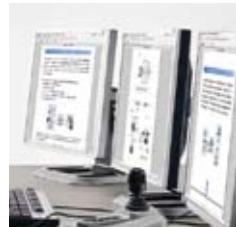


Technische gids over netwerkvideo.

Technologieën en factoren om te overwegen voor een geslaagde inzet van op IP gebaseerd beveiligingstoezicht en toepassingen voor controle op afstand.



Welkom bij de technische gids over netwerkvideo van Axis

Het overschakelen naar open videosystemen, in combinatie met de voordelen van netwerken, digitale beeldverwerking en camera-intelligentie, betekent een veel effectievere methode voor beveiligingstoezicht en controle op afstand dan in het verleden ooit mogelijk is geweest. Netwerkvideo biedt alle voordelen van analoge video, met daarbij een breed scala aan innovatieve functies en eigenschappen die alleen met digitale technologie mogelijk zijn.

Voordat u uw eigen systeem gaat installeren, moet u bedenken welke functies vereist zijn. Even belangrijke overwegingen zijn prestaties, interoperabiliteit, schaalbaarheid, flexibiliteit en toekomstbestendige functionaliteit. In deze gids komen stap voor stap al deze factoren aan de orde waardoor u wordt geholpen om tot een oplossing te komen die optimaal gebruik maakt van alles wat netwerkvideotechnologie u te bieden heeft.

Het beste in netwerkvideo

Axis is de wereldmarktleider op het gebied van netwerkvideo. We waren de eersten die de voordelen van netwerkvideotechnologie toepasten op professionele videobeveiliging en bewaking op afstand toen we in 1996 met de eerste netwerkcamera ter wereld kwamen. Met meer dan twintig jaar ervaring in netwerktechnologieën, het grootste aantal geïnstalleerde netwerkvideoproducten en sterke samenwerkingsverbanden met marktleiders over de hele wereld, is Axis de uitgelezen partner op het gebied van netwerkvideo.

Flexibele en schaalbare oplossingen

Axis gebruikt open technologiestandaards voor eenvoudige integratie en schaalbaarheid en biedt een volledig assortiment netwerkvideo-oplossingen voor toepassingen voor beveiliging en bewaking op afstand in veel verschillende industrietakken. Ons uiterst geavanceerde assortiment omvat netwerkcamera's die nieuwe functionaliteit toevoegen aan de categorie die ze vertegenwoordigen en videoservers/encoders waarmee een voordelige overstap naar het beste op het gebied van netwerkvideotechnologie mogelijk wordt gemaakt. We bieden ook uitgebreide software-oplossingen voor videobeheer en een volledige reeks accessoires.



Inhoudsopgave

Netwerkvideo: overzicht, voordelen en toepassingen 7

1.1 Overzicht van een netwerkvideosysteem	7
1.2 Voordelen	8
1.3 Toepassingen	12
1.3.1 Detailhandel	12
1.3.2 Transport	12
1.3.3 Onderwijs	13
1.3.4 Industrie	13
1.3.5 Stadsbewaking	13
1.3.6 Overheid	13
1.3.7 Zorginstellingen	14
1.3.8 Bank- en geldwezen	14

Netwerkcamera's 15

2.1 Wat is een netwerkcamera?	15
2.2 Typen netwerkcamera's	16
2.2.1 Vaste netwerkcamera's	17
2.2.2 Vaste domenetwerkcamera's	17
2.2.3 PTZ-camera's en PTZ-domecamera's	18
2.3 Netwerkcamera's voor dag en nacht	21
2.4 Megapixelnetwerkcamera's	23
2.5 Richtlijnen voor het kiezen van een netwerkcamera	24

Camera-elementen 27

3.1 Lichtgevoeligheid	27
3.2 Lenselementen	28
3.2.1 Beeldveld	28
3.2.2 Passende lens en sensor	30
3.2.3 Standaarden voor lensmontage	31
3.2.4 F-getal en belichting	31
3.2.5 Handmatige of automatische iris	32
3.2.6 Scherptediepte	33
3.3 Beeldsensors	34
3.3.1 CCD-technologie	34
3.3.2 CMOS-technologie	34
3.3.3 Megapixelsensors	35
3.4 Beeldscantechnieken	35
3.4.1 Geïnterlineerd scannen	35
3.4.2 Progressief scannen	36
3.5 Beeldverwerking	37
3.5.1 Achtergrondcompensatie	37
3.5.2 Belichtingszones	37
3.5.3 Breed dynamisch bereik	37
3.6 Een netwerkcamera installeren	38

Camerabescherming en -behuizingen	39
4.1 Cameraomhulsels in het algemeen	39
4.2 Doorzichtige afschermkap	40
4.3 Een vaste camera in een behuizing plaatsen	40
4.4 Omgevingsbescherming	41
4.5 Bescherming tegen vandalisme en sabotage	41
4.5.1 Camera/behuizingsontwerp	41
4.5.2 Montage	42
4.5.3 Plaatsing van de camera	43
4.5.4 Intelligentie video	43
4.6 Montagetypen	43
4.6.1 Plafondmontages	43
4.6.2 Wandmontages	44
4.6.3 Paalmontages	44
4.6.4 Relingmontages	44
Video-encoders	45
5.1 Wat is een video-encoder?	45
5.1.1 Componenten van de video-encoder en overwegingen	46
5.1.2 Gebeurtenisbeheer en intelligente video	47
5.2 Zelfstandige video-encoders	47
5.3 In rekken gemonteerde video-encoders	48
5.4 Video-encoders met PTZ- en PTZ-dome-camera's	48
5.5 Deïnterlinieringstechnieken	49
5.6 Videodecoder	50
Resoluties	51
6.1 NTSC- en PAL-resoluties	51
6.2 VGA-resoluties	52
6.3 Megapixelresoluties	53
6.4 HDTV-resoluties (High-definition television)	54
Videocompressie	55
7.1 Basisprincipes van de compressie	55
7.1.1 Videocodec	55
7.1.2 Beeldcompressie tegenover videocompressie	56
7.2 Compressie-indelingen	59
7.2.1 Motion JPEG	59
7.2.2 MPEG-4	60
7.2.3 H.264 of MPEG-4 Part 10/AVC	60
7.3 Variabele en constante bitsnelheden	61
7.4 Standaarden vergelijken	61
Audio	63
8.1 Audiotoepassingen	63
8.2 Audio-ondersteuning en apparatuur	64
8.3 Audiomodi	65
8.3.1 Simplex	65
8.3.2 Half-duplex	66

8.3.3	Full-duplex	66
8.4	Audiodetectie-alarm	66
8.5	Audiocompressie	66
8.5.1	Samplingfrequentie	67
8.5.2	Bitsnelheid	67
8.5.3	Audiocodecs	67
8.6	Audio- en videosynchronisatie	67
Netwerktechnologieën		69
9.1	LAN-netwerk en Ethernet	69
9.1.1	Typen Ethernet-netwerken	70
9.1.2.	Switch	71
9.1.3	PoE (Power over Ethernet)	73
9.2	Internet	75
9.2.1	IP-adressering	76
9.2.2	Datatransportprotocollen voor netwerkvideo	80
9.3	VLAN's	82
9.4	Servicekwaliteit (QoS)	82
9.5	Netwerkbeveiliging	84
9.5.1	Gebruikersnaam- en wachtwoordverificatie	84
9.5.2	IP-adresfiltering	84
9.5.3	IEEE 802.1X	84
9.5.4	HTTPS of SSL/TLS	85
9.5.5	VPN (Virtueel particulier netwerk)	85
Draadloze technologieën		87
10.1	WLAN-standaarden 10.1 802.11	88
10.2	Beveiliging van WLAN	88
10.2.1	WEP (Wired Equivalent Privacy)	89
10.2.2	WPA/WPA2 (WiFi Protected Access)	89
10.2.3	Aanbevelingen	89
10.3	Draadloze bruggen	89
Videobeheersystemen		91
11.1	Hardwareplatforms	91
11.1.1	Pc-serverplatform	91
11.1.2	NVR-platform	92
11.2	Softwareplatforms	93
11.2.1	Ingebouwde functionaliteit	93
11.2.2	Windows-clientsoftware	93
11.2.3	Software op internet	94
11.2.4	Schaalbaarheid van videobeheersoftware	94
11.2.5	Open software versus leveranciersspecifieke software	94
11.3	Systeemfuncties	94
11.3.1	Weergave	95
11.3.2	Multistreaming	95
11.3.3	Video-opname	96
11.3.4	Opname en opslag	97
11.3.5	Gebeurtenisbeheer en intelligente video	97

6 INHOUDSOPGAVE

11.3.6 Functies voor administratie en beheer	102
11.3.7 Beveiliging	103
11.4 Geïntegreerde systemen	104
11.4.1 Application Programming Interface (API)	104
11.4.2 Verkooppunten (POS)	104
11.4.3 Toegangscontrole	105
11.4.4 Gebouwbeheer	105
11.4.5 Industriële regelsystemen	106
11.4.6 RFID	106
Overwegingen voor bandbreedte en opslag	107
12.1 Berekeningen voor bandbreedte en opslag	107
12.1.1 Bandbreedtevereisten	107
12.1.2 Het berekenen van de opslagbehoefte	108
12.2 Opslag op de server	110
12.3 NAS en SAN	110
12.4 Redundante opslag	112
12.5 Systeemconfiguraties	113
Hulpmiddelen	115
Axis Communications' Academy	117
Contactgegevens	118

Netwerkvideo: overzicht, voordelen en toepassingen

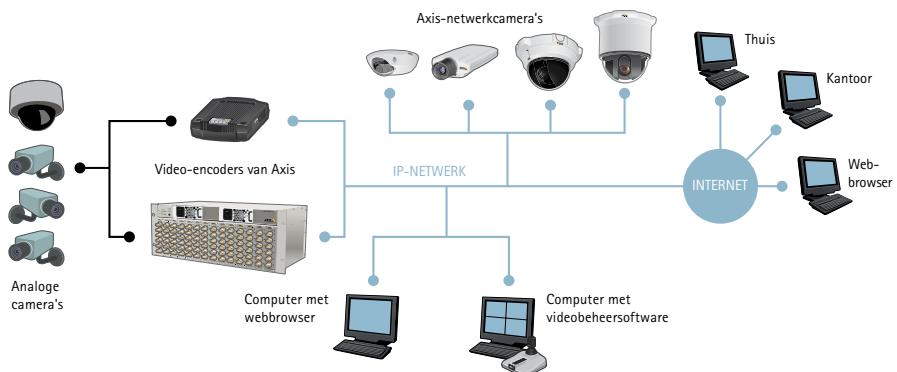
Netwerkvideo wordt, net als andere soorten communicatie zoals e-mail, webservices en computertelefonie, via bedrade of draadloze IP-netwerken uitgevoerd. Digitale video- en audiostreams en overige gegevens worden via dezelfde netwerkinfrastructuur gecommuniceerd. Netwerkvideo biedt gebruikers, vooral in de markt voor beveiligings-toezicht, veel voordelen ten opzichte van traditionele analoge CCTV-systemen (closed-circuit television).

In dit hoofdstuk wordt een overzicht gegeven van netwerkvideo, de voordelen en de toepassingen ervan in verschillende bedrijfstakken. Er worden vaak vergelijkingen met een analoog videosurveillance-systeem gemaakt om een beter begrip van de reikwijdte en de mogelijkheden van een digitaal netwerkvideosysteem te krijgen.

1.1 Overzicht van een netwerkvideosysteem

Netwerkvideo, dat ook wel op IP gebaseerde videosurveillance of IP-surveillance wordt genoemd bij toepassing in de beveiligingsindustrie, maakt gebruik van een bedraad of draadloos IP-netwerk als backbone voor de overdracht van digitale video, audio en andere gegevens. Wanneer de Power over Ethernet-technologie (PoE) wordt toegepast, kan het netwerk ook worden gebruikt om netwerkvideoproducten van stroom te voorzien.

Met een netwerkvideosysteem kunnen videobeelden vanaf elke willekeurige plaats op het netwerk worden bewaakt en opgenomen, hetzij vanaf een LAN (Local Area Network) of vanaf een WAN (Wide Area Network) zoals internet.



Afbeelding 1.1a Een netwerkvideosysteem bestaat uit veel verschillende onderdelen, zoals netwerkkamera's, video-encoders en videobeheersoftware. De overige onderdelen, waaronder het netwerk, opslag en server zijn allemaal standaard IT-apparatuur.

De belangrijkste onderdelen van een netwerkvideosysteem zijn de netwerkkamera, de video-encoder (wordt gebruikt om op analoge camera's aan te sluiten), het netwerk, de server en opslag en de videobeheersoftware. Aangezien de netwerkkamera en de video-encoder computer gebaseerde apparaten zijn, hebben deze mogelijkheden waaraan een analoge CCTV-camera niet kan voldoen. De netwerkkamera, de video-encoder en de videobeheersoftware worden beschouwd als de belangrijkste pijlers van een IP-surveillanceoplossing.

Het netwerk, de server en opslagonderdelen zijn allemaal standaard IT-apparatuur. Een van de belangrijkste voordelen van netwerkvideo is de mogelijkheid om gewone, algemeen in de handel verkrijgbare apparatuur te gebruiken. Andere onderdelen van een netwerkvideosysteem zijn onder andere accessoires zoals camerabehuizingen, PoE midspans en actieve splitters. Alle onderdelen van netwerkvideo worden uitgebreid in andere hoofdstukken besproken.

1.2 Voordelen

Het digitale netwerkvideosurveillance-systeem biedt veel voordelen en geavanceerde functies die bij een analoog videosurveillance-systeem niet kunnen worden geboden. Deze voordelen bestaan onder andere uit toegang op afstand, hoge beeldkwaliteit, gebeurtenisbeheer en intelligente videofuncties, eenvoudige integratiemogelijkheden en betere schaalbaarheid, flexibiliteit en kostenbeheer.

- > **Toegang op afstand:** Netwerkkamera's en video-encoders kunnen op afstand worden geconfigureerd en zijn op afstand toegankelijk, waardoor meerdere bevoegde gebruikers altijd live en opgenomen videobeelden kunnen bekijken vanaf vrijwel elke netwerklocatie ter wereld. Dit is een voordeel wanneer gebruikers toegang tot de videobeelden willen geven aan een derde, bijvoorbeeld een beveiligingsbedrijf. In een traditioneel analoog CCTV-systeem

moeten gebruikers zich daadwerkelijk op een specifieke locatie voor bewaking bevinden om de videobeelden te kunnen bekijken en te beheren en is toegang tot de videobeelden buiten deze locatie niet mogelijk zonder apparatuur zoals een video-encoder of een digitale netwerkvideorecorder (DVR). Een DVR is de digitale opvolger van de videocasetterecorder.

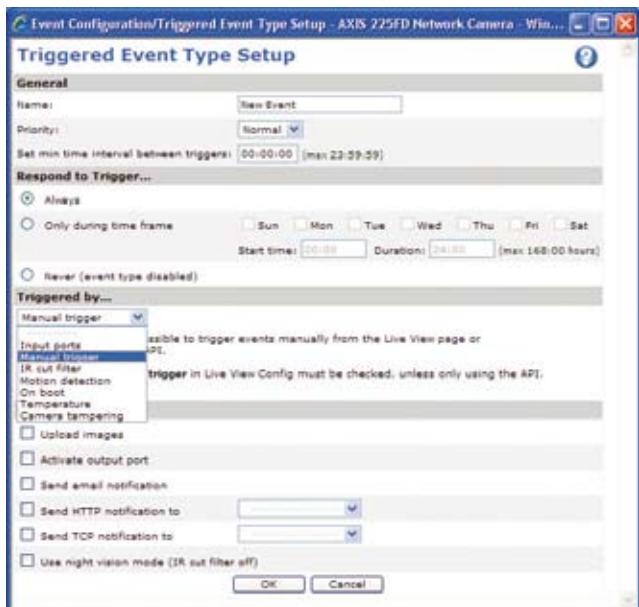
- > **Hoge beeldkwaliteit:** In een toepassing voor videosurveillance is hoge beeldkwaliteit zeer belangrijk voor het duidelijk vastleggen van een incident en voor het kunnen herkennen van de betrokken personen of voorwerpen. Met technologieën voor progressief scannen en megapixels biedt een netwerkcamera een betere beeldkwaliteit en een hogere resolutie dan een analoge CCTV-camera. *Raadpleeg voor meer informatie over progressief scannen en megapixels de hoofdstukken 2, 3 en 6.*

De beeldkwaliteit blijft ook beter behouden in een netwerkvideosysteem dan in een analoog bewakingssysteem. Bij de huidige analoge systemen waar een DVR als opnamemedium wordt gebruikt, vinden veel omzettingen van analoog naar digitaal plaats: eerst worden in de camera analoge signalen omgezet naar digitale signalen en vervolgens worden deze voor overdracht weer omgezet naar analoge signalen; daarna worden de analoge signalen gedigitaliseerd voor de opname. Bij elke omzetting van analoge en digitale indeling en met bekabelingsafstanden vermindert de kwaliteit van de opgenomen beelden. Hoe groter de afstand voor analoge videosignalen is, des te zwakker deze signalen worden.

Bij een digitaal IP-surveillancesysteem worden beelden van een netwerkcamera eenmaal gedigitaliseerd en blijven deze digitaal zonder onnodige omzettingen en is er geen vermindering van de beeldkwaliteit als gevolg van het afleggen van een lange afstand op een netwerk. Daarnaast kunnen digitale beelden gemakkelijker worden opgeslagen en worden opgehaald dan wanneer gebruik wordt gemaakt van analoge videobanden.

- > **Gebeurtenisbeheer en intelligente video:** Er worden vaak te veel videobeelden opgenomen en er is vaak te weinig tijd om deze te analyseren. Met geavanceerde netwerkcamera's en video-encoders met ingebouwde intelligentie of analysefuncties kan dit probleem worden opgelost door beperking van het aantal oninteressante opnamen en door het inschakelen van geprogrammeerde antwoorden. Dergelijke functies zijn niet beschikbaar in een analoog systeem.

Netwerkcamera's en video-encoders van Axis beschikken over ingebouwde functies zoals videobewegingsdetectie, audiodetectiealarm, actief tamperingalarm, ingangs-/uitgangsaansluitingen (I/O) en functies voor alarmbeheer en gebeurtenisbeheer. Met deze functies kunnen continu ingangen door de netwerkcamera's en video-encoders worden geanalyseerd voor het detecteren van een gebeurtenis en voor het automatisch reageren op een gebeurtenis door middel van acties zoals het maken van video-opnamen en het verzenden van alarmmeldingen.



Afbeelding 1.2a Een gebeurtenisactivering instellen met behulp van de gebruikersinterface van de netwerk-camera.

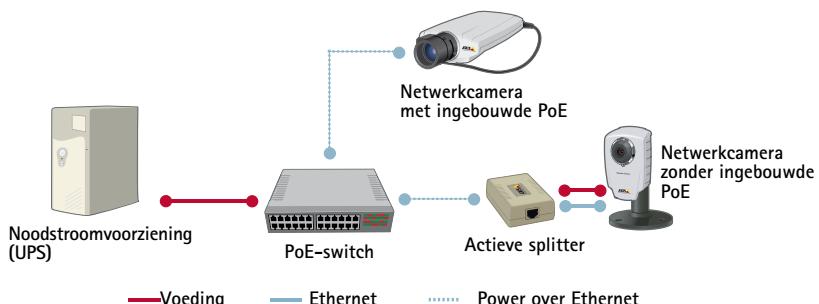
Functies voor gebeurtenisbeheer kunnen worden geconfigureerd met behulp van de gebruikersinterface van het netwerkvideoproduct of met een softwareprogramma voor video-beheer. Gebruikers kunnen de alarmen of gebeurtenissen definiëren door het type activering in te stellen en door in te stellen wanneer de activering gebruikt moet worden. Reacties kunnen ook worden geconfigureerd (bijvoorbeeld het opnemen bij een of meerdere locaties, hetzij lokaal en/of een externe locatie voor beveiligingsdoeleinden, het activeren van externe apparaten zoals alarmen, lampen en deuren en het verzenden van notificaties aan gebruikers). *Raadpleeg hoofdstuk 11 voor meer informatie over geïntegreerde systemen.*

- > **Eenvoudige, toekomstbestendige integratie:** Netwerkvideoproducten die zijn gebaseerd op open standaarden kunnen eenvoudig worden geïntegreerd met informatiesystemen die geautomatiseerd zijn en die gebaseerd zijn op Ethernet, met audio- of beveiligingssystemen en andere digitale apparaten, als aanvulling op videobeheer en toepassingssoftware. Videobeelden van een netwerkcamera kunnen bijvoorbeeld worden geïntegreerd in een POS-systeem (kassa) of in een gebouwbeheersysteem. *Raadpleeg hoofdstuk 11 voor meer informatie over geïntegreerde systemen.*
- > **Schaalbaarheid en flexibiliteit:** Een netwerkvideosysteem kan worden uitgebreid wanneer daar behoefte aan is. IP-systemen bieden mogelijkheden voor meerdere netwerkcamera's en video-encoders en andere soorten toepassingen voor het delen van hetzelfde bedrade of

draadloze netwerk voor gegevenscommunicatie. Er kan dus een onbeperkt aantal netwerkvideoproducten aan het systeem worden toegevoegd zonder ingrijpende of dure wijzigingen van de netwerkinfrastructuur. Dit is niet het geval bij een analoog systeem. Bij een analoog videosysteem moet van elke camera een speciale coaxkabel rechtstreeks naar een weergave-/opnamestation lopen. Er moeten ook afzonderlijke audiokabels worden gebruikt wanneer geluid wordt vereist. Netwerkvideoproducten kunnen vrijwel op elke locatie worden geplaatst en vanaf vrijwel elke locatie in een netwerk worden gebruikt en het systeem kan zo open en gesloten zijn als wenselijk is.

- > **Effectief kostenbeheer:** Een IP-surveillancesysteem brengt gewoonlijk lagere totale eigendomskosten met zich mee dan een traditioneel analoog CCTV-systeem. Er is vaak binnen een organisatie al een IP-netwerkinfrastructuur aanwezig die wordt gebruikt voor andere toepassingen. Een netwerkvideotoepassing kan dus gebruik maken van de bestaande infrastructuur. IP-netwerken en draadloze oplossingen zijn ook minder dure alternatieven dan traditionele coax- en fiberkabels voor een analoog CCTV-systeem. Daarnaast kunnen digitale videostromen over de hele wereld worden verstuurd met behulp van een verscheidenheid aan interoperabele infrastructuurelementen. Beheers- en apparatuurkosten zijn ook lager omdat back-endtoepassingen en opslagvoorzieningen gebruik maken van standaard open-systeemservers en niet van eigen hardware zoals een DVR bij een analoog CCTV-systeem.

Daarnaast kan de PoE-technologie (Power over Ethernet), die niet kan worden toegepast in een analoog videosysteem, worden gebruikt in een netwerkvideosysteem. Door middel van PoE kunnen netwerkapparaten stroom krijgen van een PoE-switch of PoE-midspan via dezelfde Ethernetkabel waarmee de gegevens (videobeelden) worden overgedragen. Met PoE zijn de installatiekosten aanzienlijk lager en kan de betrouwbaarheid van het systeem worden vergroot. *Raadpleeg hoofdstuk 9 voor meer informatie over PoE.*



Afbeelding 1.2b Een systeem dat gebruikt maakt van Power over Ethernet.

1.3 Toepassingen

Netwerkvideo kan worden gebruikt in een vrijwel onbeperkt aantal toepassingen, maar wordt het meest gebruikt voor beveiligingstoezicht of bewaking op afstand van mensen, plaatsen, gebouwen en activiteiten. Hieronder staan enkele gebruikelijke mogelijkheden voor toepassingen in de belangrijkste bedrijfstakken.

1.3.1 Detailhandel



Het gebruik van netwerkvideosystemen kan diefstal aanzienlijk beperken, de veiligheid van medewerkers verbeteren en het winkelbeheer optimaliseren. Een belangrijk voordeel van netwerkvideo is dat het kan worden geïntegreerd met het EAS-systeem van de winkel (electronic article surveillance) of met een POS-systeem (kassa) om een beeld en overzicht te krijgen van activiteiten betreffende derving. Met het systeem kunnen mogelijke incidenten en vals alarm snel worden gedetecteerd. Netwerkvideo biedt een hoog niveau van interoperabiliteit en geeft het allerhoogste investeringsrendement.

Met netwerkvideo kan ook worden vastgesteld wat het meest bezochte gedeelte van de winkel is en kan een overzicht van klantenactiviteiten en koopgedrag worden gegeven waardoor de indeling van een winkel of een display kan worden geoptimaliseerd. Netwerkvideo kan ook worden gebruikt wanneer de schappen moeten worden bijgevuld en wanneer er meer kassa's moeten worden geopend vanwege lange wachtrijen.

1.3.2 Transport



Het gebruik van netwerkvideo kan de persoonlijke veiligheid en de algehele veiligheid vergroten op luchthavens, snelwegen, treinstations, in andere vervoersomgevingen en ook in mobiele vervoersmiddelen zoals bussen, treinen en cruiseschepen. Netwerkvideo kan ook worden gebruikt om verkeerssituaties in de gaten te houden voor het beperken van files en het verbeteren van efficiency. Voor veel installaties in de transportsector worden de beste systemen vereist voor een hoge beeldkwaliteit (die kan worden verkregen door de technologie voor progressief scannen in netwerkcamera's), hoge beeldfrequentie en lange retentietijden. In sommige omgevingen waar hoge eisen worden gesteld, zoals in bussen en treinen, biedt Axis netwerkcamera's die tegen temperatuurwisselingen, vochtigheid, stof, trillingen en vandalisme zijn bestand.

1.3.3 Onderwijs



Het gebruik van netwerkvideosystemen helpt bij het ontmoedigen van vandalisme en zorgt voor een grotere veiligheid voor medewerkers en leerlingen, vanaf het kinderdagverblijf tot de universiteit. In onderwijsinstellingen waar al een IT-infrastructuur aanwezig is, biedt netwerkvideo een gunstiger en goedkopere oplossing dan een analoog systeem omdat er vaak geen nieuwe kabels worden vereist. Daarnaast kunnen met de gebeurtenisbeheerfuncties van netwerkvideo alarmen worden gegeven en krijgen beveiligingsmedewerkers nauwkeurige, realtime beelden waarop zij hun beslissingen kunnen baseren. Netwerkvideo kan ook worden gebruikt voor leren op afstand, bijvoorbeeld door studenten die zelf geen bijeenkomsten kunnen bijwonen.

1.3.4 Industrie



Netwerkvideo kan worden gebruikt voor bewaking, voor grotere efficiency in productielijnen, productieprocessen en logistieke systemen en voor het beveiligen van pakhuizen en voor systemen voor voorraadcontrole. Netwerkvideo kan tevens worden gebruikt voor het opzetten van virtuele vergaderingen en het verkrijgen van technische ondersteuning op afstand.

1.3.5 Stadsbewaking



Netwerkvideo is een van de meest nuttige middelen om misdaad te bestrijden en burgers te beschermen. Netwerkvideo kan worden gebruikt om de misdaad te detecteren en te ontmoedigen. Door het gebruik van draadloze netwerken kan netwerkvideo effectief in de gehele stad worden ingezet. Door de mogelijkheden van netwerkvideo voor bewaking op afstand kan de politie snel reageren op misdaad die worden gepleegd bij live weergave.

1.3.6 Overheid



Netwerkvideoproducten worden gebruikt om allerlei openbare gebouwen te beveiligen, van musea en kantoren tot bibliotheken en gevangenissen. Camera's die bij de ingangen en uitgangen zijn geplaatst, kunnen registreren wie naar binnen en buiten gaat, 24 uur per dag. Deze worden gebruikt om vandalisme te voorkomen en de veiligheid van de medewerkers te vergroten. Met intelligente video-toepassingen zoals het tellen van mensen, biedt netwerkvideo statistische gegevens, zoals het aantal bezoekers in een gebouw.

1.3.7 Zorginstellingen



Met netwerkvideo kan de patiënt op een goedkope, maar kwalitatief goede manier in de gaten worden gehouden en met oplossingen voor videosurveillance wordt de veiligheid en de beveiliging van de medewerkers, patiënten, bezoekers en het gebouw verbeterd. Bevoegde ziekenhuismedewerkers kunnen bijvoorbeeld live-videobeelden op meerdere locaties bekijken, activiteiten detecteren en van afstand assistentie verlenen.

1.3.8 Bank- en geldwezen



Netwerkvideo wordt gebruikt in beveiligingstoepassingen in bankvestigingen, hoofdkantoren van banken en bij geldautomaten. Banken maken al sinds lange tijd gebruik van bewaking en hoewel de meeste installaties nog steeds analoog zijn, begint netwerkvideo zijn intrede te doen, vooral bij banken die hoge beeldkwaliteit op prijs stellen en die mensen in bewakingsvideobeelden gemakkelijk willen kunnen herkennen.

Netwerkvideo is een beproefde technologie en er wordt steeds meer overgeschakeld van analoge systemen naar IP-surveillance in de videosurveillance-industrie. *Ga voor meer casestudy's naar www.axis.com/success_stories/*

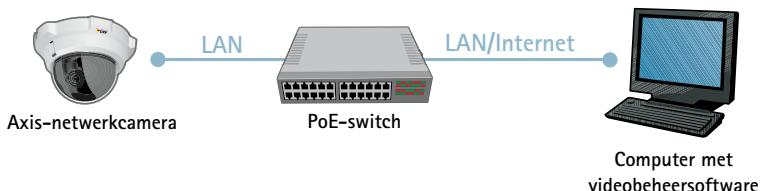
Netwerkkamera's

Er is een groot assortiment netwerkkamera's dat aan de meest uiteenlopende vereisten kan voldoen. In dit hoofdstuk wordt beschreven wat een netwerkkamera is en wordt uitleg gegeven over de verschillende cameratypes. U vindt hier ook informatie over dag-en-nacht- en megapixelnetwerkkamera's. Aan het einde van het hoofdstuk vindt u een gids voor het selecteren van camera's. *Raadpleeg hoofdstuk 3 voor meer informatie over de cameraonderdelen.*

2.1 Wat is een netwerkkamera?

Een netwerkkamera, ook vaak een IP-camera genoemd, kan worden omschreven als een camera en een computer in één. De hoofdonderdelen van een netwerkkamera zijn onder andere een lens, een beeldsensor, één of meerdere processors en geheugen. De processors worden gebruikt voor beeldverwerking, compressie, videoanalyse en netwerkfunctionaliteiten. Het geheugen wordt gebruikt voor het opslaan van de firmware (computerprogramma) van de netwerkkamera en voor het lokaal opnemen van reeksen videobeelden.

Net als een computer heeft de netwerkkamera een eigen IP-adres. Het apparaat wordt direct verbonden met een netwerk en kan overal worden geplaatst waar een netwerkverbinding is. Dit verschilt van een webcam die alleen kan werken wanneer de webcam is aangesloten op een pc via de USB- of IEEE 1394-poort. Om deze te gebruiken moet de software op de pc geïnstalleerd zijn. Een netwerkkamera biedt webserver-, FTP- (File Transfer Protocol) en e-mailfunctionaliteiten en bevat veel andere andere IP-netwerk- en beveiligingsprotocollen.



Afbeelding 2.1a Een netwerkkamera wordt direct op het netwerk aangesloten.

Een netwerkkamera kan worden geconfigureerd om videobeelden te verzenden via een IP-netwerk voor live weergave en/of om continu op geplande tijden op te nemen tijdens een gebeurtenis of op aanvraag van bevoegde gebruikers. Vastgelegde beelden kunnen worden gestreamd als Motion JPEG, MPEG-4 of H.264-video met verschillende netwerkprotocollen. U kunt deze ook uploaden als afzonderlijke JPEG-beelden via FTP, e-mail of HTTP (Hypertext Transfer Protocol). *Raadpleeg hoofdstukken 7 en 9 voor meer informatie over respectievelijk videocompressie-indelingen en netwerkprotocollen.*

Naast het vastleggen van videomateriaal bieden Axis-netwerkkamera's ook gebeurtenisbeheer en intelligente videofuncties, zoals videobewegingsdetectie, audiodetectie, actief tamperingalarm en automatisch volgen. De meeste netwerkkamera's beschikken ook over in-/uitgangen (I/O) voor het aansluiten van externe apparaten, zoals sensoren en relais. Andere mogelijke functies zijn audio-functionaliteiten en ingebouwde ondersteuning voor PoE (Power over Ethernet). Axis-netwerkkamera's bieden ook geavanceerde functies voor beveiliging en netwerkbeheer.



Afbeelding 2.1b Voor- en achterkant van een netwerkkamera.

2.2 Typen netwerkkamera's

Netwerkkamera's kunnen worden geklassificeerd op basis van het feit of deze alleen voor binnengebruik of voor zowel binnen- als buitengebruik zijn ontworpen. Netwerkkamera's voor buitengebruik beschikken vaak over een auto-irislenzen om de hoeveelheid licht waaraan de beeldsensor wordt blootgesteld, te regelen. Een buitencamera vereist ook een externe, beschermende behuizing, tenzij er al een beschermende omhulling is voorzien in het cameraontwerp. Er zijn ook behuizingen verkrijgbaar voor binnencamera's die bescherming nodig hebben in slechte omstandigheden met bijvoorbeeld stof en vocht, maar ook tegen vandalisme en sabotage. Sommige cameraontwerpen beschikken al over ingebouwde functies tegen vandalisme en sabotage, zodat in dat geval geen externe behuizing nodig is. *Raadpleeg hoofdstuk 4 voor meer informatie over camerabescherming en -behuizingen.*

Netwerkkamera's, of ze nu voor binnen- of buitengebruik zijn, kunnen verder worden opgesplitst in categorieën van vaste, vaste dome-, PTZ- en PTZ-domenetwerkkamera's.

2.2.1 Vaste netwerkcamera's

Een vaste netwerkcamera die kan worden geleverd met een vaste of varifocale lens, is een camera die een vast beeldveld (normaal/telelens/groothoek) krijgt nadat het apparaat is gemonterd. Een vaste camera is het traditionele cameratype waarbij de camera en de richting waarin deze wijst, duidelijk zichtbaar is. Dit type camera vormt de beste keuze bij toepassingen waar het nuttig is om de camera duidelijk zichtbaar te maken. Bij een vaste camera is het doorgaans mogelijk de lens te veranderen. Een vaste camera kan worden geïnstalleerd in een behuizing die bestemd is voor installatie binnen of buiten.



Afbeelding 2.2a Vaste netwerkcamera's met draadloze en megapixelversies.

2.2.2 Vaste domenetwerkcamera's

Bij vaste domenetwerkcamera's, ook mini-domes genoemd, gaat het in principe om vaste camera's die vooraf in een kleine, koepelvormige behuizing zijn geïnstalleerd. De camera kan alle kanten op worden gericht. Het grote voordeel is het discrete, onopvallende ontwerp plus het feit dat moeilijk te zien is naar welke kant de camera is gericht. De camera is ook bestand tegen sabotage. Een van de beperkingen van een vaste domecamera is dat het toestel zelden wordt geleverd met een verwisselbare lens. En zelfs als de lens verwisselbaar is, blijft de keuze van lenzen beperkt door de ruimte binnenin de domebehuizing. Als compensatie wordt vaak een varifocale lens geleverd waarmee het beeldveld van de camera kan worden aangepast.

Vaste domecamera's van Axis zijn ontworpen met verschillende types omhulsels, zoals vandalismebestendige omhulsels en/of omhulsels met een beschermingsgraad IP66 voor installaties buitenhuis. Er is geen externe behuizing vereist. Een dergelijke camera wordt meestal aan de muur of het plafond bevestigd.



Afbeelding 2.2b Vaste domenetwerkcamera's. Van links naar rechts: AXIS 209FD en AXIS 216FD (ook verkrijgbaar in verstevigde en megapixelversies), AXIS P3301 en AXIS 225FD.

2.2.3 PTZ-camera's en PTZ-domecamera's

Een PTZ- of PTZ-domecamera kan handmatig of automatisch pannen, kantelen en in- en uitzoomen op een gebied of object. Alle PTZ-opdrachten worden via dezelfde netwerkabel gestuurd als voor video-overdracht; er moeten geen RS-485-draden worden geïnstalleerd zoals bij een analoge PTZ-camera.

Dit zijn enkele functies die in een PTZ- of PTZ-domecamera geïntegreerd kunnen zijn:

- > **Elektronische beeldstabilisator (EIS).** Bij buiteninstallaties zijn PTZ-domecamera's met een zoomfactor van meer dan 20x gevoelig voor trillingen en bewegingen die worden veroorzaakt door verkeer of wind. EIS helpt de invloeden van de trillingen in een video te verminderen. Naast het verkrijgen van een efficiëntere video, verkleint EIS ook de bestandsgrootte van het gecomprimeerde beeld waardoor waardevolle opslagruimte wordt bespaard.
- > **Privacy-maskering.** Met privacy-maskering kunnen bepaalde gebieden van een scène worden geblokkeerd of verborgen voor weergave en opname. Deze functie kan in verschillende netwerkvideoproducten beschikbaar worden gemaakt. In een PTZ- of PTZ-domecamera heeft deze functie de mogelijkheid de privacy-maskering te behouden, zelfs wanneer het beeldveld van de camera verandert omdat de maskering meebeekt met het coördinaten-systeem.



Afbeelding 2.2c Met een ingebouwde privacy-maskering (grijze rechthoek in beeld), kan de camera privacy garanderen voor gebieden die niet door een surveillancetoepassing moeten gedekt.

- > **Vooraf ingestelde posities.** Veel PTZ- en PTZ-domecamera's bieden de mogelijkheid een aantal vooraf ingestelde posities (doorgaans tussen 20 en 100 posities) te programmeren. Zodra de vooraf ingestelde posities in de camera zijn geprogrammeerd, kan de operator snel van de ene naar de volgende positie gaan.
- > **E-flip.** Wanneer een PTZ-domecamera aan een plafond wordt gemonteerd en wordt gebruikt om een persoon die binnenkomt te volgen, zoals in een winkel, zullen er situaties zijn waarin een persoon net onder de camera zal lopen. Wanneer de persoon verder wordt gevolgd, zouden zonder de E-flip-functie de beelden ondersteboven worden weergegeven. In dergelijke gevallen draait E-flip beelden elektronisch 180 graden. Dit gebeurt automatisch en zal niet door een operator worden gemerkt.
- > **Auto-flip.** In tegenstelling tot PTZ-domecamera's, beschikken PTZ-camera's normaal niet over een volledige doorlopende pan van 360 graden. Dit is te wijten aan een mechanische stop die verhindert dat camera een doorlopende cirkelvormige beweging maakt. Met de functie Auto-flip kan een PTZ-netwerkkamera echter de camerakop onmiddellijk 180 graden draaien en doorgaan met pannen voorbij het nulpunt. De camera kan vervolgens een voorbijgaande persoon of object in elke richting volgen.
- > **Automatisch volgen.** Automatisch volgen is een intelligente videofunctionaliteit die automatisch een bewegende persoon of wagen detecteert en deze volgt binnen het dekkingsbereik van de camera. Automatisch volgen is vooral nuttig bij onbemande videosurveillance-situaties waar de incidentele aanwezigheid van mensen of voertuigen speciale aandacht vereist. De functionaliteit biedt een aanzienlijke verlaging de kosten van een surveillance-systeem omdat er minder camera's nodig zijn om een scène te dekken. Daarnaast biedt de functie ook een betere efficiëntie van de oplossing omdat een PTZ-of PTZ-domecamera hiermee gebieden van een scène met activiteit kan opnemen.

Hoewel PTZ- en PTZ-domecamera's soortgelijke functies delen, zijn er toch enkele verschillen:

- > PTZ-netwerkkamera's hebben geen volledige doorlopende pan van 360 graden vanwege een mechanische stop. Dit betekent dat de camera geen persoon kan volgen die voortdurend in een volledige cirkel rond de camera loopt. Uitzondering hierop zijn PTZ-camera's die zijn uitgerust met de Auto-flip-functie, zoals de AXIS 215 PTZ-netwerkkamera.
- > PTZ-netwerkkamera's zijn niet gemaakt voor continu automatisch gebruik of voor zogenoemde wachtronden waarbij de camera automatisch van de ene vooraf ingestelde positie naar de andere gaat.

In de volgende hoofdstukken vindt u meer informatie over PTZ-netwerkkamera's die beschikbaar zijn in mechanische en niet-mechanische versies en over PTZ-domennetwerkkamera's.

Mechanische PTZ-netwerkcamera's

Mechanische PTZ-camera's worden hoofdzakelijk binnenshuis gebruikt en in toepassingen waarbij een operator werkzaam is. De optische zoom op PTZ-camera's ligt standaard tussen 10x en 26x. Een PTZ-camera kan aan een plafond of een muur worden gemonteerd.



Afbeelding 2.2d PTZ-netwerkcamera's. Van links naar rechts: AXIS 212 PTZ-V (niet-mechanisch), AXIS 213 PTZ, AXIS 214 PTZ en AXIS 215 PTZ.

Niet-mechanische PTZ-netwerkcamera's

Een niet-mechanische PTZ-netwerkcamera, zoals de AXIS 212 PTZ en de vandalismebestendige versie ervan (zoals hierboven is weergegeven), biedt mogelijkheden voor het onmiddellijk pannen, kantelen en zoomen zonder bewegende delen zodat er geen slijtage is. Met een groothoeklens biedt de camera een breder beeldveld dan bij een mechanische PTZ-netwerkcamera.



Afbeelding 2.2e Beelden van een niet-mechanische PTZ-netwerkcamera. Links een overzichtbeeld van 140 graden met VGA-resolutie; rechts het beeld na 3x inzoomen.

Een niet-mechanische PTZ-camera gebruikt een megapixelbeeldsensor en biedt een operator de mogelijkheid onmiddellijk in te zoomen op een deel van een scène zonder enig verlies van beeldresolutie. Dit wordt bereikt door het voorstellen van een overzichtbeeld met VGA-resolutie (640x480 pixels), ondanks het feit dat de camera een beeld met een veel hogere resolutie vastlegt. Wanneer de camera de opdracht krijgt in te zoomen op een deel van het overzichtbeeld, gebruikt de camera de originele megapixelresolutie om een volledige 1:1-verhouding met VGA-resolutie te bieden. Het resulterende close-upbeeld biedt goede details terwijl de scherpte behouden blijft. Met een normale digitale zoom verliest het ingezoomde beeld vaak details en

scherpte. Een niet-mechanische PTZ-camera is ideaal voor discrete, aan de muur gemonteerde installaties.

PTZ-domenetwerkcamera's

PTZ-domenetwerkcamera's kunnen een breed gebied dekken door een grotere flexibiliteit in de functies voor het pannen, kantelen en zoomen. Hierdoor is een doorlopende pan van 360 graden en een kantelhoek van doorgaans 180 graden mogelijk. PTZ-domecamera's zijn ideaal voor gebruik in discrete installaties vanwege hun ontwerp, montage (vooral bij montages aan verlaagd plafond) en de moeilijkheid om de beeldhoek van de camera te zien (de koepelvormige afschermkap kan doorzichtig of rookkleurig zijn). Een PTZ-domenetwerkcamera is ook mechanisch robuust voor continu gebruik in de modus voor wachtronden, waarbij de camera automatisch, in een vooraf vastgestelde volgorde of in willekeurige volgorde, van de ene vooraf ingestelde positie naar de andere gaat. Normaal kunnen maximaal 20 wachtronden op verschillende tijdstippen tijdens de dag worden ingesteld en geactiveerd. In de wachtrondemodus kan één PTZ-domenetwerkcamera een gebied dekken waar 10 vaste netwerkcamera's zouden nodig zijn. Het belangrijkste nadeel is dat op elk gegeven moment slechts één locatie kan worden bewaakt, terwijl de andere 9 gebieden onbewaakt zijn.

De optische zoom van een PTZ-dome ligt standaard tussen 10x en 35x. Een PTZ-dome wordt vaak gebruikt in situaties waar een operator werkzaam is. Dit type camera wordt bij gebruik binnenshuis doorgaans aan een plafond gemonteerd en bij gebruik buitenshuis op een paal of de muur van een gebouw.

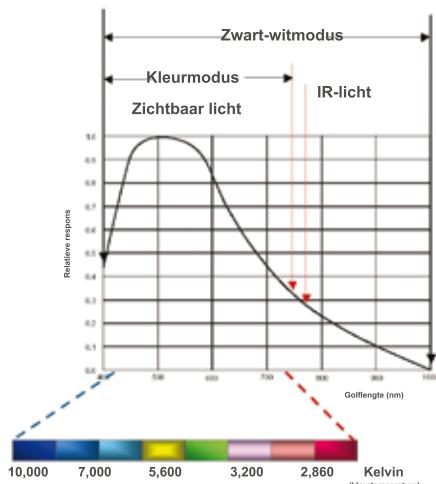


Afbeelding 2.2f PTZ-domenetwerkcamera's. Van links naar rechts: AXIS 231D+, AXIS 232D+, AXIS 233D.

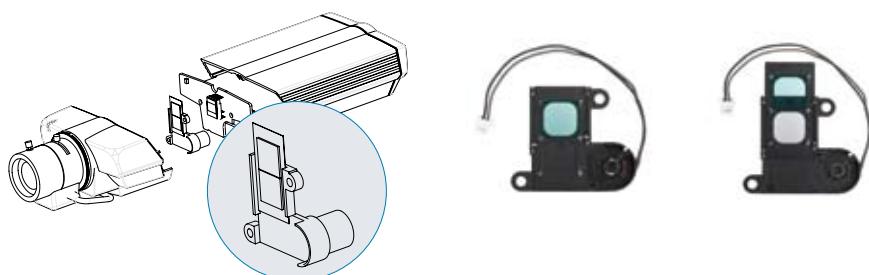
2.3 Netwerkcamera's voor dag en nacht

Alle typen netwerkcamera's –vast, vaste dome, PTZ en PTZ-dome– bieden dag- en nachtfuncties. Een camera voor dag en nacht is ontworpen voor gebruik in buiteninstallaties of in binne-nomgevingen met een zwakke belichting. Een kleurennetwerkcamera voor dag en nacht biedt kleurenbeelden tijdens de dag. Naarmate het licht onder een bepaald niveau daalt, kan de camera automatisch naar de nachtmodus schakelen om gebruik te maken van near-infrarood licht (NIR) om zwart-witbeelden met hoge kwaliteit te bieden.

Near-infraroodlicht dat tussen 700 nanometer (nm) en circa 1000 nm ligt, ligt buiten het bereik van het menselijke oog, maar de meeste camerahouders kunnen het detecteren en gebruiken. Overdag gebruikt een dag-en-nacht-camera een IR-filter. IR-licht wordt gefilterd zodat de kleuren van de beelden niet worden vervormd wanneer het menselijk oog ze ziet. Wanneer de camera in de nachtmodus (zwart-wit) is, wordt het IR-filter verwijderd zodat de lichtgevoeligheid van de camera kan dalen tot 0,001 lux of lager.



Afbeelding 2.3a De grafiek toont hoe een beeldsensor reageert op zichtbaar en near-IR-licht. Near-IR-licht heeft een bereik van 700 nm tot 1000 nm.



Afbeelding 2.3b Beeld links, IR-filter in een dag/nacht-netwerkcamera; midden, positie van het IR-filter overdag; rechts, positie van het IR-filter 's nachts.

Dag-en-nacht-camera's zijn nuttig in omgevingen waar het gebruik van kunstlicht wordt beperkt. Dit zijn situaties met videosurveillance bij zwakke verlichting, geheime bewaking en discrete toepassingen zoals bij verkeersbewaking waar heldere lichten de bestuurders 's nachts kunnen hinderen.

Er kan ook een IR-licht dat near-infrarood licht biedt, worden gebruikt in combinatie met een dag-en-nacht-camera als verbetering van de capaciteit van de camera om video's van hoge kwaliteit te produceren bij een zwakke verlichting of bij nachtopnamen. *Meer informatie over IR-lichten kunt u vinden op de website van Axis op www.axis.com/products/cam_irillum*



Afbeelding 2.3c Links, beeld zonder IR-licht; rechts, beeld met IR-licht.

2.4 Megapixelnetwerkcamera's

Megapixelnetwerkcamera's die verkrijgbaar zijn als vaste en vaste domecamera's van Axis, zijn uitgerust met een megapixelbeeldsensor om beelden met een miljoen of meer pixels te leveren. Dit is een pixelresolutie die minstens 2 keer beter is dan wat door analoge camera's wordt geleverd.

Een vaste megapixelnetwerkcamera kan op een van de volgende twee manieren worden gebruikt: kijkers kunnen door middel van deze camera meer details zien in een beeld met een hogere resolutie. Dit kan handig zijn bij het identificeren van mensen en objecten, of kan worden gebruikt om een groter deel van een scène te dekken als de beeldresolutie dezelfde blijft als bij een niet-megapixelcamera.

Megapixelcamera's zijn tegenwoordig doorgaans minder lichtgevoelig dan een niet-megapixel-netwerkcamera. De videostromen met hogere resolutie die door een megapixelcamera worden gegenereerd, stellen ook meer eisen aan de netwerkbandbreedte en opslagruimte voor de opnames. Dit kan echter worden verminderd door gebruik te maken van de videocompressiestandaard H.264. *Raadpleeg hoofdstuk 7 voor meer informatie over H.264.*

2.5 Richtlijnen voor het kiezen van een netwerkcamera

Door het gevarieerde aanbod van beschikbare netwerkcamera's is het nuttig over enkele richtlijnen te beschikken bij het kiezen van een netwerkcamera.

- > **Definieer het doel van de surveillance: overzicht of zeer gedetailleerd.** Overzichtbeelden hebben het doel een algemeen beeld van het scene of de algemene bewegingen van mensen weer te geven. Zeer gedetailleerde beelden zijn belangrijk voor de identificatie van personen of objecten (bijv. gezichts- of nummerplaatherkenning, surveillance op verkooppunten). Het doel van de surveillance bepaalt het beeldveld, de plaatsing van de camera en het vereiste type camera/lens. *Raadpleeg hoofdstuk 3 voor meer informatie over lenzen.*
- > **Dekkingsgebied.** Bepaal voor een bepaalde locatie het aantal interessegebieden, hoeveel van deze gebieden moeten worden gedekt en of de gebieden relatief dichtbij elkaar of ver van elkaar liggen. Het type camera en het vereiste aantal camera's wordt aan de hand van het gebied vastgesteld.
 - *Megapixel of niet-megapixel.* Als er bijvoorbeeld twee relatief kleine interessegebieden zijn die dicht bij elkaar liggen, kan een megapixelcamera met een groothoeklens worden gebruikt in plaats van twee niet-megapixelcamera's.
 - *Vast of PTZ.* (In de volgende context verwijzen vaste camera's ook naar vaste domes en PTZ-camera's naar PTZ-domes). Een gebied kan gedekt worden door meerdere vaste camera's of enkele PTZ-camera's. Denk eraan dat een PTZ-camera met hoge optische zoomfunctionaliteiten zeer gedetailleerde beelden kan bieden en een groot gebied kan bewaken. Een PTZ-camera kan echter een vluchige weergave van één deel van het dekkingsgebied per keer bieden, terwijl een vaste camera op elk ogenblik volledige dekking van het gebied kan leveren. Om optimaal gebruik te maken van de mogelijkheden van een PTZ-camera is een operator vereist of moet een automatisch ronde worden ingesteld.
- > **Omgeving binnens- of buitenshuis.**
 - *Lichtgevoeligheid en belichtingsvereisten* Bij buitenomgeving raden wij u aan dag-en-nacht-camera's te gebruiken. Houd rekening met de vereiste lichtgevoeligheid van de camera en kijk of er extra verlichting of gespecialiseerde verlichting, zoals een IR-lamp, nodig is. Denk eraan dat de lux-metingen op netwerkcamera's van verschillende leveranciers van netwerkvideoproducten niet kunnen worden vergeleken, omdat er geen industrietstandaard is voor het meten van de lichtgevoeligheid.
 - *Behuizing.* Als de camera buiten moet worden geplaatst of in een omgeving waar het apparaat moet worden beschermd tegen stof, vochtigheid of vandalisme, is een behuizing vereist. *Raadpleeg hoofdstuk 4 voor meer informatie over behuizingen.*

- > **Openlijke of geheime surveillance** Dit kan u helpen bij het kiezen van camera's, naast de behuizing en montages die een niet-discrete of discrete installatie bieden.

Andere belangrijke overwegingen met betrekking tot de vereiste functies van een camera zijn de onder andere:

- > **Beeldkwaliteit.** Beeldkwaliteit is een van de belangrijkste aspecten van elke camera, maar het is moeilijk om dit vast te stellen en te meten. De beste manier om de beeldkwaliteit vast te stellen is het installeren van verschillende camera's en de video te bekijken. Als het vastleggen van bewegende objecten duidelijk een prioriteit is, is het belangrijk dat de netwerkcamera de progressieve scantechnologie gebruikt. *Raadpleeg hoofdstuk 3 voor meer informatie over progressief scannen..*
- > **Resolutie.** Voor toepassingen die gedetailleerde beelden vereisen, zijn megapixelcamera's mogelijk de beste keuze. *Raadpleeg hoofdstuk 6 voor meer informatie over megapixelresolutie.*
- > **Compressie.** De drie videocompressiestandaarden die worden aangeboden in netwerkvideo producten van Axis, zijn H.264, MPEG-4 en Motion JPEG. H.264 is de nieuwste standaard en biedt grote besparingen in bandbreedte en opslagruimte. *Raadpleeg hoofdstuk 7 voor meer informatie over compressie.*
- > **Audio.** Als er audio vereist is, moet u overwegen of er audio in één richting of in twee richtingen nodig is. Axis-netwerkcamera's met audio-ondersteuning worden geleverd met een ingebouwde microfoon en/of een ingang voor een externe audio-bron en een luidspreker of een lijnuitgang voor externe luidsprekers. *Raadpleeg hoofdstuk 8 voor meer informatie over audio.*
- > **Gebeurtenisbeheer en intelligente video.** Functies voor gebeurtenisbeheer worden vaak geconfigureerd met een videobeheerprogramma en worden ondersteund door ingangen/uitgangen en intelligente videofuncties in een netwerkcamera of video-encoder. Het maken van opnamen op basis van gebeurtenisactivering vanaf ingangen en intelligentie videofuncties in een netwerkvideoproduct biedt besparingen in bandbreedte en opslagruimte. Operators kunnen hierdoor meer camera's beheren omdat niet alle camera's live bewaking vereisen, tenzij een alarm/gebeurtenis optreedt. *Raadpleeg hoofdstuk 11 voor meer informatie over functies voor gebeurtenisbeheer.*
- > **Netwerkfuncties.** Overwegingen zijn onder andere PoE; HTTPS-codering voor het coderen van videostromen voordat deze via het netwerk worden verzonden; IP-adresfilter die toegangsrechten verleent of weigert aan gedefinieerde IP-adressen; IEEE802.1X om toegang tot een netwerk te controleren; IPv6; en draadloze functionaliteit. *Raadpleeg hoofdstuk 9 voor meer informatie over netwerk- en beveiligingstechnologieën.*

- > **Open interface- en toepassingssoftware.** Een netwerkvideoproduct met een open interface biedt betere mogelijkheden voor de integratie met andere systemen. Het is ook belangrijk dat het product wordt ondersteund door goede toepassingssoftware en door beheersoftware die eenvoudige installatie en upgrades van netwerkvideoproducten mogelijk maakt. Axis-producten worden zowel ondersteund door eigen videobeheersoftware als door een uitgebreide verscheidenheid aan softwareoplossingen voor videobeheer van meer dan 550 van haar Application Development Partners. *Raadpleeg hoofdstuk 11 voor meer informatie over videobeheersystemen.*

Een andere belangrijke overweging is, behalve de keuze van de netwerkkamera, de keuze van de leverancier van de netwerkvideoproducten. Aangezien behoeften groeien en veranderen, moet de leverancier worden beschouwd als een partner op lange termijn. Dit betekent dat het belangrijk is dat u een leverancier kiest die een volledige productlijn aanbiedt van netwerkvideoproducten en -accessoires die zowel aan de huidige als aan de toekomstige behoeften kunnen voldoen. De leverancier moet ook innovatie, ondersteuning, upgrades en productontwikkelingen op lange termijn leveren.

Zodra een beslissing is genomen over de benodigde camera, is het een goed idee een exemplaar te kopen en de kwaliteit ervan te testen voordat u grotere hoeveelheden bestelt.

Camera-elementen

Er zijn enkele camera-elementen die de beeldkwaliteit en het beeldveld beïnvloeden. Daarom is het belangrijk dat u deze elementen begrijpt wanneer u een netwerkcamera kiest. We hebben het hier over de lichtgevoeligheid van een camera, het type lens, het type beeldsensor en de scantechniek, maar ook over de beeldverwerkingsfuncties. In dit hoofdstuk wordt dit allemaal verder toegelicht. Aan het einde van het hoofdstuk vindt u enkele richtlijnen die betrekking hebben op de installatie.

3.1 Lichtgevoeligheid

De lichtgevoeligheid van een netwerkcamera wordt vaak opgegeven in lux. Dit komt overeen met het niveau van verlichting waarbij een camera een acceptabel beeld produceert. Hoe lager de lux-specificatie, hoe beter de lichtgevoeligheid van de camera is. Normaal is er minstens 200 lux nodig om een object te verlichten zodat een goede beeldkwaliteit kan worden verkregen. Over het algemeen kunnen we stellen dat het beeld verbetert naarmate het onderwerp beter belicht wordt. Met te weinig licht wordt het scherpstellen moeilijk en zal het beeld korrelig en/of donker zijn. Voor het opnemen van beelden met goede kwaliteit in een zwak belichte of donkere omgeving is een dag-en-nacht-camera die gebruik maakt van een near-infraroodlicht verplicht. *Raadpleeg hoofdstuk 2 voor meer informatie over dag-en-nacht-camera's.*

Verschillende lichtomstandigheden zorgen voor een verschillende belichting. Heel wat natuurtaferelen hebben een relatief complexe belichting met schaduwen en heldere delen die verschillende lux-aflezingen bieden. Het is daarom belangrijk te onthouden dat één lux-aflezing niet volstaat om de lichtomstandigheden voor een scène als geheel aan te geven.

Verlichting	Lichtomstandigheid
100.000 lux	Fel zonlicht
10.000 lux	Sterk daglicht
500 lux	Kantoorverlichting
100 lux	Slecht verlichte ruimte

Tabel 3.1a Voorbeelden van verschillende verlichtingsniveaus.

Veel fabrikanten vermelden het minimale verlichtingsniveau dat een netwerkkamera nodig heeft om een acceptabel beeld voor te brengen. Dergelijke specificaties zijn wel nuttig wanneer u een vergelijking wilt maken van de lichtgevoeligheid van camera's die door dezelfde fabrikant zijn gemaakt, maar zijn minder nuttig wanneer u de waarden wilt vergelijken van camera's van verschillende fabrikanten. De reden hiervoor is dat verschillende fabrikanten verschillende methoden gebruiken en verschillende criteria hanteren voor acceptabele beelden. Om een goede vergelijking te maken tussen de prestaties van twee verschillende camera's bij weinig licht moeten ze naast elkaar worden geplaatst en een bewegend object bij weinig licht weergeven.

3.2 Lenselementen

Een lens of lensassemblage op een netwerkkamera voert verschillende functies uit. Dit zijn onder andere:

- > Het beeldveld definiëren. Dit betekent dat er wordt bepaald hoeveel van een scène of welk detailniveau moet worden vastgelegd.
- > De hoeveelheid licht controleren die door de beeldsensor gaat zodat een beeld correct wordt belicht.
- > Scherpstellen door elementen binnen de lensassemblage af te stellen of door de afstand tussen de lensassemblage en de beeldsensor aan te passen.

3.2.1 Beeldveld

Wanneer u een camera kiest, is het belangrijk dat u rekening houdt met het vereiste beeldveld. Dit is het dekkingsgebied en de mate van details die u wilt zien. Het beeldveld wordt bepaald door de brandpuntsafstand van de lens en het formaat van de beeldsensor. Beide items worden vermeld op het gegevensblad van de netwerkkamera.

De brandpuntsafstand van een lens wordt gedefinieerd als de afstand tussen de ingangslens (of een specifiek punt in een ingewikkelde lensassemblage) en het punt waar alle lichtstralen samenkommen in één punt (doorgaans de beeldsensor van de camera). Hoe langer de brandpuntsafstand, hoe smaller het beeldveld.

De snelste manier om uit te zoeken welke brandpuntsafstand voor de lens is vereist voor een gewenst beeldveld is het gebruiken van een roterende lenscalculator of een online lenscalculator (www.axis.com/tools), die beide verkrijgbaar zijn bij Axis. De grootte van de beeldsensor van een netwerkkamera is standaard $1/4"$, $1/3"$, $1/2"$ en $2/3"$ en moet ook worden gebruikt in de berekening. (Het nadeel hiervan is dat de lenscalculator geen rekening houdt met een mogelijke geometrische vervorming van een lens.)

Het beeldveld kan in drie typen worden onderverdeeld:

- > **Normale weergave:** biedt hetzelfde beeldveld als het menselijke oog.
- > **Telelensweergave:** een smaller beeldveld met doorgaans fijnere details dan door het menselijke oog kan worden waargenomen. Een telelens wordt gebruikt wanneer het surveillance-object klein is of zich ver van de camera bevindt. Een telelens heeft doorgaans minder mogelijkheden voor het verzamelen van licht dan een normale lens.
- > **Groothoekweergave:** een grotere beeldhoek met minder details dan in de normale weergave. Een groothoeklens biedt doorgaans een goede scherptediepte en redelijke prestaties bij weinig licht. Groothoeklenzen zorgen soms voor geometrische vervormingen zoals het 'visoog'-effect.



Afbeelding 3.2a Verschillende beeldvelden: groothoekweergave (links); normale weergave (midden); telelensweergave (rechts).



Afbeelding 3.2b Lenzen van netwerkcamera's met verschillende brandpuntsafstanden: groothoeklens (links); normale lens (midden); telelens (rechts).

Er zijn drie hoofdtypen lenzen:

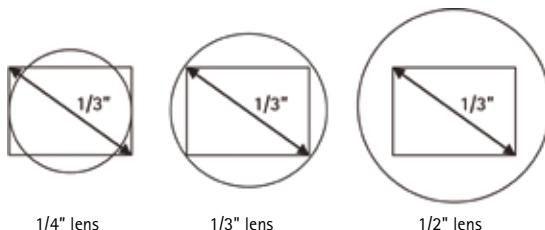
- > **Vaste lens:** een dergelijke lens biedt een vaste brandpuntsafstand. Dit betekent dat er slechts één beeldveld is (normaal, telelens of groothoek). Een algemene brandpuntsafstand van een vaste netwerkcameralens is 4mm.

- > **Varifocuslens:** dit type lens biedt een verscheidenheid van brandpuntsafstanden, en daarom verschillende beeldvelden. Het beeldveld kan handmatig worden aangepast. Telkens wanneer het beeldveld wordt gewijzigd, moet de gebruikte lens handmatig opnieuw worden scherpgesteld. Varifocuslenzen voor netwerkcamera's bieden vaak brandpuntsafstanden die liggen tussen 3 en 8 mm.
- > **Zoomlens:** Zoomlenzen lijken op varifocuslenzen omdat ze de gebruiker de mogelijkheid bieden verschillende beeldvelden te selecteren. Met zoomlenzen moet de lens echter niet opnieuw worden scherpgesteld wanneer het beeldveld wordt gewijzigd. De focus kan worden behouden binnen een bereik van brandpuntsafstanden, bijv. 6 tot 48 mm. De aanpassing van de lens kan handmatig worden gemaakt of gemotoriseerd via de afstandsbediening. Wanneer voor een lens bijvoorbeeld een zoomcapaciteit van 3x wordt vermeld, wordt verwiesen naar de verhouding tussen de langste en kortste brandpuntsafstand van de lens.

3.2.2 Passende lens en sensor

Als een netwerkcamera een verwisselbare lens heeft, is het belangrijk een lens te kiezen die geschikt is voor de camera. Een lens gemaakt voor een beeldsensor van 1/2 inch werkt bij een beeldsensor van 1/2 inch, 1/3 inch en 1/4 inch, maar niet bij een beeldsensor van 2/3 inch.

Als een lens is gemaakt voor een kleinere beeldsensor dan de sensor die in de camera is gemonteerd, zal het beeld zwarte hoeken hebben (*bekijk de linkerafbeelding in afbeelding 3.2c hieronder*). Als een lens is gemaakt voor een grotere beeldsensor dan de sensor die in de camera is gemonteerd, is het beeldveld kleiner dan de capaciteit van de lens omdat een deel van de informatie 'verloren' zal gaan buiten de beeldsensor (*bekijk de rechteraafbeelding in afbeelding 3.2c hieronder*). Deze situatie zorgt voor een telelenseffect omdat alles eruitziet alsof erop is ingezoomd.



Afbeelding 3.2c Voorbeelden van verschillende lenzen, gemonteerd op een beeldsensor van 1/3 inch.

Wanneer u een lens op een megapixelcamera vervangt, is een lens van hoge kwaliteit vereist omdat megapixelsensors pixels hebben die veel kleiner zijn dan de pixels op een VGA-sensor (640x480 pixels). Het wordt aanbevolen de lensresolutie af te stemmen op de cameraresolutie om optimaal gebruik te maken van de capaciteiten van de camera.

3.2.3 Standaarden voor lensmontage

Wanneer u een lens vervangt, is het ook belangrijk dat u het type lensmontage van de netwerk-camera kent. Er zijn twee hoofdstandaarden die voor netwerkcamera's worden gebruikt: CS-mount en C-mount. Beide hebben een schroefdraad van 1 inch (2,54 mm) en ze zien er hetzelfde uit. Het verschil is de afstand tussen de lens en de sensor als de lens is aangebracht op de camera:

- > **CS-mount.** De afstand tussen sensor en lens moet 12,5 mm zijn.
- > **C-mount.** De afstand tussen sensor en lens moet 17,526 mm zijn.

Een oude C-mount-lens kan op een camera met CS-mount worden gemonteerd met behulp van een afstandsstuk van 5 mm (C/CS-adapting). Als u een camera niet kunt scherpstellen, hebt u vermoedelijk het verkeerde type lens gebruikt.

3.2.4 F-getal en belichting

In situaties met weinig licht, in het bijzonder in binnenumgevingen, is het belangrijk dat u bij een netwerkcamera rekening houdt met de capaciteiten van de lens voor het verzamelen van licht. Dit kan worden vastgesteld door het f-getal van de lens, ook bekend als f-stop. Een f-getal bepaalt hoeveel licht er door een lens kan gaan. Een f-getal is de verhouding van de brandpuntsafstand van de lens ten opzichte van de diameter van de lensopening of de irisopening. Dat wil zeggen: f-getal = brandpuntsafstand/opening.

Hoe kleiner het f-getal (een korte brandpuntsafstand ten opzichte van lensopening of een grote lensopening ten opzichte van de brandpuntsafstand), hoe beter de capaciteit van de lens om licht te verzamelen. Dat wil zeggen dat er meer licht door de lens wordt doorgelaten naar de beeldsensor. In situaties met weinig licht, produceert een lager f-getal doorgaans een betere beeldkwaliteit. (Sommige sensors kunnen echter, vanwege de manier waarop ze zijn ontworpen, niet profiteren van een lager f-getal in situaties met weinig licht.) Anderzijds vergroot een hoger f-getal de scherppte diepte. Dit wordt uitgelegd in paragraaf 3.2.6. Een lens met een lager f-getal is gewoonlijk duurder dan een lens met een hoger f-getal.

F-getallen worden vaak genoteerd als F/x. De schuine streep geeft de deling aan. F/4 betekent dat de irisdiameter gelijk moet zijn aan de brandpuntsafstand gedeeld door 4. Als een camera een lens van 8 mm heeft, moet het licht dus door een irisopening met een diameter van 2 mm heen. Hoewel lenzen met een automatisch verstelbare iris (DC-iris) een reeks f-getallen hebben, wordt vaak alleen de maximale waarde van het bereik voor het verzamelen van licht (kleinste f-getal) vermeld. De capaciteit voor het verzamelen van licht of het f-getal van een lens en de belichtingstijd (dat wil zeggen de duur van de blootstelling van de beeldsensor aan licht) zijn de twee hoofdelementen die bepalen hoeveel licht een beeldsensor ontvangt. Een derde element is 'gain', een versterker die wordt gebruikt om het beeld helderder te maken. Het verhogen van de versterking verhoogt echter ook het niveau van de korrel (korreligheid) in een beeld, zodat de voorkeur wordt gegeven aan het aanpassen van de belichtingstijd of van de irisopening.

In sommige Axis-camera's kunnen limieten voor de belichtingstijd en gain worden ingesteld. Hoe langer de belichtingstijd, hoe meer licht een beeldsensor ontvangt. Heldere omgevingen vereisen een kortere belichtingstijd, terwijl situaties met weinig licht een langere belichtingstijd vereisen. Het is belangrijk dat u weet dat het verhogen van de belichtingstijd ook de bewegingsvervaging vergroot, terwijl het vergroten van de irisopening het nadeel heeft dat de scherptediepte wordt verminderd. Dit wordt hieronder uitgelegd in paragraaf 3.2.6.

Wanneer u beslist over de belichting, wordt een kortere belichtingstijd aanbevolen wanneer een snelle beweging of een hoge framesnelheid wordt vereist. Bij een langere belichtingstijd wordt bij een slechte verlichting de beeldkwaliteit verbeterd, maar kan de bewegingsvervaging worden vergroot en de totale framesnelheid worden vertraagd omdat er meer tijd nodig is om elk frame te belichten. Bij sommige netwerkcamera's betekent een automatische belichtingsinstelling dat de framesnelheid zal toenemen of afnemen naarmate hoeveel licht er beschikbaar is. Alleen wanneer het lichtniveau afneemt, is het belangrijk kunstlicht of een framesnelheid met voorrang of beeldkwaliteit te overwegen.



Afbeelding 3.2d De gebruikersinterface van een camera met opties voor het instellen van onder andere de belichting in situaties met weinig licht.

3.2.5 Handmatige of automatische iris

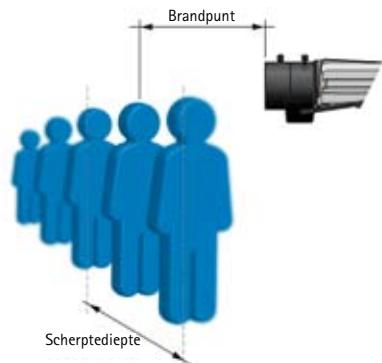
In binnenomgevingen waar constante verlichtingsniveaus mogelijk zijn, kan een handmatige irislens worden gebruikt. Dit type lens is voorzien van een ring om de iris te verstelken of de iris is vast ingesteld op een bepaald f-getal. Axis gebruikt deze laatste optie voor haar netwerkcamera's voor binnen.

Voor buitengebruik en in situaties waarin de sceneverlichting voortdurend verandert, wordt een lens met een automatisch verstelbare iris aanbevolen. De irisopening wordt bestuurd door de camera en wordt gebruikt om het optimale verlichtingsniveau voor de beeldsensor te behouden als de instellingen voor de belichting en gain niet beschikbaar zijn of niet in de netwerkcamera worden gebruikt. De iris kan ook worden gebruikt om de scherptediepte (uitgelegd in de onderstaande paragraaf) te beheren en scherpere beelden te krijgen. De meeste automatische irislens-

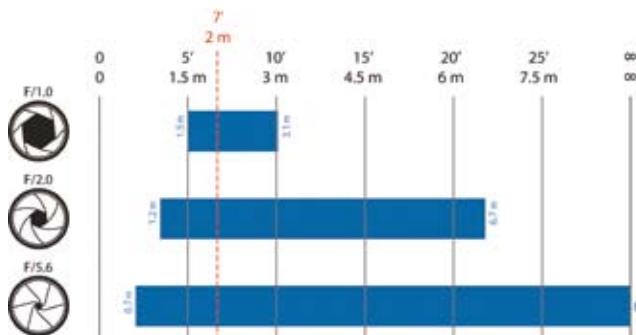
zen worden bestuurd door de processor van de camera via gelijkstroom (DC) en worden daarom 'DC-irislenzen' genoemd. Alle buitencamera's van Axis, zowel vast, vaste dome, PTZ of PTZ-dome, gebruiken DC-iris- of auto-irislenzen.

3.2.6 Scherptediepte

Een criterium dat belangrijk kan zijn voor een videosurveillancetoepassing is de scherptediepte. Scherptediepte verwijst naar de afstand voor en achter het brandpunt waar objecten tegelijk scherp lijken. De scherptediepte kan bijvoorbeeld belangrijk zijn bij het bewaken van een parkeerplaats, waar het nodig kan zijn de nummerplaten van auto's op een afstand van 20, 30 en 50 meter te herkennen. De scherptediepte wordt beïnvloed door drie factoren: brandpuntsafstand, irisdiaometer en afstand van de camera tot het onderwerp. Een lange brandpuntsafstand, een grote irisopening of een korte afstand tussen de camera en het onderwerp zullen de scherptediepte beperken.



Afbeelding 3.2e Scherptediepte: Stelt u zich een rij mensen voor die achter elkaar staan. De scherptediepte is goed als het brandpunt in het midden van de rij ligt en het mogelijk is de gezichten te herkennen van iedereen die zich meer dan 15 meter voor en achter het middelpunt bevindt.

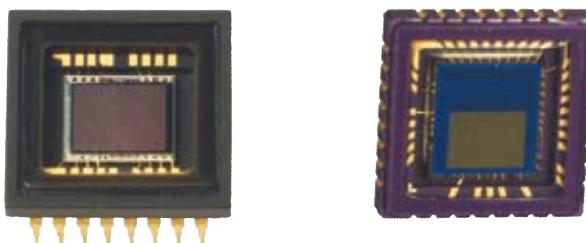


Afbeelding 3.2f Irisopening en scherptediepte. De bovenstaande afbeelding is een voorbeeld van de scherptediepte voor verschillende f-getallen met een brandpuntsafstand van 2 meter. Met een hoog f-getal (kleinere irisopening) kunnen objecten over een langere afstand worden scherpgesteld. (Afhankelijk van de pixelgrootte, kunnen zeer kleine irisopeningen een beeld vervagen door diffractie.)

3.3 Beeldsensors

Wanneer het licht door een lens gaat, wordt het scherpgesteld op de beeldsensor van de camera. Een beeldsensor is samengesteld uit meerdere photosites (lichtgevoelige diode) en elke photosite komt overeen met een beeldelement, beter bekend onder de naam "pixel", op een beeldsensor. Elke pixel op een beeldsensor registreert de hoeveelheid licht waaraan deze is blootgesteld en converteert deze in een overeenkomend aantal elektronen. Hoe helderder het licht, hoe meer elektronen worden gegenereerd. Bij de bouw van een camera kunnen er voor de beeldsensor van de camera twee hoofdtechnologieën worden gebruikt:

- > **CCD** (charge-coupled device)
- > **CMOS** (complementary metal-oxide semiconductor)



Afbeelding 3.3a Beeldsensors: CCD (links); CMOS (rechts).

Hoewel CCD- en CMOS-sensors vaak worden gezien als rivalen, heeft elk type unieke sterke en zwakke punten waardoor het geschikt is voor verschillende toepassingen. CCD-sensors worden vervaardigd volgens een technologie die speciaal voor de camera-industrie is ontwikkeld. De eerste CMOS-sensors waren gebaseerd op de standaardtechniek die al veelvuldig werd gebruikt, zoals voor geheugenchips in pc's. Moderne CMOS-sensors gebruiken een meer gespecialiseerde technologie en de kwaliteit van de sensors neemt snel toe.

3.3.1 CCD-technologie

CCD-sensors worden al meer dan 30 jaar in camera's gebruikt en beschikken over veel nuttige eigenschappen. CCD-sensors bieden doorgaans een iets betere lichtgevoeligheid dan CMOS-sensors en produceren iets minder ruis. Een grotere lichtgevoeligheid leidt tot een grotere beeldkwaliteit onder omstandigheden met weinig licht. CCD-sensors zijn echter duurder en complexer om in een camera te worden geïntegreerd. Een CCD kan ook tot 100 keer meer stroom verbruiken dan een gelijkwaardige CMOS-sensor..

3.3.2 CMOS-technologie

Recente ontwikkelingen in de technologie van de CMOS-sensors brengen deze sensor dichter bij hun CCD-tegenhanger op het vlak van beeldkwaliteit. De totaalprijs van een camera met een CMOS-sensor is lager, want deze sensor bevat alle logische schakelingen die nodig zijn voor het inbouwen in een camera. In vergelijking met CCD's bieden CMOS-sensors meer integratiemogelijkheden en meer functies. CMOS-sensors kunnen ook sneller worden uitgelezen (wat een voordeel is

wanneer beelden met hoge resolutie nodig zijn) en hebben een lagere systeemgrootte. Megapixel-CMOS-sensors zijn op grote schaal verkrijgbaar en zijn goedkoper dan megapixel-CCD-sensors.

3.3.3 Megapixelsensors

Vanwege de kosten zijn veel megapixelsensors (dit zijn sensors die een miljoen of meer pixels bevatten) in megapixelcamera's even groot of iets groter dan VGA-sensors die een resolutie bieden van 640x480 (307.200) pixels. Dit betekent dat de grootte van elke pixel op een megapixelsensor kleiner is dan op een VGA-sensor. Een megapixelsensor, zoals een 1/3-inch 2-megapixelsensor, heeft bijvoorbeeld een pixelgrootte van 3 µm (micrometer/micron) per pixel. Ter vergelijking: de pixelgrootte van een 1/3 inch VGA-sensor is 7,5 µm. Terwijl de megapixelcamera dus een hogere resolutie en meer details biedt, is dit type minder lichtgevoelig dan de VGA-tegenhanger omdat de pixels kleiner zijn en het licht dat door een object wordt weerkaatst, over meer pixels wordt gespreid.

3.4 Beeldscantechnieken

Geïnterlineerde en progressieve scanning zijn twee technieken die tegenwoordig beschikbaar zijn voor het lezen en weergeven van informatie die door de beeldsensors wordt geproduceerd. Geïnterlineerd scannen wordt hoofdzakelijk gebruikt in CCD's. Progressief scannen wordt in CCD- of CMOS-sensors gebruikt. Netwerkcamera's kunnen gebruik maken van beide scantechnieken. (Analoge camera's kunnen echter alleen de geïnterlineerde scantechniek gebruiken voor het overdragen van beelden via een coaxkabel en voor het weergeven van die beelden op analoge beeldschermen.)

3.4.1 Geïnterlineerd scannen

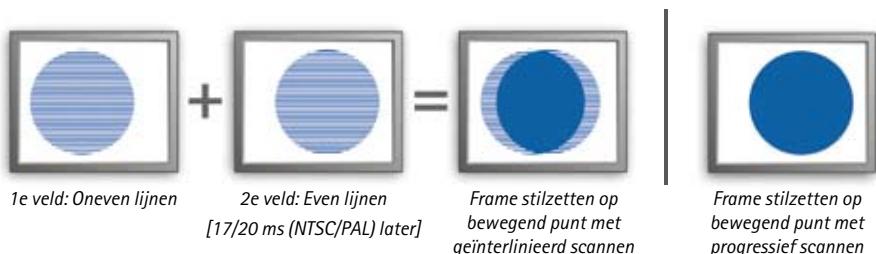
Wanneer een geïnterlineerd beeld vanaf een CCD wordt geproduceerd, worden twee velden met lijnen gegenereerd: een veld dat de oneven lijnen weergeeft en een tweede veld dat de even lijnen weergeeft. Om het oneven veld te maken, wordt echter zowel informatie van de oneven als van de even lijnen op een CCD-sensor gecombineerd. Hetzelfde geldt voor het even veld, waar informatie van zowel de even als oneven lijnen wordt gecombineerd om op elke andere lijn een beeld te vormen.

Wanneer u een geïnterlineerd beeld verzendt, wordt slechts de helft van het aantal lijnen (afwisselend tussen oneven en even lijnen) van een beeld per keer verzonden. Hierdoor wordt het gebruik van de bandbreedte met de helft verminderd. De monitor, bijvoorbeeld een gewone tv, moet ook de geïnterlineerde techniek gebruiken. Eerst worden de oneven lijnen en daarna de even lijnen van een beeld weergegeven. Daarna wordt het beeld vernieuwd met afwisselend 25 (PAL) of 30 (NTSC) frames per seconden, zodat het menselijke visuele systeem deze als volledige beelden interpreert. Alle analoge video-indelingen en enkele moderne HDTV-indelingen zijn geïnterlineerd. Hoewel de interliniëringstechniek artefacten of vervormingen creëert door 'ontbrekende' gegevens, zijn ze niet erg zichtbaar op een geïnterlineerde monitor.

Wanneer u echter geïnterlineerde video weergeeft op progressieve-scanmonitors, zoals computerschermen, die de lijnen van een beeld achtereenvolgens scannen, worden de artefacten duidelijker zichtbaar. De artefacten die als 'tearing' kunnen worden gezien, worden veroorzaakt door de lichte vertraging in het interval voor het vernieuwen van een oneven en even lijn, omdat slechts de helft van de lijnen een bewegend beeld kan bijhouden, terwijl de andere helft wacht om te worden vernieuwd. Dit zal vooral opvallen wanneer de video wordt gestopt en een stilgezet frame van de video wordt geanalyseerd.

3.4.2 Progressief scannen

Met een beeldsensor met progressieve scan worden waarden voor elke pixel op de sensor verkregen en worden alle lijnen van de beeldgegevens opeenvolgend gescand om zo een full-frame beeld te produceren. Met andere woorden: het opgenomen beeld wordt niet in verschillende velden opgesplitst, zoals bij geïnterlineerd scannen. Met progressief scannen wordt een volledig beeldframe via een netwerk verzonden en wanneer het op een computerscherm met progressieve scan wordt weergegeven, worden alleen lijnen, stuk voor stuk en in perfecte volgorde, op het scherm geplaatst. Bewegende objecten kunnen daarom beter op computerschermen worden weergegeven door middel van de progressieve scantechniek. In een videosurveillancetoepassing kan het van groot belang zijn om details te kunnen zien in een bewegend onderwerp (bijvoorbeeld van iemand die wegrent). De meeste Axis-netwerkkamera's gebruiken de progressieve scantechniek.



Afbeelding 3.4a Links wordt een geïnterlineerd scanbeeld weergegeven op een progressieve (computer) monitor. Rechts een beeld met progressieve scan op een computerscherm.



Afbeelding 3.4b Links een JPEG-afbeelding op volledig formaat (704x576 pixels) vanaf een analoge camera met geïnterlineerd scannen. Rechts een JPEG-afbeelding op volledig formaat (640x480 pixels) van een Axis-netwerkkamera met progressieve scantechnologie. Beide camera's hebben hetzelfde type lens gebruikt en de snelheid van de auto was in beide gevallen 20 km/u. De achtergrond is in beide beelden zuiver. De bestuurder is echter alleen duidelijk zichtbaar in het beeld dat de progressieve scantechnologie gebruikt.

3.5 Beeldverwerking

Er kunnen drie functies worden ondersteund in netwerkcamera's om de beeldkwaliteit te verbeteren. Deze functies zijn: achtergrondcompensatie, belichtingzones en breed dynamisch bereik.

3.5.1 Achtergrondcompensatie

Wanneer de automatische belichting van een camera probeert de helderheid van een beeld weer te geven zoals het menselijke oog een scène zou waarnemen, kan deze gemakkelijk voor de gek worden gehouden. Met een sterk tegenlicht kunnen objecten op de voorgrond donker lijken. Netwerkcamera's met achtergrondcompensatie streven ernaar beperkte gebieden met een sterke verlichting te negeren, alsof deze niet aanwezig zijn. Hierdoor zijn objecten op de voorgrond zichtbaar, hoewel de heldere gebieden overbelicht zullen zijn. Met dergelijke belichtingssituaties kan ook worden gewerkt door het dynamische bereik van de camera te vergroten. Dit wordt hieronder besproken in paragraaf 3.5.3.

3.5.2 Belichtingszones

Naast het omgaan met beperkte gebieden met een sterke verlichting, moet de automatische belichting van de netwerkcamera ook bepalen welk gebied van een beeld de belichtingswaarde moet bepalen. De voorgrond (doorgaans het onderste deel van een beeld) kan bijvoorbeeld meer belangrijke informatie bevatten dan de achtergrond, zoals de hemel (doorgaans het bovenste deel van een beeld). De algemene belichting mag niet worden bepaald door de minder belangrijke gebieden van een scene. Bij geavanceerde Axis-netwerkcamera's kan de gebruiker de belichtingszones gebruiken om het gebied van een scene - midden, links, rechts, boven of onder - te selecteren dat beter moet worden belicht.

3.5.3 Breed dynamisch bereik

Sommige netwerkcamera's van Axis bieden een breed dynamisch bereik om te kunnen omgaan met een groot aantal belichtingsomstandigheden in een scene. In een scene met extreem heldere en donkere gebieden of bij tegenlichtsituaties waar een persoon voor een helder venster staat, zal een standaard camera een beeld produceren waarin objecten in de donkere gebieden nauwelijks zichtbaar zijn. Een breed dynamisch bereik lost dit op door het toepassen van technieken, zoals het gebruik van verschillende belichtingen voor verschillende objecten in een scene, om objecten in zowel heldere als donkere gebieden zichtbaar te maken.



Afbeelding 3.5a Links beeld zonder breed dynamisch bereik. Rechts, beeld waarop een breed dynamisch bereik is toegepast.

3.6 Een netwerkcamera installeren

Nadat u een netwerkcamera hebt aangeschaft, is de manier waarop deze is geïnstalleerd, net zo belangrijk. Hieronder vindt u enkele aanbevelingen over de beste manier om videosurveillance van hoge kwaliteit te bereiken, gebaseerd op de plaatsing van de camera en de omgevingsoverwegingen.

- > **Dool van de surveillance.** Als u een overzicht wilt van een gebied om de beweging van mensen of objecten te kunnen volgen, moet u ervoor zorgen dat een camera die geschikt is voor de taak, op een positie wordt geplaatst die voldoet aan deze doelstelling. Als het de bedoeling is een persoon of object te identificeren, moet de camera zo worden geplaatst of scherpgesteld, dat deze het detailniveau vastlegt dat nodig is voor identificatiiedoelen. Het is ook mogelijk dat de plaatselijke politie u richtlijnen kan geven over de beste positie voor uw camera.
- > **Gebruik veel licht of voeg licht toe waar dat nodig is.** Het is doorgaans gemakkelijk en voordelig om sterke lampen toe te voegen aan binnen- en buitenomgevingen om de benodigde verlichtingsomstandigheden te bieden voor het vastleggen van goede beelden.
- > **Vermijd direct zonlicht** omdat dit de camera kan 'verblinden' en de prestaties van de beeldsensor kan verminderen. Plaats de camera zo, dat de zon van achter de camera komt.
- > **Vermijd tegenlicht.** Dit probleem doet zich regelmatig voor als wordt geprobeerd een object op te nemen voor een raam. Om dit probleem te vermijden, moet u de camera verplaatsen of, indien mogelijk, gordijnen gebruiken en de jaloezieën sluiten. Als het niet mogelijk is de camera te verplaatsen, kunt u ook frontale verlichting toevoegen. Camera's die een breed dynamisch bereik ondersteunen, zijn beter voor het werken met een tegenlichtscenario.
- > **Verminder het dynamische bereik van het scene.** Wanneer bij buitenomgevingen teveel lucht wordt weergegeven, kan dit leiden tot een te hoog dynamisch bereik. Als de camera geen breed dynamisch bereik ondersteunt, kunt u dit oplossen door de camera hoog boven de grond te monteren, eventueel op een paal.
- > **Pas de camera-instellingen aan.** Het kan soms nodig zijn de instellingen voor de witbalans, helderheid en scherpte aan te passen om een optimaal beeld te verkrijgen. In situaties met weinig licht moeten gebruikers altijd voorrang geven aan de framesnelheid of de beeldkwaliteit.
- > **Wettelijke overwegingen.** Videosurveillance kan worden beperkt of verboden door wetten die per land verschillen. Wij raden u aan de wetgeving in de lokale regio te raadplegen voordat u een videosurveillance-systeem installeert. Het kan bijvoorbeeld nodig zijn u te registreren of een licentie te verkrijgen voor videosurveillance, vooral in publieke gebieden. Het kan verplicht zijn om videosurveillance door middel van een bord weer te geven. Voor videoopnamen kunnen tijd- en datumstempels worden vereist. Er kunnen voorschriften zijn die bepalen hoe lang een video mag worden bewaard. Audio-opnamen kunnen worden verboden of toegestaan.

Camerabescherming en -behuizingen

Surveillancecamera's worden vaak in zeer veeleisende omgevingen geplaatst. De camera's kunnen bescherming vereisen tegen regen, warme en koude omgevingen, stof, corrosieve stoffen, trillingen en vandalisme. Fabrikanten van camera's en camera-accessoires gebruiken verschillende methoden om te voldoen aan dergelijke omgevingsuitdagingen. Oplossingen omvatten het plaatsen van camera's in afzonderlijke, beschermende behuizingen, het ontwerpen van ingebouwde cameraomhulsels voor speciale doeleinden en/of het gebruik van intelligente algoritmen die een wijziging in de gebruiksomstandigheden van een camera kunnen detecteren en gebruikers hiervan op de hoogte brengen. In de onderstaande paragrafen worden onderwerpen behandeld als afdekkingen, het plaatsen van vaste camera's in omhulsels, omgevingsbescherming, bescherming tegen vandalisme en sabotage en de montagetypes.

4.1 Cameraomhulsels in het algemeen

Wanneer de omgevingsvereisten buiten de gebruiksomstandigheden van de camera liggen, is een beschermende behuizing vereist. Camerabehuizingen worden in verschillende formaten en kwaliteiten en met verschillende functies geleverd. Behuizingen zijn vervaardigd uit metaal of plastic en kunnen doorgaans worden onderverdeeld in twee typen: vaste camerabehuizingen en domecamerabehuizingen. Wanneer u een omhulsel kiest, moet u rekening houden met verschillende zaken. Enkele daarvan zijn:

- > Zijdelingse of schuifopening (voor vaste camerabehuizingen)
- > Montagebeugels
- > Doorzichtige of rookkleurige koepel (voor domecamerabehuizingen)
- > Kabelbeheer
- > Temperatuur en andere waarden (overweeg de behoefte aan een verwarmingsapparaat, een zonnescherm, een ventilator en ruitenwissers)
- > Voeding (12 V, 24 V, 110 V, enz.)
- > Niveau van vandalismebestendigheid

Enkele behuizingen hebben ook randapparatuur, zoals antennes voor draadloze toepassingen. Een externe antenne is alleen vereist als de behuizing van metaal is gemaakt. De draadloze camera in een plastic behuizing werkt zonder het gebruik van een externe antenne.

4.2 Doorzichtige afschermkap

Het 'raam' of de doorzichtige beschermkap van een omhulsel is doorgaans vervaardigd uit glas van hoge kwaliteit of uit duurzaam, polycarbonaat plastic. Omdat ramen werken als optische lenzen, moeten deze van hoge kwaliteit zijn om het effect op de beeldkwaliteit te minimaliseren. Wanneer er ingebouwde onvolkomenheden zijn in het doorzichtige materiaal, wordt de helderheid beïnvloed. Er worden hogere eisen gesteld aan de vensters van de behuizingen voor PTZ-camera's en PTZ domecamera's. De ramen moeten niet alleen een speciale vorm hebben in de vorm van een koepel, maar deze moeten ook een hoge helderheid hebben omdat onvolkomenheden, zoals vuildeeltjes, kunnen worden vergroot, vooral wanneer camera's met een hoge zoomfactor zijn geïnstalleerd. Als de dikte van het raam bovendien ongelijkmatig is, kan een rechte lijn er gebogen uitzien in het resulterende beeld. Een koepel van hoge kwaliteit mag zeer weinig invloed hebben op de beeldkwaliteit, ongeacht het zoomniveau en de lenspositie van de camera.

De dikte van een koepel kan worden verhoogd om bestand te zijn tegen zware klappen, maar hoe dikker de afschermkap, hoe meer kans er bestaat op onvolkomenheden. Een grotere dikte kan ook ongewenste weerkaatsing en breking van het licht vormen. Dikke afschermkappen moeten daarom voldoen aan hogere vereisten als het effect op de beeldkwaliteit moet worden geminimaliseerd.

Er zijn verschillende dome-afschermkappen of koepels beschikbaar in doorzichtige of rookkleurige versies. Naast het feit dat de rookkleurige versies een discretere installatie bieden, doen deze ook in hoge mate dienst als een soort zonnebril door de hoeveelheid licht waarover de camera beschikt te verminderen. Dit zal dan ook invloed hebben op de lichtgevoeligheid van de camera.

4.3 Een vaste camera in een behuizing plaatsen

Wanneer u een vaste camera in een omhulsel installeert, is het belangrijk dat de lens van de camera vlak tegen het raam is geplaatst om eventuele schittering te voorkomen. Anders verschijnen weerspiegelingen van de camera en de achtergrond in het beeld. Om de weerspiegeling te verminderen kan een speciale deklaag worden aangebracht op het glas voor de lens.

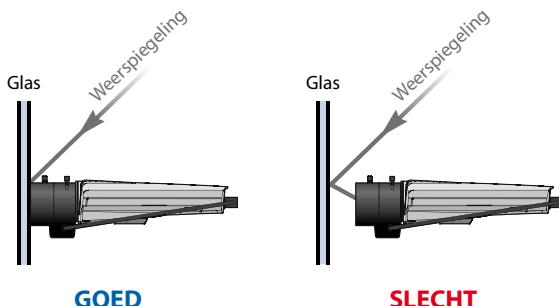


Figure 4.3a Wanneer u een camera achter glas installeert, is de correcte plaatsing van de camera belangrijk om weerspiegeling te voorkomen.

4.4 Omgevingsbescherming

De belangrijkste omgevingsbedreigingen voor een camera – vooral een camera die buitenshuis is geïnstalleerd – zijn kou, warmte, water en stof. Behuizingen met ingebouwde verwarmingsapparaten en ventilators (blazers) kunnen worden gebruikt in omgevingen met lage en hoge temperaturen. In warme omgevingen kunnen camera's worden geplaatst in omhulsels die een actieve koeling hebben met een afzonderlijke warmtewisselaar. Om bestand te zijn tegen water en stof, worden de behuizingen (vaak met een IP66-classificatie) nauwkeurig verzegeld. In situaties waar camera's kunnen worden blootgesteld aan zuren, zoals in de voedingssector, worden behuizingen in roestvrij staal vereist. Sommige gespecialiseerde behuizingen kunnen onder druk worden gezet, ze kunnen worden ondergedompeld, kogelbestendig worden gemaakt of worden ontworpen voor installatie in potentieel explosieve locaties. Er kunnen ook speciale omhulsels worden gevraagd uit esthetische overwegingen.

Andere omgevingselementen zijn onder andere wind en verkeer. Om trillingen te voorkomen, vooral op camera-installaties die op een paal zijn gemonteerd, is een kleine en veilig gemonterde behuizing ideaal. De termen 'binnenbehuizing' en 'buitenbehuizing' verwijzen vaak naar het niveau van de omgevingsbescherming. Een binnenbehuizing wordt vooral gebruikt om het binnendringen van stof te voorkomen en bevat geen verwarming en/of ventilator. De termen zijn misleidend omdat de locatie, zowel binnen als buiten, niet altijd overeenkomt met de omstandigheden op de installatielocatie. Een camera die bijvoorbeeld in een vrieskamer wordt geplaatst, zal een 'buitenbehuizing' vereisen met een verwarmingsapparaat.

Het beschermingsniveau dat door een omhulsel wordt geboden, of het nu ingebouwd of los van de camera wordt geleverd, wordt vaak aangegeven door de classificaties die zijn bepaald door standaarden zoals IP, de afkorting voor Ingress Protection (soms ook bekend als de International Protection), en die in de hele wereld van toepassing zijn; NEMA(National Electrical Manufacturers Association) in de VS.; en IK-classificaties voor externe mechanische invloeden die van toepassing zijn in Europa. Wanneer een camera in een potentieel explosieve omgeving moet worden geïnstalleerd, zijn andere standaarden aan de orde, zoals IECEx, een wereldwijde certificering en ATEX, een Europese certificering. *Meer informatie over de IP-classificatie vindt u hier: www.axis.com/products/cam_housing/ip66.htm*

4.5 Bescherming tegen vandalisme en sabotage

In sommige surveillancetoepassingen zijn camera's blootgesteld aan vijandige en gewelddadige aanvallen. Hoewel een camera of de behuizing nooit in elke situatie 100% bescherming kan garanderen tegen destructief gedrag, kan vandalisme worden beperkt door rekening te houden met verschillende aspecten: camera-/behuizingsontwerp, montage, plaatsing en gebruik van een intelligent video-alarm.

4.5.1 Camera/behuizingsontwerp

Behuizingen en verwante componenten die uit metaal zijn vervaardigd, bieden een betere bescherming tegen vandalen dan behuizingen in plastic. De vorm van de behuizing of camera is

een andere factor. Een behuizing of een traditionele vaste camera die uitsteekt uit een muur of plafond is kwetsbaarder voor aanvallen (bijv. trappen of slaan) dan meer discreet ontworpen behuizingen of omhulsels voor een vaste dome of PTZ-domecamera. De zachte, ronde afschermkap van een vaste dome of PTZ-dome maakt het bijvoorbeeld moeilijker het beeldveld van de camera te blokkeren door een kledingstuk over de camera te hangen. Hoe meer een behuizing of camera een geheel vormt met een omgeving of wordt vermomd als iets anders dan een camera, zoals een buitenlamp, hoe beter de camera tegen vandalisme is beschermd.



Afbeelding 4.5a Voorbeelden van vaste camerabehuizingen. Alleen de behuizingen in het midden en rechts zijn geclasseerd als vandalismebestendig.



Afbeelding 4.5b Voorbeelden van vandalismebestendige behuizingen voor een kleine of compacte vaste netwerk-camera (links), voor een vaste domenetwerkcamera (midden) en voor een PTZ-camera (rechts).

4.5.2 Montage

Ook de manier waarop camera's en behuizingen worden gemonteerd, is belangrijk. Een traditionele vaste netwerkcamera en een PTZ-domecamera die op het oppervlak van een plafond is gemonteerd, zijn kwetsbaarder voor aanvallen dan een vaste dome of PTZ-domecamera die gelijk met het plafond of de muur is gemonteerd, waarbij alleen het doorzichtige deel van de camera of behuizing zichtbaar is.



Afbeelding 4.5c Voorbeelden van gelijk met het plafond gemonteerde behuizingen voor vaste netwerkcamera's.

Een andere belangrijke overweging is de manier waarop de bekabeling op een camera wordt gemonteerd. Hier wordt een maximale bescherming geboden wanneer de kabel direct door de muur of het plafond achter de camera wordt getrokken. Hierdoor zijn er geen zichtbare kabels

waarmee kan worden geknoeid. Als dat niet mogelijk is, moet een metalen elektriciteitsbuis worden gebruikt om kabels tegen aanvallen te beschermen.

4.5.3 Plaatsing van de camera

De plaatsing van de camera is ook een belangrijke factor in het ontmoedigen van vandalisme. Door een camera buiten bereik op hoge muren of aan het plafond te bevestigen, kunnen veel impulsieve aanvallen worden voorkomen. Het nadeel kan de beeldhoek zijn die echter enigszins kan worden gecompenseerd door een andere lens te selecteren.

4.5.4 Intelligente video

De functie voor het actieve tamperingalarm van Axis helpt u de camera's te beschermen tegen vandalisme. Deze functie kan detecteren of een camera in een andere richting is geplaatst, is verduisterd of gesaboteerd en kan een alarm naar de operator sturen. Dit is vooral nuttig bij installatie met honderden camera's in veeleisende omgevingen waar het controleren van de juiste werking van alle camera's zeer moeilijk is. Het is ook nuttig in situaties waar de beelden niet live worden weergegeven en operators op de hoogte kunnen worden gebracht wanneer er camera's werden gesaboteerd.

4.6 Montagetypen

De camera's moeten op alle soorten locaties worden geplaatst en dit vereist een groot aantal variaties in het type montage.

4.6.1 Plafondmontages

Plafondmontages worden vooral gebruikt in installaties binnenshuis. Het omhuisel zelf kan het volgende type zijn:

- > **Een oppervlaktemontage:** wordt direct op het oppervlak van een plafond gemonteerd en is daarom volledig zichtbaar.
- > **Een vlakke montage:** wordt in het plafond gemonteerd waarbij alleen delen van een camera en behuizing (doorgaans de koepel) zichtbaar zijn.
- > **Een hangende montage:** een behuizing die aan een plafond wordt gehangen zoals een kroonluchter.



Afbeelding 4.6a Een voorbeeld van een oppervlaktemontage (links), een vlakke montage (midden) en een hangende montage (rechts).

4.6.2 Wandmontages

Wandmontages worden vaak gebruikt om camera's binnen of buiten een gebouw te monteren. De behuizing is verbonden met een arm die op een muur wordt gemonteerd. Geavanceerde montagesystemen bevatten een kabelpacking binnenzijde om de kabel te beschermen. Om een omhulsel in een hoek van een gebouw te installeren, kan een normale wandmontage in combinatie met een extra hoekadapter worden gebruikt. Andere speciale montages zijn onder andere een pendant-kit-montage waarmee een vaste netwerkkamera kan worden gemonteerd in een stijl die lijkt op een PTZ-domebehuizing.



Afbeelding 4.6b Een voorbeeld van een wandmontage met een hangmontagekit voor een vaste domecamera.

4.6.3 Paalmontages

Op locaties zoals een parkeerterrein, wordt een paalmontage vaak samen met een PTZ-camera gebruikt. Dit type montage houdt doorgaans rekening met de invloed van de wind. De afmetingen van de paal en de montage zelf moeten zijn ontwikkeld om trillingen te minimaliseren. Kabels zijn vaak in de paal ingesloten en de uitgangen moeten goed worden afgedicht. Meer geavanceerde PTZ-domecamera's hebben ingebouwde elektronische beeldstabilisatie om de effecten van wind en trillingen te beperken.

4.6.4 Relingmontages

Relingmontages worden gebruikt voor op het dak gemonteerde behuizingen of om de camera hoger te plaatsen voor een betere beeldhoek.



Afbeelding 4.6c Een voorbeeld van een relingmontage.

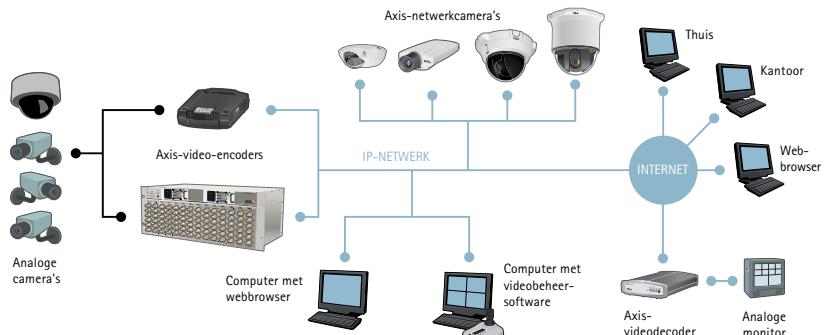
Axis biedt een online hulpmiddel dat gebruikers helpt de juiste behuizing en de benodigde montageaccessoires te herkennen. Bezoek www.axis.com/products/video/accessories/configurator/

Video-encoders

Dankzij video-encoders, ook bekend als videoservers, kan een bestaand analoog CCTV-videosurveillance-systeem in een netwerkvideosysteem worden geïntegreerd. Video-encoders spelen een belangrijke rol in installaties waar vele analoge camera's moeten worden onderhouden. In dit hoofdstuk wordt beschreven wat een video-encoder is en wat de voordelen ervan zijn. Daarnaast vindt u hier een overzicht van alle onderdelen en de verschillende types video-encoders die verkrijgbaar zijn. Naast een paragraaf over videodecoders is er ook een korte besprekking van de interliniëringstechnieken.

5.1 Wat is een video-encoder?

Een video-encoder biedt een analoog CCTV-systeem de mogelijkheid te migreren naar een netwerkvideosysteem. Hierdoor kunnen gebruikers profiteren van de voordelen van netwerkvideo, zonder dat ze analoge uitrusting, zoals analoge CCTV-camera's en coaxiale bekabeling, moeten weggooien. Een video-encoder wordt via een coaxkabel aangesloten op een analoog videocamera en converteert analoge videosignalen naar digitale videostromen die vervolgens via een bekabeld of draadloos IP-netwerk (bijv. LAN, WLAN of internet) worden verzonden. Om digitale video weer te geven en/of op te nemen, kunnen computerschermen en pc's worden gebruikt in plaats van DVR's of videorecorders en analoge beeldschermen.



Afbeelding 5.1a Een illustratie van de manier waarop analoge videocamera's en analoge beeldschermen kunnen worden geïntegreerd in een netwerkvideosysteem met video-encoders en -decoders.

Dankzij het gebruik van video-encoders, zijn analoge videocamera's van alle types, zoals vaste, binnen/buiten-dome, pan/tilt/zoom en gespecialiseerde camera's zoals de zeer gevoelige thermische camera's en microscoopcamera's, extern toegankelijk en kunnen ze van op afstand worden bestuurd via een IP-netwerk. Een video-encoder biedt ook andere voordelen zoals gebeurtenisbeheer, intelligente videofuncties en geavanceerde beveiligingsmaatregelen. Daarnaast biedt de encoder schaalbaarheid en een gemakkelijke integratie in andere beveiligingssystemen.



Afbeelding 5.1b Een zelfstandige, eenkanaals video-encoder met audio, I/O-aansluitingen (ingang/uitgang) voor het besturen van externe apparaten zoals sensors en alarmen, seriële poorten (RS-422/485) voor het besturen van analoge PTZ-camera's en etherjetaansluiting met PoE-ondersteuning (Power over Ethernet).

5.1.1 Componenten van de video-encoder en overwegingen

Video-encoders van Axis bieden veel functies die ook bij netwerkkamera's beschikbaar zijn. Hieronder vindt u enkele van de hoofdcomponenten van de video-encoder:

- > Analoge video-ingang voor het aansluiten van een analoge camera met een coaxkabel.
- > Processor voor het uitvoeren van het besturingssysteem van de video-encoder, netwerk- en beveiligingsfuncties, voor het coderen van analoge video's met verschillende compressieformaten en voor videoanalyse. De processor bepaalt de prestaties van een video-encoder. Deze worden doorgaans gemeten in beelden per seconde in de hoogste resolutie. Geavanceerde video-encoders kunnen een volledige beeldsnelheid (30 beelden per seconde met analoge NTSC-camera's of 25 beelden per seconde met analoge PAL-camera's) bieden in de hoogste resolutie voor elk videokanaal. Video-encoders beschikken ook over de automatische sensor om automatisch te herkennen of het binnenvkomende analoge videosignaal een NTSC- of PAL-standaard is. *Raadpleeg Hoofdstuk 6 voor meer informatie over NTSC- en PAL-resoluties.*
- > Geheugen voor het opslaan van de firmware (computerprogramma) met flash en voor het opslaan in een buffergeheugen van videobeelden (met RAM).
- > Ethernet/PoE-poort (Power over Ethernet) om een verbinding te maken met een IP-netwerk voor het verzenden en ontvangen van gegevens en voor het aandrijven van de eenheid en de aangesloten camera als Power over Ethernet wordt ondersteund. *Raadpleeg Hoofdstuk 9 voor meer informatie over Power over Ethernet (PoE).*

- > Seriële poort (RS-232/422/485), vaak gebruikt voor het besturen van de pan/tilt/zoom-functionaliteit van een analoge PTZ-camera.
- > Ingangen/uitgangen voor het aansluiten van externe apparaten, zoals sensors om een alarmgebeurtenis te detecteren, en relais om bijv. een lampje in te schakelen als reactie op een gebeurtenis.
- > Audio-ingang voor het aansluiten van een microfoon of een apparaat met lijningang, en audio-uitgang voor het aansluiten van luidsprekers.

Video-encoders voor professionele systemen moeten voldoen aan hoge eisen op het vlak van betrouwbaarheid en kwaliteit. Wanneer u een video-encoder kiest, moet u ook andere zaken overwegen, zoals het aantal ondersteunde analoge kanalen, de beeldkwaliteit, compressieformaten, de resolutie, de beeldsnelheid en eigenschappen zoals pan/tilt/zoom-ondersteuning, audio, gebeurtenisbeheer, intelligente video, Power over Ethernet en beveiligingsfunctionaliteiten.

5.1.2 Gebeurtenisbeheer en intelligente video

Een van de belangrijkste voordelen van video-encoders van Axis is de mogelijkheid functies te bieden voor gebeurtenisbeheer en intelligente video. Dit zijn capaciteiten die niet door een analoog videosysteem kunnen worden geleverd. Dankzij ingebouwde videofuncties, zoals bewegingsdetectie in een video met meerdere vensters, audiodetectie, een actief tamperingalarm en ingangen voor externe sensors, kan een videosurveillance-systeem via een netwerk voortdurend alert zijn om een gebeurtenis te detecteren. Zodra een gebeurtenis wordt gedetecteerd, kan het systeem automatisch reageren met acties zoals het maken van video-opnamen, het verzenden van waarschuwingen per e-mail of sms, het inschakelen van lichten, het openen of sluiten van deuren of het activeren van alarmen. *Raadpleeg Hoofdstuk 11 voor meer informatie over gebeurtenisbeheer en intelligente video.*

5.2 Zelfstandige video-encoders

Het gebruikelijkste type video-encoder is de zelfstandige versie die een- of meerkanals (vaak 4) aansluitingen voor analoge camera's biedt; een meerkanals video-encoder is ideaal voor situaties waarin er verschillende analoge camera's op een externe locatie zijn geïnstalleerd of die zich op een redelijke afstand van de centrale controlekamer bevinden. Via de meerkanals video-encoder, kunnen videosignalen van externe camera's dezelfde netwerkbekabeling gebruiken waardoor de kosten voor de bekabeling worden beperkt.

In situaties waarin er werd geïnvesteerd in analoge camera's, maar er nog geen coaxkabels zijn geïnstalleerd, is het aanbevolen zelfstandige video-encoders dicht bij de analoge camera's te gebruiken en te plaatsen. Dit beperkt de installatiekosten aangezien het hierdoor niet nodig is nieuwe coaxkabels naar een centrale locatie te trekken omdat de video via een Ethernet-netwerk kan worden verzonden. Hierdoor is er ook geen sprake van het verlies van beeldkwaliteit

dat optreedt als video over grote afstanden wordt verzonden via coaxkabels. Bij coaxkabels neemt de videokwaliteit af naarmate de signalen een grotere afstand moeten overbruggen. Een video-encoder produceert digitale beelden, zodat de beeldkwaliteit niet afneemt door de afstand die is aangelegd door een digitale videostroom.



Afbeelding 5.2a *Een illustratie van de manier waarop een kleine, eenkanaals video-encoder naast een analoge camera kan worden geplaatst in een camerabehuizing.*

5.3 In rekken gemonteerde video-encoders

In rekken gemonteerde video-encoders bewijzen hun nut wanneer grote aantallen analoge camera's via coaxkabels met een speciale regelkamer zijn verbonden. Hierdoor kunnen talrijke analoge camera's worden verbonden en beheerd vanaf één rack op een centrale locatie. In een rack kunnen meerdere verschillende video-encoderblades worden gemonteerd, waardoor u een flexibele, uitbreidbare oplossing met een hoge dichtheid wordt geboden. Een video-encoderblade kan één, vier of zes analoge camera's ondersteunen. Een blade kan worden gezien als een video-encoder zonder behuizing, maar kan niet zelfstandig werken. Hiervoor moet de blade in een rack worden gemonteerd.



Afbeelding 5.3a *Wanneer de AXIS Q7900 Rack (hier weergegeven) is volledig uitgerust met 6-kanaals video-encoderblades, biedt deze plaats voor maar liefst 84 analoge camera's.*

Video-encoderracks van Axis ondersteunen functies zoals hot swapping van blades. D.w.z. dat de blades kunnen worden verwijderd of geïnstalleerd zonder dat u het rack hoeft uit te schakelen. De racks zijn ook voorzien van seriële communicatiepoorten en in-/uitgangen voor elke video-encoderblade, naast een standaard voeding en gedeelde Ethernet-netwerkverbinding(en).

5.4 Video-encoders met PTZ- en PTZ-dome-camera's

In een netwerkvideosysteem, worden de pan/tilt/zoom-opdrachten vanaf een bedieningspaneel overgedragen via hetzelfde IP-netwerk als de videotransmissie en doorgestuurd naar de analoge PTZ- of PTZ-dome-camera via de seriële poort van de video-encoder (RS-232/422/485). Dankzij video-encoders is het daarom mogelijk analoge PTZ-camera's te besturen over lange afstanden,

zelfs via het internet. (in een analoog CCTV-systeem zou elke PTZ-camera voor de hele weg tot bij de camera, afzonderlijke en specifieke seriële bekabeling vanaf het bedieningspaneel, met joystick en andere bedieningsknoppen, vereisen.)

Om een specifieke PTZ-camera te besturen, moet een stuurprogramma worden geüpload naar de video-encoder. Veel fabrikanten van video-encoders bieden PTZ-stuurprogramma's voor de meeste analoge PTZ- en PTZ-dome-camera's. Er kan ook een PTZ-stuurprogramma worden geïnstalleerd op de pc waarop de videobeheersoftware wordt uitgevoerd als de seriële poort van de video-encoder is ingesteld als een seriële server die de opdrachten alleen doorgeeft.



Afbeelding 5.4a Een analoge PTZ-dome-camera kan worden bestuurd via de seriële poort van de video-encoder (bijv. RS-485) zodat de camera extern kan worden beheerd via een IP-netwerk.

De meest gebruikte seriële poort voor het besturen van PTZ-functies is de RS-485. Een van de voordelen van de RS-485 is het feit dat het de mogelijkheid biedt meerdere PTZ-camera's te besturen met getwiste paren draden in een serieverbinding van de ene dome-camera naar de andere. De maximale afstand van een RS-485-kabel, zonder het gebruik van een versterker, bedraagt 1.220 meter bij baudrates tot 90 kbit/s.

5.5 Deïnterliniëringstechnieken

Video van analoge camera's is ontworpen om te worden weergegeven op analoge beeldschermen zoals traditionele tv-toestellen, die een techniek gebruiken die geïnterlineerd scannen wordt genoemd. Met geïnterlineerd scannen, worden twee opeenvolgende geïnterlineerde lijnvelden weergegeven om een beeld te vormen. Wanneer dergelijke video wordt weergegeven op een computerscherm die een andere techniek met de naam progressief scannen gebruikt, worden de interliniërende effecten (d.i. scheur- of kameffect) van bewegende beelden zichtbaar. Om ongewenste interliniëringseffecten te beperken, kunnen verschillende deïnterliniëringstechnieken worden gebruikt. Bij geavanceerde video-encoders van Axis hebben gebruikers de keuze tussen twee verschillende deïnterliniëringstechnieken: adaptieve interpolatie en overvloeien.



Afbeelding 5.5a Links, een close-up van een geïnterlineerd beeld, weergegeven op een computerscherm; rechts, hetzelfde geïnterlineerde beeld waarop de deïnterliniëringstechniek is toegepast.

Adaptieve interpolatie biedt de beste beeldkwaliteit. De techniek bestaat eruit slechts één van de twee opeenvolgende velden te gebruiken en interpolatie te gebruiken om het andere lijnenveld te maken om een volledig beeld te vormen.

Bij **overvloei(en)** worden twee opeenvolgende velden samengevoegd en worden ze als één beeld weergegeven zodat alle velden aanwezig zijn. Het beeld wordt vervolgens gefilterd voor het verzachten van de bewegingsartefacten of het "kameffect" dat wordt veroorzaakt door het feit dat twee velden op licht verschillende tijdstippen werden vastgelegd. De overvloeitechniek vereist niet zoveel vermogen van een processor als de adaptieve interpolatie.

5.6 Videodecoder

Een videodecoder decodeert digitale video en audio die afkomstig is van een video-encoder of netwerkcamera, in analoge signalen. Deze signalen kunnen vervolgens worden gebruikt door analoge monitors, zoals standaard tv-toestellen en videoswitches. Een typische situatie zou zich kunnen voordoen in een detailhandelomgeving waarin traditionele monitoren worden gebruikt in publieke ruimten om te laten zien dat er videosurveillance is.

Aan andere gebruikelijke toepassing voor videodecoders is het gebruik in een analoog-naar-digitaal-naar-analoog configuratie voor het transporteren van videobeelden over grote afstanden. De kwaliteit van digitale video wordt niet beïnvloed door de afgelegde afstand. Dit is niet het geval wanneer analoge signalen over lange afstanden worden verzonden. Het enige nadeel kan een zeker niveau van latentie zijn, van 100 ms tot enkele seconden, afhankelijk van de afstand en de kwaliteit van het netwerk tussen de eindpunten.



Afbeelding 5.6a *Encoders en decoders kunnen worden gebruikt om video van een analoge camera naar een analoge monitor over grote afstanden te transporteren.*

Een videodecoder heeft de capaciteit om video's van meerdere camera's achtereenvolgens te decoderen en weer te geven. D.w.z. dat de video van de ene camera wordt gedecodeerd en enkele seconden wordt weergegeven voordat wordt overgeschakeld naar de volgende camera.

Resoluties

Resolutie in een analoge en een digitale omgeving is vergelijkbaar, maar er zijn enkele belangrijke verschillen in de gebruikte definities. Bij analoge video bestaat een beeld uit lijnen, zogenaamde televisielijnen, omdat de analoge videotechnologie is voortgekomen uit de televisie-industrie. In een digitaal systeem is een beeld opgebouwd uit vierkante pixels. In de onderstaande paragrafen vindt u een beschrijving van de verschillende resoluties die netwerkvideo kan bieden. Dit zijn onder andere NTSC, PAL, VGA, megapixel en HDTV.

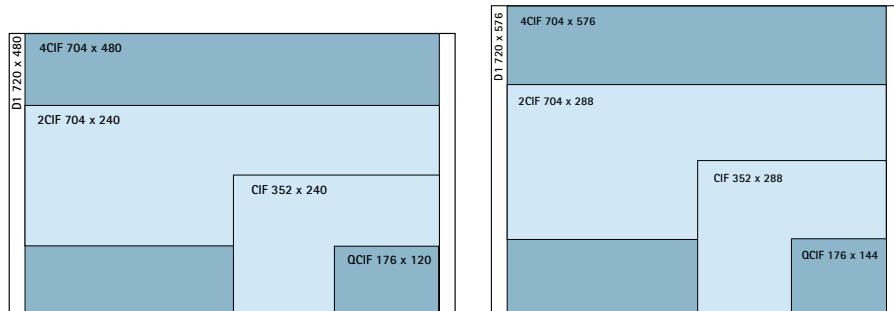
6.1 NTSC- en PAL-resoluties

NTSC- (National Television System Committee) en PAL-resoluties (Phase Alternating Line) zijn analoge videostandaarden. Deze zijn relevant voor netwerkvideo omdat video-encoders dergelijke resoluties bieden wanneer ze signalen van analoge camera's digitaliseren. De huidige PTZ- en PTZ-dome-netwerkcamera's bieden ook NTSC- en PAL-resoluties omdat dergelijke camera's tegenwoordig een camerablok gebruiken (waarin de camera-, zoom-, autofocus- en auto-iris-functies zijn opgenomen), die zijn gemaakt voor analoge videocamera's, in combinatie met een ingebouwd video-encoderbord.

In Noord-Amerika en Japan is de NTSC-standaard de meest gebruikte standaard voor analoge video. In Europa en veel Aziatische en Afrikaanse landen wordt de PAL-standaard gebruikt. Beide standaarden komen oorspronkelijk voort uit de televisie-industrie. NTSC heeft een resolutie van 480 lijnen en gebruikt een vernieuwingsfrequentie van 60 geïnterlineerde velden per seconde (of 30 volledige frames per seconde). Een nieuwe naamgevingsconventie die het aantal lijnen, het type scan en de vernieuwingsfrequentie definieert voor deze standaard, is 480i60 ("i" staat voor geïnterlineerd scannen). PAL heeft een resolutie van 576 lijnen en gebruikt een vernieuwingsfrequentie van 50 geïnterlineerde velden per seconde (of 25 volledige frames per seconde). De nieuwe naamgevingsconventie voor deze standaard is 576i50. De totale hoeveelheid informatie per seconde is voor beide standaarden gelijk.

Bij het digitaliseren van analoog videomateriaal hangt het maximale aantal pixels dat kan worden gecreëerd, af van het aantal televisielijnen dat beschikbaar is voor digitalisering. De maximale grootte van een gedigitaliseerd beeld is standaard D1 en de meest gebruikte resolutie is 4CIF.

Wanneer een gedigitaliseerde analoge video wordt weergegeven op een computerscherm, kunnen interliniërings-effecten zoals tearing verschijnen en kunnen de vormen enigszins zijn vervormd omdat de pixels die worden gegenereerd, mogelijk niet overeenkomen met de vierkante pixels op het computerscherm. Interliniërings-effecten kunnen worden verminderd door middel van deinterliniërings-technieken (zie Hoofdstuk 5), terwijl de correctie van de beeldverhouding op video kan worden toegepast voordat deze wordt weergegeven. Hierdoor bent u er bijvoorbeeld van verzekerd dat een cirkel in een analoge video een cirkel blijft wanneer deze op een computerscherm wordt weergegeven.



Afbeelding 6.1a Links verschillende NTSC-beeldresoluties. Rechts verschillende PAL-beeldresoluties.

6.2 VGA-resoluties

Bij systemen die 100% digitaal zijn en op netwerkkamera's zijn gebaseerd, kunnen resoluties worden geboden die zijn afgeleid van de computersector en die wereldwijd zijn gestandaardiseerd. Dit biedt ook een betere flexibiliteit. De beperkingen van NTSC en PAL zijn dan irrelevant. VGA (Video Graphics Array) is een grafisch weergavesysteem voor pc's dat oorspronkelijk is ontwikkeld door IBM. De resolutie is gedefinieerd als 640x480 pixels. Dit is een algemene indeling die door niet-megapixel-netwerkkamera's wordt gebruikt. De VGA-resolutie is doorgaans geschikter voor netwerkkamera's omdat op VGA-gebaseerde video vierkante pixels produceert die overeenkomen met de pixels op computerschermen. Computermonitoren kunnen resoluties in VGA of meervouden van VGA verwerken.

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

Tabel 6.2 VGA-resoluties..

6.3 Megapixelresoluties

Een netwerkcamera die een megapixelresolutie biedt, gebruikt een megapixelsensor om een beeld te leveren dat één miljoen of meer pixels bevat. Hoe meer pixels een sensor heeft, hoe meer potentieel de sensor heeft voor het vastleggen van fijnere details en voor het produceren van een beeld met hogere kwaliteit. Megapixelnetwerkcamera's kunnen worden gebruikt zodat gebruikers meer details kunnen zien (ideaal voor de identificatie van mensen en objecten) of om een groter gebied van een scene weer te geven. Dit voordeel is een belangrijke overweging bij videosurveillancetoepassingen.

Beeldschermformaat	Aantal megapixels	Pixels
SXGA	1,3 megapixels	1280x1024
SXGA+ (EXGA)	1,4 megapixels	1400x1050
UXGA	1,9 megapixels	1600x1200
WUXGA	2,3 megapixels	1920x1200
QXGA	3,1 megapixels	2048x1536
WQXGA	4,1 megapixels	2560x1600
QSXGA	5,2 megapixels	2560x2048

Tabel 6.3 Enkele megapixelindelingen.

De megapixelresolutie is één gebied waarop netwerkcamera's uitblinken ten opzichte van analoge camera's. De maximale resolutie die een conventionele analoge camera kan bieden nadat het video-signalen gedigitaliseerd in een digitale videorecorder of een video-encoder, is D1, d.w.z. 720x480 pixels (NTSC) of 720x576 pixels (PAL). De D1-resolutie komt overeen met maximaal 414.720 pixels of 0,4 megapixel. Ter vergelijking: een gebruikelijke megapixelindeling van 1280x1024 pixels geeft een resolutie van 1,3 megapixel. Dit is meer dan driemaal de resolutie die door analoge CCTV-camera's kan worden geleverd. Netwerkcamera's met 2 en 3 megapixels zijn ook verkrijgbaar en in de toekomst zullen er naar verwachting nog hogere resoluties volgen.

De megapixelresolutie biedt ook een hogere mate van flexibiliteit om beelden met verschillende beeldverhoudingen te leveren. (Beeldverhouding is de verhouding tussen de breedte en de hoogte van een beeld.) Een conventionele tv-monitor toont een beeld met een beeldverhouding van 4:3. Megapixelnetwerkcamera's van Axis kunnen, naast andere verhoudingen, ook dezelfde verhouding bieden, zoals 16:9. Het voordeel van de 16:9-beeldverhouding is dat onbelangrijke details die zich doorgaans in het bovenste of onderste deel van een beeld met conventioneel formaat bevinden, niet aanwezig zijn. Hierdoor kunnen de bandbreedte en de opslagvereisten worden beperkt.



Afbeelding 6.3a Illustratie van de beeldverhoudingen 4:3 en 16:9.

6.4 HDTV-resoluties (High-definition television)

HDTV biedt een resolutie die maximaal vijfmaal hoger is dan bij standaard analoge tv. HDTV heeft ook een betere kleurechtigheid en een 16:9-beeldverhouding. De twee belangrijkste HDTV-standaarden die door SMPTE (Society of Motion Picture and Television Engineers) zijn gedefinieerd, zijn SMPTE 296M en SMPTE 274M.

SMPTE 296M (HDTV 720P) definieert een resolutie van 1280x720 pixels met hoge kleurechtigheid in een 16:9-beeldverhouding met progressieve scanning bij 25/30 Hertz (Hz), wat overeenkomt met 25 of 30 frames per seconde, afhankelijk van het land en bij 50/60 Hz (50/60 frames per seconde).

SMPTE 274M (HDTV 1080) definieert een resolutie van 1920x1080 pixels met hoge kleurechtigheid in een 16:9-beeldverhouding met geïnterlinieerd of progressief scannen bij 25/30 Hz en 50/60Hz. Een camera die voldoet aan de SMPTE-standaarden, geeft aan dat de HDTV-kwaliteit wordt gevuld en dient alle voordelen van HDTV te hebben met betrekking tot resolutie, kleurechtigheid en beeldsnelheid.

De HDTV-standaard is gebaseerd op vierkante pixels, zoals bij computerschermen. HDTV-video van netwerkvideoproducten kan daarom zowel op HDTV-schermen als op standaard computerschermen worden weergegeven. Bij HDTV-video met progressieve scan hoeft er geen conversie of deïnterlinieringstechniek worden toegepast wanneer de video door een computer moet worden verwerkt of op een computerscherm moet worden weergegeven.

Videocompressie

Bij videocompressietechnologieën gaat het om het verminderen en verwijderen van redundante videogegevens, zodat een digitaal videobestand effectief kan worden verzonden via een netwerk en worden opgeslagen op computerschijven. Met efficiënte compressietechnieken kan een bestand aanzienlijk worden verkleind met weinig of geen ongunstig effect op de visuele kwaliteit. De videokwaliteit kan echter worden beïnvloed als het bestand verder wordt verkleind door het compressieniveau voor een bepaalde compressietechniek te verhogen. Er zijn verschillende compressietechnologieën, zowel fabrikantspecifieke als industriestandaard, beschikbaar. De meeste leveranciers van netwerkvideo's gebruiken tegenwoordig standaard compressietechnieken. De standaarden zijn belangrijk om de compatibiliteit en interoperabiliteit te garanderen. Deze zijn vooral relevant voor de videocompressie omdat het mogelijk is dat de video voor verschillende doeleinden wordt gebruikt. Bij sommige videosurveillancetoepassingen moet de video tot een aantal jaren na de opnamedatum kunnen worden bekijken. Door gebruik te maken van de standaarden kunnen eindgebruikers nu kiezen uit verschillende leveranciers en zijn ze niet langer gebonden aan één leverancier voor het ontwerpen van een videosurveillance systeem.

Axis gebruikt drie verschillende videocompressiestandaarden. Dit zijn Motion JPEG, MPEG-4 Part 2 (of gewoon MPEG-4 genoemd) en H.264. H.264 is de nieuwste en meest efficiënte videocompressiestandaard. In dit hoofdstuk worden de basisprincipes van compressie behandeld en wordt een beschrijving van de drie eerder vermelde standaarden gegeven.

7.1 Basisprincipes van de compressie

7.1.1 Videocodec

Bij het compressieproces wordt een algoritme toegepast op de bronvideo om een gecomprimeerd bestand te maken dat gereed is voor transmissie of opslag. Om het gecomprimeerde bestand af te spelen, wordt een omgekeerd algoritme toegepast om een video te produceren die virtueel dezelfde inhoud weergeeft als de originele bronvideo. De tijd die nodig is voor het comprimeren, verzenden, decomprimeren en weergeven van een bestand, wordt latentie genoemd. Hoe geavanceerder het compressiealgoritme, hoe hoger de latentie.

Een paar algoritmen dat samenwerkt, wordt een videocodec genoemd (encoder/decoder). Videocodecs van verschillende standaarden zijn normaal niet onderling compatibel. Dat wil zeggen dat video-inhoud die met de ene standaard wordt gecomprimeerd, niet kan worden gedecomprimeerd met een andere standaard. Een MPEG-4-decoder werkt bijvoorbeeld niet met een H.264-encoder. Dit is eenvoudig te wijten aan het feit dat één algoritme de uitvoer van een ander algoritme niet correct kan decoderen. Het is echter mogelijk veel verschillende algoritmen in dezelfde software of hardware te implementeren zodat meerdere indelingen naast elkaar kunnen bestaan.

7.1.2 Beeldcompressie tegenover videocompressie

Verschillende compressiestandaarden gebruiken verschillende methoden voor het comprimeren van gegevens en daarom zijn de resultaten verschillend qua bitsnelheid, kwaliteit en latentie. Compressiealgoritmen worden onderverdeeld in twee typen: beeldcompressie en videocompressie.

Beeldcompressie gebruikt de intraframe-coderingstechnologie. De gegevens worden binnen het beeldframe verminderd door onnodige informatie die mogelijk niet wordt waargenomen door het menselijke oog, te verwijderen. Motion JPEG is een voorbeeld van een dergelijke compressiestandaard. Beelden in een Motion JPEG-reeks worden gecodeerd of gecomprimeerd als individuele JPEG-beelden.



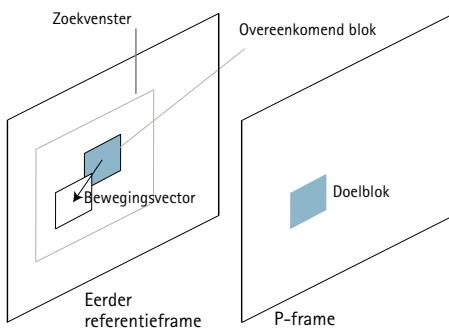
Afbeelding 7.1a Met de JPEG-indeling worden de drie beelden in de bovenstaande reeks gecodeerd en als afzonderlijke unieke beelden (I-frames) verzonden, zonder enige afhankelijkheid van elkaar.

Videocompressie-algoritmen zoals MPEG-4 en H.264 gebruiken interframe prediction om de videogegevens tussen een reeks frames te verminderen. Dit zijn onder andere technieken zoals verschilcodering waarbij het ene frame wordt vergeleken met een referentieframe en alleen pixels die zijn gewijzigd ten opzichte van het referentieframe, worden gecodeerd. Op deze manier wordt het aantal pixelwaarden dat is gecodeerd en verzonden, verminderd. Wanneer een dergelijke gecodeerde reeks wordt weergegeven, verschijnen de beelden als in de originele videoreeks.



Afbeelding 7.1b Met verschilcodering wordt alleen het eerste beeld (l-frame) volledig gecodeerd. In de twee volgende beelden (P-frames) worden verwijzingen gemaakt naar het eerste beeld voor de statische elementen, in dit het geval het huis. Alleen de bewegende delen, hier de lopende man, worden gecodeerd met bewegingsvectoren. Hierdoor wordt de hoeveelheid informatie die wordt verzonden en opgeslagen, verminderd.

Andere technieken zoals op blokken gebaseerde bewegingscompensatie kunnen worden toegepast om de gegevens verder te verminderen. Op blokken gebaseerde bewegingscompensatie houdt rekening met het gedeelte in een nieuw frame in een videoreeks dat in een eerder frame kan worden teruggevonden, eventueel op een andere locatie. Deze techniek splitst een frame op in reeksen van macroblokken (blokken pixels). Een nieuw frame kan per blok worden samengesteld of 'voorspeld' door een overeenkomend blok in een referentieframe te zoeken. Als een overeenkomst wordt gevonden, codeert de encoder de positie waar het overeenkomende blok kan worden gevonden in het referentieframe. Het coderen van de bewegingsvector, zoals dit wordt genoemd, neemt minder bits in beslag dan wanneer de werkelijke inhoud van een blok zou moeten worden gecodeerd.



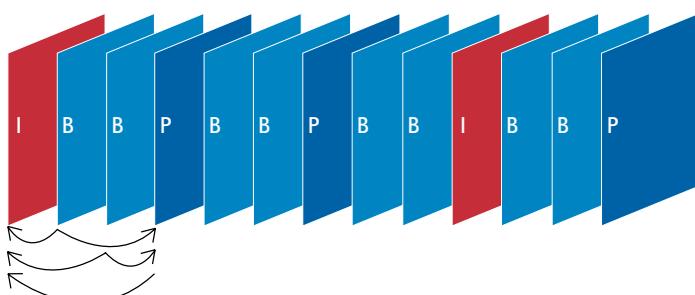
Afbeelding 7.1c Illustratie van op blok gebaseerde bewegingscompensatie.

Bij de interframe-voorspelling, wordt elk frame in een reeks beelden geklassificeerd als een bepaald type frame, zoals een l-frame, P-frame of B-frame.

Een I-frame of intraframe is een zelfstandig frame dat onafhankelijk kan worden gedecodeerd, zonder enige verwijzing naar andere beelden. Het eerste beeld in een videoreeks is altijd een I-frame. I-frames zijn nodig als startpunten voor nieuwe kijkers of als punten voor het opnieuw synchroniseren als de verzonden bitstroom is beschadigd. I-frames kunnen worden gebruikt om functies voor snel vooruitspoelen, terugspoelen en andere willekeurige toegangsfuncties te implementeren. Een encoder voegt automatisch I-frames in met regelmatige intervallen of op aanvraag als wordt verwacht dat er nieuwe klanten zullen bijkomen om een stroom te bekijken. Het nadeel van I-frames is dat deze veel meer bits verbruiken. Aan de andere kant genereren deze echter niet veel artefacten die worden veroorzaakt door ontbrekende gegevens.

Een P-frame, de afkorting voor predictive interframe, verwijst naar delen van eerdere I- en P-frames om het frame te coderen. P-frames gebruiken doorgaans minder bits dan I-frames. Een nadeel is echter dat ze zeer gevoelig zijn voor transmissieproblemen vanwege de complexe afhankelijkheid van eerdere P- en/of I-frames.

Een B-frame of bi-predictive inter frame is een frame dat zowel naar een eerder referentieframe als naar een toekomstig frame verwijst. Het gebruik van B-frames verhoogt de latentie.



Afbeelding 7.1d Een standaard reeks met I-, B- en P-frames. Een P-frame kan alleen verwijzen naar voorgaande I- of P-frames, terwijl een B-frame zowel naar voorgaande als naar volgende I- of P-frames kan verwijzen.

Wanneer een videodecoder een video herstelt door de bitstroom per frame te decoderen, moet het decoderen altijd starten met een I-frame. Als P- en B-frames worden gebruikt, moeten deze samen met de referentieframes worden gedecodeerd.

Met de netwerkvideoprodukten van Axis kunnen gebruikers de GOV-lengte (group of video = videogroep) instellen. Deze lengte bepaalt hoeveel P-frames moeten worden verzonden voordat een ander I-frame wordt verzonden. Door de frequentie van de I-frames te verlagen (langere GOV), kan de bitsnelheid worden verlaagd. Om de latentie te beperken worden geen B-frames gebruikt.

Naast de verschilcodering en de bewegingscompensatie kunnen andere geavanceerde methoden worden gebruikt om de gegevens verder te verminderen en de videokwaliteit te verbeteren. H.264 ondersteunt bijvoorbeeld geavanceerde technieken zoals voorspellingsschema's voor het coderen van I-frames, een verbeterde bewegingscompensatie met nauwkeurigheid tot op de subpixels en een in-loop deblokkeringsfilter om de blokranden te verzachten (artefacten). Meer informatie over H.264-technieken kunt u vinden in het whitepaper van Axis over H.264 op www.axis.com/corporate/corp/tech_papers.htm

7.2 Compressie-indelingen

7.2.1 Motion JPEG

Motion JPEG of M-JPEG is een digitale videoreeks die is samengesteld uit een reeks individuele JPEG-beelden. (JPEG is de afkorting voor Joint Photographic Experts Group.) Wanneer er 16 beeldframes of meer worden weergeven per seconde, kan de kijker bewegende video waarnemen. Volledig bewegende videobeelden worden waargenomen bij 30 (NTSC) of 25 (PAL) frames per seconde.

Een van de voordelen van Motion JPEG is dat elk beeld in een videoreeks dezelfde gegarandeerde kwaliteit kan hebben die is vastgesteld door het compressieniveau dat is gekozen voor de netwerkcamera of video-encoder. Hoe hoger het compressieniveau, hoe lager de bestandsgrootte en beeldkwaliteit. In sommige situaties, zoals bij weinig licht of wanneer een scène complex wordt, kan het beeldbestand relatief groot worden en meer bandbreedte en opslagruimte in beslag nemen. Om te verhinderen dat er meer bandbreedte en opslag wordt gebruikt, bieden netwerkvideoproducenten van Axis de gebruiker de mogelijkheid een maximale bestandsgrootte voor een beeldframe in te stellen.

Omdat er geen afhankelijkheid is tussen de frames in Motion JPEG, is een Motion JPEG-video robuust, wat betekent dat als er één beeld wegvalt tijdens de transmissie, de rest van de video niet wordt beïnvloed.

Motion JPEG is een standaard zonder licentie. Deze standaard heeft een brede compatibiliteit en is populair in toepassingen waar afzonderlijke frames in een videoreeks vereist zijn, bijvoorbeeld voor analyse, en waar lagere framesnelheden, standaard 5 frames per seconde of lager, worden gebruikt. Motion JPEG kan ook nodig zijn voor toepassingen die integratie vereisen in systemen die alleen Motion JPEG ondersteunen.

Het grootste nadeel van Motion JPEG is dat het geen gebruik maakt van videocompressietechnieken die de gegevens verminderen, omdat het een reeks stilstaande, volledige beelden betreft. Het resultaat is dat het een relatief hoge bitsnelheid of lage compressieverhouding voor de geleverde kwaliteit heeft in vergelijking met videocompressiestandaarden, zoals MPEG-4 en H.264.

7.2.2 MPEG-4

Wanneer MPEG-4 wordt vermeld in videosurveillancetoepassingen wordt doorgaans verwezen naar MPEG-4 Part 2, ook bekend als MPEG-4 Visual. Net als alle MPEG-standaarden (Moving Picture Experts Group) is dit een standaard met licentie. Gebruikers moeten daarom per bewakingsstation licentiekosten betalen. MPEG-4 ondersteunt toepassingen met een lage bandbreedte en toepassingen die beelden met hoge kwaliteit vereisen, geen beperkingen toestaan op de framesnelheid en een vrijwel onbeperkte bandbreedte nodig hebben.

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

H.264, ook bekend als MPEG-4 Part 10/AVC voor Advanced Video Coding, is de nieuwste MPEG-standaard voor videocodering. Volgens de verwachtingen zal H.264 in de komende jaren de voorkeursvideostandaard worden. Reden hiervoor is dat een H.264-encoder, zonder in te boeten aan beeldkwaliteit, de grootte van een digitaal videobestand kan verkleinen met meer dan 80% in vergelijking met de Motion JPEG-indeling en tot 50% meer dan de MPEG-4-standaard. Dit betekent dat er minder netwerkbandbreedte en opslagruimte vereist is voor een videobestand. Vanuit een ander standpunt wordt dus een veel hogere videokwaliteit bereikt voor een bepaalde bitsnelheid.

H.264 is gezamenlijk gedefinieerd door standaardiseringsorganisaties in de telecommunicatie-(ITU-T's Video Coding Experts Group) en IT-sector (ISO/IEC Moving Picture Experts Group) en er wordt verwacht dat deze op veel grotere schaal zal worden overgenomen dan eerdere standaarden. In de videosurveillance-industrie zal H.264 zeer waarschijnlijk het snelst aanslaan in toepassingen waar behoefte is aan hogere framesnelheden en een hogere resolutie, zoals bij de surveillance van snelwegen, luchthavens en casino's, waar het gebruik van 30/25 (NTSC/PAL) frames per seconde de norm is. Hier zullen de meeste kosten worden bespaard vanwege minder bandbreedtevereisten en minder opslagvereisten.

Van H.264 wordt ook verwacht dat deze standaard het gebruik van megapixelcamera's zal versnellen omdat de zeer efficiënte compressietechnologie grote bestanden en hoge bitsnelheden die zijn gegenereerd, kan beperken zonder in te boeten aan beeldkwaliteit. Er zijn echter nadelen. Terwijl H.264 besparingen op netwerkbandbreedte en opslagkosten biedt, worden netwerkkamera's en bewakingsstations met hogere prestaties vereist.

H.264-encoders van Axis gebruiken het basisprofiel. Dit betekent dat alleen I- en P-frames worden gebruikt. Dit profiel is ideaal voor netwerkkamera's en video-encoders aangezien de lage latentie wordt verkregen omdat er geen B-frames worden gebruikt. Een lage latentie is van essentieel belang bij videosurveillancetoepassingen met live surveillance, vooral wanneer PTZ- of PTZ-domecamera's worden gebruikt.

7.3 Variabele en constante bitsnelheden

Met MPEG-4 en H.264 kunnen gebruikers een gecodeerde videotraject met een variabele of constante bitsnelheid toestaan. De optimale selectie is afhankelijk van de toepassing en de netwerkinfrastructuur.

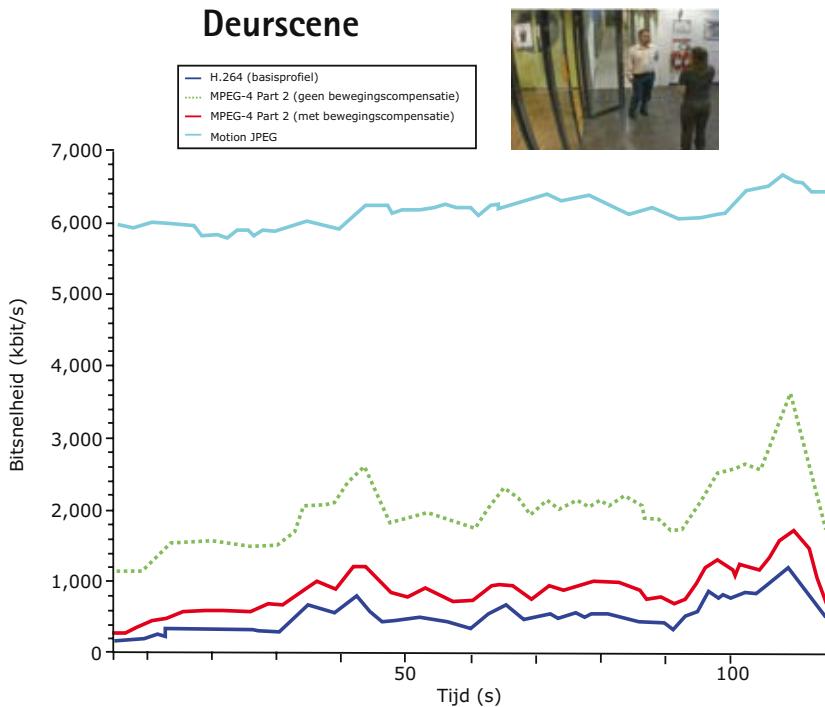
Met VBR (variable bit rate = variabele bitsnelheid) kan een vooraf gedefinieerd niveau voor de beeldkwaliteit worden behouden, ongeacht de beweging of het ontbreken van beweging in een scène. Dit betekent dat het gebruik van de bandbreedte zal toenemen wanneer er veel activiteit is in een scène en zal afnemen wanneer er geen beweging is. Dit is vaak gewenst in videosurveillance-toepassingen waar behoefte is aan hoge kwaliteit, vooral als er beweging is in een scène. Aangezien de bitsnelheid kan verschillen, zelfs wanneer een gemiddelde doelbitsnelheid is gedefinieerd, moet de netwerkinfrastructuur (beschikbare bandbreedte) in staat zijn hoge doorvoersnelheden te ondersteunen.

Door de beperkte beschikbare bandbreedte is de aanbevolen modus normaal CBR (constant bit rate = constante bitsnelheid) omdat deze modus een constante bitsnelheid genereert die vooraf kan worden gedefinieerd door een gebruiker. CBR heeft echter een nadeel. Als er bijvoorbeeld meer activiteit is in een scène die resulteert in een bitsnelheid die hoger is dan de doelsnelheid, leidt de beperking om de bitsnelheid constant te houden tot een lagere beeldkwaliteit en framesnelheid. Netwerkvideoproducten van Axis bieden de gebruiker de mogelijkheid voorrang te geven aan de beeldkwaliteit of aan de framesnelheid wanneer de bitsnelheid de doelbitsnelheid overschrijdt.

7.4 Standaarden vergelijken

Bij het vergelijken van de prestaties van MPEG-standaarden, zoals MPEG-4 en H.264, is het belangrijk dat u weet dat de resultaten kunnen verschillen tussen encoders die dezelfde standaard gebruiken. Dit is te wijten aan het feit dat de ontwerper van een encoder kan kiezen om verschillende hulpmiddelen die door een standaard zijn gedefinieerd, te implementeren. Zolang de uitvoer van een encoder voldoet aan de indeling en de decoder van een standaard, is het mogelijk verschillende implementaties uit te voeren. Een MPEG-standaard kan daarom geen bepaalde bitsnelheid of kwaliteit garanderen. Bovendien kunnen er geen goede vergelijkingen worden uitgevoerd zonder eerst te definiëren hoe de standaarden in een encoder zijn geïmplementeerd. In tegenstelling tot een encoder moet een decoder alle vereiste delen van een standaard implementeren om een compatibele bitstroom te decoderen. Een standaard bepaalt exact hoe een decompressie-algoritme elke bit van een gecomprimeerde video moet herstellen.

De grafiek op de volgende pagina geeft een vergelijking tussen bitsnelheden, met hetzelfde niveau beeldkwaliteit, van de volgende videotrajecten: Motion JPEG, MPEG-4 Part 2 (geen bewegingscompensatie), MPEG-4 Part 2 (met bewegingscompensatie) en H.264 (basisprofiel).



Afbeelding 7.4a De H.264-encoder van Axis heeft tot 50% minder bits per seconde gegenereerd voor een voorbeeldvideoreeks dan een MPEG-4-encoder met bewegingscompensatie. De H.264-encoder is minstens drie keer efficiënter dan een MPEG-4-encoder zonder bewegingscompensatie en minstens zes keer efficiënter dan met Motion JPEG.

Audio

Hoewel het gebruik van audio in videosurveillance-systeem nog steeds niet op grote schaal wordt gebruikt, kan dit niet alleen de capaciteiten van het systeem om gebeurtenissen te detecteren en te interpreteren verbeteren, maar ook kan de audiocommunicatie via een IP-netwerk verlopen. Het gebruik van audio kan in sommige landen echter worden beperkt. Wij raden u daarom aan de lokale instanties hierover te raadplegen.

De onderwerpen die in dit hoofdstuk worden beschreven zijn onder andere toepassings-scenario's, audio-apparatuur, audiomodi, audiodetectie-alarm, audiocompressie en audio/video-synchronisatie.

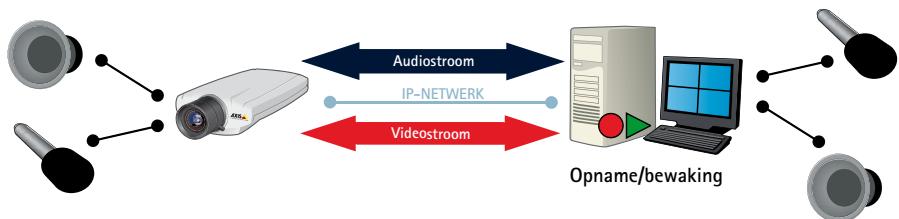
8.1 Audiotoepassingen

Wanneer u over audio beschikt als een geïntegreerd deel van een videosurveillance-systeem, kan dit een waardevolle aanvulling zijn voor de capaciteit van het systeem om gebeurtenissen en noodsituaties te detecteren en te interpreteren. Audio biedt de mogelijkheid om een gebied van 360 graden af te dekken en biedt een videosurveillance-systeem daarmee de mogelijkheid de dekking uit te breiden buiten het blikveld van een camera. Het is mogelijk een PTZ- of PTZ-domecamera (of de operator van een camera) de opdracht te geven een audio-alarm visueel te controleren.

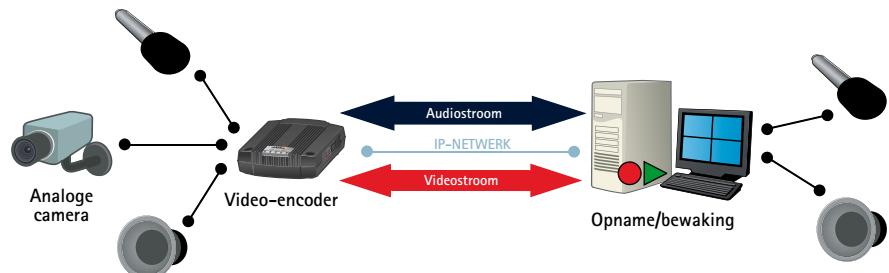
Audio kan ook worden gebruikt om gebruikers niet alleen de mogelijkheid te bieden om mee te luisteren in een gebied, maar ook om opdrachten of aanvragen aan bezoekers of indringers door te geven. Als een persoon die in het beeldveld van een camera staat, zich verdacht gedraagt, zoals rondslenteren in de buurt van een geldautomaat of het betreden van een gebied waar toegang verboden is, kan een veiligheidsagent een verbale waarschuwing zenden naar die persoon. In een situatie waarin een persoon gewond is, kan het een voordeel zijn als u op afstand kunt communiceren met het slachtoffer en deze kunt melden dat hulp onderweg is. Toegangsbeheer – met andere woorden: de ‘portier’ op afstand bij een ingang – is een ander toepassingsgebied. Andere toepassingen hebben onder andere een externe helpdesk-situatie (bijvoorbeeld een onbemande parkeergarage) en video-overgaderingen. Een audiovisueel surveillance-systeem verhoogt de doelmatigheid van een beveiligings- of externe surveillance-oplossing door het verbeteren van de mogelijkheden van een externe gebruiker om informatie te ontvangen en te communiceren.

8.2 Audio-ondersteuning en apparatuur

Audio-ondersteuning kan gemakkelijker worden geïmplementeerd in een netwerkvideosysteem dan in een analoog CCTV-systeem. In een analoog systeem moeten afzonderlijke audio- en videokabels worden geïnstalleerd van eindpunt naar eindpunt, dat wil zeggen van de camera- en microfoonlocatie naar de weergave/opnamelocatie. Als de afstand tussen de microfoon en het station te groot is, moet gebalanceerde audioapparatuur worden gebruikt. Hierdoor nemen de installatiekosten en de moeilijkheden toe. In een netwerkvideosysteem verwerkt een netwerkcamera met audio-ondersteuning de audio en verzendt deze audio en video via dezelfde netwerk-kabel voor bewaking en/of opname. Hierdoor hoeft u geen extra kabels te installeren en wordt het synchroniseren van audio en video veel eenvoudiger.



Afbeelding 8.2a Een netwerkvideosysteem met geïntegreerde audio-ondersteuning. Audio- en videotstromen worden via dezelfde netwerk-kabel verzonden.



Afbeelding 8.2b Sommige video-encoders hebben ingebouwde audio zodat het mogelijk is audio toe te voegen, zelfs als analoge camera's worden gebruikt in een installatie.

Een netwerkcamera of video-encoder met geïntegreerde audiofunctionaliteit bevat vaak een ingebouwde microfoon en/of microfoon-/lijningang. Met ondersteuning voor een microfoon/lijningang hebben gebruikers de mogelijkheid een ander type of een andere kwaliteit microfoon te gebruiken dan de microfoon die in de camera of video-encoder is geïntegreerd. Dit biedt u ook de mogelijkheid het netwerkvideoproduct te verbinden met meer dan één microfoon en de microfoon kan zich op een bepaalde afstand van de camera bevinden. De microfoon moet altijd zo dicht mogelijk bij de geluidsbron worden geplaatst om ruis te beperken. Bij een full-duplexmodus in twee richtingen moet de microfoon uit de buurt van de luidspreker en op een bepaalde afstand worden geplaatst om rondzingen van de luidspreker te beperken.

Heel wat netwerkvideoproducten van Axis worden niet met een ingebouwde luidspreker geleverd. Een actieve luidspreker – een luidspreker met ingebouwde versterker – kan direct op een netwerkvideoproduct met audio-ondersteuning worden aangesloten. Als een luidspreker geen ingebouwde versterker heeft, moet u deze eerst aansluiten op een versterker die vervolgens op een netwerkkamera/video-encoder wordt aangesloten.

Om storing en ruis te minimaliseren, moet u altijd een afgeschermd audiokabel gebruiken. Zorg dat deze kabel niet dicht bij voedingskabels en kabels met schakelsignalen van hoge frequentie wordt geplaatst. Audiokabels moeten zo kort mogelijk worden gehouden. Als een lange audiokabel vereist is, moet gebalanceerde audio-apparatuur – dat wil zeggen een kabel, versterker en microfoon die allemaal gebalanceerd zijn – worden gebruikt om ruis te beperken..

8.3 Audiomodi

Afhankelijk van de toepassing kan het nodig zijn audio in slechts één richting of in beide richtingen te zenden. Dit kan gelijktijdig plaatsvinden of in één richting per keer. Er zijn drie basismodi voor de audiocommunicatie: simplex, half-duplex en full-duplex.

8.3.1 Simplex



Afbeelding 8.3a In de simplexmodus wordt audio in slechts één richting verzonden. In dit geval wordt de audio door de camera naar de operator verzonden. Toepassingen zijn onder andere externe bewaking en videosurveillance.



Afbeelding 8.3b In dit voorbeeld van een simplexmodus wordt audio door de operator naar de camera verzonden. Dit kan bijvoorbeeld worden gebruikt om een persoon die op de camera zichtbaar is gesproken instructies te geven, of om een potentiële autodief van een parkeerterrein te verjagen.

8.3.2 Half-duplex



Afbeelding 8.3c In half-duplexmodus wordt de audio in beide richtingen verzonden, maar kan slechts naar één richting per keer worden verzonden. Dit lijkt op de werking van een walkie-talkie.

8.3.3 Full-duplex



Afbeelding 8.3d In full-duplexmodus wordt audio tegelijkertijd van en naar de operator verzonden. Deze communicatiemodus lijkt op een telefoongesprek. Full-duplex vereist dat de client-pc over een geluidskaart beschikt die full-duplex audio ondersteunt

8.4 Audiodetectie-alarm

Een audiodetectie-alarm kan worden gebruikt als aanvulling op videobewegingsdetectie omdat dit kan reageren op gebeurtenissen in gebieden die te donker zijn voor een correcte werking van de videobewegingsdetectie. Deze optie kan ook worden gebruikt om activiteit te detecteren in gebieden buiten het beeldveld van de camera.

Wanneer geluiden, zoals het breken van een raam of stemmen in een kamer, worden gedetecteerd, kunnen deze een netwerkcamera activeren om video en audio te verzenden en op te nemen, e-mails of andere waarschuwingen te verzenden en externe apparaten, zoals alarminstallaties, te activeren. Op dezelfde manier kunnen alarmingen, zoals bewegingsdetectie en deurcontacten worden gebruikt om video- en audio-opnamen te activeren. In een PTZ- of PTZ-domecamera kan de audio-alarmdetectie de camera activeren om automatisch te draaien naar een vooraf ingestelde locatie, zoals een bepaald raam.

8.5 Audiocompressie

Analoge audiosignalen moeten worden geconverteerd naar digitale audio via een samplingproces en moeten vervolgens worden gecomprimeerd om de grootte te beperken voor een efficiënte transmissie en opslag. De conversie en compressie vinden plaats via een audiocodec, een algoritme dat audiogegevens codeert en decodeert.

8.5.1 Samplingfrequentie

Er zijn heel wat verschillende audiocodecs die verschillende samplingfrequenties en compressieniveaus ondersteunen. Samplingfrequentie verwijst naar het aantal keren dat een voorbeeld van een analoog audiosignaal per seconde wordt genomen en wordt gedefinieerd in hertz (Hz). Algemeen geldt, hoe hoger de samplingfrequentie, hoe beter de audiokwaliteit en hoe meer bandbreedte en opslag benodigd is.

8.5.2 Bitsnelheid

De bitsnelheid is een belangrijke instelling in audio omdat dit het compressieniveau bepaalt en daardoor ook de audiokwaliteit. Algemeen geldt, hoe hoger het compressieniveau (hoe lager de bitsnelheid), hoe lager de audiokwaliteit. De verschillen in de audiokwaliteit van codecs kan bijzonder goed waarneembaar zijn bij hoge compressieniveaus (lage bitsnelheden), maar niet bij lage compressieniveaus (hoge bitsnelheden). Hogere compressieniveaus kunnen ook meer latentie of vertraging veroorzaken, maar bieden een grotere besparing op het gebied van bandbreedte en opslag.

De bitsnelheden die het vaakst worden geselecteerd met audiocodecs liggen tussen 32 kbit/s en 64 kbit/s. Audiobitsnelheden vormen, net als videobitsnelheden, een belangrijke overweging waarmee rekening moet worden gehouden wanneer u de vereisten berekent voor de totale bandbreedte en opslag.

8.5.3 Audiocodecs

De netwerkvideoproducten van Axis ondersteunen drie audiocodecs. De eerste is AAC-LC (Advanced Audio Coding – Low Complexity), ook bekend als MPEG-4 AAC en vereist een licentie. AAC-LC is, vooral bij een samplefrequentie van 16 kHz of hoger en een bitsnelheid van 64 kbit/s, de aanbevolen codec wanneer de best mogelijke audiokwaliteit is vereist. De andere twee codecs zijn G.711 en G.726. Dit zijn technologieën zonder licentie.

8.6 Audio- en videosynchronisatie

De synchronisatie van audio- en videogegevens wordt uitgevoerd door een mediaspeler (een computerprogramma dat wordt gebruikt voor het afspelen van multimediestanden) of door een multimediaframework, zoals Microsoft DirectX dat een verzameling is van API's (application programming interfaces) die multimediestanden verwerkt.

Audio en video worden via een netwerk verzonden als twee afzonderlijke pakketstromen. Om de client of speler de mogelijkheid te bieden een perfecte synchronisatie uit te voeren van de audio- en videostromen, moeten de audio- en videopakketten van een tijdstempel worden voorzien. Het toevoegen van tijdstempels aan videopakketten die Motion JPEG-compressie gebruiken, wordt mogelijk niet altijd ondersteund in een netwerkcamera.

Als dat het geval is en als het belangrijk is gesynchroniseerde video en audio te hebben, is het videoformaat dat u moet kiezen MPEG-4 of H.264, omdat dergelijke videostromen, samen met de audiotroom, worden verzonden door middel van RTP (Real-time Transport Protocol) die tijdstempels toevoegt aan video- en audiopakketten. Er zijn echter toch veel situaties waarbij synchrone audio minder belangrijk is of zelfs ongewenst, bijvoorbeeld als de audio wordt uitgeleisterd maar niet opgenomen.

Netwerktechnologieën

Er worden verschillende netwerktechnologieën gebruikt om de vele voordelen van een netwerkvideosysteem te ondersteunen en te bieden. Dit hoofdstuk start met een uiteenzetting over een LAN-netwerk en in het bijzonder over Ethernet-netwerken en de componenten die dit ondersteunen. Ook het gebruik van PoE (Power over Ethernet) wordt besproken. Daarna vindt u meer uitleg over communicatie via internet met toelichtingen over IP-adressering (Internet Protocol): wat het inhoudt en hoe het werkt, waaronder het krijgen van toegang tot netwerkvideoprodukten via internet. U vindt hier ook een overzicht van de protocollen voor datatransport in netwerkvideo's.

Andere onderwerpen die in dit hoofdstuk worden besproken, zijn onder andere virtuele LAN-netwerken en Servicekwaliteit (QoS) en de verschillende manieren om communicatie via IP-netwerken te beveiligen. *Raadpleeg hoofdstuk 10 voor meer informatie over draadloze technologieën.*

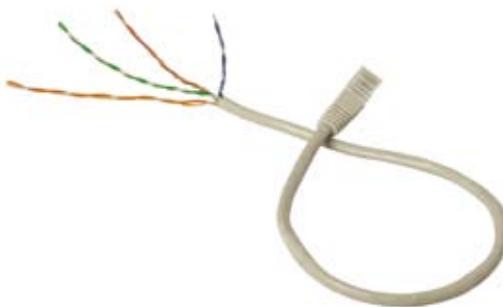
9.1 LAN-netwerk en Ethernet

Een LAN-netwerk wordt gevormd door een groep computers die onderling verbonden zijn in een gelokaliseerd gebied om met elkaar te communiceren en apparatuur, zoals printers, te delen. De gegevens worden verzonden in de vorm van pakketten. Om de transmissie van deze pakketten te regelen, kunnen verschillende technologieën worden gebruikt. De LAN-technologie die het meest wordt gebruikt is Ethernet en dit is vastgelegd in een standaard die IEEE 802.3 wordt genoemd. (Andere typen van LAN-netwerktechnologieën zijn onder andere Token ring en FDDI.)

Ethernet gebruikt een stertopologie waarin de afzonderlijke knooppunten (apparaten) onderling worden verbonden in een netwerk via actieve netwerkapparatuur, zoals switches. Een LAN kan twee tot duizenden netwerkapparaten bevatten.

Het fysieke transmissiemedium voor een bekabeld LAN werkt met kabels, hoofdzakelijk getwiste paren of glasvezel. Een getwiste kabel bestaat uit acht draden die vier paren getwiste koperdraden vormen en wordt gebruikt met RJ-45-stekkers en contactdozen. De maximale kabellengte van een getwist paar is 100 m. Voor een glasvezelkabel ligt de maximale lengte tussen 10 en

70 km, afhankelijk van het type vezel. Afhankelijk van het type getwiste draad of glasvezelkabel dat wordt gebruikt, kunnen de gegevensnelheden tegenwoordig 100 Mbit/s tot 10.000 Mbit/s zijn.



Afbeelding 9.1a *Een bekabeling met getwiste draden bevat vier paren getwiste draden die doorgaans aan het eind zijn aangesloten op een RJ-45-stekker.*

Als vuistregel geldt dat u altijd een netwerk moet bouwen met een grotere capaciteit dan momenteel nodig is. Om te garanderen dat een netwerk voorbereid is op de toekomst, wordt het aanbevolen een netwerk zo te ontwerpen, dat slechts 30% van de capaciteit wordt gebruikt. Omdat steeds meer toepassingen tegenwoordig via netwerken worden uitgevoerd, zijn steeds hogere netwerkprestaties vereist. Hoewel u netwerkswitches (wordt hieronder besproken) na enkele jaren gemakkelijk kunt upgraden, zal het vervangen van de bekabeling moeilijker worden.

9.1.1 Typen Ethernet-netwerken

Fast Ethernet

Fast Ethernet verwijst naar een Ethernet-netwerk dat gegevens kan overdragen met een snelheid van 100 Mbit/s. Dit kan worden gebaseerd op een getwiste draad of op een glasvezelkabel. (Het oudere 10 Mbit/s Ethernet wordt nog steeds geïnstalleerd en gebruikt, maar dergelijke netwerken bieden onvoldoende bandbreedte voor bepaalde netwerkvideotoepassingen.)

De meeste apparaten die met een netwerk zijn verbonden, zoals een laptop of netwerkcamera, zijn uitgerust met een 100BASE-TX/10BASE-T Ethernet-interface, meestal een 10/100-interface genoemd, die zowel 10 Mbit/s als Fast Ethernet ondersteunt. Het type getwiste kabel dat Fast Ethernet ondersteunt, wordt een Cat. 5-kabel genoemd.

Gigabit Ethernet

Gigabit Ethernet, dat ook kan worden gebaseerd op een getwiste draad of een glasvezelkabel, levert een gegevensnelheid van 1.000 Mbit/s (1 Gbit/s) en wordt steeds populairder. Volgens de verwachtingen zal dit systeem Fast Ethernet binnenkort vervangen als de erkende standaard.

Het type getwiste draden dat Gigabit Ethernet ondersteunt, is een Cat. 5e-kabel. In dit type kabel worden de vier paren getwiste draden in de kabel allemaal gebruikt om hoge gegevenssnelheden te bereiken. Voor netwerkvideosystemen worden kabelcategorieën Cat. 5e en hoger aanbevolen. De meeste interfaces zijn compatibel met oudere apparatuur met 10 en 100 Mbit/s Ethernet. Deze worden over het algemeen 10/100/1000-interfaces genoemd.

Voor transmissies over langere afstanden kunnen glasvezelkabels zoals 1000BASE-SX (tot 550 m) en 1000BASE-LX (tot 550 m met multi-mode glasvezel en 5.000 m met single-mode glasvezel) worden gebruikt.



Afbeelding 9.1b Langere afstanden kunnen worden overbrugd door het gebruik van glasvezelkabels. Glasvezel wordt standaard gebruikt in de backbone van een netwerk en niet in knooppunten zoals een netwerkcamera.

10 Gigabit Ethernet

10 Gigabit Ethernet is de nieuwste generatie en levert een gegevenssnelheid van 10 Gbit/s (10.000 Mbit/s). Hierbij kan een glasvezelkabel of een getwiste draad worden gebruikt. 10GBASE-LX4, 10GBASE-ER en 10GBASE-SR gebaseerd op een optische glasvezelkabel, kunnen worden gebruikt om afstanden tot maar liefst 10.000 m te overbruggen. Met een getwiste draadoplossing is een kabel van zeer hoge kwaliteit (Cat-6a of Cat-7) vereist. 10 Gbit/s Ethernet wordt vooral gebruikt voor backbones in high-end-toepassingen die hoge gegevenssnelheden vereisen.

9.1.2. Switch

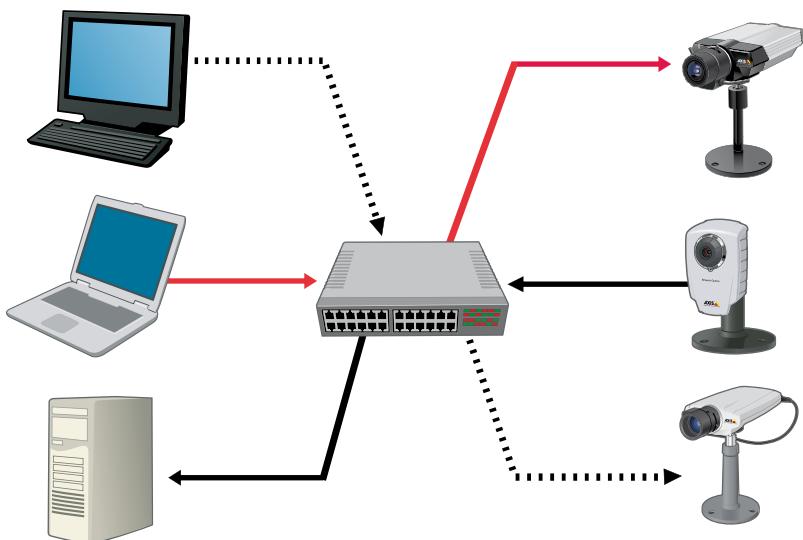
Wanneer slechts twee apparaten direct met elkaar moeten communiceren via een getwiste draad, kan een zogenaamde crossover-kabel worden gebruikt. De crossover-kabel kruist simpelweg het transmissiepaar aan het ene uiteinde van de kabel met het ontvangende paar aan het andere uiteinde, en omgekeerd.

Om meerdere apparaten in een LAN in een netwerk te combineren, is echter netwerkapparatuur zoals een netwerkswitch vereist. Wanneer u een netwerkswitch gebruikt, wordt een gewone netwerkkabel gebruikt in plaats van een crossover-kabel.

De belangrijkste functie van een netwerkswitch bestaat uit het doorsturen van gegevens van het ene apparaat naar het andere binnen hetzelfde netwerk. Dit gebeurt op een efficiënte manier omdat gegevens van het ene apparaat naar een ander apparaat kunnen worden geleid zonder andere apparaten op hetzelfde netwerk te beïnvloeden.

Het werkt als volgt: een switch registreert de MAC-adressen (Media Access Control) van alle apparaten die ermee verbonden zijn. (Elk netwerkapparaat heeft een uniek MAC-adres dat is samengesteld uit een reeks cijfers en letters die door de fabrikant zijn ingesteld. U kunt dit adres vaak terugvinden op het productlabel.) Wanneer een switch gegevens ontvangt, stuurt deze de gegevens alleen door naar de poort die verbonden is met een apparaat met het geschikte doel-MAC-adres.

De prestaties van de switches worden doorgaans aangeduid in snelheden per poort en in backplane- of interne snelheden (zowel in bitsnelheden als in pakketten per seconde). De poortsnelheden geven de maximale snelheden op specifieke poorten aan. Dit betekent dat de snelheid van een switch, bijvoorbeeld 100 Mbit/s, ook vaak de prestatie van elke poort aangeeft.



Afbeelding 9.1c Met een netwerkswitch wordt de gegevensoverdracht bijzonder efficiënt beheerd omdat het gegevensverkeer van het ene apparaat naar het andere kan worden geleid zonder andere poorten op de switch te beïnvloeden.

Normaal biedt een netwerkswitch simultane ondersteuning voor verschillende gegevenssnelheden. De meest gebruikelijke snelheden waren in het verleden 10/100, met ondersteuning van 10 Mbit/s en Fast Ethernet. De 10/100/1000-switches nemen echter intussen al snel de plaats in als standaardswitch, waardoor 10 Mbit/s, Fast Ethernet en Gigabit Ethernet tegelijk worden ondersteund. De overdrachtsnelheid en -modus tussen een poort op een switch en een aangesloten apparaat worden doorgaans vastgesteld via 'auto-negotiation' (automatisch onderhandelen) waarbij de hoogste algemene gegevenssnelheid en de beste overdrachtmodus worden gebruikt. Via een switch kan een aangesloten apparaat ook werken in full-duplex-modus, wat betekent dat het gegevens tegelijkertijd kan verzenden en ontvangen. Hierdoor worden hogere prestaties bereikt.

Switches kunnen met verschillende eigenschappen of functies worden geleverd. Sommige switches bevatten de functie van een router (zie paragraaf 9.2). Een switch kan ook PoE (Power over Ethernet) of Servicekwaliteit (QoS) (zie paragraaf 9.4) ondersteunen. In dit geval wordt bepaald hoeveel bandbreedte wordt gebruikt door verschillende toepassingen.

9.1.3 PoE (Power over Ethernet)

PoE (Power over Ethernet) biedt de mogelijkheid om apparaten die met een Ethernet-netwerk zijn verbonden, van stroom te voorzien via dezelfde kabel als voor de gegevenscommunicatie. PoE (Power over Ethernet) wordt op grote schaal gebruikt om stroom te leveren aan IP-telefoons, draadloze toegangspunten en netwerkcamera's in een LAN.

Het grootste voordeel van PoE is de daarmee samenhangende kostenbesparing. U hoeft geen erkende elektricien in te huren of een afzonderlijke elektrische leiding te installeren. Dit is vooral een voordeel in moeilijk te bereiken gebieden. Het feit dat er geen stroomkabel hoeft te worden geïnstalleerd kan, afhankelijk van de locatie van de camera, een besparing betekenen van enkele honderden euro per camera. Wanneer u over PoE beschikt, is het ook gemakkelijker een camera naar een nieuwe locatie te verplaatsen of camera's toe te voegen aan een videosurveillancestelsel.

Daarnaast kan PoE een videosysteem veiliger maken. Een videosurveillancestelsel met PoE kan van stroom worden voorzien vanuit de serverruimte. Deze stroom wordt vaak ondersteund door een UPS (Uninterruptible Power Supply). Dit betekent dat het videosurveillancestelsel zelfs bij een stroomuitval kan blijven werken. Vanwege de voordelen van PoE wordt het aanbevolen dit systeem te gebruiken met zoveel mogelijk apparaten. De voeding die beschikbaar is via de switch of midspan met PoE moet voldoende zijn voor de aangesloten apparaten en de apparaten moeten de stroomclassificatie ondersteunen. Ze worden uitgebreider toegelicht in de onderstaande paragrafen.

802.3af-standaard en High PoE

De meeste PoE-apparaten die tegenwoordig op de markt zijn, voldoen aan de IEEE 802.3af-standaard die in 2003 is gepubliceerd. De IEEE 802.3af-standaard gebruikt standaardkabels van de categorie 5 of hoger en zorgt ervoor dat de gegevensoverdracht niet wordt beïnvloed. In de standaard wordt het apparaat dat de stroom levert, het PSE-apparaat (Power Sourcing Equipment) genoemd. Dit kan een switch of midspan met PoE zijn. Het apparaat dat de stroom ontvangt, is een PD (powered device). De functionaliteit is normaal ingebouwd in een netwerkapparaat zoals een netwerkcamera of wordt geleverd in een zelfstandige splitter (zie paragraaf hieronder).

Compatibiliteit met oudere apparaten zoals netwerkapparaten die niet met PoE compatibel zijn, is gegarandeerd. De standaard bevat een methode voor automatische identificatie als een apparaat PoE ondersteund. Pas wanneer deze is gecontroleerd, wordt er stroom geleverd aan het apparaat. Dit betekent ook dat de Ethernet-kabel die op een PoE-switch is aangesloten, geen stroom levert als deze niet is aangesloten op een PoE-apparaat. Hierdoor wordt het risico op elektrische schokken tijdens het installeren of herbekabelen van een netwerk voorkomen. In een getwiste kabel

bevinden zich vier paren getwiste draden. PoE kan de twee 'reserve' draadparen gebruiken of de stroom overzetten naar de draadparen die voor de gegevensoverdracht worden gebruikt. Switches met ingebouwde PoE leveren vaak stroom via de twee draadparen die worden gebruikt voor de gegevensoverdracht, terwijl midspans doorgaans de twee reserveparen gebruiken. Een PD ondersteunt beide opties. Volgens IEEE 802.3af biedt een PSE een spanning van 48 V DC met een maximaal vermogen van 15,4 W per poort. Aangezien er stroomverlies is op een getwiste kabel, is slechts 12,95 W gegarandeerd voor een PD. De IEEE 802.3af-standaard definieert verschillende prestatiecategorieën voor PD's.

PSE, zoals switches en midspans, leveren normaal een bepaalde hoeveelheid voeding, standaard 300 tot 500 W. Op een switch met 48 poorten betekent dat 6 tot 10 W per poort als alle poorten zijn verbonden met apparaten die PoE gebruiken. Tenzij de PD's stroomclassificatie ondersteunen, moet de volledige 15,4 W worden voorbehouden aan elke poort die PoE gebruikt. Dit betekent dat een switch met 300 W slechts stroom kan leveren aan 20 van de 48 poorten. Als alle apparaten de switch echter laten weten dat ze Klasse 1-apparaten zijn, zal deze 300 W voldoende zijn om alle poorten van stroom te voorzien.

Klasse	Minimaal vermogensniveau op PSE	Maximaal vermogensniveau gebruikt door PD	Gebruik
0	15,4 W	0,44 W - 12,95 W	standaard
1	4,0 W	0,44 W - 3,84 W	optioneel
2	7,0 W	3,84 W - 6,49 W	optioneel
3	15,4 W	6,49 W - 12,95 W	optioneel
4	Behandelen als Klasse 0		Voorbehouden voor toekomstig gebruik

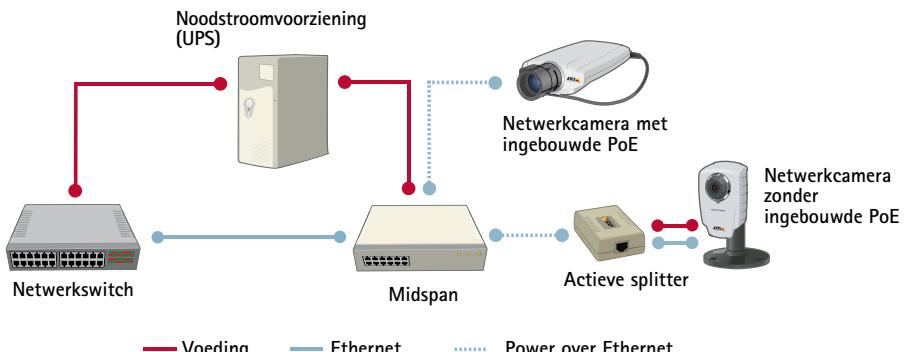
Tabel 9.1a Stroomclassificaties volgens IEEE 802.3af.

De meeste vaste netwerkkamera's kunnen stroom ontvangen via PoE met de IEEE 802.3af-standaard en worden normaal herkend als Klasse 1- of 2-apparaten. Met de pre-standaard IEEE 802.3at of PoE+ wordt de stroomlimiet verhoogd tot minstens 30 W via twee draadparen van een PSE. De definitieve specificaties moeten nog worden bepaald en naar verwachting zal de standaard midden 2009 worden goedgekeurd.

Intussen kunnen midspans en splitters die voldoen aan de pre-standaard IEEE 802.3at (High PoE) worden gebruikt voor apparaten zoals PTZ- en PTZ-domecamera's met motorbesturing en voor camera's met verwarmingsapparaten en ventilatoren, die meer vermogen vereisen dan kan worden geleverd door de IEEE 802.3af-standaard.

Midspans en splitters

Midspans en splitters (ook bekend als actieve splitters) zijn apparaten die een bestaand netwerk in staat stellen PoE (Power over Ethernet) te ondersteunen.



Afbeelding 9.1d Een bestaand systeem kan worden uitgebreid met de PoE-functionaliteit door middel van een midspan en splitter.

De midspan die vermogen toevoegt aan een Ethernet-kabel wordt tussen de netwerkswitch en de van stroom voorziene apparaten geplaatst. Om te controleren of de gegevensoverdracht niet wordt beïnvloed, is het belangrijk dat u onthoudt dat de maximale afstand tussen de gegevenbron (bijv. switch) en de netwerkkamera's niet meer is dan 100 m. Dit betekent dat de midspan en actieve splitter(s) binnen een afstand van 100 m moeten worden geplaatst. Een splitter wordt gebruikt om de stroom en gegevens in een Ethernet-kabel te splitsen in twee afzonderlijke kabels die vervolgens kunnen worden aangesloten op een apparaat dat geen ingebouwde PoE-ondersteuning heeft. Aangezien PoE of High PoE alleen 48 V DC levert, bestaat een andere functie van de splitter uit het verlagen van de spanning naar het geschikte niveau voor het apparaat, bijv. 12 of 5 V. Midspans en splitters met PoE en High PoE zijn verkrijgbaar bij Axis.

9.2 Internet

Om gegevens te verzenden tussen een apparaat op het ene LAN-netwerk naar een ander apparaat op een ander LAN, is een standaard manier van communiceren vereist omdat LAN-netwerken verschillende typen technologie kunnen gebruiken. Deze behoefte ligt aan de basis van de ontwikkeling van IP-adressering en veel IP-protocollen voor communicatie via internet, een wereldwijd systeem van onderling verbonden computernetwerken. (LAN's kunnen IP-adressering en IP-protocollen ook gebruiken voor het communiceren binnen een LAN-netwerk, hoewel het gebruik van MAC-adressen al volstaat voor interne communicatie.) Voordat IP-adressering wordt toegelicht, vindt u hieronder eerst uitleg over enkele basiselementen voor communicatie via internet, zoals routers, firewalls en internetproviders.

Routers

Om gegevenspakketten van het ene LAN naar een ander door te sturen via internet, moet een netwerkapparaat, de netwerkrouter, worden gebruikt. Een router leidt informatie van het ene netwerk naar een ander netwerk op basis van IP-adressen. Deze stuurt alleen gegevenspakketten door die naar een ander netwerk moeten worden verzonden. Een router wordt meestal gebruikt om een lokaal netwerk op internet aan te sluiten. Routers worden doorgaans gateways genoemd.

Firewalls

Een firewall is ontworpen om onbevoegde toegang tot of vanaf een particulier netwerk te voorkomen. Een firewallscan kan zowel in hardware, in software of in een combinatie van beide worden geïmplementeerd. Firewalls worden vaak gebruikt om te verhinderen dat onbevoegde internetgebruikers toegang krijgen tot particuliere netwerken die verbonden zijn met internet. Berichten van of naar internet gaan door de firewall, die elk bericht onderzoekt en berichten die niet voldoen aan de opgegeven beveiligingscriteria, blokkeert.

Internetverbindingen

Om een LAN met internet te verbinden, moet een netwerkverbinding via een internetprovider (ISP) tot stand worden gebracht. Bij het verbinden met internet worden termen zoals upstream en downstream gebruikt. Upstream beschrijft de overdrachtsnelheid waarmee de gegevens van het apparaat kunnen worden geüpload naar internet, bijvoorbeeld wanneer een video wordt verzonden vanaf een netwerkcamera. Downstream is de overdrachtsnelheid voor het downloaden van bestanden, bijvoorbeeld wanneer video wordt ontvangen door een bewakingscomputer. In de meeste scenario's, zoals een laptop die met internet is verbonden, is het downloaden van informatie van internet de belangrijkste snelheid waarmee rekening moet worden gehouden. Bij een netwerkvideotoepassing met een netwerkcamera op een externe locatie is de upstreamsnelheid belangrijker omdat de gegevens (video) van de netwerkcamera worden geüpload naar internet.

9.2.1 IP-adressering

Elk apparaat dat via internet wil communiceren met andere apparaten moet een uniek en geschikt IP-adres hebben. IP-adressen worden gebruikt voor het identificeren van de verzend- en ontvangstapparaten. Er zijn momenteel twee IP-versies: IP-versie 4 (IPv4) en IP-versie 6 (IPv6). Het belangrijkste verschil tussen de twee is dat de lengte van een IPv6-adres langer is (128 bits ten opzichte van 32 bits voor IPv4-adres). De adressen die tegenwoordig het meest worden gebruikt, zijn IPv4-adressen.

9.2.1.1 IPv4-adressen

IPv4-adressen zijn in vier blokken gegroepeerd en elk blok wordt gescheiden door een punt. Elk blok stelt een getal voor tussen 0 en 255; bijvoorbeeld 192.168.12.23. Bepaalde blokken IPv4-adressen zijn exclusief gereserveerd voor particulier gebruik. Deze particuliere IP-adressen zijn 10.0.0.0 tot 10.255.255.255, 172.16.0.0 tot 172.31.255.255 en 192.168.0.0 tot 192.168.255.255. Dergelijke adressen kunnen alleen worden gebruikt op particuliere netwerken en mogen niet naar internet worden doorgestuurd via een router. Alle apparaten die via internet willen communiceren, moeten hun eigen individuele, openbare IP-adres hebben. Een openbaar IP-adres is

een adres dat wordt toegewezen door een internetprovider (ISP). Een ISP kan een dynamisch IP-adres toewijzen dat tijdens een sessie kan veranderen of een statisch adres waarvoor meestal maandelijks een bijdrage betaald moet worden.

Poorten

Een poortnummer definieert een specifieke service of toepassing zodat de ontvangende server (bijv. netwerkcamera) weet hoe de binnenkomende gegevens moeten worden verwerkt. Wanneer een computer gegevens verzendt die aan een specifieke locatie zijn gekoppeld, voegt deze meestal automatisch het poortnummer toe aan een IP-adres, zonder dat de gebruiker hiervan op de hoogte is. Poortnummers liggen tussen 0 tot 65535. Bepaalde toepassingen gebruiken poortnummers die vooraf aan deze toepassingen zijn toegewezen door de Internet Assigned Numbers Authority (IANA). Een webservice via HTTP is bijvoorbeeld standaard toegewezen aan poort 80 op een netwerkcamera.

IPv4-adressen instellen

Wanneer een netwerkcamera of een video-encoder moet kunnen werken in een IP-netwerk, moet een IP-adres worden toegewezen aan het apparaat. Er zijn twee manieren op een IPv4-adres in te stellen voor een netwerkvideoproduct van Axis: 1) automatisch via DHCP (Dynamic Host Configuration Protocol) en 2) handmatig door een statisch IP-adres, een subnetmasker en het IP-adres van de standaardrouter in te voeren in de interface van het netwerkvideoproduct, of door gebruik te maken van een beheerprogramma zoals AXIS Camera Management. DHCP beheert een groep IP-adressen die dynamisch kunnen worden toegewezen aan een netwerkcamera/video-encoder. De DHCP-functie wordt vaak uitgevoerd door een breedbandrouter, die op zijn beurt IP-adressen krijgt van een internetprovider. Het gebruiken van een dynamisch IP-adres betekent dat het IP-adres voor een netwerkapparaat dagelijks kan veranderen. Bij dynamische IP-adressen wordt het aanbevolen dat gebruikers een domeinnaam (bijv. www.mijncamera.com) voor het netwerkvideoproduct registreren op een dynamische DNS-server (Domain Name System) die de domeinnaam voor het product altijd kan koppelen aan elk IP-adres dat op dat moment is toegewezen. (Een domeinnaam kan worden geregistreerd bij enkele populaire dynamische DNS-sites zoals www.dyndns.org. Axis biedt ook haar eigen AXIS Internet Dynamic DNS Service op www.axiscam.net, toegankelijk via de webinterface van een netwerkvideoproduct van Axis.)

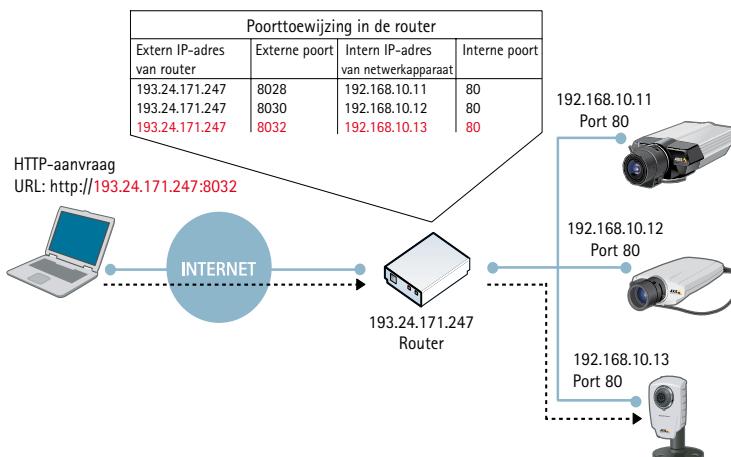
Het instellen van een IPv4-adres via DHCP, gebeurt als volgt. Wanneer een netwerkcamera/video-encoder online komt, verzendt deze een aanvraag waarin de configuratie van een DHCP-server wordt gevraagd. De DHCP-server antwoordt met een IP-adres en subnetmasker. Het netwerkvideoproduct kan vervolgens een dynamische DNS-server bijwerken met het huidige IP-adres, zodat gebruikers toegang kunnen krijgen tot het product via een domeinnaam. Met AXIS Camera Management kan de software automatisch IP-adressen zoeken en instellen en de verbindingssstatus weergeven. De software kan ook worden gebruikt om statische, particuliere IP-adressen toe te wijzen voor netwerkvideoproducten van Axis. Dit wordt aanbevolen wanneer videobeheersoftware wordt gebruikt voor de toegang tot netwerkvideoproducten. In een netwerkvideosysteem met potentieel honderden camera's is een softwareprogramma zoals AXIS Camera Management nodig om het systeem effectief te beheren. *Raadpleeg hoofdstuk 11 voor meer informatie over videobeheer.*

NAT (Network address translation)

Wanneer een netwerkapparaat met een particulier IP-adres informatie via internet wil verzenden, moet dit gebeuren via een router die NAT ondersteunt. Met deze techniek kan een router een particulier IP-adres omzetten naar een openbaar IP-adres zonder dat de verzendhost dat weet.

Port forwarding

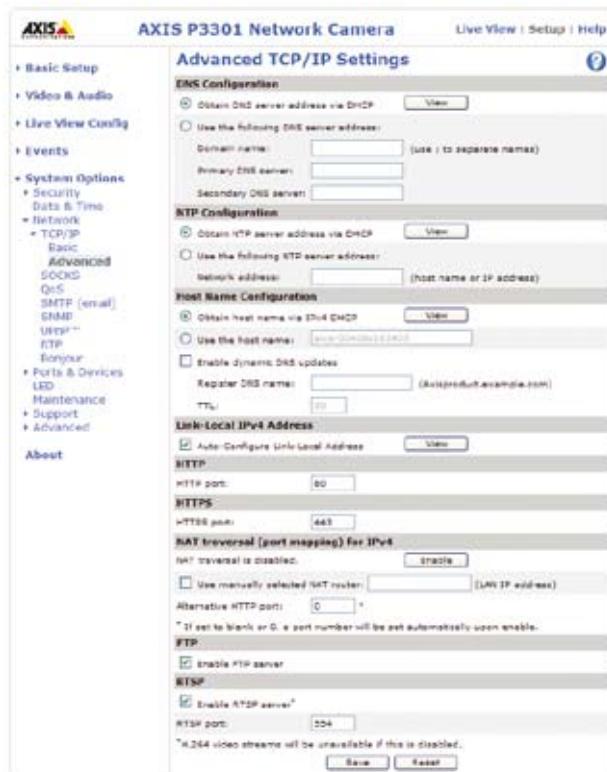
Om via internet toegang te krijgen tot camera's die zich op een particulier LAN bevinden, moet het openbaar IP-adres van de router samen met het overeenkomende poortnummer voor de netwerk-camera/video-encoder op het particuliere netwerk worden gebruikt. Een webservice via HTTP wordt standaard toewezen aan poort 80. Wat gebeurt er wanneer er meerdere netwerkcamera's/video-encoders zijn die poort 80 gebruiken voor HTTP in een particulier netwerk? In plaats van het standaard HTTP-poortnummer voor elk netwerkvideoproduct te wijzigen, kan een router worden geconfigureerd om een uniek HTTP-poortnummer te koppelen aan het particuliere IP-adres van een netwerkvideoproduct en de standaard HTTP-poort. Dit is een proces dat 'port forwarding' wordt genoemd. Port forwarding werkt als volgt. De binnenvloeiende gegevenspakketten bereiken de router via het openbare (externe) IP-adres van de router en een specifiek poortnummer. De router is geconfigureerd om gegevens die binnenkomen op een vooraf gedefinieerd poortnummer door te sturen naar een specifiek apparaat aan de particuliere netwerkzijde van de router. De router vervangt vervolgens het adres van de afzender door het eigen particuliere (intern) IP-adres. Voor een ontvangende client lijkt het alsof de pakketten afkomstig zijn van de router. Het omgekeerde gebeurt met uitgaande gegevenspakketten. De router vervangt het particuliere IP-adres van het bronapparaat door het openbare IP-adres van de router voordat de gegevens via internet worden verzonden.



Afbeelding 9.2a Dankzij de 'port forwarding' in de router zijn netwerkcamera's met particuliere IP-adressen op een lokaal netwerk toegankelijk via internet. In deze afbeelding weet de router dat de gegevens die binnenkomen op poort 8032 (aanvraag), moeten worden doorgestuurd naar een netwerkcamera met een particulier IP-adres 192.168.10.13 poort 80. De netwerkcamera kan vervolgens beginnen met het verzenden van video.

Port forwarding gebeurt doorgaans door eerst de router te configureren. Verschillende routers hebben verschillende manieren om 'port forwarding' uit te voeren en er zijn websites, zoals www.portforward.com die stapsgewijze instructies bieden voor verschillende routers. Bij port forwarding wordt de interface van de router meestal geopend via een internetbrowser. Daarna wordt het openbare (externe) IP-adres van de router ingevoerd, samen met een uniek poortnummer dat vervolgens wordt toegewezen aan het interne IP-adres van het specifieke netwerkvideo-product en het poortnummer ervan voor de toepassing.

Om de taak van port forwarding te vergemakkelijken, biedt Axis de NAT traversal-functie in veel van zijn netwerkvideoproducten. NAT traversal zal automatisch proberen de poorttoewijzing in een NAT-router op het netwerk te configureren met UPnP™. In de interface van het netwerkvideoproduct kunnen gebruikers handmatig het IP-adres van de NAT-router invoeren. Als een router niet handmatig is opgegeven, zoekt het netwerkvideoproduct automatisch NAT-routers op het netwerk en selecteert het de standaardrouter. Als er geen poort handmatig is ingevoerd, zal de service daarnaast automatisch een HTTP-poort selecteren.



Afbeelding 9.2b Met netwerkvideoproducten van Axis kan port forwarding worden ingesteld met NAT traversal.

9.2.1.2 IPv6-adressen

Een IPv6-adres wordt geschreven in een hexadecimale notatie met dubbele punten die het adres onderverdelen in acht blokken van elk 16 bits, bijv. 2001:0da8:65b4:05d3:1315:7c1f:0461:7847. De belangrijkste voordelen van IPv6 zijn onder andere het beschikbaar stellen van een zeer groot aantal IP-adressen en de mogelijkheid om het IP-adres van een apparaat automatisch te configureren met behulp van het MAC-adres. Voor communicatie via internet vraagt en ontvangt de host de benodigde prefix van het openbare adresblok en aanvullende informatie van de router. In dat geval worden de prefix en de suffix van de host gebruikt, zodat DHCP voor de toewijzing van IP-adressen en het handmatig instellen van IP-adressen niet langer nodig is met IPv6. Port forwarding is evenmin nog nodig. Andere voordelen van IPv6 zijn onder andere het hernummeren voor het vergemakkelijken van het schakelen van volledige bedrijfsnetwerken tussen providers, een snellere routering, point-to-point-versleuteling volgens IPSec en connectiviteit via hetzelfde adres bij het veranderen van netwerken (Mobiele IPv6). Een IPv6-adres wordt in een URL tussen vierkante haken geplaatst en een specifieke poort kan op de volgende manier worden geadresseerd: [http://\[2001:0da8:65b4:05d3:1315:7c1f:0461:7847\]:8081/](http://[2001:0da8:65b4:05d3:1315:7c1f:0461:7847]:8081/)

Het instellen van een IPv6-adres voor een netwerkvideoproduct van Axis is even eenvoudig als het inschakelen van een vakje om IPv6 in het product in te schakelen. Het product ontvangt vervolgens een IPv6-adres volgens de configuratie in de netwerkrouter.

9.2.2 Datatransportprotocollen voor netwerkvideo

Het TCP (Transmission Control Protocol) en UDP (User Datagram Protocol) zijn de IP-protocollen die worden gebruikt voor het verzenden van gegevens. Deze transportprotocollen treden op als dragers voor talrijke andere protocollen. Zo wordt bijvoorbeeld HTTP (Hyper Text Transfer Protocol), dat wordt gebruikt om via internet te surfen op webpagina's van servers over de hele wereld, gedragen door TCP.

TCP biedt een betrouwbaar, op verbindingen gebaseerd transmissiekanaal. TCP zorgt voor het proces waarbij grote brokken gegevens worden onderverdeeld in kleinere pakketten en zorgt ervoor dat gegevens die vanaf de ene kant worden verzonden, worden ontvangen aan de andere kant. De betrouwbaarheid van TCP door opnieuw verzenden kan aanzienlijke vertragingen opleveren. TCP wordt doorgaans gebruikt wanneer betrouwbare communicatie de voorkeur krijgt boven transportlatentie.

UDP is een verbindingsloos protocol en garandeert niet de aflevering van de verzonden gegevens, zodat de toepassing zelf het volledige controlemechanisme en de foutcontrole moet verzorgen. UDP biedt geen transmissies van verloren gegevens en veroorzaakt daarom geen verdere vertragingen.

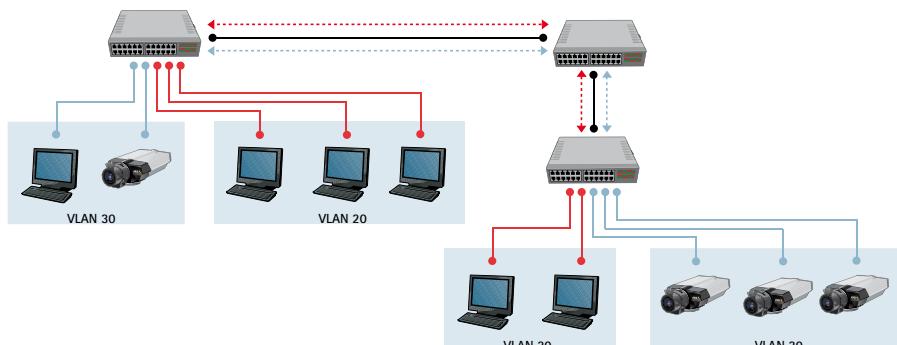
Protocol	Transport protocol	Poort	Gemeenschappelijk gebruik	Netwerk video gebruik
FTP (File Transfer Protocol)	TCP	21	Overdracht van bestanden via internet/intranet	De overdracht van beelden of video vanaf een netwerkkamera/video-encoder naar een FTP-server of naar een toepassing.
SMTP (Send Mail Transfer Protocol)	TCP	25	Protocol voor het verzenden van e-mailberichten	Een netwerkkamera/video-encoder kan beelden of alarmmeldingen verzenden met de ingebouwde e-mailclient.
HTTP (Hyper Text Transfer Protocol)	TCP	80	Wordt gebruikt om op het web te surfen, d.w.z. om webpagina's op te halen van webservers	De meest gebruikte manier om video over te dragen vanaf een netwerkkamera/video-encoder waarbij het netwerkvideo-apparaat voornamelijk werkt als een webserver die de video beschikbaar maakt voor de gebruiker die de aanvraag heeft ingediend of voor de toepassings-server.
HTTPS (Hypertext Transfer Protocol over Secure Socket Layer)	TCP	443	Wordt gebruikt om webpagina's op een veilige manier te openen met behulp van de coderingstechnologie	Beveiligen van de transmissie van video van netwerkkamera's/video-encoders.
RTP (Real Time Protocol)	UDP/TCP	Niet gedefinieerd	RTP-gestandaardiseerd pakketformaat voor het leveren van audio en video via internet—vaak gebruikt bij het streamen van mediasystemen of videovergaderingen	Een algemene manier voor het verzenden van op H.264/MPEG-gebaseerde netwerkvideo en voor het synchroniseren van video en audio omdat RTP volgnummering en tijdstempels voor gegevenspakketten biedt. Hierdoor kunnen de gegevenspakketten opnieuw worden samengesteld in de juiste volgorde. De transmissie kan unicast of multicast zijn.
RTSP (Real Time Streaming Protocol)	TCP	554	Wordt gebruikt voor het instellen en beheren van multimedia-sessies via RTP	

Tabel 9.2a *Algemene TCP/IP-protocollen en -poorten die worden gebruikt voor netwerkvideo.*

9.3 VLAN's

Wanneer een netwerkvideosysteem wordt ontworpen, is er vaak de behoefte om het netwerk gescheiden te houden van andere netwerken, zowel vanwege de veiligheid als vanwege de prestaties. Op het eerste gezicht is de voor de hand liggende keuze het bouwen van een afzonderlijk netwerk. Terwijl het ontwerp wordt vereenvoudigd, worden de kosten voor de aanschaf, de installatie en het onderhoud van het netwerk vaak hoger dan wanneer gebruik wordt gemaakt van en technologie die VLAN (virtueel LAN-netwerk) wordt genoemd.

VLAN is een technologie voor het virtueel segmenteren van netwerken, een functie die door de meeste netwerkswitches wordt ondersteund. Dit kan worden bereikt door de netwerkgebruikers in logische groepen te splitsen. Alleen gebruikers in een specifieke groep zijn in staat gegevens uit te wisselen of krijgen toegang tot bepaalde bronnen op het netwerk. Als een netwerkvideosysteem in een VLAN wordt gesegmenteerd, krijgen alleen de servers op dat VLAN toegang tot de netwerkkamera's. VLAN's bieden doorgaans een betere en voordeligere oplossing dan een afzonderlijk netwerk. IEEE 802.1Q is het primaire protocol dat wordt gebruikt bij het configureren van VLAN's. Dit protocol labelt elk frame of pakket met extra bytes om aan te geven bij welk virtueel netwerk het pakket hoort.

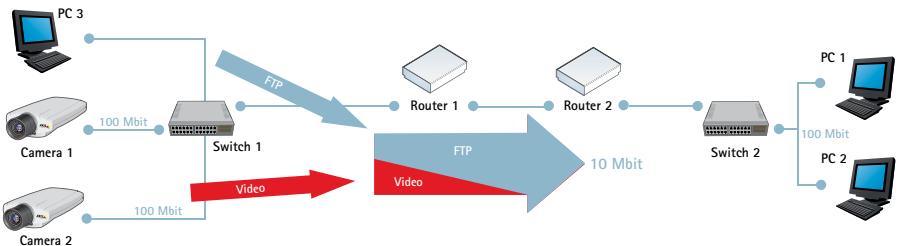


Afbeelding 9.3a In deze afbeelding zijn de VLAN's ingesteld via meerdere switches. Eerst worden beide verschillende LAN's gesegmenteerd in VLAN 20 en VLAN 30. De verbindingen tussen de switches zorgen voor gegevensoverdracht van verschillende VLAN's. Alleen leden van hetzelfde VLAN kunnen gegevens uitwisselen, hetzij binnen hetzelfde netwerk of via verschillende netwerken. VLAN's kunnen worden gebruikt om een videonetwerk te scheiden van een kantoornetwerk.

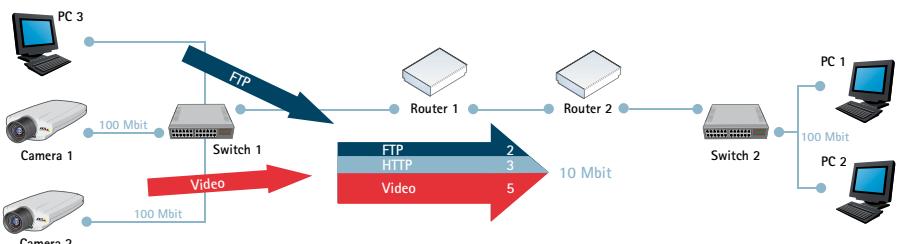
9.4 Servicekwaliteit (QoS)

Aangezien verschillende toepassingen, zoals telefoon, e-mail en surveillancevideo, mogelijk hetzelfde IP-netwerk gebruiken, bestaat de noodzaak om te bepalen hoe netwerkbronnen worden gedeeld om te voldoen aan de vereisten van elke service. Eén oplossing is ervoor zorgen dat netwerk routers en switches op een verschillende manier werken op verschillende soorten services (spraak, gegevens en video) wanneer het verkeer het netwerk passeert. Door Servicekwaliteit (QoS) te gebruiken, kunnen verschillende netwerktoepassingen naast elkaar bestaan in hetzelfde netwerk, zonder dat deze elkaar bandbreedte gebruiken.

De term Servicekwaliteit (QoS= Quality of Service) verwijst naar een aantal technologieën zoals Differentiated Service Codepoint (DSCP), die het gegevenstype in een gegevenspakket kunnen identificeren en hierdoor de pakketten kunnen opsplitsen in klassen voor verkeer waarvoor een voorkeur kan worden ingesteld voor het doorsturen. De belangrijkste voordelen van een QoS-bewust netwerk zijn onder andere de mogelijkheid om verkeer voorrang te verlenen, zodat kritieke stromen kunnen worden bediend vóór stromen met een lagere voorrang, en de grotere betrouwbaarheid in een netwerk door het beheren van de hoeveelheid bandbreedte die een toepassing kan gebruiken, waardoor het gevecht om bandbreedte tussen toepassingen kan worden beheerd. PTZ-verkeer, dat vaak als kritiek wordt beschouwd, en een lage latentie vereist, is een typisch geval waarbij QoS kan worden gebruikt om een snelle respons op verplaatsingsaanvragen te garanderen. De eerste vereiste voor het gebruik van QoS binnen een videonetwerk is dat alle switches, routers en netwerkvideoproducten QoS moeten ondersteunen.



Afbeelding 9.4a Normaal (niet-QoS-bewust) netwerk. In dit voorbeeld bewaakt PC1 twee videostromen van camera's 1 en 2, waarbij de streaming van elke camera plaatsvindt met 2,5 Mbit/s. PC2 start plotseling een bestandsoverdracht van PC3. In dit scenario probeert de bestandsoverdracht de volledige capaciteit van 10 Mbit/s tussen routers 1 en 2 te gebruiken, terwijl de videostromen proberen hun totaal van 5 Mbit/s te behouden. De hoeveelheid bandbreedte die aan het surveillancesysteem wordt gegeven, kan niet langer worden gegarandeerd en de videoframesnelheid zal waarschijnlijk worden verlaagd. In het ongunstigste geval zal het FTP-verkeer alle beschikbare bandbreedte verbruiken.



Afbeelding 9.4b QoS-bewust netwerk. Hier is Router 1 geconfigureerd om tot 5 Mbit/s van de beschikbare 10Mbit/s te gebruiken voor het streamen van video. FTP-verkeer mag 2 Mbit/s gebruiken en HTTP en al het andere verkeer kunnen maximum 3 Mbit/s gebruiken. Met deze opsplitsing zullen videostromen altijd beschikken over de benodigde bandbreedte. Bestandsoverdrachten worden beschouwd als minder belangrijk en krijgen minder bandbreedte, maar er zal nog steeds bandbreedte beschikbaar zijn voor het surfen op internet en voor ander verkeer. Denk eraan dat deze maxima alleen van toepassing zijn wanneer het netwerk ver zadigd is. Als er ongebruikte bandbreedte beschikbaar is, kan dit worden gebruikt door elk type verkeer.

9.5 Netwerkbeveiliging

Er zijn verschillende beveiligingsniveaus met betrekking tot het beveiligen van informatie die wordt verzonden via IP-netwerken. Het eerste niveau is verificatie en machtiging. De gebruiker of het apparaat identificeert zichzelf bij het netwerk en de externe kant via een gebruikersnaam en wachtwoord, die vervolgens worden geverifieerd voordat het apparaat in het systeem wordt toegestaan. Extra beveiliging kan worden bereikt door het coderen van de gegevens om te verhinderen dat anderen de gegevens gebruiken of lezen. Algemene methoden zijn HTTPS (ook bekend als SSL/TLS), VPN en WEP of WPA in draadloze netwerken.. (*Raadpleeg Hoofdstuk 10 voor meer informatie over draadloze beveiliging.*) Het gebruik van codering kan de communicatie vertragen, afhankelijk van het type implementatie en de codering die wordt gebruikt.

9.5.1 Gebruikersnaam- en wachtwoordverificatie

Het gebruik van een gebruikersnaam- en wachtwoordverificatie is de meest fundamentele methode voor het beveiligen van gegevens op een IP-netwerk en kan voldoende zijn wanneer geen hoge beveiligingsniveaus vereist zijn of waar het videonetwerk is gesegmenteerd van het hoofdnetwerk zodat onbevoegde gebruikers geen fysieke toegang tot het videonetwerk hebben. De wachtwoorden kunnen worden gecodeerd of gedecodeerd bij de verzending. De eerste oplossing biedt de beste beveiliging. Netwerkvideoprodukten van Axis bieden wachtwoordbeveiliging op meerdere niveaus. Er zijn drie niveaus: Beheerder (volledige toegang tot alle functionaliteiten), Operator (toegang tot alle functionaliteiten behalve de configuratiepagina's), Kijker (alleen toegang tot live video).

9.5.2 IP-adresfiltering

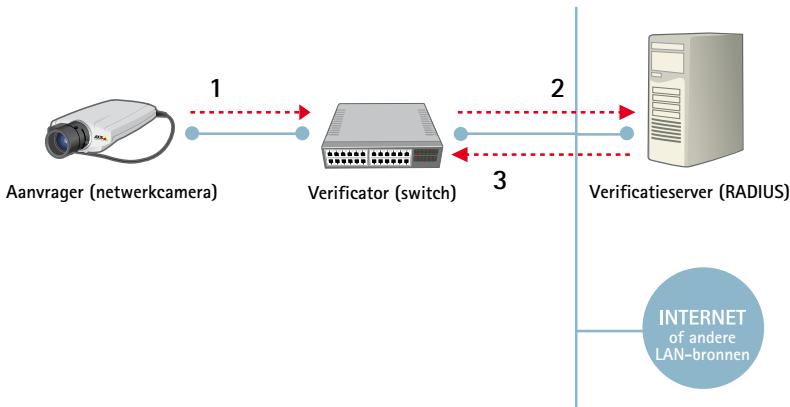
Netwerkvideoprodukten van Axis bieden IP-adresfiltering die toegangsrechten verleent of weigert aan gedefinieerde IP-adressen. Een standaard configuratie is het configureren van de netwerkcamera's om alleen het IP-adres toe te staan van de server die als host optreedt voor de videobeheersoftware om zo toegang te krijgen tot de netwerkvideoprodukten.

9.5.3 IEEE 802.1X

Veel netwerkvideoprodukten van Axis ondersteunen IEEE 802.1X. Dit levert de verificatie voor apparaten die met een LAN-poort zijn verbonden. IEEE 802.1X brengt een point-to-point-verbinding tot stand of verhindert toegang vanaf de LAN-poort als de verificatie mislukt. IEEE 802.1X verhindert de zogenaamde 'port-hijacking', waarbij een onbevoegde computer toegang krijgt tot het netwerk door op een netwerkaansluitingpunt binnen of buiten een gebouwte komen. IEEE 802.1X is nuttig bij netwerkvideotoepassingen omdat netwerkcamera's zich vaak op openbare plaatsen bevinden waar een vrij toegankelijk netwerkaansluitpunt een beveiligingsrisico kan veroorzaken. In de huidige bedrijfsnetwerken wordt IEEE 802.1X een basisvereiste voor alles wat met een netwerk wordt verbonden.

In een netwerkvideosysteem kan IEEE 802.1X als volgt werken: 1) Een netwerkcamera stuurt een aanvraag voor netwerktoegang naar een switch of toegangspunt; 2) de switch of het toegangspunt stuurt de aanvraag door naar een verificatieserver; bijvoorbeeld een RADIUS-server (remote

authentication dial-in user service), zoals een Microsoft IAS-server (Internet Authentication Service); 3) als de verificatie is gelukt, geeft de server de switch of het toegangspunt de opdracht de poort te openen om de gegevens voor de netwerkcamera toegang te verlenen om door de switch te gaan en via het netwerk te worden verzonden.



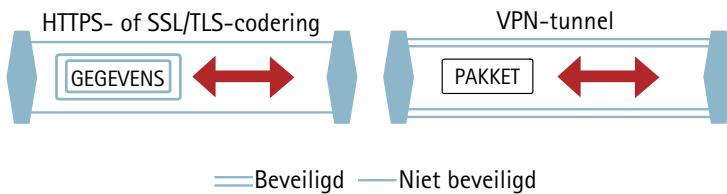
Afbeelding 9.5a IEEE 802.1X biedt op een poort gebaseerde beveiliging en heeft een aanvrager (bijv. een netwerkcamera), een verificator (bijv. een switch) en een verificatieserver nodig. Stap 1: netwerktoegang vereist; stap 2: aanvraag doorgestuurd naar verificatieserver; stap 3: verificatie is gelukt en de switch krijgt de opdracht de netwerkcamera toe te staan gegevens via het netwerk te verzenden.

9.5.4 HTTPS of SSL/TLS

HTTPS (Hyper Text Transfer Protocol Secure) is identiek aan HTTP maar er is één belangrijk verschil: de overgedragen gegevens worden gecodeerd met SSL (Secure Socket Layer) of TLS (Transport Layer Security). Deze beveiligingsmethode past codering toe op de gegevens zelf. Veel netwerkvideoproducten van Axis hebben een ingebouwde ondersteuning voor HTTPS. Hierdoor kan de video veilig worden weergegeven via een webbrowser. Het gebruik van HTTPS kan echter de communicatieverbinding vertragen en daardoor de framesnelheid van de video vertragen.

9.5.5 VPN (Virtueel particulier netwerk)

Met VPN kan een veilige 'tunnel' tussen twee communicerende apparaten worden gemaakt, zodat een veilige en beveiligde communicatie via internet mogelijk is. In een dergelijke opstelling wordt het originele pakket gecodeerd, inclusief de gegevens en hun koptekst die informatie kan bevatten zoals de bron- en doeladressen, het type informatie dat wordt verzonden, het pakketnummer in de reeks pakketten en de pakketlengte. Het gecodeerde pakket wordt vervolgens ingekapseld in een ander pakket dat alleen de IP-adressen van de twee communicerende apparaten toont (bijvoorbeeld routers). Deze opstelling beschermt het verkeer en de inhoud ervan tegen onbevoegde toegang en alleen de apparaten met de juiste 'sleutel' kunnen werken in het VPN. Er is er geen toegang tot de gegevens en de gegevens kunnen niet worden bekeken met behulp van de netwerkapparaten tussen de client en de server.



Afbeelding 9.5b Het verschil tussen HTTPS (SSL/TLS) en VPN is dat alleen in HTTPS de eigenlijke gegevens van een pakket worden gecodeerd. Met VPN kan het volledige pakket worden gecodeerd en ingekapseld om een beveiligde 'tunnel' te maken. Beide technologieën kunnen parallel worden gebruikt, maar dit wordt niet aanbevolen omdat elke technologie overhead zal toevoegen en de prestaties van het systeem zal doen afnemen.

Draadloze technologieën

Draadloze technologie biedt voor videosurveillancetoepassingen een flexibele, kostenbesparende en snelle manier om camera's in te zetten, vooral bij grote oppervlakten zoals een parkeerplaats of een stadscentrum. Het is niet nodig een kabel onder de grond door te trekken. In oudere gebouwen, die als monument worden beschermd, is draadloze technologie wellicht de enige mogelijkheid wanneer er geen standaard Ethernet-kabels mogen worden geïnstalleerd. Axis biedt camera's met ingebouwde draadloze ondersteuning. Netwerkcamera's zonder ingebouwde draadloze technologie kunnen nog steeds in een draadloos netwerk worden geïntegreerd wanneer een draadloze brug wordt gebruikt.



Afbeelding 10a Een draadloze netwerkcamera van Axis die gebruik maakt van 802.11b/g.



Afbeelding 10b Wanneer een draadloze brug wordt gebruikt, kan elke netwerkcamera in een draadloos netwerk worden gebruikt.

10.1 WLAN–standaarden 10.1 802.11

De meest gebruikte draadloze standaard voor WLAN's (wireless local area networks) is de 802.11-standaard van IEEE. Hoewel er ook andere standaarden en merkgebonden technologieën zijn, hebben de 802.11 draadloze standaarden als voordeel dat deze actief zijn in een spectrum waar geen licentie benodigd is, met andere woorden: er hoeven geen licentiekosten worden betaald voor het instellen en functioneren van het netwerk. De belangrijkste extensies van de standaarden zijn 802.11b, 802.11g, 802.11a en 802.11n.

802.11b, dat is goedgekeurd in 1999, werkt in het 2.4 GHz-bereik en levert datasnelheden tot maximaal 11 Mbit/s. Tot 2004 waren de meeste WLAN-producten gebaseerd op 802.11b.

802.11g, dat is goedgekeurd in 2003, is de meest gebruikelijke variant van 802.11 op de markt. Het werkt in het 2.4 GHz-bereik en levert gegevensnelheden tot maximaal 54 Mbit/s. WLAN-producten zijn meestal compatibel met 802.11b/g.

802.11a, dat is goedgekeurd in 1999, werkt in het 5 GHz-frequentiebereik en levert datasnelheden tot maximaal 54 Mbit/s. Het 5 GHz-frequentiebereik is echter niet beschikbaar voor gebruik in delen van Europa waar dit bereik is toegewezen aan militaire radarsystemen. In dergelijke gebieden moeten WLAN-componenten van 5 GHz in overeenstemming met de 802.11a/h-standaard zijn. Een ander nadeel van 802.11a is dat het signaalbereik kleiner is dan dat van 802.11g, omdat dit in een hogere frequentie werkt. Als gevolg daarvan zijn er veel meer toegangspunten nodig voor overdracht in het 5 GHz-bereik dan in het 2.4 GHz-bereik.

802.11n, dat nog niet gereed en goedgekeurd is, is de volgende generatie standaard waarmee datasnelheden tot maximaal 600 Mbit/s mogelijk zijn. Producten die 802.11n ondersteunen, zijn gebaseerd op een concept van de standaard.

Wanneer u een draadloos netwerk instelt, moet u rekening houden met de bandbreedtecapaciteit van het toegangspunt en met de bandbreedtevereisten voor de netwerkapparaten. In het algemeen is de nuttige gegevensdoorvoer die wordt ondersteund door een bepaalde WLAN-standaard circa de helft van de bitsnelheid die door een standaard wordt bepaald, als gevolg van signaal- en protocoloverhead. Met netwerkkamera's die 802.11g ondersteunen, kunnen niet meer dan vier of vijf van dergelijke camera's worden aangesloten op een draadloos toegangspunt.

10.2 Beveiliging van WLAN

Vanwege de aard van draadloze communicatie kan iedereen met een draadloos apparaat dat aanwezig is in een gebied dat door een draadloos netwerk wordt gedekt, het netwerk delen en gegevens die worden overgedragen onderscheppen, tenzij het netwerk is beveiligd.

Om onbevoegde toegang tot de overgedragen gegevens en tot het netwerk te voorkomen, zijn er technologieën zoals WEP en WPA/WPA2 ontwikkeld, waardoor onbevoegde toegang wordt voorkomen en wordt voorkomen dat gecodeerde gegevens niet via het netwerk worden verzonden.

10.2.1 WEP (Wired Equivalent Privacy)

Door WEP kunnen personen zonder de juiste sleutel geen toegang tot het netwerk krijgen. Er zijn echter zwakke punten in WEP. Dit zijn onder andere sleutels die relatief kort zijn en andere foutjes waardoor sleutels gereconstrueerd kunnen worden door middel van een relatief klein deel onderschept verkeer. Tegenwoordig wordt WEP niet meer als voldoende veilig beschouwd omdat er een verscheidenheid aan hulpprogramma's gratis op internet verkrijgbaar is waarmee een WEP-sleutel die geacht wordt geheim te zijn, gekraakt kan worden.

10.2.2 WPA/WPA2 (WiFi Protected Access)

De beveiliging wordt aanzienlijk verbeterd door WPA, waarmee de tekortkomingen in de WEP-standaard worden opgelost. WPA voegt een standaardmethode toe voor het verspreiden van gecodeerde sleutels.

10.2.3 Aanbevelingen

Enkele richtlijnen voor het gebruik van draadloze camera's voor bewaking:

- > Activeer de gebruikersnaam / het wachtwoord voor aanmelding in de camera's.
- > Activeer de codering (HTTPS) in de draadloze router / camera's. Dit moet worden gedaan voordat de sleutels of referenties voor WLAN worden ingesteld, om te voorkomen dat er onbevoegd toegang tot het netwerk wordt verkregen door gestolen referenties.
- > Zorg dat draadloze camera's beveiligingsprotocollen ondersteunen zoals IEEE 802.1X en WPA/WPA2.

10.3 Draadloze bruggen

Sommige oplossingen maken gebruik van andere standaarden dan de overheersende standaard IEEE 802.11 en bieden grotere prestaties en veel grotere afstanden in combinatie met een zeer sterke beveiling. Twee algemeen gebruikte technologieën zijn microgolf en laser, die kunnen worden gebruikt om gebouwen of locaties met elkaar te verbinden met een 'point-to-point' dataverbinding met hoge snelheid.

Videobeheersystemen

Een belangrijk aspect van een videosurveillance-systeem is het beheren van videobeelden voor live weergave, opnemen, afspelen en opslag. Wanneer deze systemen uit slechts één camera of enkele camera's bestaan, kunnen weergaven en enkele basis-video-opnamen worden beheerd via de ingebouwde webinterface van de netwerkcamera's en video-encoders. Wanneer het systeem uit meer dan enkele camera's bestaat, wordt het aanbevolen om een beheersysteem voor netwerkvideo te gebruiken.

Tegenwoordig zijn er honderden verschillende videobeheersystemen beschikbaar, die geschikt zijn voor verschillende besturingssystemen (Windows, UNIX, Linux en Mac OS), marktsegmenten en talen. U moet rekening houden met de keuze van het hardwareplatform (pc via een server of een pc via een netwerkvideorecorder), het softwareplatform, de systeemfuncties, waaronder installatie en configuratie, gebeurtenisbeheer, intelligente video, beheer en beveiliging en integratiemogelijkheden met andere systemen zoals POS (verkooppunten) of gebouwenbeheer.

11.1 Hardwareplatforms

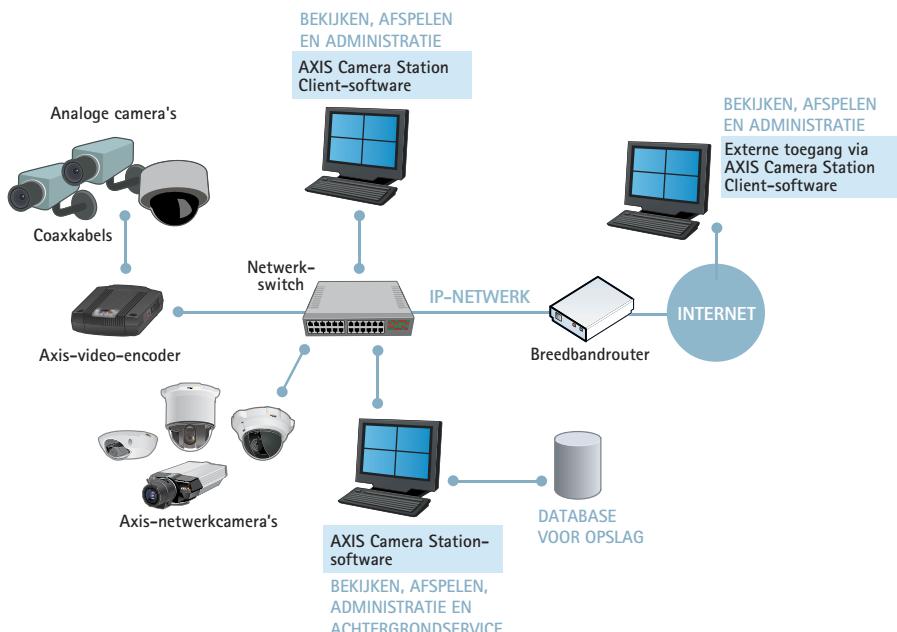
Er zijn twee verschillende typen hardwareplatforms voor een beheersysteem voor netwerkvideo: een pc-serverplatform met een of meer pc's die een softwareprogramma voor videobeheer uitvoeren en een platform dat gebaseerd is op een netwerkvideorecorder (NVR), wat merkgebonden hardware is met vooraf geïnstalleerde videobeheersoftware.

11.1.1 Pc-serverplatform

Voor een oplossing voor videobeheer die is gebaseerd op een pc-serverplatform zijn pc-servers nodig en in de handel verkrijgbare opslagapparatuur voor een optimale prestatie voor het speciale doel van het systeem. Bij een dergelijk open platform is het eenvoudiger om functionaliteit aan het systeem toe te voegen, zoals meer of externe opslag, firewalls, beveiliging tegen virusen en intelligente videoalgoritmen, parallel met een softwareprogramma voor videobeheer.

Een pc-serverplatform kan ook volledig worden uitgebreid waardoor elk gewenst aantal netwerkvideoproducten aan het systeem kan worden toegevoegd. De systeemhardware kan worden

uitgebreid of worden geüpgraded om aan hogere prestatievereisten te kunnen voldoen. Een open platform kan gemakkelijker met andere systemen worden geïntegreerd, zoals toegangscontrole-, gebouwbeheer- en industriële regelsystemen. Hierdoor kunnen gebruikers via één programma en één gebruikersinterface videotoezicht en overig toezicht van het gebouw beheren. *Raadpleeg hoofdstuk 12 voor meer informatie over servers en opslag.*

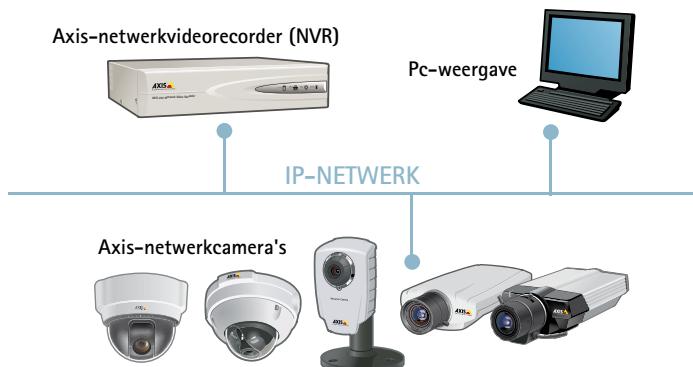


Afbeelding 11.1a *Een netwerkvideosurveillance-systeem via een open pc-serverplatform met AXIS Camera Station-software voor videobeheer.*

11.1.2 NVR-platform

Een netwerkvideorecorder wordt geleverd als één geheel met vooraf geïnstalleerde functies voor videobeheer. In dit opzicht is een NVR gelijk aan een DVR. Sommige DVR's, die vaak hybride DVR's worden genoemd, hebben een NVR-functie, dat wil zeggen de mogelijkheid om ook netwerkvideo op te nemen. NVR-hardware is vaak merkgebonden en speciaal bedoeld voor video-beheer. Deze hardware is bedoeld voor specifieke opnametaken, het analyseren en afspeLEN van netwerkvideo en er kunnen vaak geen andere toepassingen op gebruikt worden. Het besturingssysteem kan Windows, UNIX/Linux of merkgebonden zijn.

Een NVR is ontworpen voor optimale prestaties voor een bepaalde hoeveelheid camera's, waardoor dit systeem gewoonlijk minder schaalbaar is dan een pc-serversysteem. Hierdoor is dit apparaat geschikt voor kleinere systemen waarbij het aantal camera's binnen de grenzen blijft van de bedoelde capaciteit van de NVR. Een NVR is gewoonlijk eenvoudiger te installeren dan een pc-serverplatformsysteem.



Afbeelding 11.1b Een netwerkvideosurveillance-systeem dat gebruik maakt van een NVR.

11.2 Softwareplatforms

Er kunnen verschillende softwareplatforms worden gebruikt voor videobeheer. Dit zijn onder andere de ingebouwde webinterface, die zich in veel netwerkvideoproducten bevindt of het gebruik van een afzonderlijk softwareprogramma voor videobeheer dat een Windows-programma of een webinterface kan zijn.

11.2.1 Ingebouwde functionaliteit

U hebt via het netwerk toegang tot netwerkcamera's en video-encoders van Axis door het IP-adres van het product op de computer in te typen in het adres-/locatieveld van een webbrowser. Zodra er verbinding is gemaakt met het netwerkvideoproduct wordt de startpagina van het product automatisch weergegeven in de webbrowser, samen met koppelingen naar de configuratiepagina's van het product.

De ingebouwde webinterface van Axis-netwerkvideoproducten biedt eenvoudige functies voor opnemen, dat wil zeggen het handmatig opnemen van videostromen (H.264, MPEG-4, Motion JPEG) op een server door op een pictogram te klikken of het door een gebeurtenis geactiveerd opnemen van afzonderlijke JPEG-afbeeldingen op een of meerdere locaties. Het door een gebeurtenis geactiveerd opnemen van videostromen is mogelijk met netwerkvideoproducten die lokaal opslaan ondersteunen. In dergelijke gevallen worden de videostromen opgenomen op de SD-/SDHC-kaart van het product. Voor grotere opnameflexibiliteit met betrekking tot modi (bijvoorbeeld continue of geplande opnamen) en functies wordt een afzonderlijk softwareprogramma voor videobeheer vereist. Het configureren en beheren van een netwerkvideoproduct via de ingebouwde webinterface werkt alleen wanneer een klein aantal camera's deel van het systeem uitmaakt.

11.2.2 Windows-clientsoftware

Van de afzonderlijke softwareprogramma's voor videobeheer zijn Windows-clientprogramma's het meest populair. Er zijn ook softwareprogramma's op internet beschikbaar.

Met een Windows-clientprogramma moet de software voor videobeheer eerst op de opnameserver worden geïnstalleerd. Vervolgens kan een clientsoftwareprogramma voor weergave worden geïnstalleerd op dezelfde opnameserver of op een andere pc, lokaal op hetzelfde netwerk waar de opnameserver zich bevindt of extern op een weergavestation op een afzonderlijk netwerk. In sommige gevallen kunnen gebruikers ook met een clienttoepassing schakelen tussen verschillende servers waarop de videobeheersoftware is geïnstalleerd, waardoor videobeheer in een groot systeem of op veel externe locaties mogelijk is.

11.2.3 Software op internet

Een softwareprogramma voor videobeheer op internet moet eerst op een pc-server worden geïnstalleerd die zowel een webserver als een opnameserver bedient. Vervolgens kunnen gebruikers op alle soorten netwerkcomputers overal ter wereld door een webbrowser te gebruiken toegang krijgen tot de videobeheerserver en tot de netwerkproducten die deze beheert..

11.2.4 Schaalbaarheid van videobeheersoftware

De schaalbaarheid van de meeste videobeheersoftware, met betrekking tot het aantal camera's en frames per seconde dat kan worden ondersteund, wordt in de meeste gevallen door de hardwarecapaciteit beperkt in plaats door de software. Het opslaan van videobestanden stelt andere eisen aan de opslaghardware omdat het mogelijk wordt vereist om continu op te slaan in plaats van alleen op te slaan tijdens reguliere openingstijden. Daarnaast genereren videobeelden grote hoeveelheden gegevens die hoge eisen aan de opslagoplossing stellen. *Raadpleeg hoofdstuk 12 voor meer informatie over servers en opslag.*

11.2.5 Open software versus leveranciersspecifieke software

Softwareprogramma's voor videobeheer kunnen worden verkregen via leveranciers van netwerkvideoproducten. Deze programma's ondersteunen alleen de netwerkvideoapparatuur van de leverancier. Er bestaan ook softwareprogramma's die meerdere merken netwerkvideoproducten ondersteunen. Deze zijn vaak afkomstig van onafhankelijke bedrijven. Er is een verscheidenheid aan softwareoplossingen van meer dan 550 Application Development Partners van Axis beschikbaar. Zie www.axis.com/partner/adp

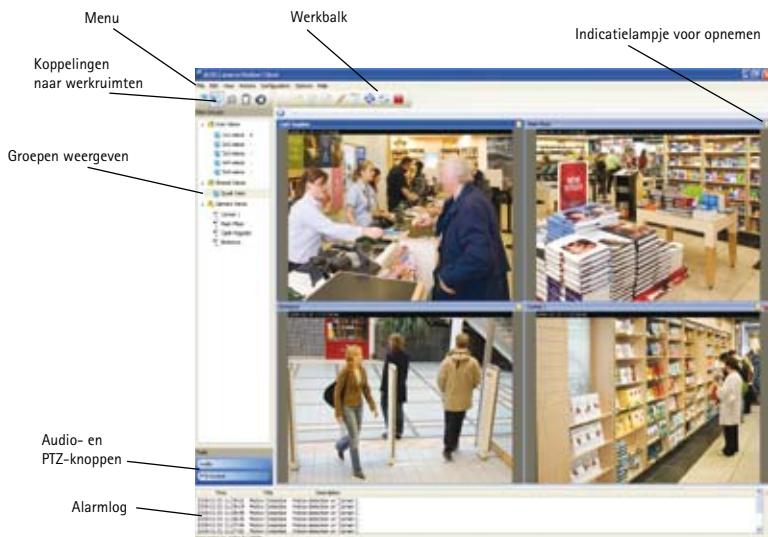
11.3 Systeemfuncties

Er kunnen veel verschillende functies worden ondersteund door een videobeheersysteem. Enkele veelgebruikte functies worden hieronder weergegeven:

- > Gelijktijdig videobeelden van verschillende camera's weergeven
- > Video en audio opnemen
- > Functies voor gebeurtenisbeheer met onder andere intelligente video zoals videobewegingsdetectie
- > Administratie en beheer van de camera
- > Zoekopties en afspeLEN
- > Toegangscontrole voor gebruikers en activiteitenregistratie (audit)

11.3.1 Weergave

Een belangrijke functie van een videobeheersysteem is het op efficiënte en gebruiksvriendelijke wijze weergeven van live en opgenomen videomateriaal. Met de meeste toepassingen voor videobeheersoftware kunnen meerdere gebruikers in verschillende modi kijken, zoals deelweergave (voor gelijktijdige weergave van verschillende camera's), volledig scherm of volgen met de camera (waarbij weergaven van verschillende camera's automatisch worden weergegeven, de een na de ander).

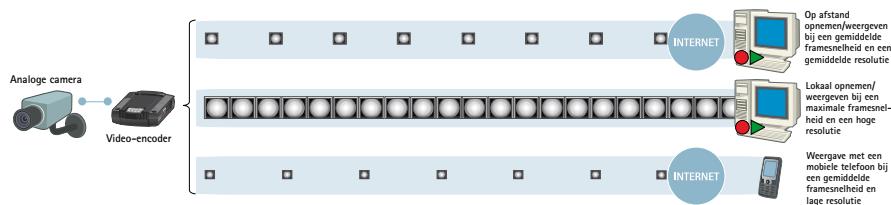


Afbeelding 11.3a Live weergavescherm van AXIS Camera Station

Veel softwareprogramma's voor videobeheer bieden ook een functie voor afspelen van verschillende camera's waardoor gebruikers gelijktijdig genomen opnamen van verschillende camera's kunnen bekijken. Hierdoor krijgen gebruikers de mogelijkheid om een uitvoerig beeld van een gebeurtenis te krijgen, wat nuttig is bij een onderzoek. Extra functies zijn mogelijk het weergeven vanaf en het toewijzen van meerdere monitors waardoor er overlays van camerapictogrammen ontstaan die de locaties van de camera's op een kaart van het gebouw of het gebied weergeven.

11.3.2 Multistreaming

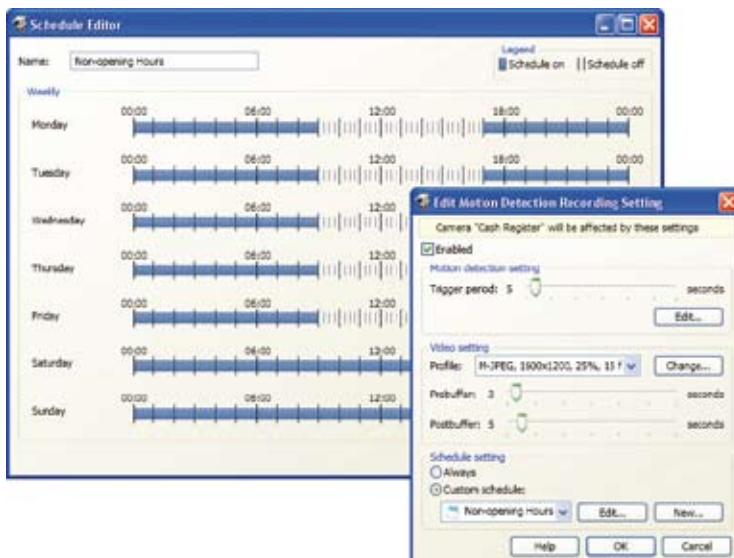
Met de geavanceerde netwerkkamera's kunt u multistreaming inschakelen, waardoor meerdere stromen van een netwerkkamera of een video-encoder afzonderlijk kunnen worden geconfigureerd met verschillende framesnelheden, compressie-indelingen en resoluties en naar verschillende ontvangers kunnen worden verzonden. Met deze mogelijkheid wordt het gebruik van netwerkbandbreedte geoptimaliseerd.



Afbeelding 11.3b Met meerdere, afzonderlijk te configureren videotstromen kan videomateriaal met verschillende framesnelheden en resoluties naar verschillende ontvangers worden verzonden.

11.3.3 Video-opname

Met videobeheersoftware zoals AXIS Camera Station kunnen handmatig video-opnamen worden gemaakt, continu en door activering (door beweging of alarm). Continue opnamen en opnamen door activering kunnen op geplande tijden op elke dag van de week worden uitgevoerd. Voor een continue opname wordt doorgaans meer schijfruimte gebruikt dan voor een opname die door een alarm wordt geactiveerd. Een opname die door een alarm wordt geactiveerd wordt bijvoorbeeld in werking gezet door videobewegingsdetectie of door externe ingangen via de ingangspoort van de camera of de video-encoder. Met geplande opnamen kunnen tijdschema's voor zowel continue opnamen en opnamen die door alarm/beweging worden geactiveerd ingesteld.



Afbeelding 11.3c Instellingen voor geplande opnamen met een combinatie van continue opnamen en opnamen die door alarm/beweging worden geactiveerd, die worden toegepast met AXIS Camera Station-software voor videobeheer.

Zodra de opnamemethode is geselecteerd, kan de kwaliteit van de opnamen worden vastgesteld door het selecteren van de video-indeling (bijvoorbeeld H.264, MPEG-4, Motion JPEG), resolutie, compressieniveau en framesnelheid. Deze parameters zijn van invloed op de hoeveelheid bandbreedte die wordt gebruikt en op de grootte van de opslagruimte die wordt vereist.

Netwerkvideoprodukten kunnen, afhankelijk van de resolutie, verschillende mogelijkheden voor framesnelheden hebben. Te allen tijde op alle camera's opnemen en/of weergeven bij maximale framesnelheid (30 frames per seconde bij NTSC-standaard en 25 frames per seconde bij PAL-standaard) is meer dan hetgeen vereist wordt voor de meeste toepassingen. Onder normale omstandigheden kunnen framesnelheden lager worden ingesteld (bijvoorbeeld één tot vier frames per seconde) om de opslagvereisten aanzienlijk te verminderen. In het geval van alarm (bijvoorbeeld wanneer videobewegingsdetectie of een externe sensor is geactiveerd) kan een afzonderlijke stroom met een hogere framesnelheid voor opname worden verzonden.

11.3.4 Opname en opslag

Bij de meeste videobeheersoftware wordt het standaard Windows-bestandssysteem voor opslag gebruikt en kan dus elk willekeurig systeemstation of bij het netwerk behorende station worden gebruikt voor het opslaan van videobeelden. Bij een softwareprogramma voor videobeheer is er mogelijk meer dan één niveau voor opslag mogelijk. Bijvoorbeeld wanneer opnamen voornamelijk op een primaire vaste schijf (de lokale vaste schijf) worden gemaakt en het archiveren plaatsvindt op lokale schijven, op bij het netwerk behorende stations of op externe vaste schijven. Gebruikers kunnen angeven hoe lang beelden op de primaire vaste schijf moeten blijven voordat deze automatisch worden verwijderd of naar het archiveringsstation worden verplaatst. Gebruikers kunnen ook voorkomen dat door gebeurtenissen geactiveerde videobeelden automatisch worden gewist door deze speciaal te markeren of in het systeem te vergrendelen.

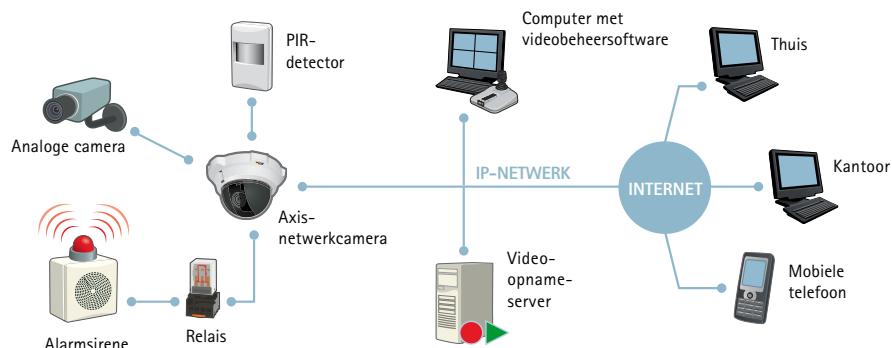
11.3.5 Gebeurtenisbeheer en intelligente video

Gebeurtenisbeheer heeft betrekking op het herkennen of creëren van een gebeurtenis die wordt geactiveerd door invoer, hetzij van ingebouwde functies in de netwerkvideoprodukten of van andere systemen zoals verkoopaansluitpunten of intelligente videosoftware, en op het configureren van het netwerkvideosurveillancesysteem zodat dit automatisch reageert op de gebeurtenis door bijvoorbeeld videobeelden op te nemen, waarschuwingsberichten te verzenden en verschillende zaken te activeren zoals deuren en lichten.

Functies voor gebeurtenisbeheer en intelligente video kunnen samen zorgen dat een videosurveillance-systeem efficiënter gebruik maakt van de bandbreedte en opslagruimte van het netwerk. Live camerabewaking is niet constant vereist omdat er waarschuwingsberichten naar gebruikers kunnen worden verzonden wanneer er zich een gebeurtenis voordoet. Alle geconfigureerde reacties kunnen automatisch worden geactiveerd, waardoor de reactietijden worden verbeterd. Met behulp van gebeurtenisbeheer kunnen gebruikers meer camera's in de gaten houden.

Zowel functies voor gebeurtenissenbeheer als intelligente video kunnen in een netwerkvideo-product of in een softwareprogramma voor videobeheer worden ingebouwd en uitgevoerd. Het kan ook door beide functies worden uitgevoerd, dat wil zeggen dat een softwareprogramma voor videobeheer gebruik kan maken van een functie voor intelligente video die is ingebouwd in een netwerkvideoproduct. In dat geval kan de functionaliteit voor intelligente video, zoals videobevegingsdetectie en manipulatie van de camera, worden uitgevoerd door het netwerkvideoproduct. Dit kan in het beheersoftwareprogramma worden aangegeven in verband met het nemen van verdere stappen. Deze procedure biedt een aantal voordelen:

- > Er kan efficiënter gebruik worden gemaakt van bandbreedte en opslagruijte omdat het niet nodig is dat een camera continu videobeelden naar een videobeheerserver verzendt voor analyse van mogelijke gebeurtenissen. Het analyseren vindt plaats op het netwerkvideoproduct en er worden alleen videostromen voor opname en/of weergave verzonden wanneer zich een gebeurtenis voordoet.
- > Het is niet noodzakelijk dat de videobeheerserver over een snelle verwerkingscapaciteit beschikt, waardoor er kosten bespaard kunnen worden. Het uitvoeren van intelligente-video algoritmen is CPU-intensief.
- > Schaalbaarheid is mogelijk. Wanneer een server intelligente-videoalgoritmen moet uitvoeren, kunnen op elk moment slechts een aantal camera's worden beheerd. Met de intelligente functie in de netwerkkamera of in de video-encoder wordt een snelle reactietijd bereikt en kan een zeer groot aantal camera's proactief worden beheerd.

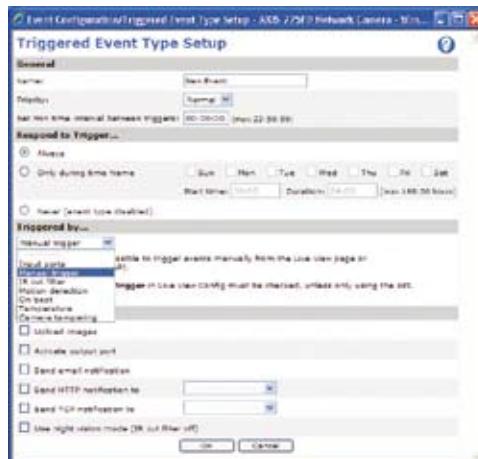


Afbeelding 11.3d Gebeurtenisbeheer en intelligente video maken het mogelijk dat een bewakingssysteem continu beschikbaar is voor het analyseren van invoer om gebeurtenissen te detecteren. Zodra een gebeurtenis wordt gedetecteerd, kan het systeem automatisch reageren met acties zoals het maken van video-opnames en het verzenden van waarschuwingen.

Gebeurtenisactivering

Een gebeurtenis kan gepland of geactiveerd zijn. Gebeurtenissen kunnen bijvoorbeeld worden geactiveerd door:

- > **Ingangspoort(en):** De ingangspoort(en) op een netwerkcamera of video-encoder kunnen worden aangesloten op externe apparaten zoals een bewegingsensor of een deurbel.
- > **Handmatige activering:** Een gebruiker kan knoppen gebruiken om handmatig een gebeurtenis te activeren.
- > **Videobewegingsdetectie:** Wanneer een camera een bepaalde beweging in het bewegingsdetectievenster van de camera detecteert, kan een gebeurtenis worden geactiveerd. *Raadpleeg pagina 102 voor meer informatie over videobewegingsdetectie.*
- > **Manipulatie van de camera:** Deze functie, waarmee een camera kan detecteren wanneer deze doelbewust is afgedekt, is verplaatst of niet meer is scherpgesteld, kan worden gebruikt om een gebeurtenis te activeren. *Raadpleeg hoofdstuk 8 voor meer informatie over een actief tamperingalarm.*
- > **Activering door geluid:** Hiermee kan een camera met ingebouwde audio-ondersteuning een gebeurtenis activeren wanneer audio boven of onder een bepaald drempelniveau wordt gedetecteerd. *Raadpleeg hoofdstuk 8 voor meer informatie over audiobronnen.*
- > **Temperatuur:** Wanneer de temperatuur buiten het bereik van de camera stijgt of zakt, kan een gebeurtenis worden geactiveerd.



Afbeelding 11.3e Gebeurtenisactivering instellen met behulp van een webinterface van een Axis-netwerkvideoproduct.

Reacties

Netwerkvideoproducten of een softwareprogramma voor videobeheer kunnen worden geconfigureerd om altijd of op bepaalde ingestelde tijdstippen te reageren op gebeurtenissen. Wanneer een gebeurtenis is geactiveerd, kunnen onder andere de volgende gangbare reacties worden geconfigureerd:

- > Afbeeldingen uploaden of videostromen opnemen op aangegeven locaties en met een bepaalde framesnelheid. Wanneer u de functie voor gebeurtenisactivering in de webinterface van de netwerkproducten van Axis gebruikt, kunnen alleen JPEG-afbeeldingen worden geüpload. Wanneer u een softwareprogramma voor videobeheer gebruikt, kan een video-stroom met een gespecificeerde compressie-indeling (H.264/MPEG-4/Motion JPEG) en compressieniveau door het netwerkvideoproduct worden ingesteld.
- > Uitgangspoort activeren: De uitgangspoort(en) op een netwerkkamera of video-encoder kan/ kunnen worden aangesloten op externe apparaten zoals een alarm. (Meer informatie over uitgangspoorten wordt hieronder gegeven.)
- > E-mailmelding verzenden: Hierdoor worden gebruikers gewaarschuwd dat er een gebeurtenis heeft plaatsgevonden. Er kan ook een afbeelding in de e-mail worden bijgevoegd.
- > HTTP/TCP-melding verzenden: Dit is een waarschuwing aan een videobeheersysteem dat vervolgens bijvoorbeeld opnamen kan starten.
- > Ga naar de vooraf ingestelde PTZ-apparatuur: Deze functie is mogelijk beschikbaar bij PTZ-camera's of PTZ-domecamera's. Hiermee kan de camera naar een bepaalde plek worden gericht, zoals een raam, wanneer een gebeurtenis plaatsvindt.
- > Een SMS (Short Message Service) met informatie over het alarm verzenden of een MMS (Multimedia Messaging Service) met een afbeelding van de gebeurtenis verzenden.
- > Een audiowaarschuwing op het videobeheersysteem activeren.
- > Een pop-up op het scherm inschakelen met weergaven van een camera waar een gebeurtenis is geactiveerd.
- > Procedures tonen die de gebruiker dient te gebruiken.

Daarnaast kan pre- en post-alarm beeldbuffering worden ingesteld, waardoor door een netwerkvideoproduct een ingestelde lengte en framesnelheid van opgenomen videomateriaal voor en na het activeren van een gebeurtenis kan worden verzonden. Hierdoor kan een completer beeld van een gebeurtenis worden gekregen.

Ingangs-/uitgangspoorten

In vergelijking met analoge camera's is bij netwerkkamera's en video-encoders de geïntegreerde ingangs- en uitgangspoorten (I/O) een unieke functie. Met deze poorten kan een netwerkvideoproduct worden aangesloten op externe apparaten en kunnen deze apparaten worden ingeschakeld om via een netwerk te worden beheerd. Een netwerkkamera of video-encoder die bijvoorbeeld via de ingangspoort is aangesloten op een externe alarmsensor kan worden ingesteld om alleen video-beelden te verzenden wanneer de sensor wordt geactiveerd. Het scala aan apparaten dat kan worden aangesloten op de ingangspoort van een netwerkvideoproduct is vrijwel oneindig. Het basisprincipe is dat elk apparaat dat heen en weer kan schakelen tussen een open en een gesloten

circuit, kan worden aangesloten op een netwerkkamera of video-encoder. De belangrijkste functie van de uitgangspoort van een netwerkvideoproduct is om externe apparaten te activeren, automatisch dan wel via afstandsbediening door een operator of een softwaretoepassing.

Type apparaat	Beschrijving	Gebruik
Deurcontact	Eenvoudige magneetschakelaar die het openen van een deur of raam detecteert.	Wanneer het circuit wordt verbroken (deur wordt geopend), kunnen afbeeldingen/videobeelden en meldingen vanaf de camera worden verzonden.
Passieve infrarood-detector (PIR)	Een sensor die beweging detecteert op basis van warmteafgifte.	Wanneer beweging wordt gedetecteerd, wordt het circuit door de PIR verbroken en kunnen afbeeldingen/videobeelden en meldingen vanaf de camera worden verzonden.
Glasbreukdetector	Een actieve sensor die luchtdruk in een kamer meet en plotselinge daling van de luchtdruk detecteert. (De sensor kan van stroom worden voorzien door de camera.)	Wanneer een daling in de luchtdruk wordt gedetecteerd, wordt het circuit verbroken en kunnen afbeeldingen/videobeelden en meldingen vanaf de camera worden verzonden.

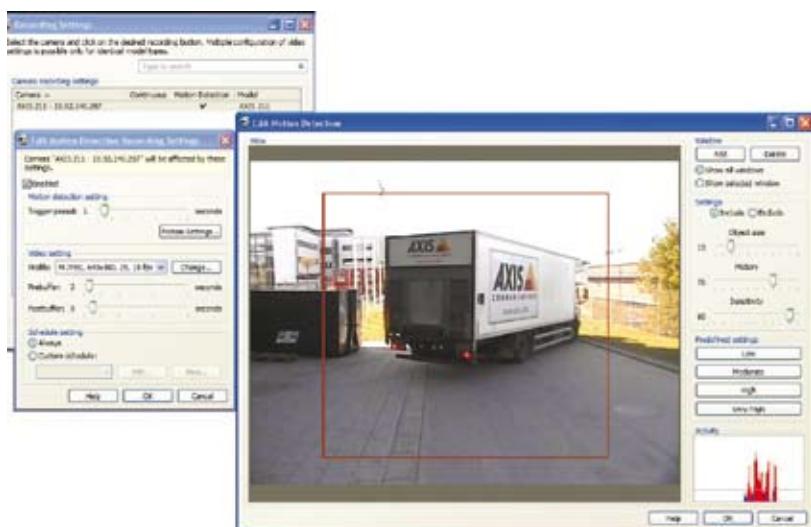
Tabel 11.3a Voorbeeld van apparaten die kunnen worden aangesloten op de ingangspoort.

Type apparaat	Beschrijving	Gebruik
Deurrelais	Een relais (solenoïde) die het openen en sluiten van de deurvergrendeling regelt.	Het vergrendelen/ontgrendelen van een deur kan worden gestuurd door een operator op afstand (via het netwerk) of kan een automatische reactie zijn op een alarmgebeurtenis.
Sirene	Alarmsirene die afgaat als een alarm wordt gedetecteerd.	Het netwerkvideoproduct kan de sirene activeren bij detectie van beweging door de ingebouwde videobewegingsdetectie of op basis van 'informatie' uit de digitale ingang.
Alarm/inbraakssysteem	Een alarmbeveiligingssysteem waarmee constant een doorgaans gesloten of open alarmcircuit wordt bewaakt.	Het netwerkvideoproduct kan werken als geïntegreerd deel van het alarmsysteem door te dienen als sensor en het alarmsysteem aan te vullen met door gebeurtenissen geactiveerde video-overdracht.

Tabel 11.3b Voorbeeld van apparaten die kunnen worden aangesloten op de uitgangspoort.

Videobewegingsdetectie

Videobewegingsdetectie (VMD) is een gangbare functie in videobeheersystemen. Het is een methode voor het definiëren van activiteit in een scène door het analyseren van beeldgegevens en variaties in beeldreeksen. Met VMD (videobewegingsdetectie) kan beweging worden gedetecteerd in elk gedeelte van een camerabeeld. Gebruikers kunnen een aantal 'inclusief' vensters (een speciaal deel in een camerabeeld waar de beweging gedetecteerd moet worden) en 'exclusief' vensters (delen binnen een 'inclusief' venster die genegeerd moeten worden) configureren. Met VMD kunt u voorrang aan opnamen geven, de hoeveelheid opgenomen videobeelden verkleinen en eenvoudiger naar gebeurtenissen zoeken.



Afbeelding 11.3f Videobewegingsdetectie instellen in Axis Camera Station-software voor videobeheer.

Actief tamperingalarm

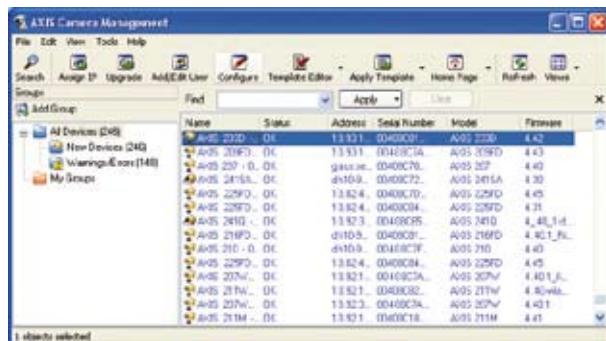
Deze functie voor intelligente video, die in veel netwerkvideoproducten van Axis is geïntegreerd, kan worden gebruikt als gebeurtenisactivering wanneer een camera op de een of andere manier is gemanipuleerd, bijvoorbeeld wanneer de camera onbedoeld anders is gericht, is geblokkeerd, onscherp is gesteld of met verf is bespoten, is afgedekt of beschadigd. Zonder een dergelijke detectie kunnen bewakingscamera's minder effectief zijn.

11.3.6 Functies voor administratie en beheer

Alle toepassingen voor videobeheersoftware hebben de mogelijkheid om basiscamera-instellingen, framesnelheid, resolutie en compressie-indeling toe te voegen en te configureren, maar enkele bevatten ook meer geavanceerd functies, zoals detectie van nieuwe camera's en volledig apparaatbeheer. Hoe groter een videosurveillance-systeem wordt, des te belangrijker het is om netwerkapparaten efficiënt te kunnen beheren.

Softwareprogramma's voor een eenvoudiger beheer van netwerkcamera's en video-encoders in een installatie bieden vaak de volgende functies:

- > Videoapparaten opzoeken in het netwerk en de verbindingssatus weergeven
- > IP-adressen instellen
- > Afzonderlijke of meerdere apparaten configureren
- > Firmware-upgrades van meerdere apparaten beheren
- > Toegangsrechten voor gebruikers beheren
- > Een configuratieoverzicht geven waarmee gebruikers ter plekke een overzicht van alle camera- en opnameconfiguraties kunnen krijgen.



Afbeelding 11.3g Met AXIS Camera Management-software kunt u eenvoudig geconfigureerde netwerkvideoproducten zoeken, installeren en configureren.

11.3.7 Beveiliging

Een belangrijk onderdeel van videobeheer is beveiliging. Bij een netwerkvideoproduct of video-beheersoftware moet het volgende worden gedefinieerd of ingesteld:

- > Bevoegde gebruikers
- > Wachtwoorden
- > Verschillende niveaus voor gebruikerstoegang, bijvoorbeeld:
 - Beheerder: toegang tot alle functies (in de AXIS Camera Station-software kan een beheerder bijvoorbeeld kiezen tot welke camera's en functies een gebruiker toegang mag hebben).
 - Operator: toegang tot alle functies behalve bepaalde configuratiepagina's
 - Kijker: alleen toegang tot live video vanaf geselecteerde camera's

11.4 Geïntegreerde systemen

Wanneer video wordt geïntegreerd met andere systemen zoals verkooppunten (POS) en gebouwbeheer kunnen gegevens uit andere systemen worden gebruikt om functies te activeren, zoals op gebeurtenissen gebaseerde opnamen in het netwerkvideosysteem. Omgekeerd geldt dit ook. Daarnaast kunnen gebruikers profiteren van een gemeenschappelijke interface voor het beheren van verschillende systemen.

11.4.1 Application Programming Interface (API)

Alle netwerkvideoprodukten van Axis hebben een op HTTP gebaseerde API (Application Programming Interface) of een netwerkinterface genaamd VAPIX®, waarmee ontwikkelaars eenvoudiger toepassingen kunnen maken voor ondersteuning van de netwerkvideoprodukten. Met een softwareprogramma voor videobeheer of een gebouwenbeheersysteem dat gebruik maakt van VAPIX® kunnen beelden van netwerkproducten van Axis worden opgevraagd, netwerkkamerafuncties worden bediend (bijvoorbeeld PTZ en relais) en interne parameterwaarden worden ingesteld of opgehaald. In feite kan een systeem alles doen wat de webinterface van de netwerkvideoprodukten biedt en zelfs meer, zoals het vastleggen van niet-gecomprimeerde beelden in een bitmap-bestandsindeling. Een wereldwijd open industrieforum, ONVIF, is begin 2008 door Axis, Bosch en Sony opgezet om de netwerkinterface van netwerkvideoprodukten te standaardiseren. Een standaard netwerkinterface garandeert eindgebruikers een grotere interoperabiliteit en flexibiliteit wanneer deze netwerkvideosystemen van meerdere leveranciers bouwen. *Raadpleeg voor meer informatie www.onvif.org*

11.4.2 Verkooppunten (POS)

Door de introductie van netwerkvideo in verkoopomgevingen is de integratie van video met PoS-systemen (verkooppunten) eenvoudiger geworden.

Door de integratie kunnen alle kassatransacties worden gekoppeld aan het videomateriaal van de transacties. Hierdoor kan diefstal en fraude die wordt gepleegd door medewerkers en klanten worden voorkomen. Afwijkende situaties op verkooppunten zoals retouren, handmatig ingevoerde waarden, regelcorrecties, het annuleren van transacties, aankopen door medewerkers, kortingen, speciaal geprijsde producten, het ruilen van producten en terugbetalingen kunnen visueel worden gecontroleerd aan de hand van het vastgelegde videomateriaal. Met een PoS-systeem met geïntegreerde videosurveillance is het eenvoudiger om verdachte activiteiten te zoeken en te controleren.

Op gebeurtenissen gebaseerde opnamen kunnen worden toegepast. Een PoS-transactie of -afwijking of het openen van een kassalade kan bijvoorbeeld worden gebruikt om een camera te activeren voor het opnemen en de opname van een tag te voorzien. Het scene voorafgaand aan en na een gebeurtenis kan worden vastgelegd met behulp van opnamebuffering voor en na de gebeurtenis. Op gebeurtenissen gebaseerde opnamen verhogen de kwaliteit van het opgenomen materiaal en beperken de opslagvereisten en de hoeveelheid tijd die benodigd is om naar incidenten te zoeken.



Afbeelding 11.4a Een voorbeeld van een PoS-systeem dat is geïntegreerd met videosurveillance. In dit screenshot worden de kassabonnen samen met de videobeelden van de gebeurtenis weergegeven. Met dank aan Milestone Systems voor de foto.

11.4.3 Toegangscontrole

Wanneer een videobeheersysteem met het toegangscontrolesysteem van een bedrijf wordt geïntegreerd, moet toegang tot het bedrijf en de ruimte worden geregistreerd met video. Er kan bijvoorbeeld bij alle deuren op video worden vastgelegd wanneer iemand een bedrijf binnentreedt of verlaat. Hiermee kan visuele controle worden toegepast wanneer zich uitzonderlijke gebeurtenissen voordoen. Daarnaast kunnen gebeurtenissen waarbij een persoon met een andere persoon mee naar binnen glipt, worden geregistreerd. Het mee naar binnen glippen vindt bijvoorbeeld plaats wanneer iemand zijn of haar toegangspasje opzettelijk of onopzettelijk gebruikt om andere personen toegang te verschaffen zonder dat deze zelf een pasje hoeven te gebruiken.

11.4.4 Gebouwbeheer

Video kan worden geïntegreerd in een gebouwbeheersysteem (BMS) waarmee een aantal systemen kan worden bediend, van systemen voor verwarming, ventilatie, en airconditioning (HVAC) tot systemen voor beveiliging, veiligheid, energie en brandalarmen. Voorbeelden van enkele toepassingen:

- > Door een alarm bij apparatuurstoring kan, naast het activeren van alarmen bij BMS, een camera worden geactiveerd om videomateriaal te tonen aan een operator.

- > Door een brandalarmsysteem kan een camera worden geactiveerd om buitendeuren te controleren en om met opnemen te beginnen voor beveiligingsdoeleinden.
- > Met intelligente video kan bij gebeurtenissen zoals evacuaties het aantal personen in een gebouw worden gedetecteerd via een open of een onbeveiligde deur.
- > Informatie uit de videobewegingsdetectiefunctie van een camera die in een vergaderruimte is geplaatst, kan worden gebruikt bij systemen voor verlichting en verwarming om het licht en de verwarming uit te schakelen zodra de ruimte is verlaten. Daarbij wordt ook energie bespaard.

11.4.5 Industriële regelsystemen

Bij complexe industriële automatiseringssystemen is visuele controle op afstand vaak gunstig en vereist. Een operator hoeft het bedieningspaneel niet te verlaten om een proces te controleren, omdat deze toegang tot het netwerk heeft door middel van dezelfde interface als die bij het bewaken van het proces wordt gebruikt. Daarnaast kan bij een onjuiste werking de netwerkcamera worden geactiveerd om beelden te verzenden. In sommige gevoelige processen in steriele kamers of in installaties met gevaarlijke chemicaliën kan videosurveillance zelfs de enige methode zijn voor visuele toegang tot een proces. Dit geldt ook voor elektriciteitsnetten die gebruik maken van een krachtcentrale op een zeer afgelegen locatie.

11.4.6 RFID

Systemen voor opsporing waarbij gebruik wordt gemaakt van RFID (identificatie met radiogolven) of gelijksoortige methoden worden in veel toepassingen gebruikt om items te kunnen volgen. Een voorbeeld hiervan is het verwerken van bagage op luchthavens; hierbij wordt de bagage gevolgd en naar de juiste bestemming gestuurd. Wanneer dit is geïntegreerd met videosurveillance is er visueel bewijs wanneer er bagage kwijt of beschadigd is en kunnen zoekmethoden worden geoptimaliseerd.

Overwegingen voor bandbreedte en opslag

De vereisten voor netwerkbandbreedte en opslag zijn belangrijke overwegingen bij het ontwerpen van een videosurveillance-systeem. Factoren hiervoor zijn het aantal camera's, de gebruikte afbeeldingsresolutie, het compressietype en -ratio, framesnelheden en de complexiteit van het scene. In dit hoofdstuk worden, samen met informatie over opslagoplossingen en diverse systeemconfiguraties, enkele richtlijnen voor het ontwerpen van een systeem gegeven.

12.1 Berekeningen voor bandbreedte en opslag

De bandbreedte en opslagruijte die benodigd is voor netwerkvideoproducten hangt af van de configuratie. Zoals eerder opgemerkt, hangt dit af van het volgende:

- > Het aantal camera's
- > Of de opname continu is of op een gebeurtenis gebaseerd
- > Het aantal uren per dag dat met de camera opnamen worden gemaakt
- > Frames per seconde
- > Beeldresolutie
- > Type videocompressie: Motion JPEG MPEG-4, H.264
- > Omgeving: Beeldcomplexiteit (bijvoorbeeld een grijze muur of een bos), belichtingsomstandigheden en mate van beweging (in een kantoor of overvolle treinstations)
- > Hoe lang gegevens bewaard moeten blijven

12.1.1 Bandbreedtevereisten

In een klein surveillance-systeem met 8 tot 10 camera's kan een basisnetwerkswitch van 100 megabit (Mbit) worden gebruikt zonder rekening te hoeven houden met de bandbreedtebeperkingen. De meeste bedrijven kunnen een surveillance-systeem van deze omvang implementeren in hun bestaande netwerk.

Bij het implementeren van tien of meer camera's kunt u de netwerkbelasting schatten door middel van enkele vuistregels:

- > Een camera die is geconfigureerd om beelden van hoge kwaliteit met hoge framesnelheden te leveren, gebruikt circa 2 tot 3 Mbit/s van de beschikbare netwerkbandbreedte.
- > Bij meer dan 12 tot 15 camera's kunt u overwegen om een switch te gebruiken met een gigabitbackbone. Wanneer een gigabit-ondersteunende switch wordt gebruikt, moet op de server waarop de beheersoftware wordt uitgevoerd een gigabit-netwerkadapter worden geïnstalleerd.

Technologieën waarmee het verbruik van bandbreedte kan worden beheerd, bevatten het gebruik van VLAN's op een netwerk met een switch, servicekwaliteit (QoS) en op gebeurtenissen gebaseerde opnamen. *Raadpleeg voor meer informatie over deze onderwerpen hoofdstuk 9 en 11.*

12.1.2 Het berekenen van de opslagbehoefte

Zoals eerder opgemerkt, is het gebruikte type videocompressie een van de factoren die van invloed is op de opslagvereisten. De compressie-indeling H.264 is verreweg de meest efficiënte compressietechniek die tegenwoordig beschikbaar is. Een H.264-encoder kan, zonder concessies aan de beeldkwaliteit te doen, de grootte van een digitaal videobestand meer dan 80% terugbrengen in vergelijking met de Motion JPEG-indeling en tot meer dan 50% in vergelijking met de standaard MPEG-4 (Part 2). Dit betekent dat er veel minder netwerkbandbreedte en opslagruimte worden vereist voor een H.264-videobestand. Voorbeelden van berekeningen voor opslag voor alle drie compressie-indelingen die in de onderstaande tabellen worden weergegeven. Vanwege een aantal variabelen die van invloed zijn op de gemiddelde bitsnelheden zijn de berekeningen niet zo duidelijk voor H.264 en MPEG-4. Met Motion JPEG is er een duidelijke formule omdat Motion JPEG uit een afzonderlijk bestand voor elk beeld bestaat. Opslagvereisten voor Motion JPEG-opnamen variëren afhankelijk van de framesnelheid, resolutie en compressieniveau.

Berekening voor H.264:

Geschatte bitsnelheid / 8 (bits in een byte) x 3600 s = kB per uur / 1000 = MB per uur

MB per uur x bedrijfsuren per dag / 1000 = GB per dag

GB per dag x gewenste opslagtermijn = benodigde opslagruimte

Camera	Resolutie	Geschatte bitsnelheid (Kbit/s)	Frames per seconde	MB/uur	Bedrijfsuren	GB/dag
Nr. 1	CIF	110	5	49.5	8	0.4
Nr. 2	CIF	250	15	112.5	8	0.9
Nr. 3	4CIF	600	15	270	12	3.2
Totaal voor de 3 camera's en 30 dagen opslag = 135 GB						

Tabel 12.1a *Bovenstaande cijfers zijn gebaseerd op veel beweging in een scène. Met minder veranderingen in een scène kunnen de cijfers 20% lager zijn. De mate van beweging in een scène kan grote gevolgen hebben voor de benodigde opslagruimte.*

Berekening voor MPEG-4:

Geschatte bitsnelheid / 8 (bits in een byte) x 3600 s = kB per uur / 1000 = MB per uur

MB per uur x bedrijfsuren per dag / 1000 = GB per dag

GB per dag x gewenste opslagtermijn = benodigde opslagruimte

NB: Bij de formule wordt geen rekening gehouden met de mate van beweging, hetgeen een belangrijke factor is die de grootte van de benodigde opslag kan beïnvloeden.

Camera	Resolutie	Geschatte bitsnelheid (Kbit/s)	Frames per seconde	MB/uur	Bedrijfsuren	GB/dag
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
Totaal voor de 3 camera's en 30 dagen opslag = 204 GB						

Tabel 12.1b

Berekening voor Motion JPEG:

Beeldformaat x frames per seconde x 3600 s = Kilobyte (kB) per uur / 1000 = Megabyte MB per uur

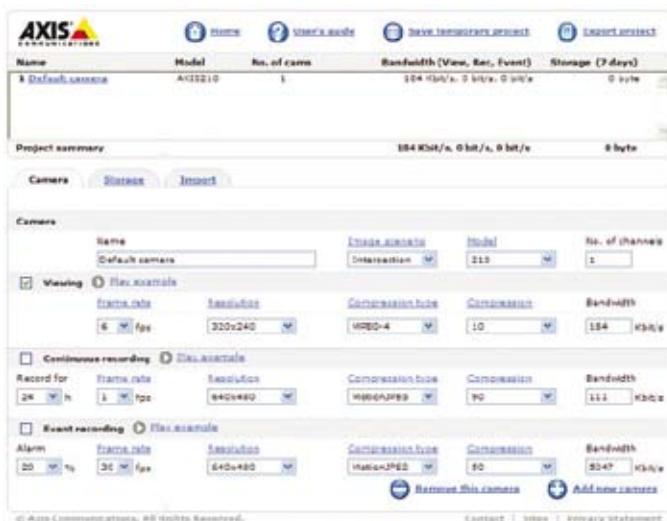
MB per uur x bedrijfsuren per dag / 1000 = Gigabyte GB per dag

GB per dag x gewenste opslagtermijn = benodigde opslagruimte

Camera	Resolutie	Geschatte bitsnelheid (Kbit/s)	Frames per seconde	MB/uur	Bedrijfsuren	GB/dag
No. 1	CIF	13	5	234	8	1.9
No. 2	CIF	13	15	702	8	5.6
No. 3	4CIF	40	15	2160	12	26
Totaal voor de 3 camera's en 30 dagen opslag = 1002 GB						

Tabel 12.1c

Een nuttig hulpmiddel bij het schatten van vereisten voor bandbreedte en opslag is de AXIS Design Tool, waartoe u toegang hebt op het volgende internetadres: www.axis.com/products/video/design_tool/



Afbeelding 12.1a De AXIS Design Tool heeft een geavanceerde functie voor projectbeheer waarmee bandbreedte en opslag kunnen worden berekend voor een groot en complex systeem.

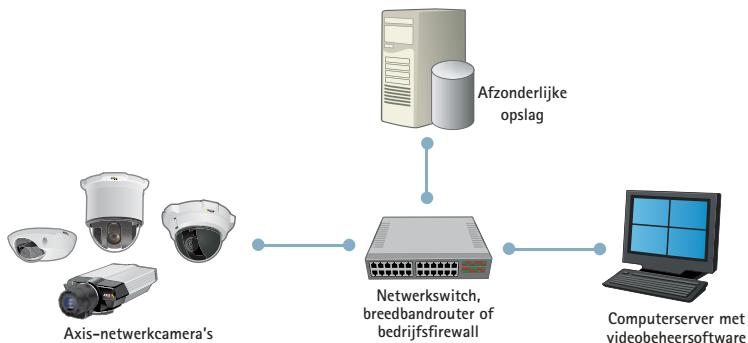
12.2 Opslag op de server

Afhankelijk van de CPU (central processing unit) van de pc-server, de netwerkkaart en het interne RAM (Random Access Memory) kan een server een bepaald aantal camera's, frames per seconde en grootte van beelden verwerken. De meeste pc's kunnen twee tot vier vaste schijven bevatten en elke schijf kan maximaal 300 gigabyte (GB) bevatten. In een installatie van kleine of gemiddelde omvang wordt de pc die de videobeheersoftware uitvoert ook gebruikt voor het opnemen van videomateriaal. Dit wordt een direct aangesloten opslag genoemd.

Met de AXIS Camera Station-software voor videobeheer is bijvoorbeeld één vaste schijf geschikt voor het opslaan van opnamen van zes tot acht camera's. Met meer dan 12 tot 15 camera's moeten er ten minste twee vaste schijven worden gebruikt om de belasting van de schijf te splitsen.

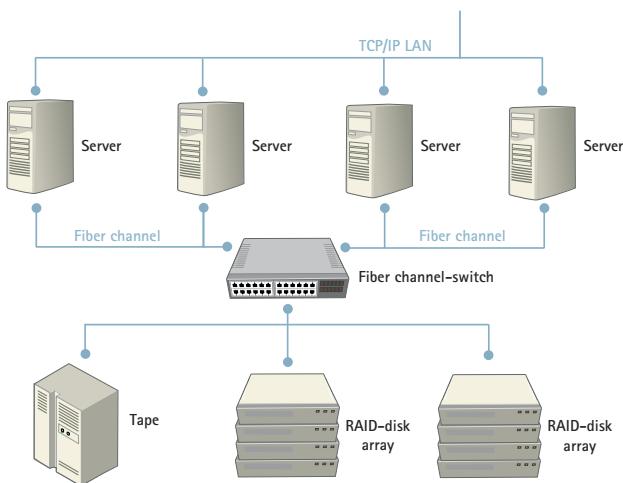
12.3 NAS en SAN

Wanneer de hoeveelheid opgeslagen gegevens en beheersvereisten de limieten van een direct aangesloten opslag overschrijdt, kan met een NAS (network-attached storage) of een SAN (storage area network) een toename van opslagruijte, flexibiliteit en herstelmogelijkheden worden gerealiseerd.



Afbilding 12.3a NAS (network-attached storage)

Bij NAS wordt één opslagapparaat direct aangesloten op een LAN en verzorgt deze de opslag voor alle clients op het netwerk. Een NAS-apparaat is eenvoudig te installeren en gemakkelijke te beheren. Hiermee wordt een goedkope opslagoplossing geboden. Het biedt echter een beperkte doorvoer voor inkomende gegevens omdat het maar één netwerkverbinding heeft, die eventueel problemen kan opleveren bij hoogwaardige systemen. SAN's zijn netwerken met hoge snelheid en voor speciale doeleinden ten behoeve van opslag. Deze zijn doorgaans via glasvezel aangesloten op een of meer servers. Gebruikers hebben toegang tot de opslagapparaten op het SAN via de servers en de opslagruijte is schaalbaar tot honderden terabytes. Centrale gegevensopslag vermindert de hoeveelheid administratie en biedt een flexibel opslagsysteem met hoge prestaties voor gebruik in omgevingen met meerdere servers. Fiber Channel-technologie wordt over het algemeen gebruikt voor gegevensoverdracht van vier gigabits per seconde en voor het opslaan van grote hoeveelheden gegevens die in grote mate redundant zijn.

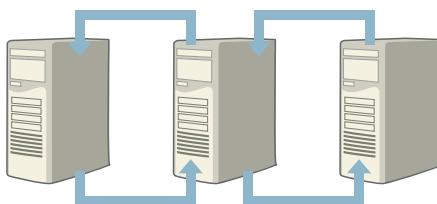


Afbilding 12.3b Een SAN-architectuur waarbij opslagapparaten dicht bij elkaar zijn geplaatst en de servers de opslagcapaciteit delen.

12.4 Redundante opslag

Bij SAN-systemen wordt redundantie in het opslagapparaat ingebouwd. Met redundantie in een opslagsysteem kan videomateriaal of kunnen andere gegevens gelijktijdig worden opgeslagen op meer dan één locatie. Dit biedt een back-up voor het herstellen van videomateriaal wanneer een gedeelte van het opslagsysteem onleesbaar wordt. Er zijn een aantal opties voor deze toegevoegde opslaglaag in een IP-surveillancesysteem, waaronder een RAID (Redundant Array of Independent Disks), gegevensreplicatie, serverclustering en meerdere video-ontvangers.

RAID. RAID is een methode voor een ordeningstandaard, waarbij gewone extra vaste schijven op elkaar worden aangesloten op een manier waardoor het besturingssysteem ze ziet als één grote vaste schijf. Met een RAID-installatie worden gegevens over meerdere vaste schijven met voldoende redundantie verspreid zodat gegevens kunnen worden hersteld wanneer één schijf niet functioneert. Er zijn verschillende RAID-niveaus, van vrijwel geen redundantie tot een volledig gespiegeld oplossing, waarbij er geen verstoring en geen gegevensverlies is wanneer een vaste schijf wordt beschadigd.



Afbeelding 12.4a Gegevensreplicatie.

Gegevensreplicatie. Dit is een veel voorkomende functie in veel netwerkbesturingssystemen: Bestandservers in een netwerk zijn geconfigureerd zodat deze gegevens van elkaar kunnen repliceren, waardoor er een back-up kan worden gemaakt wanneer één server uitvalt.

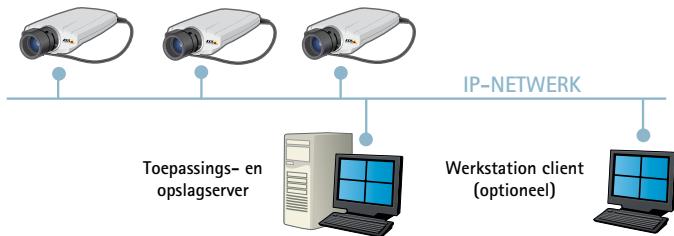
Serverclustering. Een veel voorkomende methode voor serverclustering is dat twee servers met hetzelfde opslagapparaat werken, zoals bij een RAID-systeem. Wanneer één server uitvalt, neemt de andere server, die exact hetzelfde is geconfigureerd, het over. Deze servers kunnen zelfs hetzelfde IP-adres delen, waardoor de zogenaamde 'failover' volledig transparant is voor gebruikers..

Meerdere video-ontvangers. Een veel gebruikte methode om herstel bij calamiteiten te garanderen en het op een externe locatie opslaan van netwerkvideomateriaal te garanderen, is het videomateriaal gelijktijdig verzenden naar twee verschillende servers op verschillende locaties. Die servers kunnen zijn voorzien van RAID, in clusters werken of hun gegevens repliceren naar servers op weer een andere locatie. Dit is een nuttige aanpak wanneer surveillancesystemen zich op gevaarlijke of moeilijk toegankelijke plaatsen bevinden, zoals in openbaar-vervoersomgevingen of industriële omgevingen.

12.5 Systeemconfiguraties

Klein systeem (1 tot 30 camera's)

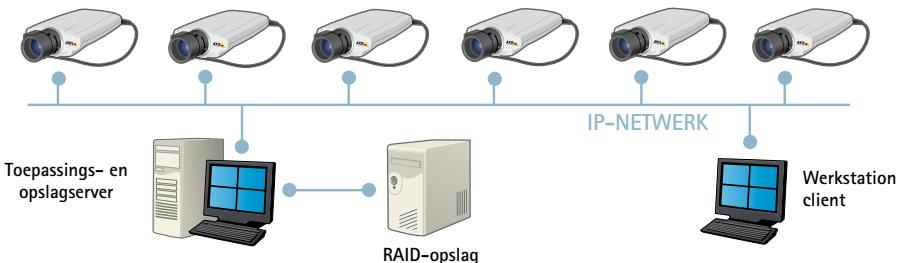
Een klein systeem bestaat doorgaans uit één server die een surveillancetoepassing uitvoert die het videomateriaal op een lokale vaste schijf opslaat. De video wordt weergegeven en beheerd door dezelfde server. Hoewel de meeste weergave en het meeste beheer plaatsvindt op de server kan een client (lokaal of op afstand) worden aangesloten voor hetzelfde doel.



Afbeelding 12.5a Een klein systeem.

Middelgroot systeem (25 tot 100 camera's)

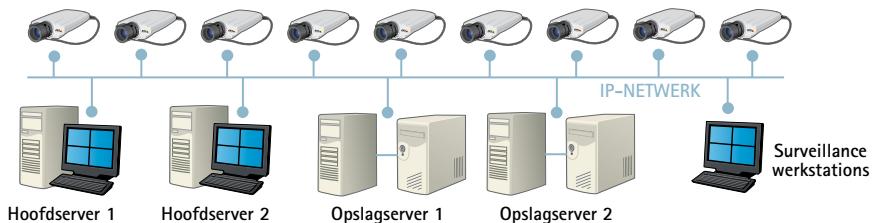
Een normale, middelgrote installatie heeft een server waaraan extra opslagmogelijkheden zijn toegevoegd. De opslag is doorgaans met RAID geconfigureerd voor een betere prestatie en betrouwbaarheid. Het videomateriaal wordt doorgaans vanaf een client weergegeven en beheerd, in plaats vanaf de opnameserver zelf.



Afbeelding 12.5b Een middelgroot systeem.

Groot gecentraliseerd systeem (50 tot +1000 camera's)

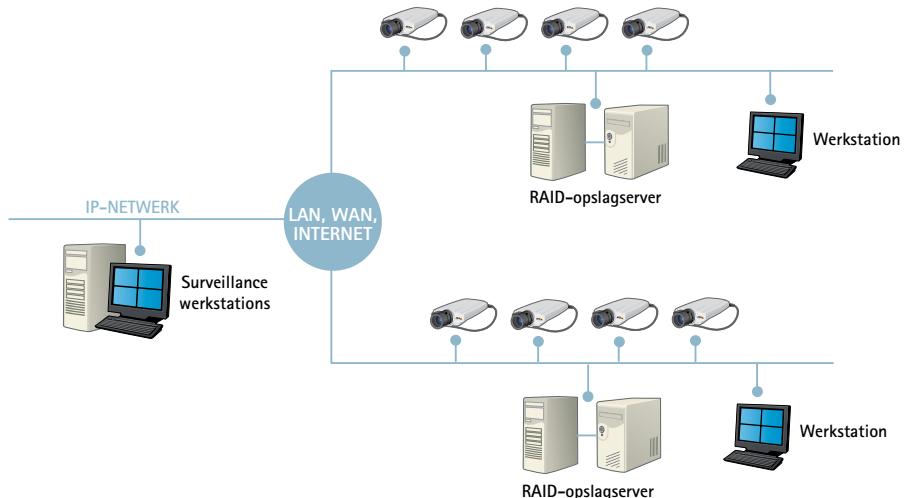
Een grote installatie vereist hoogwaardige prestatie en betrouwbaarheid om de grote hoeveelheid gegevens en bandbreedte te kunnen beheren. Hiervoor zijn meerdere servers met specifieke taken vereist. Een hoofdserver beheert het systeem en beslist welk soort videomateriaal wordt opgeslagen op welke opslagserver. Aangezien er specifieke opslagservers zijn, is het mogelijk om de belasting te verdelen. Bij een dergelijke installatie is het ook mogelijk om het systeem uit te breiden door meer opslagservers toe te voegen wanneer dit nodig is en onderhoud te plegen zonder het gehele systeem uit te schakelen.



Afbeelding 12.5c Een groot gecentraliseerd systeem.

Groot gedistribueerd systeem (25 tot meer dan 1000 camera's)

Wanneer voor meerdere locaties surveillance met gedistribueerd beheer wordt vereist, kunnen gedistribueerde opnamesystemen worden gebruikt. Op elke locatie wordt videomateriaal van lokale camera's opgenomen en opgeslagen. De hoofdcontroller kan op elke locatie opnamen laten weergeven en beheren.



Afbeelding 12.5d Een groot gedistribueerd systeem



Hulpmiddelen

Axis biedt een verscheidenheid aan hulpmiddelen en informatiebronnen voor het ontwerpen van IP-surveillancesystemen. Veel van deze hulpmiddelen zijn toegankelijk via de website van Axis: www.axis.com/tools

Lenscalculators

Met dit hulpmiddel kunt u de brandpuntsafstand van de lens berekenen die u nodig hebt om een specifieke scène op een bepaalde afstand vast te leggen.

Camera Reach Tool

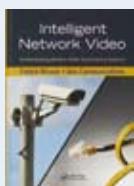
Dit hulpmiddel is gericht op het opname- en gezichtherkenningsvermogen van Axis netwerkcamera's op verschillende afstanden en in combinatie met verschillende lenzen. Met dit hulpmiddel kunt u ook uw weg te vinden in de productportfolio van Axis om de camera te zoeken die het geschiktst is voor uw toepassing.

AXIS Design Tool

Met dit berekeningshulpmiddel op simulatiebasis, dat online of op een DVD verkrijgbaar is, kunt u de bandbreedte- en opslagvereisten voor specifieke netwerkvideoprojecten bepalen.

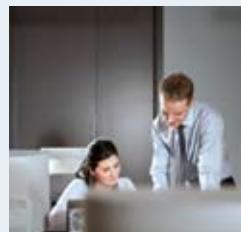
Axis Housing Configurator

Met dit hulpmiddel kunt u zoeken naar de juiste behuizingen en andere accessoires zoals beugels, voedingen en kabels voor uw specifieke cameratoepassing.



Intelligente netwerkvideo: moderne surveillancesystemen begrijpen

Dit boek van 390 pagina's (hardcover) is geschreven door Fredrik Nilsson en Axis Communications. Dit is het eerste boek dat uitgebreid ingaat op geavanceerde digitale mogelijkheden voor digitale netwerken en intelligente video. Dit boek dat is gepubliceerd in september 2008, kan worden aangeschaft via Amazon, Barnes & Noble en CRC Press of door contact op te nemen met het plaatselijke Axis-kantoor.



Axis Communications' Academy

Nummer één op het gebied van kennis van netwerkvideo.

Meer te weten komen over netwerkvideotechnologieën met het trainingsprogramma van Axis.

- > Profiteer van een breed cursusaanbod
- > Train met praktijkvoorbeelden
- > Ontvang training van ervaren experts
- > Zorg dat u een streepje voor krijgt op de concurrentie

De videosurveillancemarkt is aan het veranderen aangezien oudere analoge systemen geleidelijk worden vervangen door netwerkvideotechnologie. Nieuwe technieken, toepassingen en integratiemogelijkheden vormen de drijvende kracht achter deze overgang. Om de steeds scherpere concurrentie op deze markt aan te kunnen, heeft u gedegen vaardigheden en expertise op IP gebaseerde video-oplossingen nodig. Sla de handen ineen met Axis Communications' Academy, de nummer één op het gebied van kennis van netwerkvideo, om er zeker van te zijn dat u de concurrentie altijd een stapje voorblijft.

Kennis van de basisprincipes verwerven

Network Video Fundamentals en Video Solution Fundamentals vormen de bouwstenen van het trainingsprogramma van de Axis Communications' Academy. De basisprincipes zijn ontwikkeld en verder verfijnd om aan te sluiten op de opleidingseisen van professionals op het gebied van analoge CCTV, maar ook op die van IT-specialisten. Ongeacht uw achtergrond kunt u dus de gespecialiseerde technische kennis verwerven die u nodig hebt om succesvol te kunnen werken met producten en oplossingen van Axis.

Kijk op www.axis.com/nl/academy

Contactgegevens

www.axis.com/request

HOOFDKANTOOR, ZWEDEN

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

ARGENTINIË

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

AUSTRALIË

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

BRAZILIË

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

CANADA

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

CHINA

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

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

DUITSLAND, OOSTENRIJK, ZWITSERLAND

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

FRANKRIJK, BELGIË, LUXEMBURG

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

HONG KONG

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

INDIA

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

ITALIË

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

JAPAN

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

Contactgegevens

www.axis.com/request

KOREA

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

MEXICO

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

NEDERLAND

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

RUSSISCHE FEDERATIE

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

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

SPANJE

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

TAIWAN

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

VERENIGDE ARABISCHE

EMIRATEN

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

VERENIGD KONINKRIJK

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

VERENIGDE STATEN

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

ZUID-AFRIKA

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

PO Box 70939

Bryanston 2021

Over Axis Communications

Axis is een IT bedrijf met netwerkvideo-oplossingen voor professionele installaties. Axis is wereldmarktleider in netwerkvideoproducten, initiator van de groeiende verschuiving van analoge naar digitale video bewaking. Axis focust zich met haar producten en oplossingen op surveillance en controle op afstand, en zijn gebaseerd op innovatieve, open technologische platforms.

Axis is een Zweeds bedrijf, wereldwijd werkzaam met kantoren in meer dan 20 landen en werkt samen met partners in meer dan 70 landen. Axis is opgericht in 1984, en staat genoteerd aan de NASDAQ OMX Stockholm, onder de beurstikker AXIS. Voor meer informatie over Axis Communications BV, bezoek onze website www.axis.com