Technischer Leitfaden zur Netzwerk-Videotechnologie

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

AXIS COMMUNICATIONS

Technischer Leitfaden zur Netzwerk-Videotechnologie

Offene Videosysteme haben, zusammen mit der Netzwerk-, Digitalbild- und Kameratechnologie, die Grundlage für einen enormen technologischen Effizienzschub bei der Sicherheits- und Fernüberwachung gesorgt. Netzwerk-Video bietet nicht nur alle Vorzüge herkömmlicher Analogtechnik, sondern auch innovative Funktionen, die erst durch die Digitaltechnologie möglich geworden sind.

Bevor Sie Ihr System einrichten, sollten Sie sich mit seinen Möglichkeiten befassen. Ebenso wichtig sind Faktoren wie Leistung, Kompatibilität, Skalierbarkeit, Flexibilität und Zukunftssicherheit. Dieses Handbuch führt Sie durch diese Faktoren und hilft Ihnen beim Finden einer Lösung, die das volle Potenzial der Netzwerk-Videotechnologie ausschöpft.

Spitzenstellung auf dem Weltmarkt

Axis ist der Weltmarktführer in der Netzwerktechnologie. Seit 1984 entwickeln wir Lösungen, die den Nutzen Ihres Netzwerks erhöhen. Seit 1996 konzentrieren wir uns dabei hauptsächlich auf Netzwerk-Videolösungen. Mit mehr als 600.000 Netzwerk-Videoprodukten für den professionellen Einsatz und über 3 Millionen installierten Netzwerkprodukten verfügt Axis über den Erfahrungshorizont, den Sie für Ihr Unternehmen brauchen. Die langjährige Erfahrung und unsere Spitzenstellung bei der technologischen Weiterentwicklung machen Axis zur ersten Adresse, wenn es um Netzwerk-Video geht.

Axis hat sich auf professionelle Videolösungen für Sicherheitsüberwachung, Fernüberwachung und Broadcasting spezialisiert. Zu unserer Produktpalette gehören Netzwerk-Kameras, Videoserver, Videodecoder, Videoverwaltungssoftware und ein umfangreiches Sortiment an Audio- und Videozubehör.

Spitzenstellung in der Technologie

Das Kernstück des Axis Produktangebotes ist eine IP-basierte Technologie-Plattform, die im eigenen Hause entwickelt wurde. Dadurch kann unser Unternehmen sein Produktangebot schnell und kostengünstig an neue Anwendungen und Produktbereiche anpassen. Diese Technologie ermöglicht eine einfache Installation und die Konzipierung kompakter und leistungsstarker Lösungen, mit denen Geräte rasch und sicher in praktisch alle kabellosen oder kabelgebundenen Netzwerke eingebunden werden können.

Inhaltsverzeichnis

1. Einführung in die netzwerk-videotechnik 7
1.1. Was ist Netzwerk-Video? 7
1.2. Was genau ist eine Netzwerk-Kamera? 8
1.3. Was ist ein Videoserver? 10
1.4. Was versteht man unter Video-Verwaltungssoftware? 10

2. Die evolution der video-überwachungssysteme 13
2.1. Analoge CCTV-Systeme mit Videorecorder 13
2.2. Analoge CCTV-Systeme mit DVR 14
2.3. Analoge CCTV-Systeme mit Netzwerk-DVR 14
2.4. Netzwerk-Videosysteme mit Videoservern 15
2.5. Netzwerk-Videosysteme mit Netzwerk-Kameras 15

3. Bildgenerierung 17
3.1. CCD- und CMOS-Sensoren 17
3.2. Progressive Abtastung oder Halbbild-Video? 18
3.2.1. Zeilensprungverfahren (Halbbild) 18
3.2.2. Progressive Abtastung 19
3.2.3. Beispiel: Erfassen bewegter Objekte 19
3.3. Komprimierung 20
3.3.1. Komprimierungsstandards für Einzelbilder 20
3.3.2. Video-Komprimierungsstandards 21
3.4. Bildauflösung 24
3.4.1. Bildauflösung unter NTSC und PAL 24
3.4.2. VGA-Auflösung 25
3.4.3. MPEG-Auflösung 25
3.4.4. Auflösungen im Megapixel-Bereich 26
3.5. Einsatz bei Tag und Nacht 27

Hinweise zum Einsatz von Kameras 29
4.1. Verwenden von Netzwerk-Kameras 29
4.1.1. Kameratypen 29
4.1.2. Auswahl der Objektive 31
4.1.3. Montage im Innen- und Außenbereich 34
4.1.4. Praktische Empfehlungen 34
4.2. Einsatz von analogen Kameras mit Videoservern 36
4.2.1. Einbau von Videoservern in ein Rack 36
4.2.2. Videoserver mit einem Anschluss 37
4.2.3. Videoserver mit PTZ- und Dome-Kameras 37
4.2.4. Video-Decoder 38

5. IP-Netzwerk-Technik 39
5.1. Ethernet 39
5.2. Power-over-Ethernet 40
5.3. Kabellose Netzwerke 41
5.4. Datentransportmethoden 43
5.4.1 IP-Adressen 43
5.4.2 IPv6 44
5.4.3 Datenübertragungsprotokolle für Netzwerk-Video 44
5.4.4 Übertragungsmethoden für Netzwerk-Video Unicasting, Multicasting und Rundsendung 45
5.5. Netzwerksicherheit 45
5.5.1 Sichere Übertragung 45
5.5.2 Sicherheit in kabellosen Netzwerken 47
5.5.3 Schutz von einzelnen Geräten 48
5.6 QoS (Quality of Service) 48
5.7. Weitere Informationen zu Netzwerk-Technologien und Geräten 50

6. Kriterien für die Systemkonfiguration 53
6.1. Kriterien für das Systemdesign 53
6.1.1 Bandbreite 53
6.1.2 Speicherplatz 54
6.1.3 Redundanz 56
6.1.4 Skalierbarkeit 57
6.1.5 Steuerung der Bildrate 57
6.2. Speicheranforderungen 58
6.2.1 Direkt angeschlossener Festplattenspeicher 58
6.2.2 Netzwerkspeicher (NAS) und Speichernetzwerk (SAN) 59
6.2.3 RAID (Redundant Array of Independent Disks) 59
6.3. Sicherheitsfunktionen 60
6.4. Verwalten von Großsystemen 60

7. Videoverwaltung 63
7.1 Hardware-Plattformen 63
7.1.1 PC-Server-Plattformen 64
7.1.2 NVR-Plattformen 64
7.2 Videoverwaltung: Überwachung und Aufzeichnung 65
7.2.1 Überwachen mit der Web-Oberfläche 65
7.2.2 Überwachung mit Hilfe der Videoverwaltung 66
7.2.3 Aufzeichnung von Netzwerk-Video 66

7.3 Systemmerkmale 67
7.3.1 Video-Bewegungserkennung 67
7.3.2 Audio 69
7.3.3 Digitale Ein- und Ausgänge 70
7.4 Integrierte Systeme 72

8. Intelligente Videosysteme 73
8.1 Was ist unter intelligentem Video zu verstehen? 73
8.2 Intelligente Videoarchitektur 73
8.2.1 DVRs und zentrale Analyse 73
8.2.2 Netzwerk-Videosysteme und verteilte Intelligenz 74
8.3 Typische Anwendungen 75
8.3.1 Personenzählung 75
8.3.2 Erkennung von Autokennzeichen 75
8.3.3 Zugangsschranken: Stolperdraht für Straftäter 76
8.4 Komponenten auf der Basis offener Standards 76

Kurzanleitung: Checkliste für den Aufbau eines Netzwerk-Video Systems 77
1. Analoge Kamera/DVR oder Netzwerk-Kamera? 77
2. Auswahl einer Netzwerk-Kamera: Die wichtigsten Kriterien für die richtige Entscheidung 82
3. Richtlinien für den Aufbau Ihres Netzwerk-Video Projektes 84
4. Projekttools 85

AXIS Academy 87

Kontaktinformationen 91

Einführung in die Netzwerk-Videotechnik

Die Video-Überwachungsbranche bietet heute ein breites Sortiment an Systemen und Geräten zur Überwachung und für die Sicherheit von Personen und Eigentum an. Um die Tragweite und das Potenzial eines integrierten, volldigitalen Systems verständlich zu machen, wenden wir uns zunächst den Kernkomponenten eines Netzwerk-Videosystems zu: der Netzwerk-Kamera, dem Videoserver und der Video-Verwaltungssoftware. Bei der Wahl eines geeigneten Systems ist es sinnvoll, die verfügbaren Technologien im Hinblick auf das gewünschte Anwendungsgebiet und die Anforderungen (Kosteneffizienz, Skalierbarkeit, Benutzerfreundlichkeit und Flexibilität) zu vergleichen.

1.1. Was ist Netzwerk-Video?

Netzwerk-Video, oft auch als IP-Überwachung für bestimmte Anwendungsgebiete bei der Sicherheits- und Fernüberwachung betrachtet, gibt den Benutzern die Möglichkeit, Video über ein IP-Netzwerk (LAN/WAN/Internet) zu überwachen und aufzuzeichnen.

Anders als bei analogen Systemen, die eine spezielle Punkt-zu-Punkt-Verkabelung erfordern, dient beim Netzwerk-Video das Netzwerk als Daten-Transportmittel. Der Begriff „Netzwerk-Video“ bezieht sich sowohl auf Video- als auch auf Audioquellen, die über das System verfügbar sind. Bei Netzwerk-Video-Anwendungen werden digitale Datenströme über ein kabelgebundenes oder kabelloses IP-Netzwerk an einen beliebigen Standort geleitet. Daher kann die Video-Überwachung und -Aufzeichnung überall im Netzwerk durchgeführt werden

Netzwerk-Video eignet sich für fast jede Situation. In der Praxis wird es jedoch in erster Linie für zwei Bereiche eingesetzt:

- **Sicherheitsüberwachung**
  Dank ihrer großen Funktionsmöglichkeiten ist die Netzwerk-Videotechnik ein ideales Hilfsmittel für die Sicherheitsbranche. Die Flexibilität der Digitaltechnik verbessert die Möglichkeiten zum Schutz von Personen und Eigentum erheblich. Solche Systeme sind daher eine besonders attraktive Option für Unternehmen, die derzeit CCTV einsetzen.

- **Fernüberwachung**
  Mit Netzwerk-Video können Informationen an allen Schlüsselpunkten des Einsatzbereichs gesammelt und live in Echtzeit angezeigt werden. Dadurch eignet sich diese Technik ideal zur lokalen und fernen Überwachung von Geräten, Personen und Standorten. Eingesetzt wird Netzwerk-Video zum Beispiel im Verkehrswesen und bei der Überwachung von Fertigungsstraßen oder von mehreren Handelsfilialen.

Die wichtigsten vertikalen Märkte, auf denen Netzwerk-Videosysteme erfolgreich installiert wurden, sind:

- **Bildungswesen**
  Sicherheits- und Fernüberwachung von Spielbereichen, Korridoren und Klassenzimmern sowie die Sicherheitsüberwachung der Gebäude.
- **Verkehrswesen**
  Fernüberwachung von Bahnhöfen und Gleisen, Autobahnen, Fernstraßen und Flughäfen.
- **Bankwesen**
  Traditionelle Sicherheitsanwendungen für Bankzentralen, Zweigstellen und Geldautomaten.
- **Regierungswesen**
  Für Überwachungseinsätze und zur Erhöhung der öffentlichen Sicherheit.
- **Einzelhandel**
  Zur Sicherheits- und Fernüberwachung: das Sicherheitsmanagement von Geschäften wird vereinfacht und verbessert.
- **Industrie**
  Überwachung von Fertigungsprozessen, Logistiksystemen, Lager- und Bestandskontrolle.

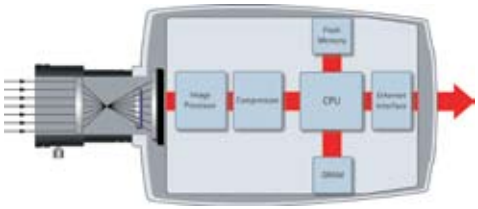
1.2. Was genau ist eine Netzwerk-Kamera?

Netzwerk-Kameras lassen sich als Kombination aus Kamera und Computer beschreiben. Sie erfassen und übertragen Live-Bilder direkt über ein IP-Netzwerk und ermöglichen es befugten Benutzern, Video über eine IP-basierte Standard-Netzwerk-Infrastruktur lokal oder entfernt anzuzeigen, zu speichern und zu verwalten.

Produktübersicht
Netzwerk-Kameras verfügen über eine eigene IP-Adresse. Sie werden an das Netzwerk angeschlossen und verfügen über einen integrierten Webserver, FTP-Server, E-Mail-Client, Alarm-Management und Programmfunktionen. Netzwerk-Kameras müssen nicht an einen PC angeschlossen werden. Sie arbeiten unabhängig und können an jeder kompatiblen IP-Schnittstelle mit dem Netzwerk verbunden werden. Davon unterschieden werden müssen Web-Kameras: Letztere müssen über USB oder IEEE1394 an einen PC angeschlossen werden, der ihre Daten weiterverarbeitet.

Neben Video bieten Netzwerk-Kameras weitere Funktionen und können verschiedene Datentypen über dieselbe Netzwerk-Anbindung transportieren, zum Beispiel Ein- und Ausgangsdaten, Audio, serielle Daten (über serielle Schnittstellen) oder PTZ-Daten zur Kamerasteuerung.

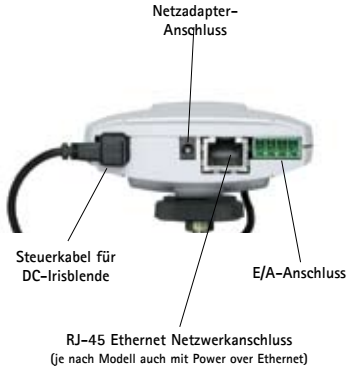
Kamera-Komponenten



Innenansicht einer Netzwerk-Kamera. Prozessor, Flash- und DRAM-Speicher sind abgestimmt auf Netzwerkanwendungen.

Front-Ansicht Rück-Ansicht

Front-Ansicht Rück-Ansicht



Vergleich zwischen Netzwerk- und Analog-Kameras

In den letzten Jahren hat die Netzwerk-Kamera die analoge Kamera technisch eingeholt und erfüllt jetzt dieselben Anforderungen und Spezifikationen. In puncto Leistung hat sie die Analog-Kamera dank ihrer hochmodernen Funktionen, die weiter unten beschrieben werden, sogar überholt.

Kurz gesagt ist eine Analog-Kamera ein Erfassungsgerät, das Signale in nur einer Richtung überträgt und auf DVR- und Bedienerebene endet. Netzwerk-Kameras hingegen übertragen Daten in beide Richtungen und sind im restlichen System vollständig integriert, wodurch eine verteilte und skalierbare Umgebung entsteht. Sie kommunizieren mit mehreren Anwendungen gleichzeitig, um verschiedene Aufgaben zu erfüllen und können zum Beispiel Bewegungen erkennen und melden oder verschiedene Video-Datenströme versenden.

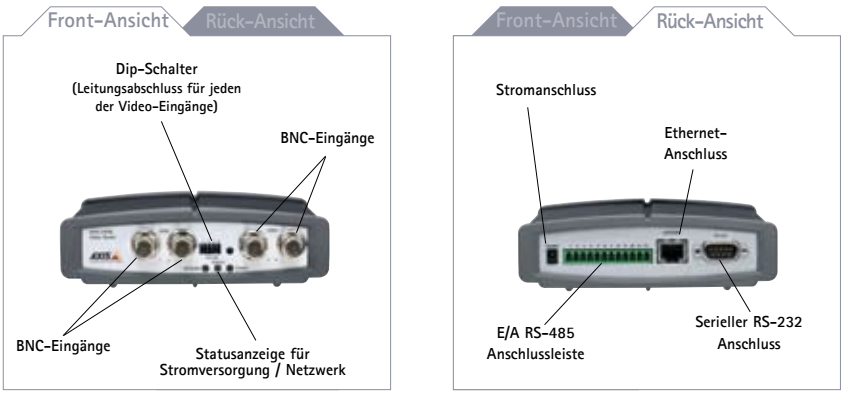
Weitere Informationen zum Einsatz von Netzwerk-Kameras finden Sie in Kapitel 4.1 auf Seite 29.

1.3. Was ist ein Videoserver?

Videoserver ermöglichen den Umstieg auf ein Netzwerk-Videosystem, ohne dass der Anwender seine vorhandene, analoge Ausrüstung aufgeben muss. Sie verschafft den analogen Geräten neue Funktionen und macht dezidierte Komponenten wie Koaxialkabel, Monitore und Videorecorder überflüssig. Die Videorecorder werden nicht mehr benötigt, weil die Aufzeichnung mit PC-Standard-Servern bewerkstelligt werden kann.

Produktübersicht
Videoserver verfügen meist über ein bis vier Analogschnittstellen zum Anschließen von Analog-Kameras sowie über eine Ethernet-Schnittstelle für die Anbindung an das Netzwerk. Ebenso wie Netzwerk-Kameras verfügen sie über einen integrierten Webserver, einen Komprimierungschip und ein Betriebssystem, damit eingehende Analogdaten digitalisiert, übertragen und über das Computernetzwerk aufgezeichnet werden können, so dass sie leichter abgerufen und angezeigt werden können.

Neben dem Video-Eingang bieten Videoserver weitere Daten- und Anschlusstypen: digitale Ein- und Ausgangsdaten, Audiodaten sowie serielle Schnittstellen für serielle Daten oder zur PTZ-Kamerasteuerung. Der gesamte Datenaustausch mit dem Netzwerk wird dabei über dieselbe Netzwerkschnittstelle geleitet. Videoserver können auch mit unterschiedlichsten Spezialkameras wie hochempfindlichen Schwarzweiß-Kameras, Minikameras oder Mikroskop-Kameras verbunden werden.



Weitere Informationen zur Kombination von Analog-Kameras mit Videoservern finden Sie in Kapitel 4.2 auf Seite 36.

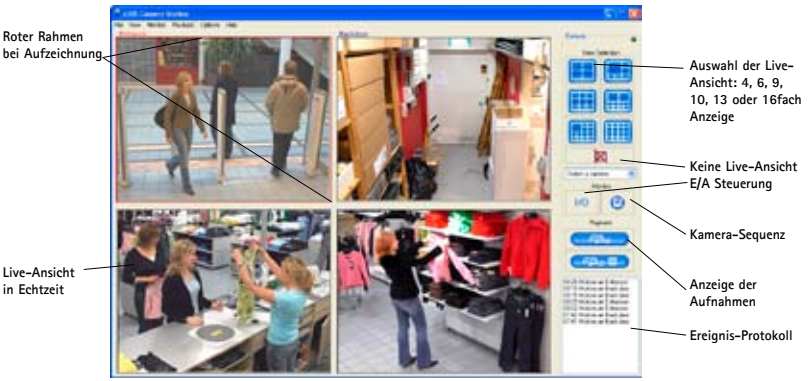
1.4. Was versteht man unter Video-Verwaltungssoftware?

Video-Verwaltungssoftware, die auf einem Windows- oder Unix/Linux-Server ausgeführt wird, bildet die Basis zur Video-Überwachung, -Analyse und -Aufzeichnung. Es sind viele verschiedene Software-Produkte für die unterschiedlichsten Anforderungen auf dem Markt. Ein Standard-Browser genügt als Anzeigeprogramm für viele Anwendungen von Netzwerk-Video, besonders wenn nur eine oder wenige Kameras gleichzeitig angezeigt werden sollen. Er nutzt dabei die Internet-Schnittstelle der Netzwerk-Kamera bzw. des Videoservers.

Sollen mehrere Kameras gleichzeitig erfasst werden, wird spezielle Video-Verwaltungssoftware benötigt. Es sind viele verschiedene Video-Verwaltungsprogramme erhältlich. In ihrer einfachsten Form bieten sie eine Live-Anzeige sowie Speicher, und Abruffunktionen für Videosequenzen. Komfortablere Programme bieten Funktionen wie:

- Gleichzeitiges Anzeigen und Aufzeichnen von Live-Video von mehreren Kameras
- Mehrere Aufzeichnungsmodi: fortlaufend, geplant, nach Alarmmeldungen und bei gemeldeten Bewegungen
- Verarbeitung hoher Bildraten und großer Datenaufkommen
- Umfassende Suchfunktionen für aufgezeichnete Ereignisse
- Entfernter Zugriff über Browser, Client-Software und PDA-Clients
- Steuerung von PTZ- und Dome-Kameras
- Alarmverwaltungsfunktionen (akustische Warnung, Popup-Fenster oder E-Mail)
- Unterstützung vor Vollduplex-Audio in Echtzeit
- Intelligente Video-Überwachung

Beispiel einer Windows-basierten Videoverwaltung Software



Weitere Informationen zu Video-Verwaltungssoftware finden Sie in Kapitel 6.3 auf Seite 60.

Anwendungsentwicklung

Axis bietet Anwendungssoftware für verschiedenste Anforderungen an. Damit ein möglichst breites Software-Angebot zur Verfügung steht, können unabhängige Entwickler und Partner Axis Videoprodukte in ihre Anwendungen integrieren.

Axis hat ein standardisiertes Befehlspaket für CGI-Programme entwickelt. (CGI steht für „Common Gateway Interface“, gemeinsame Gateway-Schnittstelle.) Diese Anweisungen bilden zusammen die Axis HTTP-API. In ihrer einfachsten Form können CGI-Befehle für Bewegungserkennung, Ereignissteuerung, Alarm-Benachrichtigung über E-Mail, entferntes Speichern von Videos usw. direkt in die URL-Zeile des Browsers eingegeben werden.

Axis hat zudem ein Software-Entwicklungskit entwickelt (SDK). Mit dem Kit und der dazugehörigen Dokumentation können Entwickler Videoprodukte von Axis in Windows-Anwendungen integrieren. Außerdem können Scripts zur Ausführung auf den Videoprodukten programmiert werden. Dadurch kann die Funktionaliät der Videoprodukte genau an spezielle Erfordernisse angepasst werden. *Weitere Informationen zur Unterstützung von Entwicklern finden Sie unter www.axis.com/techsup/cam_servers/dev/*

Axis ADP-Programm

Die ADP-Partner von Axis bieten ein breites Spektrum an umfassenden Software-Lösungen an, die unterschiedlichen Spezifikationen und Anforderungen Rechnung tragen: von der Einsteiger-Software bis zu Komplettanwendungen für die meisten Branchensegmente.

Weitere Informationen zu den Axis ADP-Partnern finden Sie unter www.axis.com/partner/adp_intro.htm

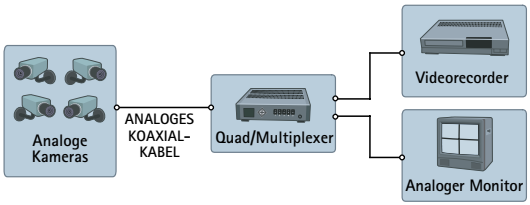
Die Evolution der Video-Überwachungssysteme

Video-Überwachungssysteme gibt es seit ca. 25 Jahren. Die zunächst rein analog angelegten Systeme weichen zunehmend digitalen Nachfolgern. Heutige Systeme sind den frühen analogen Rohrkameras, die an einen Videorecorder angeschlossen wurden, weit überlegen. Sie basieren auf Netzwerk-Kameras und PC-Servern, die Video in einem volldigitalen System aufzeichnen. Allerdings gibt es zwischen den vollanalogen und volldigitalen Systemen verschiedene teildigitale Lösungen. Sie enthalten eine Reihe digitaler Komponenten, sind aber nicht durchgängig digitalisiert.

Alle Systeme, die in den Abschnitten 2.2 und 2.3 beschrieben werden, sind solche teildigitalen Videosysteme. Nur die Systeme in Kapitel 2.4 und 2.5 stellen echte Netzwerk-Videosysteme dar, die Videodaten fortlaufend über ein IP-Netzwerk transportieren und uneingeschränkte Skalierbarkeit und Flexibilität bieten.

2.1. Analoge CCTV-Systeme mit Videorecorder

Ein analoges CCTV-System mit Videorecorder stellt ein vollanaloges System mit Koaxialausgang dar, an dem der Videorecorder zum Aufzeichnen der Bilder angeschlossen ist. Für den Videorecorder werden handelsübliche VHS-Videokassetten verwendet. Das Video wird nicht komprimiert. Bei Aufzeichnungen mit normaler Bildrate bietet ein Band höchstens 8 Stunden Aufzeichnungsdauer. In größeren Systemen kann ein Quad oder ein Multiplexer zwischen Kamera und Videorecorder installiert werden. Dank des Quad/Multiplexers können mehrere Kameras an denselben Videorecorder angeschlossen werden, was jedoch zu Lasten der Bildrate geht. Zur Anzeige des Videos dient ein analoger Monitor.

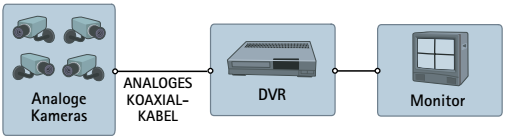


2.2. Analoge CCTV-Systeme mit DVR

Analoge CCTV-Systeme mit DVR (digitalem Videorecorder) sind Analogsysteme mit digitaler Aufzeichnung. Bei einem digitalen Videorecorder wird das Videoband durch Festplatten ersetzt. Das Video muss hierbei digitalisiert und komprimiert werden, damit so viele Bilder wie möglich gespeichert werden können. Bei den früheren DVRs war der Festplattenspeicher und damit auch die Aufzeichnungsdauer begrenzt, oder es musste eine geringe Bildrate in Kauf genommen werden. Dank der Entwicklung neuer Festplatten ist der Festplattenspeicher kein wesentliches Problem mehr. Die meisten DVRs verfügen über mehrere Video-Eingänge, meistens 4, 9 oder 16, bieten also auch die Funktionalität von Quadgeräten und Multiplexern.

Das DVR-System bietet zusätzlich folgende Vorteile:

- Kein Bandwechsel erforderlich
- Durchgängige Bildqualität

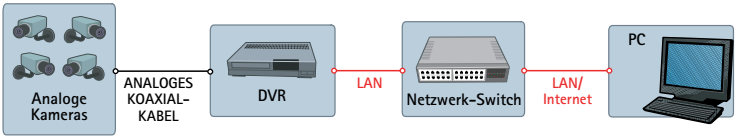


2.3. Analoge CCTV-Systeme mit Netzwerk-DVR

Analoge CCTV-Systeme mit Netzwerk-DVR sind teildigitale Systeme, die über einen digitalen Netzwerk-Videorecorder mit Ethernet-Schnittstelle am Netzwerk angeschlossen sind. Da das Video im DVR digitalisiert und komprimiert wird, kann es über ein Computernetzwerk an einen entfernten PC übertragen werden. Einige Systeme können sowohl Live-Video als auch Aufzeichnungen überwachen; andere Systeme eignen sich nur für Aufzeichnungen. Zudem benötigen einige Systeme einen speziellen Windows-Client zur Überwachung des Videos, während andere mit einem Standard-Browser auskommen; letztere bieten bei der Fernüberwachung mehr Flexibilität.

Das Netzwerk-DVR-System bietet zusätzlich folgende Vorteile:

- Entfernte Video-Überwachung per PC
- Fernbedienung des Systems

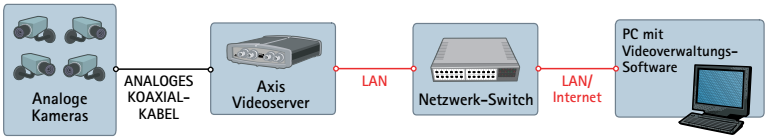


2.4. Netzwerk-Videosysteme mit Videoservern

Netzwerk-Videosysteme mit Videoservern bestehen aus einem Videoserver, einem Netzwerk-Switch und einem PC mit Video-Verwaltungssoftware. Die Analogkamera wird an den Videoserver angeschlossen, der das Video digitalisiert und komprimiert. Der Videoserver selbst ist mit einem Netzwerk verbunden und überträgt das Video über einen Netzwerk-Switch an einen PC, der die Videodaten auf Festplatten aufzeichnet. Hier handelt es sich um ein echtes Netzwerk-Videosystem.

Netzwerk-Videosysteme mit Videoservern bieten zusätzlich folgende Vorteile:

- Verwendung von Standard-Netzwerk- und -Server-Hardware zur Aufzeichnung und Verwaltung von Video
- System kann in Schritten von je einer Kamera skaliert werden
- Entfernte Aufzeichnung ist möglich
- Zukunftssicherheit, da sich das System durch weitere Netzwerk-Kameras leicht erweitern lässt



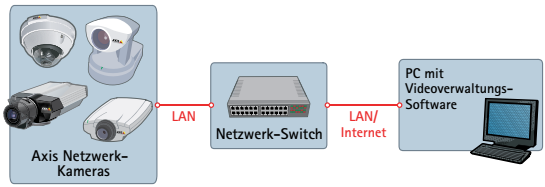
Dieses Diagramm zeigt ein echtes Netzwerk-Videosystem, bei dem Videoinformationen fortlaufend über ein IP-Netzwerk übertragen werden. Ein Videoserver dient als Brücke zwischen dem analogen Sicherheitssystem und der digitalen, IP-basierten Videolösung.

2.5. Netzwerk-Videosysteme mit Netzwerk-Kameras

Netzwerk-Kameras sind eine Kombination aus einer Kamera und einem Computer, der das Video digitalisiert und komprimiert, und verfügen über eine Netzwerk-Schnittstelle. Das Video wird via Netzwerk-Switches in einem IP-basierten Netzwerk übertragen und von einem Standard-PC mit Video-Verwaltungssoftware aufgezeichnet. Hier handelt es sich um ein echtes Netzwerk-Videosystem, das vollständig digital und ohne analoge Komponenten arbeitet.

Netzwerk-Videosysteme mit Netzwerk-Kameras bieten zusätzlich folgende Vorteile:

- Hochauflösende Kameras (Megapixel)
- Durchgängige Bildqualität
- Power over Ethernet und drahtlose Übertragung
- PTZ, Audio, digitale Ein- und Ausgänge über IP zusammen mit Video
- Uneingeschränkte Flexibilität und Skalierbarkeit



Dieses Diagramm zeigt ein echtes Netzwerk-Videosystem mit Netzwerk-Kameras, bei dem Videoinformationen fortlaufend über ein IP-Netzwerk übertragen werden. Das System schöpft alle Vorteile der Digitaltechnik aus und bietet von der Kamera bis zum Viewer an jedem Standort eine gleichbleibend hohe Bildqualität.

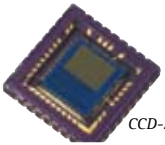
Bildgenerierung

Die Bausteine für die Bildqualität bei Netzwerk-Video

Die Bildqualität ist natürlich eines der wichtigsten, wenn nicht überhaupt DAS wichtigste Merkmal der Kamera. Das gilt ganz besonders für die Sicherheits- und Fernüberwachung, wenn es um Eigentum oder gar Menschenleben geht. Doch wie kann eine hohe Bildqualität erzeugt werden? Diese Frage wird beim Festlegen der technischen Daten für ein neues System häufig gestellt, wenn es um die Beschaffung und Installation neuer Netzwerk-Kameras geht. Anders als herkömmliche Analogkameras, bieten Netzwerk-Kameras nicht nur die Möglichkeit zur Erfassung und Darstellung von Bildern sondern auch deren Verwaltung und digitalen Komprimierung für die Übertragung im Netzwerk. Die Bildqualität kann stark variieren und hängt von mehreren Faktoren wie der Wahl von Optik und Bildsensor ab, aber auch von der Qualität der Algorithmen im Verarbeitungschip.

In diesem Kapitel werden einige Schlüsselbereiche beleuchtet, die bei der Auswahl der Netzwerk-Kameras für die jeweilige Überwachungsanwendung zu beachten sind.

3.1. CCD- und CMOS-Sensoren



CCD-Sensor

CMOS-Sensor

Der Bildsensor der Kamera dient zur Umwandlung von Licht in elektrische Impulse. Bei der Konstruktion einer Kamera stehen zwei Technologien für den Bildsensor der Kamera zur Verfügung:

- CCD (Charged Coupled Device)
- CMOS (Complementary Metal Oxide Semiconductor)

CCD-Sensoren werden mit einem Verfahren gefertigt, das speziell für die Kamera-Herstellung entwickelt wurde, während CMOS-Sensoren auf einer Standard-Technologie basieren, die sehr häufig für Speicherchips eingesetzt wird, zum Beispiel in PCs.

CCD-Technologie
CCD-Sensoren werden seit über zwanzig Jahren in Kameras eingebaut und bieten gegenüber CMOS-Sensoren zahlreiche qualitative Vorteile, nicht zuletzt auch eine höhere Lichtempfindlichkeit. Durch die höhere Lichtempfindlichkeit steigt die Bildqualität bei schlechten Lichtbedingungen. CCD-Sensoren sind jedoch kostspieliger, da sie nicht nach einem standardisierten Verfahren gefertigt werden und der Einbau in eine Kamera komplex ist. Außerdem kann es bei sehr hellen Objekten in einer Bildszene (zum Beispiel bei einer Lampe oder direkter Sonneneinstrahlung) zu einem "Auslaufen" mit vertikalen Streifen über und unter dem Objekt kommen, das als Nachzieheffekt bezeichnet wird.

CMOS-Technologie
Die neuesten Entwicklungen bei CMOS-Sensoren haben den Unterschied zu CCD-Sensoren zwar verringert; sie eignen sich jedoch nach wie vor nicht für Kameras, bei denen es auf erstklassige Bildqualität ankommt. CMOS-Sensoren machen Kameras preisgünstiger, da sie die gesamte Kameralogik bereits enthalten. Außerdem ermöglichen Sie kleinere Baugrößen. Es sind auch große Sensoren erhältlich, die für verschiedene Netzwerk-Kameras Megapixel-Auflösungen bieten. Ein Nachteil bei CMOS-Sensoren ist derzeit noch die vergleichsweise geringe Lichtempfindlichkeit. In normal hellen Umgebungen ist dies kein Problem, doch bei schlechten Lichtbedingungen wird der Unterschied deutlich. Es entstehen sehr dunkle oder verrauschte Bilder.

3.2. Progressive Abtastung oder Halbbild-Video?

Heute stehen zwei verschiedene Technologien zur Wiedergabe von Video zur Verfügung: das Zeilensprungverfahren (Halbbild) und die progressive Abtastung. Die gewählte Technik hängt von Anwendung und Zweck des Videosystems ab, insbesondere davon, ob das System bewegte Objekte erfassen muss und wieweit im bewegten Bild Details erkennbar sein sollen.

3.2.1. Zeilensprungverfahren (Halbbild)

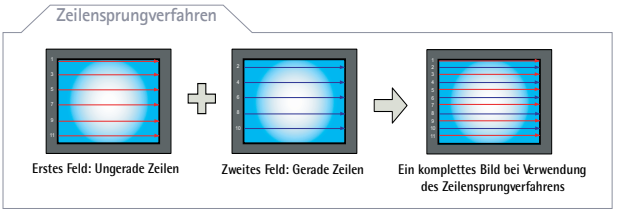
Das Zeilensprungverfahren wurde ursprünglich für Fernseh-Bildröhren entwickelt. Das Bild setzt sich bei einem Standard-Fernsehgerät aus 576 sichtbaren Zeilen zusammen. Gerade und ungerade Zeilen werden abwechselnd mit 30 fps aktualisiert. Durch die kleine Verzögerung zwischen geraden und ungeraden Bildzeilen entsteht zuweilen ein Zackenmuster, da die Hälfte der Zeilen sich mit dem bewegten Bild verändert, während die andere Hälfte noch auf die Aktualisierung wartet.

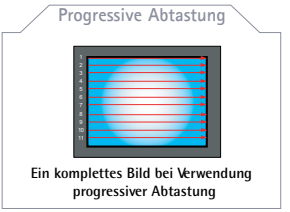
Die Auswirkungen des Zeilensprungverfahrens können durch einen Progressivfilter teilweise kompensiert werden. Er rechnet Halbbilder zu Vollbildern um. Da weniger Zackenmuster gebildet werden, verbessert sich die Bildqualität. Dieses Verfahren wird auch als Zeilendopplung bezeichnet. Bestimmte Netzwerk-Videoprodukte wie Axis Videoserver verfügen über einen Progressivfilter, der die Bildqualität bei höchster Auflösung (4CIF) verbessert. Die Bewegungsunschärfe, die durch das analoge Videosignal der Analogkamera entsteht, wird dadurch eliminiert.

Das Zeilensprungverfahren hat bei Kameras, TV und VHS-Video lange Jahre gut funktioniert und ist für bestimmte Anwendungen noch heute gut geeignet. Mit dem Aufkommen der LCD-Technologie, von TFT-Monitoren, DVDs und Digitalkameras wurde jedoch eine alternative Darstellungstechnik entwickelt, die als progressive Abtastung bezeichnet wird.

3.2.2. Progressive Abtastung

Bei der progressiven Abtastung wird im Gegensatz zum Zeilensprungverfahren das ganze Bild 16-mal pro Sekunde Zeile für Zeile erfasst. Die erfassten Bilder werden also nicht mehr in zwei Halbbilder geteilt. Computermonitore benötigen zur Darstellung von Bildern keine Halbbilder. Sie setzen Zeile für Zeile in der gewöhnlichen Reihenfolge um, d.h. 1, 2, 3, 4, 5, 6, 7 usw. Auf diese Weise wird das Bildflimmern vermieden. Bei Überwachungsanwendungen kann die Detailtreue bei einem bewegten Bild entscheidend sein, zum Beispiel, wenn jemand schnell die Flucht ergreift. Allerdings wird ein hochwertiger Monitor benötigt, um dieses Abtastverfahren optimal zu nutzen.



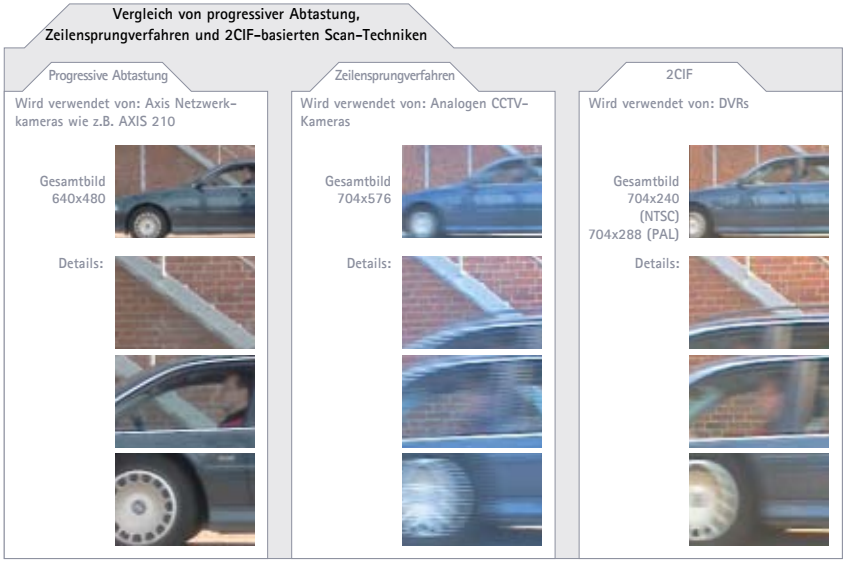


3.2.3. Beispiel: Erfassen bewegter Objekte

Wenn eine Kamera ein bewegtes Objekt erfasst, hängt die Bildschärfe im Einzelbild von der eingesetzten Technologie ab. Vergleichen Sie diese JPEG-Bilder, die von drei verschiedenen Kameras mit progressiver Abtastung, 4CIF-Halbbild und 2CIF-Halbbild aufgenommen wurden.

Beachten Sie dabei:

- *Alle Bildsysteme erzeugen ein klares Bild des Hintergrunds*
- *Stufige Kanten bei Bewegung mit Zeilensprungverfahren*
- *Verwischte Bewegung durch mangelnde Auflösung im 2CIF-Beispiel*
- *Nur bei progressiver Abtastung kann der Fahrer identifiziert werden*



Hinweis: Bei diesen Beispielen waren alle Kameras mit demselben Objektiv ausgestattet. Das Auto war 20 km/h schnell.

3.3. Komprimierung

Viele Komprimierungsstandards zur Auswahl
Die Bild- und Videokomprimierung kann mit oder ohne Qualitätseinbußen erfolgen. Bei der verlustfreien Komprimierung wird jedes Pixel unverändert beibehalten, so dass das Bild bei der Dekomprimierung originalgetreu wiederhergestellt wird. Allerdings ist das Komprimierungsverhältnis dabei sehr klein; die Datenreduzierung ist beschränkt. Ein bekannter verlustfreier Komprimierungsstandard ist das GIF-Format. Da das Komprimierungsverhältnis klein ist, sind solche Formate für Netzwerk-Videolösungen kaum geeignet, bei denen große Bildmengen gespeichert und übertragen werden müssen. Daher wurden mehrere verlustreiche Komprimierungsverfahren und -standards entwickelt. Die grundlegende Idee besteht in der Reduzierung von Elementen, die für das menschliche Auge unsichtbar sind. Dadurch lässt sich das Komprimierungsverhältnis erheblich erhöhen.

Bei der Komprimierung gibt es zudem zwei verschiedene Ansätze: die Komprimierung von Einzelbildern und die Video-Komprimierung.

3.3.1. Komprimierungsstandards für Einzelbilder

Alle Komprimierungsstandards für Einzelbilder konzentrieren sich auf nur ein Bild zur gleichen Zeit. Der bekannteste und meistgenutzte Standard ist JPEG.

JPEG
JPEG wurde zunächst Mitte der 80-er Jahre von der *Joint Photographic Experts Group* standardisiert. JPEG-Bilder können in einem Standard-Browser dekomprimiert und angezeigt werden. Die JPEG-Komprimierung kann auf mehreren Stufen erfolgen, die vom Benutzer ausgewählt werden und bestimmen, wie stark ein Bild komprimiert wird. Die gewählte Komprimierungsstufe wirkt sich direkt auf die gewünschte Bildqualität aus. Neben der Komprimierungsstufe hängt die Höhe des Komprimierungsverhältnisses auch vom Bild selbst ab. Zum Beispiel kann aus einer weißen Wand eine relativ kleine Bilddatei (mit entsprechend hohem Komprimierungsverhältnis) erzeugt werden, während dieselbe Komprimierungsstufe bei einem komplexen, gemusterten Motiv eine größere Datei (geringeres Komprimierungsverhältnis) erzeugt.

Die beiden nachstehenden Bilder zeigen den Zusammenhang von Komprimierungsverhältnis und Bildqualität für dasselbe Motiv bei zwei verschiedenen Komprimierungsstufen.

Komprimierungsgrad "niedrig"
Komprimierungsverhältnis 1:16
6% der ursprünglichen Dateigröße
Keine sichtbare Verschlechterung der Bildqualität

Komprimierungsgrad "hoch"
Komprimierungsverhältnis 1:96
1% der ursprünglichen Dateigröße
Deutliche Verschlechterung der Bildqualität

JPEG2000

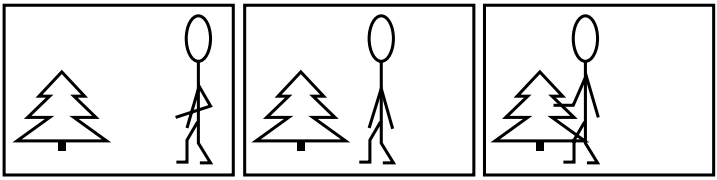
Ein weiterer Komprimierungsstandard für Einzelbilder ist JPEG2000. Auch dieser Standard wurde von der *Joint Photographic Experts Group* entwickelt. Er wurde vor Allem für medizinische Anwendungen und die Einzelbild-Fotografie entwickelt. Bei einem niedrigen Komprimierungsverhältnis führt er zu ähnlichen Ergebnissen wie JPEG; bei relativ hoher Komprimierung schneidet er etwas besser ab. JPEG2000 wird bisher jedoch nur von wenigen Browsern, Viewern und Bildverarbeitungsprogrammen unterstützt.

3.3.2. Video-Komprimierungsstandards

Video als Sequenz von JPEG-Bildern: Motion JPEG (M-JPEG)

Motion JPEG ist der gängigste Standard für Netzwerk-Videosysteme. Netzwerk-Kameras erfassen, wie digitale Einzelbildkameras, einzelne Bilder und komprimieren sie in das JPEG-Format. Die Netzwerk-Kamera kann zum Beispiel 30 solcher Einzelbilder (30 fps = 30 Bilder pro Sekunde) erfassen und komprimieren und sie später wieder als fortlaufenden Bildfluss über ein Netzwerk an ein Anzeigegerät weiterleiten. Bei einer Bildrate von mindestens 16 fps empfindet der Betrachter die Bildfolge als vollständig bewegte Bilder. Diese Methode wird als Motion JPEG oder M-JPEG bezeichnet.
Da jedes Einzelbild ein vollständiges JPEG-komprimiertes Bild ist, ist die Qualität bei allen Bildern gleich und wird von der Komprimierungsstufe bestimmt, die für die Netzwerk-Kamera oder den Videoserver gewählt wurde.

Beispiel für eine Sequenz aus drei vollständigen JPEG-Bildern



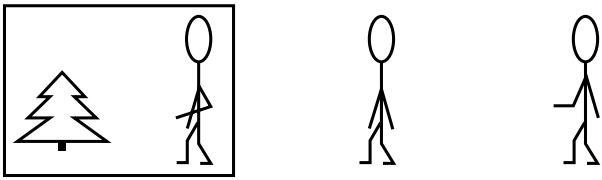
H.263

Das Komprimierungsverfahren H.263 zielt auf eine Video-Übertragung mit fester Bitrate. Ihr Nachteil besteht in einer geminderten Bildqualität bei bewegten Objekten. H.263 wurde ursprünglich für Videokonferenzen und nicht für Überwachungsaufgaben entwickelt, bei denen die Detailtreue wichtiger als die Bitrate ist.

MPEG

Eines der bekanntesten Audio- und Videostromverfahren ist MPEG (Ende der 80-er Jahre von der *Motion Picture Experts Group* entwickelt). Dieser Abschnitt konzentriert sich auf den Teil der MPEG Videostandards, der sich direkt auf Video bezieht.

Das Grundprinzip von MPEG besteht in dem Vergleich von zwei komprimierten Bildern, die über das Netzwerk übertragen werden. Das erste komprimierte Bild wird als Bezugsgröße genutzt. Nur die Bestandteile der folgenden Bilder, die sich von diesem Bezugsbild unterscheiden, werden gesendet. Das Netzwerk-Anzeigegerät rekonstruiert dann alle Bilder aus dem Bezugsbild und den Differenzdaten. Obwohl die Videokomprimierung mit MPEG komplexer ist, führt sie zu einem niedrigeren Datenaufkommen im Netzwerk als unter Motion JPEG. Dies ist auf der folgenden Seite zu erkennen, wo nur die Daten für die Differenz zwischen dem zweiten und dem dritten Bild übertragen werden.



Natürlich ist MPEG noch weitaus komplexer als oben beschrieben; oft werden zusätzlich Techniken oder Tools für Parameter wie die Antizipierung von Bewegungen in einer Szene und die Identifizierung von Objekten genutzt. Es gibt eine Reihe verschiedener MPEG-Standards:

- **MPEG-1** wurde 1993 zum Speichern von digitalem Video auf CDs veröffentlicht. Daher sind die meisten MPEG-1-Encoder auf eine Ziel-Bitrate von ca. 1,5 Mbit/s bei CIF-Auflösung ausgelegt. Bei MPEG-1 liegt der Schwerpunkt darauf, die Bit-Rate auf Kosten einer schwankenden Bildqualität relativ konstant zu halten. Die Bildqualität ist meist mit VHS-Video zu vergleichen. Die Bildrate ist bei MPEG-1 auf 25 (PAL)/30 (NTSC) fps festgelegt.

- **MPEG-2** wurde 1994 als Standard bestätigt und ist für hochwertiges digitales Video (DVD), hochauflösendes Fernsehen (HDTV), interaktive Speichermedien (ISM), DBV (digitales Rundsendeverfahren) und Kabelfernsehen (CATV) gedacht. Das MPEG-2-Projekt zielte darauf ab, die MPEG-1-Komprimierung auf größere Bilder und eine höhere Bildqualität auszudehnen und dafür eine niedrigere Komprimierungsrate und eine höhere Bitrate in Kauf zu nehmen. Ebenso wie bei MPEG-1 ist die Bildrate fest auf 25 (PAL) bzw. 30 (NTSC) fps eingestellt.

- **MPEG-4** wurde als Weiterentwicklung von MPEG-2 umfassend neu strukturiert. MPEG-4 umfasst zahlreiche neue Tools zum Senken der Bitrate, mit denen eine bestimmte Bildqualität für eine bestimmte Anwendung oder Bildszene erzielt werden kann. Außerdem ist die Bildrate nicht mehr starr auf 25 bzw. 30 fps festgelegt. Allerdings sind die meisten Tools zum Senken der Bitrate bisher für Echtzeit-Anwendungen irrelevant. Einige Tools erfordern so viel Rechenleistung, dass sie die Gesamtzeit zum Kodieren und Dekodieren (also die Wartezeit) stark erhöhen. Daher sind sie nur für Anwendungen wie die Kodierung von Studiofilmen oder animierten Filmen interessant. Tatsächlich standen die meisten Tools, die unter MPEG-4 für Echtzeit-Anwendungen geeignet sind, bereits unter MPEG-1 und MPEG-2 zur Verfügung.

Der Grundgedanke besteht darin, dass man sich für einen Video-Komprimierungsstandard entscheiden sollte, der weit verbreitet ist und eine hohe Bildqualität gewährleistet, wie M-JPEG oder MPEG-4.

MPEG-4 (Teil 10)
Die beiden Gruppen hinter H.263 und MPEG-4 haben sich vor kurzem zu einem Team zusammengeschlossen, das den Video-Komprimierungsstandard der nächsten Generation gemeinsam entwickeln will: AVC (für „Advanced Video Coding“), auch als H.264 oder MPEG-4 Teil 10 bezeichnet. Mit dem neuen Standard soll eine besonders hohe Datenkomprimierung erreicht werden. Dadurch ließe sich eine hohe Videoqualität bei Bitraten erzielen, die deutlich unter den Anforderungen der bisherigen Standards angesiedelt wären, jedoch ohne die Komplexität der Algorithmen wesentlich zu erhöhen, so dass die Umsetzung des Standards praktisch und finanziell bewältigt werden kann.

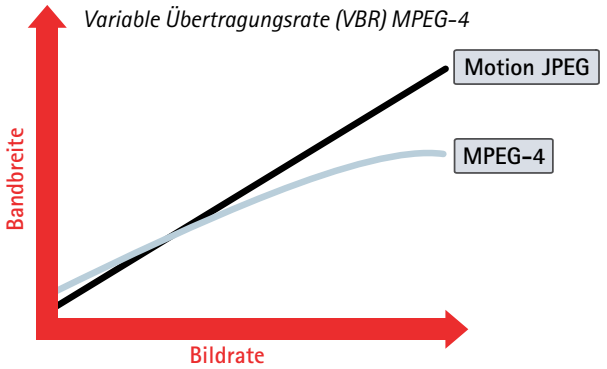
Vor- und Nachteile von Motion JPEG, MPEG-2 und MPEG-4
Aufgrund seiner Einfachheit ist der weit verbreitete Standard Motion JPEG, der in vielen Systemen Einsatz findet, oft eine gute Wahl. Zwischen der Bilderfassung in einer Kamera, der Kodierung, der

Übertragung im Netzwerk, Dekodierung und schließlich Anzeige an einem Anzeigegerät, liegen jeweils nur kurze Verzögerungen. Anders ausgedrückt, verursacht Motion JPEG wegen seiner einfachen Struktur wenig Wartezeit (Bildkomprimierung und vollständige Einzelbilder) und eignet sich daher bestens zur Bildverarbeitung, zum Beispiel zur Bewegungsmeldung oder Objektverfolgung. Jede gängige Bildauflösung, von der Handy-Anzeige (QVGA) bis zur vollen Videogröße (4CIF) und darüber (Megapixel) steht unter Motion JPEG zur Verfügung.

Das System gewährleistet Bildqualität unabhängig davon, wie komplex Bewegungen oder Bilder sind und bietet zugleich die Flexibilität, den richtigen Kompromiss zwischen einer hohen Bildqualität bei niedriger Komprimierung und niedriger Bildqualität bei hoher Komprimierung zu finden, so dass auch kleinere Bildgrößen und damit eine geringere Bildrate und Bandbreitenauslastung möglich sind. Die Bildrate kann problemlos angepasst werden, um die Bandbreiten-Nutzung einzuschränken, ohne die Bildqualität einzuschränken.

Allerdings entstehen unter Motion JPEG relativ umfangreiche Bilddatenvolumen, die im Netzwerk übertragen werden. In dieser Hinsicht bietet MPEG den Vorteil, dass ein geringeres Datenvolumen pro Zeiteinheit (Bitrate) als bei Motion JPEG über das Netzwerk übertragen werden muss, soweit keine niedrige Bildrate gewählt wird (siehe unten). Wenn im Netzwerk nur eine begrenzte Bandbreite verfügbar ist oder Video mit einer hohen Bildrate aufgezeichnet werden muss, aber nur wenig Speicher zur Verfügung steht, ist oft MPEG empfehlenswert. Der MPEG-Standard bietet eine relativ hohe Bildqualität bei niedriger Bitrate (Bandbreitennutzung). Allerdings wird die niedrigere Bandbreite mit einer komplexeren Kodierung/Dekodierung erkauft, die ihrerseits die Wartezeit im Vergleich mit Motion JPEG verlängern kann. Zu beachten ist auch, dass sowohl für MPEG-2 als auch für MPEG-4 Lizenzgebühren entrichtet werden müssen.

Das Diagramm unten zeigt die unterschiedliche Bandbreiten-Nutzung zwischen Motion JPEG und MPEG-4 bei einer gegebenen Bildszene mit Bewegungsablauf. Bei niedrigeren Bildraten kann die Komprimierung mit MPEG-4 weniger Ähnlichkeiten zwischen benachbarten Bildern nutzen; aufgrund des hohen Verwaltungsaufwands, den das MPEG-4 Streaming-Format erfordert, entspricht die genutzte Bandbreite in etwa Motion JPEG. Bei höheren Bildraten erfordert MPEG-4 wesentlich weniger Bandbreite als Motion JPEG.



Unterstützung von MPEG-4 durch Axis

Die meisten Axis Netzwerk-Videoprodukte verfügen über eine Echtzeit-Videokodierung, die gleichzeitig MPEG-4- und Motion JPEG-Datenströme erzeugen kann. Dadurch kann der Benutzer die bestmögliche Bildqualität für die Aufzeichnung wählen und zugleich den Bandbreitenbedarf für die Live-Übertragung gering halten.

Die Umsetzung von MPEG-4 durch Axis entspricht dem Industriestandard ISO/IEC 14496-2 (auch als MPEG-4 Visual oder MPEG-4 Teil 2 bezeichnet). Netzwerk-Videoprodukte von Axis unterstützen das Advanced Simple Profile (ASP) bis Stufe 5 und den möglichen Einsatz von Simple Profile (SP). Dank der vielfältigen Einstellungsmöglichkeiten können Bandbreite und Qualität der Datenströme optimal ausbalanciert werden. Die Axis Media Control (AMC) mit integriertem MPEG-4-Decoder macht das Anzeigen von Datenströmen und die Integration in Anwendungen zu einem Kinderspiel.

Außerdem lässt die Multicast-Unterstützung von Axis eine unbegrenzte Anzahl von Betrachtern zu, ohne die Leistung des Netzwerksystems herabzusetzen. *Weitere Informationen zum Multicasting finden Sie in Kapitel 5.4.4 auf Seite 45.*

Gibt es einen Komprimierungsstandard, der immer passt?

Zu dieser Frage und bei der Konzeption einer Netzwerk-Video-Anwendung müssen die folgenden Themen erörtert werden:

- Welche Bildrate wird benötigt?
- Wird immer dieselbe Bildrate benötigt?
- Wird eine fortlaufende Aufzeichnung/Überwachung benötigt oder nur im Fall von Bewegungen bzw. Ereignissen?
- Wie lange soll das Video gespeichert werden?
- Welche Auflösung wird benötigt?
- Welche Bildqualität wird benötigt?
- Welche Wartezeit (Gesamtzeit für das Kodieren und Dekodieren) ist akzeptabel?
- Wie stabil und sicher muss das System sein?
- Welche Bandbreite bietet das Netzwerk?
- Wie hoch ist das Budget für das System?

Ausführliche Informationen zu digitalen Video-Komprimierungsverfahren finden Sie im Axis White Paper unter www.axis.com/corporate/corp/tech_papers.htm

3.4. Bildauflösung

Die Auflösung folgt in der analogen und der digitalen Welt den selben Prinzipien. Dennoch gibt es einige Unterschiede bei der Definition. Analoge Videobilder setzen sich aus Bildzeilen (genauer: TV-Bildzeilen) zusammen, da diese Technologie aus der Fernsehtechnik entwickelt wurde. Bei digitalen Systemen besteht das Bild aus einzelnen Bildpunkten, den sogenannten Pixeln.

3.4.1. Bildauflösung unter NTSC und PAL

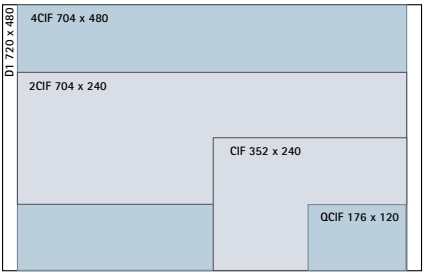
In Nordamerika und Japan ist die Fernsehnorm NTSC der vorherrschende analoge Videostandard, während in Europa das PAL-System (Phase Alternation by Line) üblich ist. Beide Normen entstammen der Fernsehtechnik. NTSC bietet eine Bildauflösung mit 480 Bildzeilen und eine Wiederholungsrate von 60 Halbbildern pro Sekunde (oder 30 Vollbildern/Sekunde = 30 fps). PAL bietet eine Auflösung von 576 Bildzeilen bei 50 Halbbildern pro Sekunde (oder 25 fps). Insgesamt wird bei beiden Normen dieselbe Datenmenge pro Sekunde übertragen.

Bei der Digitalisierung von analogem Video hängt die maximale Anzahl an erstellbaren Pixeln von der Anzahl der Fernsehzeilen ab, die zur Digitalisierung bereitstehen. Unter NTSC beträgt die maximale Größe des digitalen Bildes 720 x 480 Pixel. Unter PAL beträgt sie 720 x 576 Pixel (D1). Am häufigsten

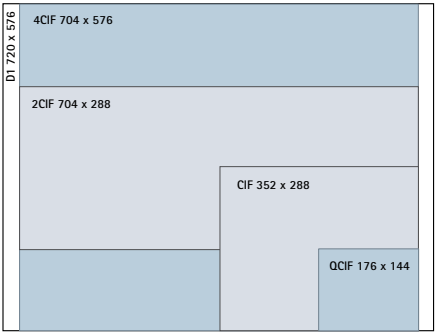
wird eine Auflösung von 4CIF genutzt, was unter PAL 704 x 576 und unter NTSC 704 x 480 Pixel entspricht. Die Auflösung 2CIF entspricht 704 x 240 (NTSC) bzw. 704 x 288 Pixel (PAL); die Anzahl der horizontalen Zeilen wird also halbiert. Normalerweise wird auf dem Monitor jede horizontale Zeile zweimal abgebildet (sog. „Zeilendopplung"), um ein korrektes Seitenverhältnis zu erzeugen. Mit dieser Methode kann einer Bewegungsunschärfe entgegen gewirkt werden.

Zuweilen wird ein Viertel des CIF-Bildes verwendet. Dieses Viertel wird kurz als QCIF (für „Quarter CIF") bezeichnet.

Unterschiedliche Auflösungen mit NTSC



Unterschiedliche Auflösungen mit PAL



3.4.2. VGA-Auflösung

Durch die Einführung der Netzwerk-Kameras können vollständig digitalisierte Systeme konzipiert werden. Dadurch werden die Einschränkungen von NTSC und PAL bedeutungslos. Mehrere neue Bildauflösungen, die aus dem Computersektor stammen, wurden eingeführt. Sie bieten mehr Flexibilität und sind nicht zuletzt weltweit anerkannte Standards.

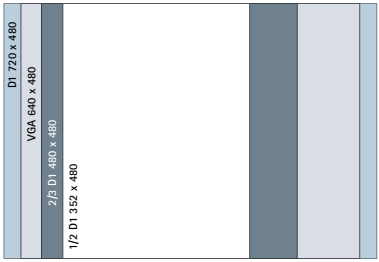
VGA ist eine Abkürzung für Video Graphics Array, einem grafischen Anzeigesystem für PCs, das ursprünglich von IBM entwickelt wurde. Es bietet eine Auflösung von 640 x 480 Pixeln und entspricht somit weitgehend den Formaten von NTSC und PAL. Die VGA-Auflösung eignet sich für Netzwerk-Kameras normalerweise besser, da das Video in der Regel auf einem Computerbildschirm wiedergegeben wird, der die VGA-Auflösung oder ein Vielfaches davon nutzt. QVGA (Quarter VGA) ist mit einer Auflösung von 320 x 240 Pixeln ebenfalls ein gebräuchliches Format und entspricht in etwa der Größe von CIF. QVGA wird auch als SIF (Standard Interchange Format, Standard-Austauschformat) bezeichnet, dies führt manchmal zu Verwechslungen mit CIF. Weitere VGA-basierte Bildauflösungen sind XVGA (1024 x 768 Pixel) und 1280 x 960 Pixel, (4-faches VGA mit Mexapixel-Auflösung). *Weitere Informationen finden Sie in Abschnitt 3.4.4. auf Seite 26.*

3.4.3. MPEG Auflösung

Als MPEG-Auflösung wird zumeist eine der folgenden Bildauflösungen bezeichnet:

- 704x576 pixels (PAL 4CIF)
- 704x480 pixels (NTSC 4CIF)
- 720x576 pixels (PAL oder D1)
- 720x480 pixels (NTSC oder D1)

Bild mit Auflösungen, die unter MPEG üblich sind:

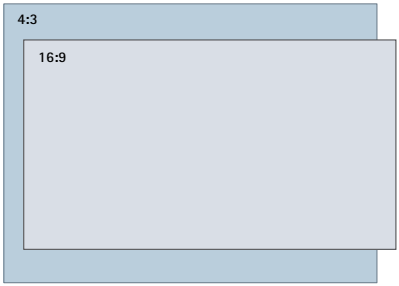


3.4.4. Auflösungen im Megapixel-Bereich

Je höher die Auflösung ist, desto mehr Details sind im Bild zu erkennen. Diese Überlegung ist bei Video-Überwachungsanwendungen wichtig, wenn es darum geht, dass ein Straftäter auf einem hochauflösenden Bild identifiziert werden kann. Die maximale Bildauflösung von Analogkameras unter NTSC und PAL nach der Digitalisierung des Videosignals in einem DVR oder einem Videoserver beträgt 400.000 Pixel (704 x 576 = 405504). 400.000 entspricht 0,4 Megapixel.

Auch wenn die Überwachungsbranche gelernt hat, mit solchen Einschränkungen zu leben, macht die moderne Netzwerk-Kameratechnik jetzt höhere Auflösungen möglich. Ein gebräuchliches Megapixel-Format ist 1280 x 1024, was einer Auflösung von 1,3 Megapixel entspricht, der 3-fachen Auflösung von Analogkameras. Kameras mit 2 Megapixel und 3 Megapixel sind ebenfalls erhältlich, und für die Zukunft werden noch höhere Auflösungen erwartet.

Megapixel-Netzwerk-Kameras bieten zudem den Vorteil verschiedener Seitenverhältnisse. Standard-CCTVs weisen ein Seitenverhältnis von 4:3 auf, während bei Kinofilmen und Breitbildschirmen 16:9 üblich ist. Dieses Seitenverhältnis ist vorteilhaft, da bei den meisten Bildern der obere und untere Rand nicht von Interesse ist, aber wertvolle Pixel und damit Bandbreite und Speicherplatz beansprucht. Bei einer Netzwerk-Kamera kann das Seitenverhältnis beliebig bestimmt werden.

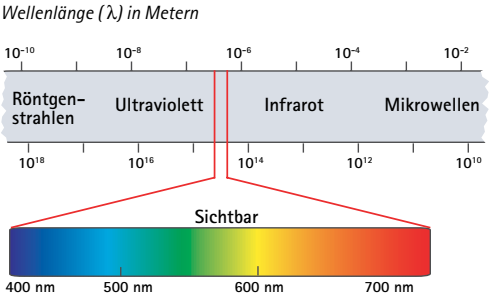


Zudem können PTZ-Funktionen (Schwenken, Neigen, Zoom) digital ohne Auflösungsverlust ausgeführt werden; der Bediener wählt den für die Anzeige gewünschten Ausschnitt der Megapixel-Bilder aus. Die Kamera muss hierzu nicht mechanisch bewegt werden. Dies erhöht die Zuverlässigkeit beträchtlich.

3.5. Einsatz bei Tag und Nacht

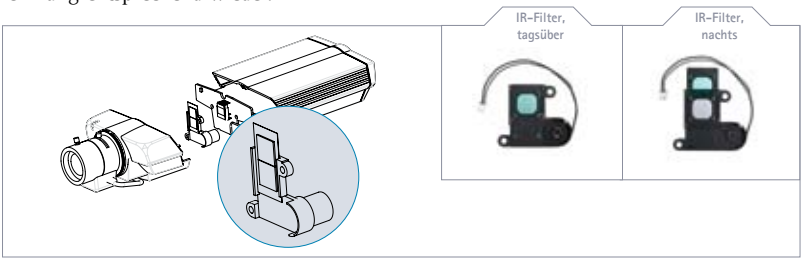
Bestimmte Umgebungen und Situationen eignen sich nur bedingt für den Einsatz von Kunstlicht. In diesen Fällen bieten sich oft Infrarot-Kameras an. Sie eignen sich für Video-Überwachungssituationen bei schlechten Lichtverhältnissen, aber auch für diskrete und verdeckte Anwendungen. Infrarot-Kameras nutzen das für das menschliche Auge unsichtbare Infrarotlicht und können zum Beispiel nach Einbruch der Dunkelheit in Wohngebieten eingesetzt werden, ohne Anwohner zu stören. Ebenso praktisch sind sie für Aufgaben, bei denen die Kameras möglichst nicht entdeckt werden sollen.

Lichtwahrnehmung
Licht ist Strahlung in Form von energetischen Wellen, das innerhalb eines bestimmten Spektrums liegt. Das menschliche Auge nimmt jedoch nur einen Teil des Lichts wahr (Wellenlängen zwischen ~400 und 700 Nanometer oder nm). Unterhalb des blauen Lichtbereichs, also knapp außerhalb des sichtbaren Spektrums, befindet sich das ultraviolette Licht; über dem roten Bereich das infrarote Licht.



Infrarotlicht (Wärmestrahlung) wird von allen Objekten abgestrahlt: z.B. von Menschen, Tieren und Pflanzen. Wärmere Objekte wie Menschen und Tiere setzen sich darin deutlich vom kühleren Hintergrund ab. Bei schlechten Lichtbedingungen, zum Beispiel nachts, kann das menschliche Auge keine Farben wahrnehmen und nur Schwarz, Weiß und Grautöne voneinander unterscheiden.

Wie funktionieren die Tag-/Nacht-Funktion oder der Infrarot-Sperrfilter?
Während das menschliche Auge nur Licht zwischen dem blauen und roten Bereich wahrnimmt, kann der Bildsensor einer Farbkamera ein größeres Spektrum erfassen. Der Bildsensor kann langwellige Infrarot-Wellen wahrnehmen. Trifft jedoch Infrarotlicht bei Tageslicht auf den Sensor, werden die Farben, die das menschliche Auge wahrnimmt, verzerrt. Daher sind alle Farbkameras mit einem Infrarot-Sperrfilter ausgestattet - ein optischer Glasfilter, der zwischen dem Objektiv und dem Bildsensor eingesetzt wird. Er entfernt das Infrarotlicht und gibt Farbbilder der menschlichen Wahrnehmung entsprechend wieder.



Wenn die Lichtstärke abnimmt und sich das Bild verdunkelt, kann der Infrarot-Sperrfilter automatisch* entfernt werden, so dass die Kamera das Infrarotlicht nutzen kann und Bilder auch in sehr dunklen Umgebungsbedingungen "wahrnimmt". Zur Vermeidung von Farbverzerrungen schaltet die Kamera oft in den Schwarzweiß-Modus und kann auf diese Weise hochwertige Schwarzweiß-Bilder erzeugen. Der Infrarot-Sperrfilter in den Axis Tages-/Nachtlichtkameras kann ebenfalls über die Kameraschnittstelle entfernt werden.

**Ob der Infrarot-Sperrfilter automatisch vor den Bildsensor geschoben bzw. entfernt werden kann, hängt vom Fabrikat der Kamera ab.*

Hinweise zum Einsatz von Kameras

Damit ein Netzwerk-Videosystem eine möglichst gute Leistung erzielt, müssen einige Grundregeln beachtet werden. In diesem Kapitel werden einige dieser Regeln erörtert, insbesondere die Wahl der Kamerakomponenten, die Positionierung und Installation der Kamera und die Faktoren, die berücksichtigt werden müssen, um in Innen- und Außenbereichen eine möglichst hohe Bildqualität und Dateilgenauigkeit sicherzustellen. Außerdem werden praktische Beispiele für die Installation gezeigt, bei denen analoge Video-Komponenten zusammen mit Netzwerk-Videosystemen eingesetzt werden.

4.1. Verwenden von Netzwerk-Kameras

4.1.1 Kameratypen

Wenn ein neues Videoüberwachungssystem installiert werden soll und keine Analogkameras vorhanden sind, empfehlen sich in der Regel Netzwerk-Kameras, die in vielen Ausführungen für unterschiedlichste Anforderungen erhältlich sind.

Aufgrund der großen Auswahl an modernen Netzwerk-Kameras können fast alle Anforderungen in allen vertikalen Märkten und Systemgrößen abgedeckt werden. Ebenso wie bei Analogkameras sind verschiedene Netzwerk-Kameramodelle erhältlich.

Unbewegliche Netzwerk-Kameras
Unbewegliche Kameras, bestehend aus Grundkamera und Objektiv, entsprechen dem traditionellen Kameratyp. Bei bestimmten Anwendungen ist es von Vorteil, wenn die Kamera auffällt. In diesen Fällen sind unbewegliche Kameras die beste Wahl, da sie ebenso gut zu erkennen sind wie die Richtung, in die sie zeigen. Zudem besitzen die meisten unbeweglichen Kameras Wechselobjektive des Typs C/CS. Zum Schutz der unbeweglichen Kameras ist eine Installation in Innenraum- oder Außengehäusen möglich.

Feste Netzwerk-Kuppel-Kameras
Feste Netzwerk-Kuppel-Kameras, auch als Mini-Domes bezeichnet, bestehen im Wesentlichen aus einer unbeweglichen Kamera, die fest in einem kleinen Kuppelgehäuse installiert ist. Die Aufnahmerichtung der Kamera ist frei wählbar. Ihr größter Vorteil liegt in ihrem unauffälligen, unaufdringlichen Design. Zudem ist die Aufnahmerichtung nur schwer zu erkennen. Allerdings sind feste Kuppel-Kameras meist nicht mit Wechselobjektiven ausgestattet, und selbst wenn mehrere Objektive zur Auswahl stehen, sind die Wechselmöglichkeiten durch den Platz im Kuppelgehäuse eingeschränkt.

PTZ-Netzwerk-Kameras
PTZ-Kameras verfügen über eine Schwenk-, Neige- und Zoomfunktion, die manuell oder automatisch bedient wird. Im manuellen Betrieb kann die PTZ-Kamera zum Beispiel einem Kunden in einem Einzelhandelsgeschäft folgen. PTZ-Kameras werden vorzugsweise in Innenräumen und in Bereichen eingesetzt, in denen die Aufnahmerichtung von außen erkennbar sein soll. Die meisten PTZ-Kameras lassen sich nicht um volle 360° schwenken und eignen sich nicht für den automatischen Dauerbetrieb ("Rundgangüberwachung"). Der optische Zoom liegt zwischen 18x und 26x.

Netzwerk-Kuppel-Kameras
Netzwerk-Kuppel-Kameras bieten dieselben Vorteile wie feste Kuppel-Kameras: Sie sind unauffällig, und ihre Aufnahmerichtung ist von außen nur schwer zu erkennen. Im Gegensatz zur PTZ-Kamera bietet die Netzwerk-Kuppel-Kamera einen Schwenkwinkel von 360°. Zudem zeichnet sie sich durch mechanische Robustheit aus und eignet sich für den Dauerbetrieb als Rundgangüberwachungssystem, das sich täglich zwischen etwa 10 voreingestellten Positionen bewegt. Bei der Rundgangüberwachung kann eine einzelne Kamera einen Bereich abdecken, für den sonst 10 unbewegliche Kameras erforderlich wären. Allerdings kann sie jeweils nur einen Zielbereich überwachen, so dass die anderen 9 Positionen im entsprechenden Zeitabschnitt unbeaufsichtigt bleiben. Der optische Zoom liegt zwischen 18x und 30x. Für die Außeninstallation sind Zoom-Faktoren über 20x aufgrund von windbedingten Erschütterungen und Positionsschwankungen eher ungeeignet.

Nichtmechanische PTZ-Netzwerk-Kameras
Mit der Einführung der Netzwerk-Kameras hat sich ein neuer PTZ-Kameratyp auf dem Markt durchgesetzt: die so genannte nichtmechanische PTZ-Kamera. Mittels eines Megapixel-Sensors kann die Kamera zwischen 140 und 360° abdecken. Der Bediener kann die Kamera ohne mechanischen Positionswechsel in jede Richtung schwenken, neigen oder zoomen. Dadurch entfällt der Verschleiß von beweglichen Teilen. Zudem kann der Positionswechsel sofort vollzogen werden, der bei herkömmlichen PTZ-Kameras bis zu einer Sekunde beanspruchen kann. Die besten nichtmechanischen PTZ-Kameras sind mit einem 3 Megapixel Sensor bestückt. Um eine gute Bildqualität zu gewährleisten, sollten Neige- und Schwenkwinkel auf 140° und der Zoomfaktor auf 3x beschränkt werden. Größere Überwachungswinkel oder Zoomfaktoren beeinträchtigen die Bildqualität.

Die beschriebenen Kameratypen sind in zahlreichen Konfigurationen erhältlich. Dazu gehören:

- Vandalismus-geschützte Modelle mit entsprechendem Schutzgehäuse
- Wetterfeste Modelle mit entsprechendem Schutzgehäuse
- Tag & Nacht-Modelle, die automatisch zwischen Tagaufnahmen mit Farbvideo und Nachtaufnahmen mit Schwarzweißbildern umschalten und schlechte Lichtbedingungen durch Infrarotbeleuchtung ausgleichen. *Siehe hierzu Abschnitt 3.5 auf Seite 27.*

Nach der Wahl des Kameratyps müssen die passenden Objektive, Gehäuse und andere wichtige Systemkomponenten ausgesucht werden. Bei der Installation müssen zugunsten einer möglichst hohen Überwachungsqualität verschiedene Kriterien bei der Wahl der Kameraposition berücksichtigt werden.

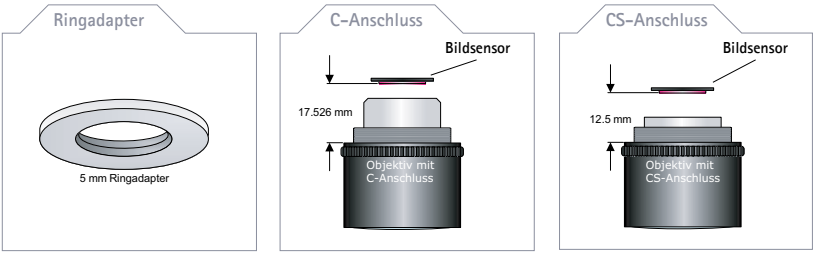
4.1.2. Auswahl der Objektive

Objektive mit C-Anschluss oder CS-Anschluss

Objektive sind mit zwei verschiedenen Fassungen erhältlich, dem C-Anschluss und dem CS-Anschluss. Beide haben einen Gewindedurchmesser von 1" (2,54 cm) und lassen sich auf den ersten Blick nicht unterscheiden. Sie unterscheiden sich im Abstand der Objektive zum Sensor:

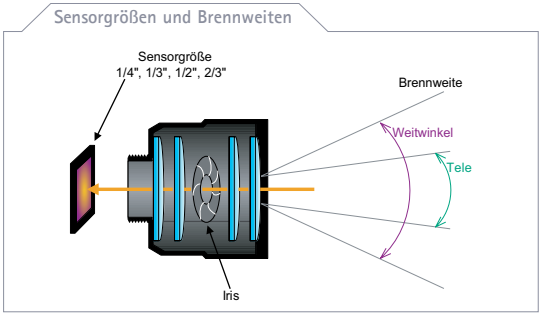
- CS-Anschluss: der Abstand zwischen Sensor und Objektiv muss 12,5 mm betragen.
- C-Anschluss: der Abstand zwischen Sensor und Objektiv muss 17,5 mm betragen. Mit einem 5 mm starken Abstandhalter (C/CS-Ringadapter) können C-Objektive zu Objektiven mit CS-Anschluss umgewandelt werden.

Der ältere Anschlusstyp ist der C-Anschluss. Der neuere CS-Anschluss ist eine Weiterentwicklung, die geringere Fertigungskosten und kleinere Sensoren ermöglicht. Fast alle heutigen Kameras und Objektive werden mit CS-Anschluss ausgeliefert. Man kann ein älteres C-Anschluss-Objektiv mit Hilfe eines C/CS-Ringadapters an eine Kamera mit CS-Anschluss anschließen. Wenn sich eine Kamera nicht scharf stellen lässt, besitzen Sie vermutlich den falschen Objektivtyp.



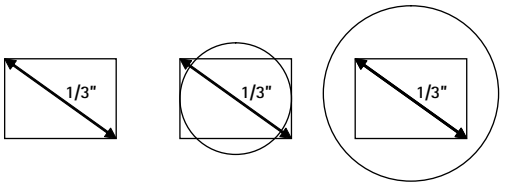
Sensorgröße

Bildsensoren sind in verschiedenen Größen wie 2/3", 1/2", 1/3" und 1/4" erhältlich; die Objektive werden passend zu diesen Größen gefertigt. Achten Sie bei der Wahl des Objektivs darauf, dass es zu Ihrer Kamera passt. Ein Objektiv für einen 1/2" Sensor eignet sich für Sensoren der Größen 1/2", 1/3" und 1/4", jedoch nicht für 2/3" Sensoren.



Wenn Sie ein Objektiv für einen kleineren Sensor einsetzen, erhält das Bild schwarze Ecken. Wenn Sie ein Objektiv für einen größeren Sensor als den der Kamera einsetzen, verringert sich das Sichtfeld im Vergleich zum Standardfeld des Objektivs. Ein Teil der Informationen geht außerhalb des Chips verloren.

Beispiele für unterschiedliche Objektive in Kombination mit einem 1/3" Sensor



Brennweite

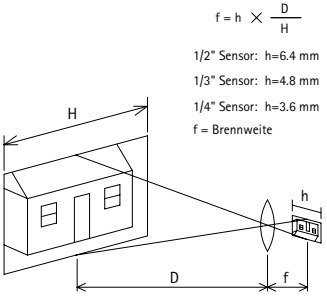
Die Brennweite bestimmt das horizontale Sichtfeld bei bestimmten Entfernungen: je größer die Brennweite, desto enger ist das Sichtfeld.

Objektiv- und Sensorgröße	1/2"	1/3"	1/4"
Brennweite	12 mm	8 mm	6 mm

Beispiele für erforderliche Brennweite zur Erzielung eines horizontalen Sichtfelds von ca. 30°

Die meisten Hersteller stellen einfache Schieberechner zum Berechnen der Brennweite des Objektivs aus der Szenengröße und der Brennweite zur Verfügung.

Um zu erkennen, dass sich eine Person auf einem Display befindet, muss sie normalerweise mindestens 10 % der Bildhöhe einnehmen. Wenn sie genau erkannt werden soll, muss sie mindestens 30 % des Bilds abdecken. Daher ist es wichtig, die Fähigkeiten der ausgewählten Kameras und die resultierende Anzeige genau zu prüfen, bevor Sie das System in Betrieb nehmen.



Berechnung in Metern
Wie breit kann ein Objekt sein, das aus einer Entfernung von 3 m vollständig dargestellt wird, wenn Sie über einen 1/4"-Sensor und ein 4 mm Objektiv verfügen?
H = D x h / f = 3 x 3,6 / 4 = 2,7 Meter

Berechnung in Fuß
Wie breit kann ein Objekt sein, das aus einer Entfernung von 10 Fuß vollständig dargestellt wird, wenn Sie über einen 1/4"-Sensor und ein 4 mm Objektiv verfügen?
H = D x h / f = 10 x 3,6 / 4 = 9 Fuß
H = D x h / f = 3 x 3.6 / 4 = 2.7 meters

Objektivtypen

- Fixfokus-Objektiv
  Die Brennweite ist unveränderlich (z. B. 4 mm).
- **Varifokus-Objektiv**
  Mit diesem Objektiv können Sie die Brennweite (das Sichtfeld) manuell einstellen. Beim Ändern der Brennweite muss die Schärfe neu eingestellt werden. Der gängigste Objektivtyp lässt Brennweiten zwischen 3,5 und 8 mm zu.
- **Zoom-Objektiv**
  Die Brennweite kann innerhalb eines bestimmten Bereichs eingestellt werden (z. B. 6 bis 48 mm). Die Schärfe bleibt beim Einstellen der Brennweite unverändert. Das Objektiv kann entweder manuell oder motorisch eingestellt werden, so dass auch eine Fernbedienung möglich ist.

Varifokus-Objektiv

Fixfokus-Objektiv

Irisblende

Netzwerk-Kameras kontrollieren die Lichtmenge, die auf die Bildverarbeitungseinheit trifft, normalerweise über die Irisblende oder durch das Einstellen der Belichtungszeit. Bei herkömmlichen Kameras ist die Belichtungszeit unveränderlich. Die Irisblende regelt die Lichtmenge, die durch das Objektiv gelangt. Es gibt verschiedene Arten von Irisblenden:

- Manuelle Blenden:
  Die Iris einer manuellen Blende wird normalerweise bei der Installation der Kamera an die vorherrschenden Lichtverhältnisse angepasst. Manuelle Blenden können nicht auf veränderte Lichtverhältnisse reagieren. Daher wird die Irisblende auf einen Durchschnittswert eingestellt, der sich für variable Bedingungen eignet.

- Automatische Irisblende
  In Außenbereichen und bei ständig wechselnden Lichtbedingungen ist ein Objektiv mit automatisch einstellbarer Iris empfehlenswert. Das Iris-System wird von der Kamera kontrolliert und stetig verändert, um eine optimale Lichtmenge für den Bildsensor zu erzielen.
  - DC-gesteuerte Irisblende: Die Irisblende wird an der Außenseite einer Kamera angebracht und wird vom Prozessor der Kamera gesteuert.
  - Video-gesteuerte Irisblende: Die Irisblende wird durch das Videosignal gesteuert.

Bei Kameras für den Außenbereich wird eine automatische Irisblende empfohlen. Die Irisblende optimiert die Lichtmenge, die die Kamera erreicht, automatisch und schützt den Bildsensor vor einer Überbelichtung. Kleine Blendendurchmesser reduzieren die Lichtmenge und verbessern dadurch die Tiefenschärfe (Schärfe bei größeren Entfernungen). Große Blenden dagegen ermöglichen eine höhere Bildqualität bei schlechten Lichtverhältnissen. Die Blende wird durch die Zahl F bestimmt.

F = Brennweite / Blende
Der Blendenwert F ist der Quotient zwischen Brennweite und effektivem Objektdurchmesser. Er wirkt sich auf die Lichtmenge aus, die auf den Sensor auftrifft und spielt für das entstehende Bild eine wichtige Rolle.

Je größer der Blendenwert F ist, desto weniger Licht wird zum Sensor durchgelassen. Je kleiner der Blendenwert ist, desto mehr Licht trifft auf den Sensor auf, so dass bei schlechten Lichtbedingungen eine bessere Bildqualität erzielt werden kann. Die nachstehende Tabelle zeigt die Lichtmenge, die bei verschiedenen Blendenwert-Beispielen den Sensor erreicht.

Blendenwert F	f1.0	f1.2	f1.4	f1.7	f2.8	f4.0	f5.6
% an durchgelassenem Licht	20%	14.14%	10%	7.07%	2.5%	1.25%	0.625%

Bei Szenen mit schwacher Beleuchtung wird empfohlen, vor der Linse einen Neutraldichtefilter anzubringen. Er reduziert die Lichtmenge, die durch das Objektiv einfällt, gleichmäßig über das gesamte sichtbare Spektrum und zwingt die Irisblende, sich zum Ausgleich vollständig zu öffnen. Viele Netzwerk-Kameras verfügen heute über eine automatische Irisblendensteuerung, um sicherzustellen, dass das Bild das ganze Jahr über und zu verschiedenen Tageszeichen klar bleibt, auch wenn sich die Lichtverhältnisse stetig ändern.

4.1.3. Montage im Innen- und Außenbereich

Kameragehäuse
Wenn eine Kamera im Außenbereich oder in relativ widrigen Umgebungen montiert wird, benötigen Sie ein wetterfestes bzw. Vandalismus-gesichertes Schutzgehäuse. Kameragehäuse sind in verschiedenen Größen, Qualitäten und Ausführungen erhältlich, zum Beispiel auch mit integrierten Lüftern zur Kühlung oder mit Heizgeräten.

Eine vollständige Liste der erhältlichen Gehäuse zur Montage von Axis Netzwerk-Kameras in aggressiven, feuchten oder staubigen Umgebungen finden Sie unter www.axis.com/products/cam_housing.

4.1.4. Praktische Empfehlungen

Damit Ihre Kamera hochwertige Bilder erzeugt, sollten Sie einige Grundregeln beherzigen. Sie gelten für Netzwerk-Kameras ebenso wie für jeden anderen Kameratyp. Die folgenden, einfachen Tipps sollen Ihnen dabei helfen, gute Aufnahmen zu machen.

- **Leuchten Sie den Aufnahmebereich gut aus**
  Die meisten schlechten Bilder leiden unter schwachem Umgebungslicht. Generell gilt: je mehr Licht, desto besser die Bilder. Bei einer schwachen Ausleuchtung werden die Bilder verrauscht und verlieren durch „dumpfe“ Farbtöne an Schärfe. Professionelle Fotografen arbeiten stets mit starken Lampen. Lux ist die Standard-Maßeinheit für die Lichtmenge. Für gute Bildaufnahmen sind mindestens 200 Lux erforderlich. Hochwertige Kameras können teilweise auch noch bei einer Lichtmenge von mindestens 1 Lux arbeiten. Bilder können also noch bei 1 Lux aufgenommen

werden, weisen dann aber keine hohe Qualität auf. Verschiedene Hersteller wenden zur Angabe der Lichtempfindlichkeit unterschiedliche Maßstäbe an. Dadurch lassen sich Kameras nur schwer vergleichen, ohne die aufgenommenen Bilder in Augenschein zu nehmen.

Umgebung	Lux
Starkes Sonnenlicht	100,000
Normales Tageslicht	10,000
Gängige Büro-Beleuchtung	500
Schwach beleuchteter Raum	100

- **Vermeiden Sie Gegenlicht**
  Versuchen Sie, extrem helle Bildbereiche zu vermeiden. Helle Bilder werden schnell überbelichtet (helles Weiß), so dass die Objekte zu dunkel erscheinen. Typischerweise tritt das Problem bei der Aufnahme von Objekten hinter einer Fensterscheibe auf.

- **Senken Sie den Kontrast**
  Die Kamera stellt die Belichtung so ein, dass die durchschnittliche Lichtmenge im Bild einem gewissen Wert entspricht. Wenn man versucht, einen Menschen vor einer weißen Wand aufzunehmen, erscheint er meistens zu dunkel. Das Problem lässt sich jedoch leicht lösen, indem die weiße Hintergrundfarbe durch einen Grauton ersetzt wird.

Montage von Kameras im Außenbereich

- **Objektive**
  Für den Außenbereich sollte stets ein Objektiv mit automatischer Blende verwendet werden. Automatische Irisblenden regeln die Lichtmenge, die den Bildsensor erreicht. Dadurch wird die Bildqualität optimiert und der Bildsensor vor Schäden durch starke Sonneneinstrahlung geschützt.

- **Direkte Sonneneinstrahlung**
  Wichtig! Direkte Sonneneinstrahlung sollte in einem Bild stets vermieden werden. Durch direkte Sonneneinstrahlung wird die Kamera im Laufe der Zeit „blind“, so dass die kleinen Farbfilter auf dem Sensorchip ausbleichen. Die Kamera sollte daher möglichst parallel zur Sonneneinstrahlung positioniert werden.

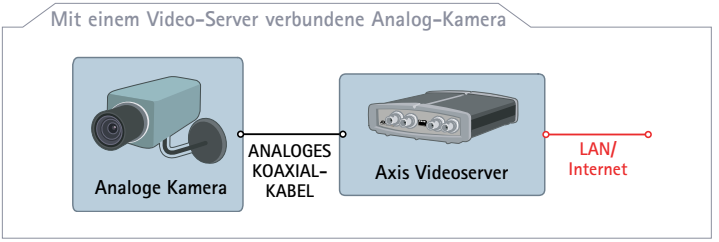
- **Kontrast**
  Achten Sie darauf, dass nicht zu viel Himmel auf dem Bild erscheint, da sonst der Kontrast zu hoch wird, weil die Kamera sich auf ein mittleres Belichtungsniveau für den Himmel einstellt. Entsprechend wird das eigentlich gewünschte Motiv zu sehr abgedunkelt. Dies lässt sich zum Beispiel vermeiden, indem die Kamera möglichst hoch angebracht wird, nötigenfalls an einer Stange. Verwenden Sie steife Befestigungselemente, um Erschütterungen durch Windstöße zu vermeiden.

- **Spiegelungen**
  Wenn die Kamera hinter Fensterglas montiert wird, zum Beispiel in einem Gehäuse, muss das Objekt nahe am Glas positioniert werden. Andernfalls wird das Bild durch Spiegelungen aus der Kamera und dem Hintergrund beeinträchtigt. Zur Verringerung von Spiegeleffekten sind spezielle Beschichtungen erhältlich, die auf dem Glas vor dem Objektiv aufgebracht werden können.

- **Ausleuchtung**
  Beim Nachteinsatz kann eine zusätzliche, externe Lichtquelle erforderlich sein. Sie muss so angebracht werden, dass Spiegelungen und Schattenwurf vermieden werden. Zur verdeckten Überwachung können anstelle gewöhnlicher Lichtquellen (sogenanntes „Weißlicht“) Infrarotleuchten verwendet werden. Infrarotlicht ist für das menschliche Auge unsichtbar, reicht aber aber für die Aufnahme von Bildern mit Infrarot-Kameras aus. Man kann infrarotempfindliche Netzwerk-Kameras direkt an das Netzwerk anschließen oder herkömmliche Infrarot-Kameras über einen Videoserver in das Netzwerk einspeise. *Hinweis: Farbkameras sind für Infrarotlicht ungeeignet. Manche Kameras können zwischen einem Tageslicht-Farbbetrieb und einem Infrarotmodus für Nachaufnahmen umschalten, der das Bild dann ohne Farbgebung erfasst. Weitere Informationen zum Tag- und Nachteinsatz finden Sie in Kapitel 3.5 auf Seite 27.*

4.2. Einsatz von analogen Kameras mit Videoservern

Analoge Kameras jedweder Art – von unbeweglichen Kameras über Dome-Kameras, Innen- und Außenkameras, unbeweglichen Dome-Kameras bis zu PTZ-Kameras und Spezialsystemen – können mit Hilfe von Videoservern in ein digitales Netzwerk eingebunden werden. Das Koaxialkabel der analogen Kamera wird einfach mit dem analogen Eingang des Videoservers verbunden. Der Videoserver digitalisiert und komprimiert das Video und überträgt es über ein lokales Netzwerk oder das Internet. Das eingespeiste Video wird ebenso wie der Videodatenstrom aus einer Netzwerk-Kamera über das Netzwerk transportiert und steht zur Integration in Netzwerk-Videosysteme bereit. Kurz gefasst konvertiert der Videoserver die Analogkamera zu einer Netzwerk-Kamera.



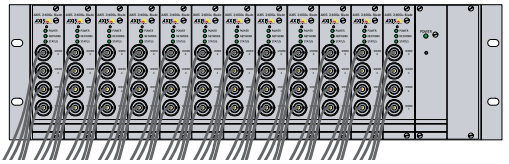
Je nachdem, welche Konfiguration, wie viele Kameras welchen Typs eingesetzt werden und ob ein Koaxialkabel vorhanden ist, können verschiedene Typen von Videoservern eingesetzt werden.

4.2.1. Rack-mounted video servers

Die meisten Unternehmen verfügen über einen eigenen Kontrollraum, der als Zentrale für elektronischen Geräte dient. Auf diese Weise können Vorgänge für kritische Informationen in einer sicheren und geschützten Umgebung wirksam überwacht werden. Bei Gebäuden mit zahlreichen installierten Analogkameras ist dafür eine aufwändige Verlegung von Koaxialkabeln zum Kontrollraum erforderlich.

Wenn die Koaxialkabel bereits verlegt und im zentralen Kontrollraum verfügbar sind, kann ein Videoserver-Rack nützlich sein, der einer Reihe von Blade-Videoservern Platz bietet. Im Rack können die Server zentral verwaltet werden. Er enthält Einschübe für bis zu 12 austauschbare Blade-Videoserver; an der Rückseite der einzelnen Einschübe stehen Anschlüsse für Netzwerk, seriellen Datenaustausch und Eingänge/Ausgänge zur Verfügung, dazu ein gemeinsames Netzteil. In einem 19-Zoll-Standardrack mit 3 Geräteeinheiten (3 U) bringt man normalerweise bis zu 48 Kanäle mit voller Framerate unter und erhält eine kompakte, Platz sparende Lösung.

Komplett mit Koaxialkabeln ausgestattetes Rack



4.2.2. Eigenständige Videoserver

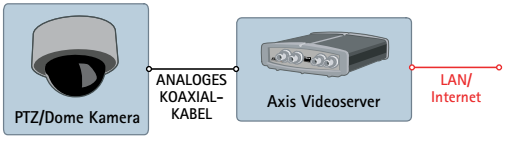
Bei Video-Überwachungssytemen mit analogen Kameras ohne installierte Koaxialkabel sollte an jeder Kamera ein eigenständiger Videoserver installiert werden. Dadurch kan man nicht nur die Verlegungskosten für den Transport der Datenkabel senken, sondern vermeidet auch ein Absinken der Bildqualität, das bei längeren Koaxialverbindungen in Kauf genommen werden müsste. Da Videoserver digitale Bilder erzeugen, bleibt die Bildqualität auch bei größeren Entfernungen erhalten.

Analog-Kamera und Video-Server in einem Gehäuse

4.2.3. Videoserver mit PTZ- und Dome-Kameras

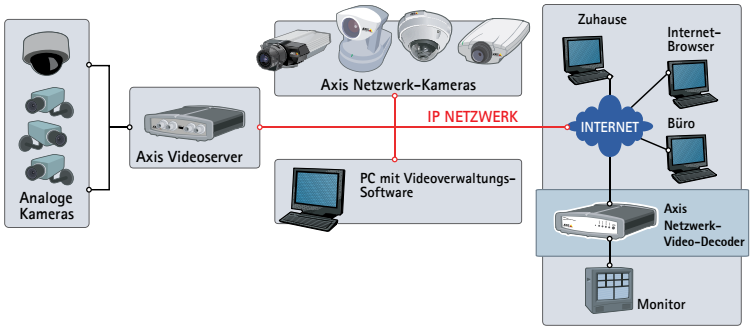
PTZ-Kameras können sowohl an eigenständige Videoserver als auch an Rack-montierte Videoserver angeschlossen werden. Zu diesem Zweck ist an jedem Videoserver eine serielle Schnittstelle (RS232/422/485) angebracht. Wenn ein Videoserver mit einer Schnittstelle direkt an der Kamera aufgestellt wird, müssen keine zusätzlichen Kabel für die PTZ-Steuerung der Kamera verlegt werden. Außerdem kann die Kamera per Internet auch über längere Entfernungen hinweg bedient werden. Zur Steuerung der jeweiligen PTZ-Kamera muss im Videoserver ein passender Treiber bereitstehen. Für die Axis Videoserver sind PTZ-Treiber für die meisten gängigen PTZ- und Dome-Kameras verfügbar, die auf den Videoserver hochgeladen werden können. Es kann auch ein Treiber auf dem PC, auf dem die Videoverwaltung ausgeführt wird, verwendet werden, sofern der serielle Anschluss als serieller Server konfiguriert wird, der die Befehle durchlaufen lässt.

Mit einem Video-Server verbundene PTZ/Dome Kamera



4.2.4. Video-Decoder

Bei einigen Anlagen müssen die Netzwerk-Video- und Audioströme auf vorhandenen analogen Überwachungsgeräten überwacht werden. Mit einem Netzwerk-Video-Decoder werden die digitalen Video- und Audio-Datenströme in analoge Signale zurückkonvertiert, die dann von regulären TV-Geräten, analogen Monitoren und Video-Umschaltern verwertet werden können. Encoder/Decoder sind eine sehr kostengünstige Möglichkeit zur Übertragung von analogem Video über längere Entfernungen hinweg (analog – digital – analog).



Mit Hilfe eines Netzwerk-Video-Decoders kann Video und Audio auch aus entfernten Analog-Kameras oder –Systemen auf vorhandenen analogen Monitoren wiedergegeben werden, selbst wenn die Kameras in einer anderen Stadt installiert sind.

IP-Netzwerk-Technik

Das Internet-Protokoll (IP) ist inzwischen das meistgenutzte Kommunikationsprotokoll für Computer. Es dient als Basisprotokoll für Internet-basierte Kommunikationsformen wie E-Mail-Übertragung, Web und Multimedia. Ein Grund für seine weite Verbreitung ist seine Skalierfähigkeit. Es ist für kleine Installationen ebenso geeignet wie für hochkomplexe, groß angelegte Konfigurationen und wird durch ein wachsendes Angebot an leistungsstarken, kostengünstigen und branchenbewährten Technologien und Geräten unterstützt.

Dieses Kapitel gibt Ihnen einen Überblick über die verschiedenen IP-basierten Technologien, mit denen Sie alle Vorteile eines Netzwerk-Videosystems ausschöpfen können.

5.1. Ethernet

In modernen Büroumgebungen sind Computer in der Regel über TCP/IP in ein Ethernet-Netzwerk eingebunden. Ethernet-Netzwerke sind schnell und relativ preisgünstig. Die meisten modernen Computer verfügen über eine Ethernet-Schnittstelle oder lassen sich problemlos mit einer Ethernet-Netzwerkkarte (NIC) ausstatten.

Gebräuchliche Ethernet-Typen

10 Mbit/s (10 Mbps) Ethernet
Dieser Standard wird aufgrund seiner begrenzten Kapazität in professionellen Netzwerken kaum noch eingesetzt und wird seit Ende der 90er Jahre durch 100 Mbit/s Ethernet abgelöst. Die gebräuchlichste Topologie für 10 Mbit/s Ethernet wurde als 10BASE-T bezeichnet; sie nutzt 4 Leitungen (zwei verdrillte Leitungspaare) in einem CAT 3- oder CAT 5-Kabel. Zentrales Element dieser Topologie ist ein Hub oder Switch, der für jeden Netzwerkknoten eine Schnittstelle bereitstellt. Für Fast Ethernet und Gigabit Ethernet ist dieselbe Konfiguration gebräuchlich.

Fast Ethernet (100 Mbit/s)
Fast Ethernet unterstützt Datenraten bis zu 100 Mbit/s und ist der gängigste Ethernet-Typ in modernen Computernetzwerken. 100BASE-T ist die Bezeichnung für den wichtigsten Standard. Fast Ethernet ist aktueller und schneller als 10 Mbit Ethernet, unterscheidet sich ansonsten jedoch nicht vom älteren Typ. Der 100BASE-T-Standard ist in folgenden Ausführungen erhältlich:

- 100BASE-TX: doppelt verdrillte Kupferleitungen (CAT 5).
- 100BASE-FX: 100 Mbit/s Ethernet über Glasfaser.

Hinweis: Die meisten 100 Mbit Netzwerk-Switches unterstützen sowohl 10 Mbit als auch 100 Mbit und sind damit rückwärtskompatibel. Sie werden daher auch als 10/100 Netzwerk-Switches bezeichnet.

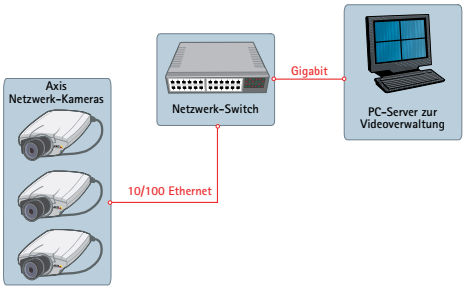
Gigabit Ethernet (1000 Mbit/s)

Dies ist der neueste Standard, den die Hersteller von Netzwerkprodukten für Desktop-Computer empfehlen. Er wird allerdings zumeist für Backbones zwischen Netzwerk-Servern und Netzwerk-Switches eingesetzt. 1000 Mbit/s hat sich dort bereits durchgesetzt und liegt in den folgenden Ausführungen vor:

- 1000BASE-T: 1 Gbit/s über CAT 5e- oder CAT 6-Kupferkabel.
- 1000BASE-SX: 1 Gbit/s über Mehrmodenfaser (bis zu 550 m).
- 1000BASE-LX: 1 Gbit/s über Mehrmodenfaser (bis zu 550 m). Gegenüber der Monomode-Faser optimiert für längere Strecken (bis zu 10 km).
- 1000BASE-LH: 1 Gbit/s über Monomode-Faser (bis zu 100km). Lösung für lange Strecken.

10 Gigabit Ethernet (10 000 Mbit/s)

Dieser Ethernet-Typ wird als neue Option für Backbones in Firmennetzwerken betrachtet. Beim Standard 10 Gigabit Ethernet werden unterschiedliche Übertragungswege für LAN, WAN und MAN (Metropolitan Area Network, Stadtnetzwerk) genutzt. Er wird gegenwärtig durch den erweiterten Standard IEEE 802.3ae geregelt und soll in eine überarbeitete Version des Standards IEEE 802.3 übernommen werden.



5.2. Power-Over-Ethernet

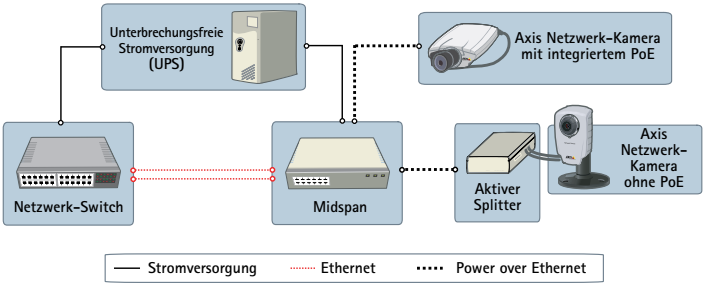
Mit Power-over-Ethernet (PoE) wird die Stromversorgung in eine Standard-LAN-Infrastruktur integriert. Sie ermöglicht die Stromversorgung eines Netzwerkgeräts, z. B. eines IP-Telefons oder einer Netzwerk-Kamera, mit demselben Kabel, das für die Netzwerkverbindung verwendet wird. Sie macht Steckdosen an den Kamerastandorten überflüssig. Dies vereinfacht eine ununterbrochene Stromversorgung zur Sicherstellung des Betriebs rund um die Uhr an jedem Tag der Woche.

Die PoE-Technologie wird durch den Standard IEEE 802.3af geregelt. Dieser stellt sicher, dass weder Übertragungsleistung noch Reichweite des Netzwerks beeinträchtigt werden. Der über die Infrastruktur das LANs gelieferte Strom wird automatisch aktiviert, wenn ein kompatibles Endgerät erkannt wird und für herkömmliche Geräte blockiert, wenn diese nicht kompatibel sind. Mit dieser Funktion können Benutzer herkömmliche und PoE-kompatible Geräte beliebig und ohne Risiko gemeinsam in ihrem Netzwerk einsetzen.

Bei diesem Standard werden bis zu 15,4 W am Switch oder Midspan bereitgestellt. Effektiv stehen am Gerät bzw. an der Kamera bis zu 12,9 W zur Verfügung – genug Energie für Kameras im Innenbereich. Kameras für den Außenbereich sowie PTZ- und Dome-Kameras haben meist einen höheren Energiebedarf, so dass PoE für sie weniger gut geeignet ist. Einige Hersteller bieten auch proprietäre Produkte an, die für diese Anwendungen genügend Leistung bereitstellen. Da sie dem Industriestandard jedoch nicht entsprechen, ist kein kombinierter Betrieb mit anderen Marken möglich. Der Standard 802.3af unterstützt auch die sogenannte Stromklassifizierung. Sie ermöglicht eine Aushandlung der Leistungsaufnahme zwischen dem PoE-Gerät und den Verbrauchern. Dadurch kann ein intelligenter Switch eine ausreichend hohe, aber nicht überflüssige Leistung für das Gerät, in diesem Fall die Kamera, bereitstellen. Der Switch kann unter Umständen mehrere PoE-Ausgänge versorgen.

Power-Over-Ethernet

PoE funktioniert über Standard-Ethernet-Netzwerkkabel (d. h. CAT-5), mittels derer die Stromversorgung direkt über Datenports erfolgt, an die die Netzwerkgeräte angeschlossen sind. Inzwischen bieten die meisten Hersteller Netzwerk-Switches mit PoE-Unterstützung an. Wenn bereits Netzwerk/Switch-Strukturen vorhanden sind, kann sich der Kunde diese Funktion zu Nutze machen, wenn er einen so genannten Midspan an den Switch anschließt, der die Energie in das Netzwerkkabel einspeist. Alle Netzwerk-Kameras ohne eigenes PoE können über einen aktiven Splitter in das PoE-System integriert werden. Das folgende Diagramm veranschaulicht, wie eine Netzwerk-Kamera über ein Netzwerkkabel mit Strom versorgt und selbst bei einem Stromausfall weiter ordnungsgemäß betrieben werden kann.



5.3. Kabellose Netzwerke

Obgleich heutzutage in den meisten Gebäuden kabellose Netzwerke bestehen, kann eine kabellose Lösung in manchen Situationen sowohl finanziell als auch funktional entscheidende Vorteile bieten. Sie bietet sich zum Beispiel für denkmalgeschützte Gebäude an, bei denen keine Verlegung von Kabeln ohne Beschädigung der Bausubstanz möglich wäre oder für Einrichtungen, in denen die Kamera regelmäßig versetzt werden soll, ohne ständig neue Kabel zu verlegen. Ein weiteres Anwendungsbeispiel für kabellose Verbindungen wäre die Vernetzung von zwei Gebäuden oder Standorten ohne teure und komplexe Vorarbeiten.

Kabellose Strukturen gibt es sowohl für analoge als auch für vernetzte Videosysteme, beschränken sich also nicht auf Netzwerke. Es gibt zwei Hauptkategorien für die kabellose Kommunikation:

- **Wireless LAN (auch als WLAN bezeichnet):**
  LANs sind definitionsgemäß lokale Netzwerke, decken also kürzere Entfernungen ab und sind auf den Innenbereich beschränkt. Die Standards für WLAN sind inzwischen hinreichend genau definiert, so dass Geräte verschiedener Hersteller gut zusammenarbeiten.

- **Wireless bridges**
  Wenn Gebäude oder Standorte über Highspeed-Schnittstellen verbunden werden sollen, ist eine Punkt-zu-Punkt-Datenverbindung erforderlich, die auch für längere Entfernungen und hohe Transferraten geeignet ist. Häufig wird dafür Mikrowellen- oder Laserfunk eingesetzt.

WLAN-Standards

802.11a
Standard auf dem 5 GHz Band mit bis zu ~24 Mbit/s effektivem Datendurchsatz bei bis zu 30 m (Außenbereich). Die verfügbare Produktauswahl ist relativ beschränkt. Theoretisch können bis zu 54 Mbit/s erreicht werden.

802.11b
Standard, der bis zu ~5 Mbit/s effektivem Datendurchsatz bei bis zu 100 m (Außenbereich) bietet und das 2,4 GHz-Band nutzt. Theoretisch können bis zu 11 Mbit/s erreicht werden.

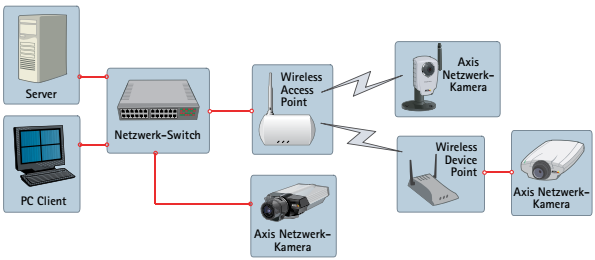
802.11g
Dies ist der gebräuchlichste Standard. Er bietet eine höhere Leistung als 802.11b und ermöglicht einen effektiven Datendurchsatz bis zu ~24Mbit/s bei bis zu 100 m (Außenbereich). Genutzt wird das 2,4 GHz-Band. Theoretisch können bis zu 54 Mbit/s erreicht werden.

802.11n
Die nächste Generation des WLAN-Standards 802.11. Der tatsächliche Durchsatz wird bei über 100 Mbit/s liegen.

Drahtloser Breitband-Zugang

802.16 - WiMAX
IEEE 802.16, auch als WiMAX bezeichnet, ist eine Spezifikation für regionale Breitbandfunknetze, die auf wenige Kilometer begrenzt sind (metropolitan access networks oder MANs) und auf einer Punkt-zu-Mehrpunkt-Architektur basieren. Der Standard legt die Nutzung der Bandbreite in den lizenzierten Frequenzbereichen zwischen 10 und 66 GHz und unter 11 GHz fest. 802.16 unterstützt sowohl beim Upload als auch beim Download von einer Funkstation sehr hohe Bitraten. Unterstützt werden Entfernungen bis zu 50 km und Dienste wie VoIP.

Typisches Netzwerk, mit verkabelten und kabellosen Verbindungen



Dieses Diagramm zeigt eine gängige Verwendungsweise kabelloser Technologie:

- Als Zentraleinheit fungiert hier ein Netzwerk-Switch. Auf der linken Seite sind ein Server (oben) und ein PC Client (unten) über kabelgestütztes Ethernet angeschlossen. In direkter Nähe zum Netzwerk Switch befindet sich ein Wireless Access Point. Dieser regelt den Verkehr mit allen kabellosen Geräten in Reichweite.
- Zwei kabellose Geräte sind in diesem Diagramm dargestellt: Die AXIS 207W Netzwerk-Kamera und ein Wireless Device Point Dieses Gerät stellt kabellose Kommunikation zur Verfügung und stellt eine direkte Verbindung zum Wireless Access Point her.

Entsprechend ist es auch möglich, Server und PC kabellos anzuschließen. Da die Bandweite kabelloser Verbindungen gegenüber kabelgestützten begrenzt ist, sollten nach Möglichkeit die kabelgestützten Varianten bevorzugt werden.

Sicherheit in kabellosen Netzwerken
Es liegt in der Natur der kabellosen Kommunikation, dass grundsätzlich jeder an einem Netzwerk teilnehmen und verteilte Dienste nutzen kann, der selbst ein kabelloses Gerät besitzt und sich im Funkbereich befindet. Daher ist Sicherheit ein wichtiger Gesichtspunkt.

Weitere Informationen zur Sicherheit in kabellosen Netzwerken finden Sie in Abschnitt 5.5.2 auf Seite 47.

Wireless bridges
Es sind Lösungen möglich, die nicht auf dem dominierenden Standard 802.11 beruhen und neben einer höheren Leistung bei größeren Entfernungen ein sehr hohes Maß an Sicherheit bieten. Hierzu gehört auch der Einsatz von anderen Funkfrequenzen, zum Beispiel im Mikrowellenbereich. Auch optische Systeme wie Laser-Verbindungen werden oft eingesetzt. Mikrowellen-Verbindungen können bis zu 1000 Mbit/s auf Entfernungen bis zu 130 km bereitstellen. Bei Standorten außerhalb des Funkbereichs aller dieser Systeme gibt es die Möglichkeit der Satellitenkommunikation. Aufgrund betriebsbedingter Beschränkungen bei der Übertragung zum Satelliten und zurück zur Erde ist die Wartezeit relativ lang und kann mehrere Sekunden betragen. Daher eignet sie sich weniger gut für Funktionen wie die manuelle Kuppelsteuerung und Videokonferenzen, wenn es auf schnelle Umsetzung ankommt. Bei größeren Bandbreiten ist die satellitengestützte Kommunikation zudem sehr kostspielig.

5.4. Datentransportmethoden

5.4.1. IP-Adressen

Eine IP-Adresse (Internet Protocol Address) ist eine eindeutige Nummer, mit der sich Geräte in einem Netzwerk entsprechend dem IP-Standard ausweisen und gegenseitig ansprechen. IP-Adressen bestehen jeweils aus vier Zahlen zwischen 0 und 255, die durch einen Punkt getrennt werden. Ein Beispiel für eine solche Adresse wäre 192.36.253.80.

Die IP-Adresse besteht aus einer Netzwerk- und einer Host-Adresse. Die Grenze zwischen den beiden Teiladressen wird durch eine Netzwerkmaske oder eine Präfixlänge festgelegt. Die Netzwerkmaske 255.255.255.0 z. B. legt fest, dass die drei ersten Byte die Netzwerkadresse darstellen und das letzte Byte die Host-Adresse. Die Präfixlänge ist eine andere Möglichkeit zur Festlegung dieser Grenze. Die Adresse in unserem Beispiel besitzt eine Präfixlänge von 24 Bit (also 192.36.253.80/24).

Bestimmte Adressblöcke sind für die private Nutzung reserviert:

10.0.0.0/8	(Netzmaske 255.0.0.0)
172.16.0.0/12	(Netzmaske 255.240.0.0)
192.168.0.0/16	(Netzmaske 255.255.0.0)

Diese Adressen sind für private IP-Netzwerke vorgesehen und können nicht nach außen in das öffentliche Internet geroutet werden.

5.4.2. IPv6

IPv6, oder Internet Protocol Version 6, ist als Weiterentwicklung des Internet Protocol konzipiert und wird eine Zeit lang parallel zum älteren IPv4 bestehen. IPv6 soll dem Internet ein beständiges Wachstum ermöglichen. Das gilt sowohl für die Anzahl der angeschlossenen Hosts als auch für die Datenmenge, die insgesamt übertragen wird.

Die wichtigste Verbesserung gegenüber IPv4 liegt in der Verlängerung der IP-Adresse von 32 auf 128 Bit. Sie schafft Raum für einen massiven Ausbau des Internet, da eine unbegrenzte Anzahl von Netzwerken und Systemen für die verschiedensten Ziele und Einsatzbereiche integriert werden kann. Zum Beispiel soll IPv6 jedem Mobiltelefon und Mobilgerät eine eigene Adresse bieten.

5.4.3. Datenübertragungsprotokolle für Netzwerk-Video

Das gebräuchlichste Protokoll zur Übertragung von Daten in Computernetzwerken ist TCP/IP. TCP/IP fungiert als Träger für zahlreiche weitere Protokolle wie HTTP (Hyper Text Transfer Protocol), das Protokoll zur Darstellung von Web-Seiten auf Servern überall auf der Welt, die mit dem Internet verbunden sind.

TCP/IP-Protokolle und Schnittstellen für Netzwerk-Video
Für die Übertragung von Netzwerk-Video werden häufig die folgenden Protokolle und Schnittstellen genutzt:

Protokoll	Transport-Protokoll	Port	Gängige Verwendung	Verwendung durch Netzwerk-Video
FTP File Transfer Protocol	TCP	21	Übertragung von Dateien über Internet/Intranet	Übertragung von Bildern oder Video von Netzwerkkamera / Videoserver zu einem FTP-Server oder einer Anwendung
SMTP Simple Mail Transfer Protocol	TCP	25	Protokoll zum Versenden von E-Mail-Nachrichten	Eine Netzwerkkamera / ein Videoserver kann Bilder oder Alarm-Benachrichtigungen über den integrierten E-Mail-Client versenden
HTTP Hyper Text Transfer Protocol	TCP	80	Wird verwendet, um im Internet zu surfen und Webseiten anzuzeigen	Der gängigste Weg, Video von einer Netzwerkkamera / einem Videoserver zu übertragen. Hierbei fungiert das Netzwerk-Video-Gerät als Web-Server und stellt Benutzern die Videodaten zur Verfügung
HTTPS Hypertext Transfer Protocol over Secure Socket Layer	TCP	443	Wird verwendet, um mit Hilfe von Verschlüsselungs-Technologie eine sichere Verbindung zu Webseiten aufzubauen	Sichere Video-Übertragung von einer Netzwerkkamera / einem Videoserver kann auch dazu verwendet werden, die sendende Kamera mit Hilfe eines digitalen X.509 Zertifikats zu authentifizieren
RTP Real Time Protocol	UDP/TCP	Nicht definiert	Standardisiertes Paketformat zum Empfang von Audio und Video über das Internet. Oft verwendet für Streaming Media Systeme oder Videokonferenzen	Ein gängiger Weg, um MPEG-basierte Netzwerk-Video-Daten zu übertragen. Die Übertragung kann an einen (Unicast) oder mehrere (Multicast) Benutzer gleichzeitig erfolgen
RTSP Real Time Streaming Protocol	TCP	554	Einrichtung und Kontrolle von Multimedia-Sitzungen über RTP	

IP verwendet zwei Transportprotokolle: TCP (Transmission Control Protocol) und UDP (User Datagram Protocol). TCP stellt einen zuverlässigen, verbindungsgestützten Übertragungskanal bereit. Das Protokoll bricht längere Datenabschnitte in kleinere Pakete auf, die vom physischen Netzwerk verarbeitet werden können, und sorgt dafür, dass die Daten des Senders beim gewünschten Empfänger ankommen. Im Gegensatz dazu ist UDP ein verbindungsunabhängiges Protokoll. Es gewährleistet nicht die Übergabe der gesendeten Daten und überlässt die gesamte Kontrolle und Fehlerprüfung der eigentlichen Anwendung.

Im Allgemeinen wird TCP verwendet, wenn es mehr auf die Zuverlässigkeit der Kommunikation ankommt als auf die Transportlatenz. Die Zuverlässigkeit von TCP bei erneuter Übertragung, wird mitunter durch spürbare Verzögerungen erkauft. UDP andererseits lässt keine Neuübertragung verlorener Daten zu, sodass keine zusätzlichen Verzögerungen entstehen.

5.4.4. Übertragungsmethoden für Netzwerk-Video Unicasting, Multicasting und Rundsendung

Es gibt mehrere Methoden zur Übertragung von Daten über ein Computernetzwerk:

- *Unicast* - Sender und Empfänger kommunizieren auf Punkt-zu-Punkt-Basis. Die Datenpakete sind an einen einzigen Empfänger adressiert und müssen von den weiteren Computern im Netzwerk nicht verarbeitet werden.
- *Multicast* - Ein einzelner Sender kommuniziert mit mehreren Empfängern in einem Netzwerk. Mit Multicasting wird der Datenverkehr im Netzwerk verringert, wenn mehrere Empfänger dieselbe Quelle zur gleichen Zeit darstellen möchten. Auf diese Weise genügt ein einziger Datenstrom für Hunderte von Empfängern. Der größte Unterschied zum Unicasting besteht darin, dass der Videostrom nur einmal versendet werden muss. Multicasting (genauer, IP-Multicasting) wird häufig zusammen mit RTP-Übertragungen eingesetzt.
- *Rundsendung* - Sendung eines Teilnehmers an alle anderen Teilnehmer. In einem LAN sind Rundsendungen normalerweise auf ein bestimmtes Netzwerksegment beschränkt. Für die Übertragung von Netzwerk-Video spielen sie praktisch keine Rolle.

5.5. Netzwerksicherheit

Es gibt mehrere Möglichkeiten, für Sicherheit in einem Netzwerk und zwischen verschiedenen Netzwerken und Clients zu sorgen. Von den Daten, die über das Netzwerk übertragen werden und der Nutzung des Netzwerks bis zum Netzwerkzugriff, kann jeder Aspekt kontrolliert und abgesichert werden.

5.5.1. Sichere Übertragung

Eine sichere Datenübertagung lässt sich mit einem Kurierdienst vergleichen, der ein wertvolles und sensibles Dokument vom Absender zum Empfänger transportiert und übergibt. Wenn der Kurier beim Absender eintrifft, wird er normalerweise gebeten, sich auszuweisen. Danach entscheidet der Absender, ob es sich um den Kurier handelt als den er sich ausgibt, und ob er vertrauenswürdig ist. Wenn alles in

Ordnung zu sein scheint, wird ihm der sicher verschlossene und versiegelte Aktenkoffer ausgehändigt, den er dann zum Empfänger bringt. Auf der Empfängerseite wird dasselbe Verfahren noch einmal durchgeführt und das Siegel auf seine Unversehrtheit überprüft. Nachdem der Kurier gegangen ist, entriegelt der Empfänger den Aktenkoffer und entnimmt das Dokument, um es zu lesen. Auf ähnliche Weise wird eine sichere Kommunikation hergestellt. Dieser Vorgang besteht aus drei Schritten:

Authentifizierung
Bei diesem ersten Schritt weist sich der Benutzer oder das Gerät gegenüber dem Netzwerk und dem Teilnehmer am anderen Ende aus. Dazu muss er im Netzwerk oder System eine Art von Identitätsnachweis erbringen, zum Beispiel über einen Benutzernamen und ein Kennwort, ein X509-Zertifikat (SSL) und den Standard 802.1x.

Autorisierung
Im nächsten Schritt muss die Authentifizierung autorisiert und angenommen werden; hier wird überprüft, ob es sich um das Gerät handelt, als das es sich ausgibt. Die angegebene Identität wird in einer Datenbank oder mit einer Liste richtiger und anerkannter Identitäten abgeglichen. Nach der Autorisierung ist die Verbindung zwischen dem Gerät und dem System vollständig hergestellt.

Authentifizierung über IEEE 802.1x

Der Standard 802.1x entstand aus dem Bedürfnis nach mehr Sicherheit in der kabellosen Netzwerktechnik und zählt heute zu den meistverbreiteten Authentifizierungsmethoden.
IEEE 802.1X bietet Geräten an einer LAN-Schnittstelle die Möglichkeit zur Authentifizierung über eine Punkt-zu-Punkt-Verbindung und unterbindet den Zugriff, wenn die Authentifizierung fehlschlägt.

Funktionsweise
Clients und Server in einem 802.1x Netzwerk authentifizieren sich gegenseitig mit Hilfe von digitalen Zertifikaten, die von einer Zertifizierungsstelle ausgestellt werden. Die Zertifikate werden dann von einer weiteren Instanz überprüft. Das kann ein als RADIUS-Server bezeichneter Authentifizierungsserver sein, zum Beispiel der Microsoft Internet Authentication Service.

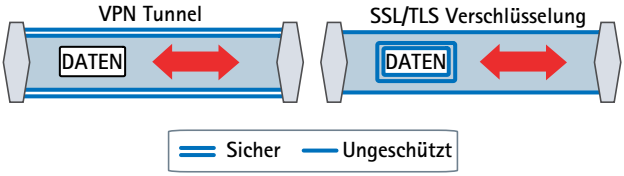
Das Axis Netzwerk-Videosystem legt sein Zertifikat dem Netzwerk-Switch vor, der es an den RADIUS-Server weiterleitet. Der RADIUS-Server prüft das Zertifikat und bestätigt es oder weist es zurück. Je nach seiner Antwort lässt der Switch den Zugriff das Netzwerk über einen vorkonfigurierten Port zu oder unterbindet ihn.

Dadurch ist es möglich, Netzwerk-Sockets offen und verfügbar zu halten: Der Access Point verbindet den Teilnehmer nur dann mit dem Netzwerk, wenn er sich entsprechend ausweisen kann.

Datenschutz
Im letzten Schritt wird der erforderliche Datenschutz umgesetzt. Die Kommunikation wird verschlüsselt, so dass andere Netzwerk-Teilnehmer die Daten nicht nutzen oder lesen können. Je nach Implementierung und Art der Verschlüsselung kann die Verschlüsselung die Leistung stark beeinträchtigen. Der Datenschutz kann auf verschiedene Weise gewährleistet werden. Zu den gängigen Methoden gehören VPN und SSL/TLS (auch als HTTPS bekannt):

- **VPN** (Virtual Private Network)
  VPNs bauen einen sicheren Tunnel zwischen den VPN-Verbindungspunkten auf. Im VPN können nur Geräte mit dem richtigen Schlüssel aktiv werden. Netzwerkgeräte zwischen dem Client und dem Server können weder auf die Daten zugreifen noch sie darstellen. Im VPN können mehrere Standorte über das Internet sicher und geschützt miteinander verbunden werden.

- SSL/TLS
  Eine weitere Methode, für Sicherheit zu sorgen, ist die Verschlüsselung der eigentlichen Daten. In diesem Fall wird kein sicherer Tunnel wie bei der VPN-Lösung eingerichtet, sondern die Daten selbst werden abgesichert. Hierbei stehen verschiedene Verschlüsselungstechniken wie SSL, WEP und WPA bereit. Die beiden letztgenannten Verfahren werden in kabellosen Netzwerken eingesetzt. Bei SSL, das auch als HTTPS bezeichnet wird, installiert das Gerät bzw. der Computer ein Zertifikat, das lokal vom Benutzer ausgegeben oder von einer externen Vergabestelle wie Verisign ausgestellt werden kann.



5.5.2. Sicherheit in kabellosen Netzwerken

Es liegt in der Natur der kabellosen Kommunikation, dass jeder Anwender mit einem kabellosen Gerät, der sich in Reichweite des Netzwerks befindet, am Netzwerk teilnehmen und gemeinsame Dienste nutzen kann. Daraus ergibt sich ein Sicherheitsbedarf.

WEP
WEP (Wireless Equivalent Privacy) verschlüsselt die Kommunikation mit RSA RC4 und verhindert, dass Anwender ohne den richtigen Schlüssel auf das Netzwerk zugreifen können.

Aufgrund mehrerer Sicherheitslücken ist WEP anfällig für Angriffe und kann daher nicht die erforderliche Sicherheit bieten. Die größten Schwachpunkte liegen bei WEP im statischen Codierschlüssel und dem kurzen Initialisierungsvektor. Da WEP mit billigen Standardprodukten angegriffen werden kann, sollten sich kabellose Netzwerke aus Sicherheitsgründen nicht auf WEP stützen.

WPA
Mit WPA (WiFi Protected Access) wurden die wichtigsten Sicherheitslücken von WEP gestopft. Unter WPA wechselt der Schlüssel für jeden übertragenen Frame mittels TKIP (Temporal Key Integrity Protocol). Der Initialisierungsvektor wurde von 24 auf 48 Bit verlängert. WPA gilt als die ausreichende Grundstufe für Sicherheit im kabellosen Netzwerk.

Noch etwas mehr Sicherheit bietet WPA2. WPA2 setzt AES (Advanced Encryption Standard) anstelle von TKIP ein. AES ist das derzeit beste verfügbare Verschlüsselungsverfahren für kabellose Netzwerke. WPA2 bietet ebenfalls Authentifizierung nach 802.1x *(siehe Abschnitt über 802.1x)*.

5.5.3. Schutz von einzelnen Geräten

Zur Sicherheit gehört auch der Schutz einzelner Geräte vor unbefugten Eindringlingen, die versuchen, auf die Einheit zuzugreifen, sowie der Schutz vor Viren und anderen Gefährdungen. Der Zugriff auf PC oder andere Server kann über Benutzernamen und Kennwörter abgesichert werden, die mindestens 6 Zeichen lang sein sollten (je länger, desto besser) und sowohl Ziffern als auch Buchstaben enthalten sollten. Groß- und Kleinbuchstaben sollten willkürlich kombiniert werden. Bei PCs können auch Sicherheits-Tools wie Finger-Scanner und Chipkarten eingesetzt werden, die eine schnellere Anmeldung ermöglichen. Zum Schutz der Geräte vor Viren, Würmern und anderen Schadprogrammen wird ein guter Virenscanner mit aktuellen Signaturen empfohlen. Er sollte auf allen Computern installiert werden. Außerdem sollte das Betriebssystem regelmäßig mit den aktuellen Sicherheitsupdates und Wartungsversionen des Herstellers auf den neuesten Stand gebracht werden.

Bei der Verbindung von LANs mit dem Internet sollte unbedingt eine Firewall verwendet werden. Sie dient als Torwächter und blockiert oder beschränkt den Datenverkehr ins und aus dem Internet. Außerdem kann sie Informationen filtern, die durch die Firewall geleitet werden oder den Zugriff auf bestimmte entfernte Standorte beschränken.

5.6. QoS (Quality of Service)

Heutzutage schmelzen grundlegend unterschiedliche Netzwerkarchitekturen zu einem IP-Netzwerk zusammen. Zum Beispiel entwickeln sich Telefon- und Videonetze (CCTV) in Richtung IP. In solchen Netzwerken muss man festlegen, wie Netzwerkressourcen gemeinsam genutzt werden, damit die Anforderungen der verschiedenen Dienste erfüllt werden. Ein möglicher Ansatz lässt beim Datenverkehr im Netzwerk ein unterschiedliches Verhalten von Netzwerk-Routern und Switches für unterschiedliche Dienste (Sprache, Daten, Video) zu. Diese Technik wird als DiffServ (für Differentiated Services, differenzierte Dienste) bezeichnet. Mit Hilfe von QoS *(Quality of Service)* können verschiedene Netzanwendungen in einem Netzwerk nebeneinander existieren.

Definition
Mit dem Begriff "QoS" wird eine Reihe von Verfahren bezeichnet, die eine gewisse Qualität für verschiedene Dienste im Netz gewährleisten. Dienstgüte kann zum Beispiel eine eingehaltene Bandbreitenanforderung, geringe Latenz, Verlustfreiheit bei der Paketübertragung usw. bedeuten. Die wichtigsten Vorteile eines QoS-optimierten Netzwerks lassen sich folgendermaßen zusammenfassen:

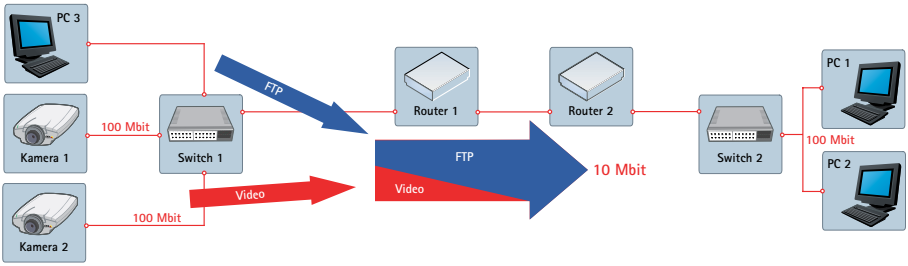
- Fähigkeit, Übertragungsprioritäten festzulegen, sodass kritische Datenströme vor weniger dringlichen bedient werden.
- Größere Zuverlässigkeit im Netzwerk dank der Kontrolle der Bandbreite, die einer Anwendung zugestanden wird und dadurch Kontrolle über die Bandbreitenkonkurrenz zwischen Anwendungen.

QoS und Netzwerk-Video: Anforderungen
Um QoS in einem Netzwerk mit Netzwerk-Videoprodukten umzusetzen, müssen die folgenden Anforderungen eingehalten werden:

- Alle Netzwerk-Switches und Router müssen QoS unterstützen. Das ist wichtig, um Ende/Ende-Funktionalität für QoS zu erreichen.
- Die verwendeten Netzwerk-Videoprodukte müssen QoS-fähig sein.

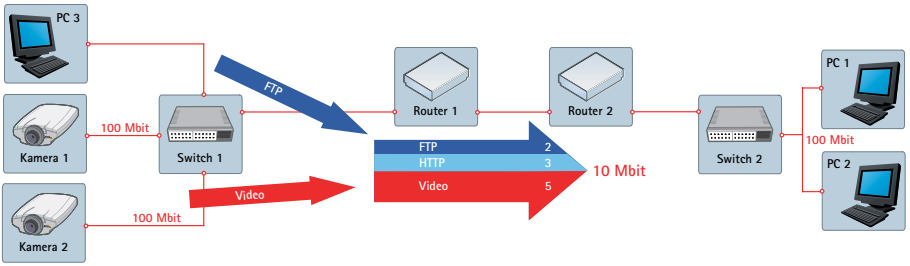
Beispiel für einen QoS-Aufbau

Abbildung 1: Herkömmliches Netzwerk ohne QoS-Umsetzung



In diesem Beispiel überwacht PC1 zwei Videodatenströme aus den Kameras 1 und 2. Beide Kameras versenden Datenströme mit 2,5 Mbit/s. Plötzlich startet PC2 eine Dateiübertragung von PC3. In diesem Fallbeispiel beansprucht die Dateiübertragung die volle Kapazität von 10 Mbit/s zwischen den beiden Routern R1 und R2, während die Videodatenströme versuchen, ihre insgesamt 5 Mbit/s zu behalten. Die Bandbreite, die dem Überwachungssystem zugeteilt wurde, kann nicht mehr gewährleistet werden, und die Video-Bildrate wird wahrscheinlich gesenkt werden. Im schlimmsten Fall lastet der FTP-Datenverkehr die gesamte verfügbare Bandbreite aus.

Abbildung 2: QoS-fähiges Netzwerk



Der Router R1 wurde so eingerichtet, dass bis zu 5 Mbit/s der verfügbaren 10 Mbit/s für das Videostreaming reserviert sind. Der FTP-Übertragung werden 2 Mbit/s zugestanden, HTTP und dem weiteren Datenverkehr bis zu 3 Mbit/s. Bei dieser Aufteilung steht für die Videodatenströmen stets die erforderliche Bandbreite zur Verfügung. Dateiübertragungen gelten als weniger wichtig und erhalten weniger Bandbreite; dennoch steht auch für Web-Browser und andere Anwendungen Bandbreite zur Verfügung. Diese Höchstgrenzen gelten nur, wenn es zu einem Engpass im Netzwerk kommt. Wenn ungenutzte Bandbreite zur Verfügung steht, kann sie von jeder beliebigen Anwendung genutzt werden.

PTZ-Übertragungen

PTZ-Daten werden oft als kritisch eingeschätzt und erfordern eine geringe Latenz, damit Bewegungsanforderungen schnell umgesetzt werden können. Dies ist ein typisches Beispiel dafür, dass QoS die benötigte Sicherheit gewähren kann. Die QoS-Kontrolle der PTZ-Übertragung in Axis Netzwerk-Videoprodukten wird vom ActiveX Viewer AXIS Media Control (AMC) übernommen, der beim ersten Zugriff mit Microsoft Internet Explorer auf das Axis Produkt automatisch installiert wird.

5.7. Weitere Informationen zu Netzwerk-Technologien und Geräten

Hubs, switches und bridges

Hubs dienen in erster Linie als Anschlusskästen, mit denen sich mehrere Geräte einen Ethernet-Anschluss teilen können. Normalerweise können zwischen 5 und 24 Geräte an einen Hub angeschlossen werden. Wenn zusätzliche Geräte verwendet werden sollen, kann ein weiterer Hub angeschlossen werden. Sie machen das Netzwerk schneller, indem Sie geschaltete Hubs verwenden, die eine gleichzeitige Übertragung von Datenpaketen zulassen.

Gateways und router

Gateways und Router dienen im Wesentlichen der Paketweiterleitung und werden auf Schicht 3 (d.h. auf der IP-Schicht) ausgeführt. Die Weiterleitungsentscheidungen werden auf Basis von IP-Adressen und IP-Routertabellen getroffen. Mit einem Gateway können zwei Netzwerke mit unterschiedlicher Architektur zu einem Netzwerk gebündelt werden.

NAT-Router

Jedes Gerät, das mit dem Internet verbunden ist, muss mit einer eindeutigen öffentlichen IP-Adresse gekennzeichnet sein. Öffentliche IP-Adressen sind bei Internetdienstanbietern erhältlich. Ein LAN mit privaten Adressen kann über einen NAT (Network Address Translator), der die internen, privaten Adressen zu öffentlichen Adressen umsetzt, mit dem Internet verbunden werden.

Gateways

Ein Gateway bietet eine bequeme Möglichkeit zum Aufbau eines lokalen Netzwerks. Das Gateway ist eine Kombination aus Router, Umschalter und NAT und wird von zahlreichen Herstellern angeboten.

DHCP-Servers

Die Verwaltung der IP-Adressen kostet umso mehr Zeit, je mehr Geräte in einem Netzwerk zu verwalten sind. Mit einem DHCP-Server kann man jedoch den Zeitaufwand und die Anzahl der IP-Adressen in Grenzen halten. Der DHCP-Server weist Netzwerk-Geräten automatisch eine IP-Adresse zu, wenn die Verbindung zum Netzwerk hergestellt wird.

DNS-Server

Größere Netzwerke verfügen über einen Namensserver (“DNS”, Domain Name Server). Er weist Namen entsprechende IP-Adressen zu und merkt sich die jeweilige Kombination. Der Benutzer kann sich zum Beispiel die Bezeichnung „Tuer“ für die Kamera über der Tür leichter merken als die eigentliche IPAdresse, 192.36.253.80.

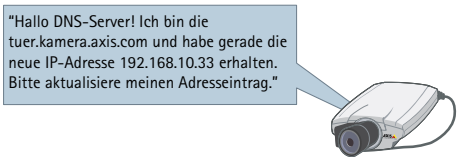
Firewall

Eine Firewall dient dazu, nicht autorisierte Zugriffe auf ein oder von einem privaten Netzwerk zu unterbinden. Firewalls können in Form von Hardware, Software oder als Hardware/Software-Kombination aufgebaut werden. Firewalls werden oft dazu genutzt, unbefugte Internet-Teilnehmer vom Zugriff auf private Netzwerke fern zu halten, die mit dem Internet verbunden sind, insbesondere Intranets. Alle Nachrichten, die in das oder aus dem Intranet gelangen, müssen die Firewall passieren, die jede Nachricht

untersucht und alle Nachrichten blockiert, die den festgelegten Sicherheitskriterien nicht entsprechen. Mit einer Firewall kann zum Beispiel gewährleistet werden, dass Videoterminals auf die Kameras zugreifen können, während die Kommunikation von anderen Computern mit den Kameras abgeblockt wird.

DDNS und dynamische IP-Adressen
Dynamisches DNS dient dazu, die Verknüpfung eines Domänennamen mit einer wechselnden IP-Adresse aufrecht zu erhalten, da nicht alle Computer statische IP-Adressen nutzen. Wenn sich ein Anwender mit dem Internet verbindet, weist ihm der Internet-Anbieter eine ungenutzte IP-Adresse aus einem IP-Adresspool zu. Diese Adresse wird nur für die Dauer der betreffenden Verbindung genutzt. Durch die dynamische Adressvergabe können die verfügbaren IP-Adressen von einem größeren Teilnehmerkreis genutzt werden. Der Internet-Anbieter mit DDNS nutzt ein bestimmtes Programm, das auf dem Anwender-Computer ausgeführt wird. Es spricht den DNS-Dienst bei jeder Änderung der IP-Adresse durch den Anbieter an und aktualisiert danach die DNS-Datenbank mit der geänderten IP-Adresse. Auf diese Weise müssen andere Anwender die geänderte IP-Adresse nicht kennen, wenn sie sich mit dem betreffenden Computer verbinden möchten, selbst wenn die IP-Adresse des Domänennamens häufig wechselt.

Bei einer Netzwerk-Videoanwendung z. B. kann man sich den beschreibenden Namen einer Überwachungskamera an der Eingangstür wie “tuer.kamera.axis.com” leichter merken. Unter DHCP kann sich die IP-Adresse der Kamera jedoch von Zeit zu Zeit ändern. Eine statische Verknüpfung zwischen “tuer.kamera.axis.com” und der IP-Adresse der Kamera “192.36.253.80” kann daher nach einiger Zeit ungültig werden. Dieses Problem wird von DDNS gelöst: Wenn die Kamera ihre IP-Adresse wechselt, nimmt sie Kontakt mit dem DNS-Server auf und aktualisiert den zugeordneten Adresseintrag.



SNMP
SNMP (Simple Network Management Protocol) ist ein Satz von Protokollen zur Verwaltung komplexer Netzwerke, mit dem u. A. vernetzte Geräte entfernt gesteuert und verwaltet werden können.

IPSec
IPSec (“IP Security”, IP-Sicherheit) besteht aus einem Satz von Protokollen, die einen sicheren Austausch von Paketen auf der IP-Ebene unterstützen. IPSec-Protokoll kommt vor Allem in VPNs (Virtual Private Networks) zum Einsatz.

UPnP
UPnP (Universal Plug and Play) ist eine Netzwerkarchitektur, die Netzwerkgeräte, Software und Peripherie von mehr als 400 Anbietern kompatibel hält, die Mitglieder des Universal Plug and Play Forum sind. UPnP eignet sich für verkabelte und unverkabelte Netzwerke und kann von allen Betriebssystemen unterstützt werden. Es ermöglicht eine nahtlose Verbindung der verschiedenen Geräte und erleichtert dadurch die Implementierung von Netzwerken in privaten und in Unternehmensumgebungen.

Mit UPnP können z. B. Netzwerk-Kameras erkannt werden. Wenn Sie eine Kamera zum ersten Mal anschließen, erhält sie möglicherweise eine Adresse vom DHCP-Server, die Sie nicht kennen. Mit UPnP können Sie nach Kameragräten suchen und sich die Adressen anzeigen lassen.

Weitere Informationen über Netzwerk-Technologien und Netzwerk-Geräte finden Sie im Internet unter www.axis.com/products/video/about_networkvideo.

Kriterien für die Systemkonfiguration

Videosysteme beschränken sich heutzutage nicht mehr auf das passive Aufzeichnen und Archivieren von (meist nutzlosen) Daten; sie können eine Situation aktiv auswerten und entsprechende Maßnahmen treffen.

Angesichts der neuen Möglichkeiten und einer Vielzahl neuer Methoden zur Videoverwaltung lautet die wichtigste Frage, welche Anforderungen Ihre Anwendung erfüllen soll und welche Funktionen dazu benötigt werden. Wenn Sie Ihre Anforderungen festgelegt haben, sollten bestimmte Kriterien erwogen werden, damit ein System entsteht, das die Möglichkeiten der Netzwerk-Videotechnologie voll ausschöpft. Diese Kriterien werden im Folgenden erläutert.

6.1. Kriterien für das Systemdesign

6.1.1. Bandbreite

Axis Netzwerk-Video-Produkte verwenden konfigurationsabhängige Bandbreiten. So hängt die Nutzung der Bandbreite einer Kamera von verschiedenen Faktoren ab:

- Bildgröße
- Kompression
- Bildrate (Bilder pro Sekunde)
- Komplexität des Bildes

Es gibt verschiedene Methoden, mit denen Sie das meiste aus Ihrem Netzwerk-Video-System herausholen und die Auslastung der Bandbreite verwalten können; diese schließen den Einsatz folgender Techniken ein:

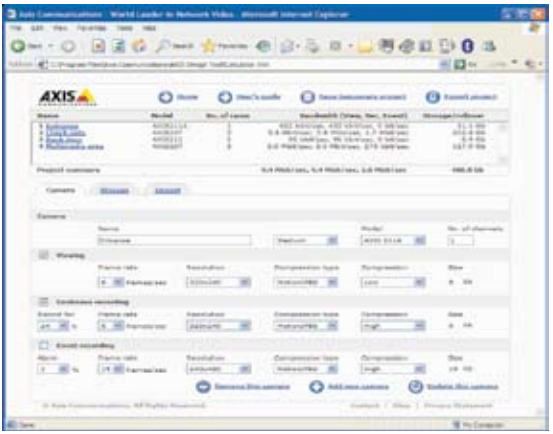
- **Switched Network:** Durch den Einsatz des Network Switching, einer heutzutage weit verbreiteten Netzwerktechnik, können derselbe Computer und das Videonetzwerk in zwei autonome Netzwerke aufgetrennt werden. Auch wenn diese Netzwerke tatsächlich miteinander verbunden bleiben, trennt sie der Netzwerk-Switch logisch in zwei virtuelle und unabhängige Netzwerke.

- **Schnellere Netzwerke:** In dem Maße, wie die Preise für Switches und Router fallen, werden Gigabyte-Netzwerke immer erschwinglicher. Durch die Reduzierung des Effekts einer begrenzten Bandbreite steigert der Trend zu schnelleren Netzwerken den potenziellen Wert der Fernüberwachung über Netzwerke.

- **Ereignisgesteuerte Bildrate:** 30 Bilder pro Sekunde (fps) auf allen Kameras zu jeder Zeit ist mehr als das, was für die meisten Anwendungen benötigt wird. Mit den Konfigurationsmöglichkeiten und der integrierten Intelligenz des Netzwerk-Kamera-/Video-Servers können die Bildraten unter normalen Bedingungen niedriger gesetzt werden, beispielsweise auf 1-3 fps, um die Auslastung der Bandbreite deutlich zu reduzieren. Wird durch die Bewegungserkennung ein Alarm ausgelöst, kann die Aufzeichnungsgeschwindigkeit der Bildrate automatisch auf ein höheres Niveau angehoben werden. In vielen Fällen sendet die Kamera nur Videodaten über das Netzwerk, wenn die Videobilder eine Aufzeichnung rechtfertigen, was durchaus nur in 10% der Zeit der Fall sein kann. 90% der Zeit wird nicht über das Netzwerk übertragen.

Berechnung der erforderlichen Bandbreite
Ein Bandbreitenrechner hilft, die Bandbreite zu bestimmen, die ein Netzwerk-Videoprodukt nutzen wird. Die Berechnung erfolgt anhand der Bildgröße und Bildrate. Außerdem wird berechnet, wie viel Speicherplatz eine aufgezeichnete Bildfolge erfordert.

Beispielhafte Darstellung eines Bandbreitenrechners einer Netzwerkkamera



Um spezifische Bandbreiten-Anforderungen zu berechnen, können Sie von folgender Adresse einen Bandbreitenrechner beziehen: www.axis.com/techsup/cam_servers/bandwidth/

6.1.2. Speicherplatz

Netzwerk-Videosysteme verursachen einen zusätzlichen Festplattenspeicherbedarf. Daraus ergibt sich eine Reihe von Fragen, von der Höhe des zusätzlichen Speicherbedarfs bis zur Ausfallsicherheit des Festplattensystems. Informationen zu den verschiedenen Speicherkonzepten finden Sie in Kapitel 6.4 auf Seite 61.

Berechnung des Speicherbedarfs

Erforderlicher Festplattenspeicher
Kriterien für die Berechnung des Speicherbedarfs:

- Anzahl der Kameras
- Länge der täglichen Aufzeichnungsdauer für die Kamera
- Aufbewahrungsdauer für aufgezeichnete Daten
- Nur bei Bewegungserkennung (ereignisgesteuert) oder fortlaufende Aufzeichnung
- Weitere Parameter wie Bildrate, Komprimierung, Bildqualität und Komplexität

Bitte beachten Sie, dass die nachstehenden Berechnungen nur Beispiele sind und weder Verwaltungsdaten noch andere technische Fragen berücksichtigen, aus denen größere Dateien resultieren können. Im Berechnungsbeispiel ist der Speicherplatz für das Betriebssystem und die Videoverwaltung nicht enthalten.

JPEG/Motion JPEG

Bei JPEG/Motion JPEG werden einzelne Dateien übertragen. Der Speicherbedarf hängt von Bildrate, Bildauflösung und Komprimierung ab: Die Kameras 1, 2 und 3 in der Tabelle generieren einen unterschiedlichen Speicherbedarf, je nach ihrer Bildrate (fps, Bilder pro Sekunde) und der eingestellten Bildauflösung.

Berechnung:
Bildgröße x Bilder pro Sekunde (fps) x 3600 s = KB pro Stunde / 1000 = MB pro Stunde
MB pro Stunde x Betriebsstunden pro Tag / 1000 = GB täglich
GB täglich x erforderliche Aufbewahrungsdauer in Tagen = Speicherbedarf

Kamera	Auflösung	Bildgröße (KB)	Bilder pro Sekunde	MB/Stunde	Betriebszeit in Stunden	GB/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 = 1002 GB

MPEG-4

Unter MPEG-4 werden die Bilder in einem fortlaufenden Datenstrom und nicht als einzelne Dateien übertragen. Der entsprechende Speicherbedarf wird von der Bitrate bestimmt, die die Menge der übertragenen Videodaten angibt. Die Bitrate ergibt sich aus Bildrate, Bildauflösung und Komprimierung sowie den Grad der Bewegung in der Bildszene.

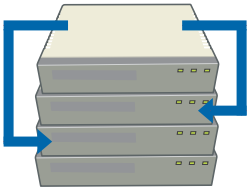
Berechnung:
Bitrate / 8 (Bit pro Byte) x 3600 s = KB pro Stunde / 1000 = MB pro Stunde
MB pro Stunde x Betriebsstunden pro Tag / 1000 = GB täglich
GB täglich x erforderliche Lagerfrist in Tagen = Speicherbedarf

Kamera	Auflösung	Übertragungsrate (kBit/s)	Bilder pro Sekunde	MB/Stunde	Betriebszeit in Stunden	GB/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

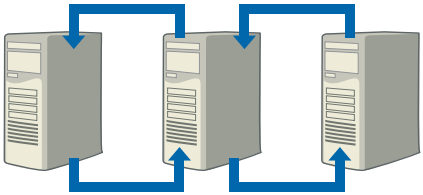
Gesamter Speicherbedarf für die drei Kameras bei 30 Tagen Aufbewahrungsdauer = 204 GB

6.1.3. Redundanz

- **Festplatten-RAID** ist im Wesentlichen eine Methode zur redundanten Aufteilung von Daten über mehrere Laufwerke. Durch die Redundanz können bei einem Festplattenausfall alle Daten aus den verbleibenden Festplatten wiederhergestellt werden. *Weitere Informationen zum RAID-Speicherverfahren finden Sie auf Seite 59.*

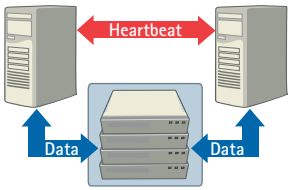


- **Die Datenreplizierung** ist ein Merkmal vieler Netzwerk-Betriebssysteme: Die Dateiserver im Netzwerk sind so konfiguriert, dass sie die Daten wechselseitig replizieren.



- **Die Datensicherung auf Bändern** ist eine alternative oder ergänzende Möglichkeit. Auf dem Markt sind verschiedene Sicherungsprogramme und Hardwaregeräte erhältlich. Es wird empfohlen, Bänder mit den gesicherten Daten als Schutz vor Feuer oder Diebstahl extern aufzubewahren.

- **Server-Cluster:** Es gibt viele Cluster-Methoden. Bei Datenbank- und Mailservern werden oft zwei Server eingesetzt, die dasselbe Speichergerät nutzen, meist ein RAID-System: Fällt ein Server aus, übernimmt der andere Server (mit identischer Konfigurierung) seine Aufgabe. In der Regel teilen sich die beiden Server sogar dieselbe IP-Adresse. Die Übernahme wird dem Benutzer also bewusst gemacht.



- **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, die an getrennten Standorten installiert sind. Die Server können wiederum mit RAID ausgestattet sein, als Cluster konfiguriert werden oder ihre Daten mit weiteren, entfernten Servern replizieren.

6.1.4. Skalierbarkeit

Die Skalierbarkeit hängt vom gewählten Systemtyp ab und muss daher bei der Planung des Videosystems berücksichtigt werden.

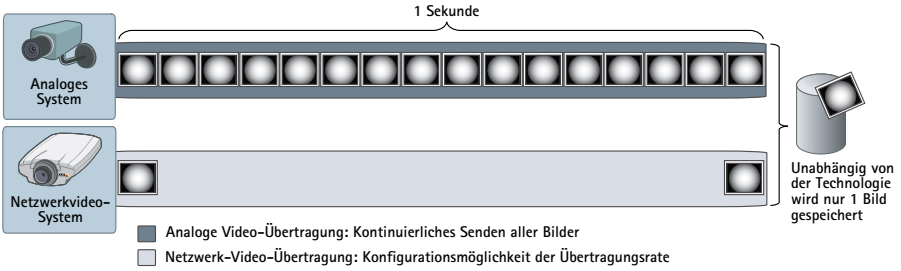
- **Skalierungsschritte:** DVR-Systeme verfügen normalerweise über 4, 9 oder 16 Kamera-Eingänge. Daher sind sie in Schritten von 4, 9 oder 16 skalierbar. Bei Systemen mit 15 Kameras ist das kein Problem, bei 17 Kameras durchaus. Wird auch nur eine Kamera hinzugefügt, müsste ein zusätzliches DVR installiert werden. Netzwerk-Videosysteme sind weitaus flexibler und können in Schritten von je einer Kamera skaliert werden.

- **Anzahl der Kameras pro Recorder:** In Netzwerk-Videosystemen übernimmt ein PC-Server die Aufzeichnung und Verwaltung des Videos. Der PC-Server kann je nach Leistungsanforderungen gewählt werden. Die Leistung wird oft als Anzahl von Bildern pro Sekunde (fps) für das Gesamtsystem angegeben. Wenn für jede Kamera 30 fps benötigt werden, kann jeder Server nur 25 Kameras aufzeichnen. Genügen 2 fps, können 300 Kameras von einem Server verwaltet werden. Das bedeutet, dass die Systemleistung effizient genutzt wird und optimiert werden kann.

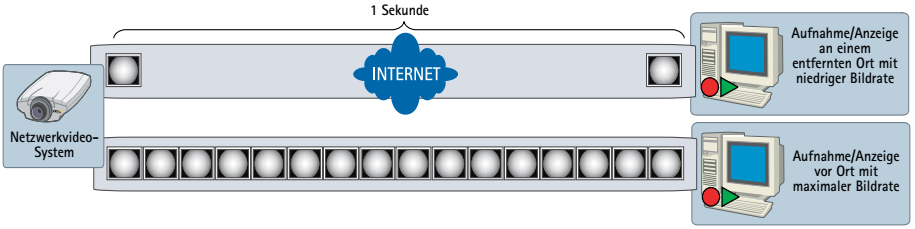
- **Systemgröße:** Bei größeren Installationen lässt sich ein Netzwerk-Videosystem auf einfache Weise skalieren. Wenn höhere Bildraten oder eine längere Aufzeichnungsdauer erforderlich sind, kann der PC-Server, der das Video verwaltet, durch zusätzliche Rechenleistung oder Speicherkapazität aufgerüstet werden. Noch einfacher ist der Einsatz eines weiteren PC-Servers, der zentral oder an einem entfernten Ort installiert werden kann.

6.1.5. Steuerung der Bildrate

Netzwerk-Video lässt eine „Bildratensteuerung“ zu – im Gegensatz zu analogen Systemen, bei denen die Kamera kontinuierlich Videodaten versendet. Eine Bildratensteuerung in Netzwerk-Videosystemen bedeutet, dass die Netzwerk-Kamera bzw. der Videoserver Bilder nur mit der angegebenen Bildrate versendet. Das Netzwerk wird von nicht benötigten Videodaten entlastet. Die Netzwerk-Kamera, der Videoserver oder die Netzwerkverwaltung kann so konfiguriert werden, dass zum Beispiel beim Erkennen einer Aktivität die Bildrate angehoben wird.



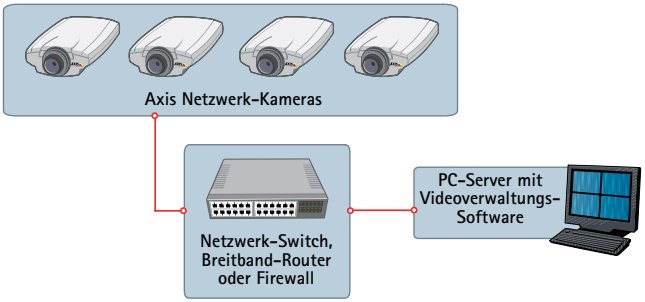
Außerdem kann das Video mit unterschiedlichen Bildraten an verschiedene Empfänger übertragen werden. Das ist vor Allem von Vorteil, wenn die Bandbreite für Verbindungen zu entfernten Standorten begrenzt ist.



6.2. Speicheranforderungen

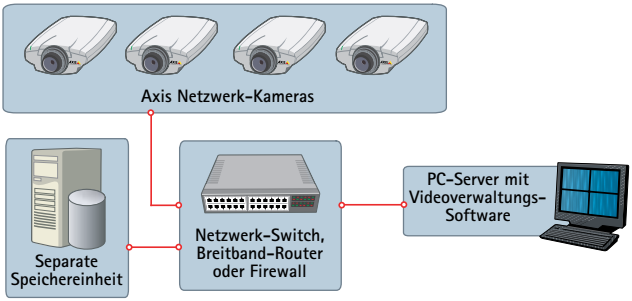
Verschiedene Festplattenlösungen
Der Festplattenspeicher kann auf zwei verschiedene Arten organisiert werden: er kann sich am eigentlichen Server befinden, auf dem die Anwendung ausgeführt wird, oder er kann getrennt vom Server als eigenständiges Speichersystem betrieben werden.

6.2.1. Direkt angeschlossener Festplattenspeicher



Dies dürfte bei kleineren bis mittelgroßen Installationen die gängigste Lösung für den Festplattenspeicher sein. Die Festplatte ist in dem PC installiert, auf dem die Videoverwaltung ausgeführt wird (Anwendungsserver). Der verfügbare Speicherplatz wird vom PC und der Anzahl der Festplatten bestimmt, die darin Platz finden. Die meisten PCs bieten Platz für 2 Festplatten, manche Systeme für bis zu vier Festplatten. Jede Festplatte kann bis zu ca. 300 GB fassen. Daraus ergibt sich insgesamt ein Festplattenspeicher von ca. 1,2 TB.

6.2.2. Netzwerkspeicher (NAS) und Speichernetzwerk (SAN)



NAS

Der Netzwerkspeicher besteht aus einem einzelnen Speichergerät, das direkt an ein LAN angeschlossen wird und als gemeinsam genutzter Massenspeicher für alle Netzwerk-Clients dient. NAS-Geräte sind leicht zu installieren und zu verwalten. Sie stellen eine kostengünstige Lösung für einen erhöhten Speicherbedarf dar, bieten aber nur einen beschränkten Datendurchsatz für eingehende Daten.

SAN

Ein Speichernetzwerk ist ein spezielles Hochgeschwindigkeitsnetzwerk, das als Massenspeicher dient und über Glasfaser an einen oder mehrere Server angeschlossen wird. Die Benutzer können über die Server auf alle Speichergeräte des SAN zugreifen, wobei der Speicher auf mehrere Hundert Terabyte ausgebaut werden kann. Der zentrale Datenspeicher senkt den Verwaltungsaufwand und stellt einen flexiblen Hochleistungs-Speicherpool für Multiserver-Umgebungen zur Verfügung.

Während der NAS ein Speichergerät darstellt, bei dem die ganze Datei auf nur einer Festplatte gespeichert wird, besteht das SAN aus einer Reihe von Geräten, so dass die Datei blockweise auf mehrere Festplatten aufgeteilt werden kann. Diese Art von Festplattenkonfiguration ermöglicht sehr große und skalierbare Festplattenlösungen, die umfangreiche Datenvolumen mit einem hohen Maß an Redundanz aufnehmen können. Für die Videoverwaltung stehen Lösungen beiden Typs zur Verfügung.

6.2.3. RAID (Redundant Array of Independent Disks)

RAID ist die Anordnung von Standard-Festplatten zu einem Gesamtsystem, das vom Betriebssystem als eine einzige logische Festplatte betrachtet wird.

RAID kann in verschiedenen Stufen umgesetzt werden, die ein unterschiedliches Maß an Redundanz bieten – von einer praktisch redundanzfreien Lösung bis zu einer vollständigen Datenspiegelung, bei der Festplatten im laufenden Betrieb ohne Unterbrechung des Betriebssystems ausgetauscht werden können, ohne dass es bei einem Festplattenausfall zu einem Datenverlust kommt.

Die gängigsten RAID-Stufen werden in der folgenden Tabelle aufgelistet.

RAID-Stufe	Eigenschaften
RAID-0	Daten werden zugunsten einer höheren Schreib/Lesegeschwindigkeit auf zwei oder mehrere Festplatten verteilt. Es wird jedoch keine Redundanz erzielt.
RAID-1	Auch als Festplattenspiegelung bezeichnet. Daten werden auf mindestens zwei Festplatten doppelt vorgehalten. Es werden jedoch keine Daten verteilt. Beide Festplatten können gleichzeitig gelesen werden. Die Schreibleistung ist so hoch wie bei einer einzelnen Festplatte.
RAID-5	Diese Stufe umfasst ein rotierendes Paritäts-Array, das eine Überschneidung aller Lese- und Schreibvorgänge ermöglicht. Zur Rekonstruktion verloren gehender Daten werden Paritätsinformationen gespeichert.

6.3. Sicherheitsfunktionen

Bei allen Video-Überwachungssystemen ist der Datenschutz ein wichtiges Kriterium. Video-Analyse und Netzwerk-Kameras können hierbei richtungsweisende Ansätze anbieten. CCTV-Kameras senden nur einen einzigen Video-Datenstrom, der leicht abgefangen werden kann. Im Gegensatz dazu können Netzwerk-Kameras die Videoübertragung im Netzwerk verschlüsseln, sodass sie von Dritten weder angezeigt noch manipuliert werden kann. Das System kann auch zur Authentifizierung der Verbindung mit Hilfe verschlüsselter Zertifikate eingerichtet werden, die nur eine spezielle Netzwerk-Kamera akzeptieren, wodurch verhindert wird, dass sich irgendjemand in die Leitung hineinhackt.

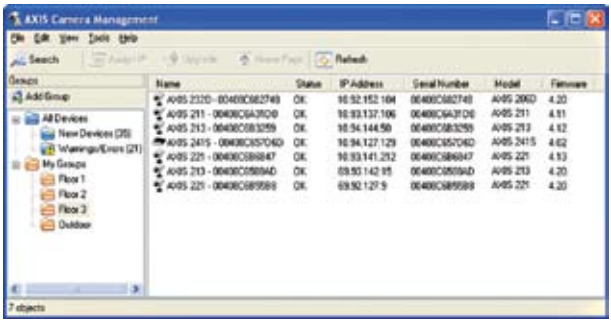
Zum Schutz vor einer Manipulation digitaler Bilder stehen moderne technische Verfahren wie Zeitstempel und Wasserzeichen bereit. Mit Hilfe von Verarbeitungsprotokollen lässt sich nachvollziehen, wer welche Bilder abgerufen hat und welche Bearbeitungsschritte dabei vorgenommen wurden.

Wasserzeichen sind verschlüsselte Kennzeichnungen, mit denen die Netzwerk-Kamera den Videodatenstrom versieht. Die Wasserzeichen geben Zeit, Ort und Benutzernamen an und protokollieren Alarmmeldungen, die für eine bestimmte Aufnahmesequenz ausgegeben wurden. Digitale Wasserzeichen bleiben für den Betrachter unsichtbar. Hierzu werden die Wasserzeichen willkürlich in der Datei verteilt, so dass sie von Unbefugten weder gefunden noch manipuliert werden können.

6.4. Verwalten von Großsystemen

Netzwerk-Videoprodukte sind mit einem integrierten Webserver ausgestattet, der den Zugriff aus dem Netzwerk ermöglicht. Der Webserver sorgt für die Live-Übertragung, aber auch für den autorisierten Zugriff auf interne Einstellungen für Konfiguration und Firmware-Upgrades. Bei Systemen mit einer begrenzten Anzahl an Netzwerk-Kameras oder Videoservern genügt der integrierte Webserver in der Regel. Größere Systeme können jedoch qualifizierte Verwaltungstools erforderlich machen.

Auf der Basis von Standard-Netzwerkprotokollen können Verwaltungstools neue Geräte im Netzwerk automatisch ermitteln und anzeigen, auch wenn sie noch keine gültige IP-Adresse besitzen. Mittels einer gut definierten API wie AXIS VAPIX™ API kann das Verwaltungstool grundlegende Merkmale der gefundenen Geräte anzeigen wie die Modellbezeichnung und die aktuelle Firmware-Version. Außerdem hilft es bei der Festlegung von IP-Adressen, gibt den Verbindungsstatus von lokalen und entfernten Videosystemen an und erlaubt Konfigurierungen oder Firmware-Updates von mehreren Geräten gleichzeitig oder im Stapelbetrieb. Zentrale Verwaltungstools erleichtern nicht nur die Systemwartung sondern tragen auch zu einer Verringerung der Wartungskosten bei.



AXIS Camera Management kann auf mehrere hundert Kameras skaliert werden und eignet sich für systemübergreifende Konfigurierungen und Firmware-Upgrades.

Videoverwaltung

Netzwerk-Kameras sind immer nur so gut wie die konfigurierten Videoverwaltungssysteme, mit denen sie gesteuert werden. Sie sollten so beschaffen sein, dass der Anwender die Videoausgabe effizient überwachen, analysieren und speichern kann. Im Folgenden werden die zwei Ansätze zur Verwaltung der Netzwerk-Videoausgabe miteinander verglichen: die PC-Server-Plattform und die NVR-Plattform mit einem dezidierten Gerät wie dem NVR (Netzwerk-Videorecorder). Außerdem werden verschiedene Möglichkeiten zur Einrichtung von Ereignisverwaltung, Bewegungserkennung und Audiofunktionen beleuchtet.

Systeme auf der Basis einer Netzwerk-Videoplattform können in andere Systeme wie Zugangskontrolle oder Gebäudeverwaltung integriert werden. Umgekehrt können Informationen aus den Fremdsystemen Funktionen im Netzwerk-Videosystem auslösen, so dass z. B. Bilder gespeichert werden können, die im Zusammenhang mit bestimmten Ereignissen stehen.

7.1. Hardware-Plattformen

Für die Netzwerk-Videoverwaltung stehen zwei verschiedene Plattformtypen zur Auswahl: die PC-Server-Plattform und die NVR-Plattform (Netzwerk-Videorecorder). Obwohl beide Typen auf einem PC aufsetzen, unterscheiden sie sich wesentlich.

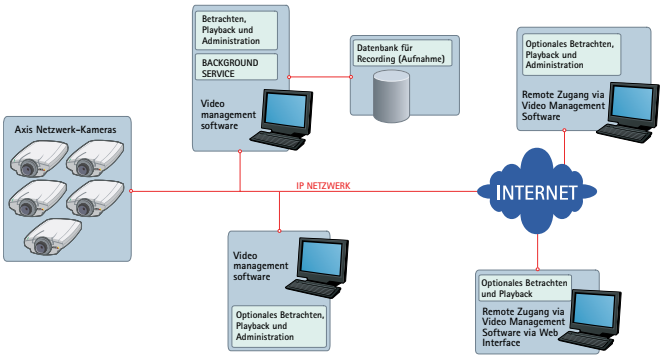
PC-Serverplattformen basieren auf Standard-Hardwarekomponenten, die im Hinblick auf maximale Leistung ausgewählt werden. Bei PC-Serverplattformen können vorhandene Standardkomponenten weitergenutzt werden, zum Beispiel als zusätzliche oder externe Speichergeräte oder zusätzliche Fernbedienungsstationen, und parallel zur Videoanwendung können weitere Programme wie Firewalls oder Virenschutzprogramme ausgeführt werden.

NVR-Plattformen unterscheiden sich von PC-Serverlösungen vor Allem dadurch, dass der NVR als eigenständiges Gerät mit vorinstallierten Videoverwaltungsfunktionen geliefert wird. Definitionsgemäß dient er ausschließlich zur Aufzeichnung, Analyse und Wiedergabe von Netzwerkvideo. Auf NVRs können keine weiteren Anwendungen installiert oder ausgeführt werden. Die NVR-Hardware ist fest an diese Anwendungen gebunden, und nur mit Mühe lassen sich solche Geräte zu Aufgaben heranziehen, die nicht zur ursprünglichen Spezifikation gehören.

Systeme auf der Basis von Netzwerkplattformen sind uneingeschränkt skalierbar. Kameras und Lizenzen können nacheinander hinzugefügt werden, und Sie können die Systemhardware erweitern, um erhöhte Anforderungen an die Leistung zu befriedigen. Diese Plattform eignet sich für die Installation von Systemen mit zahlreichen Kameras und kann auf die Standard-Vorgaben der kundenseitigen IT-Abteilung für Serverhardware und Software im Netzwerk abgestimmt werden.

7.1.1. PC-Server-Plattformen

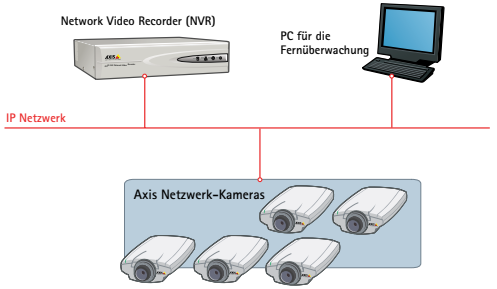
PC-Server-Plattformen basieren auf Standard-Hardwarekomponenten, die für die spezifischen Anforderungs- und Leistungskriterien ausgewählt werden, z. B. externe Speichergeräte oder Doppelprozessorsysteme.



Daher können Kundenwünsche bei der Hardware-Auswahl berücksichtigt werden, und der Kunde muss auf bewährte Anbieter und Dienstleister nicht verzichten.

7.1.2. NVR-Plattformen

Der Netzwerk-Videorecorder ähnelt im Hinblick auf Aufnahme und Wiedergabe einem digitalen Videorecorder (DVR). DVRs sind Hybridsysteme, an die Analogkameras angeschlossen werden können, die aber Video digital auf der Festplatte speichern. NVRs sind reine Digitalsysteme, die digitale Bilder bzw. Video-Datenströme über das Netzwerk beziehen und dann ebenfalls digital auf der Festplatte speichern. Manche DVR-Modelle besitzen eine einfache Netzwerkschnittstelle, über die sich Bilder entfernt abspielen lassen. NVRs kommen ohne eigene Monitore und Tastaturen aus. Alle Anzeige- und Verwaltungsaufgaben der NVRs werden entfernt über Netzwerk mit dem PC abgewickelt.



NVRs sind auf eine optimale Leistung für eine festgelegte Anzahl an Kameras ausgelegt, was ihre Skalierbarkeit im Vergleich zu PC-Serverplattformen einschränkt. Daher eignen sie sich vor Allem für kleinere Systemkonfigurationen, bei denen die Anzahl der Kameras im Rahmen der NVR-Kapazität bleibt. NVRs bieten gegenüber PC-Server-Plattformen den Vorteil, dass sie relativ einfach einzurichten sind.

7.2. Videoverwaltung: Überwachung und Aufzeichnung

Zur Videoverwaltung eines Netzwerk-Videosystems gehören die Video-Überwachung, die mit einem Browser oder einer speziellen Videoverwaltungssoftware durchgeführt werden kann, und die Video-Aufzeichnung. Die Video-Aufzeichnung kann mit einer Videoverwaltung durchgeführt werden, die auf einem PC installiert ist, oder mit Hilfe eines Netzwerk-Videorecorders.

7.2.1. Überwachen mit der Web-Oberfläche

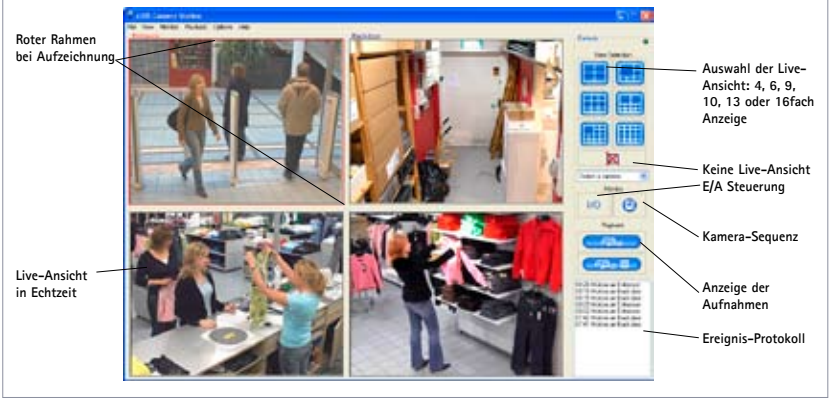
In einem Netzwerk-Videosystem kann das Video an jedem Netzwerkknoten abgerufen werden, soweit er Zugriff auf einen Browser bietet. Jede Kamera verfügt über einen integrierten Webserver mit IP-Adresse. Um die Bilder am PC abzurufen, muss man daher nur einen Browser öffnen und die IP-Adresse der Kamera in die Adresszeile eintragen:

Wenn der Computer die Verbindung aufgebaut hat, ist die Netzwerk-Kamera “Start-Seite” automatisch auf dem Web Browser angezeigt. Diese Start Seite zeigt Live Video Aufnahmen von der Kamera zusammen mit Hyperlinks für die Änderung des Kamera Set-Up, wie Bild Auflösung, Netzwerk und E-Mail Settings - sofern das System mit Sicherheits/Passwort Einschränkungen eingerichtet wurde.

7.2.2. Überwachung mit Hilfe der Videoverwaltung

Video kann zwar direkt in einem Standard-Browser dargestellt werden; Sie können jedoch auch eine Videoverwaltung installieren, wenn Sie weitere Funktionen wie das Speichern und Verwalten von Video nutzen möchten. Auf dem Markt sind zahlreiche Softwarelösungen erhältlich, die von unabhängigen Anwendungen für einen einzelnen PC bis zur komfortablen, Client/Server-basierten Software reicht, die mehrere Benutzer gleichzeitig unterstützt. Zu den allgemein üblichen Funktionen gehören die Video-Überwachung, die Ereignisverwaltung und Warnfunktionen für Alarmsituationen, zum Beispiel das Auslösen einer Sirene oder Versenden von E-Mails.

Beispiel einer Windows-basierten Videoverwaltung Software



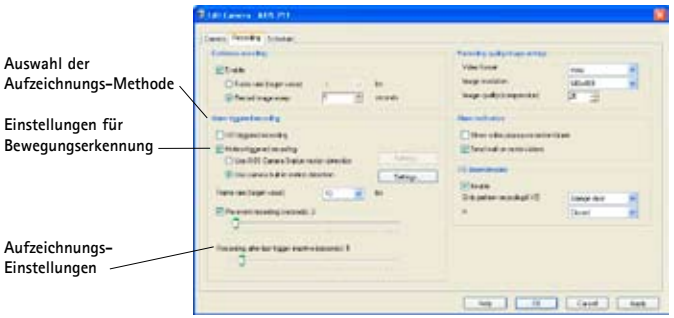
7.2.3. Aufzeichnung von Netzwerk-Video

Für die Aufzeichnung von Netzwerk-Video gibt es mehrere Möglichkeiten:

Für einfache Aufzeichnungen genügen die internen Kamerafunktionen, mit denen anhand von geplanten oder ausgelösten Ereignissen Einzelbilder oder Videobilder erfasst werden können. Diese Bilder werden dann auf einen FTP-Server oder auf die Festplatte eines Computers hochgeladen.

Mit einem dezidierten Netzwerk-Videorecorder (NVR) können Datenströme aus den entfernten Netzwerk-Kameras und Videoservern erfasst und auf einer Festplatte gespeichert werden. Als NVR kann ein vernetzter Standard-PC oder ein spezieller Festplattenserver für Videoaufzeichnungen dienen, auf dem eine entsprechende Anwendung installiert ist.

Beispiel: Aufnahmeoberfläche der AXIS Camera Station Software

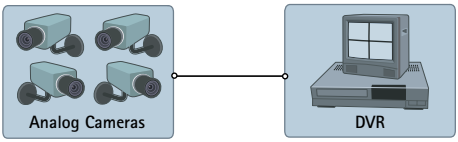


7.3. Systemmerkmale

7.3.1. Video-Bewegungserkennung

Die Video-Bewegungserkennung ist eine Möglichkeit zur Definition von Aktivität in einer Szene. Hierzu werden Bilddaten und Unterschiede in eine Reihe von Bildern analysiert.

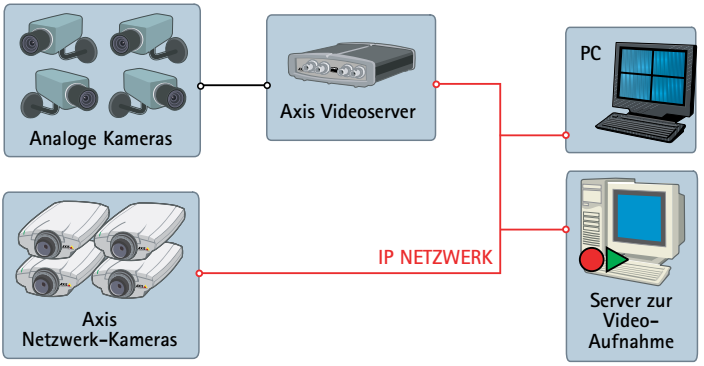
Video-Bewegungserkennung in DVR-Systemen
Die Kameras werden an den DVR angeschlossen, der die Video-Bewegungserkennung für die Videoströme durchführt. Dadurch kann der DVR die Menge der aufgezeichneten Videodaten reduzieren, Aufzeichnungen in eine Rangfolge bringen und Bewegungen in einem bestimmten Bildbereich als Suchbegriff verwenden, wenn nach Ereignissen gesucht wird. Der Nachteil dieser Methode liegt darin, dass die Video-Bewegungserkennung prozessorlastig ist. Wird sie auf mehreren Kanälen durchgeführt, wird das DVR-System stark beansprucht.

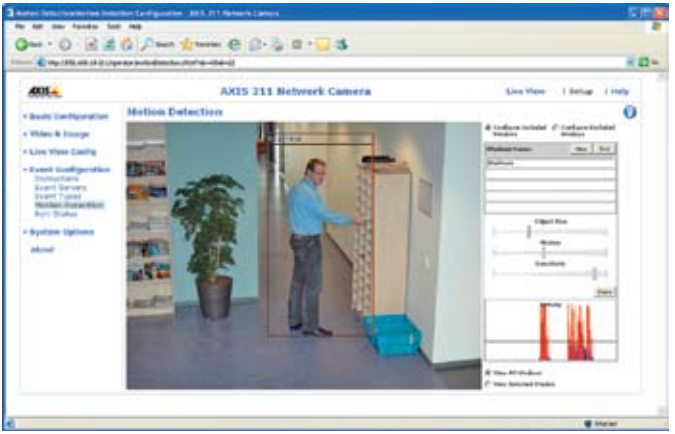


Bewegungserkennung in Netzwerk-Videosystemen
Eine Integrierung der Video-Bewegungserkennung in Netzwerk-Kameras oder Videoservern bietet gegenüber dem obigen Szenario entscheidende Vorteile. Der wichtigste Vorteil ist die direkte Verarbeitung der Video-Bewegungserkennung in der Kamera bzw. auf dem Server. Die Arbeitslast wird für alle Aufzeichnungsgeräte im System verringert. Außerdem ermöglicht dies eine ereignisgesteuerte Überwachung. In diesem Fall werden keine Videodaten (oder nur Video mit niedriger Bildrate) an den Bediener oder das Aufzeichnungssystem gesendet, solange in der Szene keine Aktivität erkannt wird.

Video-Bewegungserkennungsdaten mit Informationen über die Aktivität können auch in den Videostrom eingebunden werden. Das erleichtert die Suche nach Aktivitäten im aufgezeichneten Material. Die Video-Bewegungserkennung kann auch von der Videoverwaltung übernommen werden, so dass auch Netzwerk-Kameras ohne eigene Erkennungsfunktionalität für die Video-Bewegungserkennung eingesetzt werden können.

VMD mit Netzwerk-Video-Ausstattung





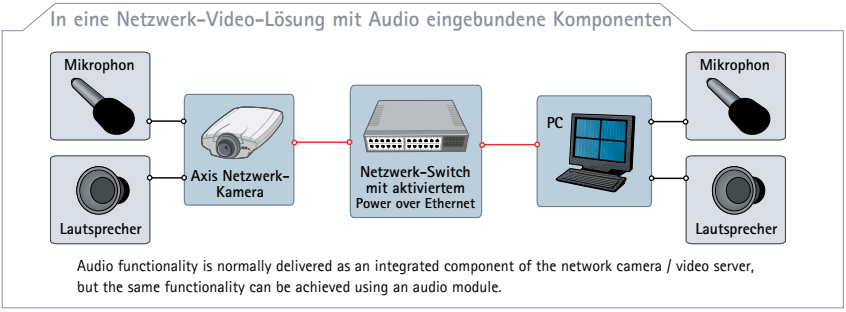
Vorteile von lokaler Video-Bewegungserkennung am Endgerät (Netzwerk-Kamera und Videoserver im Vergleich zu Systemen mit zentraler Analyse wie DVRs)

- Schonen der Bandbreite
- Senkung der Prozessorauslastung auf dem Aufzeichnungsserver
- Sparen von Speicherplatz
- Die Kamera kann mit anderen Systemen, die E/A-Schnittstellen besitzen, interagieren (zum Beispiel Alarm auslösen)

7.3.2. Audio

Audio lässt sich leicht in Netzwerk-Video integrieren, da Netzwerke Daten jedes Typs übertragen können. Dadurch entfällt eine gesonderte Kabelverlegung – im Gegensatz zu analogen Systemen, bei denen die beiden Endpunkte mit einem Audiokabel verbunden werden müssen. Eine Netzwerk-Kamera zeichnet den Ton auf, integriert ihn in den Video-Datenstrom und überträgt ihn zur Überwachung und/oder Aufzeichnung über das Netzwerk.

Dadurch steht Audio auch aus entfernten Standorten zur Verfügung. Zum Beispiel kann die Überwachungsabteilung in der Firmenzentrale mit „Überwachungsszenen" an entfernten Filialen interagieren. Sie können mögliche Eindringlinge darauf aufmerksam machen, dass sie unter Überwachung stehen, und in bestimmten Situationen mithören, um eine zusätzliche, akustische Überprüfung durchzuführen. Audio kann in Netzwerk-Kameras oder Videoservern auch als unabhängige Erkennungsmethode dienen, die Videoaufzeichnungen und Alarmmeldungen auslöst, wenn der Audiopegel einen bestimmten Grenzwert überschreitet.



Audio-Übertragung

Audio kann als integrierter Bestandteil des Video-Datenstroms komprimiert und übertragen werden, wenn MPEG-1/MPEG-2/MPEG-4 oder ein H.x-Standard für Videokonferenzen verwendet wird. Audio kann auch parallel übertragen werden, wenn ein Einzelbildstandard wie JPEG verwendet wird. Wenn jedoch ein synchrone Übertragung von Audio und Video gewünscht wird, ist MPEG die erste Wahl. Dennoch gibt es viele Situationen, in denen eine Audiosynchronisierung weniger wichtig oder sogar unerwünscht ist (zum Beispiel, wenn der Ton überwacht, aber nicht aufgezeichnet werden soll).

Audiokomprimierung

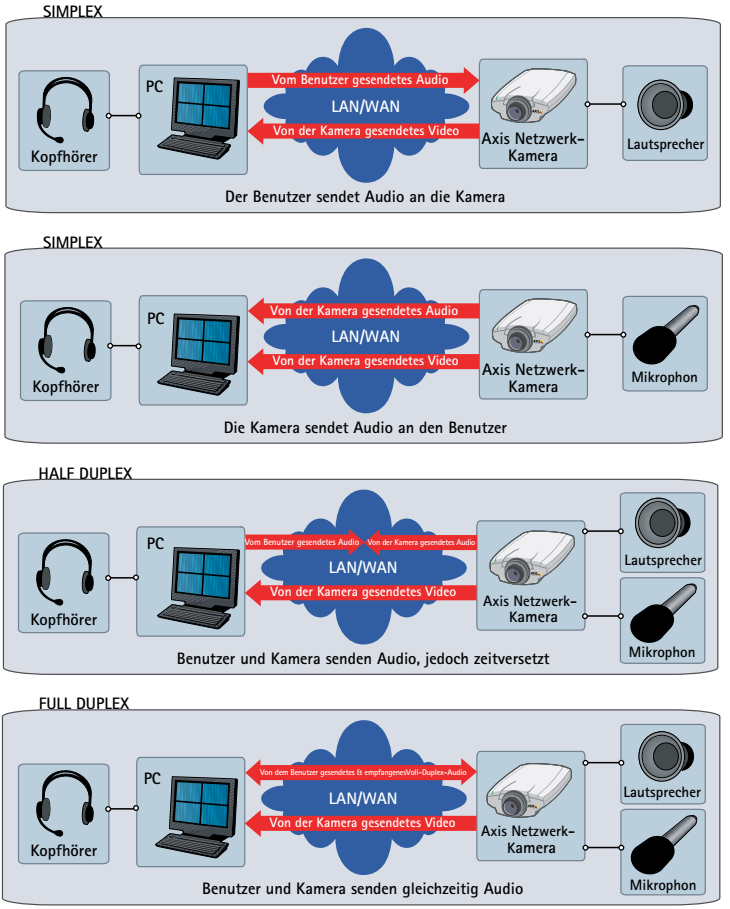
Durch die digitale Audiokomprimierung können Audiodaten effizient übertragen und gespeichert werden. Ähnlich wie bei Video gibt es verschiedene Komprimierungstechniken mit unterschiedlich hohem Komprimierungsgrad. Im Allgemeinen führt eine höhere Komprimierungsstufe zu längeren Wartezeiten. In digitaler Form bietet Audio viele Vorteile, zum Beispiel eine hohe Rauschunempfindlichkeit, Stabilität und Reproduzierbarkeit. Außerdem ermöglicht das digitale Format eine effiziente Implementierung vieler Nachbearbeitungsfunktionen wie Rauschfilter und Entzerrung.

Gängige Audio-Komprimierungsformate:

- G.711 PCM: hohe Audioqualität bei 64 Kbit/s
- G.726 ADPCM: Audio mit 32 oder 24 Kbit/s
- MP3 (ISO-MPEG Audio Layer-3), verbreitetes Format, das vor allem für Musik verwendet wird, mit Bitraten um 100 Kbit/profile), 16 kHz sampling with a bit rate of 40 kbit/s.

Audiomodi

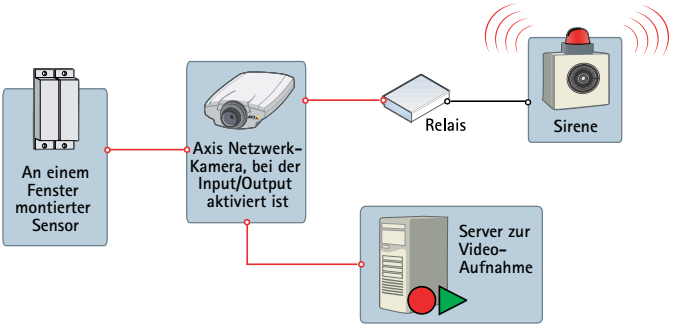
Axis Netzwerk-Kameras bieten mehrere Audiomodi zur Auswahl:



7.3.3. Digitale Ein- und Ausgänge

Ein besonderes Merkmal der Netzwerk-Videoprodukte sind die integrierten digitalen Ein- und Ausgänge, die über das Netzwerk verwaltet werden können. Mit dem Ausgang können Vorgänge ausgelöst werden, entweder automatisch oder von einem entfernten PC aus. Hierzu wird die interne Logik der Kamera genutzt. Die Eingänge können so konfiguriert werden, dass sie auf externe Sensoren wie PIRs oder auf Tastendruck reagieren und Videoübertragungen einleiten.

Die Ein- und Ausgänge können z. B. zusammen mit Alarmsensoren dazu genutzt werden, die Übertragung von nicht benötigten Videodaten zu verhindern, bis der Sensor an der Kamera eine Übertragung auslöst.



E/A Anwendungsbeispiel - Eine Kamera, die mit einer Fenstersicherung und einem Alarmsystem bzw. einer Sirene verbunden ist.

Digitale Eingänge

Das Spektrum der Geräte, die an den Eingang einer Netzwerk-Kamera angeschlossen werden können, ist nahezu unbegrenzt. Die Grundregel ist, dass jedes Gerät, das im Stande ist, einen Schaltkreis zu öffnen oder zu schließen, an eine Netzwerk-Kamera oder einen Videoserver angeschlossen werden kann.

Beispiele für Alarmgeräte und ihre Verwendung

Gerätetyp	Beschreibung	Verwendung
Türkontakt	Einfacher Magnetschalter, der das Öffnen von Türen und Fenstern erkennt	Wenn der Schaltkreis geöffnet wird (Tür geht auf), kann die Kamera bewegte Videobilder und Benachrichtigungen versenden.
PIR (passive Infraroterkennung)	Sensor, der Bewegungen anhand von Wärmestrahlung erkennt	Wenn eine Bewegung erkannt wird, unterbricht die PIR den Schaltkreis. Die Kamera kann bewegte Videobilder und Benachrichtigungen versenden.
Glasbruchmelder	Aktiver Sensor, der den Luftdruck in einem Raum misst und plötzliche Druckabsenkungen erkennt (Stromversorgung durch Kamera möglich)	Wenn eine Luftdrucksenkung erkannt wird, unterbricht der Melder den Schaltkreis. Die Kamera kann bewegte Videobilder und Benachrichtigungen versenden.

Digitale Ausgänge

Der Ausgang dient hauptsächlich dazu, dass die Kamera externe Geräte starten kann – automatisch oder per Fernbedienung durch einen Bediener oder eine Anwendung.

Beispiele für Geräte, die man an den Ausgang anschließen kann

Gerätetyp	Beschreibung	Verwendung
Tür-Relais	Relais, das Öffnen und Schließen von Türschlössern kontrolliert	Das Verschließen/Aufschlienßen einer Eingangstür kann über das Netzwerk von einem entfernten Bediener gesteuert werden.
Sirene	Warnsirene, die bei erkannter Alarmsituation ausgelöst wird	Die Kamera kann die Sirene auslösen, wenn mittels des integrierten VMD eine Bewegung entdeckt wird order wenn entsprechende Daten am digitalen Eingang eingehen.
Alarm/Einbruchserkennung	Sicherheitswarnsystem, das einen normalerweise geschlossenen oder normalerweise offenen Alarmschaltkreis ständig überwacht	Die Kamera kann als integrierter Bestandteil des Alarmsystems dienen und die Aufgabe eines Sensor übernehmen. Sie kann zudem für eine ereignisgesteuerte Videoübertragung sorgen.

7.4. Integrierte Systeme

In einem Netzwerk-Videosystem sind alle Geräte mit einem IP-Netzwerk verbunden. Dadurch kann eine kostengünstige Infrastruktur zur Übertragung von Video für die Aufzeichnung oder Überwachung genutzt werden. Sie ermöglicht auch die Integration mit anderen Systemen. Auf diese Weise kann die Funktionalität ausgebaut und die Bedienung vereinfacht werden. Es können zum Beispiel die folgenden Systeme integriert werden:

- **Zutrittskontrolle:** Bei einem Video-Überwachungssystem mit integrierter Zutrittskontrolle kann zum Beispiel Video an allen Türen erfasst werden, wenn jemand eine Einrichtung betritt oder verlässt. Gleichzeitig besteht die Möglichkeit, dem Bediener des Video-Überwachungssystems alle Bilder im System bereitzustellen, so dass Mitarbeiter oder Besucher schnell identifiziert werden können.

- **Gebäudeverwaltungssysteme (BMS):** Video kann in Gebäudeverwaltungssysteme wie Heiz-, Belüftungs- und Klimaanlagen integriert werden. Die Ein/Ausgänge der Netzwerk-Kameras können zur Dateneingabe in das System genutzt werden; ebenso können die Kameras als Bewegungsmelder, z. B. in Konferenzräumen und zur Steuerung von Heizung oder Beleuchtung verwendet werden, um Energie zu sparen.

- **Industrielle Kontrollsysteme:** In komplexen automatisierten Industrieanlagen ist oft eine Sichtkontrolle vonnöten. Der Bediener muss das Steuerpult nicht mehr verlassen, um einen Teil der Abläufe in Augenschein zu nehmen, sondern kann die Sichtkontrolle an derselben Bedienoberfläche per Netzwerk-Video vornehmen. Auch bei sensiblen Vorgängen in hochreinen Räumen oder in Einrichtungen mit gefährlichen chemischen Stoffen ist die Video-Überwachung oft die einzige Möglichkeit zu einer Sichtkontrolle. Dies gilt auch für Energieverteilungssysteme mit Umspannwerken in sehr abgelegenen Gegenden.

Intelligente Videosysteme

Videoaufzeichnungen sind heute gang und gäbe, doch aufgrund von Zeitmangel wird nur ein Bruchteil des Materials analysiert. Daher arbeiten Experten intensiv an der Entwicklung von intelligenten Videoanwendungen (IV). Derzeit befinden sich neuartige IV-Systeme in der Entwicklung, mit denen Autokennzeichen erfasst, digitalisiert und mit einer Datenbank abgeglichen werden können. Andere Beispiele für IV-Anwendungen sind Personenzähler und Zugangsschranken. Intelligente Funktionen in Endgeräten bieten wesentliche Vorteile wie die Analyse von Rohdaten, einen geringeren Arbeitsaufwand und letztlich niedrigere Personalkosten. Die intelligente Netzwerk-Kamera ist stets aktiv. Sie hält ständig Wache und wartet auf einen Impuls, der die Aufzeichnung startet. Für die maßgeschneiderte Alarmkonfiguration bietet sich eine automatische Bewegungserkennung an, die an die spezifischen Umgebungs- und Ereignisbedingungen angepasst wird.

8.1 Was ist unter intelligentem Video zu verstehen?

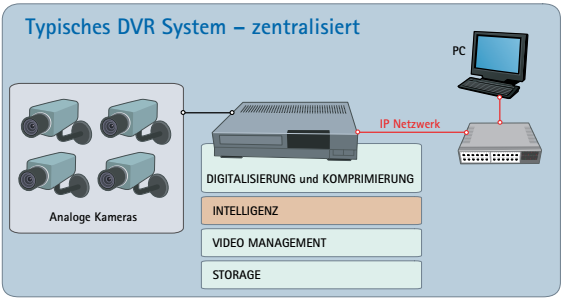
Beim intelligenten Video werden Video-Rohdaten so analysiert, dass ihnen klare Handlungsanweisungen entnommen werden können. Daher spielt die Überwachungsintelligenz bei der Qualität von Entscheidungsprozessen in zeitkritischen Situationen eine entscheidende Rolle. Es werden neue Geschäftsfelder wie die Personenzählung entstehen; *siehe hierzu Kapitel 8.3.1 auf Seite 75.*

8.2 Intelligente Videoarchitektur

8.2.1 DVRs und zentrale Analyse

Eine viel genutzte Möglichkeit zur Integration herkömmlicher CCTV-Systeme ist die direkte Übernahme von Videobildern aus den analogen Überwachungskameras in den IV-fähigen DVR. Der DVR übernimmt die intelligente Analyse (z. B. die Personenzählung oder die Verarbeitung von Autokennzeichen), digitalisiert, komprimiert und speichert dann die verbleibenden Daten, bevor er schließlich die generierten Alarmmeldungen und die Videoausgabe an die autorisierten Bediener weiterleitet.

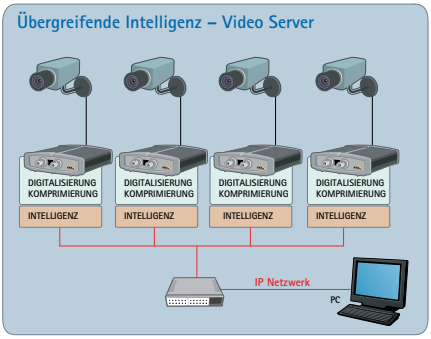
Dieser Ansatz eignet sich für Systeme mit ausreichender Kapazität für unkomprimierte Live-Videobilder, die an eine Zentrale übertragen werden. Er ist auch für Systeme mit konstanter Kamera-Anzahl denkbar, da DVRs nur Platz für eine bestimmte Anzahl an Kameras bieten und die einzelnen Einheiten sehr kostspielig sind.

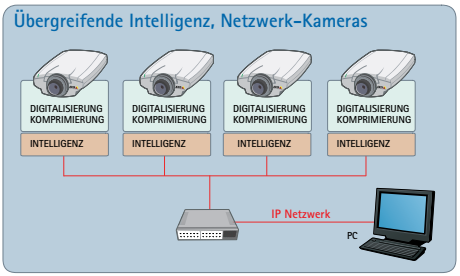


8.2.2 Netzwerk-Videosysteme und verteilte Intelligenz

Besser und leichter skalierbar als analog gestützte Systeme sind Videoserver, die lokal an Analogkameras angeschlossen werden, den Videodatenstrom bereits vor Ort analysieren, digitalisieren und komprimieren und dann erst über das Netzwerk zur Überwachung und Aufzeichnung weiterleiten.

Dieser Ansatz bietet mehrere Vorteile. Durch die lokale Digitalisierung und Komprimierung kann die bestehende Netzwerk-Infrastruktur zusammen mit dem Internet als kostengünstiges Übertragungssystem für intelligente Daten genutzt werden. So kann die Übertragung zum Beispiel auf Videodaten beschränkt werden, die durch eine Bewegungsmeldung aktiviert und zusammen mit einer Alarmmeldung an eine Überwachungszentrale weitergeleitet werden, die über die weiteren Schritte und Analysemaßnahmen entscheidet, möglicherweise gestützt auf intelligente Video-Anwendungen. Infrastruktur und Personal werden dadurch weitaus weniger stark in Anspruch genommen.

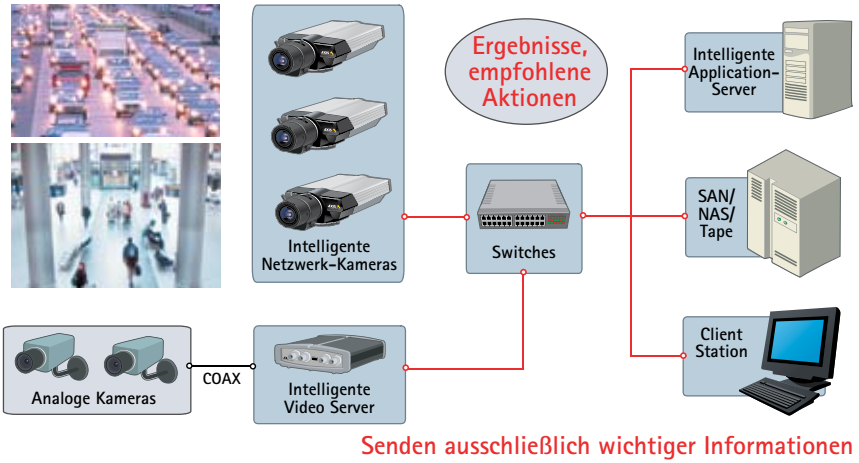




Bei einem verteilten Ansatz können intelligente Strukturen auf die spezialisierte Peripherie konzentriert werden, zum Beispiel auf die erwähnte Netzwerk-Kamera oder den Videoserver. Die Informationen können zum gegebenen Zeitpunkt an einen Zentralserver oder bestimmte Clients übertragen werden, die bestimmte Aktionen ausführen müssen.

Mit einer Basiskonfiguration können spezialisierte Strukturen genutzt werden, um Bediener anzuleiten, die mit einer bestimmten Aufgabe betreut sind. Zum Ausbau von professionellen Videosystemen lassen sich verschiedene Arten von verteilten IV-Anwendungen miteinander kombinieren. Die im Netzwerk verteilte Intelligenz bietet den Vorteil einer unbegrenzten Skalierbarkeit und somit Zukunftssicherheit im Baukastensystem.

8.3 Typische Anwendungen



8.3.1 Personenzählung

In Einzelhandelsgeschäften kann z. B. ein Netzwerk-Videosystem an allen drei Eingangstüren installiert werden.

Die Netzwerk-Videosysteme können mit einem Personenzähl-Modul bestückt werden, mit denen die eintretenden Kunden gezählt werden. Separate Geräte erzeugen Videobilder von den Kassen. Netzwerk-Kameras werden von erkannten Bewegungen ausgelöst und übertragen Videoströme an eine Zentraleinheit und einen IV-Operator, der Verweilzeiten analysiert. Ein hoher Personendurchsatz und lange Verweilzeiten sind Indikatoren für geschäftlichen Erfolg. Letztendlich helfen diese Informationen bei der Optimierung der Rentabilität.

Andere wichtige Fragen für den Einzelhandel wären: "Ab wann wirken sich Warteschlangen negativ auf die Kundenzufriedenheit aus? Wickelt eine Kasse den Kundenandrang schneller als erwartet ab? Kommen die Kunden mit der neuen Raumaufteilung zurecht?"

Netzwerk-Videosysteme können daher mehreren Zwecken dienen: der intelligenten Analyse des Kundenverhaltens, Steigerung des Umsatzes und der Rendite aufgrund der Zufriedenheit der Kunden durch die Analyse von Wartezeiten und der Beobachtung von Kundenreaktionen, so dass schnell mit der Öffnung weiterer Kassen reagiert werden kann, bevor es zu Unmutsreaktionen kommt.

8.3.2 Erkennung von Autokennzeichen

Intelligentes Parken ist eine erfolgreiche Anwendung der Kennzeichenerfassung. Es kann vorkommen, dass Kunden Dauerparkscheine verlieren und die Abrechnung anzweifeln. Die Ermittlung der richtigen Gebühr kosten Zeit und Energie. Das neue System bietet neben Monatsabrechnungen Parkbelege mit hoher Beweiskraft.

Ein weiteres Problem ist der Missbrauch von Parkplätzen für gestohlene Fahrzeuge, die der Dieb verbergen möchte, bis er sich vor Verfolgung sicher glaubt. Polizeidienststellen begrüßen die neuen intelligenten Torwächter, die Einfahrtszeiten festhalten und registrieren, welche Fahrzeuge in den einzelnen Parkbuchten abgestellt werden. Das Verbergen gestohlener Fahrzeuge wird in einer intelligenten Parkgarage ebenso unterbunden wie Manipulationen an abgestellten Pkws. Die IV-Anwendung dient somit mehreren Zwecken. Zu den Gewinnern zählen die Eigentümer der Fahrzeuge, Behörden und die Inhaber von überwachten Parkhäusern.

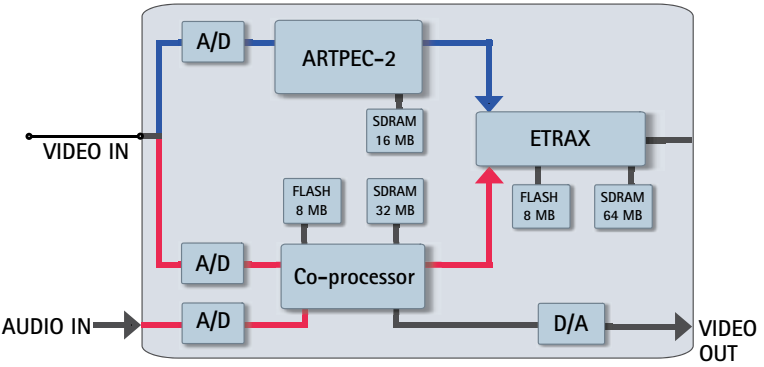
8.3.3 Zugangsschranken: Stolperdraht für Straftäter

Zugangsschranken helfen, Einbruchsversuche zu verhindern, auch wenn nur wenige Wachleute eingesetzt werden können. Durch die Schranken werden Laufwege auf eine bestimmte Richtung begrenzt. Mitarbeiter und Wachleute können das Gebäude zwar verlassen, aber ohne Rücksprache mit dem Alarmverwalter nicht mehr betreten.

Maßgeschneiderte Schranken bieten entscheidende Vorteile. Intelligente Videosysteme können die Überwachung so konfigurieren, dass Videodaten nur dann erfasst werden, wenn bestimmte Parameter erfüllt sind und auffällige Bewegungsabläufe erkannt wurden. Die Systeme können so konfiguriert werden, dass die erfassten Daten weitaus zielführender und aussagekräftiger sind.

8.4 Komponenten auf der Basis offener Standards

Zugunsten leistungsstarker, intelligenter Videoanwendungen werden Netzwerk-Videosysteme mit neuen Modulen ergänzt. Der AXIS 242S IV ist ein IV-fähiger Videoserver mit einer Schnittstelle, der mit einem DSP-Chip bestückt ist (Digital Signal Processing). Der Chip ist auf die Verarbeitung von Daten für IV-Anwendungen spezialisiert.



Offene Plattformen bilden ein Kernstück der kaufmännischen Strategie von Axis, da sie für ein attraktives Preis-Leistungsverhältnis und ein hohes Maß an Kompatibilität sorgen. Durch die offene Plattform profitieren Kunden von unserem Partnerprogramm, in dessen Rahmen modernste Software für die intelligente Analyse der Zukunft entwickelt wird.

Kurzanleitung: Checkliste für den Aufbau eines Netzwerk-Video Systems

1. Analoge Kamera/DVR oder Netzwerk-Kamera?

Im Laufe des letzten Jahres haben Netzwerk-Kameras gegenüber der Technologie von analogen Kameras deutlich aufgeholt und erfüllen nun die gleichen Anforderungen und Spezifikationen wie diese. Wie Sie im diesem Guide gesehen haben, übertreffen Netzwerk-Kameras die Leistung von analogen Kameras sogar in einigen wichtigen Bereichen. In diesem Kapitel sollen jedoch die zehn wichtigsten funktionalen Unterschiede zwischen modernen Netzwerk-Kameras und ihren überholten analogen Vettern erläutert werden, und warum ein Verständnis dieser Faktoren beim nächsten Kamerakauf eine wichtige Rolle spielt.

(1) Das Ende von Problemen bei der Zwischenzeilenabtastung

Analoge Kameras mit einer hohen Auflösung (4CIF) haben deutliche Probleme bei der Zwischenzeilenabtastung, es entstehen verschwommene, unklare Bilder. Eine Netzwerk-Kamera verwendet die Technologie der “progressiven Abtastung”, wodurch Objekte in Bewegung deutlicher abgebildet werden. Das gesamte Bild wird auf einmal erfasst, wodurch selbst bei sehr viel Bewegung kristallklare Bilder entstehen.

Erstes Feld: Ungerade Zeilen — Zweites Feld: Gerade Zeilen — Ein komplettes Bild bei Verwendung des Zeilensprungverfahrens

(2) Höhere Einsparungen und Zuverlässigkeit durch Power-over-Ethernet

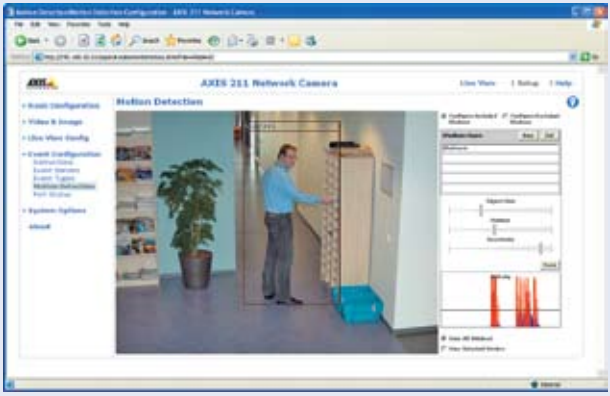
Bei der PoE-Technologie, die von analogen Kameras nicht genutzt werden kann, werden Netzwerkgeräte von einem PoE-fähigen Switch oder Midspan über dasselbe Kategorie-5-Standardkabel mit Strom versorgt, auf dem auch Daten und Videosignale übertragen werden. Da es sich hier um eine Norm handelt, sind alle Geräte zueinander kompatibel, wodurch wiederum alle Endbenutzer profitieren können. Für die Überwachung bietet PoE einen zusätzlichen Vorteil: Kameras können mit zentralem Notstrom von einem Serverraum aus versorgt werden, wodurch sie bei einem Stromausfall weiterhin einsatzbereit sind.

(3) Auflösungen im Megapixel-Bereich

Analoge Kameras sind an NTSC/PAL-Spezifikationen mit einer Auflösung gebunden, die bei 4CIF in etwa 0,4 Megapixel entspricht. Die höhere Auflösung einer Netzwerk-Kamera bietet mehr Detail und kann größere Bereiche erfassen.

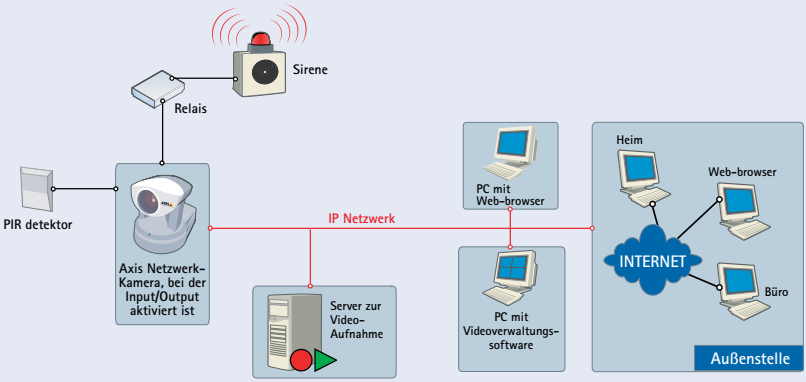
(4) Kameras mit eingebauter Intelligenz

Kameras mit eingebauter Intelligenz ermöglichen eine wesentlich produktivere und effektivere Überwachung, als dies mit einem DVR- oder einem anderem zentralen System machbar ist. Die Netzwerk-Kamera löst auch ein weiteres neuartiges Problem: den Mangel an Rechenleistung, um mehr als nur ein paar Kanäle in Echtzeit zu analysieren. Netzwerk-Kameras verfügen über spezielle hochintegrierte Hardwarekomponenten, die Aufgaben der Bildanalyse hervorragend lösen und somit die Installation von umfangreichen intelligenten Videosystemen ermöglichen.



(5) Integrierte PTZ-Technik und Eingabe-/Ausgabesteuerung

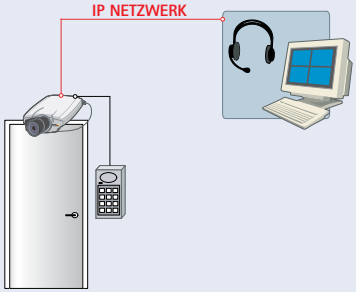
Bei analogen Kameras werden für die serielle Verbindung zur Steuerung der PTZ-Bewegung vom Videosignal getrennte Kabel benötigt. Dies ist teuer und umständlich. Die Technologie von Netzwerk-Kameras ermöglicht die PTZ-Steuerung über dasselbe Netzwerk, das auch die Videodaten transportiert. Zudem sind Netzwerk-Kameras in der Lage, Eingabe- und Ausgabesignale wie Alarme und Kontrollsperren zu integrieren. All dies bedeutet weniger Kabel, geringere Kosten und mehr Möglichkeiten in Bezug auf Funktionalität und Integration.



Beispiel: Typisches I/O Szenario – Einbindung mit Alarmfunktion

(6) Integrierte Audiodaten

Bei analogen Systemen ist kein Audio möglich, es sei denn, Sie legen separate Audioleitungen zum DVR. Netzwerk-Kameras lösen dieses Problem, indem Audiodaten von der Kamera aufgezeichnet, mit den Videodaten synchronisiert oder sogar in denselben Videostrom integriert werden.



Beispiel: Bedienung des Türöffners und der Sprechanlage durch Fernzugriff

(7) Sichere Übertragung

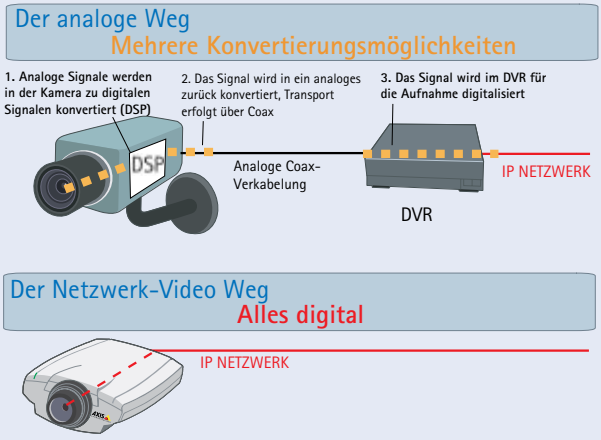
Bei einer analogen Kamera wird das Videosignal über ein Koaxialkabel ohne Verschlüsselung oder Authentifizierung übertragen. Bei einer Videoübertragung im Netzwerk kann die Kamera die Daten verschlüsseln, um so zu gewährleisten, dass sie nicht angezeigt oder manipuliert werden können. Das System kann auch zur Authentifizierung der Verbindung mit Hilfe verschlüsselter Zertifikate eingerichtet werden, die nur eine spezielle Netzwerk-Kamera akzeptieren, wodurch verhindert wird, dass sich irgendjemand in die Leitung hineinhackt. Die Netzwerk-Kamera ist auch in der Lage, verschlüsselte "Wasserzeichen" in den Videodatenstrom einzubinden, die zur Generierung einer Beweisspur Informationen zu Bild, Uhrzeit, Ort, Benutzer, Alarme und mehr enthalten.

(8) Flexible, wirtschaftliche Infrastrukturoptionen

Analoges Video wird in der Regel über teuere Koaxialkabel, über proprietäre Glasfaserleitungen oder drahtlos übertragen. Alles Verfahren, bei denen sich die Entfernung auf die Bildqualität auswirkt. Diese Situation wird durch Aspekte wie Stromversorgung, Ein-/Ausgänge und Audio weiter verkompliziert. Netzwerk-Videosysteme bewältigen diese Probleme mit wesentlich geringeren Kosten und bieten dazu eine Vielzahl weiterer Optionen. Die Netzwerk-Kamera erzeugt digitale Bilder, die keinen entfernungsbedingten Qualitätsverlust aufweisen. Weil IP-basierte Netze eine etablierte und standardisierte Technologie nutzen, fallen vergleichsweise niedrige Kosten an. Im Gegensatz zu analogen Systemen können IP-basierte Videoströme um die ganze Welt geleitet werden, wobei eine Vielfalt von kompatiblen Infrastrukturen genutzt werden.

(9) Vollwertige Digitallösung

Der CCD-Sensor in einer analogen Kamera generiert ein analoges Signal, das von einem A/D-Wandler digitalisiert wird, um die Bildverbesserung in einem DSP zu ermöglichen. Das Signal wird dann für den Transport über ein Koaxialkabel wieder zurück in ein Analogsignal konvertiert. Schließlich wird das Signal vom DVR erneut für die Aufzeichnung digitalisiert. Das sind insgesamt drei Konvertierungen, die jedes Mal mit einem Verlust der Bildqualität verbunden sind. Bei einem System mit Netzwerk-Kameras werden Bilder einmal digitalisiert und verbleiben dauerhaft im Digitalformat – keine unnötigen Konvertierungen und keine Bildverschlechterung.



(10) Geringere Gesamtbetriebskosten

Es ist naheliegend, dass alle diese anspruchsvollen Funktionen, die hier beschrieben wurden, ihren Preis haben. So können die Anschaffungskosten für eine Netzwerk-Kamera tatsächlich höher sein, falls man nur den Kamerapreis vergleicht. Vergleicht man aber die Kosten pro Kanal, ist die Netzwerk-Kamera mit allen ihren Vorteilen in punkto Flexibilität und Leistung schnell mit einem analogen System auf Basis eines DVR vergleichbar. Bei vielen Systemkonfigurationen sind die Anschaffungskosten für ein mit Netzwerk-Kameras ausgestatteten Überwachungssystem sogar niedriger als bei analogen Optionen. Diese niedrigeren Kosten für das Netzwerk-Kamerasystem sind hauptsächlich darauf zurückzuführen, dass Back-End-Anwendungen und Speichersysteme auf der Industrienorm entsprechenden Servern auf Basis von offenen Systemen lauffähig sind, und nicht auf proprietärer Hardware wie einem DVR. Dadurch werden Verwaltungs- und Gerätekosten radikal reduziert, vor allem bei größeren Systemen, bei denen Speichersysteme und Server einen wesentlichen Teil der Gesamtkosten einer Lösung darstellen. Zusätzliche Kosteneinsparungen leiten sich von der verwendeten Infrastruktur ab. IP-basierte Netzwerke wie das Internet, LANs sowie verschiedene Verbindungsmethoden wie die Drahtlostechnik lassen sich für andere Anwendungen im gesamten Unternehmen nutzen und sind wesentlich günstigere Alternativen als traditionelle Koaxial- und Glasfaserverbindungen. Somit wären die letzten möglichen Einwände gegen Netzwerk-Kameras vollständig beseitigt.

2. Auswahl einer Netzwerk-Kamera: Die wichtigsten Kriterien

Immer mehr Anbieter betreten den Netzwerk-Video Markt. Es ist also eine immer größere Anzahl an Optionen verfügbar, die mit einer Menge häufig verwirrender oder widersprüchlicher Informationen einhergehen. Wie treffen Sie eine kluge, fundierte Entscheidung, wenn Sie den Kauf einer Netzwerk-Kamera planen?

In den folgenden Richtlinien werden zehn wichtige Kriterien beschrieben, die Sie berücksichtigen sollten, wenn Sie zu der zunehmenden Gruppe von Endnutzern gehören möchten, die Netzwerk-Kameras zum Bestandteil ihrer Sicherheitstechnologie machen.

(1) Hohe Bildqualität

Wenn Sie die Bildqualität einer Netzwerk-Kamera bewerten, untersuchen Sie die folgenden Fragen: Wie hoch ist die Lichtempfindlichkeit? Grad der Bildschärfe? Verfügt sie über ein hochwertiges Objektiv? Wie ist die Bildqualität bei Bewegung im Bild? Das Datenblatt enthält wertvolle Informationen. Testen Sie jedoch einige der in Betracht gezogenen Kameras in der Praxis, um die Datenblattinformationen anhand Ihrer speziellen Anwendung besser beurteilen zu können.

(2) Teil eines umfangreichen Sortiments

Wählen Sie Anbieter, die ein umfassendes Sortiment, einschließlich unbeweglicher Kameras, Festkuppelkameras und PTZ-Kuppel-Kameras, führen. Auf diese Weise können ein oder zwei Firmen Ihren Anforderungen jetzt und in der Zukunft gerecht werden, wenn Sie Ihre Anwendung erweitern und die Funktionalität auf den Megapixel-Bereich, Drahtlos-Funktionalität und/oder Audiokommunikation nachrüsten möchten. Wenn Sie analoge Kameras nachrüsten möchten, sollte die Produktpalette Ihres Herstellers auch Videoserver (Encoder), Videodecoder, Gehäuse und weitere entsprechende Geräte umfassen.

(3) Umfassender Anwendungssupport und einfache Integration

Ist die von Ihnen benötigte Netzwerk-Kamera Teil eines geschlossenen Systems, das als Videoverwaltungssoftware nur wenige Softwareanwendungen oder vielleicht nur eine einzige Anwendung zulässt? Wählen Sie eine Netzwerk-Kamera, die über offene Schnittstellen (API bzw. Application Programming Interface) verfügt und für die mehrere Softwareanwendungen zur Auswahl verfügbar sind. Bestimmte führende Unternehmen bieten Hunderte solcher Kombinationen an. Die Anzahl der verfügbaren Optionen oder Funktionen sollte niemals durch Ihre Netzwerk-Kamera begrenzt werden. Offene, herstellerneutrale Systeme sind langfristig immer die überlegene Lösung.

(4) Komprimierung vollständig mit den Standards JPEG und MPEG-4 kompatibel

Stellen Sie sicher, dass die Kamera vollständig mit den Standards JPEG und MPEG-4 kompatibel ist. Viele Hersteller, die Kompatibilität mit einem Standard angeben, halten den Standard dennoch nicht 100-prozentig ein. Eine Kompatibilität von 99 Prozent ist so gut wie keine Kompatibilität. Die vollständige Kompatibilität gewährleistet den flexiblen Einsatz von Video für viele unterschiedliche Anwendungen. Sie stellt außerdem sicher, dass Sie das Video auch noch in zehn Jahren oder später abspielen können. Wenn ein Anbieter den MPEG-4-Standard nutzt, erkundigen Sie sich außerdem, ob die Lizenzgebühren beglichen sind und wie viele Lizenzen im Lieferumfang eines einzelnen Produkts enthalten sind. Wenn der Anbieter keine Gebühren bezahlt hat, entspricht die Komprimierung nicht dem Standard oder Sie müssen nach dem Kauf des Produkts Lizenzen bezahlen.

(5) Programme für die Verwaltung umfangreicher Bereitstellungen

Netzwerk-Kameras verfügen wie alle intelligenten Netzwerkgeräte über eine IP-Adresse und integrierte Firmware. Viele Anbieter stellen Upgrades gratis zur Verfügung. Beim Kauf müssen Sie die Kosten für die Einrichtung von IP-Adressen und eines Updates aller Kameras in der Installation berücksichtigen. Der Hersteller der Netzwerk-Kamera sollte Programme zum Verwalten dieser Prozesse anbieten und seine Angaben zu Kosten und Ausfallzeiten sollten eindeutig und im Voraus messbar sein. Die Programme des Herstellers sollten auch in der Lage sein, die Standorte aller Netzwerk-Videogeräte automatisch zu bestimmen und den Status dieser Geräte zu überwachen.

(6) Umfassende Netzwerkfunktionen und -sicherheit

Die Bildqualität ist ein wesentliches Kriterium, doch besitzen die Netzwerkfunktionen einer Kamera einen vergleichbaren Stellenwert. Ein Ethernet-Anschluss mit einer IP-Adresse ist nur eine Grundfunktion, über die alle Netzwerk-Kameras verfügen. Sie müssen weitere Faktoren berücksichtigen: Ist DHCP verfügbar, ein von vielen Organisationen verwendetes Protokoll zum Verwalten von IP-Adressen? Wird außerdem Sicherheit in Form von Verschlüsselung oder HTTPS geboten? Ein wichtiger Lackmustest ist außerdem die Einstellung Ihrer IT-Abteilung. Sind die Mitarbeiter der IT-Abteilung mit dem Einsatz einer bestimmten Netzwerk-Kamera im Netzwerk zufrieden? Sie sind die Experten und können bestimmen, ob die Funktionen der Kamera und die von ihr gebotene Sicherheit ausreichend sind.

(7) Bildsensor mit progressiver Abtastung

Progressive Abtastung ist eine Funktion, über die nur Netzwerk-Kameras verfügen. Doch nicht alle Netzwerk-Kameras können mit dieser Funktion aufwarten. Mit progressiver Abtastung werden durchwegs die besten Ergebnisse in Bezug auf Bildschärfe und Erkennbarkeit wichtiger Details erzielt. Frage: Warum ist beim Drücken der Pause-Taste die Bildqualität bei einer DVD besser als bei einem Videoband? Richtig: Die Ursache ist progressive Abtastung.

(8) Power-over-Ethernet (PoE)

Dieses Thema erscheint vielleicht als ein unwichtiger Punkt in der Kriterienliste, doch betrachten Sie ihn aus folgender Perspektive: Möchten Sie nicht hunderte von Euros pro Kamera sparen? Dies sind etwa die Kosten für die Installation der Stromversorgung eines einzelnen Kamerastandorts. Selbst für eine Installation mit 50 oder 100 Kameras ist dies eine beträchtliche Einsparung. Für Endkunden mit Hunderten von Kameras stellt dies eine Menge Geld dar. Stellen Sie sicher, dass die Power-over-Ethernet-Funktion der Kamera dem Standard IEEE 802.3af entspricht. Dies gibt Ihnen die Möglichkeit, eine Auswahl aus einer umfangreichen Palette von Netzwerk-Switches von Firmen wie Cisco, Nortel, Netgear usw. zu treffen.

(9) Verteilte Intelligenz

Intelligentes Video ist inzwischen ein Modewort. Die Technologie wird in den nächsten Jahren weiterentwickelt und immens verbessert werden, doch ist sie nur skalierbar, wenn sich die intelligenten Funktionen in der Kamera befinden. Der Grund dafür ist, dass Videointelligenz umfangreiche Verarbeitungskapazität erfordert. Wenn die Kamera diese Leistung nicht aufbringen kann, überlasten einige wenige Kameras sehr schnell die PC-Server. Wenn sich die intelligenten Funktionen in einem Endgerät wie der Kamera befinden, kann die Kamera entscheiden, wann die Videodaten gesendet und somit verarbeitet werden.

(10) Hintergrund und Schwerpunkt des Anbieters

Wie bereits erläutert, sollte bei Entscheidungen zum Kauf von Netzwerk-Kameras zukünftiges Wachstum und die Notwendigkeit weiterer Merkmale und Funktionen vorausgesetzt werden. Aus diesem Grund wird Ihr Netzwerk-Kamera-Hersteller ein Partner für lange Zeit sein.

Berücksichtigen Sie folgende Aspekte:
Über welches Sortiment an Netzwerk-Kameras und anderen Netzwerkprodukten verfügt der Hersteller? Erwirtschaftet die Firma Gewinn? Ist die Netzwerk-Kamera-Technologie der Schwerpunkt des Unternehmens oder stellen Netzwerk-Kameras nur eine Produktsparte dar? Gibt es eine lokale Niederlassung und Support vor Ort? Ist das Unternehmen global tätig und kann es seine Leistungen in mehreren Sprachen anbieten? Gibt es Referenzinstallationen? Wählen Sie eine Kamera von einem Marktführer, um sicherzustellen, dass Innovationen, Support, Nachrüstungen und Produktpfad langfristig verfügbar sind. Setzen Sie nicht die zukünftige Sicherheit aufs Spiel, nur um vorläufig einen geringen Betrag einzusparen.

3. Richtlinien für den Aufbau Ihres Netzwerk-Video Projektes

(1) Legen Sie die Szenerie und den Typ der gewünschten Netzwerk-Videoprodukte fest

- **Szenerie: Welche Umgebung soll überwacht werden? Welche Priorität messen Sie ihr bei?**
  Dadurch können Sie die Merkmale bestimmen, die Sie für Ihre Netzwerk-Kamera benötigen, wie Videoqualität, Lichtempfindlichkeit und Objektivtyp.

- **Lichtbedingungen: Benötigte Empfindlichkeit für Innen- oder Außenanwendung**
  Axis bietet nicht nur Netzwerk-Kameras für Innenräume an, sondern auch Modelle, die für Innen- und Außenbereich geeignet sind. Innen-/Außenbereichskameras verfügen über ein Variofokusobjektiv mit automatischer Blendeneinstellung. Tages- und Nachtkameras, die tagsüber Farbaufnahmen und nachts Schwarzweißbilder erzeugen, sind ebenfalls erhältlich. Überprüfen Sie die Details zur Lichtempfindlichkeit der Netzwerk-Kamera in Innen- und Außenumgebungen. Die Lichtbedingungen werden in “Lux” gemessen.

- **Abstand zwischen Kameraposition und dem Überwachungsziel**
  Hierdurch werden Kamera- und Objektivtyp festgelegt (normal, Tele, Weitwinkel), aber auch die Positionierung der Kamera(s). Einige Axis Netzwerk-Kameras sind mit Wechselobjektiven ausgestattet.

- **Benötigter Sichtwinkel: breit, eng, umfassende oder detaillierte Abdeckung (Legen Sie die Größe des sichtbaren Szeneriebereichs fest)**
  Netzwerk-Kameras werden mit festem Winkel und Fokus oder als variable, ferngesteuerte PTZ-Modelle (zum Neigen, Schwenken und Zoomen) geliefert, die einen größeren Bereich abdecken können.

- **Hohe oder niedrige Netzauslastung**
  Je höher die Netzwerkauslastung ist, desto mehr Kameras werden möglicherweise benötigt.

(2) Bestimmen Sie Ihre Anforderungen: Merkmale, Aufzeichnungs- und Speicherbedarf

- **Anwendung**
  Einfache Fernüberwachung, intelligentes Sicherheits-überwachungssystem mit erweiterter Ereignisverwaltung, Eingangs-/Ausgangsauslösern, Audiokomponente?

- **Anforderungen für Aufzeichnung und Live-Überwachung**
  Legen Sie fest, wann und wie oft Live-Bilder überwacht und aufgezeichnet werden sollen: am Tage, bei Nacht und/oder an den Wochenenden? Legen Sie die Anforderungen für jede Szenerie fest.

- **Berechnen Sie den Speicherbedarf**

- **Berechnen Sie die erforderliche Bandbreite**

(3) Legen Sie die Netzwerkanforderungen fest (LAN/WAN, drahtlos)

- **Netzwerkauslastung des bestehenden LAN: Wofür wird es bei Ihnen/bei Ihrem Unternehmen eingesetzt?**
- **Netzwerkauslastung bestehender WAN-Verbindungen**
- **Bestimmen Sie das Auslastungsmuster für einen gegebenen Zeitraum**
- **Müssen Sie das Netzwerk mit Zusatzkomponenten ausstatten (z.B. mit Switches) oder können Sie die vorhandene Infrastruktur /Gerätekonfiguration unverändert nutzen?**
- **Müssen Sie Verbindungen bei weiteren Providern anmieten, um einen Redundanzschutz zu gewährleisten?**
- **Wird ein verteilter Speicher benötigt?**

10 wichtigsten Fragen

- Sind derzeit analoge Kameras installiert?
- Sollen weitere Kameras hinzugefügt werden?
- Wie viele Kameras sollen insgesamt installiert werden?
- Sind Sie mit der Kostenstruktur eines IP-basierenden Systems vertraut?
- Sind Strom-Anschlussdosen bei den Kamerainstallationen vorgesehen?
- Werden Kameras für die Fernüberwachung benötigt?
- Arbeiten IT und Sicherheit zusammen?
- Arbeitet Ihre IT-Abteilung mit einer standardisierten IT-Plattform?
- Bietet Ihre IT-Abteilung einen 24x7 Support an?
- Trifft Ihre IT-Abteilung auch Einkaufs-Entscheidungen?

4. Kostenlose Projekttools

Axis Netzwerk-Videodesign-Tool-CD: A variety of tools that will help you design your network video project

Diese neue CD führt Sie durch die Faktoren und Einstellungen, die für eine erfolgreiche Installation von Netzwerk-Videoprodukten berücksichtigt werden sollten. Sie enthält einen Kalkulator für die Linse, eine Bilder- und Video-Gallerie sowie das neue AXIS Design Tool, einen simulationsgestützten Rechner, mit dem Sie die Bandbreite und den Speicherbedarf Ihres eigenen Netzwerk-Videoprojekts bestimmen können.

Mehrsprachiges Format: Deutsch, Englisch, Französisch, Niederländisch, Spanisch und Italienisch.

Sichern Sie sich Ihr persönliches Exemplar unter *www.axis.com/free_cd*

Netzwerk-Video beim Technologieführer erlernen

Die Zeiten ändern sich schnell! Bringen Sie Ihre Kenntnisse über Netzwerk-Video auf den neuesten Stand. Axis Communications' Academy hilft Ihnen dabei.

Die Einrichtung eines neuen Netzwerk-Videosystems, aber auch der Übergang von der vorhandenen analogen Überwachung zu einem vernetzten System erfordert einige wohlüberlegte Entscheidungen. Technische Handbücher und Anleitungen sind kein Ersatz für angeregte Gespräche mit Experten, betreute Kurse und praktische Übungen. Genau das erwartet Sie bei einem Kurs an der Academy. Bei der Video-Überwachung schreitet die Entwicklung neuer Technologien und Lösungen im Eilschritt voran. Die Academy ist eine gute Möglichkeit, auf dem Laufenden zu bleiben und sich über aktuelle Entwicklungen zu informieren. Hier erhalten Sie wertvolle Tipps und profitieren von der langjährigen Erfahrung des Technologieführers.

Seminare und Übungen zu verschiedenen Themen der Netzwerk-Videotechnologie
Ihren Anfang nahm die Netzwerk-Videotechnologie bei Axis. 1996 haben wir die erste Netzwerk-Kamera entwickelt und auf den Markt gebracht. Noch heute sind wir Technologieführer auf einem inzwischen bedeutenden Markt moderner Netzwerk-Videosysteme, die analoge Systeme immer weiter verdrängen. Die Academy setzt die viel versprechenden Perspektiven in Seminaren und praktischen Übungen um, die die unterschiedlichen Vorkenntnisse der Teilnehmer berücksichtigen. Es werden die verschiedensten Themen wie Kamera-Optik, verdeckte Video-Überwachung, beste Praktiken für das Netzwerk-Design und Kriterien für die Kamera-Wahl abgedeckt. Wir untersuchen die Stärken und Schwächen unterschiedlicher Installations-Szenarios. Die Diskussionen richten sich ganz an den Bedürfnissen der Teilnehmer aus, ganz gleich, ob sie Netzwerk-Videosysteme planen, vertreiben, warten, integrieren oder bedienen. Durch den interaktiven, dynamischen Austausch von Erfahrungen können optimierte Systemstrategien ausgearbeitet werden.

Melden Sie sich heute an der Academy an und erfahren Sie jetzt schon, was die Zukunft bringen wird.
Kurse an der Academy sind eine Investition, die sich gleich dreifach auszahlt: zeitlich, finanziell und für Ihr Nervenkostüm. Sie erfahren, wie Sie Netzwerk-Videolösungen für Sicherheitsüberwachungen und für die Fernüberwachung optimal einsetzen. Auch bei künftigen technologischen Entwicklungen und veränderten Systemanforderungen bleiben Sie am Ball: die Academy ist eine verlässliche Anlaufstelle, mit der Sie auf dem neuesten Stand bleiben, damit Ihnen künftige Möglichkeiten nicht entgehen.

Ihren Platz in einem Kurs an der Academy reservieren Sie ganz einfach bei Ihrer nächstgelegenen Axis-Niederlassung. Dort können Sie auch gerne weitere Informationen anfordern.

Anmerkungen

Anmerkungen

Kontaktinformationen

www.axis.com/request

FIRMENZENTRALE SCHWEDEN

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

AUSTRALIEN

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

CHINA

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

DEUTSCHLAND, ÖSTERREICH, DIE SCHWEIZ

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

FRANKREICH, BELGIEN, LUXEMBURG

Paris
Axis Communications S.A.
7-9 avenue Aristide Briand
94230 Cachan
Tel: +33 1 49 69 15 50
Fax: +33 1 49 69 15 59
Support:
Tel: +33 1 49 69 15 50

GROßBRITANNIEN

Hertfordshire
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:
Tel: +44 871 200 2071

HONG KONG

Hong Kong
Axis Communications Limited
21/F, ICBC Tower
Citibank Plaza 3 Garden Road
Central
Hong Kong
Tel: +852 2273 5163
Fax: +852 2273 5999

INDIEN

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

ITALIEN

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

JAPAN

Tokyo
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

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:
Tel: 800 444 2947

KOREA

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

MEXIKO

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

NIEDERLANDE

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

SINGAPUR

Singapore
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

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

SÜDAFRIKA

Johannesburg
Axis Communications SA Pty Ltd.
Hampton Park, Atterbury House, 20 Georgian Crescent
Bryanston
PO Box 70939
Bryanston 2021
Tel: +27 11 548 6780
Fax: +27 11 548 6799

TAIWAN

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

USA

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

VERENIGDE ARABISCHE EMIRATEN

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

www.axis.com

31470De/R1/0803

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 an der OMX Nordic Exchange, Large Cap, Information Technology notiert. Das Unternehmen ist weltweit mit Niederlassungen in 18 Ländern tätig und arbeitet mit Vertriebspartnern und Systemintegratoren in 70 Ländern zusammen. Weitere Informationen über Axis finden Sie unter www.axis.com

©2008 Axis Communications AB. AXIS COMMUNICATIONS, AXIS, ETRAX, ARTPEC und VAPIX sind eingetragene sowie in verschiedenen Gerichtsbezirken beantragte Marken von Axis. Alle weiteren Firmen und Produktnamen sind Marken oder eingetragene Marken der jeweiligen Firmen. Wir behalten uns das Recht vor, Änderungen ohne vorherige Ankündigungen vorzunehmen.

AXIS® COMMUNICATIONS