachungssystem veranschaulicht die Leistungsfähigkeit und das Potenzial eines digitalen Netzwerk-Videosystems.

1.1 Überblick über ein Netzwerk-Videosystem

Ein Netzwerk-Videosystem, häufig auch IP-basierte Videoüberwachung oder IP-Videoüberwachung genannt, ermöglicht die Videoüberwachung und -aufzeichnung von einer beliebigen Position im Netzwerk aus. Dies kann beispielsweise das LAN (Local Area Network) oder ein WAN (Wide Area Network) wie das Internet sein. Im LAN-Bereich wird entweder eine drahtgebundene oder drahtlose Netzwerkinfrastruktur für die Übertragung digitaler Video-, Audio- und anderer Daten genutzt. Als drahtgebundene Variante kommt Ethernet laut dem IEEE-802.3-Standard zum tragen und als drahtlose Lösung Wireless LAN (WLAN) nach dem IEEE-802.11-Standard. Im ersten Fall kann durch die Verwendung der Power over Ethernet-Technologie (PoE) die Stromversorgung der Netzwerk-Videoprodukte über das Netzwerk erfolgen.

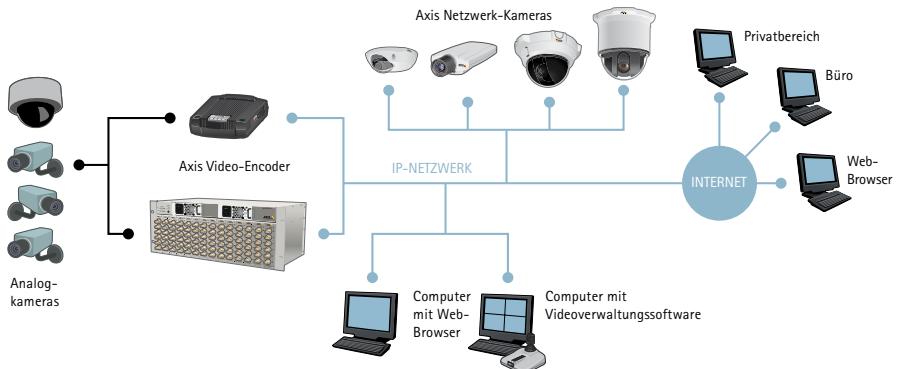


Abbildung 1.1a Ein Netzwerk-Videosystem besteht aus vielen verschiedenen Komponenten, z. B. Netzwerk-Kameras, Video-Encodern und Videoverwaltungssoftware. Bei den anderen Komponenten wie Netzwerk, Speicher und Server handelt es sich um Standard-IT-Equipment.

Die zentralen Komponenten eines Netzwerk-Videosystems sind die Netzwerk-Kameras, die Video-Encoder (für die Anbindung von analogen Kameras), das Netzwerk, der Server, das Speichermedium und die Videoverwaltungssoftware. Da Netzwerk-Kameras und Video-Encoder computerbasierte Geräte sind, bieten sie Funktionalität, die mit einer analogen CCTV-Kamera nicht erzielt werden kann. Die Netzwerk-Kameras, die Video-Encoders und die Videoverwaltungssoftware sind die Eckpfeiler einer IP-basierten Überwachungslösung.

Bei den anderen Komponenten wie Netzwerk, Speicher und Server handelt es sich um Standard-IT-Equipment. Die Möglichkeit zur Verwendung gängiger Standardprodukte ist einer der Hauptvorteile von Netzwerk-Video. Zu den anderen Komponenten eines Netzwerk-Videosystems gehören Zubehörteile, wie z. B. Kameragehäuse, PoE-Midspans und -Splitter. Die einzelnen Netzwerk-Videokomponenten werden in den folgenden Kapiteln detaillierter erörtert.

1.2 Vorteile

Das digitale Netzwerk-Videoüberwachungssystem bietet zahlreiche Vorteile und Spezialfunktionen, mit denen ein analoges Videoüberwachungssystem nicht aufwarten kann. Zu den Vorteilen gehören der Fernzugriff, die hohe Bildqualität, die Ereignisverwaltung, intelligente Videofunktionen, einfache Integrationsmöglichkeiten und eine bessere Skalierbarkeit, Flexibilität und Kosteneffizienz.

- > **Fernzugriff:** Netzwerk-Kameras und Video-Encoder sind per Fernzugriff zugänglich und konfigurierbar, wodurch mehrere autorisierte Benutzer jederzeit und von jedem vernetzten Ort weltweit Live-Videobilder und Videoaufzeichnungen abrufen können. Dies ist von Vorteil, wenn man Benutzern eines anderen Unternehmens, z. B. einer Sicherheitsfirma, Zugriff auf

die Videobilder gewähren möchte. Bei einem herkömmlichen analogen CCTV-System müssten sich die Benutzer an einem bestimmten Ort befinden, um die Videodaten anzusehen und zu verwalten. Ohne einen Video-Encoder oder einen digitalen Videorekorder (DVR) wäre ein Fernzugriff nicht möglich. Ein DVR entspricht der digitale Variante eines Videorekorders.

- > **Hohe Bildqualität:** Bei einer Videoüberwachungsanwendung ist eine hohe Bildqualität von entscheidender Bedeutung, um einen Vorgang deutlich erfassen und beteiligte Personen oder Objekte klar identifizieren zu können. Eine Netzwerk-Kamera mit progressiver Abtastung und Megapixeltechnologie kann eine bessere Bildqualität und eine höhere Auflösung liefern als eine analoge CCTV-Kamera. *Weitere Informationen zur progressiven Abtastung und zur Megapixeltechnologie finden Sie in den Kapiteln 2, 3 und 6.*

Außerdem kann die Bildqualität in einem Netzwerk-Videosystem leichter als in einem analogen Überwachungssystem sichergestellt werden. Bei den aktuellen analogen Systemen, die einen DVR als Aufzeichnungsmedium verwenden, finden zahlreiche Konvertierungen von analogen in digitale Daten statt: Zunächst werden analoge Signale in der Kamera in digitale Daten konvertiert, dann werden sie für die Übertragung wieder in analoge Signale zurück konvertiert. Anschließend werden die analogen Signale für die Aufzeichnung digitalisiert. Die Bilder verlieren bei jedem Konvertierungsvorgang und durch die Signaldämpfung auf dem Übertragungskabel an Qualität. Je weiter die analogen Videosignale transportiert werden, umso schwächer werden sie.

In einem vollständig digitalen IP-Überwachungssystem werden Bilder einer Netzwerk-Kamera einmal digitalisiert und bleiben dann im digitalen Format, sodass keine unnötigen Konvertierungen stattfinden und keine Bildverschlechterung infolge langer Übertragungswege in einem Netzwerk erfolgt. Außerdem lassen sich digitale Bilder leichter speichern und abrufen als Bilder von analogen Videobändern.

- > **Ereignisverwaltung und intelligentes Video:** Häufig werden zu viele Videodaten aufgezeichnet und es ist nicht genügend Zeit verfügbar, um sie ordnungsgemäß zu analysieren. Moderne Netzwerk-Kameras und Video-Encoder mit integrierter Intelligenz oder Analyse Funktionalität beheben dieses Problem, indem sie die Menge an irrelevanten Aufzeichnungen reduzieren und vorprogrammierte Aktionen initiieren. Solche Funktionen sind bei einem Analogsystem nicht verfügbar.

Netzwerk-Kameras und Video-Encoder von Axis bieten integrierte Funktionen wie z. B. Videobewegungserkennung, Audioerkennungsalarm, aktiven Manipulationsalarm, E/A-Verbindungen (Eingabe/Ausgabe) sowie Alarm- und Ereignisverwaltungsfunktionen. Mithilfe dieser Funktionen sind die Netzwerk-Kameras und Video-Encoder in der Lage, kontinuierlich den Dateneingang zu analysieren, um Ereignisse zu erkennen und automatisch auf ein Ereignis zu reagieren, z. B. durch Starten einer Videoaufzeichnung und Senden von Alarmbenachrichtigungen.

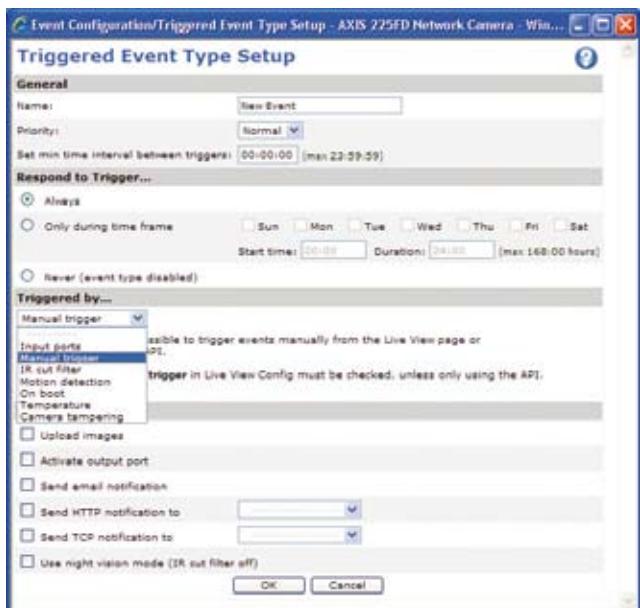


Abbildung 1.2a Einrichten eines Ereignis über die Benutzeroberfläche einer Netzwerk-Kamera.

Ereignisverwaltungsfunktionen können über die Benutzeroberfläche des Netzwerk-Video produkts oder über ein Videoverwaltungsprogramm konfiguriert werden. Benutzer können die Alarne oder Ereignisse definieren, indem sie den zu verwendenden Trigger und den Zeitraum festlegen, über den das Ereignis aktiv sein soll. Des Weiteren können die Aktionen konfiguriert werden (z. B. Aufzeichnung an einem oder mehreren Speicherorten, lokal und/oder ortsfremd aus Sicherheitsgründen, Aktivierung externer Geräte wie Alarmsirenen, Beleuchtung und Türöffner, Senden von Benachrichtigungen an Benutzer). Weitere Informationen zur Videoverwaltung finden Sie in Kapitel 11.

- > **Problemlose, zukunftssichere Integration:** Netzwerk-Videoprodukte, die auf offenen Standards basieren, können zusätzlich zu Videoverwaltungs- und Anwendungssoftware einfach mit Computer- und IP-basierten Informations-, Audio- oder Sicherheitssystemen und anderen digitalen Geräten integriert werden. Beispielsweise lässt sich die Videofunktionalität einer Netzwerk-Kamera in ein Kassenterminalsystem (POS, Point-of-Sale) oder in ein Gebäudeverwaltungssystem integrieren. Weitere Informationen zu integrierten Systemen finden Sie in Kapitel 11.
- > **Skalierbarkeit und Flexibilität:** Ein Netzwerk-Videosystem kann mit den Anforderungen seiner Benutzer wachsen. Bei IP-basierten Systemen können viele Netzwerk-Kameras und Video-Encoder sowie andere Arten von Anwendungen dasselbe drahtgebundene oder draht-

lose Netzwerk für den Datenaustausch verwenden. Daher können beliebig viele Netzwerk-Videoprodukte zum System hinzugefügt werden, ohne dass hierfür umfassende oder teure Änderungen an der Netzwerkinfrastruktur erforderlich sind. Bei einem analogen System ist dies nicht der Fall. In einem analogen Videosystem muss ein eigens dafür vorgesehenes Koaxialkabel direkt von jeder einzelnen Kamera zu einer Anzeige-/Aufzeichnungsstation gelegt werden. Wenn Audiodaten benötigt werden, sind zudem separate Audiokabel erforderlich. Netzwerk-Videoprodukte können nahezu an jedem beliebigen Ort platziert und ins Netzwerk eingebunden werden und das System kann, je nach Bedarf, mehr oder weniger offen sein.

- > **Kosteneffizienz:** Ein IP-Überwachungssystem weist gewöhnlich geringere Gesamtbetriebskosten auf als ein herkömmliches analoges CCTV-System. Meist existiert bereits eine IP-Netzwerkinfrastruktur, die beispielsweise in einer Firma für Office-Anwendungen verwendet wird, sodass eine Netzwerk-Videoanwendung einfach in die vorhandene Infrastruktur eingebunden werden kann. Drahtgebundene oder drahtlose Netzwerklösungen sind zudem deutlich günstigere als Koaxial- und Glasfaserkabel für analoge CCTV-Systeme. Darüber hinaus können digitale Videoströme über viele verschiedene kompatible Infrastrukturen um die ganze Welt geleitet werden. Die Verwaltungs- und Gerätekosten fallen ebenfalls geringer aus, da Back-End-Anwendungen und Speichersysteme auf nicht proprietären Standardservern ausgeführt werden können und nicht auf herstellerspezifischer Hardware, wie z. B. einem DVR im Falle eines analogen CCTV-Systems.

Weiterhin kann in einem Netzwerk-Videosystem die Power over Ethernet-Technologie (PoE) genutzt werden, was bei einem analogen Videosystem nicht möglich ist. PoE ermöglicht die Stromversorgung von Netzwerkendgeräten über einen PoE-fähigen Switch oder Midspan, wobei die Stromversorgung über dasselbe Ethernet-Kabel erfolgt, das auch (Video-) Daten transportiert. PoE bringt deutliche Einsparungen bei den Installationskosten mit sich und erhöht zudem die Zuverlässigkeit des Systems, indem über eine USV (Unterbrechungsfreie Stromversorgung) eine Absicherung gegen Ausfälle in der Spannungsversorgung erfolgen kann. *Weitere Informationen zu PoE finden Sie in Kapitel 9.*

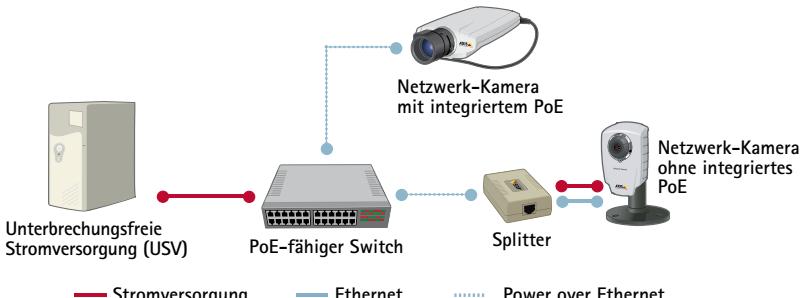


Abbildung 1.2b Ein System, das Power over Ethernet verwendet.

1.3 Anwendungsbereiche

Den Anwendungsmöglichkeiten von Netzwerk-Video sind fast keine Grenzen gesetzt. Meist kommt es jedoch im Rahmen einer Sicherheitsüberwachung oder Fernüberwachung von Personen, Plätzen, Objekten und Vorgängen zur Anwendung. Im Folgenden finden Sie einige typische Anwendungsmöglichkeiten in verschiedenen Branchen.

1.3.1 Einzelhandel



Netzwerk-Videosysteme in Einzelhandelsgeschäften können Diebstähle deutlich reduzieren, die Mitarbeitersicherheit erhöhen und das Ladenmanagement optimieren. Ein Hauptvorteil von Netzwerk-Video besteht darin, dass es in das elektronische Warenüberwachungssystem oder in ein Kassenterminalsystem (POS) integriert werden kann, um Bilder und Aufzeichnungen von Aktivitäten im Zusammenhang mit Warenschwund zu liefern. Das System ermöglicht eine schnelle Erkennung von potenziellen Vorfällen sowie von Fehlalarmen. Netzwerk-Video zeichnet sich durch eine hohe Interoperabilität aus und bietet eine rasche Investitionsrentabilität (ROI). Außerdem hilft Netzwerk-Video, die am stärksten frequentierten Bereiche in einem Laden zu identifizieren und eine Übersicht der Verbraucheraktivitäten und des Kaufverhaltens zu erstellen, um so zur Optimierung der Ladengestaltung und der Auslagen beizutragen. Es kann auch dazu verwendet werden, festzustellen, ob Regale aufgefüllt oder im Falle langer Warteschlangen weitere Kassen geöffnet werden müssen.

1.3.2 Verkehr



Netzwerk-Video kann die Personen- und allgemeine Sicherheit auf Flughäfen, Autobahnen, Bahnhöfen und bei anderen Verkehrssystemen sowie in Transportmitteln wie Bussen, Zügen und Schiffen erhöhen. Netzwerk-Video kann auch zur Überwachung der Verkehrslage eingesetzt werden, um Staus zu verringern und den Verkehrsfluss zu verbessern. Viele Installationen im Verkehrssektor erfordern erstklassige Systeme mit hoher Bildqualität (die durch die progressive Abtastung bei Netzwerk-Kameras erzielt wird), hohen Bildraten und langen Aufbewahrungszeiten. Für anspruchsvolle Umgebungen wie Busse und Züge bietet Axis Netzwerk-Kameras an, die schwankenden Temperaturen, Luftfeuchtigkeit, Staub, Erschütterungen und Vandalismus gegenüber unempfindlich sind.

1.3.3 Bildungseinrichtungen



Von Kindertagesstätten bis hin zu Universitäten – Netzwerk-Videosysteme helfen, Vandalismus vorzubeugen und die Sicherheit von Schülern und Mitarbeitern zu erhöhen. In Bildungseinrichtungen, in denen bereits eine IT-Infrastruktur vorhanden ist, stellt Netzwerk-Video eine praktischere und kostengünstigere Lösung dar als ein analoges System, da meist keine zusätzliche Verkabelung erforderlich ist. Darüber hinaus können Ereignisverwaltungsfunktionen des Netz-

werk-Videosystems Alarne generieren und Sicherheitspersonal genaue Echtzeitbilder als Entscheidungsgrundlage liefern. Netzwerk-Video kann auch für den Fernunterricht verwendet werden, z. B. für Studenten, die nicht persönlich zum Unterricht erscheinen können.

1.3.4 Industrie



Netzwerk-Video kann zur Überwachung und Optimierung von Fertigungslien, Prozessen und Logistiksystemen und zur Sicherung von Lagern und Bestandskontrollsystemen verwendet werden. Netzwerk-Video kann auch eingesetzt werden, um „virtuelle“ Konferenzen zu organisieren und technische Unterstützung über große Entfernung in Anspruch zu nehmen.

1.3.5 Stadtüberwachung



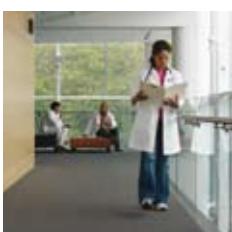
Netzwerk-Video ist eines der hilfreichsten Werkzeuge zur Verbrechensbekämpfung und für den Schutz der Bevölkerung. Es kann zur Erkennung und zur Vorbeugung eingesetzt werden. Die Verwendung von Drahtlos-Netzwerken ermöglicht eine effektive stadtweite Verteilung von Netzwerk-Videokameras. Die Fernüberwachungsfunktionen von Netzwerk-Video ermöglichen es der Polizei, auf live übertragene Bilder von kriminellen Handlungen schnell zu reagieren.

1.3.6 Behörden und öffentliche Gebäude



Netzwerk-Videoprodukte werden zum Schutz von öffentlichen Gebäuden aller Art wie z. B. Museen, Ämtern, Bibliotheken und Justizvollzugsanstalten eingesetzt. Kameras an Ein- und Ausgängen von Gebäuden können rund um die Uhr aufzeichnen, wer das Gebäude betritt und verlässt. Sie tragen dazu bei, Vandalismus zu verhindern und die Sicherheit des Personals zu erhöhen. Mit intelligenten Video-funktionen, wie dem Zählen von Personen, kann Netzwerk-Video statistische Daten liefern, z. B. die Anzahl von Besuchern eines Gebäudes.

1.3.7 Gesundheitswesen



Netzwerk-Video bietet kosteneffektive, hochwertige Patientenüberwachungs- und Videoüberwachungslösungen, die die Sicherheit von Mitarbeitern, Patienten und Besuchern sowie die Objektsicherheit erhöhen. Autorisiertes Sicherheitspersonal des Krankenhauses kann beispielsweise Live-Videobilder von unterschiedlichen Standorten anzeigen, Ereignisse erkennen und Fernunterstützung leisten.

1.3.8 Banken und Finanzwesen



Netzwerk-Video kommt in Sicherheitsbereichen von Bankfilialen, in Hauptgeschäftsstellen sowie an Geldautomaten zum Einsatz. Banken nutzen Überwachungssysteme bereits seit langem, und obwohl die meisten Installationen immer noch analog sind, kommen zunehmend auch Netzwerk-Videosysteme zum Einsatz. Dies trifft insbesondere auf Banken zu, die Wert auf eine hohe Bildqualität und die einfache Identifizierung von Personen in einem Überwachungsvideo legen.

Die Netzwerk-Videotechnologie hat sich bewährt, und in der Videoüberwachungsbranche ist ein schneller Wechsel von analogen Systemen zur IP-basierten Videoüberwachung zu beobachten. Fallstudien finden Sie unter www.axis.com/success_stories.

Netzwerk-Kameras

Es gibt eine große Bandbreite an Netzwerk-Kameras, um verschiedensten Anforderungen gerecht zu werden. In diesem Kapitel wird beschrieben, was eine Netzwerk-Kamera ist und welche Kameratypen es gibt. Es werden auch Kameras mit Tag-/Nacht-Funktion und Megapixeltechnologie beschrieben. Am Ende des Kapitels finden Sie Richtlinien für die Kameraauswahl. *Weitere Informationen zu Kameraelementen finden Sie in Kapitel 3.*

2.1 Was ist eine Netzwerk-Kamera?

Eine Netzwerk-Kamera, häufig auch als IP-Kamera bezeichnet, besteht aus einer Kamera und einem Computer, die zu einer intelligenten und kompakten Einheit zusammengefasst sind. Die Hauptkomponenten einer Netzwerk-Kamera umfassen ein Objektiv, einen Bildsensor, einen oder mehrere Prozessoren und einen Speicher. Die Prozessoren werden für die Bildverarbeitung, Komprimierung, Videoanalyse und Netzwerkfunktionen verwendet. Der Speicher wird zur Speicherung der Firmware der Netzwerk-Kamera (dem Betriebssystem) und für die lokale Aufzeichnung von Videosequenzen verwendet.

Wie ein Computer verfügt die Netzwerk-Kamera über eine eigene IP-Adresse, ist direkt mit dem Netzwerk verbunden und kann überall platziert werden, wo eine Netzwerkverbindung verfügbar ist. Eine Netzwerk-Kamera ist ein vollständig autarkes System, was eigenständig Videos über das Netzwerk übertragen kann. Dies unterscheidet sie von einer Webcam, die nur funktioniert, wenn sie über den USB- oder IEEE-1394-Anschluss an einen Computer angeschlossen ist, auf dem zudem entsprechende Software installiert sein muss. Eine Netzwerk-Kamera bietet Webserver-, FTP- und E-Mail-Funktionen und viele IP-Netzwerk- und Sicherheitsprotokolle.

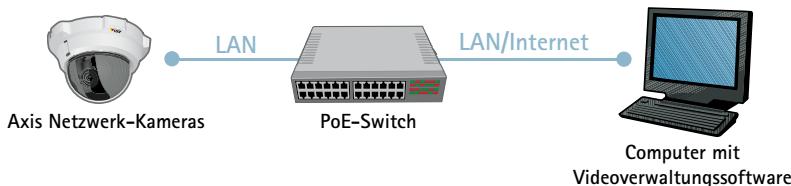


Abbildung 2.1a Eine Netzwerk-Kamera ist direkt mit dem Netzwerk verbunden.

Eine Netzwerk-Kamera kann so konfiguriert werden, dass sie Videodaten über ein IP-Netzwerk zur Live-Anzeige und/oder Aufzeichnung sendet. Letztere kann kontinuierlich, zu festgelegten Zeiten, ereignisbasiert oder auf Anforderung autorisierter Benutzer erfolgen. Erfasste Bilder können unter Verwendung verschiedener Netzwerkprotokolle als Motion JPEG-, MPEG-4- oder H.264-Datenströme gesendet oder als einzelne JPEG-Bilder per FTP, E-Mail oder HTTP (Hyper-text Transfer Protocol) hochgeladen werden. *Weitere Informationen zu Videokomprimierungsformaten und Netzwerkprotokollen finden Sie in Kapitel 7 und 9.*

Neben dem Aufnehmen von Videobildern sind Axis Netzwerk-Kameras mit Ereignisverwaltungs- und intelligenten Videofunktionen wie Videobewegungserkennung, Audioerkennung, aktivem Manipulationsalarm und automatischer Nachführung ausgestattet. Die meisten Netzwerk-Kameras bieten außerdem digitale Ein- und Ausgänge (E/A), an die externe Geräte wie Sensoren und Relais angeschlossen werden können. Darüber hinaus verfügen manche Modelle über Audiofunktionen und integrierte Unterstützung für Power over Ethernet (PoE). Axis Netzwerk-Kameras unterstützen auch erweiterte Sicherheits- und Netzwerkverwaltungsfunktionen.



Abbildung 2.1b Vorder- und Rückseite einer Netzwerk-Kamera.

2.2 Netzwerk-Kameratypen

Netzwerk-Kameras können danach eingeteilt werden, ob sie ausschließlich für den Einsatz in Innenräumen oder für den Innen- und Außenbereich ausgelegt sind. Netzwerk-Kameras für Außenbereiche verfügen häufig über eine automatische Blende, um die Lichtmenge, die den Bildsensor erreicht, zu beeinflussen. Eine Kamera für den Außenbereich benötigt außerdem ein externes Schutzgehäuse, es sei denn, die Kamera selbst sieht bereits ein Schutzgehäuse vor. Es sind auch Gehäuse für Innenraumkameras verfügbar, die vor Umgebungsbedingungen wie Staub und Luftfeuchtigkeit und vor Vandalismus oder Manipulationsversuchen geschützt werden müssen. Bei einigen Modellen ist der Vandalismus- und Manipulationsschutz bereits in die Kamera integriert, sodass kein zusätzliches Gehäuse erforderlich ist. *Weitere Informationen zum Kamerenschutz und zu Gehäusen finden Sie in Kapitel 4.*

Netzwerk-Kameras für den Innen- und Außenbereich können in fest ausgerichtete, fest ausgerichtete Dome-, PTZ- und PTZ-Dome Netzwerk-Kameras eingeteilt werden.

2.2.1 Fest ausgerichtete Netzwerk-Kameras

Eine fest ausgerichtete Netzwerk-Kamera, die mit einem Festbrennweitenobjektiv oder Varifokus-objektiv (Normal/Tele/Weitwinkel) ausgestattet sein kann, ist eine Kamera, die bei der Installation auf das zu überwachende Objekt ausgerichtet wird und Bilder mit einem bestimmten Sichtfeld liefert. Eine fest ausgerichtete Kamera entspricht dem herkömmlichen Kameratyp, bei dem die Kamera und die Richtung, in die sie zeigt, deutlich sichtbar sind. Diese Art von Kamera bietet sich vor allem in Umgebungen an, in denen die Sichtbarkeit der Kamera von Vorteil ist. Bei einer fest ausgerichteten Kamera kann in der Regel das Objektiv ausgetauscht werden. Fest ausgerichtete Kameras können, je nach Ausführung, im Innen- oder Außenbereichen installiert werden.



Abbildung 2.2a Fest ausgerichtete Netzwerk-Kameras einschließlich drahtloser und Megapixel-Versionen.

2.2.2 Fest ausgerichtete Dome-Netzwerk-Kameras (Fixed Dome)

Eine fest ausgerichtete Dome-Netzwerk-Kamera, auch als Mini-Dome bezeichnet, besteht im Wesentlichen aus einer unbeweglichen Kamera, die fest in einem kleinen Kuppelgehäuse installiert ist. Sie kann in einer beliebigen Richtung ausgerichtet werden. Ihr größter Vorteil liegt in ihrem unauffälligen, unaufdringlichen Design. Zudem ist die Ausrichtung der Kamera nur schwer zu erkennen. Darüber hinaus ist die Kamera vor Manipulationsversuchen geschützt. Allerdings sind fest ausgerichtete Dome-Kameras meist nicht mit Wechselobjektiven ausgestattet, und selbst wenn mehrere Objektive zur Auswahl stehen, sind die Wechselmöglichkeiten durch den Platz im Kuppelgehäuse eingeschränkt. Daher werden diese Kameratypen meistens mit einem Varifokusobjektiv bestückt, damit das Sichtfeld der Kamera angepasst werden kann. Fest ausgerichtete Dome-Kameras von Axis sind mit unterschiedlichen Arten von Gehäusen ausgestattet, z. B. vandalismussichere und/oder IP66-konforme Gehäuse für Außeninstallationen. Es sind keine externen Gehäuse erforderlich. Eine solche Kamera wird normalerweise an der Wand oder an der Decke montiert.



Abbildung 2.2b Fest ausgerichtete Dome-Netzwerk-Kameras. Von links nach rechts: AXIS 209FD und AXIS 216FD (auch in vandalismussicheren und Megapixel-Versionen erhältlich), AXIS P3301 und AXIS 225FD.

2.2.3 PTZ-Kameras und PTZ-Dome-Kameras

Eine PTZ-Kamera oder eine PTZ-Dome-Kamera lässt sich manuell oder automatisch schwenken und neigen und kann einen Bereich oder ein Objekt vergrößert oder verkleinert darstellen. Alle PTZ-Befehle werden über dasselbe Netzwerkkabel wie die Videodaten gesendet. Im Gegensatz zu einer analogen PTZ-Kamera müssen keine RS-485-Kabel verlegt werden. Eine PTZ-Kamera bzw. PTZ-Dome-Kamera kann unter anderem folgende Funktionen umfassen:

- > **Elektronischer Bildstabilisator (Electronic Image Stabilization, kurz EIS).** Bei Außeninstallationen sind PTZ-Dome-Kameras mit Zoomfaktoren über 20x empfindlich gegenüber Erschütterungen und Bewegungen, die durch Verkehrslasten oder Wind verursacht werden. Mithilfe von EIS können die durch Erschütterungen erzeugten Effekte reduziert werden, wo durch die Videoaufnahmen von größerem Nutzen sind. Darüber hinaus reduziert EIS aber auch die Dateigröße des komprimierten Bildes und spart dadurch wertvollen Speicherplatz.
- > **Privacy masking.** Das Privacy Masking, mit dem bestimmte Bereiche einer Szene ausgeblendet bzw. maskiert und somit nicht angezeigt und aufgezeichnet werden können, steht in verschiedenen Netzwerk-Videoproducten zur Verfügung. In einer PTZ- oder PTZ-Dome-Kamera kann der Privacy-Masking-Bereich auch dann beibehalten werden, wenn sich das Sichtfeld der Kamera ändert, da der maskierte Bereich mit dem Koordinatensystem verschoben wird.



Abbildung 2.2c Bei integrierter Privacy-Masking-Funktion (graues Rechteck im Bild) ermöglicht die Kamera das Ausblenden von Bereichen, die nicht überwacht werden sollen.

- > **Voreingestellte Positionen.** Viele PTZ- und PTZ-Dome-Kameras ermöglichen das Programmieren einer gewissen Anzahl an voreingestellten Positionen, in der Regel zwischen 20 und 100. Sobald diese voreingestellten Positionen in der Kamera festgelegt wurden, kann der Bediener über die Auswahl dieser Positionen schnell von einer Position zur nächsten wechseln.
- > **E-flip.** Wenn eine PTZ-Dome-Kamera z. B. an der Decke eines Einzelhandelsgeschäfts befestigt ist und eine Person verfolgt, die direkt unterhalb der Kamera vorbeiläuft, würden beim Weiterverfolgen der Person die Bilder ohne die E-Flip-Funktion auf dem Kopf stehend angezeigt werden. E-Flip dreht Bilder in diesen Fällen elektronisch um 180 Grad. Dieser Vorgang erfolgt automatisch und wird vom Bediener nicht bemerkt.
- > **Auto-flip.** PTZ-Kameras können im Gegensatz zu PTZ-Dome-Kameras normalerweise keinen vollständigen Schwenkvorgang von 360 Grad ausführen, da eine mechanische Sperre eine kontinuierliche kreisförmige Bewegung verhindert. Dank der Auto-Flip-Funktion ist bei einer PTZ-Netzwerk-Kamera jedoch ein sofortiges Umwenden des Kamerakopfes um 180 Grad und damit das Schwenken über den Nullpunkt hinaus möglich. Daher kann die Kamera Personen oder Objekte unabhängig von der Bewegungsrichtung weiterverfolgen.
- > **Automatische Nachführung.** Die automatische Nachführung ist eine intelligente Videofunktion, die eine Person oder ein Fahrzeug in Bewegung automatisch erkennt und diese bzw. dieses innerhalb des Abdeckungsbereichs der Kamera verfolgt. Die automatische Nachführung ist vor allem in Situationen der unbemannten Videoüberwachung von Vorteil, in denen die gelegentliche Anwesenheit von Personen oder Fahrzeugen besonderer Aufmerksamkeit bedarf. Mit dieser Funktion werden die Kosten des Überwachungssystems deutlich reduziert, da weniger Kameras für die Abdeckung einer Szene erforderlich sind. Zudem erhöht sie die Effektivität der Lösung, da sie es der PTZ- oder PTZ-Dome-Kamera ermöglicht, Bereiche einer Szene mit Aktivität aufzuzeichnen.

Zwar haben PTZ-Kameras und PTZ-Dome-Kameras ähnliche Funktionen, dennoch gibt es Unterschiede zwischen ihnen:

- > PTZ-Netzwerk-Kameras verfügen aufgrund einer mechanischen Sperre nicht über die Möglichkeit vollständiger 360-Grad-Schwenks. Dies bedeutet, dass die Kamera keine Personen verfolgen kann, die einmal rund um die Kamera herum laufen. Ausnahmen hiervon bilden PTZ-Kameras, die mit der Auto-Flip-Funktion ausgestattet sind, z. B. die AXIS 215 PTZ-Netzwerk-Kamera.
- > PTZ-Netzwerk-Kameras sind nicht für den kontinuierlichen automatischen Betrieb oder so genannte „Rundgangüberwachungen“ konzipiert, bei denen die Kamera automatisch von einer voreingestellten Position zur nächsten wechselt.

Weitere Informationen zu PTZ-Netzwerk-Kameras, die in mechanischen und nicht-mechanischen Ausführungen erhältlich sind, sowie zu PTZ-Dome-Netzwerk-Kameras finden Sie in den nächsten Abschnitten.

Mechanische PTZ-Netzwerk-Kameras

Mechanische PTZ-Kameras werden überwiegend in Innenbereichen und Umgebungen eingesetzt, bei denen ein Bediener verfügbar ist. Der optische Zoom einer PTZ-Kamera liegt in der Regel zwischen 10x und 26x. Eine PTZ-Kamera kann an der Decke oder an der Wand montiert werden.



Abbildung 2.2d PTZ-Netzwerk-Kameras. Von links nach rechts: AXIS 212 PTZ-V (nicht-mechanisch), AXIS 213 PTZ, AXIS 214 PTZ und AXIS 215 PTZ.

Nicht-mechanische PTZ-Netzwerk-Kameras

Eine nicht-mechanische PTZ-Netzwerk-Kamera, wie beispielsweise die AXIS 212 PTZ und ihre vandalismusgeschützte Version (AXIS 212 PTZ-V), bietet Schwenk-, Neige- und Zoom-Funktionen ohne bewegliche Teile, sodass es zu keiner mechanischen Verschleiß kommt. Dank eines Weitwinkelobjektivs bietet sie ein großes Sichtfeld und kann zur Überwachung eines größeren Bereiches eingesetzt werden.

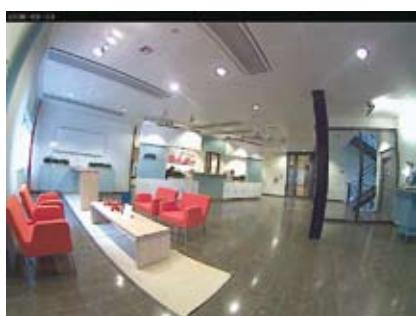


Abbildung 2.2e Bilder von einer nicht-mechanischen PTZ-Netzwerk-Kamera. Links ein 140-Grad-Übersichtsbild in VGA-Auflösung, rechts eine mit 3x-Zoom gemachte Aufnahme.

Eine nicht-mechanische PTZ-Kamera verwendet einen Megapixel-Bildsensor und ermöglicht es einem Bediener, einen beliebigen Bereich einer Szene zu vergrößern, ohne dass die Bildauflösung dadurch beeinträchtigt wird. Dies wird durch die Anzeige eines Übersichtsbilds in VGA-Auflösung (640 x 480 Pixel) erzielt, obwohl die Kamera das Bild in einer viel höheren Auflösung erfasst. Wenn die Kamera die Anweisung erhält, einen Bereich des Übersichtsbilds vergrößert darzustellen, verwendet sie die ursprüngliche Megapixel-Auflösung, um das Bild im Verhältnis 1:1 in VGA-Auflösung anzuzeigen. Die Nahaufnahme bietet dementsprechend gut sichtbare Details ohne Verlust der Schärfe. Bei einem normalen digitalen Zoom verlieren vergrößerte Bilder oftmals an Details

und Schärfe. Eine nicht-mechanische PTZ-Kamera eignet sich hervorragend für unauffällige, an der Wand montierte Installationen.

PTZ-Dome-Netzwerk-Kameras

PTZ-Dome-Netzwerk-Kameras können einen größeren Bereich abdecken, da sie eine größere Flexibilität beim Schwenken, Neigen und Zoomen bieten. Sie ermöglichen kontinuierliche Schwenks um 360 Grad und eine Neigung von 180 Grad. PTZ-Dome-Kameras eignen sich aufgrund ihres Designs, der Befestigungsart (insbesondere an Hängedecken) und des schwer erkennbaren Sichtwinkels der Kamera (Kuppelgehäuse kann klar oder getönt sein) für unauffällige Installationen. Eine PTZ-Dome-Netzwerk-Kamera zeichnet sich auch durch mechanische Robustheit beim kontinuierlichen Betrieb im Rundgangüberwachungsmodus aus, bei dem die Kamera automatisch in festgelegter oder zufälliger Reihenfolge von einer voreingestellten Position zur nächsten wechselt. Es können in der Regel bis zu 20 „Rundgänge“ eingerichtet und zu verschiedenen Tageszeiten aktiviert werden. Im Rundgangüberwachungsmodus kann eine PTZ-Dome-Netzwerk-Kamera einen Bereich abdecken, für den normalerweise mehrere fest ausgerichtete Kameras erforderlich wären. Allerdings kann sie jeweils nur einen Zielbereich überwachen, sodass die anderen Positionen im entsprechenden Zeitabschnitt unbeaufsichtigt bleiben. Der optische Zoom einer PTZ-Dome-Kamera liegt in der Regel zwischen 10x und 35x. Eine PTZ-Dome-Kamera wird häufig in Situationen eingesetzt, bei denen ein Bediener verfügbar ist. Diese Art von Kamera wird in Innenräumen gewöhnlich an der Decke befestigt und in Außenbereichen an einem Mast oder an einer Wand.



Abbildung 2.2f PTZ-Dome-Netzwerk-Kameras. Von links nach rechts: AXIS 231D+, AXIS 232D+, AXIS 233D.

2.3 Tag- und Nacht Netzwerk-Kameras

Alle Arten von Netzwerk-Kameras – fest ausgerichtete, fest ausgerichtete Dome-, PTZ- und PTZ-Dome-Kameras – können mit Tag-/Nacht-Funktionalität ausgestattet werden. Eine Tag-/Nacht-Kamera ist für den Einsatz in Außen- oder Innenbereichen mit schwacher Beleuchtung vorgesehen.

Eine farbfähige Tag-/Nacht-Netzwerk-Kamera liefert am Tag Farbbilder. Wenn die Helligkeit unter einen bestimmten Wert fällt, kann die Kamera automatisch in den Nachtsmodus wechseln, um mithilfe von Nah-Infrarot-Licht hochwertige Schwarzweißbilder zu erzeugen.

Nah-Infrarot-Licht, das zwischen 780 und etwa 1000 Nanometern (nm) liegt, kann vom menschlichen Auge nicht oder nur bedingt wahrgenommen werden. Die meisten Bildsensoren der Kameras können es jedoch erkennen und nutzen. Während des Tages verwendet eine Tag-/Nacht-Kamera einen Infrarot-Sperrfilter. Damit wird das IR-Licht herausgefiltert, sodass es die Farben der Bilder so wiedergibt, wie das menschliche Auge sie sieht. Der Infrarot-Sperrfilter ist auf einer Elektromechanik aufgebaut, so dass dieser vor den Bildsensor eingeschwenkt oder weggeschwenkt werden kann. Ist die Kamera im Nacht-Modus (Schwarzweiß), wird der Infrarot-Sperrfilter weggeschwenkt, sodass die Lichtempfindlichkeit der Kamera 0,001 Lux oder weniger beträgt und das IR-Licht zum Ausleuchten des zu überwachenden Bereiches genutzt werden kann.

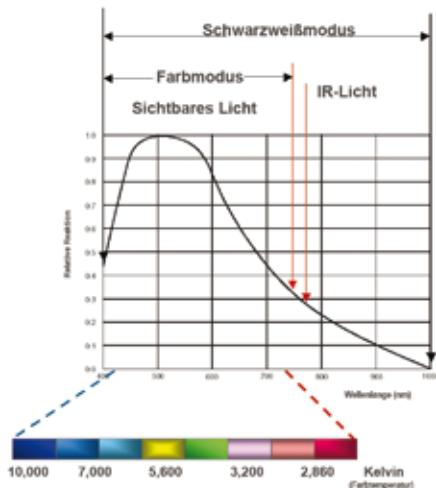


Abbildung 2.3a Das Diagramm zeigt, wie ein Bildsensor auf sichtbares und Nah-Infrarot-Licht reagiert. Nah-IR-Licht liegt im Bereich von 780 nm bis 1000 nm.

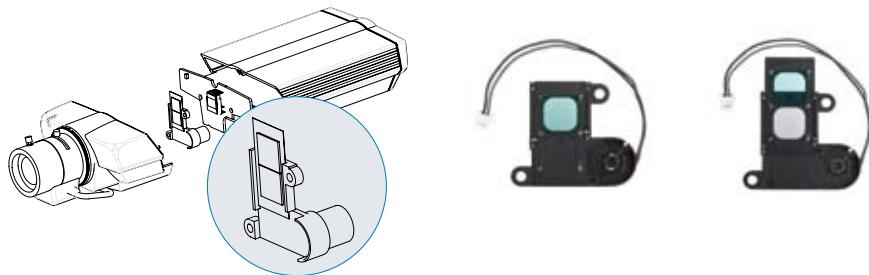


Abbildung 2.3b Links: Infrarot-Sperrfilter in Tag-/Nacht-Netzwerk-Kamera; Mitte: Position des Infrarot-Sperrfilters am Tag; Rechts: Position des Infrarot-Sperrfilters in der Nacht.

Tag-/Nacht-Kameras eignen sich für Umgebungen, in denen die Verwendung von Kunstlicht eingeschränkt ist. Dies betrifft u. a. Videoüberwachungen bei schwachem Licht, verdeckte oder unauffällige Überwachungen, z. B. die Überwachung des Verkehrs, bei der helles Licht die Fahrer nachts stören würde. Es kann auch ein IR-Strahler, der Nah-Infrarot-Licht erzeugt, in Verbindung mit einer Tag-/Nacht-Kamera verwendet werden, um deren Fähigkeit zu verbessern, auch bei schwachem Licht oder nachts qualitativ hochwertige Videobilder zu erzeugen. Weitere Informationen zu IR-Strahlern finden Sie auf der Axis-Website unter www.axis.com/products/cam_irillum



Abbildung 2.3c Links: Bild ohne IR-Strahler; Rechts: Bild mit IR-Strahler.

2.4 Megapixel-Netzwerk-Kameras

Die Megapixeltechnologie, die in fest ausgerichteten und Dome-Kameras verfügbar ist, umfasst einen Megapixel-Bildsensor, der Bilder mit mindestens einer Million Pixel liefert. Diese Auflösung ist mindestens zweimal so hoch wie die Auflösung analoger Kameras.

Eine fest ausgerichtete Megapixel-Netzwerk-Kameras können auf unterschiedlicher Weise genutzt werden: Sie kann mehr Details in einem Bild mit höherer Auflösung anzeigen, was für die Identifizierung von Personen und Objekten hilfreich ist. Sie kann aber auch verwendet werden, um einen größeren Bereich einer Szene abzudecken, wenn dieselbe Pixeldichte wie bei einer Nicht-Megapixel-Kamera verwendet wird.

Betrachtet man die Lichtempfindlichkeit, so fällt dieses heute bei den Megapixel-Kameras etwas geringer aus, als bei den herkömmlichen Kameras ohne Megapixelauflösung. Die technologische Entwicklung schreitet jedoch stetig voran, sodass die Lichtempfindlichkeit der Bildsensoren mit Megapixelauflösung immer besser wird. Die von einer Megapixel-Kamera erzeugten hochauflösenden Videoströme erfordern eine höhere Netzwerkantrittsrate und mehr Speicherplatz für Aufzeichnungen, als die Videoströme von herkömmlichen Kameras. Der höhere Bandbreiten und Speicherbedarf kann jedoch heute durch die Verwendung der effizienten H.264-Videokomprimierung weitestgehend kompensiert werden. Weitere Informationen zu H.264 finden Sie in Kapitel 7.

2.5 Richtlinien für die Auswahl einer Netzwerk-Kamera

Angesichts des großen Angebots an Netzwerk-Kameras sind Richtlinien für die Auswahl einer Netzwerk-Kamera hilfreich.

- > **Definieren des Überwachungsziels: Überblick oder Detail.** Überblick-Bilder bieten einen allgemeinen Überblick über eine Szene oder die Bewegungen von Personen. Detailbilder sind wichtig für die Identifizierung von Personen oder Objekten (z. B. Gesichter, Nummernschilder oder Kassenterminale). Das Überwachungsziel bestimmt das Sichtfeld und die Position sowie die Art der erforderlichen Kamera bzw. des erforderlichen Objektivs. *Weitere Informationen zu Objektiven finden Sie in Kapitel 3.*
- > **Abgedeckter Bereich.** 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 nah beieinander befinden oder weit voneinander entfernt sind. Der zu überwachende Bereich bestimmt den Kameratyp und die Anzahl der erforderlichen Kameras.
 - *Mit oder ohne Megapixeltechnologie.* Wenn beispielsweise zwei relativ kleine Bereiche zu überwachen sind, die nah beieinander liegen, kann unter Umständen anstelle von zwei Nicht-Megapixel-Kameras eine Megapixel-Kamera mit einem Weitwinkelobjektiv verwendet werden.
 - *Fest ausgerichtete oder PTZ.* (Im Folgenden bezieht sich der Begriff „fest ausgerichtete Kamera“ auch auf fest ausgerichtete Dome-Kameras und der Begriff „PTZ-Kameras“ auch auf PTZ-Dome-Kameras.) Ein Bereich kann von mehreren fest ausgerichteten Kameras oder einigen wenigen PTZ-Kameras abgedeckt werden. Eine PTZ-Kamera mit einem großen optischen Zoom kann Bilder mit vielen Details liefern und einen großen Bereich überwachen. Eine PTZ-Kamera überwacht jedoch, in Abhängigkeit der jeweiligen Ausrichtung, immer nur einen Teil ihres Abdeckungsbereichs, während eine fest ausgerichtete Kamera durchgängig den gesamten Abdeckungsbereich erfasst. Um die Funktionen einer PTZ-Kamera voll nutzen zu können, ist ein Bediener erforderlich oder es muss ein automatischer „Rundgang“ eingerichtet werden.
- > **Innen- und Außenbereiche.**
 - *Lichtempfindlichkeit und Beleuchtungsanforderungen.* In Außenbereichen ist die Verwendung von Tag-/Nacht-Kameras zu empfehlen. Dabei sollte überlegt werden, welche Lichtempfindlichkeit die erforderliche Kamera haben muss und ob eine zusätzliche Beleuchtung oder speielles Licht, z. B. ein IR-Strahler, erforderlich ist. Beachten Sie, dass Lux-Angaben von Netzwerk-Kameras verschiedener Hersteller nicht miteinander vergleichbar sind, da es keinen einheitlichen Industriestandard für die Messung der Lichtempfindlichkeit gibt.

- **Gehäuse.** Wenn eine Kamera im Außenbereich oder in einer Umgebung angebracht werden soll, in der sie vor Staub, Feuchtigkeit oder Vandalismus geschützt werden muss, ist ein Gehäuse erforderlich, falls die Kamera selbst die geforderten Schutzeigenschaften nicht erfüllt. *Weitere Informationen zu Gehäusen finden Sie in Kapitel 4.*
- > **Offene oder verdeckte Überwachung.** Dies hilft bei der Auswahl von Kameras, die zusätzlich zu Gehäuse und Halterung die Möglichkeit einer auffälligen oder unauffälligen Installation bieten.

Weitere wichtige Merkmale, die eine Kamera evtl. aufweisen muss, sind folgende:

- > **Bildqualität.** Die Bildqualität ist einer der wichtigsten Aspekte einer Kamera, sie ist jedoch schwer festzulegen und zu messen. Am besten lässt sich die Bildqualität ermitteln, indem verschiedene Kameras installiert und die Videobilder miteinander verglichen werden. Wenn die Erfassung von sich bewegenden Objekten Priorität hat, ist es wichtig, dass die Netzwerk-Kamera die Technologie der progressiven Bildabtastung verwendet. *Weitere Informationen zur progressiven Abtastung finden Sie in Kapitel 3.*
- > **Auflösung.** In Anwendungsbereichen, in denen detaillierte Bilder benötigt werden, sind unter Umständen Megapixel-Kameras die beste Lösung. *Weitere Informationen zur Megapixel-Auflösung finden Sie in Kapitel 6.*
- > **Komprimierung.** In Netzwerk-Videoprodukten von Axis werden je nach Model die Video komprimierungsstandards Motion JPEG und MPEG-4 oder H.264 unterstützt. H.264 ist der neueste Standard. Er bietet die besten Einsparmöglichkeiten bei Bandbreite und Speicherplatz. *Weitere Informationen zur Komprimierung finden Sie in Kapitel 7.*
- > **Audio.** Wenn Audiofunktionen benötigt werden, stellt sich die Frage, ob Ein- oder Zweiwege- Audio erforderlich ist. Axis Netzwerk-Kameras mit Audio-Unterstützung enthalten ein integriertes Mikrofon und/oder einen Eingang für ein externes Mikrofon und einen Lautsprecher oder einen Ausgang für externe Lautsprecher. *Weitere Informationen zu Audio finden Sie in Kapitel 8.*
- > **Ereignisverwaltung und intelligentes Video.** Ereignisverwaltungsfunktionen werden meist über ein Videoverwaltungsprogramm konfiguriert und von den Eingangs-/Ausgangsports und den intelligenten Videofunktionen einer Netzwerk-Kamera oder eines Video-Encoders unterstützt. Das Aufzeichnen auf der Basis von Ereignisauslösern von Eingangsports und intelligenten Videofunktionen eines Netzwerk-Videoprodukts ermöglicht Einsparungen bei der Bandbreite und dem Speicherplatz. Darüber hinaus können Bediener mehr Kameras betreuen, ohne das die Gefahr besteht, dass der Bediener durch unnötige Bildinformationen abgelenkt wird. Diese Optimierung wird ermöglicht, indem nicht alle Kameras gleichzeitig eine Livebildüberwachung durchführen, sondern nur dann, wenn ein Ereignis statt findet oder ein Alarm ausgelöst wurde. *Weitere Informationen zur Ereignisverwaltung finden Sie in Kapitel 11.*

- > **Netzwerkfunktionen.** Hierzu können Faktoren zählen wie PoE, HTTPS-Verschlüsselung zum Verschlüsseln von Videoströmen, IP-Adressfilter, die festgelegten IP-Adressen den Zugriff gewähren oder verweigern, IEEE 802.1X für die Authentifizierung über ein Netzwerk, IPv6 und WLAN-Interface. *Weitere Informationen zur Netzwerk- und Sicherheitstechnologie finden Sie in Kapitel 9.*
- > **Offene Schnittstellen und Anwendungssoftware.** Ein Netzwerk-Videoproduct mit einer offenen Schnittstelle bietet bessere Integrationsmöglichkeiten mit anderen Systemen. Außerdem ist es wichtig, dass das Produkt von einer guten Auswahl an Anwendungssoftware und Verwaltungssoftware unterstützt wird, um eine einfache Installation und Aktualisierung zu ermöglichen. Für Axis-Produkte stehen sowohl firmeneigene Videoverwaltungssoftware als auch eine Vielzahl an Videoverwaltungsprogrammen von über 600 Anwendungsentwicklungspartnern (ADP Partner) zur Verfügung. *Weitere Informationen zu Videoverwaltungs-systemen finden Sie in Kapitel 11.*

Ein weiterer wichtiger Faktor ist, neben dem Produkt selbst, der Hersteller des Netzwerk-Video-produkts. Da die Anforderungen stets wachsen und sich verändern, sollte der Hersteller als Langzeit-Partner betrachtet werden können. Das heißt, es ist wichtig, einen Hersteller auszuwählen, der eine umfassende Produktlinie an Netzwerk-Videoprodukten und Zubehör anbietet und in der Lage ist, aktuelle und zukünftige Anforderungen zu erfüllen. Der Hersteller sollte zudem Innovation, Support, Aktualisierungen und einen Produktpfad für langfristige Implementierungen bieten können.

Kameraelemente

Es gibt eine Reihe von Kameraelementen, die Einfluss auf die Bildqualität und das Sichtfeld haben. Daher ist es für die Auswahl einer Netzwerk-Kamera wichtig, diese Elemente zu kennen und zu verstehen. Dazu zählen die Lichtempfindlichkeit der Kamera, die Art des Objektivs, die Art des Bildsensors, die Bildabtastmethode sowie die Bilddatenverarbeitungsfunktionen. Diese Elemente werden in diesem Kapitel eingehend erläutert. Außerdem werden am Ende des Kapitels einige Richtlinien zur Installation aufgeführt.

3.1 Lichtempfindlichkeit

Die Lichtempfindlichkeit einer Netzwerk-Kamera wird häufig in Lux angegeben, was dem Helligkeitsniveau entspricht, bei dem eine Kamera noch ein akzeptables Bild liefern kann. Je niedriger die Lux-Angabe, desto höher ist die Lichtempfindlichkeit der Kamera. Normalerweise werden mindestens 200 Lux benötigt, um ein Objekt so zu beleuchten, dass eine gute Bildqualität erzielt werden kann. Generell lässt sich sagen: Je mehr Licht auf ein Objekt fällt, desto besser ist das Bild. Bei wenig Licht ist die Schärfeeinstellung schwieriger und das Bild kann verrauscht sein und/oder ist zu dunkel. Für gute Aufnahmen bei schwachem Licht oder bei Dunkelheit kann der Einsatz einer Tag-/Nacht-Kamera sinnvoll sein, die mit Nah-Infrarot-Licht arbeiten kann. *Weitere Informationen zu Tag-/Nacht-Kameras finden Sie in Kapitel 2.*

Unterschiedliche Lichtverhältnisse spiegeln sich in unterschiedlicher Helligkeit wider. Natürliche Orte weisen häufig sehr komplexe Lichtverhältnisse auf. Sie enthalten sowohl Schatten als auch Spitzlichter, d. h. die verschiedenen Bereiche eines Orts haben unterschiedliche Lux-Werte. Es ist daher wichtig zu berücksichtigen, dass ein Lux-Wert nicht die Lichtverhältnisse der gesamten Szene angibt.

Illuminance	Lighting condition
100,000 lux	Strong sunlight
10,000 lux	Full daylight
500 lux	Office light
100 lux	Poorly lit room

Tabelle 3.1a Beispiele für verschiedene Helligkeitsgrade.

Viele Hersteller geben an, wie viel Helligkeit mindestens erforderlich ist, damit die Netzwerk-Kamera ein akzeptables Bild erzeugt. Während diese Spezifikationen hilfreich sind, um Lichtempfindlichkeitsvergleiche bei Kameras desselben Herstellers vorzunehmen, sind sie für den Vergleich von Kameras verschiedener Hersteller nicht geeignet. Dies liegt daran, dass jeder Hersteller seine eigene Methode anwendet und unterschiedliche Kriterien eines akzeptablen Bildes hat. Um die Leistung zweier Kameras bei schwachem Licht korrekt zu beurteilen, sollten die Kameras nebeneinander betrieben werden und ihre Aufnahmen bei schwachem Licht miteinander verglichen werden. Hierbei sollten die Darstellung von bewegten als auch unbewegten Objekten verglichen werden.

3.2 Objektivelemente

Das Objektiv einer Netzwerk-Kamera ist für verschiedene Aspekte verantwortlich. Dazu gehören folgende:

- > Definieren des Sichtfelds, d. h. definieren, welcher Teil einer Szene mit welcher Detailgenauigkeit erfasst werden soll.
- > Steuern der Lichtmenge, die durch das Objektiv auf den Bildsensor fällt, damit ein Bild korrekt belichtet wird.
- > Scharfstellen durch Verschieben der Linsen im Objektiv oder Ändern des Abstands zwischen Objektiv und Bildsensor.

3.2.1 Sichtfeld

Ein Faktor, der bei der Auswahl einer Kamera zu berücksichtigen ist, ist das erforderliche Sichtfeld, d. h. der Abdeckungsbereich der Kamera und die gewünschte Detailgenauigkeit. Das Sichtfeld wird durch die Brennweite des Objektivs und die Größe des Bildsensors festgelegt. Beide Angaben sind in den technischen Daten der Netzwerk-Kamera aufgeführt.

Die Brennweite eines Objektivs ist der Abstand zwischen der Eingangslinse (optischer Mittelpunkt im Objektiv) und der Stelle, an der alle Lichtstrahlen an einem Punkt zusammenlaufen (Brennpunkt). Je länger die Brennweite, desto enger ist das Sichtfeld.

Welche Brennweite für das gewünschte Sichtfeld benötigt wird, lässt sich am schnellsten mithilfe einer Objektivrechenscheibe oder eines Online-Objektivrechners (www.axis.com/tools) ermitteln. Beide Rechner sind bei Axis erhältlich. Die Größe des Bildsensors einer Netzwerk-Kamera beträgt in der Regel 1/4", 1/3", 1/2" oder 2/3" und muss bei der Berechnung ebenfalls berücksichtigt werden. (Der Nachteil bei der Verwendung eines Objektivrechners besteht darin, dass er mögliche geometrische Verzeichnungen eines Objektivs nicht berücksichtigt und es zu kleinen Abweichungen beim Ergebnis kommen kann.)

Das Sichtfeld kann in drei Typen eingeteilt werden:

- > **Normal view:** Entspricht dem Sichtfeld des menschlichen Auges.
- > **Tele:** Ein kleineres Sichtfeld, das mehr Details liefert, als das menschliche Auge wahrnehmen kann. Ein Teleobjektiv wird verwendet, wenn das zu überwachende Objekt klein oder weit von der Kamera entfernt ist. Ein Teleobjektiv ist normalerweise weniger lichtstark als ein Normal objektiv.
- > **Weitwinkel:** Ein größeres Sichtfeld mit weniger Details als bei einem normalen Sichtfeld. Ein Weitwinkelobjektiv bietet eine gute Tiefenschärfe und eine akzeptable Leistung bei schwachem Licht. Weitwinkelobjektive erzeugen gelegentlich geometrische Verzeichnungen, wie z. B. den „Fischaugen“-Effekt.



Abbildung 3.2a Verschiedene Sichtfelder: Weitwinkel (links), Normal (Mitte), Tele (rechts).



Abbildung 3.2b Netzwerk-Kamera-Objektive mit unterschiedlichen Brennweiten: Weitwinkel (links), Normal (Mitte), Tele (rechts).

Es gibt drei Arten von Objektiven:

- > **Objektiv mit Festbrennweite:** Ein solches Objektiv hat eine Brennweite, die nicht veränderbar ist, d. h., es bietet nur ein Sichtfeld (normal, Tele oder Weitwinkel). Eine gängige feste Brennweite für Netzwerk-Kamera-Objektive ist 4 mm.
- > **Varifokusobjektivs:** Dieser Objektivtyp bietet einen Brennweitenbereich und damit auch verschiedene Sichtfelder. Das Sichtfeld kann manuell angepasst werden. Bei jeder Änderung des Sichtfelds muss das Objektiv manuell neu fokussiert werden. Varifokusobjektive für Netzwerk-Kameras bieten oftmals Brennweiten im Bereich von 3 mm bis 8 mm.

- > **Zoom-Objektiv:** Zoom-Objektive ähneln den Varifokusobjektiven, da bei ihnen unterschiedliche Sichtfelder eingestellt werden können. Bei Zoom-Objektiven muss das Objektiv jedoch nicht neu fokussiert werden, wenn das Sichtfeld geändert wird. Der Fokus kann in einem Brennweitenbereich von beispielsweise 6 mm bis 48 mm beibehalten werden. Objektiveinstellungen können manuell oder motorbetrieben per Fernsteuerung erfolgen. Wenn für ein Objektiv ein Zoomfaktor (z. B. 3x) angegeben ist, bezeichnet dies das Verhältnis zwischen der kürzesten und längsten Brennweite des Objektivs..

3.2.2 Objektiv und Bildsensor aufeinander abstimmen

Wenn eine Netzwerk-Kamera ein Wechselobjektiv hat, muss darauf geachtet werden, dass für die Kamera geeignete Objektive verwendet werden. Das Objektiv muss vom Durchmesser her mindestens so groß sein wie die Diagonale des Bildsensors, kann aber auch größer sein. Ein Objektiv für einen 1/2"-Bildsensor eignet sich für 1/2"-, 1/3"- und 1/4"-Bildsensoren, aber nicht für 2/3"-Bildsensoren.

Wenn ein Objektiv zu klein ist, weisen die erzeugten Bilder schwarze Ecken auf (*siehe linke Darstellung in Abbildung 3.2c unten*). Wenn ein Objektiv für einen größeren Bildsensor als den der Kamera konzipiert ist, ist das Sichtfeld kleiner als das theoretisch mit dem Objektiv erzielbare Sichtfeld, da ein Teil der Informationen außerhalb des Bildsensors „verloren geht“r (*siehe rechte Darstellung in Abbildung 3.2c*). Hierdurch wird ein Tele-Effekt erzeugt, da alles vergrößert erscheint.

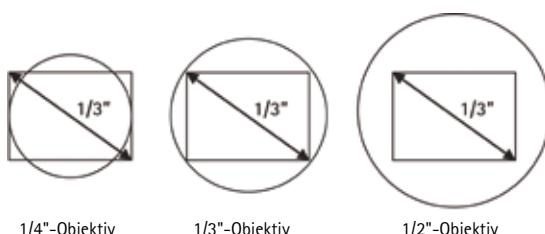


Abbildung 3.2c Beispiele für verschiedene Objektive in Kombination mit einem 1/3"-Bildsensor.

Beim Wechseln eines Objektivs an einer Megapixelkamera ist gegenüber Kameras mit VGA-Bildsensoren ein höherwertiges Objektiv erforderlich, dass ein entsprechendes Auflösvermögen bietet. Nur wenn das Objektivauf lösevermögen den Anforderungen entspricht, können die Funktionen der Megapixelkameras vollständig genutzt werden.

3.2.3 Standards bei den Objektivanschlüssen

Beim Wechseln eines Objektivs ist es wichtig, die Art des Objektivanschlusses der Netzwerk-Kamera zu kennen. Es gibt zwei Hauptstandards für Objektivanschlüsse von Netzwerk-Kameras: CS-Anschluss und C-Anschluss. Beide haben ein 1"-Gewinde und lassen sich auf den ersten Blick nicht voneinander unterscheiden. Der Unterschied besteht in dem jeweiligen Abstand des Objektivs zum Bildsensor, wenn das Objektiv an der Kamera montiert ist:

- > **CS-Anschluss.** Der Abstand zwischen Bildsensor und Objektiv muss 12,5 mm betragen.
- > **C-Anschluss.** Der Abstand zwischen Bildsensor und Objektiv muss 17,526 mm betragen.

Es ist möglich, ein Objektiv mit C-Anschluss an eine Kamera mit CS-Anschluss zu montieren. Hierzu muss ein 5-mm-Abstandsring (C/CS-Adaptring) verwendet werden. Wenn eine Kamera nicht fokussiert werden kann, wird sehr wahrscheinlich ein falsches Objektiv verwendet.

3.2.4 Öffnungsverhältnis und Belichtung

Bei schwachem Licht, vor allem in Innenräumen, ist die Lichtstärke des Objektivs einer Netzwerk-Kamera ein wichtiger Faktor. Diese wird vom so genannten Öffnungsverhältnis des Objektivs bestimmt. Dieses gibt an, wie viel Licht ein Objektiv passieren kann. Das Öffnungsverhältnis ist das Verhältnis zwischen der Brennweite und dem Durchmesser der Eintrittspupille bzw. der Blendenöffnung, d. h. Öffnungsverhältnis = Brennweite/Blendenöffnung.

Je kleiner das Öffnungsverhältnis ist (entweder kurze Brennweite relativ zur Blendenöffnung oder große Blendenöffnung relativ zur Brennweite), desto höher ist die Lichtstärke des Objektivs, d. h., es gelangt mehr Licht durch das Objektiv zum Bildsensor. Bei schwachem Licht wird mit einem kleineren Öffnungsverhältnis in der Regel eine bessere Bildqualität erzielt. (Es gibt jedoch Sensoren, die aufgrund ihres Designs bei schwachem Licht nicht in der Lage sind, von einem kleineren Öffnungsverhältnis zu profitieren.) Ein größeres Öffnungsverhältnis erhöht indes die Schärfentiefe, die in Abschnitt 3.2.6 erläutert wird. Ein Objektiv mit einem kleineren Öffnungsverhältnis ist normalerweise teurer als ein Objektiv mit einem größeren Öffnungsverhältnis.

Das Öffnungsverhältnis wird meist im Format „f/x“ angegeben. Der Schrägstrich steht für die Division. Die Angabe „f/4“ bedeutet, dass der Blendendurchmesser dem Quotienten aus Brennweite und 4 entspricht. Wenn also die Kamera ein 8-mm-Objektiv hat, beträgt der Durchmesser der Blendenöffnung, durch die das Licht einfallen kann, nur 2 mm.

Während Objektive mit Automatikblende (DC-Blende) über mehrere Öffnungsverhältnisse verfügen, wird oftmals nur die maximale Lichtstärke (kleinstes Öffnungsverhältnis) angegeben. Die Lichtstärke oder das Öffnungsverhältnis und die Belichtungszeit sind die zwei Hauptfaktoren, die beeinflussen, wie viel Licht ein Bildsensor empfängt. Ein dritter Faktor, ist die Verstärkung, sie dient dazu, das Bild heller zu machen. Mit zunehmender Verstärkung wird jedoch auch das Rauschen („Körnigkeit“) eines Bildes verstärkt. Deshalb ist es in Regel vorteilhaft, die Belichtungszeit oder die Blende an die Lichtsituation anzupassen.

Bei den meisten Axis-Kameras können Grenzwerte für die Belichtungszeit und die Verstärkung festgelegt werden. Je länger die Belichtungszeit ist, desto mehr Licht empfängt ein Bildsensor. In hellen Umgebungen ist eine kürzere Belichtungszeit erforderlich, während schwach ausgeleuchtete Szenen eine längere Belichtungszeit erfordern. Es ist wichtig zu wissen, dass bei längeren Belichtungszeiten auch die Bewegungsunschärfe zunimmt, während die Vergrößerung der Blendenöffnung den Nachteil einer verringerten Tiefenschärfe hat. Dies wird in Abschnitt 3.2.6 näher erläutert.

Eine kürzere Belichtungszeit wird empfohlen, wenn schnell bewegte Objekte aufgenommen werden sollen oder wenn eine hohe Bildrate erforderlich ist. Eine längere Belichtungszeit verbessert die Bildqualität bei schwachem Licht, verstärkt jedoch auch die Bewegungsunschärfe und senkt die Gesamtbildrate, da zur Belichtung jedes Einzelbilds mehr Zeit benötigt wird. Bei einigen Netzwerk-Kameras bewirkt eine automatische Belichtungseinstellung, dass die Bildrate je nach verfügbarem Licht erhöht oder reduziert wird. Faktoren wie Kunstlicht, Bildrate oder Bildqualität spielen nur bei mangelnder Helligkeit eine Rolle.



Abbildung 3.2d Eine Kamerabenutzeroberfläche mit Optionen zum Einstellen der Belichtung bei schwachem Licht sowie anderen Einstellungen.

3.2.5 Manuelle oder automatische Blende

In Innenräumen, in denen von einer konstanten Beleuchtung ausgegangen wird, kann ein Objektiv mit manueller Blende verwendet werden. Diese Art von Objektiv verfügt entweder über einen Ring zum Einstellen der Blende oder die Blende ist fest auf ein bestimmtes Öffnungsverhältnis eingestellt. Die Innenraum-Netzwerk-Kameras von Axis verwenden feste Öffnungsverhältnisse.

Ein Objektiv mit Automatikblende wird für Außenbereiche und für Situationen empfohlen, in denen sich die Beleuchtung ständig verändert. Die Blende wird von der Kamera gesteuert. Sie sorgt dafür, dass immer eine optimale Lichtmenge auf den Bildsensor auftrifft, wenn bei der Netzwerk-Kamera keine Einstellungen für die Belichtung und die Verstärkung verfügbar sind. Die Blende kann auch verwendet werden, um die Tiefenschärfe (wie weiter unten erläutert) zu beeinflussen und schärfere Bilder zu erzielen. Die meisten Objektive mit Automatikblenden werden vom Prozessor der Kamera über Gleichstrom (DC, Direct Current) gesteuert und heißen daher auch „DC-Blenden“-Objektive. Alle Axis-Kameras für den Außenbereich (fest ausgerichtete, fest ausgerichtete Dome-, PTZ- oder PTZ-Dome-Kameras) verwenden DC-Blenden- oder Automatikblenden-Objektive.

3.2.6 Tiefenschärfe

Ein Kriterium, das bei der Videoüberwachung möglicherweise eine wichtige Rolle spielt, ist die Tiefenschärfe. Diese bezeichnet den Bereich vor und hinter dem Schärfepunkt, in dem die Objekte

scharf dargestellt werden. Die Tiefenschärfe kann beispielsweise bei der Überwachung von Parkplätzen wichtig sein, bei der Nummernschilder in 20, 30 und 50 Metern Entfernung noch lesbar sein müssen.

Die Tiefenschärfe wird von vier Faktoren beeinflusst: Brennweite, Blendenöffnung, Abstand zwischen Kamera und Objekt und der Pixelgröße auf dem Bildsensor. Eine große Brennweite, eine große Blendenöffnung oder ein kurzer Abstand zwischen Kamera und Objekt haben eine geringere Tiefenschärfe zur Folge. Des Weiteren gilt, dass bei den Megapixelkameras Bildsensoren mit kleineren Pixeln verwendet werden, welche ebenfalls eine geringere Tiefenschärfe zur Folge haben.

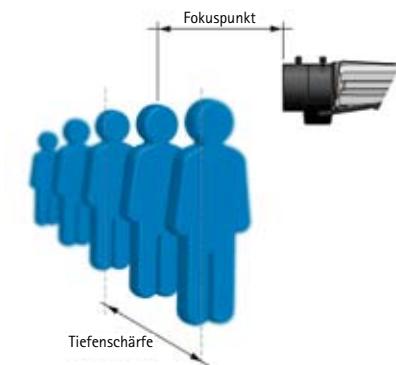


Abbildung 3.2e Tiefenschärfe: Stellen Sie sich mehrere Personen vor, die in einer Reihe hintereinander stehen. Wenn der Schärfepunkt auf der Mitte der Reihe liegt und es möglich ist, die Gesichter der Personen zu erkennen, die mehr als 15 Meter vom Mittelpunkt entfernt sind, ist die Tiefenschärfe gut.

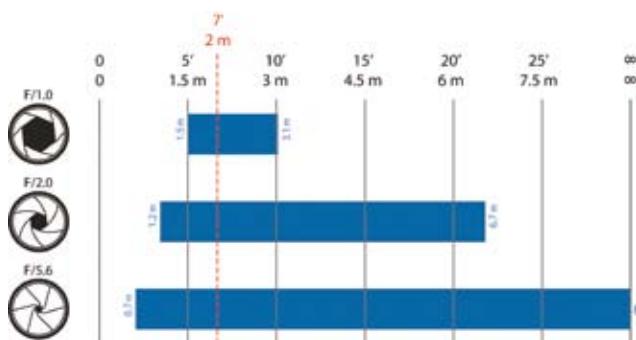


Abbildung 3.2f Blendenöffnung und Tiefenschärfe. Das Diagramm oben ist ein Beispiel für die Tiefenschärfe bei verschiedenen Öffnungsverhältnissen und einem Abstand von 2 Metern. Bei einem großen Öffnungsverhältnis (kleine Blendenöffnung) werden Objekte über eine größere Entfernung scharf abgebildet. (Je nach Pixelgröße können sehr kleine Blendenöffnungen zu Beugungsunschärfe führen.)

3.3 Bildsensoren

Das Licht, das durch ein Objektiv einfällt, wird auf dem Bildsensor der Kamera fokussiert. Ein Bildsensor besteht aus vielen Photosites, wobei jede Photosite einem Bildelement, besser unter dem Namen „Pixel“ bekannt, auf dem Bildsensor entspricht. Jedes Pixel auf einem Bildsensor registriert die Menge an Licht, der es ausgesetzt ist, und konvertiert diese in eine entsprechende Anzahl an Elektronen. Je heller das Licht ist, desto mehr Elektronen werden erzeugt. In Kameras kommen zwei Technologien für den Bildsensor zum Einsatz:

- > **CCD** (Charge-Coupled Device, ladungsgekoppeltes Bauteil)
- > **CMOS** (Complementary Metal-Oxide Semiconductor, komplementärer Metalloxid-Halbleiter)

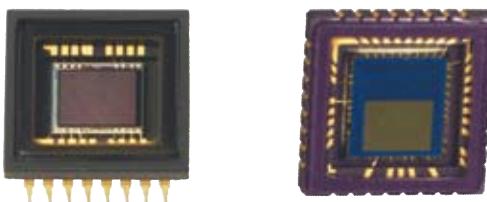


Abbildung 3.3a *Bildsensoren: CCD (links), CMOS (rechts).*

CCD- und CMOS-Sensoren werden oftmals als Konkurrenten angesehen, haben aber beide ihre individuellen Stärken und Schwächen, wodurch sie sich für unterschiedliche Anwendungsbereiche eignen. CCD-Sensoren werden mit einer Technologie produziert, die eigens für die Kameraindustrie entwickelt wurde. Frühere CMOS-Sensoren basierten auf Standardtechnologie, die bereits in großem Umfang z. B. in Speicherchips von PCs verwendet wurde. Moderne CMOS-Sensoren basieren auf einer spezielleren Technologie, und die Qualität der Sensoren nimmt stetig zu.

3.3.1 CCD-Technologie

CCD-Sensoren werden seit mehr als 30 Jahren in Kameras verwendet. Sie haben zahlreiche Vorteile. Im Allgemeinen lässt sich sagen, dass sie immer noch eine etwas bessere Lichtempfindlichkeit bieten und etwas weniger Rauschen verursachen als CMOS-Sensoren. Eine höhere Lichtempfindlichkeit führt bei schwachem Licht zu besseren Bildern. CCD-Sensoren sind jedoch teurer und Kameras mit CCD-Sensoren sind aufwändiger zu konstruieren. Ein CCD-Sensor kann zudem das Hundertfache an Strom verbrauchen wie ein äquivalenter CMOS-Sensor.

3.3.2 CMOS-Technologie

Durch die stetige Weiterentwicklungen rücken CMOS-Sensoren in puncto Bildqualität näher an ihre CCD-Konkurrenten heran. CMOS-Sensoren senken die Gesamtkosten von Kameras, da sie bereits die gesamte Logik enthalten, um die digitalisierte Bildinformation zu liefern. Im Vergleich zu CCDs bieten CMOS-Sensoren mehr Integrationsmöglichkeiten und mehr Funktionen. CMOS-Sensoren lassen sich schneller auslesen (was bei Bildern mit hoher Auflösung von Vorteil ist), haben einen geringeren Stromverbrauch auf Chip-Ebene und ermöglichen eine kleinere Systemgröße. Megapixel-CMOS-Sensoren sind weiter verbreitet und nicht so teuer wie Megapixel-CCD-Sensoren.

3.3.3 Megapixel-Sensoren

Aus Kostengründen haben viele Megapixel-Bildsensoren (Sensoren mit einer Million oder mehr Pixel) in Megapixel-Kameras dieselbe Größe oder sind nur geringfügig größer als VGA-Bildsensoren, die eine Auflösung von 640×480 (307.200) Pixel bieten. Dies bedeutet, dass die Größe der einzelnen Pixel auf einem Megapixel-Bildsensor kleiner ist als auf einem VGA-Bildsensor. Beispielsweise haben die einzelnen Pixel auf einem $1/3"$ -Bildsensor mit 2 Megapixel eine Größe von $3 \mu\text{m}$ (Mikrometer/Mikron). Im Vergleich dazu beträgt die Größe eines Pixels auf einem $1/3"$ -VGA-Bildsensor $7,5 \mu\text{m}$. Während die Megapixel-Kamera zwar eine höhere Auflösung und mehr Details bietet, ist sie jedoch weniger lichtempfindlich als eine VGA-Kamera, da die Pixelgröße kleiner ist und das von einem Objekt reflektierte Licht auf mehr Pixel verteilt wird.

3.4 Bildabtasttechniken

Das Zeilensprungverfahren und die progressive Abtastung sind die zwei heutzutage verfügbaren Techniken zum Auslesen und Anzeigen von Bildinformationen, die von Bildsensoren genutzt werden. Das Zeilensprungverfahren wird vor allem in CCD-Sensoren verwendet. Die progressive Abtastung wird in CCD- und CMOS-Sensoren verwendet. In Netzwerk-Kameras können beide Abtasttechniken zum Einsatz kommen. (Analoge Kameras können hingegen nur das Zeilensprungverfahren zum Übertragen von Bildern über ein Koaxialkabel und zum Anzeigen der Bilder auf einem analogen Monitor verwenden.)

3.4.1 Zeilensprungverfahren

Wenn ein Zeilensprungbild von einem CCD-Sensor erzeugt wird, werden zwei Felder mit Zeilen generiert: ein Feld zeigt die ungeraden Zeilen, das andere die geraden Zeilen an. Um das ungerade Feld zu erzeugen, werden jedoch die Informationen aus den ungeraden und den geraden Zeilen auf einem CCD-Sensor kombiniert. Dies gilt auch für das gerade Feld, bei dem die Informationen der geraden und ungeraden Zeilen miteinander kombiniert werden, um ein Bild auf jeder zweiten Zeile zu erzeugen.

Beim Übertragen eines Zeilensprungbilds wird immer nur die Hälfte der Zeilen (gerade oder ungerade) eines Bildes gesendet, wodurch auch die Bandbreitennutzung halbiert wird. Der Monitor, z. B. ein herkömmlicher Fernseher, muss ebenfalls mit dieser Zeilensprungtechnik arbeiten. Zuerst werden die ungeraden und dann die geraden Zeilen eines Bildes angezeigt und dann immer im Wechsel mit einer Bildrate von 25 (PAL) oder 30 (NTSC) Bildern pro Sekunde aktualisiert, sodass das menschliche Auge sie als vollständige Bilder wahrnimmt. Alle analogen Videoformate und einige moderne HDTV-Formate verwenden das Zeilensprungverfahren. Obwohl beim Zeilensprungverfahren Artefakte oder Verzerrungen aufgrund „fehlender“ Daten erzeugt werden, sind diese auf einem zeilensprungfähigen Monitor kaum erkennbar.

Wenn jedoch ein mit dem Zeilensprungverfahren erzeugtes Video auf einem Monitor angezeigt wird, der mit progressiver Abtastung arbeitet (z. B. ein Computermonitor), bei der die Zeilen eines Bildes in fortlaufender Reihenfolge gelesen werden, sind Artefakte sichtbar. Diese Artefakte, die als „Zackenbildung“ wahrgenommen werden, entstehen aufgrund der kurzen Verzögerung

zwischen den Aktualisierungen der geraden und ungeraden Zeilen, da nur die Hälfte der Zeilen eine Bewegung im Bild darstellt, während die andere Hälfte der Zeilen darauf wartet, aktualisiert zu werden. Die Artefakte sind insbesondere dann sichtbar, wenn das Video angehalten wird, um ein Standbild zu analysieren.

3.4.2 Progressive Abtastung

Bei einem Bildsensor, der mit progressiver Abtastung arbeitet, werden Werte für jedes Pixel auf dem Sensor ermittelt und die Bilddatenzeilen werden nacheinander gelesen, sodass ein vollständiges Einzelbild entsteht. Das heißt, die erfassten Bilder werden nicht wie beim Zeilensprungverfahren in Halbbilder aufgeteilt. Bei der progressiven Abtastung wird ein vollständiges Einzelbild über das Netzwerk gesendet, und bei der Anzeige auf einem entsprechenden Computermonitor werden die einzelnen Zeilen des Bildes in der richtigen Reihenfolge auf dem Bildschirm ausgegeben. Sich bewegende Objekte können daher besser mit der progressiven Abtasttechnik auf Computermonitoren dargestellt werden. Bei einer Videoüberwachungsanwendung kann es wichtig sein, Details eines sich bewegenden Objekts zu erkennen (z. B. eine flüchtende Person). Die meisten Netzwerk-Kameras von Axis verwenden die progressive Abtastung.

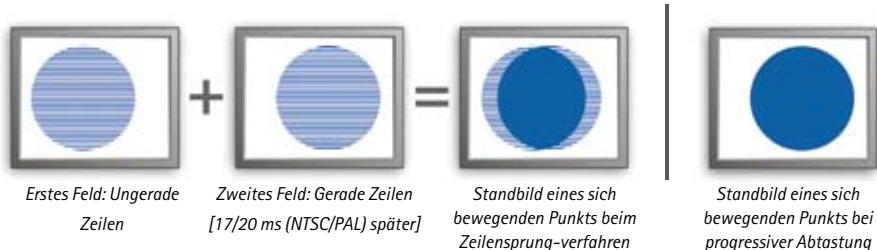


Abbildung 3.4a Links ein per Zeilensprungverfahren erzeugtes Bild auf einem Computermonitor mit progressiver Abtastung. Rechts ein per progressiver Abtastung erzeugtes Bild auf einem Computermonitor.



Abbildung 3.4b At left, a full-sized JPEG image (704x576 pixels) from an analog camera using interlaced scanning. At right, a full-sized JPEG image (640x480 pixels) from an Axis network camera using progressive scan technology. Both cameras used the same type of lens and the speed of the car was the same at 20 km/h (15 mph). The background is clear in both images. However, the driver is clearly visible only in the image using progressive scan technology.

3.5 Bildverarbeitung

Es gibt drei Funktionen zur Verbesserung der Bildqualität, die bei Netzwerk-Kameras eingesetzt werden können: Gegenlichtkompensation, Belichtungszonen und ein großer Dynamikbereich.

3.5.1 Gegenlichtkompensation

Die automatische Belichtungssteuerung einer Kamera versucht, die Helligkeit eines Bildes so einzufangen, wie das menschliche Auge sie wahrnimmt. Dabei kann sie jedoch leicht getäuscht werden. Starkes Gegenlicht kann bewirken, dass Objekte im Vordergrund dunkel dargestellt werden. Netzwerk-Kameras mit Gegenlichtkompensation versuchen, einzelne Bereiche einer Szene, die sehr hell sind, bei der Belichtungssteuerung zu ignorieren. So werden die Objekte im Vordergrund sichtbar, wobei die hellen Bereiche jedoch überbelichtet werden. Solche Lichtverhältnisse können auch durch Erhöhen des Dynamikbereiches der Kamera gehandhabt werden. Nähere Informationen hierzu finden Sie in Abschnitt 3.5.3.

3.5.2 Belichtungszonen

Neben der Bewältigung einzelner Bereiche mit starker Helligkeit muss die automatische Belichtungsfunktion einer Netzwerk-Kamera auch entscheiden, welcher Bereich einer Szene den Belichtungswert bestimmt. So enthält beispielsweise der Vordergrund (meist der untere Teil eines Bildes) möglicherweise wichtigere Informationen als der Hintergrund, z. B. der Himmel (in der Regel der obere Teil des Bildes). Die weniger wichtigen Bereiche einer Szene sollten nicht die Gesamtbelichtung bestimmen. Bei der Vielzahl der Axis Netzwerk-Kameras kann der Benutzer mithilfe von Belichtungszonen den Bereich einer Szene – Mitte, links, rechts, oben, unten – auswählen, der korrekt belichtet werden soll. Des Weiteren gibt es Kameramodelle, bei denen die Belichtungszonen frei definiert werden können.

3.5.3 Großer Dynamikbereich

Einige Axis Netzwerk-Kameras bieten einen großen Dynamikbereich (Wide Dynamic Range, kurz WDR), um unterschiedlichste Lichtverhältnisse in einer Szene besser handhaben zu können. In einer Szene mit extrem hellen und dunklen Bereichen oder in Gegenlichtsituationen, in denen z. B. eine Person vor einem hellen Fenster steht, erzeugt eine normale Kamera ein Bild, auf dem die Objekte in den dunklen Bereichen kaum zu erkennen sind. Ein großer Dynamikbereich löst dieses Problem durch die Anwendung bestimmter Techniken, z. B. die Verwendung unterschiedlicher Belichtungen für unterschiedliche Objektbereiche in einer Szene, sodass die Objekte in den hellen und dunklen Bereichen sichtbar werden.

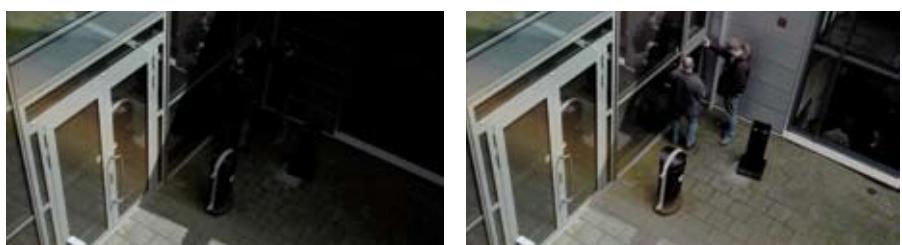


Abbildung 3.5a Links ein Bild ohne Verwendung eines großen Dynamikbereichs. Rechts ein Bild, bei dem ein großer Dynamikbereich angewendet wurde.

3.6 Installation einer Netzwerk-Kamera

Nach dem Kauf einer Netzwerk-Kamera kommt der Art der Installation große Bedeutung zu. Im Folgenden werden einige Empfehlungen gegeben, wie anhand der Kamerapositionierung und der Umgebungsbedingungen eine hochwertige Videoüberwachung erzielt werden kann.

- > **Überwachungsziel.** Wenn das Ziel darin besteht, sich einen Überblick über einen Bereich zu verschaffen, um die Bewegung von Personen und Objekten verfolgen zu können, ist darauf zu achten, dass eine für diese Aufgabe geeignete Kamera an einer passenden Position angebracht wird. Wenn das Ziel darin besteht, Personen oder Objekte identifizieren zu können, muss die Kamera so positioniert und fokussiert werden, dass sie die für die Identifikation erforderlichen Details erfasst. Polizeibehörden vor Ort können vermutlich ebenfalls Richtlinien für eine optimale Positionierung einer Kamera geben.
- > **Viel Licht verwenden oder bei Bedarf zusätzliche Lichtquellen einsetzen.** Es ist normalerweise einfach und kostengünstig, starke Lampen in Innen- und Außenbereichen zu installieren, um die erforderlichen Lichtverhältnisse für die Aufnahme guter Bilder herzustellen.
- > **Direktes Sonnenlicht vermeiden.** Sonnenlicht kann die Kamera „blenden“ und die Leistung des Bildsensors herabsetzen. Daher sollte die Kamera nach Möglichkeit so positioniert werden, dass sich die Sonne hinter der Kamera befindet.
- > **Gegenlicht vermeiden.** Typischerweise tritt das Problem bei der Aufnahme von Objekten vor einem Fenster auf. Um das Problem zu umgehen, bringen Sie die Kamera an einer anderen Stelle an oder verwenden Sie Vorhänge bzw. schließen Sie die Jalousien. Wenn die Kamera nicht an einer anderen Stelle angebracht werden kann, beleuchten Sie das Objekt von vorn. Kameras, die einen großen Dynamikbereich unterstützen, können Gegenlichtsituationen besser bewältigen.
- > **Den Dynamikbereich der Szene verringern.** Wenn in Außenbereichen zu viel Himmel von der Kamera erfasst wird, führt dies zu einem zu hohen Dynamikbereich. Wenn die Kamera keinen großen Dynamikbereich unterstützt, sollte sie hoch über dem Boden befestigt werden, bei Bedarf an einem Mast.
- > **Kameraeinstellungen anpassen.** Gelegentlich ist es notwendig, die Einstellungen für den Weißabgleich, die Helligkeit und die Schärfe anzupassen, um ein optimales Bild zu erhalten. Bei schwachem Licht muss der Benutzer zudem festlegen, ob die Bildrate oder die Bildqualität höhere Priorität hat.
- > **Rechtliche Hinweise.** Die Videoüberwachung kann gesetzlich eingeschränkt oder untersagt sein. Diesbezügliche Gesetze sind von Land zu Land verschieden. Es wird empfohlen, vor der Installation eines Videoüberwachungssystems die geltenden Gesetze zu prüfen. Es kann bei spielsweise erforderlich sein, die Videoüberwachung registrieren zu lassen oder eine Lizenz dafür anzufordern. Dies gilt für allem für öffentliche Bereiche. In der Regel sind Beschilderungen anzubringen, die auf das Vorhanden sein einer Videoüberwachung hinweisen. Die Videoaufzeichnungen müssen evtl. mit Datum- und Uhrzeitstempel versehen werden. Außerdem kann es Vorschriften bezüglich der Aufbewahrungsduer von Videodaten geben. Audioaufnahmen sind möglicherweise nicht zulässig.

Kameraschutz und Gehäuse

Überwachungskameras werden häufig in Umgebungen eingesetzt, die eine hohe Beanspruchung mit sich bringen. Sie müssen unter Umständen Regen, Hitze, Kälte, Staub, korrosiven Substanzen, Erschütterungen und Vandalismus standhalten. Hersteller von Kameras und Kamerazubehör bieten verschiedene Lösungen an, um diese Herausforderungen zu meistern. Hierzu gehören die Verwendung von separaten oder integrierten Schutzgehäusen, die für bestimmte Zwecke konzipiert sind, und/oder der Einsatz von intelligenten Algorithmen, die geänderte Betriebsbedingungen erkennen können und entsprechende Warnungen ausgeben. In den folgenden Abschnitten finden Sie Informationen zu folgenden Themen: Gehäuse, Positionieren von unbeweglichen Kameras in Gehäusen, Schutz vor schwierigen Umgebungsbedingungen, Schutz gegen Vandalismus und Manipulation sowie Befestigungsarten.

4.1 Allgemeine Hinweise zu Kameragehäusen

Wenn Sie Ihre Kamera in Umgebungen einsetzen, die den Betriebsbedingungen der Kamera nicht entsprechen, benötigen Sie ein Schutzgehäuse. Die Kameragehäuse sind in verschiedenen Größen und Ausführungen erhältlich. Es gibt Metall- und Kunststoffgehäuse. Man unterscheidet grundsätzlich zwischen zwei Arten von Gehäusen: Gehäuse für unbewegliche Kameras und Gehäuse für Dome-Kameras. Bei der Auswahl eines Gehäuses sollten Sie Folgendes in Betracht ziehen:

- > Öffnen von der Seite oder mittels Schiebeabdeckung (bei Gehäusen für unbewegliche Kameras)
- > Halterungen
- > Klare oder getönte Gehäusekuppel (bei Gehäusen für Dome-Kameras)
- > Verkabelung
- > Temperatur und andere Vorrichtungen (Bedarf an Heizung, Sonnenschutz, Lüfter und Scheibenwischer)
- > Stromversorgung (12 V, 24 V, 110 V, usw.)
- > Grad des Vandalismusschutz

In einigen Gehäusen sind zudem Peripheriegeräte eingebaut, z. B. Antennen für drahtlose Netzwerkanbindung. Bei der zur verwendeten Antennentechnik ist zu berücksichtigen, dass bei einem Metallgehäuse externe Antennen benötigt werden.

4.2 Durchsichtige Abdeckung

Die „Fenster“ bzw. durchsichtigen Abdeckungen von Gehäusen sind in der Regel aus hochwertigem Glas oder langlebigem Polycarbonatkunststoff gefertigt. Da die Fenster als optische Linsen fungieren, müssen sie von hoher Qualität sein, damit die Bildqualität nicht beeinträchtigt wird. Unebenheiten auf der glatten Oberfläche können sich negativ auf die Klarheit bzw. die Schärfe auswirken. Noch höhere Anforderungen werden an die Fenster von Gehäusen für PTZ-Kameras und PTZ-Dome-Kameras gestellt. Sie müssen nicht nur speziell geformt (kuppelförmig) sondern auch sehr klar sein, da Unebenheiten wie Schmutzpartikel bei Kameras mit hohen Vergrößerungsfaktoren vergrößert dargestellt werden. Wenn zudem die Fensterdicke uneinheitlich ist, wird im Zielbild eine Gerade möglicherweise als Kurve angezeigt. Qualitativ hochwertige Gehäuse dürfen die Bildqualität nur geringfügig beeinträchtigen, unabhängig davon, welche Zoom-Stärke verwendet wird und wie das Objektiv positioniert ist.

Es ist möglich, die Dicke des Gehäuses zum Schutz gegen starke Erschütterungen zu erhöhen. Dadurch wird jedoch auch das Risiko von Unebenheiten größer. Dickere Abdeckungen können außerdem unerwünschte Spiegelungen und Lichtbrechungen hervorrufen. Daher müssen sie höhere Anforderungen erfüllen, damit die Beeinträchtigung der Bildqualität minimiert wird. Es gibt eine Vielzahl von Dome-Abdeckungen und -Gehäusen in durchsichtiger und getönter Ausfertigung. Getönte Abdeckungen ermöglichen zwar eine verdeckte Montage, reduzieren aber – vergleichbar mit einer Sonnenbrille – die der Kamera zur Verfügung stehende Lichtmenge. Dies wirkt sich wiederum auf die Lichtempfindlichkeit der Kamera aus.

4.3 Unbewegliche Kameras in Gehäusen positionieren

Bei der Befestigung einer unbeweglichen Kamera in einem Gehäuse ist es wichtig, dass das Kameraobjektiv einen minimalen Abstand zu Fensterglas aufweist (ca. 1 bis 2 mm) und dass die Kamera im rechten Winkel zum Fensterglas montiert ist, um eine Blendwirkung zu verhindern. Andernfalls wird das Bild durch Spiegelungen aus der Kamera und dem Hintergrund beeinträchtigt. Des Weiteren sollten die LEDs an den Kameras abgeschaltet werden, da sich diese sonst ebenfalls Spiegeln könnten. Zur Verringerung von Spiegeleffekten sind spezielle Beschichtungen erhältlich, die auf dem Glas vor dem Objektiv aufgebracht werden können.

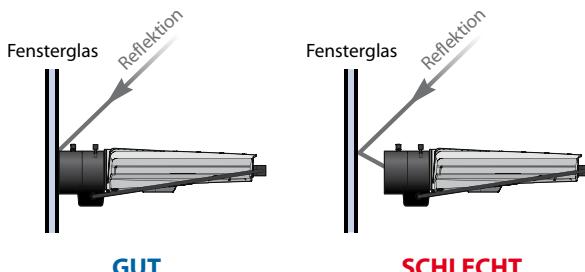


Abbildung 4.3a Wenn die Kamera hinter Fensterglas montiert wird, ist eine korrekte Positionierung wichtig, um Spiegeleffekte zu vermeiden.

4.4 Schutz vor schwierigen Umgebungsbedingungen

Die wichtigsten Umgebungsbedingungen, vor denen besonders im Außenbereich montierte Kameras geschützt werden müssen, sind Kälte, Hitze, Nässe und Staub. Gehäuse mit integrierten Heizelementen und Lüftern (Gebläse) eignen sich für den Einsatz in Umgebungen mit hohen und niedrigen Temperaturen. In Umgebungen mit hohen Temperaturen können Sie die Kameras in Gehäusen montieren, die eine aktive Kühlung mit separatem Wärmetauscher enthalten. Sicher verschlossene Gehäuse (meist nach IP66) bieten Schutz vor Nässe und Staub. Wenn Kameras Säuren ausgesetzt sind, z. B. in der Lebensmittelindustrie, werden Gehäuse aus Edelstahl benötigt. Zudem gibt es spezielle druckdichte, wasserdichte oder kugelsichere Gehäuse oder Gehäuse für den Einsatz in explosionsgefährdeten Umgebungen. Spezialgehäuse können auch aus ästhetischen Gesichtspunkten benötigt werden.

Andere Umgebungsbedingungen sind Wind und Verkehrslasten. Damit die Kameras (besonders, wenn sie an einem Mast angebracht sind) nur geringen Erschütterungen ausgesetzt sind, sollte das Gehäuse klein und fest montiert sein. Durch die Begriffe „Gehäuse für den Innenbereich“ und „Gehäuse für den Außenbereich“ wird in der Regel festgelegt, gegen welche Umgebungsbedingungen das Gehäuse schützt. Ein Gehäuse für den Innenbereich schützt normalerweise vor dem Eindringen von Staub und enthält kein Heizelement bzw. keinen Lüfter. Die Begriffe sind missverständlich, da der Standort (Innen- oder Außenbereich) nicht immer den Bedingungen am Installationsstandort entspricht. Eine Kamera, die in einem Kühlraum (Innenbereich) montiert wird, benötigt beispielsweise ein Gehäuse für den Außenbereich mit einer Heizung.

Welchen Schutzgrad die integrierten oder separaten Gehäuse bieten, wird meist durch die folgenden Klassifizierungen festgelegt: IP-Standards (Ingress Protection oder auch International Protection), die weltweit gelten, NEMA-Standards (National Electrical Manufacturers Association) für den Einsatz in den USA und IK-Standards für externe mechanische Belastungen, die europaweit gelten. Für Kameras, die in explosionsgefährdeten Umgebungen eingesetzt werden sollen, gelten andere Standards: IECEx, eine globale Zertifizierung und ATEX, eine Europäische Zertifizierung. Weitere Informationen zu IP-Standards finden Sie unter www.axis.com/products/cam_housing/ip66.htm

4.5 Schutz gegen Vandalismus und Manipulation

Bei Überwachungen sind die Kameras zuweilen dem Risiko böswilliger Gewalt ausgesetzt. Es gibt keine Kameras bzw. Gehäuse, bei denen in jeder Situation uneingeschränkter Schutz vor destruktivem Verhalten garantiert ist, dennoch können Sie den Vandalismusschutz durch Berücksichtigung der folgenden Aspekte erhöhen: Design von Kamera/Gehäuse, Montage, Aufstellungsort und Einsatz intelligenter Videoalarme.

4.5.1 Design von Kamera/Gehäuse

Gehäuse und Komponenten aus Metall bieten größeren Schutz vor Vandalismus als Kunststoffgehäuse. Ein weiterer zu berücksichtigender Faktor ist die Form des Gehäuses bzw. der Kamera. Die Gehäuse oder herkömmlichen unbeweglichen Kameras, die von der Wand oder Decke hervorragen, sind anfälliger für Angriffe (z. B. durch Schläge oder Tritte) als die unauffälligeren

Gehäuse für unbewegliche Dome- oder PTZ-Dome-Kameras. Durch die glatte, abgerundete Form ist es zudem schwieriger, das Sichtfeld der Kamera einzuschränken, etwa durch Verhängen mit einem 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 höher ist der Schutz gegen Vandalismus.



Abbildung 4.5a Beispiele für Gehäuse unbeweglicher Kameras. Nur die mittleren und rechten Gehäuse sind vandalismusgeschützt.



Abbildung 4.5b Beispiele für Gehäuse mit Vandalismusschutz für eine kleine oder kompakte fest ausgerichtete Netzwerk-Kamera (links), für eine fest ausgerichtete Dome-Netzwerk-Kamera (Mitte) und für eine PTZ-Kamera (rechts).

4.5.2 Montage

Ein weiterer wichtiger Faktor ist, wie Sie die Kameras und Gehäuse montieren. Eine herkömmliche fest ausgerichtete Netzwerk-Kamera bzw. eine PTZ-Dome-Kamera, die an der Deckenoberfläche montiert wird, ist anfälliger für Angriffe als eine fest ausgerichtete Dome- oder PTZ-Dome-Kamera, die bündig zur Decke oder Wand angebracht wird, d. h. nur der durchsichtige Teil der Kamera bzw. des Gehäuses ist sichtbar.



Abbildung 4.5c Beispiele bündig montierter Gehäuse unbeweglicher Netzwerk-Kameras.

Ein weiterer Faktor ist die Verkabelung der Kamera. Optimaler Schutz besteht, wenn das Kabel zur Kamera unter Putz verlegt ist, da dann die Kabel nicht sichtbar und somit nicht für Manipulationen anfällig sind. Wenn eine solche verdeckte Verlegung nicht möglich ist, sollte eine Kabelführung aus Metall verwendet werden, um die Kabel zu schützen.

4.5.3 Kamerapositionierung

Die Kamerapositionierung spielt ebenfalls eine wichtige Rolle bei der Reduzierung von Vandalismus. Wenn die Kamera an hohen Wänden oder an der Decke außer Handreichweite platziert ist, können viele spontane Angriffe vermieden werden. Der Nachteil dieser Positionierung liegt im Sichtwinkel, der jedoch durch die Auswahl eines anderen Objektivs und größerem Abstand zum Objekt teilweise ausgeglichen werden kann.

4.5.4 Intelligentes Video

Die aktive Manipulationsalarm-Funktion von Axis schützt Ihre Kameras gegen Vandalismus. Sie sendet einen Alarm an den Systembediener, wenn entdeckt wird, dass die Kamera neu ausgerichtet, verdeckt oder auf andere Weise manipuliert wurde. Der aktive Manipulationsalarm eignet sich besonders bei Installationen von mehreren hundert Kameras in anspruchsvollen Umgebungen, in denen es sehr schwierig ist, die ordnungsgemäße Funktion aller Kameras zu überwachen. Er ist auch sinnvoll, wenn keine Live-Anzeige erfolgt. Bei Kameramanipulationen erhalten dann die zuständigen Kamerabedienner eine Benachrichtigung.

4.6 Befestigungsarten

Kameras müssen an den verschiedensten Standorten angebracht werden. Daher wird eine Vielzahl von Befestigungsarten benötigt.

4.6.1 Deckenhalterungen

Deckenhalterungen werden überwiegend in Innenbereichen eingesetzt. Das Gehäuse kann wie folgt befestigt werden:

- > **Oberflächenmontage:** Das Gehäuse wird direkt an der Deckenoberfläche befestigt und ist somit vollständig sichtbar.
- > **Bündige Montage:** Das Gehäuse wird in der Decke angebracht, so dass nur Teile der Kamera und des Gehäuses sichtbar sind.
- > **Hängemontage:** Das Gehäuse hängt von der Decke wie ein Pendel.



Abbildung 4.6a Beispiel einer Oberflächenhalterung (links), einer bündigen Montage (Mitte) und einer Hängemontage (rechts).

4.6.2 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. Erweiterte Halterungen verfügen über eine Kabelverschraubung zum Schutz der Kabel. Wenn Sie ein Gehäuse an einer Ecke des Gebäudes anbringen möchten, benötigen Sie eine herkömmliche Wandhalterung und zusätzlich einen Eckadapter. Andere spezielle Halterungen ermöglichen eine Hängemontage. Bei dieser Befestigungsart können Sie eine unbewegliche Netzwerk-Kamera ähnlich wie ein PTZ-Dome-Gehäuse montieren.



Abbildung 4.6b Beispiel einer Wandhalterung mit Hängemontage-Kit für eine fest ausgerichtete Dome-Kamera.

4.6.3 Masten-Halterungen

Masten-Halterungen werden häufig bei PTZ-Kameras an Orten wie Parkhäusern eingesetzt. Bei dieser Befestigungsart wird gewöhnlich die Beeinträchtigung durch Wind berücksichtigt. Die Abmessungen von Mast und Halterung sollten so gewählt werden, dass die Kamera möglichst wenigen Erschütterungen ausgesetzt ist. Die Kabel befinden sich häufig im Mast und die Steckdosen müssen ordnungsgemäß versiegelt sein. Höherwertige PTZ-Dome-Kameras verfügen über eine integrierte elektronische Bildstabilisierung, die die Auswirkungen durch Wind und Erschütterungen minimiert.

4.6.4 Brüstungshalterungen

Brüstungshalterungen werden zur Befestigung von Kamera-Gehäusen auf Dächern sowie zum Erhöhen der Kamera eingesetzt, um einen besseren Sichtwinkel zu erzielen.



Abbildung 4.6c Beispiel einer Brüstungshalterung.

Axis stellt ein Online-Tool zur Verfügung, das Ihnen bei der Auswahl des geeigneten Gehäuses und dem dazugehörigen Montagezubehör hilft. *Informationen finden Sie unter www.axis.com/products/video/accessories/configurator/*

Video-Encoder

Video-Encoder, häufig auch Videoserver genannt, ermöglichen Ihnen, ein analoges CCTV-Videoüberwachungssystem in ein Netzwerk-Videosystem zu integrieren. Sie nehmen eine Schlüsselrolle ein, wenn viele analoge Kameras verwaltet werden müssen. In diesem Kapitel werden die Funktionen und Vorteile von Video-Encodern beschrieben. Es gibt einen Überblick über die Video-Encoder-Komponenten und die unterschiedlichen Typen. Darüber hinaus werden verschiedene Deinterlacing-Techniken erläutert.

5.1 Was ist ein Video-Encoder?

Ein Video-Encoder ermöglicht die Migration analoger CCTV-Systeme zu einem Netzwerk-Video-System. Benutzer können die Vorteile von Netzwerk-Video nutzen, ohne auf bereits vorhandene analoge Geräte wie z. B. analoge CCTV-Kameras und Koaxialkabel verzichten zu müssen.

Ein Video-Encoder wird mit einem Koaxialkabel an eine analoge Videokamera angeschlossen und wandelt analoge Videosignale in digitale Videoströme um, die anschließend über ein drahtgebundenes oder drahtloses Netzwerk (z. B. LAN, WLAN oder Internet) übertragen werden. Zur Anzeige und/oder Aufzeichnung der digitalen Videodaten können Sie Computerbildschirme und PCs anstelle von DVRs (Digital Video Recorder), VCRs (Video Cassette Recording) und analogen Monitoren einsetzen.

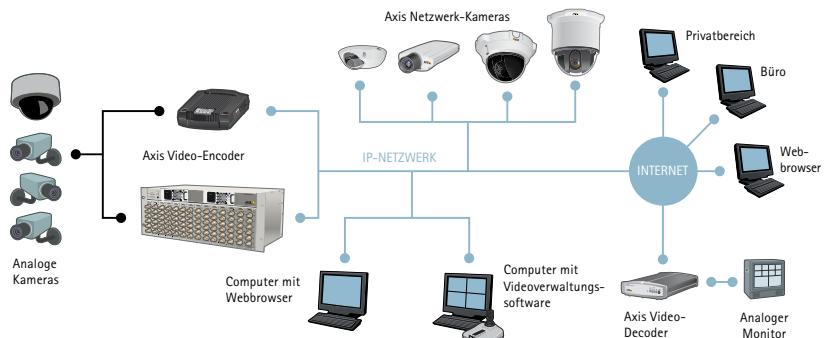


Abbildung 5.1a In der folgenden Abbildung wird dargestellt, wie Sie analoge Videokameras und analoge Monitore mithilfe von Video-Encodern und -Decodern in ein Netzwerk-Videosystem integrieren können.

Mithilfe von Video-Encodern lassen sich alle Arten von analogen Kameras wie z. B. fest ausgerichtete, Innen- und Außen-, Dome-, PTZ- und Spezialkameras, z. B. hochempfindliche Wärmebildkameras und Mikroskopkameras, über ein IP-Netzwerk einbinden und fernsteuern.

Video-Encoder bieten noch weitere Vorteile wie Ereignisverwaltungs- und intelligente Videofunktionen sowie erweiterte Sicherheitsmaßnahmen. Darüber hinaus bieten sie Skalierbarkeit und eine einfache Integration in andere Sicherheitssysteme.



Abbildung 5.1b Eigenständiger Ein-Kanal-Video-Encoder mit Audio, E/A-Anschlüssen zur Auswertung und Steuerung externer Geräte wie z. B. Sensoren und Alarmsirenen, seriellen Anschlüssen (RS-422/485) zur Steuerung analoger PTZ-Kameras und Ethernet-Netzwerkanschluss mit Power over Ethernet-Unterstützung.

5.1.1 Video-Encoder-Komponenten und Empfehlungen

Axis Video-Encoder bieten viele der für Netzwerk-Kameras zur Verfügung stehenden Funktionen. Einige der Hauptkomponenten von Video-Encodern sind:

- > Analoger Videoeingang zum Anschließen analoger Kameras über Koaxialkabel.
- > Prozessor zur Ausführung des Betriebssystems des Video-Encoders sowie der Netzwerk- und Sicherheitsfunktionen, zur Kodierung analoger Videodaten mithilfe unterschiedlicher Komprimierungsformate und zur Videoanalyse. Der Prozessor legt die Leistung des Video-Encoders fest. Sie wird üblicherweise in Bildern pro Sekunde bei der höchsten Auflösung gemessen. Moderne Video-Encoder bieten für jeden Videokanal eine volle Bildrate (30 Bilder pro Sekunde bei analogen NTSC-Kameras und 25 Bilder pro Sekunde bei analogen PAL-Kameras) bei höchster Auflösung. Axis Video-Encoder verfügen zudem über einen Autosensor, der automatisch erkennt, ob ein analoges Videosignal im NTSC-Standard- oder PAL-Standard eingeht. Weitere Informationen zu NTSC- und PAL-Auflösungen finden Sie in Kapitel 6.
- > Speicher zur Speicherung der Firmware (dem Video-Encoder-Betriebssystem) mithilfe von Flash und Pufferspeicher für Videosequenzen (mithilfe des RAM).
- > Ethernet-/PoE-Anschluss für die Verbindung mit dem IP-Netzwerk. Über das IP-Netzwerk erfolgt die Datenübertragung sowie die Stromversorgung des Geräts und der angeschlossenen Kamera, wenn Power over Ethernet unterstützt wird. Weitere Informationen zu Power over Ethernet finden Sie in Kapitel 9.

- > Serieller Anschluss (RS-232/422/485). Dieser Anschluss wird häufig zur Steuerung der PTZ-Funktionen analoger PTZ-Kameras verwendet.
- > Eingabe/Ausgabe-Anschlüsse für externe Geräte, z. B. Sensoren zur Erkennung von Alarmergebnissen und Relais zur Aktivierung von Lampen bei einem Vorfall.
- > Audio-Eingang für externe Mikrofone oder Line-in-Geräte und Audio-Ausgang für externe Aktivlautsprecher.

Video-Encoder für den professionellen Einsatz müssen hohe Anforderungen bezüglich der Zuverlässigkeit und Qualität erfüllen. Bei der Auswahl eines Video-Encoders sollte auch Folgendes berücksichtigt werden: die Anzahl der unterstützten analogen Kanäle, die Bildqualität, Komprimierungsformate, die Auflösung, die Bildrate sowie Funktionen wie PTZ-Unterstützung, Audio, Ereignisverwaltung, intelligentes Video, Power over Ethernet und Sicherheitsfunktionen.

5.1.2 Ereignisverwaltung und intelligentes Video

Ein Hauptvorteil von Axis Video-Encodern ist die Fähigkeit, Ereignisverwaltungs- und intelligente Videofunktionen bereitzustellen, die in analogen Videosystemen nicht zur Verfügung stehen. Integrierte intelligente Videofunktionen wie z. B. Videobewegungserkennung in mehreren Fenstern, Audioerkennung und aktiver Manipulationsalarm sowie Eingangssports für externe Sensoren sorgen dafür, dass das Überwachungssystem ständig aktiv ist, um Ereignisse zu erkennen. Wenn ein Ereignis erkannt wurde, kann das System selbsttätig mit Aktionen reagieren. Dazu zählen die Videoaufzeichnung, das Versenden von Warnmeldungen, z. B. E-Mails, das Einschalten von Beleuchtungen, das Öffnen bzw. Schließen von Türen und die Ausgabe von Alarmen. *Weitere Informationen zu den Ereignisverwaltungs- und den intelligenten Videofunktionen finden Sie in Kapitel 11.*

5.2 Eigenständige Video-Encoder

Die gängigsten Video-Encoder sind eigenständige Video-Encoder, die Ein-Kanal- oder Mehrkanalverbindungen (häufig vier Kanäle) zu analogen Kameras bieten. Video-Encoder mit mehreren Kanälen eignen sich hervorragend für mehrere analoge Kameras, die sich in Gebäuden bzw. an Orten befinden, die weit vom zentralen Überwachungsraum entfernt sind. Durch das Mehrkanalverfahren werden die Videosignale der einzelnen Remote-Kameras über dieselben Netzwerkkabel übertragen, wodurch Kosten für die Verkabelung eingespart werden können.

Wenn bereits Investitionen in analoge Kameras getätigt, jedoch noch keine Koaxialkabel verlegt wurden, ist der Einsatz von eigenständigen Video-Encodern empfehlenswert. Diese sollten nah an den analogen Kameras positioniert werden. Auf diese Weise werden die Installationskosten gesenkt, da keine neuen Koaxialkabel zu einem zentralen Standort verlegt werden müssen. Die Videodaten können über das Ethernet-Netzwerk gesendet werden. Außerdem werden Verluste bei der Bildqualität vermieden, die bei einer Übertragung von Videodaten mit Koaxialkabeln über größere Distanzen zu erwarten wären. Bei Koaxialkabeln nimmt die Videoqualität mit der Entfernung ab, die die Signale zurücklegen müssen.

Video-Encoder erzeugen digitale Bilder, die keinen entfernungsbedingten Qualitätsverlust aufweisen.



Abbildung 5.2a der Abbildung wird dargestellt, wie ein kleiner, Ein-Kanal-Video-Encoder neben einer analogen Kamera im Kameragehäuse positioniert wird.

5.3 In einem Rack montierte Video-Encoder

In einem Rack montierte Video-Encoder sind empfehlenswert, wenn viele analoge Kameras vorhanden sind, deren Koaxialkabel in einem speziellen Kontrollraum zusammenlaufen. Dadurch wird es möglich, eine große Anzahl analoger Kameras von einem Rack in einem zentralen Standort aus anzuschließen und zu verwalten. Ein Rack kann mehrere verschiedene Video-Encoder-Blades aufnehmen und bietet damit eine flexible, erweiterbare, kompakte Lösung. Ein Video-Encoder-Blade unterstützt eine, vier oder sechs analoge Kameras. Ein Blade ist mit einem Video-Encoder ohne Gehäuse vergleichbar. Es kann jedoch nicht unabhängig betrieben werden, sondern muss in ein Rack eingebaut werden.



Abbildung 5.3a Wenn das abgebildete AXIS Q7900 Rack vollständig mit 6-Kanal-Video-Encoder-Blades bestückt wird, können bis zu 84 analoge Kameras unterstützt werden.

Video-Encoder-Racks von Axis unterstützen das Hotswapping von Blades, also den Ein- und Ausbau von Blades im laufenden Betrieb. Sie sind zudem mit Anschlüssen für die serielle Kommunikation und Eingängen/Ausgängen für die einzelnen Video-Encoder-Blades sowie einem gemeinsamen Netzteil und gemeinsam genutzten Ethernet-Netzwerkverbindungen ausgestattet.

5.4 Video-Encoder für PTZ-Kameras und PTZ-Dome-Kameras

In einem Netzwerk-Videosystem werden PTZ-Befehle (Schwenken/Neigen/Zoomen) von einem Steuerungsgerät über dasselbe Netzwerkkabel übertragen wie die Videodaten und über den seriellen Anschluss des Video-Encoders (RS-232/422/485) an die analoge PTZ-Kamera bzw. PTZ-Dome-Kamera weitergeleitet. Video-Encoder bieten somit die Möglichkeit, analoge PTZ-Kameras über große Entfernung zu steuern, auch über das Internet. (In einem analogen CCTV-System muss

jede PTZ-Kamera einzeln mit dem Steuerungsgerät verkabelt werden, d. h. mit einem Joystick und anderen Bedienelementen.)

Zur Steuerung einer PTZ-Kamera muss für den Video-Encoder ein passender Treiber heruntergeladen werden. Viele Anbieter von Video-Encodern stellen PTZ-Treiber für die meisten analogen PTZ-Kameras und PTZ-Dome-Kameras bereit. Es kann auch ein PTZ-Treiber auf dem PC installiert werden, auf dem die Videoverwaltung ausgeführt wird, sofern der serielle Anschluss des Video-Encoders als serieller Server konfiguriert wird, der einfach nur die Befehle weiterleitet.



Abbildung 5.4a 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.

Der am häufigsten verwendete serielle Anschluss zur Steuerung von PTZ-Funktionen ist RS-485. Ein Vorteil von RS-485 ist die Fähigkeit, mehrere PTZ-Kameras mithilfe von Twisted-Pair-Kabeln in Reihe zu schalten, d. h. von einer Dome-Kamera zur nächsten. Die maximale Entfernung bei einem RS-485-Kabel ohne Repeater beträgt 1.220 Meter bei einer Baudrate bis zu 90 Kbit/s.

5.5 Deinterlacing-Techniken

Videodaten aus analogen Kameras wurden für die Anzeige auf analogen Monitoren wie herkömmlichen Fernsehgeräten konzipiert. Diese verwenden eine Technik, die als Zeilensprungverfahren bezeichnet wird. Beim Zeilensprungverfahren bilden zwei aufeinanderfolgende Zeilensprungfelder ein Bild. Wenn Sie diese Daten auf Computerbildschirmen, die die progressive Abtastung verwenden, ausgeben, treten Interlacing-Effekte (z. B. Reiben oder Kammeffekt) bei sich bewegenden Objekten auf. Zur Vermeidung dieser Interlacing-Effekte können Sie verschiedene Deinterlacing-Techniken einsetzen. Moderne Video-Encoder von Axis bieten zwei unterschiedliche Deinterlacing-Techniken an: Adaptive Interpolation und Blending.

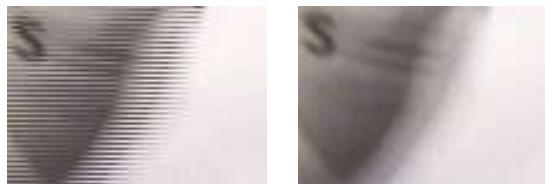


Abbildung 5.5a Links: Nahaufnahme eines Zeilensprungbilds auf einem Computerbildschirm. Rechts: Dasselbe Zeilensprungbild mit angewandter Deinterlacing-Technik.

Bei der **adaptiven Interpolation** wird die beste Bildqualität erzielt. Diese Technik verwendet nur eines der aufeinanderfolgenden Felder. Das zur Erzeugung des Vollbilds benötigte andere Feld wird durch Interpolation erstellt.

Beim **Blending** werden zwei aufeinanderfolgende Felder miteinander „verschmolzen“, sodass ein Bild mit allen Feldern entsteht. Anschließend wird das Bild gefiltert, um unerwünschte Bewegungsartefakte bzw. Kammeffekte zu entfernen, die dadurch entstanden sind, dass die beiden Felder zu unterschiedlichen Zeiten aufgenommen wurden. Die Blending-Technik ist weniger prozessorintensiv als die adaptive Interpolation.

5.6 Video-Decoder

Mit einem Video-Decoder werden die digitalen Video- und Audio-Datenströme von Video-Encoder oder Netzwerk-Kameras in analoge Signale zurückkonvertiert, die dann von analogen Monitoren wie herkömmlichen Fernsehgeräten und Video-Umschaltern verwendet werden können. Ein typischer Fall könnte ein Einzelhandelsunternehmen sein, das an öffentlichen Plätzen herkömmliche Monitore einsetzen will, um zu zeigen, dass Videoüberwachung präsent ist.

Video-Decoder werden auch häufig in einer Analog-Digital-Analog-Konfiguration zur Übertragung von Videodaten über lange Strecken eingesetzt. Die Qualität von digitalen Videodaten wird bei der Übertragung über große Entfernung nicht beeinträchtigt. Beim Senden von analogen Signalen können sich große Entfernung hingegen negativ auf die Bildqualität auswirken. Der einzige Nachteil ist möglicherweise die Latenzzeit von einigen Millisekunden. Die Latenz hängt von der Entfernung und der Netzwerkqualität zwischen den Endpunkten ab.

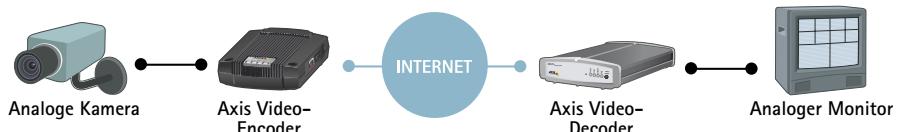


Abbildung 5.6a Mithilfe eines Encoders und eines Decoders können Videodaten über lange Entfernung von einer analogen Kamera an einen analogen Monitor übertragen werden.

Ein Video-Decoder kann Videodaten mehrerer Kameras nacheinander dekodieren und anzeigen, d. h. zunächst werden einige Sekunden lang Daten von einer Kamera dekodiert und angezeigt, anschließend wird zur nächsten Kamera gewechselt usw.

Auflösungen

Die Auflösung folgt in der analogen und in der digitalen Welt denselben Prinzipien. Dennoch gibt es einige Unterschiede bei der Definition. Analoge Videobilder setzen sich aus Zeilen bzw. TV-Zeilen zusammen, da diese Technologie aus der Fernsehtechnik entwickelt wurde. Digitale Bilder bestehen aus quadratischen Pixeln. In den folgenden Abschnitten werden die verschiedenen Auflösungen von Netzwerk-Video beschrieben. Dazu gehören NTSC, PAL, VGA, Megapixel und HDTV.

6.1 NTSC- und PAL-Auflösung

Die Auflösungen „NTSC“ (National Television System Committee) und „PAL“ (Phase Alternating Line) sind analoge Videostandards. Sie sind für Netzwerk-Video relevant, da Video-Encoder solche Auflösungen bieten, wenn sie Signale von analogen Kameras digitalisieren. Aktuelle PTZ-Netzwerk-Kameras und PTZ-Dome-Netzwerk-Kameras bieten ebenfalls NTSC- und PAL-Auflösungen, da diese Kameras heutzutage einen für analoge Videokameras entwickelten Kamerablock (mit Kamera-, Zoom-, Autofokus- und automatischen Blendenfunktionen) in Verbindung mit einer eingebauten Video-Encoder-Platine verwenden.

In Nordamerika und Japan ist der NTSC-Standard der vorherrschende Standard für Analogvideo, in Europa und in vielen asiatischen und afrikanischen Ländern wird hingegen meist der PAL-Standard verwendet. Beide Standards stammen aus der Fernsehtechnik. NTSC hat eine Auflösung von 480 Zeilen und eine Aktualisierungsrate von 60 Zeilensprungfeldern pro Sekunde (oder 30 Bilder pro Sekunde). Der neue Name, der die Anzahl der Zeilen, das Abtastverfahren und die Aktualisierungsrate widerspiegelt, ist 480i60 („i“ steht für „interlaced scanning“ [Zeilensprungverfahren]). PAL hat eine Auflösung von 576 Zeilen und eine Aktualisierungsrate von 50 Zeilensprungfeldern pro Sekunde (oder 25 Bilder pro Sekunde). Der neue Name für diesen Standard lautet 576i50. Die Gesamtmenge an Informationen pro Sekunde ist bei beiden Standards gleich.

Wenn analoges Video digitalisiert wird, basiert die maximale Menge an Pixeln, die erzeugt werden können, auf der Anzahl der verfügbaren TV-Zeilen. Die maximale Größe eines digitalisierten Bildes ist in der Regel D1 und die am häufigsten verwendete Auflösung ist 4CIF (Common Intermediate Format).

Bei der Anzeige auf einem Computerbildschirm können digitalisierte Analogvideobilder Zeilensprungeffekte (Interlacing-Effekte) aufweisen, z. B. Reiben, und die Formen können leicht verschoben sein, da die erzeugten Pixel möglicherweise nicht mit den quadratischen Pixeln auf dem Computerbildschirm übereinstimmen. Zeilensprungeffekte können durch Anwendung von Deinterlacing-Techniken (siehe Kapitel 5) verringert werden. Die Seitenverhältniskorrektur kann vor der Anzeige vorgenommen werden, um sicherzustellen, dass beispielsweise ein Kreis in einem analogen Video auch auf dem Computerbildschirm als Kreis angezeigt wird.

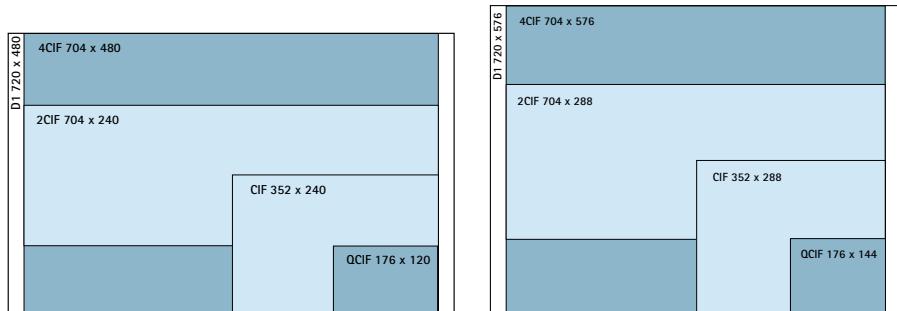


Abbildung 6.1a Links sind verschiedene NTSC-Bildauflösungen dargestellt. Rechts sind verschiedene PAL-Auflösungen zu sehen.

6.2 VGA-Auflösungen

Bei vollständig digitalen Systemen, die auf Netzwerk-Kameras basieren, können die weltweit standardisierten Auflösungen der Computertechnik verwendet werden, was eine größere Flexibilität bietet. Die Einschränkungen von NTSC und PAL sind hier irrelevant.

VGA (Video Graphics Array) ist ein Grafikanzeigesystem für PCs, das ursprünglich von IBM entwickelt wurde. Die Auflösung beträgt 640 x 480 Pixel und ist ein gängiges Format für Netzwerk-Kameras, die keine Megapixeltechnologie verwenden. Die VGA-Auflösung ist für Netzwerk-Kameras besser geeignet, da VGA-basiertes Video quadratische Pixel erzeugt, die den Pixeln auf Computerbildschirmen entsprechen. Computerbildschirme unterstützen Auflösungen in VGA oder einem Vielfachen von VGA.

Anzeigeformat	Pixel
QVGA (SIF)	320x240
VGA	640x480
SVGA	800x600
XVGA	1024x768
4x VGA	1280x960

Tabelle 6.2 VGA resolutions.

6.3 Megapixelauflösungen

Eine Netzwerk-Kamera mit einer Auflösung im Megapixelbereich verwendet einen Megapixelsensor, um Bilder zu erzeugen, die eine Million oder mehr Pixel enthalten. Je mehr Pixel ein Sensor hat, desto besser ist er in der Lage, feine Details zu erfassen und hochwertige Bilder zu erzeugen. Megapixel-Netzwerk-Kameras können verwendet werden, um mehr Details anzuzeigen (ideal für die Identifizierung von Personen und Objekten) oder um einen größeren Bereich einer Szene zu sehen. Dieser Vorteil ist ein wichtiges Kriterium bei Videoüberwachungsanwendungen.

Anzeigeformat	Anzahl der Megapixel	Pixel
SXGA	1,3 megapixels	1280x1024
SXGA+ (EXGA)	1,4 megapixels	1400x1050
UXGA	1,9 megapixels	1600x1200
WUXGA	2,3 megapixels	1920x1200
QXGA	3,1 megapixels	2048x1536
WQXGA	4,1 megapixels	2560x1600
QSXGA	5,2 megapixels	2560x2048

Tabelle 6.3 Oben sind einige Megapixelformate aufgeführt..

Die Megapixelauflösung ist ein Bereich, in dem Netzwerk-Kameras analogen Kameras überlegen sind. Die maximale Auflösung, die eine herkömmliche analoge Kamera bieten kann, nachdem das Videosignal von einem digitalen Videorecorder oder einem Video-Encoder umgewandelt wurde, ist D1, was 720×480 Pixeln (NTSC) bzw. 720×576 Pixeln (PAL) entspricht. Die D1-Auflösung entspricht einem Maximum von 414.720 Pixeln oder 0,4 Megapixeln. Zum Vergleich: Das gängige Megapixelformat von 1280×1024 Pixeln bietet eine Auflösung von 1,3 Megapixeln. Dies ist eine dreimal so hohe Auflösung wie die von analogen CCTV-Kameras. Es sind auch Netzwerk-Kameras mit einer Auflösung von 2 und 3 Megapixeln verfügbar und für die Zukunft werden sogar noch höhere Auflösungen erwartet.

Die Auflösungen im Megapixel-Bereich bieten zudem mehr Flexibilität beim Erzeugen von Bildern mit unterschiedlichen Seitenverhältnissen. (Das Seitenverhältnis ist das Verhältnis zwischen der Breite und Höhe eines Bildes.) Ein herkömmlicher Fernsehbildschirm zeigt ein Bild mit einem Seitenverhältnis von 4:3 an. Die Megapixel-Netzwerk-Kameras von Axis bieten neben diesem Format noch weitere Formate an, z. B. 16:9. Der Vorteil eines Seitenverhältnisses von 16:9 besteht darin, dass keine unwichtigen Details, die sich in der Regel im oberen und unteren Bereich eines Bildes von herkömmlicher Größe befinden, vorhanden sind, wodurch Bandbreite und Speicherplatz eingespart werden können. Des Weiteren entspricht das 16:9-Format mehr dem Seitenverhältnis des menschlichen Auges, was wiederum dazu führt, dass das Auge nicht so schnell ermüdet, wenn Videosequenzen im 16:9 anstelle 4:3 Seitenverhältnis betrachtet werden.



Abbildung 6.3a Darstellung der Seitenverhältnisse 4:3 und 16:9.

6.4 HDTV-Auflösungen (High-Definition Television)

HDTV bietet eine fünf Mal so hohe Auflösung wie analoges Standardfernsehen, eine bessere Farbtreue und ein 16:9-Format. Die beiden wichtigsten, von SMPTE (Society of Motion Picture and Television Engineers) definierten HDTV-Standards sind SMPTE 296M und SMPTE 274M.

SMPTE 296M (HDTV 720p) hat eine Auflösung von 1280 x 720 Pixeln mit einer hohen Farbtreue im 16:9-Format. Dieser Standard verwendet die progressive Abtastung bei 25/30 Hertz (Hz), die je nach Land 25 oder 30 Bilder pro Sekunde und 50/60 Hz (50/60 Bilder pro Sekunde) entspricht.

SMPTE 274M (HDTV 1080) hat eine Auflösung von 1920 x 1080 Pixeln mit einer hohen Farbtreue im 16:9-Format. Dieser Standard verwendet das Zeilensprungverfahren (1080i) oder die progressive Abtastung (1080p) bei 25/30 Hz bzw. 50/60 Hz.

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, sodass HDTV-Videobilder von Netzwerk-Videoprodukten auf HDTV-Bildschirmen oder Standard-Computermonitoren angezeigt werden können. Bei HDTV-Video mit progressiver Abtastung sind keine Konvertierungs- oder Deinterlacing-Techniken erforderlich, wenn die Videodaten von einem Computer verarbeitet oder auf einem Computerbildschirm angezeigt werden sollen.

Videokomprimierung

Bei der Videokomprimierung werden redundante Videodaten reduziert und entfernt, sodass eine digitale Videodaten effizient über ein Netzwerk übertragen und auf einer Computerfestplatte gespeichert werden kann. Mit effizienten Komprimierungstechniken kann eine deutliche Verkleinerung des Datenvolumens erzielt werden, ohne dass dies die visuelle Bildqualität merklich beeinträchtigt. Beeinträchtigungen in der Bildqualität, werden in der Regel erst ersichtlich, wenn mit einer relativ hohen Komprimierungsstufe gearbeitet wird, um das Datenvolumen auf ein Minimum zu reduzieren.

Es stehen verschiedene proprietäre und standardisierte Technologien für die Komprimierung zur Verfügung. Die meisten Netzwerk-Video-Hersteller verwenden heutzutage Standardtechnologien. Standards sind für die Gewährleistung der Kompatibilität und Interoperabilität wichtig. Sie sind insbesondere für die Videokomprimierung relevant, da Videodaten für unterschiedliche Zwecke verwendet werden können und in einigen Videoüberwachungsanwendungen auch Jahre nach dem Aufzeichnungszeitpunkt noch anzeigbar sein müssen. Durch die Verwendung von Standards sind Endbenutzer in der Lage, Geräte von verschiedenen Herstellern zu nutzen, sodass sie bei der Implementierung eines Videoüberwachungssystems nicht an einen Hersteller gebunden sind.

Axis verwendet drei verschiedene Videokomprimierungsstandards: Motion JPEG, MPEG-4 Part 2 (oder einfach MPEG-4) und H.264 (auch als MPEG-4 Part 10 oder Advanced Video Coding, kurz AVC bezeichnet). H.264 ist der neueste und effizienteste Videokomprimierungsstandard. In diesem Kapitel werden die Grundlagen der Komprimierung und die oben genannten Standards beschrieben.

7.1 Grundlagen der Komprimierung

7.1.1 Video-Codec

Bei der Komprimierung wird das Quellvideo über Algorithmen in eine komprimierte Datenstrom umgewandelt, der dann übertragen oder gespeichert werden kann. Zur Wiedergabe der komprimierten Daten werden inverse Algorithmen angewendet. Dadurch wird Video erzeugt, das im

Wesentlichen denselben Inhalt bietet wie das ursprüngliche Quellvideo. Die Zeit, die zur Komprimierung, Übertragung, Dekomprimierung und Wiedergabe der Videodaten erforderlich ist, wird als Latenz bezeichnet.

Ein zusammengehöriges Algorithmenpaar wird als Video-Codec (Encoder/Decoder) bezeichnet. Video-Codecs unterschiedlicher Standards sind normalerweise nicht miteinander kompatibel, d. h. dass Videoinhalte, die mit einem Standard komprimiert worden sind, nicht mit einem anderen Standard dekomprimiert werden können. Zum Beispiel funktioniert ein MPEG-4-Decoder nicht in Kombination mit einem H.264-Encoder, da ein bestimmter Algorithmus nicht das Ergebnis eines anderen Algorithmus dekomprimieren kann. Man kann allerdings mehrere verschiedene Algorithmen in derselben Software oder Hardware implementieren, sodass verschiedene Formate parallel bestehen können.

7.1.2 Bild- im Vergleich zu Videokomprimierung

Die verschiedenen Komprimierungsstandards nutzen unterschiedliche Methoden zur Datenreduzierung. Daher unterscheiden sie sich hinsichtlich Bitrate, Qualität und Latenz. Es gibt zwei Arten von Komprimierungsalgorithmen: Bildkomprimierung und Videokomprimierung.

Bildkomprimierung verwendet eine bildinterne Codier-Technologie. 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.



Abbildung 7.1a Im Motion JPEG-Format werden die drei Bilder in der obigen Folge codiert und als separate, eigenständige Bilder (I-Frames) übertragen, die voneinander unabhängig sind.

Videokomprimierungs-Algorithmen wie z. B. MPEG-4 und H.264 verwenden eine Interframe-Vorhersage, um die Videodaten zwischen mehreren Bildern zu reduzieren. Dies beinhaltet Techniken wie die Differenzcodierung, bei der ein Bild mit einem Referenzbild verglichen wird und nur die Pixelblöcke codiert werden, die sich im Vergleich zum Referenzbild geändert haben. Auf diese Weise wird die Anzahl der Pixelblöcke reduziert, die codiert und übertragen werden müssen. Wenn eine solche codierte Sequenz angezeigt wird, erscheinen die Bilder wie in der Original-Videosequenz.

— Übertragen — Nicht übertragen



Abbildung 7.1b 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, in diesem Fall also auf das Haus. Nur die beweglichen Teile, d. h. die laufende Person, wird mithilfe von Bewegungsvektoren codiert, wodurch die Menge an zu sendenden und zu speichernden Informationen deutlich reduziert werden kann.

Es können weitere Techniken wie der blockbasierte Bewegungsausgleich angewendet werden, um die Daten zu reduzieren. Beim blockbasierten Bewegungsausgleich wird berücksichtigt, welche Anteile des neuen Bildes einem früheren Bild in der Videosequenz entnommen werden können, ggf. aus 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. Wird eine Übereinstimmung gefunden, codiert der Encoder die Position des passenden Blocks im Referenzbild. Die Codierung dieses Bewegungsvektors erfordert eine geringere Bitmenge als der eigentliche Inhalt des codierten Blocks.

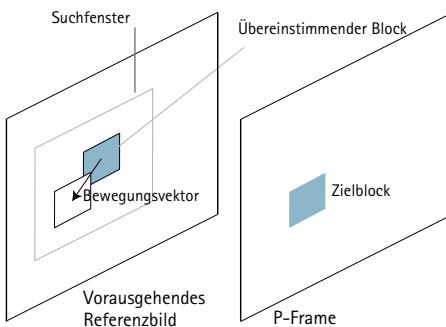


Abbildung 7.1c Darstellung des blockbasierten Bewegungsausgleichs.

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 stets ein I-Frame. I-Frames werden als Ausgangspunkte für neue Betrachter oder als Resynchronisierungspunkte benötigt, falls der übertragene Datenstrom beschädigt wurde. I-Frames eignen sich zur Implementierung für schnellen Vorlauf und Rücklauf sowie anderen Funktionen mit Direktzugriff. Encoder fügen automatisch in regelmäßigen Abständen I-Frames in den Datenstrom ein, oder auf Anforderung, falls einer Client die Wiedergabe des Videodatenstroms anfordert. Von der Größe des Datenvolumens her betrachtet, stellt ein I-Frame den größten Frametyp dar.

P-Frames („Predictive Interframe“) verweisen bei ihrer Codierung auf Bildinformationen vorausgehender I- 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. Die Größe der P-Frames ist immer davon abhängig, wie viel Redundanzen zeitlicher und räumlicher Natur, in Bezug auf das Referenzbild, vorhanden sind.

B-Frames („Bi-predictive Interframes“) haben einen bidirektionalen Bezug und verweisen zugleich auf ein vorausgehendes und auf ein nachfolgendes I- oder P-Frames. Da für die Decodierung eines B-Frames immer auf Frames in der Zukunft gewertet werden müssen, erhöht die Nutzung der B-Frames zwangsläufig die Latenz. Da im Bereich der IP-basierten Videoübertragung geringere Latzenzen angestrebt werden, werden in der Regel in diesem Bereich B-Frames keine B-Frames verwendet.

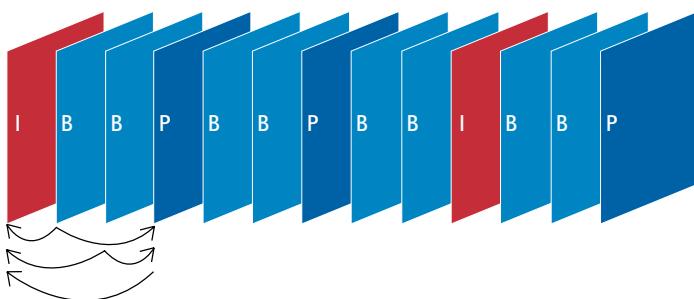


Abbildung 7.1d Typische Sequenz mit I-, B- und P-Frames. P-Frames verweisen nur auf vorausgehende I- oder P-Frames, B-Frames ggf. auch auf nachfolgende I- oder P-Frames.

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

In den Netzwerk-Videoprofilen von Axis können Benutzer über die sogenannte GOV-Länge (Group of Video) festlegen, wie lange eine zu sendenden Sequenzgruppe ist, bestehend aus einem I-Frame und mehreren P-Frames, bevor ein weiterer I-Frame gesendet wird. Durch Verringern der I-Frame-Anzahl (größere GOV-Länge) kann die erforderliche Bitrate reduziert werden.

Neben der Differenzcodierung und dem Bewegungsausgleich können weitere Methoden zur Reduzierung von Daten und zur Verbesserung der Videoqualität durchgeführt werden. Zum Beispiel unterstützt H.264 moderne Techniken wie Vorhersageschemata für die Codierung von I-Frames, einen verbesserten Bewegungsausgleich bis in den Unterpixelbereich hinein sowie einen internen Deblocking-Filter zum Glätten von Blockartefakte (Blockkanten). Weitere Informationen zu H.264-Techniken finden Sie im Axis-White Paper zu H.264 unter www.axis.com/corporate/corp_tech_papers.htm

7.2 Komprimierungsformate

7.2.1 Motion JPEG

Motion JPEG oder M-JPEG ist eine digitale Videosequenz, die aus mehreren einzelnen JPEG-Bildern besteht. (JPEG steht für Joint Photographic Experts Group.) Ab einer Bildrate von 16 Bilder pro Sekunde, nimmt der Betrachter dies als fließendes Video wahr. Ein Video mit voller Bewegungsgeschwindigkeit wird bei 30 (NTSC) oder 25 (PAL) Bilder pro Sekunde wahrgenommen.

Einer der Vorteile von Motion JPEG besteht darin, dass jedes Bild einer Videosequenz dieselbe garantierte Qualität hat, die durch die für die Netzwerk-Kamera oder den Video-Encoder ausgewählte Komprimierungsstufe bestimmt wird. Je höher die Komprimierungsstufe ist, desto kleiner ist die Dateigröße der einzelnen JPEG-Bilder. Bei der Nutzung von relativ hohen Komprimierungsstufen kann sich die Bildqualität verschlechtern. Man muss deshalb immer in Abhängigkeit der geforderten Bildqualität abwägen, wie hoch die genutzte Komprimierungsstufe sein darf. Die Dateigröße der einzelnen JPEG-Bilder, ist auch immer von der Komplexität und Situation abhängig. Bei einigen Situationen, z. B. bei schwachem Licht oder komplexen Szenen, kann eine Bilddatei relativ groß werden und mehr Bandbreite und Speicherplatz in Anspruch nehmen. Um einen Anstieg der Bandbreiten- und Speicherplatznutzung zu verhindern, können Benutzer von Axis-Netzwerk-Videoprodukten eine maximale Dateigröße für ein Einzelbild festlegen.

Da es in Motion JPEG 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 lizenzerfreier Standard. Er weist eine umfassende Kompatibilität auf und wird vor allem in Anwendungen verwendet, in denen einzelne Bilder einer Videosequenz (z. B. zu Analysezwecken) benötigt und kurze Bildraten, meist 5 Bilder pro Sekunde oder weniger, verwendet werden. Motion JPEG ist unter Umständen auch in Anwendungen erforderlich, die in Systeme integriert werden müssen, die nur Motion JPEG unterstützen.

Ein Nachteil von Motion JPEG besteht darin, dass hierbei nicht die klassischen Videokomprimierungstechniken anwendet werden, um die Datenmenge zu verringern, da es sich um eine Reihe vollständiger Einzelbilder handelt. Dies führt bezogen auf die gelieferte Qualität zu einer relativ hohen Bitrate bzw. einem geringen Komprimierungsverhältnis verglichen mit Videokomprimierungsstandards wie MPEG-4 und H.264.

7.2.2 MPEG-4

Wenn der Begriff MPEG-4 in Videoüberwachungsanwendungen verwendet wird, bezieht sich dies meistens auf MPEG-4 Part 2, auch bekannt als MPEG-4 Visual. Wie alle MPEG-Standards (Moving Picture Experts Group) handelt es sich hierbei um einen lizenzierten Standard, d. h., für Nutzung fallen Lizenzgebühren an. Axis liefert bei den Netzwerk-Videoprodukten zwei Lizenzen mit, eine für das Codieren und eine für das Decodieren. Diese beiden Lizenzen ermöglichen demnach, den Zugriff von einem Client, ohne das zusätzliche Lizenzgebühren anfallen. Erst wenn mehrere Clients zeitgleich einen MPEG-4-Videostrom von einem Axis Netzwerk-Videoprodukt abrufen möchten, müssen weitere Lizenzen hinzugekauft werden, welche allerdings im Bereich von etwa einem Euro/Stück liegen. MPEG-4 unterstützt Anwendungen mit niedriger Bandbreite und Anwendungen, die hochwertige Bilder erfordern und keine Einschränkungen bei der Bildrate und bei der Bandbreitennutzung haben.

7.2.3 H.264 oder MPEG-4 Part 10/AVC

H.264, auch als MPEG-4 Part 10/AVC für Advanced Video Coding bekannt, ist der neueste MPEG-Standard für die Video-Codierung. Es wird davon ausgegangen, dass sich H.264 in den kommenden Jahren als Videostandard durchsetzen wird. Dies ist darauf zurückzuführen, dass ein H.264-Encoder ohne Einbußen bei der Bildqualität bei digitalen Videodateien im Vergleich zu Motion JPEG eine 80 % höhere Komprimierung erreicht. Gegenüber dem Standard MPEG-4 wird durchschnittlich eine um 50 % höhere Komprimierung erzielt. Das bedeutet, dass Videodateien wesentlich weniger Netzbänder und Speicherplatz beanspruchen. Umgekehrt kann bei gleicher Bitrate eine deutlich höhere Videoqualität erzielt werden, indem Bilder mit höherer Auflösung übertragen werden.

H.264 wurde gemeinsam von Standardisierungsunternehmen der Telekommunikationsbranche (ITU-T's Video Coding Experts Group) und der IT-Branche (ISO/IEC Moving Picture Experts Group) entwickelt. Es wird davon ausgegangen, dass dieser Standard in größerem Ausmaß angewendet wird als vorhergehende Standards. In der Videoüberwachungsbranche wird sich H.264 vermutlich zuerst in Anwendungen durchsetzen, die hohe Ansprüche an Bildrate und Auflösung stellen, so bei der Überwachung von Autobahnen, Flughäfen und Spielhallen, bei der Bildraten von 30 bzw. 25 Bilder/s (NTSC bzw. PAL) die Norm sind. In diesen Bereichen ist das Potenzial von Kostenersparnissen durch geringere Anforderungen an Bandbreite und Speicher am größten.

Ebenso wird erwartet, dass H.264 die Akzeptanz von Megapixel-Kameras in der Überwachungsbranche beschleunigt, da das hocheffiziente Komprimierungsverfahren deutlich reduziertes Datenvolumen und Bitraten ohne Einbußen bei der Bildqualität ermöglicht. Allerdings muss man bei H.264 berücksichtigen, dass für die Codierung und Decodierung der Videoinformationen eine höherer Rechenleistung benötigt wird.

Die H.264-Encoder von Axis arbeiten mit dem so genannten Baseline Profil, d. h., es werden nur I- und P-Frames verwendet. Dieses Profil eignet sich ideal für Netzwerk-Kameras und Video-Encoder, da durch den Verzicht auf B-Frames niedrige Latenzen erzielt werden. Eine niedrige

Latenz ist in Videoüberwachungsanwendungen mit Live-Überwachung von entscheidender Bedeutung, insbesondere, wenn PTZ-Kameras oder PTZ-Dome-Kameras eingesetzt werden. Die Lizenzthematik ist bei H.264 vergleichbar zu MPEG-4 Part 2 (siehe Abschnitt 7.2.2), wobei H.264-Lizenzen benötigt werden.

7.3 Variable und konstante Bitraten

Bei der Verwendung von MPEG-4 und H.264 können Benutzer festlegen, ob ein codierter Videostrom eine variable oder eine konstante Bitrate nutzt. Die optimale Auswahl hängt von der Anwendung und der Netzwerkinfrastruktur ab.

Bei VBR (variable Bitrate) kann ein vordefinierter Grad an Bildqualität aufrechterhalten werden, unabhängig von vorhandenen oder nicht vorhandenen Veränderungen in einer Szene. Das heißt, es wird mehr Bandbreite benötigt, wenn eine Szene viele Aktivitäten aufweist, und weniger Bandbreite, wenn keine Veränderung vorhanden ist. Dies wird oftmals in Videoüberwachungsanwendungen gewünscht, in denen eine hohe Qualität erforderlich ist, vor allem, wenn Szenen beispielsweise bewegte Personen oder Fahrzeuge enthalten. Da die Bitrate variieren kann, auch wenn eine durchschnittliche Bitrate festgelegt ist, muss die Netzwerkinfrastruktur entsprechende Bandbreiten zur Verfügung stellen können.

Falls in der zur Verfügung stehenden Bandbreite Engpässe vorhanden sind, z.B. einem DSL-Uplink, bietet sich die Nutzung von CBR (konstante Bitrate) an. Bei diesem Modus wird ein Videostrom mit der vom Benutzer definierbaren konstanten Bitrate geliefert. Der Nachteil von CBR besteht allerdings darin, dass im Falle von erhöhter Veränderung in einer Szene, die normalerweise zu einer höheren Bildrate führen würde, die Beschränkung auf die konstante Bitrate zu einer schlechteren Bildqualität und einer niedrigeren Bildrate führt. Netzwerk-Videoprodukte von Axis ermöglichen es dem Benutzer, im Zusammenhang von CBR die Priorität auf die Bildqualität oder die Bildrate zu legen. Der Benutzer kann demnach festlegen, ob die eigentlich höhere Bitrate, durch die Reduzierung der Bildrate oder durch die Erhöhung der verwendeten Komprimierungsstufe ausgeglichen wird. Im ersten Fall, bleibt die Bildqualität weitestgehend erhalten und im zweiten Fall muss man mit einer geringeren Bildqualität rechnen, sobald viele Veränderungen in der Szene auftreten. Im Bereich der Videoüberwachung, wird in der Regel die Priorität auf die Bildqualität gesetzt, damit die Bildinformation auswertbar ist.

7.4 Standards im Vergleich

Beim Vergleichen der Leistung von MPEG-Standards wie MPEG-4 und H.264 ist es wichtig zu wissen, dass die Ergebnisse zwischen verschiedenen Codern variieren können, auch wenn sie denselben Standard verwenden. Dies hängt damit zusammen, dass die Entwickler von Codern diese mit unterschiedlichen, im Standard definierten Programmen ausstatten können. Solange die Ausgabe eines Encoders mit dem Standardformat und dem Decoder übereinstimmt, können unterschiedliche Implementierungen realisiert werden. Ein MPEG-Standard kann daher nicht

eine bestimmte Bitrate oder Bildqualität garantieren, und Vergleiche können erst dann durchgeführt werden, wenn zuvor definiert wurde, wie die Standards in einem Encoder implementiert sind. Anders als beim Encoder müssen im Decoder alle erforderlichen Bestandteile eines Standards implementiert sein, damit eine Decodierung normgerechter Bitströme gewährleistet ist. Ein Standard legt genau fest, auf welche Weise ein Dekomprimierungsalgorithmus die einzelnen Bits von komprimiertem Video wiederherstellt.

Das nachstehende Diagramm vergleicht die Bitraten der folgenden Videostandards bei gleicher Bildqualität: Motion JPEG, MPEG-4 Part 2 (ohne Bewegungsausgleich), MPEG-4 Part 2 (mit Bewegungsausgleich) und H.264 (Baseline Profil).

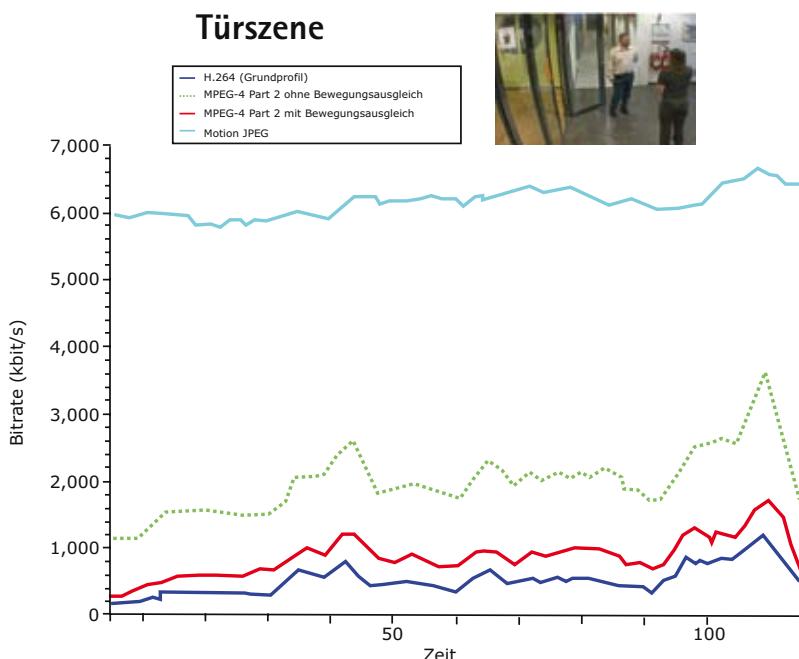


Abbildung 7.4a Der H.264-Encoder von Axis hat eine um bis zu 50 % geringere Bandbreite für eine Beispiel-Videosequenz erzeugt als ein MPEG-4-Encoder mit Bewegungsausgleich. Der H.264-Encoder erwies sich als mindestens dreimal so effizient wie ein MPEG-4-Encoder ohne Bewegungsausgleich und mindestens sechsmal so effizient wie Motion JPEG.

Audio

Die Verwendung von Audiofunktionalität in Videoüberwachungssystemen ist zwar noch nicht weit verbreitet, kann aber die Fähigkeit eines Systems, Ereignisse zu erkennen und zu interpretieren, verbessern und die Audio-Kommunikation über ein IP-Netzwerk ermöglichen. Die Verwendung von Audio ist in manchen Ländern möglicherweise gesetzlich nicht zulässig. Es wird daher empfohlen, dies vor der Implementierung zu überprüfen.

Die Themen in diesem Kapitel umfassen Anwendungsszenarien, Audiogeräte, Audio-Modi, Audioerkennungsalarme, Audio-Komprimierung und Audio-/Video-Synchronisierung.

8.1 Audio-Anwendungen

Die Integration von Audiofunktionalität in ein Videoüberwachungssystem kann die Fähigkeit eines Systems, Ereignisse und Notfallsituationen zu erkennen und zu interpretieren, auf wertvolle Weise ergänzen. Dank der Fähigkeit von Audio, 360 Grad eines Bereichs abzudecken, kann ein Videoüberwachungssystem seinen Abdeckungsbereich über das Sichtfeld der Kamera hinaus erweitern. Es kann eine PTZ-Kamera oder PTZ-Dome-Kamera (oder den Bediener dieser Kameras) anweisen, bei einem Audioalarm eine visuelle Überprüfung vorzunehmen.

Audio kann außerdem verwendet werden, um einen Bereich abzuhören und um Besuchern oder Eindringlingen Anweisungen zu erteilen oder Fragen zu stellen. Wenn sich beispielsweise eine Person im Sichtfeld einer Kamera auffällig verhält, z. B. in der Nähe eines Geldautomaten herumlüngert oder einen gesperrten Bereich betritt, kann ein entfernter Wachmann der Person eine verbale Warnung erteilen. Auch in Situationen, in denen eine Person verletzt wurde, kann es von Vorteil sein, mit der Person kommunizieren und ihr mitteilen zu können, dass Hilfe unterwegs ist. Ein weiterer Anwendungsbereich ist die Zugangskontrolle, z. B. ein ferngesteuerter „Türsteher“ an einer Eingangstür. Weitere Einsatzbereiche sind Remote-Helpdesks (z. B. in einem unbewachten Parkhaus) und Videokonferenzen. Ein audiovisuelles Überwachungssystem erhöht die Effektivität einer Sicherheits- oder Fernüberwachungslösung, indem ein nicht vor Ort befindlicher Benutzer die Möglichkeit erhält, Informationen zu empfangen und zu übermitteln.

8.2 Audio-Unterstützung und Geräte

Audio-Unterstützung lässt sich leichter in ein Netzwerk-Videosystem als in ein analoges CCTV-System implementieren. In einem analogen System müssen separate Audio- und Videokabel von einem Endpunkt zum anderen Endpunkt verlegt werden, also von der Kamera und dem Mikrofon zur Anzeige-/Aufzeichnungsstation. Wenn die Entfernung zwischen Mikrofon und Station zu groß ist, müssen Geräte zur symmetrischen Signalübertragung verwendet werden, wodurch der Implementierungsaufwand und die Installationskosten steigen. In einem Netzwerk-Videosystem verarbeitet eine Netzwerk-Kamera mit Audio-Unterstützung die Audiodaten und sendet sowohl die Audio- als auch die Videodaten über dasselbe Netzwerkkabel für die Überwachung und/oder Aufzeichnung. Dadurch ist kein zusätzlicher Verkabelungsaufwand erforderlich und die Synchronisierung von Audio und Video ist deutlich einfacher.

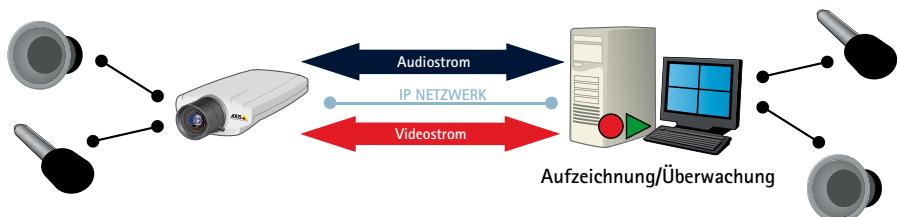


Abbildung 8.2a Ein Netzwerk-Videosystem mit integrierter Audio-Unterstützung. Audio- und Videoströme werden über dasselbe Netzwerkkabel übertragen.

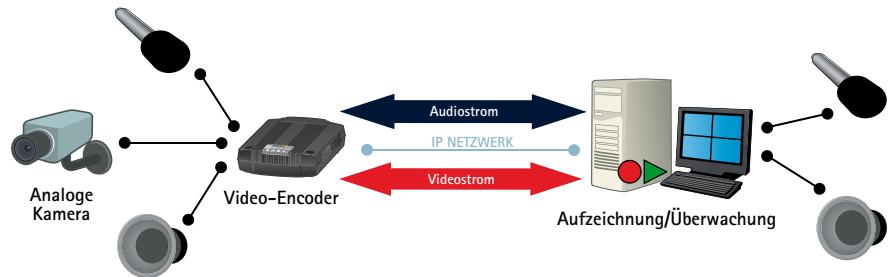


Abbildung 8.2b Einige Video-Encoder sind mit Audiofunktionalität ausgestattet, sodass Audiodaten übertragen werden können, auch wenn in einer Installation analoge Kameras verwendet werden.

Eine Netzwerk-Kamera oder ein Video-Encoder mit integrierter Audiofunktionalität enthält oftmals ein integriertes Mikrofon und/oder einen Mikro-Eingang/Line-Eingang. Ist ein Mikro-Eingang/Line-Eingang vorhanden, haben Benutzer die Möglichkeit, ein anderes, ggf. hochwertigeres Mikrofon zu verwenden, was beispielsweise eine spezielle Richtcharakteristik oder Empfindlichkeit aufweist. Außerdem ist es möglich, mehrere Mikrofone an das Netzwerk-Videoproduct anzuschließen oder das Mikrofon weiter von der Kamera entfernt aufzustellen. Das Mikrofon sollte immer so nah wie möglich an der Geräusquelle aufgestellt werden, um das Rauschen zu reduzieren. Im Zweiwege-Modus (Vollduplex) sollte ein Mikrofon in einiger Entfernung vom Lautsprecher und von diesem wegzeigend aufgestellt werden, um eine Rückkopplung zu vermeiden.

Viele Netzwerk-Videoprodukte von Axis enthalten keine integrierten Lautsprecher. Ein aktiver Lautsprecher, d. h. ein Lautsprecher mit integriertem Verstärker, kann direkt an das Netzwerk-Videoprodukt mit Audio-Unterstützung angeschlossen werden. Wenn ein Lautsprecher keinen integrierten Verstärker hat, muss er an einen Verstärker angeschlossen werden, der dann mit der Netzwerk-Kamera/dem Video-Encoder verbunden wird.

Zur Minimierung von Störungen und Rauschen sollten immer abgeschirmte Audiokabel verwendet werden. Außerdem sollten Audiokabel nicht neben Stromkabeln und Kabeln, die hochfrequente Schaltsignale übertragen, verlegt werden. Audiokabel sollten so kurz wie möglich sein. Wenn ein langes Audiokabel benötigt wird, sollten Balanced-Audio-Geräte, d. h. ausbalancierte Kabel, Verstärker und Mikrofone verwendet werden, um das Rauschen zu reduzieren.

8.3 Audiomodi

Je nach Verwendungszweck besteht möglicherweise die Anforderung, Audiodaten nur in eine (Simplex) oder in beide Richtungen (Duplex) zu senden. Im Duplexmodus können Audiodaten entweder gleichzeitig in beide Richtungen (Vollduplex) oder immer nur in jeweils eine Richtung gesendet (Halbduplex) werden.

8.3.1 Simplex



Abbildung 8.3a Im Simplexmodus werden Audiodaten nur in eine Richtung übertragen. In diesem Fall werden die Audiodaten von der Kamera an den Bediener gesendet. Zu den Verwendungszwecken gehören die Fernüberwachung und die Videoüberwachung.



Abbildung 8.3b In diesem Beispiel für den Simplexmodus werden Audiodaten vom Bediener an die Kamera gesendet. Dieser Modus kann zum Beispiel verwendet werden, um einer von der Kamera erfassten Person mündliche Anweisungen zu erteilen oder einen potentiellen Autodieb von einem Parkplatz zu verscheuchen.

8.3.2 Halbduplex



Abbildung 8.3c Im Halbduplexmodus werden Audiodaten in beide Richtungen übertragen, die Übertragung ist jedoch immer nur in eine Richtung gleichzeitig möglich. Dies ist ähnlich wie bei der Kommunikation über ein Walkie-Talkie.

8.3.3 Full duplex



Abbildung 8.3d In full-duplex mode, audio is sent to and from the operator simultaneously. This mode of communication is similar to a telephone conversation. Full duplex requires that the client PC has a sound card with support for full-duplex audio.

8.4 Audioerkennungsalarm

Der Audioerkennungsalarm kann ergänzend zur Videobewegungserkennung verwendet werden, da er auf Ereignisse in völlig dunklen Bereichen reagieren kann, die von der Videobewegungserkennungsfunktion nicht mehr erfasst werden können. Er kann auch zum Erkennen von Aktivitäten in Bereichen außerhalb des Sichtfelds der Kamera verwendet werden.

Wenn Geräusche wie z. B. das Zerbrechen eines Fensters oder Stimmen in einem Raum erkannt werden, können bestimmte Reaktionen ausgelöst werden, beispielsweise das Senden und Aufzeichnen von Video- und Audiodaten, das Senden von E-Mail- oder anderen Benachrichtigungen und das Aktivieren von externen Geräten wie etwa Alarmsirenen. Gleichermaßen können alarmrelevante Ereignisse wie die Bewegungserkennung oder Türkontakte zum Auslösen von Video- und Audioaufzeichnungen verwendet werden. In einer PTZ-Kamera oder PTZ-Dome-Kamera kann der Audioerkennungsalarm veranlassen, dass die Kamera automatisch auf eine bestimmte Stelle ausgerichtet wird, z. B. ein Fenster.

8.5 Audiokomprimierung

Analoge Audiosignale müssen mittels eines Sampling-Prozesses in digitale Audiodaten konvertiert und dann komprimiert werden, um das Datenvolumen für eine effiziente Übertragung und Speicherung zu reduzieren. Die Konvertierung und Komprimierung wird mithilfe eines Audio-Codecs ausgeführt. Dies ist ein Algorithmus, der Audiodaten codiert und decodiert.

8.5.1 Sampling-Frequenz

Es gibt viele verschiedene Audio-Codecs, die unterschiedliche Sampling-Frequenzen und Komprimierstufen unterstützen. Die Sampling-Frequenz gibt an, wie viel Mal pro Sekunde das Sample eines analogen Audiosignals abgetastet wird. Sie wird in Hertz (Hz) angegeben. Generell gilt: Je höher die Sampling-Frequenz, desto besser ist die Audioqualität und desto mehr Bandbreite und Speicherplatz werden benötigt.

8.5.2 Bitrate

Die Bitrate ist bei der Audiofunktion eine wichtige Einstellung, da sie die Komprimierstufe und damit die Audioqualität festlegt. Generell gilt: Je höher die Komprimierstufe, desto niedriger die Bitrate und desto schlechter ist allerdings die Audioqualität. Die Unterschiede bei der Audioqualität von Codecs sind vor allem bei hohen Komprimierstufen (niedrigen Bitraten) bemerkbar, nicht jedoch bei niedrigen Komprimierstufen (hohen Bitraten). Höhere Komprimierstufen können auch eine höhere Latenz (Verzögerung) bewirken, allerdings ermöglichen sie auch größere Einsparungen bei der Bandbreite und dem Speicherplatz.

Die bei Audio-Codecs am häufigsten gewählten Bitraten liegen zwischen 32 kBit/s und 64 kBit/s. Audio-Bitraten sind wie Video-Bitraten ein wichtiger zu berücksichtigender Faktor, wenn es um die Berechnung der Bandbreiten- und Speicheranforderungen geht.

8.5.3 Audio-Codecs

Netzwerk-Videoprodukte von Axis unterstützen drei Audio-Codecs. Der erste ist AAC-LC (Advanced Audio Coding - Low Complexity), auch als MPEG-4 AAC bekannt. Für diesen Codec ist eine Lizenz erforderlich (siehe Abschnitt 7.2.2). AAC-LC wird besonders bei einer Sampling-Rate von 16 kHz oder höher und einer Bitrate von 64 kBit/s empfohlen, wenn die bestmögliche Audioqualität erforderlich ist. Die anderen beiden Codecs sind G.711 und G.726, für die keine Lizenzen erforderlich sind.

8.6 Audio- und Videosynchronisierung

Die Synchronisierung von Audio- und Videodaten erfolgt mittels eines Media Players (einem Softwareprogramm zum Abspielen von Multimedia-Daten) oder eines Multimedia-Frameworks wie Microsoft DirectX, einer Sammlung aus APIs (Application Programming Interface), die Multimedia-Daten verarbeiten.

Audio- und Videodaten werden in separaten Datenpaketströmen über ein Netzwerk gesendet. Damit ein Client oder Player die Audio- und Videoströme perfekt synchronisieren kann, müssen die Audio- und Videodatenpakete mit einem Zeitstempel versehen werden. Das Versehen von Videodatenpaketen mit Zeitstempeln mithilfe der Motion JPEG-Komprimierung wird nicht von allen Netzwerk-Kameras unterstützt. Wenn dies der Fall ist, Sie aber synchronisierte Video- und Audiodaten benötigen, muss MPEG-4 oder H.264 als Videoformat gewählt werden, da solche Videoströme zusammen mit den Audioströmen unter Verwendung von RTP (Real-time Transport Protocol) gesendet werden. Dieses Protokoll versieht die Video- und Audiopakete mit einem Zeitstempel. Es gibt aber auch viele Situationen, in denen eine Audiosynchronisierung nicht wichtig oder sogar unerwünscht ist (zum Beispiel, wenn der Ton überwacht, aber nicht aufgezeichnet werden soll).

Netzwerktechnologien

Es werden verschiedene Netzwerktechnologien verwendet, die die Nutzung der vielen Vorteile eines Netzwerk-Videosystems möglich machen. In diesem Kapitel werden zunächst die Funktionsweise eines lokalen Netzwerks (LAN, Local Area Network), insbesondere eines Ethernet-Netzwerks, sowie die zugehörigen Komponenten erläutert. Auch die Verwendung von Power over Ethernet wird beschrieben.

Anschließend werden die Internet-Kommunikation, die Bedeutung und Funktionsweise von IP-Adressen (IP = Internet Protocol) sowie der Zugriff auf Netzwerk-Videoprodukte über das Internet behandelt. Es wird auch ein Überblick über die bei Netzwerk-Video verwendeten Datentransportprotokolle gegeben. Weitere in diesem Kapitel behandelte Themen betreffen virtuelle LANs und Quality of Service sowie die verschiedenen Methoden zur Sicherung der Kommunikation über IP-Netzwerke. *Weitere Informationen über Drahtlosechnologien finden Sie in Kapitel 10.*

9.1 LAN und Ethernet

Bei einem lokalen Netzwerk (LAN) handelt es sich um eine Gruppe von Computern, die in einem lokal begrenzten Bereich miteinander verbunden sind, um miteinander kommunizieren und andere Ressourcen wie z. B. Drucker gemeinsam nutzen zu können. Daten werden in Form von Paketen gesendet. Für die Übertragung dieser Pakete können verschiedene Technologien genutzt werden. Die gängigste LAN-Technologie ist das Ethernet, das in dem IEEE-802.3-Standard definiert ist. (Weitere LAN-Netzwerktechnologien sind beispielsweise „Token-Ring“ und „FDDI“, die heute allerdings kaum noch eine Bedeutung haben.)

Ethernet verwendet eine Sterntopologie, in der einzelne Knoten (Geräte) über aktive Netzwerkgeräte wie beispielsweise Switches miteinander vernetzt sind. Die Anzahl der vernetzten Geräte in einem LAN kann zwischen zwei und mehreren tausend betragen. Die Übertragung in einem drahtgebundenen LAN erfolgt in der Regel über Twisted-Pair- oder Glasfaserkabel. Ein Twisted-Pair-Kabel besteht aus acht Adern, wobei jeweils zwei Adern miteinander verdrillt sind, so dass vier Adernpaare zur Verfügung stehen. Als Anschlusstechnologie werden RJ-45-Stecker und -Buchsen verwendet. Die maximale Länge eines Twisted-Pair-Segments beträgt 100 m, dass

sich aus 90 m massiven und fest verlegten sowie 10 m flexiblen Kabel zusammen setzt. Glasfaserkabel können je nach Glasfasertyp hingegen eine maximale Länge von 10 bis 70 km haben. Abhängig vom verwendeten Twisted-Pair- oder Glasfaserkabeltyp betragen die Datenraten heutzutage zwischen 10 MBit/s und 10.000 MBit/s (10 GBit/s).

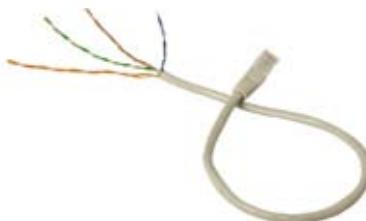


Abbildung 9.1a Twisted-Pair-Kabel bestehend aus vier Paaren verdrillter Adern, die am Ende eines RJ-45-Steckers miteinander verbunden sind.

Es ist eine Faustregel, immer ein Netzwerk aufzubauen, das eine größere Kapazität hat als gegenwärtig erforderlich. Für ein zukunftssicheres Netzwerk ist es sinnvoll, ein Netzwerk einzurichten, von dem nur 30 % der Gesamtkapazität genutzt werden. Da heutzutage immer mehr Anwendungen über Netzwerke ausgeführt werden, ist eine immer höhere Netzwerkleistung erforderlich. Während Netzwerk-Switches (siehe Beschreibung weiter unten) sich nach einigen Jahren leicht aktualisieren lassen, ist der Austausch von Kabeln meist ein aufwendigeres Unterfangen.

9.1.1 Ethernet-Netzwerke

Fast Ethernet

Fast Ethernet ist ein Ethernet-Netzwerk, das Daten mit einer Datenrate von 100 MBit/s übertragen kann. Für dieses Netzwerk können Twisted-Pair- oder Glasfaserkabel verwendet werden. (Das ältere 10-MBit/s-Ethernet ist weiterhin im Einsatz, bietet aber für manche Netzwerk-Videoanwendungen nicht die erforderliche Bandbreite.) Die meisten Geräte, die über ein Netzwerk verbunden sind, z. B. Laptops oder Netzwerk-Kameras, sind mit einer 100BASE-TX/10BASE-T-Ethernet-Schnittstelle oder kurz „10/100-Schnittstelle“ ausgestattet, die sowohl 10-MBit/s-Ethernet als auch Fast Ethernet unterstützt. Der Twisted-Pair-Kabeltyp, der Fast Ethernet unterstützt, ist das Cat-5-Kabel.

Gigabit Ethernet

Gigabit Ethernet, für das ebenfalls ein Twisted-Pair- oder ein Glasfaserkabel verwendet werden kann, bietet Datenraten von 1.000 MBit/s (1 Gbit/s) und wird immer häufiger verwendet. Man geht davon aus, dass es Fast Ethernet als Standard bald ablösen wird. Der für das Gigabit Ethernet erforderliche Twisted-Pair-Kabeltyp ist das Cat-5e-Kabel, in dem alle vier verdrillten Drahtpaare verwendet werden, um die hohen Datenraten zu erzielen. Für Netzwerk-Videosysteme werden Cat-5e- oder höherwertige Kabel empfohlen. Die meisten Schnittstellen sind abwärtskompatibel mit 10- und 100-MBit/s-Ethernet und werden üblicherweise „10/100/1000-Schnittstellen“ genannt.

Für Übertragungen über längere Distanzen 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).



Abbildung 9.1b Größere Distanzen können mit Glasfaserkabeln überwunden werden. Glasfaser wird in der Regel in den Hauptleitungen eines Netzwerks und nicht in Knoten wie z. B. einer Netzwerk-Kamera verwendet.

10-Gigabit-Ethernet

Das 10-Gigabit-Ethernet ist die neueste Netzwerkgeneration. Es liefert Datenraten von 10 GBit/s (10.000 MBit/s) und es können Glasfaser- oder Twisted-Pair-Kabel verwendet werden. 10GBASE-LX4, 10GBASE-ER und 10GBASE-SR können bei Verwendung von Glasfaserkabeln Distanzen von bis zu 10.000 m überwinden. Bei einer Twisted-Pair-Lösung sind äußerst hochwertige Kabel erforderlich (Cat-6a oder Cat-7). 10-GBit/s-Ethernet wird vor allem für das Backbone von High-End-Anwendungen verwendet, die hohe Datenraten erfordern.

9.1.2. Switch

Wenn nur zwei Geräte über ein Twisted-Pair-Kabel direkt miteinander kommunizieren müssen, kann ein so genanntes Crossover-Kabel verwendet werden. Das Crossover-Kabel kreuzt das sendende Adernpaar an einem Ende des Kabels mit dem empfangenden Adernpaar am anderen Ende und umgekehrt.

Für die Vernetzung mehrerer Geräte in einem LAN sind jedoch Netzwerkgeräte wie beispielsweise ein Netzwerk-Switch erforderlich. Bei Einsatz eines Netzwerk-Switches wird ein normales 1:1-Netzwerkkabel anstelle eines Crossover-Kabels verwendet.

Die Hauptfunktion eines Netzwerk-Switches besteht in der Weiterleitung von Daten von einem Gerät zu einem anderen im selben Netzwerk. Dies erfolgt auf effiziente Weise, da Daten direkt von einem Gerät an ein anderes geleitet werden können, ohne dass hiervon das gesamte Netzwerk belastet wird.

Ein Switch registriert die MAC-Adressen (MAC = Media Access Control) aller Geräte, die mit ihm verbunden sind. (Jedes Netzwerkgerät hat eine eindeutige MAC-Adresse, die aus einer Reihe von Ziffern und Buchstaben besteht, die der Hersteller vorgibt. Die Adresse steht meist auf dem Typenschild des Produktes und entspricht der Seriennummer.) Wenn ein Switch Daten empfängt, leitet er diese nur an den Anschluss weiter, der mit dem Gerät verbunden ist, das die richtige MAC-Zieladresse aufweist.

Die Leistung von Switches wird in der Regel in Anschluss-Anschluss-Raten und durch die Backplanekapazität angegeben (ersteres in Pakete pro Sekunde und letzteres in Bit-Raten pro Sekunde). Hierbei gilt, dass ein Switch mit der höheren Anzahl von Datenpakete pro Sekunde und Backplanekapazität eine höhere Performance aufweist. Des Weiteren wird ein Switch oftmals über die maximalen Datenraten der Anschlüsse beschrieben. Ein 100-MBit/s-Switch verfügt beispielsweise über mehrere Anschlüsse mit 100 MBit/s, also diese Angabe bezieht sich nur auf einen einzelnen Anschluss.

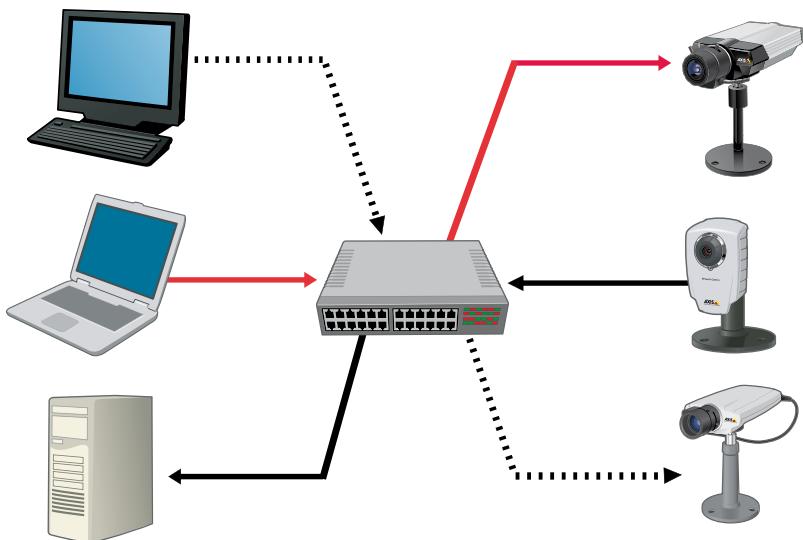


Abbildung 9.1c Bei einem Netzwerk-Switch werden Daten sehr effizient übertragen, da der Datenverkehr direkt von einem Gerät zu einem anderen geleitet werden kann, ohne dass andere Anschlüsse auf dem Switch davon betroffen sind.

Ein Netzwerk-Switch unterstützt normalerweise mehrere verschiedene Datenraten gleichzeitig. Die gängigsten Datenraten sind 10/100, bei denen sowohl das 10-MBit/s-Ethernet als auch das Fast Ethernet unterstützt wird. Jedoch werden immer häufiger 10/100/1000er Datenraten als Standard-Switch verwendet, die also je nach angeschlossenen Gerät 10-MBit/s-Ethernet, Fast Ethernet und Gigabit Ethernet unterstützen. Ein Switch ermöglicht es zudem, dass ein angeschlossenes Gerät im Vollduplex-Modus arbeitet, d. h. Daten gleichzeitig senden und empfangen kann, was eine höhere Leistung mit sich bringt. Alternativ kann auch im Halbduplexmodus gearbeitet werden. Die Datenrate und der Übertragungsmodus zwischen einem Anschluss auf dem Switch und einem angeschlossenen Gerät werden üblicherweise durch automatische Aushandlung festgelegt, der so genannten Auto-Negotiation-Funktion, wobei die höchste gemeinsame Datenrate und der beste Übertragungsmodus automatisch ausgehandelt und eingestellt werden.

Switches können zusätzlich mit unterschiedlichen Eigenschaften oder Funktionen ausgestattet sein. Einige Switches bieten die Funktion eines Routers (siehe Abschnitt 9.2) und werden in

diesem Fall als Layer-3-Switche bezeichnet. Außerdem kann ein Switch Unterstützung für Power over Ethernet bieten, d.h. Endgeräte mit Strom versorgen. Des Weiteren gibt es Switches mit Quality of Service Unterstützung (siehe Abschnitt 9.4), worüber eine priorisierte Datenweiterleitung erfolgen kann, und festgelegt werden kann, wie viel Bandbreite den verschiedenen Anwendungen zur Verfügung stehen.

9.1.3 Power over Ethernet

Power over Ethernet (PoE) bietet die Möglichkeit, an das Ethernet-Netzwerk angeschlossene Geräte über das Netzwerkkabel, das für die Datenübertragung genutzt wird, auch mit Strom zu versorgen. Power over Ethernet wird überwiegend für die Stromversorgung von IP-Telefonen, WLAN Access Points und Netzwerk-Kameras verwendet. Der Hauptvorteil von PoE sind die Kostenersparnisse. Die Beauftragung eines ausgebildeten Elektrikers und das Verlegen einer eigenen Stromleitung sind nicht erforderlich. Dies ist insbesondere in schwer zugänglichen Bereichen von Vorteil. Die Tatsache, dass kein Stromkabel verlegt werden muss, kann je nach Standort der Kamera mehrere hundert Euro pro Kamera einsparen. Mit PoE ist es zudem einfacher, den Standort einer Kamera zu verlegen oder weitere Kameras zum Videoüberwachungssystem hinzuzufügen.

Darüber hinaus kann mit der Hilfe von PoE ein Videosystem gegen Spannungsausfälle abgesichert werden. Ein Videoüberwachungssystem mit PoE kann vom Serverraum aus mit Strom versorgt werden. Der Serverraum wird häufig durch eine USV (Unterbrechungsfreie Stromversorgung) gesichert. Dies bedeutet, dass das Videoüberwachungssystem auch bei einem Ausfall der Spannungsversorgung funktionsfähig bleibt. Aufgrund seiner Vorteile wird die Verwendung von PoE bei so vielen Geräten wie möglich empfohlen. Der vom PoE-fähigen Switch oder Midspan gelieferte Strom sollte für die angeschlossenen Geräte ausreichen und die Geräte sollten die Spannungsklassifizierung unterstützen. Diese werden in den nachfolgenden Abschnitten im Detail erläutert.

802.3af-Standard und High-PoE

Die meisten derzeit erhältlichen PoE-Geräte erfüllen die Anforderungen des IEEE-802.3af-Standards, der im Jahr 2003 veröffentlicht wurde. Der IEEE-802.3af-Standard verwendet Cat-5- oder höherwertigere Kabel und gewährleistet, dass die Datenübertragung nicht beeinträchtigt wird. In der Standardbeschreibung wird das Gerät, das den Strom liefert, als „Power Sourcing Equipment“ (PSE) bezeichnet. Als PSE kommt entweder ein PoE-fähiger Switch oder so genannter Midspan in Frage. Bei einem Midspan handelt es sich um ein Gerät, welches in das Netzwerksegment zwecks Stromversorgung zwischengeschaltet werden kann. Auf diese Weise lassen sich bereits vorhandene Infrastrukturen, in denen noch keine PoE-fähigen Switches installiert sind, auf das PoE-Feature erweitern. Das Gerät, das mit Strom versorgt wird, wird als „Powered Device“ (PD) bezeichnet. Die Funktionalität wird normalerweise in ein Netzwerkgerät wie eine Netzwerk-Kamera integriert oder über einen eigenständigen Splitter (siehe Abschnitt unten) bereitgestellt.

Die Abwärtskompatibilität mit nicht PoE-kompatiblen Netzwerkgeräten ist gewährleistet. Der Standard umfasst eine Methode, mit der automatisch geprüft wird, ob ein Gerät PoE unterstützt. Nur wenn dies der Fall ist, wird auf dem Anschluss des Switches oder Midspan die Versorgungsspannung aufgeschaltet.

Ein Twisted-Pair-Kabel enthält vier Adernpaare von denen bei der Datenübertragung bis 100 MBit/s nur zwei Adernpaare für die Datenübertragung verwendet werden. PoE kann entweder die beiden nicht genutzten Adernpaare verwenden oder die beiden Adernpaare, welche auch für die Datenübertragung verwendet werden. Switches verwenden in der Regel die Adernpaare, die auch für die Datenübertragung genutzt werden, während Midspans die beiden ungenutzten Adernpaare verwenden. Ein PD unterstützt immer beide Möglichkeiten. Gemäß IEEE 802.3af liefert ein PSE pro Anschluss eine maximale Leistung von 15,4 W, die über eine Spannung von 48 V eingespeist wird. Angesichts des Leistungsverlustes bei einem Twisted-Pair-Kabel mit maximaler Länge werden bei einem PD jedoch nur 12,95 W garantiert. Der IEEE-802.3af-Standard gibt verschiedene Leistungskategorien für PDs an.

PSEs, wie Switches und Midspans, liefern normalerweise eine bestimmte Menge an Leistung, in der Regel 300 bis 500 W. Bei einem 48-Port-Switch sind das 6 bis 10 W pro Anschluss, wenn alle Anschlüsse mit PoE-fähigen Geräten verbunden sind. Sofern die PDs keine Stromklassifizierung unterstützen, müssen die kompletten 15,4 W für jeden Anschluss reserviert werden, der PoE verwendet. Dies bedeutet, dass ein 300-W-Switch eine Spannungsversorgung nur an 19 der 48 Anschlüsse liefern kann. Wenn jedoch alle Geräte dem Switch mitteilen, dass sie Klasse-1-Geräte sind, kann der 300-W-Switch alle 48 Ports mit Spannung versorgen.

Klasse	Mindeststromstärke bei PSE	Maximale Stromstärke bei PD	Verwendung
0	15,4 W	0,44 W bis 12,95 W	Standard
1	4,0 W	0,44 W bis 3,84 W	optional
2	7,0 W	3,84 W bis 6,49 W	optional
3	15,4 W	6,49 W bis 12,95 W	optional
4	Als Klasse 0 behandeln		Für künftige Nutzung reserviert

Tabelle 9.1a Stromklassifizierungen gemäß IEEE 802.3af.

Die meisten fest ausgerichteten Netzwerk-Kameras können über PoE gemäß dem IEEE-802.3af-Standard mit Strom versorgt werden und entsprechen in der Regel einem Gerät der Klasse 1 oder 2. Mit dem IEEE 802.3at-Pre-Standard oder PoE+ wird die eingespeiste Leistung auf 30 W erhöht und für das PD stehen 25,5 W zur Verfügung. Die Stromversorgung erfolgt ebenfalls über zwei Adernpaare. Es ist zu erwarten, dass der IEEE-802.3at-Standard Mitte 2009 verabschiedet. In der Zwischenzeit können dem IEEE 802.3at-Pre-Standard (High PoE) entsprechende Midspans und Splitter für Geräte wie PTZ-Kameras und PTZ-Dome-Kameras mit Motorsteuerung sowie für Kameras mit Heizelementen und Lüftern verwendet werden, die mehr Leistung benötigen, als mit dem IEEE-802.3af-Standard geliefert werden kann.

Midspans und Splitter

Midspans und Splitter sind Geräte, über die die PoE-Stromversorgung auf vorhanden Netzwerkinfrastrukturen nachträglich aufgesetzt werden kann.

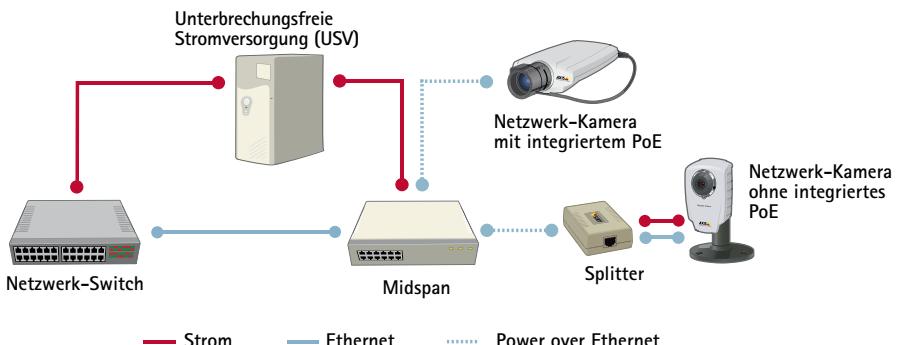


Abbildung 9.1d Ein vorhandenes System kann mithilfe eines Midspans oder eines Splitters um die PoE-Funktionalität erweitert werden.

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, ist es wichtig daran zu denken, dass die maximale Entfernung zwischen der Datenquelle (z. B. dem Switch) und den Netzwerk-Videoprodukten nicht mehr als 100 m betragen darf. Das heißt, der Midspan und der oder die aktiven Splitter müssen innerhalb der Entfernung von 100 m platziert werden.

Ein Splitter wird verwendet, um den Strom- und Datenpfad aufzutrennen und auf zwei separate Anschlüsse aufzuteilen, die dann an ein Endgerät angeschlossen werden können, das keine integrierte Unterstützung für PoE bietet. Bei der Auswahl des Splitters muss darauf geachtet werden, dass die Ausgangsspannung des Splitters mit der Versorgungsspannung des Endgerätes übereinstimmt. PoE- und High-PoE-Midspans und -Splitter sind von Axis erhältlich.

9.2 Das Internet

Um Daten von einem Gerät in einem lokalen Netzwerk an ein Gerät in einem anderen LAN zu senden, muss eine Standardkommunikationsmethode verwendet werden, da die lokalen Netzwerke möglicherweise unterschiedliche Technologien verwenden. Dieses Erfordernis führte zu der Entwicklung von IP-Adressen und den vielen IP-basierten Protokollen für die Kommunikation im Internet, bei dem es sich um ein globales System miteinander verbundener Computernetzwerke handelt. (LANs können IP-Adressen und IP-Protokolle auch für die Kommunikation innerhalb des LAN verwenden, obwohl für die interne Kommunikation die MAC-Adressen völlig ausreichen.) Vor der Erläuterung der IP-Adressen werden zunächst einige grundlegende Elemente der Internet-Kommunikation erörtert, z. B. Router, Firewalls und Internetdienstanbieter.

Router

Zum Weiterleiten von Datenpaketen von einem LAN über das Internet zu einem anderen LAN wird ein so genannter Netzwerk-Router benötigt. Ein Router leitet Informationen auf der Basis von IP-Adressen von einem Netzwerk zu einem anderen weiter. Er leitet nur Datenpakete weiter,

die an ein anderes Netzwerk adressiert sind. Ein Router wird am häufigsten für die Verbindung eines lokalen Netzwerks mit dem Internet verwendet

Firewalls

Eine Firewall hat die Aufgabe, den unbefugten Zugriff auf ein privates Netzwerk zu verhindern. Firewalls können in Hardware und/oder in Software implementiert werden. Sie werden in der Regel verwendet, um unbefugte Internet-Nutzer am Zugriff auf private, mit dem Internet verbundene Netzwerke zu hindern. Nachrichten in oder aus dem Internet passieren die Firewall, die alle Nachrichten prüft und jene blockiert, die nicht den festgelegten Sicherheitskriterien entsprechen.

Internetverbindungen

Für die Verbindung eines LAN mit dem Internet muss eine Netzwerkverbindung über einen Internetdienstanbieter hergestellt werden. Bei Verbindungen mit dem Internet werden Begriffe wie „Upstream“ und „Downstream“ verwendet. „Upstream“ beschreibt die Transferrate, mit der Daten von dem Gerät in das Internet hochgeladen werden, beispielsweise wenn Videodateien von einer Netzwerk-Kamera gesendet werden. „Downstream“ beschreibt die Transferrate für das Herunterladen von Dateien, z. B. wenn Videodateien von einem Überwachungs-PC empfangen werden. In den meisten Situationen – z. B. wenn ein Laptop mit dem Internet verbunden ist – ist die Geschwindigkeit für das Herunterladen von Informationen aus dem Internet der wichtigste Faktor. Bei einer Netzwerk-Videoanwendung mit einer Netzwerk-Kamera an einem entfernten Standort ist jedoch die Upstream-Geschwindigkeit am relevantesten, da die Daten (Video) von der Netzwerk-Kamera in das Internet hochgeladen werden.

9.2.1 IP-Adressierung

Jedes Gerät, das über das Internet mit anderen Geräten kommunizieren möchte, muss eine eindeutige und korrekte IP-Adresse haben. IP-Adressen werden zur Identifizierung der sendenden und empfangenden Geräte verwendet. Es gibt zurzeit zwei IP-Versionen: IP-Version 4 (IPv4) und IP-Version 6 (IPv6). Der Hauptunterschied zwischen diesen beiden Versionen besteht darin, dass eine IPv6-Adresse länger ist (128 Bit verglichen mit 32 Bit bei einer IPv4-Adresse). IPv4-Adressen werden derzeit am häufigsten verwendet.

9.2.1.1 IPv4-Adressen

IPv4-Adressen sind in vier Blöcke gruppiert, die jeweils durch einen Punkt voneinander getrennt sind. Jeder Block stellt eine Zahl zwischen 0 und 255 dar, z. B. 192.168.12.23. Bestimmte Blöcke von IPv4-Adressen sind eigens 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, benötigen eigene, öffentliche IP-Adressen. Eine öffentliche IP-Adresse ist eine von einem Internetdienstanbieter zugeteilte Adresse. Ein Internetdienstanbieter kann entweder eine dynamische IP-Adresse zuteilen, die sich bei jedem Verbindungsaufbau ändern kann, oder eine statische Adresse, die normalerweise nur gegen eine monatliche Gebühr erhältlich ist.

Ports

Eine Portnummer definiert einen bestimmten Dienst oder eine Anwendung, sodass der empfangende Server (z. B. die 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 ohne Wissen des Benutzers zwecks Adressierung automatisch die Portnummer hinzu. Portnummern liegen zwischen 0 und 65.535. Bestimmte Anwendungen verwenden Portnummern, die ihnen von der Internet Assigned Numbers Authority (IANA) vorab zugewiesen wurden. So wird z. B. ein Webserverdienst über HTTP üblicherweise über Port 80 zugeordnet.

IPv4-Adressen festlegen

Damit eine Netzwerk-Kamera oder ein Video-Encoder in einem IP-Netzwerk betrieben werden kann, muss ihr bzw. ihm eine IP-Adresse zugewiesen werden. Eine IPv4-Adresse für ein Netzwerk-Videoproduct von Axis kann auf zweierlei Weise festgelegt werden: erstens automatisch über DHCP (Dynamic Host Configuration Protocol) und zweitens manuell durch Eingabe einer statischen IP-Adresse, einer Subnetzmaske und der IP-Adresse des Standard-Routers. Für die Zuteilung der statischen IP-Adresse kann über das Interface des Netzwerk-Videoproducts oder über ein Verwaltungsprogramm wie z. B. AXIS Camera Management erfolgen.

Ein DHCP-Server verwaltet einen Pool aus IP-Adressen, die er dynamisch einer Netzwerk-Kamera/einem Video-Encoder zuweisen kann. Die Funktion des DHCP-Servers ist auch häufig in einem Router integriert, der die Schnittstelle zum Internet darstellt.

Mit DHCP wird eine IPv4-Adresse wie folgt festgelegt: Wenn eine Netzwerk-Kamera/ein Video-Encoder eine Netzwerkverbindung herstellt, fordert die Kamera bzw. der Encoder eine IP-Adresse von einem DHCP-Server an. Der DHCP-Server antwortet mit einer IP-Adresse, einer Subnetzmaske, IP-Adresse des Standard-Routers und gegebenenfalls weiteren Informationen.

Die Software AXIS Camera Management kann automatisch IP-Adressen suchen und festlegen und den Verbindungsstatus anzeigen. Die Software kann auch zum Zuweisen statischer, privater IP-Adressen für Axis-Netzwerk-Videoproducte verwendet werden. Dies wird empfohlen, wenn eine Videoverwaltungssoftware für den Zugriff auf die Netzwerk-Videoproducte verwendet wird. In einem Netzwerk-Videosystem mit Hunderten von Kameras ist ein Softwareprogramm wie AXIS Camera Management hilfreich, um das System effizient zu verwalten. *Weitere Informationen zur Videoverwaltung finden Sie in Kapitel 11.*

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 ist der Router in der Lage, eine private IP-Adresse eine öffentliche IP-Adresse umzuwandeln. Somit ist es möglich, dass mehrere Clients gemeinsam einen Internetzugang nutzen.

Port forwarding

Möchte man in einem LAN mehrere Netzwerkkameras oder Videoserver betreiben und deren Videos über das Internet darstellen können, so muss eine Möglichkeit geschaffen werden, dass man über den Router und dessen öffentliche IP-Adresse die einzelnen Systeme ansprechen kann. Für dieses Szenarium kann man das so genannte Port Forwarding nutzen, welches heute als Funktionsfeature von den gängigen Routern angeboten wird. Port Forwarding ermöglicht es, Daten über frei wählbare Ports zu Systemen innerhalb eines privaten Netzwerks weiterzuleiten. Ein Router wartet dazu an einem bestimmten Port auf Datenpakete. Wenn Pakete an diesem Port eintreffen, werden sie an ein bestimmtes System, repräsentiert durch eine private IP-Adresse, weitergeleitet. Die eingehenden Datenpakete werden hierbei per Destination NAT, und die ausgehenden Pakete per Source NAT maskiert. Alle Antwortdatenpakete von diesem bestimmten System werden, wenn sie zu einer eingehenden Verbindung gehören, per NAT so verändert, dass es von außen den Anschein hat, als ob der Router die Pakete versenden würde. Für die Systeme im Internet sieht es so aus, als ob der Router die Serverdienste anbietet.

In den Axis Videoprodukten können die Portnummern der einzelnen Dienste umkonfiguriert werden. So ist es beispielsweise möglich, auf den Netzwerkkameras die Portnummer des Webserverdienstes von Port 80 auf private Ports umzustellen. Möchte man mehrere Netzwerkkameras in einem internen Netzwerk betreiben und von außen über das Internet auf die Kameras zugreifen, so muss auf den einzelnen Kameras jeweils eine andere Portnummer für den Webserverdienst konfiguriert werden (siehe folgende Abb.). Des Weiteren muss am Router das Port Forwarding aktiviert und, entsprechend den Kameraeinstellungen, konfiguriert werden.

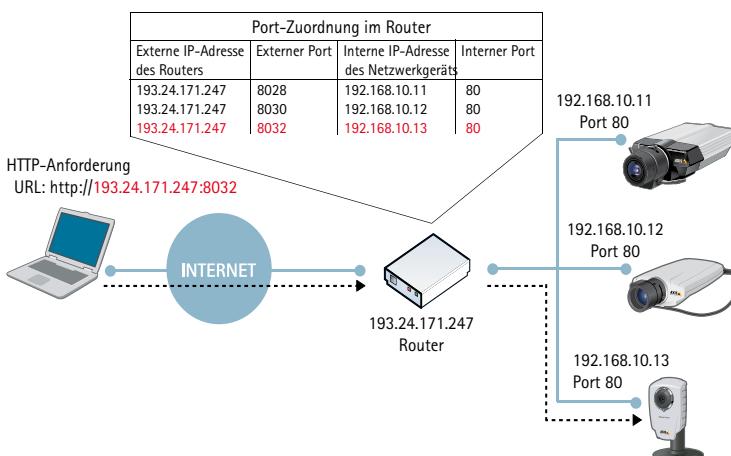


Abbildung 9.2a Dank Port-Forwarding im Router sind Netzwerk-Kameras mit privaten IP-Adressen in einem lokalen Netzwerk über das Internet zugänglich. In dieser Abbildung weiß der Router, dass er Daten (Anforderung), die bei Port 8032 eingehen, an eine Netzwerk-Kamera mit der privaten IP-Adresse 192.168.10.13 Port 80 weiterleiten muss. Die Netzwerk-Kamera kann dann mit dem Senden der Videodaten beginnen.

Beim Port-Forwarding wird in der Regel zuerst der Router konfiguriert. Verschiedene Router führen das Port-Forwarding auf verschiedene Art und Weise durch. Es gibt Websites wie z. B. www.portforward.com, die detaillierte Anweisungen für verschiedene Router enthalten. Meist beinhaltet das Port-Forwarding das Aufrufen der Router-Schnittstelle über einen Internet-Browser und die Eingabe der öffentlichen (externen) IP-Adresse des Routers sowie eine eindeutige Portnummer, die dann für die Anwendung der internen IP-Adresse des spezifischen Netzwerk-Videoproducts und dessen Portnummer zugewiesen werden.

Zur Vereinfachung des Port-Forwardings bietet Axis in vielen seiner Netzwerk-Videoproducte die NAT-Traversal-Funktion an. NAT-Traversal versucht automatisch, die Port-Zuordnung in einem NAT-Router im Netzwerk mithilfe von UPnP™ zu konfigurieren. Auf der Benutzeroberfläche des Netzwerk-Videoproducts können Benutzer manuell die IP-Adresse des NAT-Routers eingeben. Wenn ein Router nicht manuell angegeben wird, sucht das Netzwerk-Videoprodukt automatisch nach NAT-Routern im Netzwerk und wählt den Standardrouter aus. Darüber hinaus wählt der Dienst automatisch einen HTTP-Port aus, wenn manuell keiner angegeben wird.



Abbildung 9.2b Netzwerk-Videoproducte von Axis ermöglichen die Einrichtung von Port-Forwarding mithilfe von NAT-Traversal.

9.2.1.2 IPv6-Adressen

Eine IPv6-Adresse wird in Hexadezimalnotierung 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 an 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, d. h. bei IPv6 ist DHCP nicht mehr für die IP-Adresszuteilung und das manuelle Festlegen der IP-Adressen erforderlich. Auch das Port-Forwarding wird nicht mehr benötigt. Weitere Vorteile von IPv6 sind das erneute Ändern der Nummern, um das Wechseln gesamter Unternehmensnetzwerke zwischen Dienstanbietern zu vereinfachen, ein schnelleres Routing, Punkt-zu-Punkt-Verschlüsselung gemäß IPSec und die Verbindung mit der selben Adresse in wechselnden Netzwerken (Mobile IPv6).

Eine IPv6-Adresse steht in eckigen Klammern in einer URL. Ein bestimmter Port kann wie folgt adressiert werden: [http://\[2001:0da8:65b4:05d3:1315:7c1f:0461:7847\]:8081/](http://[2001:0da8:65b4:05d3:1315:7c1f:0461:7847]:8081/)

Das Festlegen einer IPv6-Adresse für ein Netzwerk-Videoproduct von Axis erfolgt ganz einfach über die Auswahl eines Kontrollkästchens, um IPv6 im Produkt zu aktivieren. Das Produkt erhält daraufhin eine IPv6-Adresse gemäß der Konfiguration im Netzwerk-Router.

9.2.2 Datenübertragungsprotokolle für Netzwerk-Video

Das Transmission Control Protocol (TCP) und das User Datagram Protocol (UDP) sind die IP-Protokolle, die zum Senden von Daten verwendet werden. Diese Übertragungsprotokolle agieren als Träger für viele andere Protokolle. Beispielsweise für HTTP (Hyper Text Transfer Protocol), das zur Darstellung von Webseiten auf Servern überall auf der Welt, die mit dem Internet verbunden sind, verwendet wird.

TCP bietet einen zuverlässige, verbindungsorientierte Datenübertragung. Es sorgt dafür, dass große Datenblöcke in kleinere Pakete aufgeteilt werden, und stellt sicher, dass die gesendeten Daten am Ziel ankommen. TCP-Zuverlässigkeit durch erneute Übertragung kann jedoch signifikante Verzögerungen mit sich bringen. Im Allgemeinen wird TCP verwendet, wenn eine zuverlässige Kommunikation wichtiger ist als die Übertragungsdauer.

UDP ist ein verbindungsloses Übertragungsprotokoll. Es bietet keinerlei Garantie für die erfolgreiche Datenübertragung und überlässt die gesamte Kontrolle und Fehlerprüfung der eigentlichen Anwendung. UDP bietet keine Übertragung von verloren gegangenen Daten, wodurch keine Verzögerungen entstehen.

Protokoll	Übertragungsprotokoll	Anschluss	Allgemeine Verwendung	Netzwerk-Videoverwendung
FTP (File Transfer Protocol)	TCP	21	Übertragung von Dateien über das Internet/Intranet	Die Übertragung von Bildern oder Videodaten von einer Netzwerk-Kamera/einem Video-Encoder auf einen FTP-Server oder an eine Anwendung
SMTP (Send Mail Transfer Protocol)	TCP	25	Protokoll zum Senden von E-Mail-Nachrichten	Eine Netzwerk-Kamera/ein Video-Encoder kann Bilder oder Alarmbenachrichtigungen über den integrierten E-Mail-Client senden.
HTTP (Hyper Text Transfer Protocol)	TCP	80	Wird zum Surfen im Web, d. h. zum Abrufen von Webseiten von Webservern verwendet	Die häufigste Methode für die Videoübertragung von einer Netzwerk-Kamera/einem Video-Encoder, bei der das Netzwerk-Videogerät im Wesentlichen als Webserver agiert und die Videodaten dem anfordernden Benutzer oder Anwendungsserver zur Verfügung stellt.
HTTPS (Hypertext Transfer Protocol over Secure Socket Layer)	TCP	443	Für den sicheren Zugriff auf Webseiten mittels Verschlüsselung	Sichere Übertragung von Videodaten von Netzwerk-Kameras/Video-Encodern.
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-Mediensystemen oder für Videokonferenzen verwendet.	Eine gängige Methode zur Übertragung von H.264/MPEG-basierten Netzwerk-Videodaten sowie für die Synchronisierung von Video und Audio, da RTP sequentielle Nummern und Zeitstempel für Datenpakete verwendet, sodass diese in der korrekten Reihenfolge wieder zusammengesetzt werden können. Die Übertragung kann per Unicast oder Multicast erfolgen.
RTSP (Real Time Streaming Protocol)	TCP	554	Wird zum Einrichten und Steuern von Multimedia-Sitzungen über RTP verwendet.	

Tabelle 9.2a Gängige TCP/IP-Protokolle und Ports, die für Netzwerk-Video verwendet werden.

9.3 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 aber oftmals 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 Separierung in logische Gruppen. Nur Geräte in einer bestimmten Gruppe 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 stellen in der Regel eine bessere und kostengünstigere Lösung dar als ein separates Netzwerk. Das primäre Protokoll, das zum Konfigurieren von VLANs verwendet wird, ist IEEE 802.1Q. Dieses Protokoll kennzeichnet jedes Einzelbild oder Datenpaket mit zusätzlichen Byte, um anzugeben, zu welchem virtuellen Netzwerk das Paket gehört.

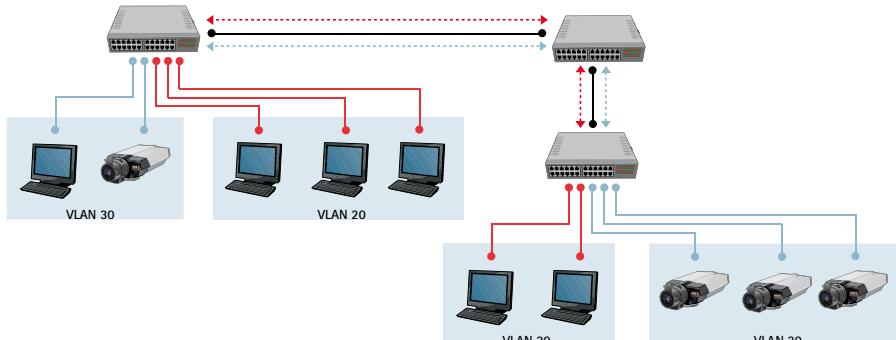


Abbildung 9.3a In dieser Abbildung werden VLANs über mehrere Switches verteilt. Zuerst wird jedes der beiden verschiedenen LANs in VLAN 20 und VLAN 30 segmentiert. Die Verbindungen zwischen den Switches übertragen Daten von verschiedenen VLANs. Nur Geräte desselben VLAN können Daten im selben Netzwerk oder über verschiedene Netzwerke hinweg austauschen. VLANs können verwendet werden, um ein Videonetzwerk von einem Büronetzwerk zu trennen.

9.4 Quality of Service

Da verschiedene Anwendungen, z. B. Telefon, E-Mail und Videoüberwachung, dasselbe Netzwerk verwenden, muss gesteuert werden, wie die Netzwerkressourcen gemeinsam genutzt werden, um die Anforderungen jedes Dienstes zu erfüllen. Eine Lösung besteht darin, beim Datenverkehr im Netzwerk ein unterschiedliches Verhalten von Routern und Switches für unterschiedliche Dienststarts (Sprache, Daten, Video) zuzulassen. Mithilfe von Quality of Service (QoS) können verschiedene Netzwerkanwendungen in einem Netzwerk nebeneinander existieren, ohne sich gegenseitig in der Bandbreitennutzung und in der Verzögerung der Datenübertragung zu beeinflussen.

Der Begriff „Quality of Service“ bezieht sich auf eine Reihe von Technologien wie z. B. Differentiated Service Codepoint (DSCP), die den Datentyp eines Datenpakets identifizieren und die Pakete in Klassen einteilen können, für die unterschiedliche Prioritäten für die Weiterleitung festgelegt werden. Ein Hauptvorteil eines QoS-Netzwerks ist die Fähigkeit, Prioritäten bezüglich des Datenverkehrs zu setzen, damit wichtige Daten vor weniger wichtigen Daten übertragen werden. Ein weiterer Vorteil ist die größere Zuverlässigkeit, indem die Bandbreite, die eine Anwendung nutzen darf, und damit die Verteilung der Bandbreitennutzung zwischen den Anwendungen gesteuert wird. PTZ-Datenverkehr, der häufig als kritisch erachtet wird und keine hohe Latenzzeit aufweisen darf, ist ein typisches Beispiel dafür, wie QoS eingesetzt werden kann, um schnelle Reaktionen auf Bewegungsereignisse zu erzielen. Damit QoS in einem Videonetzwerk verwendet werden kann, müssen alle Switches, Router und Netzwerk-Videoprodukte QoS unterstützen.

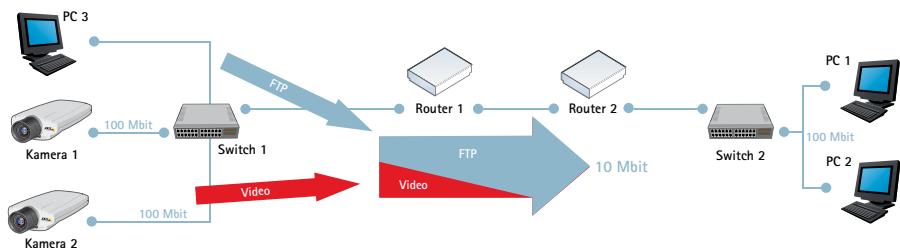


Abbildung 9.4a Gewöhnliches Netzwerk (ohne QoS). In diesem Beispiel überwacht PC1 zwei Videoströme von den Kameras 1 und 2, wobei jede Kamera die Daten mit 2,5 MBit/s überträgt. Plötzlich startet PC2 einen Dateitransfer von PC3. In diesem Beispiel wird versucht, den Dateitransfer mit der kompletten Kapazität von 10 MBit/s zwischen den Routern 1 und 2 zu nutzen, während die Videoströme versuchen, ihre Gesamtrate von 5 MBit/s beizubehalten. Die Menge an Bandbreite, die dem Überwachungssystem zur Verfügung steht, kann nicht mehr gewährleistet werden, und es ist möglich, dass die Video-Bildrate verringert wird. Im schlimmsten Fall verbraucht der FTP-Datentransfer die gesamte verfügbare Bandbreite.

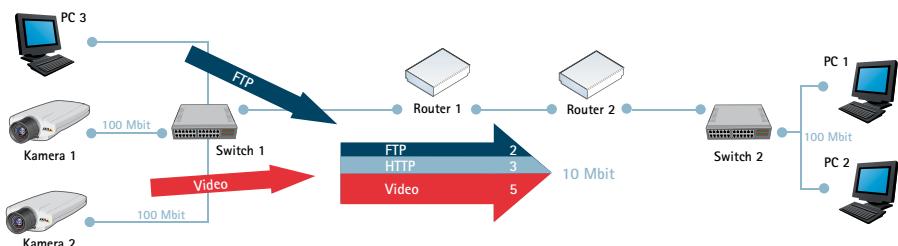


Abbildung 9.4b Netzwerk mit QoS-Funktion. Hier wurde Router 1 so konfiguriert, dass bis zu 5 MBit/s der verfügbaren 10 MBit/s für das Streamen von Videodaten reserviert bleiben. Der FTP-Datenverkehr darf 2 MBit/s nutzen und HTTP, alle anderen Datenübertragungsarten dürfen maximal 3 MBit/s verwenden. Durch diese Aufteilung steht den Videoströmen immer die erforderliche Bandbreite zur Verfügung. Dateitransfers werden als weniger wichtig betrachtet und erhalten somit weniger Bandbreite, es steht aber dennoch Bandbreite zum Surfen im Internet und für anderen Datenverkehr zur Verfügung. Beachten Sie, dass diese Einschränkungen nur gelten, wenn das Netzwerk stark ausgelastet ist. Wenn ungenutzte Bandbreite verfügbar ist, kann diese von jeder Art von Datenverkehr genutzt werden..

9.5 Netzwerksicherheit

Es gibt verschiedene Sicherheitsstufen für das Senden von Informationen über IP-Netzwerke. Die erste ist die Authentifizierung und Autorisierung. Der Benutzer oder das Gerät identifiziert sich selbst im Netzwerk und am entfernten Ende durch Eingabe eines Benutzernamens und eines Kennworts, die überprüft werden, bevor dem Gerät bzw. dem Benutzer der Zugriff auf das System gewährt wird. Zusätzliche Sicherheit kann erreicht werden, indem Daten verschlüsselt werden, damit sie für Dritte nicht lesbar sind. Gängige Verschlüsselungsmethoden sind HTTPS (auch bekannt als SSL/TLS), VPN und WEP oder WPA in drahtlosen Netzwerken (WLANs). (*Weitere Informationen über drahtlose Sicherheit finden Sie in Kapitel 10.*) Die Verwendung von Verschlüsselung kann die Kommunikation verlangsamen. Dies hängt von der Art der Implementierung und der verwendeten Verschlüsselungsmethode ab.

9.5.1 Benutzernamen- und Kennwortauthentifizierung

Die Verwendung der Benutzernamen- und Kennwortauthentifizierung ist die grundlegendste Methode zum Schutz von Daten in einem IP-basierenden Netzwerk. Sie reicht vermutlich aus, wenn keine hohen Sicherheitsstufen erforderlich sind oder wenn das Videonetzwerk vom Hauptnetzwerk abgetrennt wurde und unbefugte Benutzer keinen Zugriff auf das Videonetzwerk haben. Die Kennwörter können beim Senden verschlüsselt oder unverschlüsselt sein. Mehr Sicherheit wird durch eine Verschlüsselung erzielt. Netzwerk-Videoprodukte von Axis bieten einen mehrstufigen Kennwortschutz. Es stehen drei Stufen zur Verfügung: Administrator (Vollzugriff auf alle Funktionen), Bediener (Zugriff auf alle Funktionen außer die Konfigurationsseiten), Beobachter (Zugriff nur auf Live-Video).

9.5.2 IP-Adressfilterung

Netzwerk-Videoprodukte von Axis bieten IP-Adressfilterung, wodurch definierten IP-Adressen der Zugriff gewährt oder verweigert wird. In einer typischen Konfiguration lassen Netzwerk-Kameras nur den Zugriff der IP-Adresse des Servers zu, auf dem sich die Videoverwaltungssoftware für den Zugriff auf die Netzwerk-Videoprodukte befindet.

9.5.3 IEEE 802.1X

Viele Axis-Netzwerk-Videoprodukte unterstützen IEEE 802.1X, das die Authentifizierung von Geräten ermöglicht, die an einen LAN-Port angeschlossen sind. 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 so genannte „Port-Hijacking“, d. h. den Zugriff eines unbefugten Computers auf ein Netzwerk durch Zugriff auf eine Netzwerkbuchse innerhalb oder außerhalb eines Gebäudes. IEEE 802.1X ist bei Netzwerk-Videoanwendungen hilfreich, da sich Netzwerk-Kameras oftmals in öffentlichen Bereichen befinden und eine frei zugängliche Netzwerkbuchse gegebenenfalls ein Sicherheitsrisiko darstellen kann. In heutigen Unternehmensnetzwerken ist IEEE 802.1X eine grundlegende Anforderung für alle Geräte, die mit dem Netzwerk verbunden werden. In einem Netzwerk-Videosystem kann IEEE 802.1X wie folgt funktionieren: 1.) Eine Netzwerk-Kamera sendet eine Netzwerkzugriffsanforderung an einen Switch oder Zugriffspunkt. 2.) Der Switch oder Zugriffspunkt leitet die Anforderung an einen Authentifizierungsserver weiter, z. B. 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 oder Zugriffspunkt an, den Port zu öffnen, damit die Nutzdaten der Netzwerk-Kamera den Switch passieren und über das Netzwerk gesendet werden können.

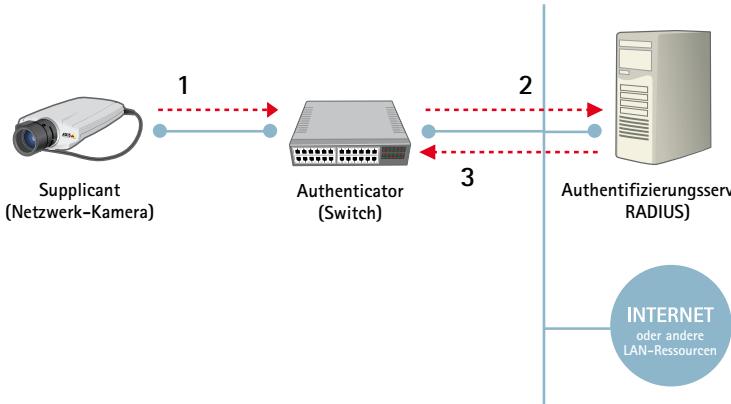


Abbildung 9.5a IEEE 802.1X bietet portbasierte Sicherheit und umfasst einen Supplicant (z. B. eine Netzwerk-Kamera), einen Authenticator (z. B. einen Switch) und einen Authentifizierungsserver. Schritt 1: Netzwerkzugriff wird angefordert. Schritt 2: Anforderung wird an Authentifizierungsserver weitergeleitet. Schritt 3: Die Authentifizierung ist erfolgreich und der Switch wird angewiesen, der Netzwerk-Kamera das Senden von Nutzdaten über das Netzwerk zu erlauben.

9.5.4 HTTPS oder SSL/TLS

HTTPS (Hyper Text Transfer Protocol Secure) ist mit HTTP identisch, jedoch mit einem wesentlichen Unterschied: die übertragenen Daten werden mit Secure Socket Layer (SSL) oder Transport Layer Security (TLS) verschlüsselt. Diese Sicherheitsmethode wendet die Verschlüsselung auf die Daten selbst an. Viele Netzwerk-Videoprodukte von Axis bieten Unterstützung für HTTPS, wodurch es möglich ist, Videobilder sicher über ein Netzwerk zu übertragen und einen Webbrowser anzuzeigen.

9.5.5 VPN (Virtual Private Network)

Mit VPN kann ein sicherer „Tunnel“ zwischen zwei miteinander kommunizierenden Geräten erstellt werden, der eine sichere Kommunikation über das Internet ermöglicht. Bei einem VPN wird das Originalpaket einschließlich der Daten und der Kopfzeile, die Informationen wie die Quell- und Zieladresse, den Typ der gesendeten Informationen, die Paketnummer der Paketsequenz sowie die Paketlänge enthalten kann, verschlüsselt. Das verschlüsselte Paket wird dann in einem weiteren Paket gekapselt, das nur die IP-Adressen der beiden kommunizierenden Geräte (Router) zeigt. Diese Vorgehensweise schützt den Datenverkehr und seinen Inhalt vor unbefugtem Zugriff und nur Geräte mit dem richtigen „Schlüssel“ können im VPN arbeiten. Netzwerkgeräte zwischen dem Client und dem Server können weder auf die Daten zugreifen noch diese darstellen.

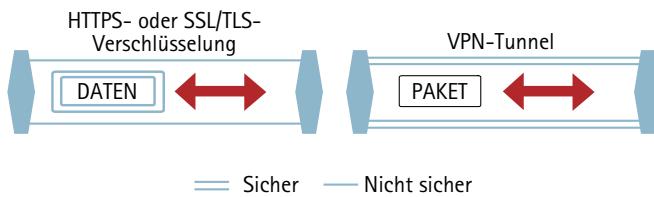


Abbildung 9.5b Der Unterschied zwischen HTTPS (SSL/TLS) und VPN besteht darin, dass bei HTTPS nur die tatsächlichen Daten eines Pakets verschlüsselt werden. Bei VPN kann das gesamte Paket verschlüsselt und gekapselt werden, um einen sicheren „Tunnel“ zu bilden. Beide Technologien können parallel verwendet werden. Dies wird jedoch nicht empfohlen, da jede Technologie zusätzlichen Overhead erzeugt und die Leistung des Systems herabsetzen kann.

Drahtlose Netzwerktechnologien

Die drahtlosen Netzwerktechnologien (WLAN) bieten für Videoüberwachungsanwendungen eine flexible, kostengünstige und schnelle Möglichkeit zum Installieren von Kameras, insbesondere in großen Bereichen wie Parkplätzen oder Innenstädten. Das Verlegen von Kabeln im Boden ist nicht notwendig. In älteren, unter Denkmalschutz stehenden Gebäuden ist die drahtlose Technologie möglicherweise die einzige Alternative, wenn keine normalen Ethernet-Kabel verlegt werden dürfen. Axis bietet Kameras mit integriertem WLAN-Interface. Auch Netzwerk-Kameras ohne integrierte WLAN-Interface können durch eine Wireless-Bridge in ein drahtlosem Netzwerk integriert werden.



Abbildung 10a Eine Netzwerk-Kamera von Axis mit WLAN-Interface, die 802.11b/g unterstützt.



Abbildung 10b Durch eine Wireless-Bridge kann jede beliebige Netzwerk-Kamera in einem drahtlosen Netzwerk eingesetzt werden.

10.1 WLAN-Standards 802.11

Der gebräuchlichste Standard im WLAN-Bereich (Wireless Local Area Network) ist der IEEE-Standard 802.11. Es gibt neben diesem auch andere Standards und proprietäre Technologien, aber der Vorteil der 802.11-Wireless-Standards liegt darin, dass er lizenzfrei betrieben werden, d. h. für die Einrichtung und den Betrieb des Netzwerks fällt keine Lizenzgebühr an. Die relevantesten Erweiterungen der Standards sind 802.11b, 802.11g, 802.11a und 802.11n.

802.11b, der 1999 veröffentlicht wurde, nutzt das 2,4-GHz-Band und erzielt Datenraten von bis zu 11 MBit/s. Bis 2004 basierten die meisten verkauften WLAN-Geräte auf dem Standard 802.11b.

802.11g, der 2003 veröffentlicht wurde, ist die am weitesten verbreitete Variante des 802.11-Standards am Markt. Er nutzt das 2,4-GHz-Band und erzielt Datenraten von bis zu 54 MBit/s. Heutige WLAN-Geräte sind in der Regel IEEE 802.11b/g kompatibel.

802.11a, der 1999 veröffentlicht wurde, überträgt im 5-GHz-Frequenzbereich und liefert Datenraten von bis zu 54 MBit/s. Problematisch ist, dass der 5-GHz-Frequenzbereich in bestimmten Teilen von Europa lange Zeit nicht verwendet werden konnte. Dies hat sich Ende 2002 geändert, seitdem ist der Betrieb von 5-GHz-WLAN-Komponenten zulässig. Damit 5-GHz-Komponenten allerdings uneingeschränkt betrieben werden dürfen, d.h. mit maximaler Sendeleistung und auf allen Kanälen, ist es jedoch erforderlich, dass die Geräte auch IEEE 802.11h konform sind. Ein Nachteil der 802.11a/h-Lösungen ist allerdings der verwendete Frequenzbereich, d.h. die elektromagnetischen Signale werden bei 5 GHz mehr gedämpft als bei 2,4 GHz. Folglich wird für den Betrieb im 5-GHz-Band eine viel höhere Anzahl an Access Points benötigt als für die Umsetzung im 2,4-GHz-Band.

Der noch nicht fertig gestellte und ratifizierte Standard der nächsten Generation, der 802.11n, ermöglicht Datenraten von bis zu 600 MBit/s. Produkte, die 802.11n unterstützen, basieren auf einem Entwurf des Standards.

Bei der Einrichtung eines drahtlosen Netzwerks müssen die Bandbreitenkapazität der Access Points und die Bandbreitenanforderungen der Netzwerkgeräte 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. Es sollten nie mehr als vier oder fünf Netzwerk-Kameras, die 802.11g unterstützen, an einen drahtlosen Access Point angeschlossen werden.

10.2 WLAN-Sicherheit

Es liegt in der Natur der drahtlosen Kommunikation, dass jeder, der ein drahtloses Gerät besitzt und sich im Funkbereich befindet, sich in ein Netzwerk einklinken und Daten abfangen kann, die darüber gesendet werden. Daher muss das Netzwerk gesichert werden.

Um den unbefugten Zugriff auf die übertragenen Daten und das Netzwerk zu verhindern, wurden Sicherheitstechnologien wie WEP und WPA/WPA2 entwickelt, die die über das Netzwerk gesendeten Daten verschlüsseln.

10.2.1 WEP (Wired Equivalent Privacy)

WEP verhindert, dass Personen, die nicht über den richtigen Schlüssel verfügen, auf das Netzwerk zugreifen können. WEP hat jedoch einige Schwachstellen. Hierzu gehören die relativ kurzen Schlüssel und andere Einschränkungen, durch die die Schlüssel aus einer vergleichsweise geringen Menge an abgefangenem Datenverkehr rekonstruiert werden können. WEP gilt heutzutage nicht mehr als sicher, weil im Internet unzählige Programme frei erhältlich sind, mit denen ein solcher „geheimer“ WEP-Schlüssel geknackt werden kann.

10.2.2 WPA/WPA2 (WiFi Protected Access)

Durch WPA wird die Sicherheit wesentlich erhöht. Die Unzulänglichkeiten des WEP-Standards wurden behoben. Mit WPA wurde eine Standardmethode zur Verteilung verschlüsselter Schlüssel eingeführt.

10.2.3 Empfehlungen

Im Folgenden werden einige Sicherheitsrichtlinien für die Verwendung drahtloser Kameras aufgeführt, die zu Überwachungszwecken eingesetzt werden:

- > Aktivieren Sie für die Kameras die Anmeldung per Benutzername und Kennwort.
- > Stellen Sie sicher, dass die drahtlosen Kameras Sicherheitsprotokolle wie IEEE 802.1X und WPA/WPA2 unterstützen.

10.3 Wireless-Bridge

Es sind Lösungen möglich, die nicht auf dem dominierenden Standard IEEE 802.11 beruhen und die neben einer höheren Leistung bei größeren Entfernungen ein sehr hohes Maß an Sicherheit bieten. Häufig werden auch Laserlicht basierte Systeme eingesetzt, um Gebäude oder Standorte über eine Hochgeschwindigkeits-Datenverbindung (Punkt-zu-Punkt) zu verbinden.

Videoverwaltungssysteme

Ein wichtiger Aspekt eines Videoüberwachungssystems ist die Verwaltung der Live-Anzeige, Aufzeichnung, Wiedergabe und Aufbewahrung. Wenn das System nur eine bzw. wenige Kameras umfasst, kann das Anzeigen sowie die einfache Videoaufzeichnung über die integrierte Weboberfläche der Netzwerk-Kameras und Video-Encoder verwaltet werden. Umfasst das System jedoch eine größere Anzahl an Kameras, wird die Verwendung eines Netzwerk-Videoverwaltungssystems empfohlen.

Derzeit stehen über hundert verschiedene Videoverwaltungssysteme zur Verfügung, die unterschiedliche Betriebssysteme (Windows, UNIX, Linux und Mac OS), Marktsegmente und Sprachen abdecken. Bei der Auswahl eines Systems müssen Faktoren wie die Hardware-Plattform (auf einem PC-Server oder Netzwerk-Videorecorder basierend), die Software-Plattform, Systemfunktionen einschließlich Installation und Konfiguration, Ereignisverwaltung, intelligentem Video, Verwaltung und Sicherheit sowie Integrationsmöglichkeiten mit anderen Systemen wie Kassenterminal- oder Gebäudeverwaltungssystemen berücksichtigt werden.

11.1 Hardware-Plattformen

Für ein Netzwerk-Videoverwaltungssystem stehen zwei verschiedene Hardware-Plattformen zur Auswahl: eine PC-Server-Plattform mit einem oder mehreren PCs, auf der eine Videoverwaltungssoftware ausgeführt wird, und eine Netzwerk-Videorecorder-Plattform (NVR), bei der es sich um proprietäre Hardware mit vorinstallierter Videoverwaltungssoftware handelt.

11.1.1 PC-Server-Plattform

Eine Videoverwaltungslösung, die auf einer PC-Server-Plattform basiert, umfasst verschiedene Standard-PC-Server und -Speichergeräte, die entsprechend dem jeweiligen System ausgewählt werden können, um eine optimale Leistung zu erzielen. Eine solch offene Plattform erleichtert das Hinzufügen weiterer Funktionalität, z. B. weiterer oder externer Speicher, Firewalls, Virenschutz und intelligente Videoalgorithmen, zusätzlich zur Videoverwaltungssoftware.

Darüber hinaus ist eine PC-Server-Plattform vollständig skalierbar, d. h. es können dem Bedarf entsprechend beliebig viele Netzwerk-Videoprodukte zum System hinzugefügt werden. Die System-Hardware lässt sich erweitern oder aktualisieren, um gestiegenen Leistungsanforderungen gerecht zu werden. Eine offene Plattform ermöglicht auch eine einfachere Integration mit anderen Systemen wie z. B. Zugangskontroll-, Gebäudeverwaltungs- und industrielle Kontrollsysteinen. Dies gibt Benutzern die Möglichkeit, Video- und andere Gebäudekontrollsysteine über ein einzelnes Programm und eine einzelne Benutzeroberfläche zu verwalten. Weitere Informationen zu Servern und zur Speicherung finden Sie in Kapitel 12.

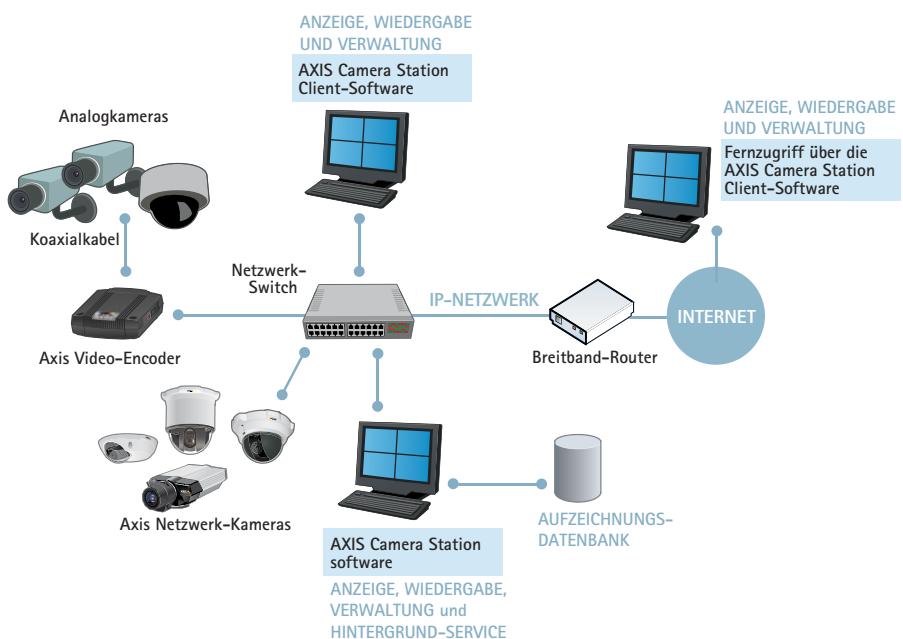


Abbildung 11.1a Netzwerk-Videoüberwachungssystem auf der Basis einer offenen PC-Server-Plattform mit der Videoverwaltungssoftware AXIS Camera Station.

11.1.2 NVR-Plattform

Ein Netzwerk-Videorecorder (NVR) ist ein Gerät mit vorinstallierten Videoverwaltungsfunktionen. In diesem Sinne ist ein NVR mit einem DVR vergleichbar. (Einige DVRs, die häufig als Hybrid-DVRs bezeichnet werden, enthalten eine NVR-Funktion, d. h., sie können auch Netzwerk-basierte Videoaufzeichnungen vornehmen).

Die NVR-Hardware ist meist proprietär und speziell für die Videoverwaltung konzipiert. Sie ist auf bestimmte Aufgaben wie das Aufzeichnen, Analysieren und Wiedergeben von Netzwerk-Video ausgerichtet, und meist ist es nicht möglich, andere Anwendungen auf dieser Hardware zu installieren. Das Betriebssystem kann Windows, UNIX/Linux oder ein proprietäres Betriebssystem sein.

NVRs sind auf eine optimale Leistung für eine festgelegte Anzahl an Kameras ausgelegt. In der Regel ist ihre Skalierbarkeit im Vergleich zu PC-Server-Plattformen eingeschränkt. Daher eignen sie sich vor allem für kleinere Systeme, bei denen die Anzahl der Kameras im Rahmen der NVR-Kapazität bleibt. NVRs lassen sich normalerweise leichter installieren als Systeme, die auf PC-Server-Plattformen basieren.



Abbildung 11.1b Ein Netzwerk-Videoüberwachungssystem, das einen NVR verwendet.

11.2 Software-Plattformen

Für die Videoverwaltung können verschiedene Software-Plattformen verwendet werden. Dazu gehören die integrierte Weboberfläche, die in vielen Netzwerk-Videoprodukten vorhanden ist, oder eine separate Videoverwaltungssoftware, die entweder eine Windows-basierte oder eine webbasierte Oberfläche bietet.

11.2.1 Integrierte Funktionalität

Der Zugriff auf Axis Netzwerk-Kameras und Video-Encoder über das Netzwerk erfolgt durch die Eingabe der IP-Adresse des Produkts im Adressfeld des Webbrowsers auf einem Computer. Sobald die Verbindung mit dem Netzwerk-Videoprodukt hergestellt wurde, wird die Startseite des Produkts zusammen mit Verknüpfungen zu den Konfigurationsseiten automatisch im Webbrowser angezeigt.

Die integrierte Weboberfläche von Axis-Netzwerk-Videoprodukten bietet einfache Aufzeichnungsfunktionen, d. h., die manuelle Aufzeichnung von Videoströmen (H.264, MPEG-4 Part 2, Motion JPEG) auf einem Server durch Klicken auf ein Symbol oder die ereignisgesteuerte Aufzeichnung einzelner JPEG-Bilder in einem oder mehreren Speicherorten. Die ereignisgesteuerte Aufzeichnung von Videoströmen ist bei Netzwerk-Videoprodukten möglich, die die lokale Speicherung unterstützen. In diesen Fällen werden die Videoströme auf der SD/SDHC-Karte des Produkts aufgezeichnet. Für mehr Flexibilität hinsichtlich der Art der Aufzeichnung (z. B. kontinuierliche oder zeitlich geplante Aufzeichnungen) und der Funktionen ist eine separate Video-

verwaltungssoftware erforderlich. Die Konfiguration und Verwaltung eines Netzwerk-Videoproducts über seine integrierte Weboberfläche ist dann möglich, wenn das System nur eine kleine Anzahl an Kameras umfasst.

11.2.2 Windows-Client-basierte Software

Bei separaten Softwareprogrammen für die Videoverwaltung werden am häufigsten Windows-Client-basierte Programme verwendet. Es stehen aber auch webbasierte Softwareprogramme zur Verfügung. Bei einem Windows-Client-basierten Programm muss die Videoverwaltungssoftware zuerst auf dem aufzeichnenden Server installiert werden. Anschließend kann ein Client-Softwareprogramm für die Anzeige auf dem Aufzeichnungsserver oder auf einem anderen PC installiert werden. Die Installation des Programms kann in dem Netzwerk, in dem sich der Aufzeichnungsserver oder ein anderer PC befindet oder auf einem externen PC in einem anderen Netzwerk erfolgen. Bei einigen Client-Anwendungen ist es sogar möglich, zwischen verschiedenen Servern, auf denen die Videoverwaltungssoftware installiert ist, zu wechseln, wodurch die Videoverwaltung eines großen Systems oder vieler entfernter Standorte ermöglicht wird.

11.2.3 Webbasierte Software

Eine webbasierte Videoverwaltungssoftware muss zuerst auf einem PC-Server installiert werden, der sowohl als Web- als auch als Aufzeichnungsserver dient. Anschließend können Benutzer mit Hilfe eines Webbrowsers über jede Art von Netzwerkcomputern überall auf der Welt auf den Videoverwaltungsserver und damit auf die von diesem verwalteten Netzwerk-Videoprodukte zugreifen.

11.2.4 Skalierbarkeit von Videoverwaltungssoftware

Die Skalierbarkeit der meisten Videoverwaltungsprogramme in Bezug auf die unterstützte Anzahl der Kameras und der Bilder pro Sekunde ist in der Regel eher durch die Hardwarekapazität statt durch die Software selbst eingeschränkt. Das Speichern von Videodateien stellt neue Herausforderungen für die Speicherhardware dar, da diese möglicherweise auf einer dauerhaften Basis und nicht nur während der normalen Geschäftsstunden in Betrieb sein muss. Darüber hinaus erzeugt Video naturgemäß große Datenmengen, wodurch hohe Anforderungen an die Speicherlösung gestellt werden. *Weitere Informationen zu Servern und zur Speicherung finden Sie in Kapitel 12.*

11.2.5 Offene im Vergleich zu herstellerspezifischer Software

Videoverwaltungsprogramme sind von den Herstellern von Netzwerk-Videoprodukten erhältlich. Sie unterstützen oftmals nur die Netzwerk-Videogeräte des Herstellers. Es gibt jedoch auch Softwareprogramme, die Netzwerk-Videoprodukte von verschiedenen Herstellern unterstützen. Sie stammen meist von unabhängigen Unternehmen. Es steht eine Vielzahl an Softwarelösungen von mehr als 550 Anwendungsentwicklungspartnern von Axis zu Verfügung. *Weitere Informationen hierzu finden Sie unter www.axis.com/partner/adp*

11.3 Systemmerkmale

Ein Videoverwaltungssystem kann viele verschiedene Funktionen unterstützen. Im Folgenden werden die gängigeren Funktionen beschrieben:

- > Gleichzeitiges Anzeigen von Videobildern von mehreren Kameras
- > Aufzeichnen von Video- und Audiodaten
- > Ereignisverwaltungsfunktionen wie intelligentes Video, z. B. Videobewegungserkennung
- > Kamerasteuerung und -verwaltung
- > Suchoptionen und Wiedergabe
- > Benutzerzugangskontrolle und Aktivitätenprotokollierung (Audit)

11.3.1 Anzeigen

Ein wesentliches Merkmal eines Videoverwaltungssystems besteht in der Möglichkeit, aufgezeichnete und Live-Videobilder in einer effizienten und benutzerfreundlichen Art und Weise anzuzeigen. Die meisten Videoverwaltungsprogramme ermöglichen es mehreren Benutzern, die Bilder in verschiedenen Modi anzuzeigen, z. B. in der geteilten Ansicht (um die Bilder verschiedener Kameras gleichzeitig anzuzeigen), im Vollbildmodus oder als Kamerasequenz (bei der die Bilder von verschiedenen Kameras automatisch nacheinander angezeigt werden).

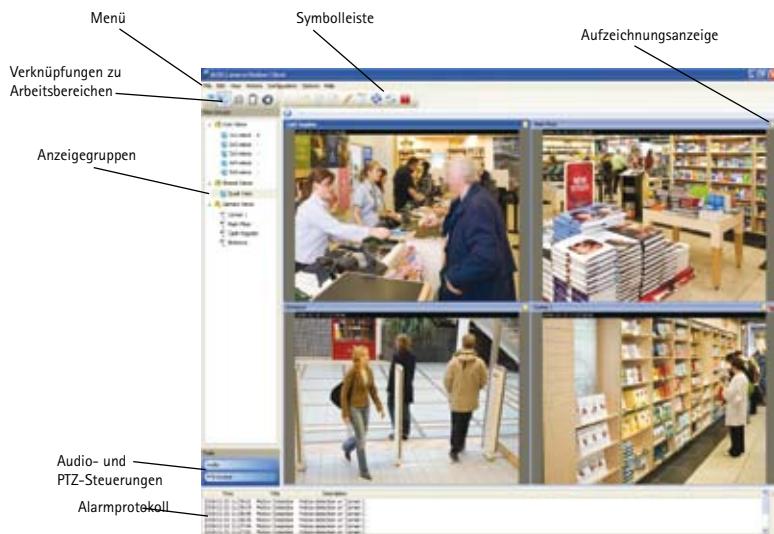


Abbildung 11.3a Live-Ansichtsbildschirm von AXIS Camera Station.

Viele Videoverwaltungsprogramme bieten auch eine Wiedergabefunktion für mehrere Kameras. Diese ermöglicht es Benutzern, mehrere Aufzeichnungen verschiedener Kameras gleichzeitig anzuzeigen. So sind Benutzer in der Lage, sich ein umfassendes Bild von einer Situation zu machen, was zum Beispiel bei polizeilichen Ermittlungen hilfreich sein kann. Weitere mögliche Funktionen sind das Anzeigen auf mehreren Monitoren sowie das Zuordnen, bei dem Kamera-Symbole, die die Standorte der Kameras darstellen, auf einer Gebäude- oder Bereichskarte angezeigt werden.

11.3.2 Multi-streaming

Die technisch ausgereiften Netzwerk-Videoprodukte von Axis ermöglichen Multi-Streaming, bei dem mehrere Videoströme von einer Netzwerk-Kamera oder von einem Video-Encoder individuell mit verschiedenen Bildraten, Komprimierungsformaten und Auflösungen konfiguriert und an verschiedene Empfänger gesendet werden können. Durch diese Fähigkeit wird die Ausnutzung der Netzwerkbandbreite optimiert.

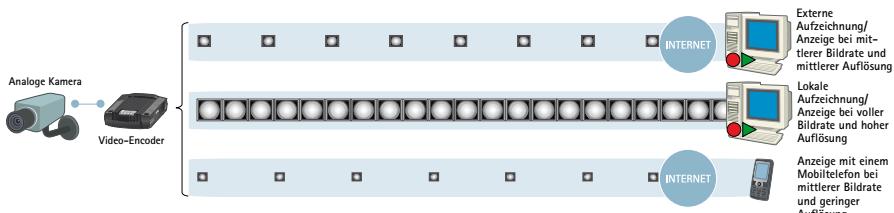


Abbildung 11.3b Mehrere, individuell konfigurierbare Videoströme können mit unterschiedlichen Bildraten und unterschiedlicher Auflösung an verschiedene Empfänger gesendet werden.

11.3.3 Videoaufzeichnung

Mit Videoverwaltungssoftware, wie z. B. der AXIS Camera Station, können Videodaten manuell, kontinuierlich oder ereignisgesteuert (durch Bewegung oder Alarm) aufgezeichnet werden. Kontinuierliche und ereignisgesteuerte Aufzeichnungen können außerdem für bestimmte Tageszeiten geplant werden. Eine kontinuierliche Aufzeichnung benötigt in der Regel mehr Festplattenspeicher als eine ereignisgesteuerte Aufzeichnung. Eine ereignisgesteuerte Aufzeichnung kann beispielsweise durch die Videobewegungserkennung oder durch externe Eingaben über den Eingangsport einer Kamera oder eines Video-Encoders ausgelöst werden. Bei geplanten Aufzeichnungen können die Zeiten sowohl für kontinuierliche als auch für ereignisgesteuerte Aufzeichnungen festgelegt werden.

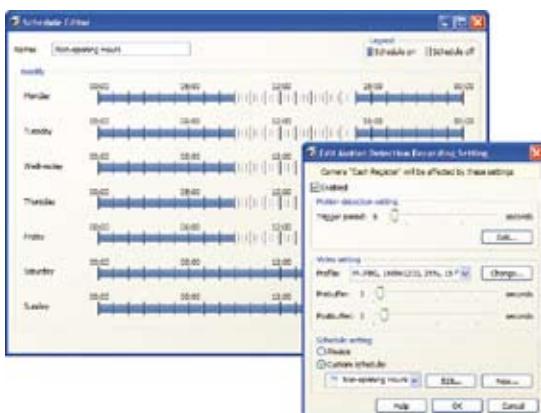


Abbildung 11.3c Geplante Aufzeichnungseinstellungen mit einer Kombination aus kontinuierlichen und ereignisgesteuerten Aufzeichnungen unter Verwendung der Videoverwaltungssoftware AXIS Camera Station.

Wenn die Aufzeichnungsmethode ausgewählt wurde, kann die Qualität der Aufzeichnungen durch Auswahl des Videoformats (z. B. H.264, MPEG-4 Part 2, Motion JPEG), der Auflösung, der Komprimierstufe und der Bildrate festgelegt werden. Diese Parameter wirken sich auf die Menge der verwendeten Bandbreite sowie auf die Menge des benötigten Speicherplatzes aus.

Netzwerk-Videoprodukte können, je nach Auflösung, verschiedene Bildraten haben. Die Aufzeichnung und/oder Anzeige bei voller Bildrate (30 Bilder pro Sekunde im NTSC-Standard und 25 Bilder pro Sekunde im PAL-Standard) auf allen Kameras und zu allen Zeiten ist mehr, als für die meisten Anwendungen erforderlich ist. Unter normalen Bedingungen kann die Bildrate niedriger eingestellt werden, z. B. auf ein bis vier Bilder pro Sekunde, um die Speicheranforderungen deutlich zu senken. Im Fall eines Alarms – wenn beispielsweise die Videobewegungserkennung oder ein externer Sensor ausgelöst werden – kann ein separater Datenstrom mit einer höheren Aufzeichnungsbildrate gesendet werden.

11.3.4 Aufzeichnung und Speicherung

Die meisten Videoverwaltungsprogramme verwenden das Standarddateisystem von Windows für die Speicherung, sodass jedes Systemlaufwerk oder über das Netzwerk angeschlossene Laufwerk zum Speichern der Videodaten verwendet werden kann. Ein Videoverwaltungsprogramm kann mehrere Speicherebenen verwenden. So können beispielsweise Aufzeichnungen auf einem primären Laufwerk (der lokalen Festplatte) gemacht werden, die Archivierung jedoch auf lokalen Datenträgern, Netzwerk- oder externen Laufwerken erfolgen. Oft können Benutzer angeben, wie lange Bilder auf der primären Festplatte verbleiben sollen, bevor sie automatisch gelöscht oder auf das Archivlaufwerk verschoben werden. Oft können sie auch verhindern, dass ereignisgesteuerte Videoaufzeichnungen automatisch gelöscht werden, indem sie speziell markieren oder im System sperren.

11.3.5 Ereignisverwaltung und intelligentes Video

Zur Ereignisverwaltung gehört das Identifizieren oder Definieren von Ereignissen, die von Netzwerk-Videoprodukten oder anderen Systemen wie Kassenterminals oder intelligenter Videosoftware ausgelöst werden, sowie das Konfigurieren der automatischen Reaktion des Netzwerk-Videoüberwachungssystems auf ein Ereignis. Dies kann z. B. das Starten der Videoaufzeichnung, das Senden von Benachrichtigungen oder das Aktivieren anderer Geräte wie Türen und Lampen sein.

Die Ereignisverwaltungs- und intelligenten Videofunktionen können zusammen interagieren, so dass das Videoüberwachungssystem die verfügbare Netzwerkbandbreite und den Speicherplatz effizienter nutzen kann. Die Live-Kameraüberwachung ist nicht die ganze Zeit erforderlich, da bei Eintreten eines Ereignisses Benachrichtigungen an Bediener gesendet werden können. Alle konfigurierten Reaktionen können automatisch aktiviert werden, was die Reaktionszeiten verbessert. Durch die Ereignisverwaltung können Bediener mehr Kameras gleichzeitig kontrollieren.

Die Ereignisverwaltungs- und intelligenten Videofunktionen können in ein Netzwerk-Videoproduct oder in eine Videoverwaltungssoftware integriert und von dort aus gesteuert werden.

Sie können auch von beiden betrieben werden, z. B. indem ein Videoverwaltungsprogramm die Vorteile der in ein Netzwerk-Videoproduct integrierten intelligenten Videofunktionen nutzt. So kann intelligente Videofunktionalität wie die Videobewegungserkennung und der Kameramanipulationsschutz vom Netzwerk-Videoproduct ausgeführt werden, während die Entscheidung über die entsprechenden durchzuführenden Aktionen dem Verwaltungsprogramms obliegt. Diese Vorgehensweise bietet zahlreiche Vorteile:

- > Sie ermöglicht eine effizientere Nutzung der Bandbreite und des Speicherplatzes, da keine Kamera dauerhaft Videodaten zur Analyse potenzieller Ereignisse an einen Videoverwaltungsserver senden muss. Die Analyse findet im Netzwerk-Videoproduct selbst statt und die Videoströme werden nur dann für die Aufzeichnung und/oder Anzeige gesendet, wenn ein Ereignis eintritt.
- > Der Videoverwaltungsserver muss keine schnelle Rechnerleistung aufweisen, sodass hier Kosteneinsparungen möglich sind. Die Ausführung intelligenter Videoalgorithmen ist CPU-intensiv.
- > Skalierbarkeit ist möglich. Wenn ein Server intelligente Videoalgorithmen ausführen müsste, könnten nur wenige Kameras gleichzeitig verwaltet werden. Durch die Integration der intelligenten Funktionalität in die Netzwerk-Kamera oder in den Video-Encoder sind schnelle Reaktionszeiten und die proaktive Verwaltung einer großen Anzahl an Kameras möglich.

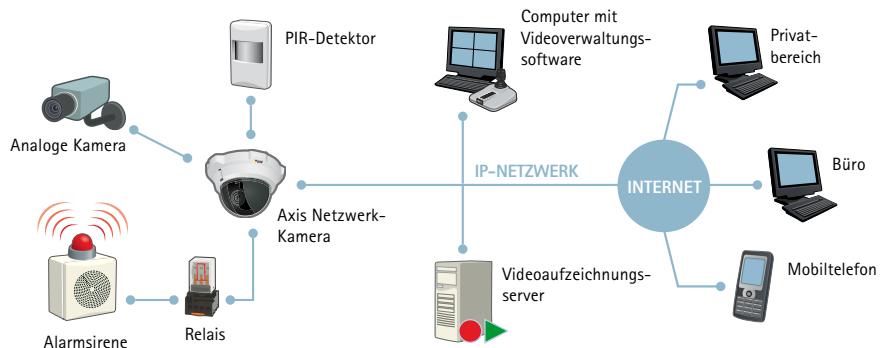


Abbildung 11.3d Ereignisverwaltung und intelligentes Video sorgen dafür, dass das Überwachungssystem ständig aktiv ist und die eingehenden Informationen analysiert, um Ereignisse zu erkennen. Wenn ein Ereignis erkannt wurde, kann das System selbstdäig mit Aktionen wie der Videoaufzeichnung und dem Versenden von Warnmeldungen reagieren.

Ereignisauslöser

Ein Ereignis kann geplant oder ausgelöst werden. Ereignisse können beispielsweise durch folgende Komponenten ausgelöst werden:

- > **Eingangsport(s):** Die Eingangssports einer Netzwerk-Kamera oder eines Video-Encoders können mit externen Geräten, wie z. B. einem Bewegungssensor oder einem Türschalter, verbunden werden.
- > **Manueller Auslöser:** Ein Bediener kann ein Ereignis über Tasten manuell auslösen.
- > **Videobewegungserkennung:** Wenn eine Kamera eine bestimmte Bewegung in ihrem Bewegungserkennungsfenster feststellt, kann ein Ereignis ausgelöst werden. *Weitere Informationen zur Videobewegungserkennung finden Sie weiter unten, in diesem Abschnitt.*
- > **Kameramanipulation:** Diese Funktion, mit der eine Kamera feststellen kann, ob sie absichtlich verdeckt, anders ausgerichtet oder die Schärfeeinstellung geändert wurde, kann zum Auslösen eines Ereignisses verwendet werden. *Weitere Informationen zum aktiven Manipulationsalarm finden Sie weiter unten, in diesem Abschnitt.*
- > **Audio-Auslöser:** Dies ermöglicht es einer Kamera mit integrierter Audiounterstützung, ein Ereignis auszulösen, wenn sie einen Geräuschpegel unter- oder oberhalb eines bestimmten Grenzwerts erkennt. *Weitere Informationen zur Audio-Erkennung finden Sie in Kapitel 8.*
- > **Temperatur:** Wenn die Temperatur den Betriebsbereich der Kamera übersteigt oder unterschreitet, kann ein Ereignis ausgelöst werden.

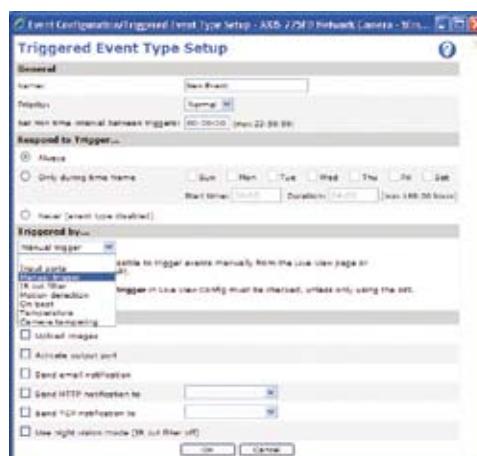


Abbildung 11.3e Festlegen von Ereignisauslösern über die Weboberfläche eines Netzwerk-Videoproducts von Axis.

Reaktionen

Netzwerk-Videoprodukte oder ein Videoverwaltungsprogramm können so konfiguriert werden, dass sie immer oder nur zu bestimmten Zeiten auf Ereignisse reagieren. Einige der häufigsten konfigurierbaren Reaktionen bei Auslösen eines Ereignisses sind folgende:

- > Hochladen von Bildern oder Aufzeichnen von Videoströmen an bestimmten Speicherorten und mit einer bestimmten Bildrate. Wenn die ereignisgesteuerte Funktionalität in der Weboberfläche von Axis Netzwerk-Videoprodukten verwendet wird, können nur JPEG-Bilder hochgeladen werden. Bei Verwendung eines Videoverwaltungsprogramms kann ein Videostrom mit einem bestimmten Komprimierformat (H.264/MPEG-4/Motion JPEG) und einer Komprimierstufe vom Netzwerk-Videoprodukt angefordert werden.
- > Aktivieren des/der Ausgangsports: Die Ausgangsports einer Netzwerk-Kamera oder eines Video-Encoders können mit externen Geräten wie z. B. Alarmsirenen verbunden werden. (Weitere Details hierzu finden Sie weiter unten.)
- > Senden einer E-Mail-Benachrichtigung: Dies teilt Benutzern mit, dass ein Ereignis eingetreten ist. Es kann auch ein Bild an die E-Mail angehängt werden.
- > Senden einer HTTP/TCP-Benachrichtigung: Dies ist eine Statusmeldung für ein Videoverwaltungssystem, welches daraufhin beispielsweise Aufzeichnungen starten kann.
- > Zu einer PTZ-Voreinstellung wechseln: Diese Funktion ist möglicherweise bei PTZ-Kameras oder PTZ-Dome-Kameras verfügbar. Sie ermöglicht es der Kamera, auf eine bestimmte Position, z. B. ein Fenster, zu zeigen, wenn ein Ereignis stattfindet.
- > Senden einer SMS (Short Message Service) mit Textinformationen über den Alarm oder einer MMS (Multimedia Messaging Service) mit einem Bild von dem Ereignis.
- > Aktivieren eines Audioalarms auf dem Videoverwaltungssystem.
- > Aktivieren eines Bildschirm-Popup-Fensters, das Bilder einer Kamera zeigt, bei der ein Ereignis eingetreten ist.
- > Anzeigen von Verfahren, die der Bediener ausführen sollte.

Darüber hinaus können Voralarm- und Nachalarm-Bildpuffer festgelegt werden, die es einem Netzwerk-Videoprodukt ermöglichen, eine bestimmte Länge und Bildrate einer Videoaufzeichnung, die vor und nach dem Auslösen eines Ereignisses erfolgt ist, zu senden. Dies kann dazu beitragen, ein umfassenderes Bild von dem Ereignis zu erhalten.

Eingangs-/Ausgangsports

Ein einmaliges Merkmal von Netzwerk-Kameras und Video-Encodern im Vergleich zu analogen Kameras sind die integrierten Eingangs- und Ausgangsports (E/A). Mithilfe dieser Ports können externe Geräte an das Netzwerk-Videoprodukt angeschlossen und über das Netzwerk verwaltet werden. So kann beispielsweise eine Netzwerk-Kamera oder ein Video-Encoder, die bzw. der über den Eingangsport mit einem externen Alarmsensor verbunden ist, so konfiguriert werden, dass sie/er Videodaten nur sendet, wenn der Sensor ausgelöst wird.

Das Spektrum der Geräte, die an den Eingang eines Netzwerk-Videoproducts angeschlossen werden können, ist nahezu unbegrenzt. Die Grundregel ist, dass jedes Gerät, das einen Schaltkreis öffnen oder schließen kann, an eine Netzwerk-Kamera oder einen Video-Encoder angeschlossen werden kann. Die Hauptfunktion des Ausgangsport eines Netzwerk-Videoproducts besteht im Auslösen externer Geräte – automatisch oder ferngesteuert durch einen Bediener oder eine Anwendung.

Gerätetyp	Beschreibung	Verwendung
Türkontakt	Einfacher Magnetschalter, der das Öffnen von Türen und Fenstern erkennt.	Wenn der Schaltkreis geöffnet wird (Tür geht auf), können Bilder/Videodaten sowie Benachrichtigungen von der Kamera gesendet werden.
PIR (Passive Infrarotsensorik)	Sensor, der Bewegungen anhand von Wärmestrahlung erkennt.	Wenn eine Bewegung erkannt wird, unterricht der PIR-Sensor den Schaltkreis und es können Bilder bzw. Videodaten sowie Benachrichtigungen von der Kamera gesendet werden.
Glasbruchmelder	Ein aktiver Sensor, der den Luftdruck in einem Raum misst und einen plötzlichen Abfall des Luftdrucks erkennt. (Der Sensor kann über die Kamera mit Strom versorgt werden.)	Wenn ein Abfall des Luftdrucks erkannt wird, unterricht der Melder den Schaltkreis, und es können Bilder bzw. Videodaten sowie Benachrichtigungen von der Kamera gesendet werden.

Tabelle 11.3a Beispiel für Geräte, die an den Eingangsport angeschlossen werden können.

Gerätetyp	Beschreibung	Verwendung
Tür-Relais	Relais, das das Öffnen und Schließen von Türschlössern überwacht.	Das Ab-/Aufschließen einer Tür kann von einem externen Bediener über ein Netzwerk oder automatisch als Reaktion auf ein Alarmereignis gesteuert werden.
Sirene	Warnsirene, die bei erkannter Alarmsituation ausgelöst wird.	Das Netzwerk-Videoprodukt kann die Sirene aktivieren, wenn es Bewegung mithilfe der integrierten Videobewegungserkennung oder anhand von „Informationen“ des digitalen Eingangs erkennt.
Alarm/Einbruchserkennung	Ein Sicherheitsalarmsystem, das einen geschlossenen oder offenen Alarmschaltkreis ständig überwacht.	Das Netzwerk-Videoprodukt kann integrierter Bestandteil des Alarmsystems sein, das die Aufgabe eines Sensors übernimmt und das Alarmsystem um ereignigesteuerte Videoübertragungen erweitert.

Tabelle 11.3b Beispiel für Geräte, die an den Ausgangsport angeschlossen werden können.

Videobewegungserkennung

Die Videobewegungserkennung ist eine gängige Funktion in Videoverwaltungssystemen. Sie bietet die Möglichkeit, Aktivität in einer Szene zu definieren. Hierzu werden Bilddaten und Unterschiede in einer Reihe von Bildern analysiert. Mit der Videobewegungserkennungsfunktion kann Bewegung in allen Sichtfeldern der Kamera erkannt werden. Benutzer können eine bestimmte Anzahl „einzubziehender“ Fenster (bestimmte Zonen im Sichtfeld der Kamera, in denen Bewegung erkannt werden soll) und „auszuschließender“ Fenster (Zonen in einem „einzubziehenden“ Fenster, die ignoriert werden sollen) festlegen. Mit der Videobewegungserkennung können Prioritäten bei der Aufzeichnung festgelegt, die Menge an Videoaufzeichnungen reduziert und das Suchen von Ereignissen vereinfacht werden.

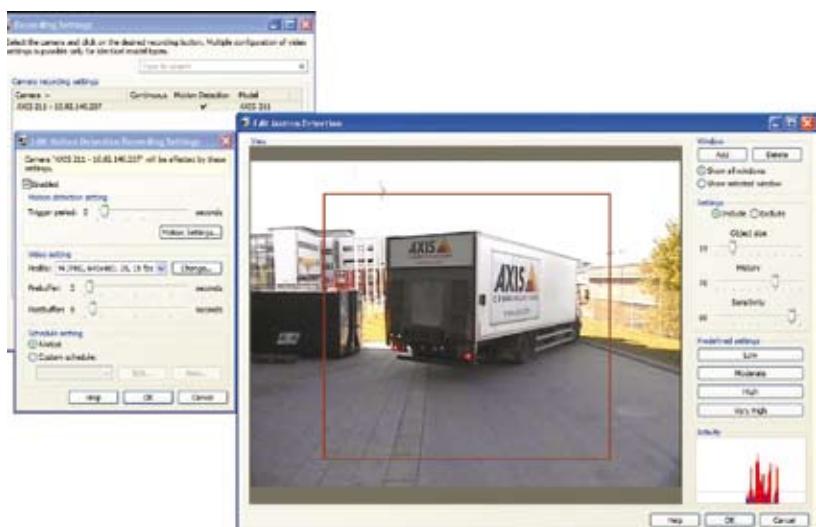


Abbildung 11.3f Einstellen der Videobewegungserkennung in der Videoverwaltungssoftware AXIS Camera Station.

Aktiver Manipulationsalarm

Diese in viele Netzwerk-Videoprodukte von Axis integrierte intelligente Videofunktion kann als ereignisgesteuerter Auslöser verwendet werden, wenn eine Kamera in irgendeiner Weise manipuliert wird, beispielsweise indem sie anders ausgerichtet, blockiert, defokussiert oder mit Farbe besprührt, abgedeckt oder beschädigt wird. Ohne eine solche Erkennungsfunktion sind Überwachungskameras nur von eingeschränktem Nutzen.

11.3.6 Verwaltungsfunktionen

Alle Videoverwaltungsprogramme bieten die Möglichkeit, grundlegende Kameraeinstellungen, die Bildrate, die Auflösung und das Komprimierformat hinzuzufügen bzw. festzulegen. Einige Programme bieten darüber hinaus erweiterte Funktionen, wie z. B. Kameraerkennung und umfassende Geräteverwaltung. Je größer ein Videoüberwachungssystem ist, umso wichtiger ist es, Netzwerkgeräte effizient zu verwalten.

Softwareprogramme, die die Verwaltung von Netzwerk-Kameras und Video-Encodern in einer Installation vereinfachen, enthalten meist die folgenden Funktionen:

- > Lokalisieren und Anzeigen des Verbindungsstatus von Videosystemen im Netzwerk
- > Festlegen von IP-Adressen
- > Konfigurieren von einem oder mehreren Geräten
- > Verwalten von Firmware-Upgrades für mehrere Geräte
- > Verwalten der Benutzerzugriffsrechte
- > Anzeigen einer Konfigurationsübersicht über alle Kamera- und Aufzeichnungskonfigurationen

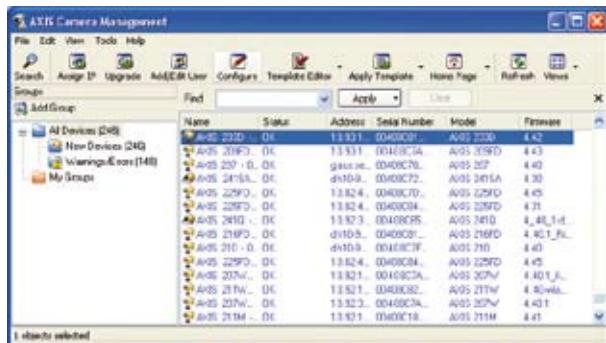


Abbildung 11.3g *AXIS Camera Management-Software erleichtert das Suchen, Installieren und Konfigurieren von Netzwerk-Videoproducten.*

11.3.7 Sicherheit

Ein wichtiger Bestandteil der Videoverwaltung ist die Sicherheit. In einem Netzwerk-Videoprodukt oder Videoverwaltungsprogramm sollten folgende Einstellungen festgelegt werden können:

- > Autorisierte Benutzer
- > Kennwörter
- > Verschiedene Benutzerzugriffsebenen, z. B.:
 - Administrator: Zugriff auf alle Funktionen (z. B. kann ein Administrator in AXIS Camera Station festlegen, auf welche Kameras und Funktionen ein Benutzer zugreifen darf)
 - Bediener: Zugriff auf alle Funktionen außer auf bestimmte Konfigurationsseiten
 - Betrachter: Zugriff nur auf Live-Videobilder von bestimmten Kameras

11.4 Integrierte Systeme

Wenn Video mit anderen Systemen wie Kassenterminal- und Gebäudeverwaltungssystemen kombiniert wird, können die Informationen der anderen Systeme zum Auslösen von Funktionen, z. B. ereignisgesteuerten Aufzeichnungen im Netzwerk-Videosystem, verwendet werden und umgekehrt. Darüber hinaus bietet dies Benutzern den Vorteil einer gemeinsamen Schnittstelle für die Verwaltung unterschiedlicher Systeme.

11.4.1 API (Application Programming Interface)

Alle Netzwerk-Videoprodukte von Axis verfügen über eine HTTP-basierte Programmierschnittstelle (API) oder eine Netzwerkschnittstelle namens VAPIX®, mit deren Hilfe Entwickler einfache Anwendungen erstellen können, die die Netzwerk-Videoprodukte unterstützen. Ein Videoverwaltungsprogramm oder ein Gebäudeverwaltungssystem, das VAPIX® verwendet, kann Bilder von Axis-Netzwerk-Videoprodukten anfordern, Netzwerk-Kamerafunktionen (z. B. PTZ und Relais) steuern und interne Parameterwerte festlegen oder abrufen. Tatsächlich ermöglicht es einem System, alle Funktionen auszuführen, die über die Weboberfläche des Netzwerk-Videoprodukts zur Verfügung stehen, sowie weitere Funktionen, z. B. das Erfassen nicht komprimierter Bilder in einem Bitmap-Dateiformat.

Ein globales, offenes Industrieforum namens ONVIF (Open Network Video Interface Forum) wurde Anfang 2008 von Axis, Bosch und Sony ins Leben gerufen, um die Netzwerkschnittstelle von Netzwerk-Videoprodukten zu standardisieren. Eine Standard-Netzwerkschnittstelle ermöglicht eine bessere Interoperabilität und bietet mehr Flexibilität für Endbenutzer beim Aufbau von Netzwerk-Videosystemen verschiedener Hersteller. *Weitere Informationen hierzu finden Sie unter www.onvif.org.*

11.4.2 Kassenterminals

Die Einführung von Netzwerk-Video im Einzelhandel hat die Integration von Video- mit Kassenterminalsystemen vereinfacht.

Durch die Integration können alle Registrierkassentransaktionen mit der Videoaufzeichnung der Transaktionen verknüpft werden. Dies hilft, Betrug und Diebstahl durch Angestellte und Kunden zu verhindern oder aufzudecken. Ausnahmenvorgänge am Kassenterminal wie z. B. Retouren, manuelle Eingabe von Daten und Preisen, Zeilenkorrekturen, Stornierungen von Transaktionen, Einkäufe von Mitarbeitern, Rabatte, speziell ausgezeichnete Artikel, Umtausch und Erstattungen können anhand der Videoaufzeichnung visuell überprüft werden. Ein Kassenterminalsystem mit integrierter Videoüberwachung erleichtert das Auffinden und Überprüfen verdächtiger Aktivitäten.

Es können ereignisgesteuerte Aufzeichnungen durchgeführt werden. Beispielsweise kann eine Kassenterminal-Transaktion oder -Ausnahme oder das Öffnen der Registrierkasse als Auslöser verwendet werden, um die Kameraaufzeichnung zu starten und die Aufzeichnung entsprechend zu kennzeichnen. Die Szene vor und nach einem Ereignis kann mithilfe von Pufferspeichern für die Aufzeichnung vor und nach dem Ereignis erfasst werden. Ereignisgesteuerte Aufzeichnungen erhöhen die Qualität des aufgezeichneten Materials und verringern die Speicheranforderungen sowie die Zeit, die zum Suchen von Vorkommnissen erforderlich ist.



Abbildung 11.4a Beispiel für ein Kassenterminalsystem mit integrierter Videoüberwachung. Diese Bildschirmabbildung zeigt die Belege zusammen mit Videoclips des Ereignisses. Abbildung mit freundlicher Genehmigung von Milesight Systems.

11.4.3 Zugangskontrolle

Die Integration eines Videoverwaltungssystems mit dem Zugangskontrollsystem eines Gebäudes ermöglicht die Videoüberwachung des Gebäude- und Raumzugangs. Beispielsweise kann eine Videoaufnahme an allen Türen immer dann durchgeführt werden, wenn eine Person das Gebäude bzw. den Raum betritt oder verlässt. Dies bietet im Falle eines außergewöhnlichen Ereignisses die Möglichkeit zur visuellen Überprüfung. Außerdem können auf diese Weise „Durchschlüpf“-Ereignisse aufgedeckt werden. Mit „Durchschlüpfen“ bezeichnet man den Vorgang, bei dem eine Person, die ihre Zugangsberechtigungskarte durch das Lesegerät zieht, einer anderen Person bewusst oder unbewusst den Zutritt ohne Karte ermöglicht.

11.4.4 Gebäudeverwaltung

Video kann mit einem Gebäudeverwaltungssystem (GVS) integriert werden, das verschiedene Systeme von der Heizung, Belüftung und Klimaanlage bis hin zu Sicherheits-, Energie- und Feueralarmsystemen verwaltet. Folgendes sind einige Verwendungsbeispiele:

- > Ein Geräteausfallalarm kann neben der Aktivierung von Alarmen im GVS die Aufzeichnung einer Kamera und die Live-Anzeige für den Bediener initiieren.
- > Ein Feueralarmsystem kann die Überwachung von Gebäudeausgängen durch eine Kamera sowie die Aufzeichnung zu Sicherheitszwecken auslösen.

- > Mit der Funktion für intelligentes Video kann die Rückkehr von Personen in ein Gebäude durch eine offene oder ungesicherte Tür nach einem Ereignis, wie beispielsweise einer Evakuierung, festgestellt werden.
- > Die Bewegungserkennungsfunktion einer Kamera, die sich in einem Besprechungsraum befindet, kann zusammen mit dem Beleuchtungs- und Heizungssystem verwendet werden, um das Licht und die Heizung automatisch auszuschalten, sobald alle Personen den Raum verlassen haben, um somit Energie zu sparen.

11.4.5 Industrielle Kontrollsysteme

In komplexen automatisierten Industrieanlagen ist eine externe Sichtkontrolle oftmals von Vorteil oder gar erforderlich. Durch die Möglichkeit, über dieselbe Oberfläche 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 bei einer Funktionsstörung das Senden von Bildern durch die Netzwerk-Kamera initiiert werden. Bei sensiblen Vorgängen in hochreinen Räumen oder in Einrichtungen mit gefährlichen chemischen Stoffen ist die Videoüberwachung oft die einzige Möglichkeit einer Sichtkontrolle. Dies gilt auch für Energieverteilungssysteme mit Umspannwerken in sehr abgelegenen Gegenden.

11.4.6 RFID

Verfolgungssysteme, die mit RFID (Funkerkennung) oder ähnlichen Methoden arbeiten, werden in vielen Bereichen zur Verfolgung von Objekten eingesetzt. Ein Beispiel hierfür ist die Gepäckverfolgung an Flughäfen, bei der Gepäckstücke verfolgt und an das richtige Ziel weitergeleitet werden. Bei einer Integration mit Videoüberwachung gibt es visuelle Beweise für den Fall, dass ein Gepäckstück verloren gegangen ist oder beschädigt wurde. Auch Suchroutinen können hierdurch optimiert werden.

Kriterien für die Bandbreite und den Speicher

Beim Entwurf eines Videoüberwachungssystems sind die Netzwerkbandbreiten- und Speicheranforderungen wichtige Faktoren. Zu den zu berücksichtigenden Faktoren gehören die Anzahl der Kameras, die verwendete Bildauflösung, der Komprimierungstyp, das Komprimierungsverhältnis, die Bildrate und die Komplexität der Szene. In diesem Kapitel werden einige Richtlinien zum Entwurf eines Systems gegeben sowie Speicherlösungen und verschiedene Systemkonfigurationen beschrieben.

12.1 Berechnung der Bandbreite und des Speicherplatzes

Wie viel Netzwerkbandbreite und Speicherplatz Netzwerk-Videoprodukte nutzen, richtet sich nach deren Konfiguration. Wie bereits erwähnt, ist dies von folgenden Kriterien abhängig:

- > Anzahl der Kameras
- > Kontinuierliche oder ereignisgesteuerte Aufzeichnung
- > Länge der täglichen Aufzeichnungsdauer für die Kamera
- > Bilder/Sekunde
- > Bildauflösung
- > Videokomprimierungstyp: Motion JPEG, MPEG-4 (Part 2), H.264
- > Szene: Bildkomplexität (z. B. eine graue Wand oder ein Wald), Lichtverhältnisse und Ausmaß der Bewegung (Büroumgebung oder belebter Bahnhof)
- > Aufbewahrungsdauer für aufgezeichnete Daten

12.1.1 Erforderliche Bandbreite

In einem kleinen Überwachungssystem mit 8 bis 10 Kameras kann ein 100 MBit/s-Basis-Netzwerk-Switch verwendet werden, ohne dass Beschränkungen der Bandbreite berücksichtigt werden müssen. Die meisten Unternehmen können ein Überwachungssystem dieser Größe in ihr bestehendes Netzwerk implementieren.

Bei der Implementierung von 10 oder mehr Kameras kann die Netzwerkbelastrung anhand einiger Faustregeln geschätzt werden:

- > Eine Kamera, die so konfiguriert ist, dass sie hochwertige Bilder bei hohen Bildraten liefert, beansprucht etwa 2 bis 3 MBit/s der verfügbaren Netzwerkanbandbreite.
- > Bei mehr als 12 bis 15 Kameras sollte die Verwendung eines Gigabit-Backbone-Switches in Erwägung gezogen werden. Wird ein Switch verwendet, der Gigabit unterstützt, sollte auf dem Server, auf dem die Videoverwaltungssoftware ausgeführt wird, ein Gigabit-Netzwerkadapter installiert sein.

Zu den Technologien, die die Verwaltung der Bandbreitennutzung ermöglichen, gehören die Verwendung von VLANs in einem Switch-Netzwerk, Quality of Service und ereignisgesteuerte Aufzeichnungen. Weitere Informationen zu diesen Themen finden Sie in den Kapiteln 9 und 11.

12.1.2 Berechnung des Speicherbedarfs

Wie bereits erwähnt, ist der Videokomprimierungstyp einer der Faktoren, die sich auf die Speicheranforderungen auswirken. Das Komprimierungsformat H.264 ist mit Abstand die effizienteste Videokomprimierungstechnik, die aktuell erhältlich ist. Ohne Einbußen bei der Bildqualität erreicht der H.264-Encoder bei digitalen Videodateien im Vergleich zu Motion JPEG eine um 80 % höhere Komprimierung. Gegenüber dem Standard MPEG-4 (Part 2) wird eine um 50 % höhere Komprimierung erzielt. Das bedeutet, dass H.264-Videodateien wesentlich weniger Netzbandbreite und Speicherplatz beanspruchen. In den folgenden Tabellen finden Sie Beispiele für die Berechnung des Speicherbedarfs der drei Komprimierungsformate. Da sich verschiedene Variablen auf die Angabe der durchschnittlichen Bitraten auswirken, können für H.264 und MPEG-4 keine genauen Berechnungen angestellt werden. Für Motion JPEG gibt es hingegen eine eindeutige Formel, weil Motion JPEG aus einer separaten Datei pro Bild besteht. Die Speicheranforderungen für Aufzeichnungen im Motion JPEG-Format sind je nach Bildrate, Auflösung und Komprimierstufe verschieden.

H.264-Berechnung:

Ungefährre Bitrate / 8 (Bit pro Byte) x 3600 s = KByte pro Stunde / 1000 = MByte pro Stunde

MByte pro Stunde x Betriebsstunden pro Tag / 1000 = GByte täglich

GByte täglich x erforderliche Aufbewahrungsfrist in Tagen = Speicherbedarf

Kamera	Auflösung	Ungefährre Bitrate (KBit/s)	Bilder/Sekunde	MByte/Stunde	Betriebss-tunden	GByte/Tag
Nr. 1	CIF	110	5	49,5	8	0,4
Nr. 2	CIF	250	15	112,5	8	0,9
Nr. 3	4CIF	600	15	270	12	3,2

Gesamter Speicherbedarf für die drei Kameras bei 30 Tagen Aufbewahrungsduer = 135 GByte

Tabelle 12.1a Diese Werte basieren auf Umgebungen mit viel Bewegung. In einer Umgebung mit weniger Änderungen sind die Werte etwa 20 % niedriger. Das Ausmaß der Bewegung in einer Umgebung kann sich wesentlich auf den erforderlichen Speicherplatz auswirken.

MPEG-4-Berechnung:

Ungefähr Bitrate / 8 (Bit pro Byte) x 3600 s = KByte pro Stunde / 1000 = MByte pro Stunde

MByte pro Stunde x Betriebsstunden pro Tag / 1000 = GByte täglich

GByte täglich x erforderliche Aufbewahrungsfrist in Tagen = Speicherbedarf

Hinweis: Bei dieser Formel wird das Ausmaß der Bewegung nicht berücksichtigt, bei der es sich um einen wichtigen Faktor handelt, der sich auf den erforderlichen Speicherplatz auswirken kann.

Kamera	Auflösung	Ungefähr Bitrate (KBit/s)	Bilder/Sekunde	MByte/Stunde	Betriebss-tunden	GByte/Tag
Nr. 1	CIF	170	5	76,5	8	0,6
Nr. 2	CIF	400	15	180	8	1,4
Nr. 3	4CIF	880	15	396	12	5

Gesamter Speicherbedarf für die drei Kameras bei 30 Tagen Aufbewahrungsdauer = 210 GByte

Tabelle 12.1b

Motion JPEG-Berechnung:

Bildgröße x Bilder pro Sekunde (fps) x 3600 s = Kilobyte (KByte) pro Stunde/1000 = Megabyte (MByte) pro Stunde

MByte pro Stunde x Betriebsstunden pro Tag / 1000 = Gigabyte (GByte) pro Tag

GByte täglich x erforderliche Aufbewahrungsfrist in Tagen = Speicherbedarf

Kamera	Auflösung	Ungefähr Bitrate (KBit/s)	Bilder/Sekunde	MByte/Stunde	Betriebss-tunden	GByte/Tag
Nr. 1	CIF	13	5	234	8	1,9
Nr. 2	CIF	13	15	702	8	5,6
Nr. 3	4CIF	40	15	2160	12	26

Gesamter Speicherbedarf für die drei Kameras bei 30 Tagen Aufbewahrungsdauer = 1005 GByte

Tabelle 12.1c

Ein hilfreiches Programm zur Einschätzung der Bandbreiten- und Speicheranforderungen ist das AXIS Design Tool, auf das Sie unter folgender Web-Adresse zugreifen können: www.axis.com/products/video/design_tool/

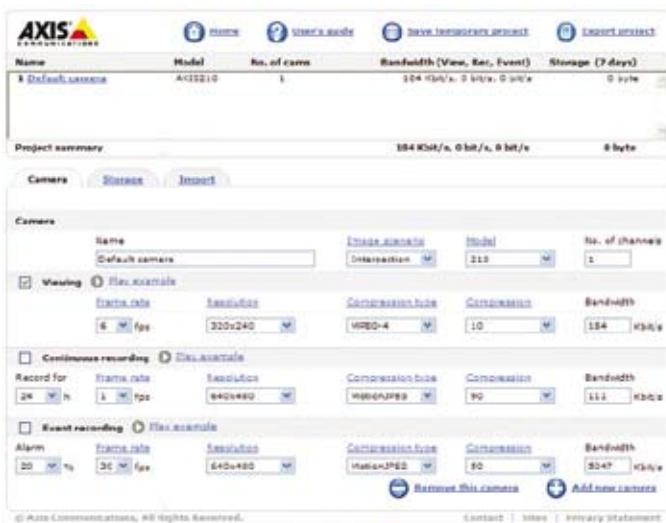


Abbildung 12.1a Das AXIS Design Tool bietet erweiterte Funktionen für das Projektmanagement, mit deren Hilfe die erforderliche Bandbreite und der Speicherplatz für große, komplexe Systeme berechnet werden kann.

12.2 Serverbasierter Speicher

Je nach CPU, Netzwerkkarte und internem RAM (Random Access Memory) eines PC-Servers kann dieser eine bestimmte Anzahl an Kameras, Bilder pro Sekunde und Bildgrößen verarbeiten. Die meisten PCs bieten Platz für 2 bis 4 Festplatten mit jeweils bis zu 300 GByte. In einer kleinen bis mittleren Installation wird der PC, auf dem die Videoverwaltungssoftware ausgeführt wird, auch für die Videoaufzeichnung verwendet. Dies wird als direkt angeschlossener Speicher bezeichnet.

Bei Verwendung der Videoverwaltungssoftware AXIS Camera Station können beispielsweise Aufzeichnungen von 6 bis 8 Kameras auf einer Festplatte gespeichert werden. Bei mehr als 12 bis 15 Kameras sollten mindestens 2 Festplatten eingesetzt werden, um die Last aufzuteilen. Ab 50 Kameras wird empfohlen, einen zweiten Server zu verwenden.

12.3 NAS und SAN

Wenn die Anforderungen an Speicherplatz und Speicherverwaltung größer sind als die verfügbare Kapazität der angeschlossenen Festplatten, sorgt ein Netzwerkspeicher (NAS) bzw. ein Speichernetzwerk (SAN) für mehr Speicherplatz, Flexibilität und Wiederherstellbarkeit.

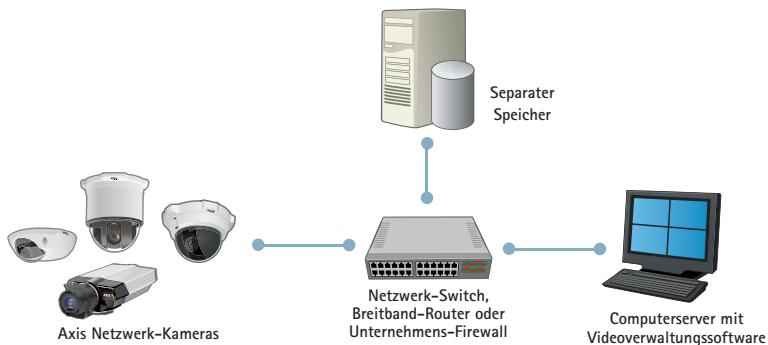


Abbildung 12.3a Netzwerkspeicher

Der NAS besteht aus einem einzelnen Speichergerät, das direkt an ein LAN angeschlossen wird und als gemeinsam genutzter Massenspeicher für alle Netzwerk-Clients dient. Ein NAS-Gerät ist eine kostengünstige Speicherlösung, die sich einfach installieren und verwalten lässt. Es bietet jedoch nur einen beschränkten Datendurchsatz für eingehende Daten, weil es nur eine Netzwerkverbindung hat, was in Hochleistungssystemen problematisch sein kann. SANs sind spezielle Hochgeschwindigkeitsnetzwerke, die als Massenspeicher dienen und in der Regel über Glasfaser an einen oder mehrere Server angeschlossen werden. 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 Multiserver-Umgebungen zur Verfügung. Die Fibre Channel-Technologie wird häufig eingesetzt, um Datenübertragungsraten von 4 GBit/s zu erreichen und große Datenmengen mit einem hohen Maß an Redundanz zu speichern.

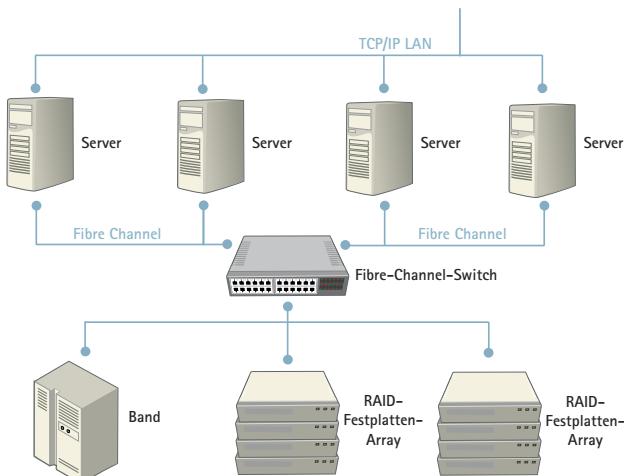


Abbildung 12.3b Eine SAN-Architektur, in der Speichereinheiten miteinander kombiniert werden und die Server die Speicherkapazität gemeinsam nutzen.

12.4 Redundante Speicherung

SAN-Systeme sorgen für Redundanzen im Speichergerät. Durch Redundanzen in einem Speichersystem können Videos oder andere Daten gleichzeitig an mehreren Speicherorten gespeichert werden. Auf diese Weise ist für die Wiederherstellung eines Videos ein Backup vorhanden, falls ein Teil des Speichersystems unlesbar wird. Diese Extra-Speicherebene kann in einem IP-Überwachungssystem auf unterschiedliche Weise bereitgestellt werden, beispielsweise durch RAID (Redundant Array of Independent Disks), Datenreplizierung, Server-Cluster und mehrere Video-Empfänger.

RAID. RAID ist die Anordnung von Standard-Festplatten zu einem Gesamtsystem, das vom Betriebssystem als eine einzige 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. RAID kann in verschiedenen Stufen umgesetzt werden, 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.

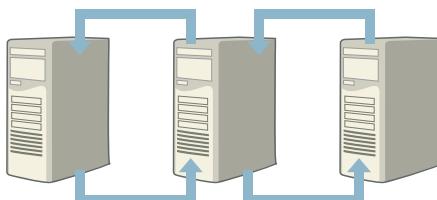


Abbildung 12.4a *Datenreplizierung.*

Datenreplizierung. Die Datenreplizierung ist ein Merkmal vieler Netzwerk-Betriebssysteme. Die Dateiserver in einem Netzwerk sind so konfiguriert, dass sie die Daten untereinander replizieren, wodurch ein Backup besteht, wenn ein Server ausfällt.

Server-Cluster. Eine typische Server-Cluster-Methode besteht aus zwei Servern, die mit demselben Speichergerät arbeiten, wie beispielsweise ein RAID-System. Wenn ein Server ausfällt, übernimmt der andere identisch konfigurierte Server. Dieser Server kann sogar dieselbe IP-Adresse haben, damit das so genannte Failover für die Benutzer vollständig transparent wird.

Mehrere Video-Empfänger. Eine gängige Methode für die Notfallwiederherstellung und das externe Speichern von Netzwerk-Video 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 replizieren. Dies ist ein besonders nützlicher Ansatz, wenn sich die Überwachungssysteme in gefährlichen oder schwer zugänglichen Bereichen befinden, wie beispielsweise in Massentransportmitteln oder in Industrieanlagen.

12.5 Systemkonfigurationen

Kleines System (1 bis 30 Kameras)

Ein kleines System besteht in der Regel aus einem Server, auf dem eine Überwachungsanwendung ausgeführt wird, die das Video auf einer lokalen Festplatte aufzeichnet. Das Video wird über denselben Server angezeigt und verwaltet. Obwohl die meisten Anzeige- und Verwaltungsaufgaben auf dem Server ausgeführt werden, kann zum selben Zweck ein Client (lokal oder remote) angeschlossen werden.

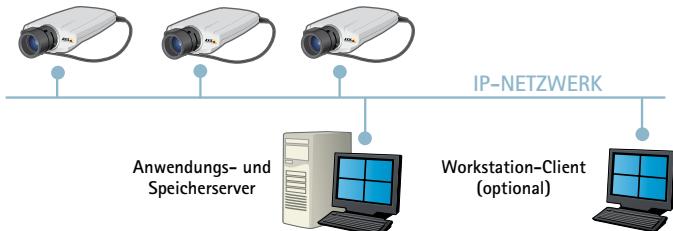


Abbildung 12.5a Ein kleines System.

Mittleres System (25 bis 100 Kameras)

Für eine typische Installation mittlerer Größe wird ein Server mit zusätzlichem Speicher verwendet. Der Speicher wird normalerweise mit RAID konfiguriert, um die Leistung und die Zuverlässigkeit zu erhöhen. Das Video wird normalerweise nicht über den Aufzeichnungsserver, sondern über einen Client angezeigt und verwaltet.

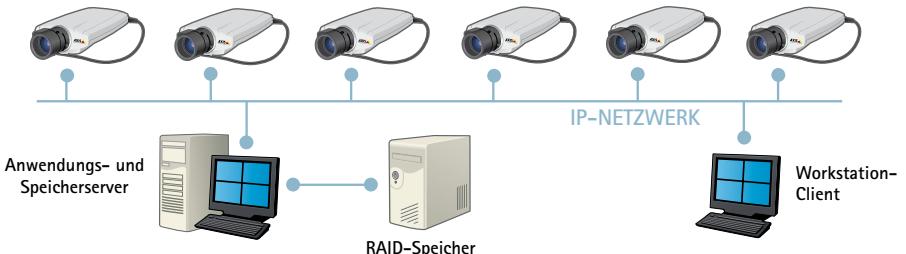


Abbildung 12.5b Ein mittleres System.

Großes zentrales System (50 bis über 1000 Kameras)

Für eine große Installation ist eine hohe Leistung und Zuverlässigkeit erforderlich, damit die hohe Daten- und Bandbreitenmenge verarbeitet werden kann. Hierfür werden mehrere Server benötigt, denen bestimmte Aufgaben zugewiesen sind. Ein Master-Server steuert das System und entscheidet, welche Videos auf welchem Speicherserver gespeichert werden. Da spezielle Speicherserver vorhanden sind, ist eine Lastverteilung möglich. In einem solchen Setup ist es auch möglich, das System zu vergrößern, indem bei Bedarf weitere Speicherserver hinzugefügt werden und Wartungen durchgeführt werden können, ohne das gesamte System abschalten zu müssen.

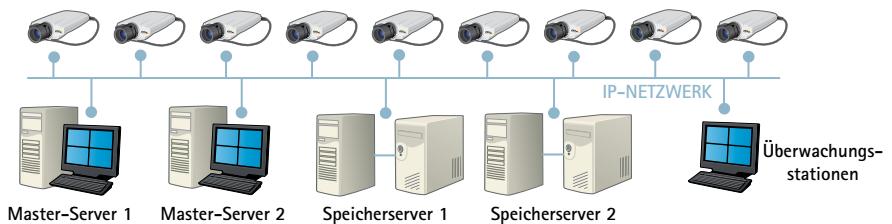


Abbildung 12.5c Ein großes zentrales System.

Großes verteiltes System (25 bis über 1000 Kameras)

Für die Überwachung mehrerer Standorte, die zentral verwaltet werden sollen, können verteilte Aufzeichnungssysteme verwendet werden. An jedem Standort wird das Video über lokale Kameras aufgezeichnet und gespeichert. Der Master-Controller kann die Aufzeichnungen aller Standorte anzeigen und verwalten.

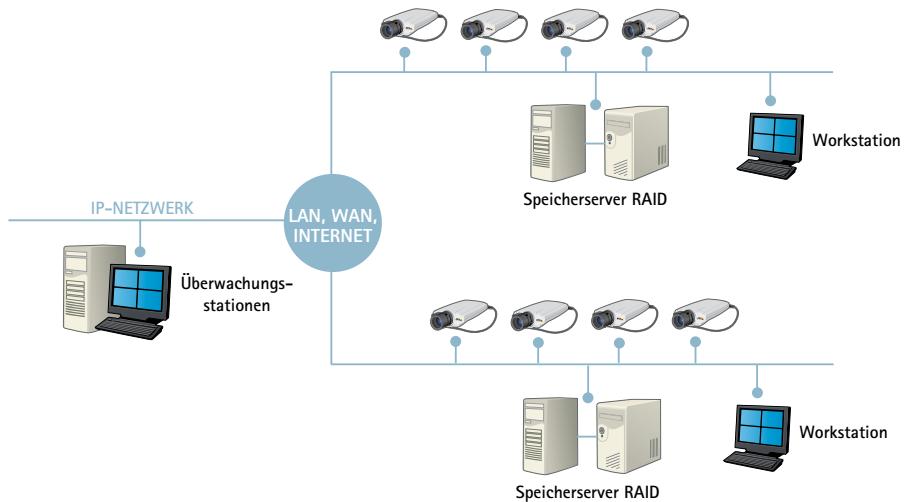


Abbildung 12.5d Ein großes verteiltes System



Tools und Ressourcen

Axis bietet für den Entwurf eines IP-Überwachungssystems viele hilfreiche Tools und Informationsressourcen an. Die meisten davon können über die Axis-Website abgerufen werden: www.axis.com/tools

Objektivrechner

Mit diesem Tool berechnen Sie die erforderliche Brennweite des Objektivs, um eine bestimmte Szene in einer bestimmten Entfernung zu erfassen.

Tool für die Kamerareichweite

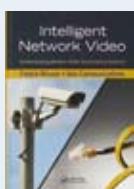
Das Tool erweitert die Möglichkeiten der Axis Netzwerk-Kameras hinsichtlich der Erfassung von Umgebungen und der Erkennung von Objekten bei verschiedenen Entfernungen und in Kombination mit unterschiedlichen Objektiven. Es erleichtert Ihnen außerdem die Orientierung im Produktsortiment von Axis, um die für Ihre Zwecke optimal geeignete Kamera zu finden.

AXIS Design Tool

Mit diesem simulationsgestützten Rechner, der online oder auf DVD erhältlich ist, können Sie die Bandbreite und den Speicherbedarf Ihres eigenen Netzwerk-Videoprojekts bestimmen.

Axis-Konfigurator für Gehäuse

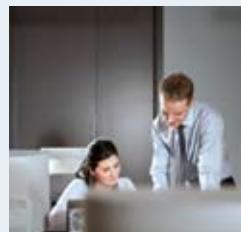
Dieses Tool hilft Ihnen dabei, die richtigen Gehäuse und ergänzendes Zubehör wie z. B. Halterungen, Netzteile und Kabel für Ihre spezielle Kameraanwendung zu finden.



Intelligent Network Video:

Understanding modern surveillance systems

Dieses 390-seitige Buch wurde von Fredrik Nilsson und Axis Communications geschrieben. Es ist die erste Ressource, die detailliert die erweiterten digitalen Netzwerk- und intelligenten Videofunktionen beschreibt. Es wurde im September 2008 veröffentlicht und kann über Amazon, Barnes & Noble und CRC Press bestellt werden. Sie können sich aber auch an eine Axis-Niederlassung wenden.



Axis Communications' Academy

Die erste Adresse für fundiertes Wissen im Bereich Netzwerk-Video.

Absolvieren Sie das Schulungsprogramm von Axis, um mehr über Netzwerk-Video-technologien zu erfahren.

- > Vielfältiges Kursangebot
- > Praxisorientierte Schulungen
- > Schulung durch führende Experten
- > Wettbewerbsvorteile sichern

Die allmähliche Umstellung älterer analoger Systeme auf die Netzwerk-Videotechnologie führt zu einem Umbruch im Videoüberwachungsmarkt. Dieser Umbruch wird durch neue Verfahren, Anwendungen und Integrationsmöglichkeiten beschleunigt. Um den zunehmenden Wettbewerb auf diesem Markt erfolgreich zu bestehen, benötigen Sie überdurchschnittliche Kenntnisse zu IP-basierten Videosystemen. Nutzen Sie die Axis Communications' Academy, die erste Adresse für fundiertes Wissen im Bereich Netzwerk-Video, um den Wettbewerbern immer einen Schritt voraus zu sein.

Erlernen der Grundlagen

"Grundlagen von Netzwerk-Video" und "Grundlagen von Videolösungen" sind die Basiskomponenten des Schulungsprogramms der Axis Communications' Academy. Die Grundlagen wurden so ausgearbeitet, dass sie den Fortbildungsanforderungen von Experten für herkömmliche analoge CCTV-Technologie und für IT-Systeme entsprechen. Sie können daher, unabhängig von Ihren bisherigen Kenntnissen, genau das Maß an erweitertem technischen Fachwissen erreichen, das Sie für die erfolgreiche Arbeit mit den Produkten und Lösungen von Axis benötigen.

Informieren Sie sich unter www.axis.com/academy

Kontaktinformationen

www.axis.com/request

FIRMENZENTRALE

SCHWEDEN

Axis Communications AB
Emdalavägen 14
SE-223 69 Lund
Tel: +46 46 272 18 00
Fax: +46 46 13 61 30

ARGENTINIEN

Axis Communications
Av. Del Libertador 2442, Piso 4,
CP B1636SR Olivos
Buenos Aires
Tel. +54 11 5368 0569
Fax +54 11 5368 2100 Int. 0569

AUSTRALIEN

Axis Communications Pty Ltd.
Level 27, 101 Collins Street
Melbourne VIC 3000
Tel: +613 9221 6133

BRASILIEN

Axis Communications
Rua Mario Amaral 172, 13º
Andar, Conjunto 131
04002-020, São Paulo
Tel. +55 11 3050 6600

CHINA

Shanghai Axis Communications
Equipment Trading Co.,Ltd.
Room 6001, Novel Building
887 Huai Hai Zhong Rd.
Shanghai 200020
Tel: +86 21 6431 1690

CHINA (weiter)

Beijing Axis Communications
Rm. 2003, Tower B
Tian Yuan Gang Center C2
Dongsanhuan North Road
Chaoyang District
Beijing 100027
Tel: +86 10 8446 4990
Fax: +86 10 8286 2489

DEUTSCHLAND, ÖSTERREICH, SCHWEIZ

Axis Communications GmbH
Lilienthalstr. 25
DE-85399 Hallbergmoos
Tel: +49 811 555 08 0
Fax: +49 811 555 08 69
Support: +49 1805 2947 78

FRANKREICH, BELGIEN, LUXEMBURG

Axis Communications SAS
Antony Parc I
2 à 8 place du Général de
Gaulle, 92160 Antony
France
Tel : +33 (0)1 40 96 69 00
Fax : +33 (0)1 46 74 93 79

GROSSBRITANNIEN

Axis Communications (UK) Ltd
Suite 6-7, Ladygrove Court
Hitchwood Lane
Preston, Nr Hitchin
Hertfordshire SG4 7SA
Tel: +44 146 242 7910
Fax: +44 146 242 7911
Support: +44 871 200 2071

HONGKONG

Axis Communications Limited
Unit 1801, 18/F
88 Gloucester Road, Wanchai
Hong Kong
Tel: +852 2511 3001
Fax: +852 2511 3280

INDIEN

Axis Video Systems India
Private Limited
Kheny Chambers
4/2 Cunningham Road
Bangalore 560002
Karnataka
Tel: +91 (80) 4157 1222
Fax: +91 (80) 4023 9111

ITALIEN

Axis Communications S.r.l.
Corso Alberto Picco, 73
10131 Torino
Tel: +39 011 819 88 17
Fax: +39 011 811 92 60

JAPAN

Axis Communications K.K.
Shinagawa East 1 Tower 13F
2-16-1 Konan
Minato-ku Tokyo 108-0075
Tel: +81 3 6716 7850
Fax: +81 3 6716 7851

Kontaktinformationen

www.axis.com/request

KANADA

Axis Communications, Inc.
117 Lakeshore Road East
Suite 304
Mississauga ON L5G 4T6
Tel: +1 800 444 AXIS (2947)
Fax: +1 978 614 2100
Support: +1 800 444 2947

KOREA

Axis Communications Korea Co., Ltd.
Rm 407, Life Combi B/D.
61-4 Yoido-dong
Yeongdeungpo-Ku, Seoul
Tel: +82 2 780 9636
Fax: +82 2 6280 9636

MEXIKO

AXISNet, S.A. de C.V.
Unión 61, 2º piso
Col. Escandón, Mexico City
México, D.F., C.P. 11800
Tel: +52 55 5273 8474
Fax: +52 55 5272 5358

NIEDERLANDE

Axis Communications BV
Glashaven 38
NL-3011 XJ Rotterdam
Tel: +31 10 750 46 00
Fax: +31 10 750 46 99
Support: +31 10 750 46 31

RUSSISCHE FÖDERATION

000 Axis Communications
Leningradsky prospekt
31/3, of.405
125284, Moscow
Tel: +7 495 940 6682
Fax: +7 495 940 6682

SINGAPUR

Axis Communications
(S) Pte Ltd.
7 Temasek Boulevard
#11-01A Suntec Tower 1
Singapore 038987
Tel: +65 6 836 2777
Fax: +65 6 334 1218

SPANIEN

Axis Communications
C/ Yunque 9, 1A
28760 Tres Cantos, Madrid
Tel: +34 91 803 46 43
Fax: +34 91 803 54 52
Support: +34 91 803 46 43

SÜDAFRIKA

Axis Communications SA
Pty Ltd.
Hampton Park, Atterbury
House, 20 Georgian Crescent
Bryanston, Johannesburg
Tel: +27 11 548 6780
Fax: +27 11 548 6799

PO Box 70939
Bryanston 2021

TAIWAN

Axis Communications Ltd.
8F-11,101 Fushing North Road
Taipei
Tel: +886 2 2546 9668
Fax: +886 2 2546 1911

USA

Axis Communications Inc.
100 Apollo Drive
Chelmsford, MA 01824
Tel: +1 978 614 2000
Fax: +1 978 614 2100
Support: +1 800 444 2947

VEREINIGTE ARABISCHE EMIRATE

Axis Communications
Middle East
PO Box 293637
DAFZA, Dubai
Tel: +971 4 609 1873

Hintergrund Axis Communications

Axis ist ein IT-Unternehmen, das Netzwerk-Videolösungen für professionelle Installationen anbietet. Das Unternehmen ist der weltweite Marktführer im Bereich Netzwerk-Video und treibt den Wechsel von analoger zu digitaler Videoüberwachungs-Technologie an. Die Produkte und Lösungen von Axis konzentrieren sich auf Anwendungen wie Sicherheits- und Fernüberwachung und basieren auf einer innovativen und offenen Technologie-Plattform.

Axis ist ein schwedisches Unternehmen und weltweit mit Niederlassungen in mehr als 20 Ländern tätig und arbeitet mit Vertriebspartnern in mehr als 70 Ländern zusammen. Axis wurde 1984 gegründet und ist an der NASDAQ OMX Stockholm unter dem Börsenschreiber AXIS notiert. Weitere Informationen über Axis finden Sie unter www.axis.com