



Guide technique de la vidéo sur IP

Juin 2025

Introduction

Nous avons créé ce *Guide technique de la vidéo sur IP* pour vous aider à utiliser vos systèmes de surveillance vidéo sur IP Axis et vous permettre de suivre les évolutions technologiques. Notre guide est une ressource complète pour toute personne impliquée dans le développement, la mise en œuvre et la maintenance des systèmes de vidéosurveillance Axis. Il offre un aperçu complet de la surveillance vidéo sur IP et couvre les développements récents en matière de cloud, d'analyse et de systèmes de gestion vidéo (VMS).

Nous espérons que vous trouverez ce *Guide technique de la vidéo sur IP* utile !

Table des matières

1.	Vidéo sur IP : présentation, avantages et applications	9
1.1	Vue d'ensemble d'un système vidéo sur IP	9
1.2	Avantages	10
1.3	Applications	12
2.	Caméras réseau	14
2.1	Qu'est-ce qu'une caméra réseau ?	14
2.1.1	Plateforme d'applications AXIS Camera (ACAP)	17
2.1.2	Interface de programmation d'applications	17
2.1.3	ONVIF	17
2.2	Fonctions de caméra permettant de gérer des scènes difficiles	18
2.2.1	Plage dynamique étendue (WDR)	18
2.2.2	Technologie Lightfinder	18
2.2.3	Fonctionnalité jour/nuit	19
2.2.4	Éclairage IR intégré	19
2.2.5	OptimizedIR	20
2.2.6	Objectifs à faible valeur f	20
2.2.7	Régulation automatique du diaphragme	21
2.2.8	La bonne résolution	21
2.2.9	Imagerie thermique	21
2.2.10	Stabilisation d'image	22
2.3	Fonctions de la caméra pour faciliter l'installation	23
2.3.1	Installation en extérieur possible dès la sortie d'usine	23
2.3.2	Caméras mises au point en sortie d'usine	23
2.3.3	Mise au point à distance et zoom	23
2.3.4	Mise au point du foyer arrière	24
2.3.5	Réglage de l'angle de caméra sur 3 axes	24
2.3.6	Format corridor	24
2.3.7	Redressement d'image	25
2.3.8	Compteur de pixels	25
2.4	Types de caméras réseau	25
2.4.1	Caméras en boîtier	26
2.4.2	Caméras cylindriques	26
2.4.3	Caméras-dômes	26
2.4.3.1	Caméras à dôme embarquées	27
2.4.3.2	Caméras panoramiques	28
2.4.4	Caméras modulaires	30

2.4.5	Caméras PTZ	33
2.4.5.1	Technologie Sharpdome	36
2.4.6	Caméras thermiques	37
2.4.7	Caméras avec boîtiers antidéflagrants	40
3.	Paramètres d'une caméra	43
3.1	Sensibilité à la lumière	43
3.2	Objectifs	44
3.2.1	Types d'objectifs	45
3.2.2	Champ de vision	45
3.2.3	Chiffre F et exposition	47
3.2.4	Types de diaphragme	47
3.2.5	Profondeur de champ	48
3.2.6	Adaptation de l'objectif et du capteur	49
3.2.7	Types d'objectifs de surveillance	50
3.2.8	Mise au point	51
3.2.9	Précision PTRZ	53
3.3	Filtre infrarouge amovible (fonctionnalité jour / nuit)	53
3.4	Capteurs d'image	56
3.5	Contrôle d'exposition	57
3.5.1	Priorité de l'exposition	57
3.5.2	Zones d'exposition	58
3.5.3	Compensation de contre-jour	58
3.5.4	Plage dynamique	58
3.5.5	Imagerie WDR	59
3.6	Alarme de détérioration	61
3.7	Détection sonore	61
4.	Encodeurs vidéo	62
4.1	Qu'est-ce qu'un encodeur vidéo ?	62
4.1.1	Composants d'encodeur vidéo et considérations	63
4.1.2	Gestion des événements et analyse vidéo	64
4.2	Encodeurs vidéo avec caméras PTZ analogiques	64
4.3	Techniques de désentrelacement	64
4.4	Décodeurs vidéo	66
5.	Résolutions vidéo	67
5.1	Résolutions mégapixels	67
5.2	Résolutions de télévision haute définition (TVHD)	67
5.3	Résolutions Ultra-HD	68
5.4	Rapports	69

6.	Compression vidéo	72
6.1	Bases de compression	72
6.1.1	Codec vidéo	72
6.1.2	Différence entre compression d'image et compression vidéo	73
6.2	Formats de compression	75
6.2.1	H.264	76
6.2.2	H.265	76
6.2.3	AV1	77
6.2.4	Zipstream pour H.264, H.265 et AV1	77
6.2.5	Motion JPEG	79
6.2.6	JPEG	80
6.3	Débits binaires moyens, variables et maximum	80
6.4	Comparaison des normes	81
7.	Audio	84
7.1	Détection sonore	84
7.1.1	Périphériques et technologie de connectivité audio	84
7.1.2	Amélioration de la détection audio	86
7.1.3	Analyse audio	86
7.2	Sortie audio	87
7.2.1	Sortie audio en vidéosurveillance	87
7.2.2	Systèmes audio sur IP pour la sonorisation	88
7.3	Modes de communication audio	89
7.4	Codecs audio	90
7.5	Synchronisation de l'audio et de la vidéo	90
8.	Radar	92
8.1	Une technologie non visuelle qui complète la vidéosurveillance	92
8.2	Dispositifs radar	92
8.3	Radars intégrés à un système de surveillance	93
9.	Contrôle d'accès	95
9.1	Qu'est-ce que le contrôle d'accès ?	95
9.2	Pourquoi IP dans le contrôle d'accès ?	96
9.3	Composants d'un système de contrôle d'accès	97
9.3.1	Contrôleurs de porte réseau	98
9.3.2	Lecteurs	98
9.3.3	Modules de relais d'E/S réseau	98
9.3.4	Systèmes de gestion d'accès	99
10.	Visiophones réseau	100

10.1	Dispositifs de communication multifonctions pour une sécurité accrue	100
11.	Dispositifs portables	102
11.1	Objectif des caméras-piétons	102
11.2	Caméras-piétons	103
11.3	Solution de caméra-piéton Axis	104
11.4	Solution embarquée	106
12.	Fonctions d'analyse	107
12.1	L'analytique au service d'un monde plus sûr et plus intelligent	107
12.2	Avantages des fonctions d'analyse	108
12.2.1	Surveillance en temps réel	108
12.2.2	Recherche efficace	110
12.2.3	Repérer les tendances et les schémas	110
12.2.4	Confidentialité	111
12.3	Architecture système : où la vidéo est-elle analysée ?	111
12.4	Facilité d'utilisation des images : base d'excellentes performances analytiques	112
12.5	Intelligence artificielle	113
12.6	Plateforme d'applications AXIS Camera (ACAP)	114
13.	Technologies réseau	115
13.1	Réseaux locaux et Ethernet	115
13.1.1	Types de réseaux Ethernet	116
13.1.2	Connexion de périphériques et de commutateurs réseau	116
13.1.3	Alimentation par Ethernet	118
13.2	Envoyer des données sur Internet	121
13.2.1	Adressage IP	122
13.2.1.1	Adresses IPv4	122
13.2.1.2	Adresses IPv6	124
13.2.2	Protocoles de transport de données pour la vidéo sur IP	124
13.2.3	SIP	126
13.3	Réseaux locaux virtuels	127
13.4	Qualité de service	128
14.	Protection du système	131
14.1	Protection du réseau	131
14.1.1	IEEE 802.1X	131
14.1.2	HTTPS (HTTP sur TLS)	132
14.1.3	Infrastructure de clé publique (PKI) fiable	133
14.1.4	NTS Network Time Protocol	133
14.1.5	Isolement du réseau	133

14.2	Normes de cybersécurité	134
14.2.1	ETSI EN 303 645	134
14.2.2	FIPS (Federal Information Processing Standard) 140	134
14.2.3	Critères communs (CC)	134
14.3	Protection des dispositifs	134
14.3.1	Plateforme de cybersécurité intégrée	135
14.3.2	Gestion des comptes utilisateurs	136
14.3.3	Filtrage d'adresses IP	136
14.3.4	Mise à jour des logiciels des périphériques	136
14.4	Protection du VMS	137
14.5	Protection physique	137
15.	Technologies sans fil	139
15.1	Normes WLAN 802.11	139
15.2	Sécurité WLAN	140
15.2.1	WPA2™ ¹	140
15.3	Ponts sans fil	141
15.4	Réseau maillé sans fil	141
15.5	Réseaux 4G et 5G	141
15.6	Z-Wave®	142
15.7	Zigbee®	142
16.	Systèmes de gestion vidéo	143
16.1	Types de systèmes de gestion vidéo	143
16.1.1	Systèmes basés sur le cloud	144
16.1.1.1	AXIS Camera Station Edge	144
16.1.2	Réseaux privés	145
16.1.2.1	AXIS Camera Station Pro	146
16.1.3	Solutions personnalisées des partenaires Axis	148
16.2	Caractéristiques du système	148
16.3	Systèmes intégrés	149
16.3.1	Contrôle d'accès	150
16.3.2	Point de vente	150
16.3.3	Gestion des bâtiments	150
16.3.4	Systèmes de contrôle industriel	151
16.3.5	RFID	151
17.	Technologies cloud	152
17.1	Passage au cloud	152
17.2	Installations cloud	153
17.3	Axis Cloud Connect	153

18.	Considérations de conception du système	155
18.1	Sélection d'une caméra	155
18.1.1	Types de caméras	155
18.1.2	Qualité d'image	157
18.1.3	Résolution	157
18.1.4	Compression	160
18.1.5	Fonctions réseau	161
18.1.6	Autres fonctionnalités	162
18.2	Installation d'une caméra réseau	163
18.2.1	Objectif de surveillance	163
18.2.2	Gestion de l'éclairage difficile	163
18.2.3	Choix de l'objectif	164
18.3	Protection physique de la caméra	164
18.3.1	Protection et classification	165
18.3.2	Boîtiers externes	166
18.3.2.1	Mise en boîtier d'une caméra fixe	166
18.3.3	Dômes transparents	167
18.3.4	Protection contre le vandalisme et le sabotage	167
18.3.5	Types de supports	169
18.4	Éléments à considérer pour la bande passante et le stockage	172
18.4.1	Bits ou octets ?	172
18.4.2	Exigences en matière de passante	174
18.4.3	Exigences en matière de stockage	175
18.4.4	Configurations du système	175
18.4.5	Stockage local	178
18.4.6	Stockage sur serveur	180
18.4.7	NAS et SAN	180
18.4.8	Stockage redondant	182
19.	Outils et ressources	185
19.1	Recherche et comparaison de produits	185
19.2	Planification et conception de sites	185
19.3	Installation et gestion des systèmes	186
20.	Axis Communications Academy	187
20.1	Développement d'une expertise pour une entreprise plus intelligente	187

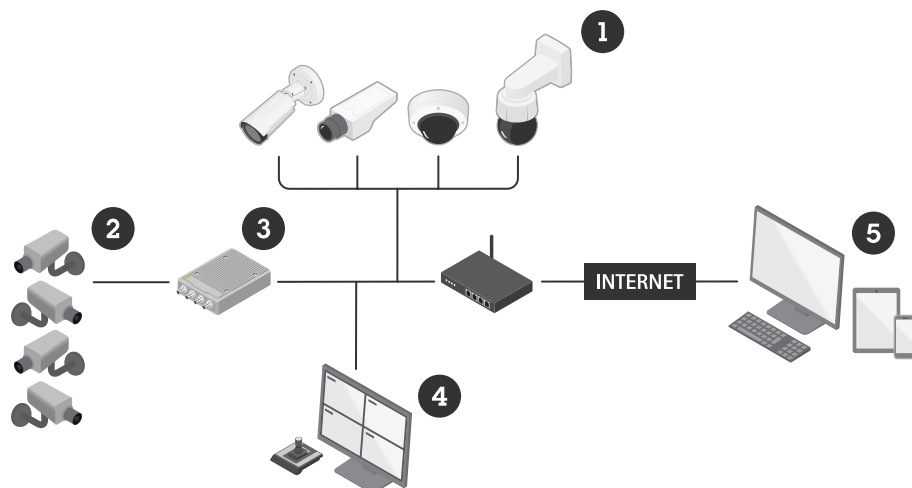
1. Vidéo sur IP : présentation, avantages et applications

Un système vidéo sur IP utilise des réseaux IP standard pour le transport vidéo et audio. Les flux vidéo et audio numérisés sont envoyés sur des réseaux IP filaires ou sans fil, permettant la surveillance et l'enregistrement vidéo depuis n'importe quel point du réseau. Grâce à une multitude de fonctionnalités avancées, la vidéo sur IP a beaucoup à offrir en termes de surveillance de sécurité. La vidéo haute qualité, l'évolutivité et l'intelligence intégrée de la vidéo sur IP améliorent la capacité du personnel de sécurité à protéger les personnes, les biens et les actifs.

1.1 Vue d'ensemble d'un système vidéo sur IP

La vidéo en réseau, souvent appelée *vidéosurveillance sur IP* ou *surveillance sur IP*, telle qu'elle est appliquée dans le secteur de la sécurité, utilise un réseau IP filaire ou sans fil comme structure de base pour le transport des données vidéo, audio et autres données numériques. Le réseau transporte également l'alimentation des périphériques vidéo sur IP via la technologie PoE (Power over Ethernet).

Un système vidéo sur IP permet de surveiller et d'enregistrer la vidéo depuis n'importe quel point du réseau, qu'il s'agisse d'un réseau local (LAN) ou d'un réseau étendu (WAN) tel qu'Internet.



Un système vidéo sur IP avec des caméras réseau (1), des caméras analogiques (2) connectées via des encodeurs vidéo (3) et un logiciel de gestion vidéo (4). Les autres composants, notamment le réseau, le stockage et les serveurs, sont tous des équipements informatiques standard. L'accès distant est possible depuis un ordinateur ou un périphérique mobile (5).

Les composants de base d'un système de vidéo sur IP comprennent la caméra réseau, l'encodeur vidéo (utilisé pour connecter les caméras analogiques à un réseau IP), le réseau, le serveur et le stockage, et le logiciel de gestion vidéo (VMS). Comme les caméras réseau et les encodeurs vidéo sont basés sur ordinateur, leurs capacités sont meilleures que celles d'une caméra CCTV analogique.

Le réseau, le serveur et les composants de stockage sont tous des équipements couramment disponibles sur le marché : il s'agit de l'un des principaux avantages de la vidéo sur IP. Il peut également comprendre des accessoires, tels que des supports, des injecteurs PoE et des joysticks. Chaque composant de vidéo sur IP sera traité plus en détail dans d'autres chapitres.

1.2 Avantages

Un système de surveillance vidéo sur IP entièrement numérique offre une multitude de fonctionnalités avancées. La vidéo sur IP offre une haute qualité d'image, une accessibilité à distance, des analyses, des possibilités d'intégration faciles, une évolutivité, une flexibilité, une rentabilité et une communication sécurisée.

- > **Haute qualité d'image.** Dans la vidéosurveillance, il est essentiel d'avoir une qualité d'image élevée pour capturer un incident et identifier les personnes ou objets impliqués. Grâce aux technologies de balayage progressif et TVHD / mégapixels, une caméra réseau peut offrir une haute qualité d'image et une résolution élevée. Pour en savoir plus sur la qualité de l'image, voir les chapitres , , et .
- > **Accessibilité à distance.** Les caméras réseau et les encodeurs vidéo peuvent être configurés à distance, permettant à plusieurs utilisateurs autorisés d'afficher des vidéos en direct et enregistrées à tout moment et depuis pratiquement n'importe quel emplacement connecté. Si nécessaire, les utilisateurs pourront ainsi permettre à un tiers, tel qu'un centre de surveillance d'alarmes ou les forces de l'ordre, d'avoir également accès à la vidéo.
- > **Analyses.** Dans la vidéo sur IP, une caméra peut être bien plus qu'une simple source de données vidéo. Les analyses de la caméra sont utilisées pour extraire des informations utiles de quantités colossales de vidéo et déclencher des actions instantanées, automatiques si nécessaire. Cela peut consister à avertir le personnel de sécurité ou de démarrer un enregistrement vidéo lors de la détection d'événements spécifiques. Les analyses qui utilisent des algorithmes de deep learning pour la détection et la classification des objets peuvent extraire des informations très détaillées sur les personnes et les véhicules d'une scène, permettant ainsi des recherches extrêmement précises et efficaces. Pour en savoir plus sur les analyses, voir le chapitre .
- > **Intégration facile et évolutive.** Les produits de vidéo sur IP basés sur des normes ouvertes peuvent être facilement intégrés aux différents systèmes de gestion vidéo disponibles. La vidéo d'une caméra réseau peut également être intégrée à d'autres systèmes, tels que les points de vente, le contrôle des accès ou un système de gestion de bâtiment. Pour plus d'informations sur les systèmes intégrés, voir le chapitre .
- > **Flexibilité et évolutivité.** Un système de vidéo sur IP peut se développer en même temps que les besoins de l'utilisateur. Les produits vidéo et d'autres types d'applications partagent le même réseau IP filaire ou sans fil pour communiquer des données. De la vidéo, de l'audio, des commandes PTZ et d'E/S, d'autres données, ainsi que l'alimentation, sont transportées sur le même câble, et autant de périphériques que nécessaire peuvent être ajoutés au système sans modifications importantes ou coûteuses de l'infrastructure de réseau. Les périphériques peuvent être placés et mis en réseau dans pratiquement n'importe quel endroit, et le système peut être aussi ouvert ou fermé que souhaité. Comme un système de vidéo sur IP est basé sur des équipements et des protocoles informatiques standard, il peut bénéficier de ces technologies à mesure que le système se développe. Par exemple, la vidéo peut être stockée sur des serveurs redondants placés dans des sites distincts pour renforcer la fiabilité et la sécurité, et des outils peuvent être utilisés pour le partage de charge automatique, la gestion de réseau et la maintenance du système.

- > **Rentabilité.** Un système de surveillance IP a généralement un coût total de possession faible. Les applications de vidéo sur IP peuvent venir se greffer sur l'infrastructure de réseau existante et déjà utilisée pour d'autres applications au sein d'une organisation. Les coûts de gestion et d'équipement sont également faibles, puisque les applications et le stockage dorsaux fonctionnent sur des serveurs basés sur des systèmes ouverts standard, et non sur du matériel propriétaire tel que des enregistreurs vidéo numériques dans le cas d'un système de vidéosurveillance analogique (CCTV). De nombreux périphériques vidéo sur IP sont alimentés par la technologie PoE (Power over Ethernet), qui fournit l'alimentation via le même câble Ethernet qui transporte les données (vidéo). PoE permet de réduire les coûts d'installation et facilite la sauvegarde. Pour en savoir plus sur PoE, voir le chapitre .
- > **Communication sécurisée.** Les périphériques vidéo sur IP et leurs flux vidéo peuvent être sécurisés de nombreuses façons. Par exemple, il est possible de mettre en œuvre l'authentification du nom d'utilisateur et du mot de passe, le filtrage d'adresse IP, l'authentification à l'aide de la norme IEEE 802.1X, le cryptage des données via HTTPS (SSL/TLS), et d'utiliser plusieurs niveaux d'accès utilisateur. Pour en savoir plus sur la sécurité réseau, voir le chapitre .
- > **Sécurité accrue.** Les périphériques Axis sont protégés par la plateforme de cybersécurité matérielle Axis Edge Vault, qui réduit leur exposition aux risques de cybersécurité et leur permet de fonctionner dans le cadre d'une unité sécurisée et fiable au sein du réseau. Axis Edge Vault met en œuvre des fonctions de cybersécurité telles que le système d'exploitation signé (ce qui garantit qu'AXIS OS n'est pas compromis), le démarrage sécurisé (en veillant au rejet de tout code non authentifié ou modifié pendant le processus de démarrage) et la vidéo signée (vérification de l'authenticité de la vidéo via une signature dans le flux vidéo).

Les installations vidéo analogiques existantes peuvent migrer vers un système de vidéo sur IP et tirer parti de certains avantages numériques à l'aide d'encodeurs vidéo et de dispositifs tels que des adaptateurs Ethernet sur câble coaxial, qui réutilisent les câbles coaxiaux existants. Pour en savoir plus sur les encodeurs et décodeurs vidéo, voir le chapitre .

1.3 Applications

La vidéo sur IP peut être utilisée dans un nombre quasi illimité d'applications. Le plus souvent, elle est utilisée pour la surveillance de sécurité ou la surveillance à distance des personnes, des lieux, des biens et des opérations. De plus en plus, la vidéo sur IP est également utilisée pour améliorer l'efficacité de l'entreprise à mesure que le nombre d'applications d'analyse augmente. Vous trouverez ci-dessous des possibilités d'application dans des segments clés de l'industrie.

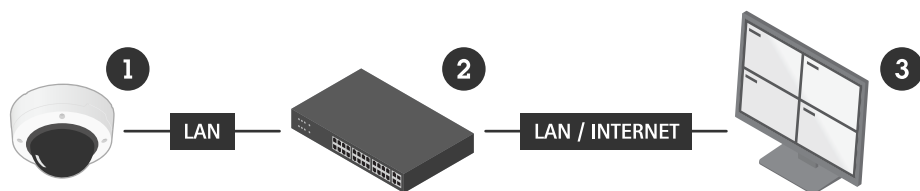
- > **Commerces.** Les systèmes de vidéo sur IP dans les magasins de détail peuvent réduire considérablement le vol, améliorer la sécurité du personnel et optimiser la gestion du magasin.
- > **Transport.** La vidéo sur IP aide à protéger les passagers, le personnel et les biens dans tous les types de transport.
- > **Services bancaires et financiers.** Les systèmes de vidéo sur IP permettent aux banques de surveiller efficacement leur siège social, leurs succursales et leurs guichets automatiques à partir d'un emplacement central.
- > **Surveillance urbaine.** La vidéo sur IP est l'un des outils les plus utiles pour lutter contre le crime et protéger les citoyens. Elle peut être utilisée pour détecter et dissuader les intrus.
- > **Enseignement.** Des garderies aux universités, les systèmes de vidéo sur IP aident à prévenir le vandalisme et à accroître la sécurité du personnel et des étudiants.
- > **Gouvernement.** La vidéo sur IP peut être utilisée par les forces de l'ordre, l'armée et les douanes. C'est aussi un moyen efficace de sécuriser toutes sortes de bâtiments publics.
- > **Santé.** La vidéo sur IP permet aux hôpitaux et aux établissements de santé d'améliorer la sécurité globale du personnel, des patients et des visiteurs.
- > **Secteur industriel.** La vidéo sur IP sécurise efficacement les périmètres et les locaux, et peut être utilisée pour surveiller et augmenter l'efficacité des lignes de fabrication, des processus et des systèmes logistiques.
- > **Infrastructure critique.** Qu'il s'agisse d'une centrale solaire, d'une sous-station électrique ou d'un centre de retraitement de déchets, la vidéo sur IP peut contribuer à assurer une exploitation sûre, sécurisée et ininterrompue. Les données de production provenant de sites distants peuvent être enrichies d'informations visuelles.

2. Caméras réseau

Les caméras réseau ou caméras IP offrent une grande variété de fonctionnalités pour répondre aux exigences de quasiment tous les systèmes de surveillance. Ce chapitre décrit ce qu'est une caméra réseau, les options et les fonctions dont elle peut être dotée, ainsi que les différents types de caméras disponibles : caméras fixes, caméras PTZ (panoramique/inclinaison/zoom), caméras modulaires, caméras thermiques et caméras avec boîtier antidéflagrant.

2.1 Qu'est-ce qu'une caméra réseau ?

La caméra réseau, également appelée caméra IP, est principalement utilisée pour envoyer de la vidéo / de l'audio sur un réseau IP tel qu'un réseau local (LAN) ou Internet. La caméra réseau permet de visualiser en direct et/ou d'enregistrer en continu, à des heures spécifiques, sur demande ou sur événement. La vidéo peut être enregistrée localement et/ou à distance, et la vidéo peut devenir accessible partout où il existe un accès à un réseau IP.



Une caméra réseau (1) se connecte à un commutateur réseau (2) et la vidéo est accessible (3) sur le réseau.

La caméra réseau regroupe à la fois une caméra et un ordinateur. Elle est composée principalement d'un objectif, d'un capteur d'image, d'un ou plusieurs processeurs et d'une mémoire. Les processeurs sont utilisés pour le traitement de l'image, la compression, l'analyse vidéo et les

fonctionnalités de mise en réseau. La mémoire sert principalement au stockage du logiciel du périphérique, mais également pour le stockage vidéo.

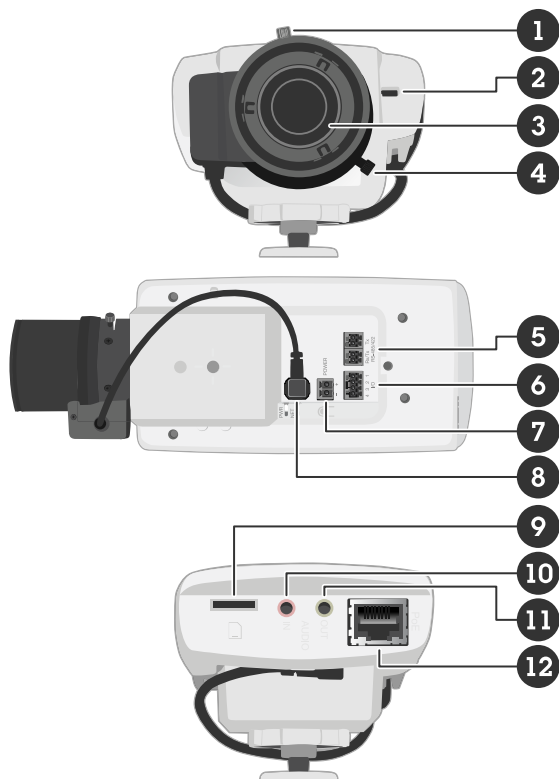
À l'instar d'un ordinateur, la caméra possède sa propre adresse IP, est directement connectée à un réseau filaire ou sans fil et peut être placée partout où il y a une connexion réseau. La caméra Web, elle, ne peut fonctionner que lorsqu'elle est connectée à un PC.

En plus de capturer de la vidéo, les caméras réseau permettent une gestion des événements qui vous permet de programmer des réponses automatiques à des événements prédéfinis. Les interventions types comprennent l'envoi d'alertes vidéo et d'e-mail en direct, l'activation de périphériques tels que des portes et des lumières, et l'activation d'enregistrements vidéo. En enregistrant uniquement lorsque quelque chose de spécifique se produit dans la scène, vous utilisez plus efficacement la bande passante réseau et l'espace de stockage.

Les caméras réseau prennent en charge l'analyse, qui extrait automatiquement ce qui est important dans le flux vidéo et l'utilise pour fournir des informations exploitables. Les analyses qui sont intégrées à la caméra (analyse en périphérie) ont plusieurs avantages, tels que la réduction des besoins de transmission réseau et une faible latence pour les scénarios qui nécessitent une réponse rapide. La technologie Axis Scene Intelligence associe des technologies avancées de traitement d'image à l'analyse en périphérie et le deep learning pour créer une base supérieure pour des performances analytiques cohérentes. Elle permet également à la caméra de s'adapter automatiquement en cas de changement de situation.

De nombreuses caméras réseau disposent d'une prise en charge de l'audio. Elles peuvent être dotées de ports d'entrée/sortie audio, ou de la possibilité de connecter des périphériques audio grâce à la technologie de conversion des ports ou la technologie bord à bord (qui fournissent des fonctions audio intégrées à la caméra). Les caméras réseau sont également souvent dotées de ports d'entrée/sortie qui permettent le raccordement à d'autres périphériques externes tels que des détecteurs de mouvement, des relais de verrouillage de porte et des alertes audio/visuelles.

La plupart des caméras vidéo sur IP sont alimentées par la technologie PoE (Power over Ethernet), ce qui signifie que l'alimentation est fournie par le câble réseau. Elles possèdent également un emplacement de carte mémoire pour le stockage local des enregistrements.



Avant, dessous et arrière d'une caméra réseau typique.

1. Commande de zoom
2. Microphone interne
3. Objectif P-Iris
4. Levier de mise au point
5. Port série
6. Bloc terminal E/S
7. Connecteur d'alimentation
8. Connecteur de l'iris
9. Fente pour carte mémoire
10. Entrée audio
11. Sortie audio
12. Connecteur réseau

Les caméras Axis sont installées sur un réseau via AXIS Camera Station Edge ou AXIS Camera Station Pro, systèmes de gestion vidéo (VMS) qui détectent et configurent automatiquement la caméra. Les clients avancés dotés de grandes installations peuvent utiliser AXIS Device Manager pour configurer les caméras. Il est également possible d'accéder à une caméra directement via ses pages Web intégrées en entrant son adresse IP dans un navigateur. La configuration concerne, par exemple, l'accès utilisateur, les paramètres de la caméra, la résolution, la fréquence d'image, le format de compression (H.264/H.265/AV1), ainsi que les règles pour les événements.

Les caméras Axis prennent également en charge une multitude d'accessoires qui étendent leurs capacités. Par exemple, les caméras peuvent être connectées à un réseau fibre optique à l'aide d'un commutateur de conversion de média ou pour coaxer des câbles à l'aide d'un adaptateur Ethernet sur câble coaxial prenant en charge PoE.

2.1.1 Plateforme d'applications AXIS Camera (ACAP)

La plupart des caméras Axis (ainsi que les haut-parleurs, les interphones et les produits radar) sont pris en charge par la Plateforme d'applications AXIS Camera (ACAP). ACAP est une plateforme ouverte d'applications pour un large éventail de secteurs et de cas d'utilisation et elle active des applications d'analyses, accessibles à partir du site Web d'Axis ou de fournisseurs tiers. Ces applications peuvent être téléchargées et installées sur les périphériques. ACAP permet également de développer des applications personnalisées et d'exécuter des applications à la périphérie (complètement ou partiellement) en combinant des analyses avancées à la périphérie et des technologies basées sur le cloud ou sur des serveurs. Pour en savoir plus sur ACAP, voir www.axis.com/developer-community/acap

2.1.2 Interface de programmation d'applications

Tous les produits de vidéo réseau d'Axis disposent d'une interface de programmation (API) appelée VAPIX®. VAPIX permet aux développeurs d'incorporer facilement les produits vidéo d'Axis et leurs fonctionnalités intégrées dans d'autres solutions logicielles.

2.1.3 ONVIF

La plupart des produits vidéo réseau d'Axis sont conformes à ONVIF. ONVIF®¹ est un forum mondial ouvert, fondé par Axis, Bosch et Sony en 2008, dont l'objectif est de normaliser l'interface réseau des produits de vidéo sur IP et de contrôle des accès de différents fabricants afin d'assurer une interopérabilité accrue. Il donne aux utilisateurs la possibilité d'utiliser des produits conformes à ONVIF provenant de différents fabricants dans un système de sécurité sur IP multifournisseur. ONVIF est aujourd'hui approuvé par la majorité des plus grands fabricants mondiaux de produits de

sécurité sur IP, et compte plus de 500 sociétés membres. Pour plus d'informations, visitez www.onvif.org

¹ONVIF est une marque commerciale d'ONVIF, Inc.

2.2 Fonctions de caméra permettant de gérer des scènes difficiles

La qualité vidéo des caméras de sécurité peut être affectée négativement par des conditions météorologiques difficiles ou des niveaux de luminosité faibles ou très fluctuants. Ce chapitre identifie les facteurs et les fonctionnalités des caméras qui ont un impact sur la capacité des caméras à gérer des scènes difficiles.

2.2.1 Plage dynamique étendue (WDR)

Lorsque le niveau de luminosité change dans la scène, la caméra Axis s'ajuste automatiquement pour assurer une exposition optimale. L'option WDR (plage dynamique étendue) est recommandée pour les situations difficiles avec des scènes contenant à la fois des parties lumineuses et sombres. Cette fonction est activée par défaut et constitue la meilleure façon d'utiliser les caméras Axis car elle ne nécessite pas d'ajustements au fil du temps. La fonction WDR permet souvent à la caméra de combiner des temps d'exposition courts dans les parties lumineuses de la scène et des temps d'exposition longs dans les zones sombres. L'image résultante est correctement exposée dans toutes les zones. Pour plus de détails sur l'imagerie WDR, voir la section .

2.2.2 Technologie Lightfinder

La vidéosurveillance couleur permet de mieux identifier les personnes, les véhicules et les incidents. Les caméras dotées de la technologie Axis Lightfinder sont extrêmement sensibles à la lumière et peuvent fournir des images couleur en mode jour avec une luminosité de 0,08 lux ou moins. Tout cela est rendu possible en sélectionnant le capteur d'image et l'objectif les mieux adaptés, et grâce au savoir-faire d'Axis en matière de traitement d'image et au développement de puces ASIC internes. Ces éléments de Lightfinder s'améliorant régulièrement, Lightfinder, est également en évolution constante. Lightfinder 2.0, qui convient même pour les caméras dotées de résolutions jusqu'à 4K, représente un changement majeur dans cette évolution, avec une sensibilité à la lumière accrue, une reproduction des couleurs plus réaliste et un réglage personnalisé pour les utilisateurs avancés.



À gauche : une image aux couleurs vives et nettes, produite par une caméra Lightfinder 2.0, même si l'intensité lumineuse était de seulement 0,05 lux sous le pont. À droite : un instantané de la même scène manipulé pour visualiser la façon dont la scène apparaît à l'œil humain.

2.2.3 Fonctionnalité jour/nuit

Les caméras réseau avec fonctionnalité jour / nuit disposent d'un filtre infrarouge à retrait automatique. Le filtre est activé pendant la journée, ce qui permet à la caméra de produire des couleurs identiques à celles perçues par l'œil humain. La nuit, le filtre est retiré pour permettre à la caméra de profiter de la lumière quasi-infrarouge et produire des images noir et blanc de bonne qualité. Cela permet de tirer le meilleur parti des capacités d'une caméra réseau en cas de luminosité faible.



À gauche : mode jour. À droite : mode nocturne.

2.2.4 Éclairage IR intégré

En cas de faible luminosité ou d'obscurité totale, les éclairages infrarouge intégrés dans la caméra ou le projecteur infrarouge installé séparément augmentent la capacité de la caméra à utiliser la lumière infrarouge pour produire des images en noir et blanc de qualité. La lumière proche

infrarouge émise par la lune, les réverbères ou les éclairages infrarouges ne sont pas visibles à l'œil nu, mais le capteur d'image d'une caméra le détecte.

Les voyants infrarouges intégrés aux caméras Axis peuvent être ajustés pour correspondre à l'angle de vue et activés automatiquement dans l'obscurité, sur événement ou sur demande des utilisateurs.



À gauche : un instantané en mode nocturne capturé sans éclairages infrarouges (une faible quantité de lumière passe sous la porte dans le coin gauche de la pièce). À droite : un instantané en mode nocturne capturé à l'aide d'éclairages infrarouges.

2.2.5 OptimizedIR

Les caméras Axis avec OptimizedIR offrent une combinaison unique et puissante de l'intelligence de la caméra et de la technologie LED de pointe grâce aux solutions IR intégrées à la caméra Axis les plus sophistiquées. Parmi ces solutions, on trouve une technologie brevetée permettant un éclairage régulier dans le champ de vision variable de la caméra, une gestion extrêmement efficace de la chaleur et l'utilisation de LED haute qualité et longue portée qui sont réglées précisément avec la caméra. OptimizedIR est en développement constant, avec l'ajout de nouvelles fonctionnalités avancées.

2.2.6 Objectifs à faible valeur f

Les objectifs de caméras ayant un chiffre f inférieur ont une meilleure capacité de collecte de lumière. En général, plus le chiffre f est faible, plus elle est performante dans des conditions de faible luminosité. Il peut arriver que certains types d'éclairage soient plus faciles à gérer avec un chiffre f plus élevé. La sensibilité à la lumière de la caméra dépend à la fois de son objectif, du capteur d'image et du traitement de l'image. Vous trouverez plus de détails sur les objectifs et les capteurs d'image au chapitre .

2.2.7 Régulation automatique du diaphragme

Pour les scènes dont les niveaux de luminosité sont changeants, un diaphragme réglable automatiquement (diaphragme DC, P-Iris ou objectif i-CS) est recommandé pour obtenir le bon niveau d'exposition. Les caméras avec un diaphragme P-IrisP ou un objectif i-CS ont un meilleur contrôle du diaphragme pour une qualité d'image optimale dans toutes les conditions d'éclairage. Plus de détails sont couverts dans le chapitre .

2.2.8 La bonne résolution

La résolution d'une caméra est définie par le nombre de pixels sur le capteur d'image. Une caméra dotée d'un capteur *mégapixel* fournit des images d'un million de pixels ou plus.

Une résolution élevée est généralement souhaitée. Avec un angle de vue large, une caméra à résolution plus élevée offre une zone de couverture plus large. Avec un angle de vue étroit, une caméra avec une résolution plus élevée offre plus de détails, ce qui aide à mieux identifier les personnes et les objets.

Mais tandis que l'industrie de la surveillance ne cesse d'évoluer vers des résolutions plus élevées, les fabricants ont cherché à conserver une taille de capteur identique dans le but d'éviter l'augmentation du coût d'un capteur plus grand. Cela signifie que chaque pixel doit être plus petit et que les pixels plus petits sont capables de capturer moins de lumière. Si l'on augmente simplement le nombre de pixels sur un capteur de la même taille, on obtient une meilleure résolution, mais votre image peut également présenter une qualité moindre, en particulier dans les scènes à faible luminosité. Une caméra avec un capteur d'environ 4 mégapixels offre généralement un équilibre entre la résolution et la sensibilité à la lumière car elle produit une taille de pixels suffisante, sans qu'il soit nécessaire d'utiliser un capteur plus grand et plus coûteux.

Les caméras prenant en charge HDTV 720p (1280 x 720 pixels), HDTV 1080p (1920 x 1080 pixels), WQHD (2560x1440 pixels) et 4K Ultra HD (3840 x 2160 pixels), respectivement d'environ 1, 2, 4 et 8,5 mégapixels, respectent les normes qui garantissent une fréquence d'image maximale, une haute fidélité des couleurs et un rapport d'aspect de 16:9.

2.2.9 Imagerie thermique

Outre la lumière du soleil, la lumière artificielle et la lumière proche infrarouge, le rayonnement thermique peut également être utilisé pour générer des images. Une caméra thermique ne nécessite aucune source de lumière ; elle détecte le rayonnement thermique émis par un objet plus chaud que le zéro absolu (0 K).

Les caméras thermiques peuvent être utilisées pour détecter des sujets dans l'obscurité complète, dans la fumée ou le brouillard, ou lorsque les sujets sont obscurcis par des ombres ou un arrière-plan complexe. Ces caméras ne sont pas non plus éblouies par les lumières fortes. Les caméras thermiques sont idéales à des fins de détection et peuvent être utilisées en complément des caméras conventionnelles pour améliorer l'efficacité du système de surveillance. Pour plus d'informations sur les caméras thermiques, voir la section .



À gauche : image provenant d'une caméra conventionnelle dans une scène brumeuse. À droite : image provenant d'une caméra thermique dans la même scène brumeuse.

2.2.10 Stabilisation d'image

Une caméra de surveillance montée dans un lieu exposé, tel qu'un poteau élevé ou un panneau de signalisation à proximité d'une route passante, peut être secouée par le vent ou le passage des véhicules. Cela peut rendre la vidéo floue, en particulier si un objectif zoom puissant est utilisé. Des caméras moins sensibles aux vibrations rendent l'installation plus flexible et offrent plusieurs options de montage, même si les vibrations doivent être évitées dans la mesure du possible. Comme une vidéo stabilisée contient comparativement moins de mouvements, elle nécessite moins de ressources en bande passante et en stockage qu'une vidéo affectée de secousses.

Les techniques de stabilisation de l'image en temps réel peuvent rendre la sortie vidéo moins sensible aux vibrations et maintenir la qualité de l'image.

- > La **stabilisation d'image électronique (OIS)** s'appuie généralement sur des gyroscopes ou des accéléromètres pour détecter et mesurer les vibrations de la caméra. Cette méthode est particulièrement utile lors de l'utilisation de longues distances focales et fonctionne bien dans des conditions de faible luminosité. Le principal inconvénient d'une solution optique est son prix.
- > La **stabilisation d'image électronique (EIS)** repose sur des algorithmes de modélisation du mouvement de la caméra, qui sont ensuite utilisés pour corriger les images. Cette méthode est

économique, mais ne permet pas toujours de distinguer le mouvement physique induit par les vibrations du mouvement perçu causé par des objets se déplaçant rapidement devant la caméra.

Axis s'appuie sur une méthode de stabilisation qui correspond à une hybridation des deux techniques. La fonction Axis est appelée *stabilisation d'image électronique* (EIS). Elle combine des gyroscopes avancés associés à des algorithmes optimisés pour constituer un système robuste et fiable. Elle couvre une large gamme de fréquences de vibration et s'adapte à des amplitudes faibles ou élevées. L'EIS d'Axis peut toujours faire la distinction entre les vibrations induites physiquement et le mouvement perçu. Le système est très performant même par faible luminosité car il s'appuie sur les informations des gyroscopes plutôt que sur le contenu vidéo pour calculer les mouvements. Pour la même raison, le système peut toujours faire la distinction entre les mouvements perçus et les vibrations induites physiquement.

2.3 Fonctions de la caméra pour faciliter l'installation

Les caméras Axis intègrent des fonctionnalités qui rendent les produits faciles à installer et à utiliser, ainsi que plus fiables, en réduisant au minimum les erreurs d'installation.

2.3.1 Installation en extérieur possible dès la sortie d'usine

Les produits Axis conçus pour l'extérieur sont prêts à être installés en extérieur dès leur déballage. Aucun boîtier séparé n'est requis et les produits sont vendus avec des vis captives qui ne peuvent pas tomber de leurs orifices. Les produits sont conçus pour fonctionner à différentes températures et offrent une protection contre la poussière, la pluie et la neige. Certains de nos produits répondent même aux normes militaires de fonctionnement dans les climats extrêmes.

2.3.2 Caméras mises au point en sortie d'usine

Les caméras Axis avec objectif à focale fixe sont prêtes à l'emploi en usine, pour éviter de faire la mise au point pendant l'installation, rendant celle-ci plus rapide et plus facile. En effet, les caméras avec objectif à focale fixe et un champ de vision large ou intermédiaire ont généralement une grande profondeur de champ (la portée au sein de laquelle les objets proches et lointains sont nets). Pour en savoir plus sur la distance focale, les chiffres f et la profondeur de champ, voir le chapitre .

2.3.3 Mise au point à distance et zoom

Les caméras avec objectif à focale variable, mise au point à distance et zoom évitent d'avoir à ajuster manuellement, sur place, la mise au point et le champ de vision, lorsque la caméra est

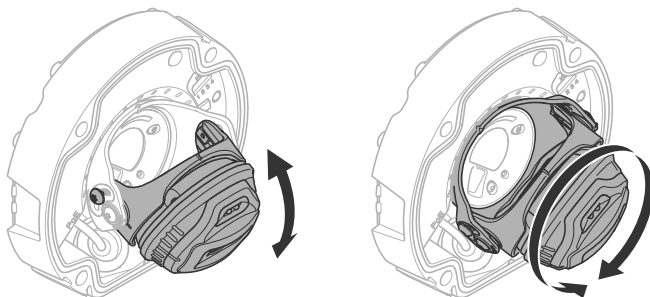
installée. Cela peut être fait à distance grâce au moteur d'objectif de la caméra, depuis un ordinateur connecté au réseau.

2.3.4 Mise au point du foyer arrière

Les caméras avec objectif à focale variable, support CS et mise au point à distance permettent d'effectuer la mise au point à distance à partir d'un ordinateur, en ajustant progressivement la position du capteur d'image. Les objectifs disponibles en option permettent également d'utiliser cette fonctionnalité.

2.3.5 Réglage de l'angle de caméra sur 3 axes

La caméra dôme Axis est conçue avec un réglage d'angle à 3 axes qui permet au porte-objectif (comprenant la lentille et le capteur d'image) de faire un panoramique, de s'incliner et de pivoter. La caméra peut ainsi être montée sur un mur ou au plafond. Les utilisateurs peuvent alors facilement ajuster la direction de la caméra et redresser l'image. Grâce à la flexibilité de l'ajustement de la caméra, associée à la possibilité de faire pivoter l'image à l'aide de son interface Web, il est possible d'obtenir un flux vidéo orienté verticalement (format couloir).



Réglage de l'angle de caméra sur 3 axes

2.3.6 Format corridor

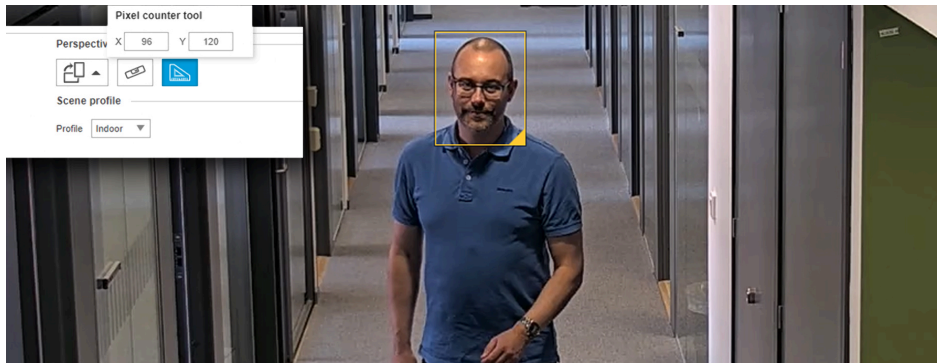
Le Corridor Format permet à une caméra fixe de fournir une vidéo orientée verticalement. Le format vertical optimise la couverture de zones telles que les couloirs, les halls et les allées, en maximisant la qualité d'image tout en réduisant l'utilisation de la bande passante et du stockage. Il permet notamment aux caméras réseau TVHD de fournir une vidéo avec un rapport d'aspect de 9:16. Pour ce faire, avec une caméra dôme, il faut d'abord tourner l'objectif à 90° (ou avec une caméra compacte ou à boîtier, en pivotant l'intégralité de la caméra), puis tourner l'image vidéo à 90° dans la page Web de la caméra.

2.3.7 Redressement d'image

Le redressement d'image est un outil de traitement d'image qui permet de corriger numériquement de légers biais mécaniques en faisant pivoter l'image (autour de l'axe longitudinal). L'objectif est de niveler l'image avec l'horizon.

2.3.8 Compteur de pixels

Le compteur de pixels Axis est une aide visuelle en forme de cadre avec un compteur correspondant pour montrer la largeur et la hauteur du cadre. Le compteur de pixels permet de garantir que la résolution vidéo est suffisamment bonne pour atteindre certains objectifs, comme l'identification faciale, mais aussi pour vérifier que la résolution d'un objet répond aux exigences réglementaires ou des clients. Pour plus de détails sur les densités de pixels recommandées selon les objectifs de la surveillance, voir le chapitre .



Compteur de pixels Axis affichant la résolution en pixels d'un visage.

2.4 Types de caméras réseau

Les caméras réseau peuvent être conçues pour une utilisation à l'intérieur uniquement ou pour une utilisation aussi bien à l'intérieur qu'à l'extérieur. Une caméra d'extérieur est fournie avec un boîtier de protection externe. Pour plus de détails sur la protection, voir la section .

2.4.1 Caméras en boîtier



Une caméra à boîtier est un type de caméra de surveillance traditionnelle. La caméra et sa direction d'observation sont facilement visibles, ce qui la rend idéale pour dissuader les vandales et intrus. La plupart des caméras à boîtier sont munies d'un objectif interchangeable, qui peut être fixe, à focale variable ou à zoom motorisé. Ce type de caméra est disponible pour une utilisation intérieure et extérieure. Les caméras à boîtier Axis pour usage extérieur sont pré-installées dans des boîtiers de protection.

2.4.2 Caméras cylindriques



Les caméras cylindriques ont un design petit et mince, comparé aux caméras à boîtier. Elles sont conçues pour l'extérieur, et peuvent donc être placées aussi bien à l'intérieur qu'à l'extérieur, sans protection supplémentaire. Toutes les caméras cylindriques Axis sont équipées d'un illuminateur IR intégré qui permet la surveillance par faible luminosité ou dans l'obscurité totale. Comme avec les caméras à boîtier, la direction de visualisation de la caméra est évidente. Sur les caméras cylindriques, cependant, il n'est pas possible de changer d'objectif.

2.4.3 Caméras-dômes



Les caméras dômes sont des caméras fixes préinstallées dans un petit boîtier en forme de dôme. Le principal avantage de cette caméra réside dans son design discret et imperceptible. De plus, les personnes dans le champ de vision de la caméra ont du mal à voir dans quelle direction pointe la caméra. Un large choix d'accessoires permet une installation encore plus discrète, comme des boîtiers noirs, des supports encastrés et des dômes fumés. La caméra dôme est également plus

résistante au sabotage que les autres caméras fixes. Elle peut être équipée d'un objectif à zoom fixe, à focale variable ou d'un objectif à zoom motorisé.

Les caméras dômes sont conçues avec différents types et niveaux de protection, tels que la résistance au vandalisme et à la poussière, et les certifications IP66, IP67 et NEMA 4x pour les installations extérieures. Aucun boîtier externe n'est requis. Ces caméras sont généralement montées sur un mur, au plafond ou sur un poteau.

2.4.3.1 Caméras à dôme embarquées



La catégorie des caméras embarquées comprend les caméras modulaires, les caméras à dôme et les caméras panoramiques.

Les caméras embarquées sont spécialement conçues pour la surveillance dans le matériel roulant, les bus et d'autres véhicules. Les conditions de la surveillance embarquée varient en fonction du type de véhicule dans lequel la caméra est utilisée. Dans certaines zones d'utilisation, comme dans les trains, il existe des protocoles et des réglementations spécifiques à respecter, et seuls les produits testés spécifiquement pour ces environnements doivent être utilisés. Toutefois, la conception des caméras de surveillance embarquée doit généralement être particulièrement robuste. En effet, les caméras doivent résister à des conditions difficiles qu'entraînent les vibrations, les chocs et les secousses, ainsi que la poussière, l'eau et les variations de température. L'apparence discrète d'une caméra embarquée est souvent associée à une alarme de sabotage active qui permet de détecter et d'empêcher les tentatives de redirection et de dérèglement de la caméra.



Une caméra dôme embarquée fixée au plafond d'un bus.

2.4.3.2 Caméras panoramiques



Caméras panoramiques : un capteur unique, un multicapteur, une solution multidirectionnelle et une solution combinant une caméra multidirectionnelle à une caméra PTZ.

Une caméra panoramique est une caméra à dôme qui offre une couverture de zone étendue et d'excellents détails d'image, dans une installation efficace à caméra unique. La caméra peut être mono-capteur, multicapteur ou multidirectionnelle.

Une caméra panoramique à capteur unique possède un objectif grand angle qui offre une vue de type fisheye (grand angle) à 360°. La vue peut être transformée, en direct ou sur du matériel enregistré, en diverses vues rectangulaires, y compris en format panoramique, double panoramique ou vue quadruple (en simulant quatre caméras).



Une caméra panoramique à un seul capteur offre plusieurs modes de visualisation, tels que la vue d'ensemble à 360°, la vue quadravision et le panorama.

Une caméra multicapteur fournit une couverture continue à 180°, très détaillée et avec une déformation minimale. Comme elle possède plusieurs capteurs, elle combine un champ de vision étendu, une bonne qualité d'image et une densité de pixels élevée. Elle utilise un réglage universel de balance des blancs et une exposition synchronisée pour tous les capteurs. Grâce à ses images assemblées en toute transparence, une caméra multicapteur élimine également les angles morts.



Vue à 180° depuis une caméra multicapteur.

Une caméra multidirectionnelle avec une couverture à 360 ° est une caméra panoramique avec des têtes de caméra réglables individuellement. Elle est idéale, par exemple, dans les magasins, les halls d'entrée et les entrepôts.

Une solution combinant une caméra panoramique multidirectionnelle à une caméra PTZ s'avère particulièrement utile aux carrefours, par exemple.

2.4.4 Caméras modulaires



Caméras modulaires, y compris les unités principales et les unités de détection.

Les caméras modulaires Axis sont conçues pour fournir une installation flexible et discrète. Se fondant dans l'environnement, elles peuvent être utilisées pratiquement n'importe où. Les capteurs peuvent être installés dans des espaces restreints, utilisés dans les bus et les voitures de police, intégrés à des machines telles que les guichets automatiques, et placés au niveau des yeux à la sortie des bâtiments pour une capture optimale du visage. Elles se destinent particulièrement aux applications de surveillance et d'analyse vidéo et audio hautement discrètes.

Une caméra modulaire est un concept de caméra en deux parties, où l'unité principale peut être installée jusqu'à 30 mètres (98 pieds) du capteur. Le capteur contient l'objectif et le capteur d'image ; l'unité principale traite l'image. Ce concept divisé permet plus de flexibilité en termes de matériel et d'installation. L'unité principale et le capteur peuvent facilement être échangés ou déplacés après l'installation initiale. Les câbles amovibles assurent une maintenance ou une mise à niveau simplifiée. Une installation discrète réduit également le risque d'altération.

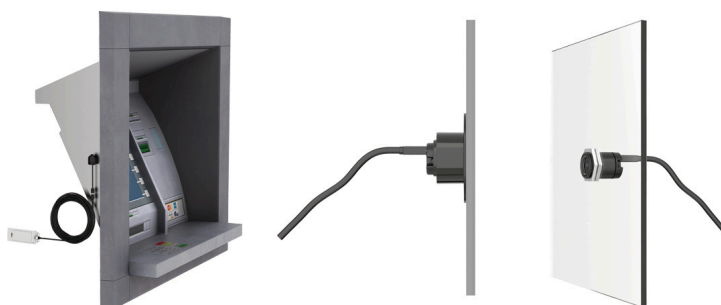


La série de caméras modulaires AXIS F propose une gamme de caméras modulaires hautes performances conçues pour la surveillance intérieure, extérieure et embarquée. La série comprend deux unités principales robustes, deux unités principales à boîtier seul reconnues par l'UL, plusieurs options de câbles et des unités de capteurs pour une large gamme d'applications.

Les caméras modulaires constituent également une solution rentable lorsque vous avez besoin d'installer plusieurs caméras dans une seule zone. Il existe des unités principales à un et quatre canaux ; une unité principale à quatre canaux peut se connecter à quatre capteurs. Grâce à des longueurs de câble maximales de 30 m (98 pi), une unité principale équipée de quatre capteurs peut couvrir des zones plus étendues et plus petites. Quatre capteurs connectés permettent également la diffusion simultanée et multiple de flux vidéo et en quadrivision via une adresse IP unique. Une unité principale, qu'elle prenne en charge un ou quatre canaux vidéo, nécessite une seule licence VMS et un port de commutateur pour une surveillance économique.

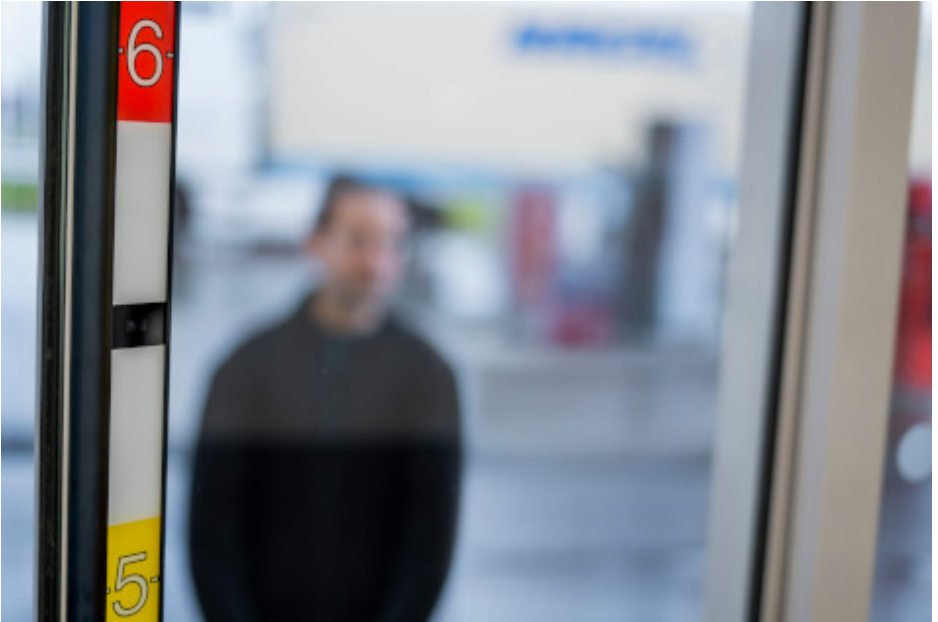


Visionnage en quadrivision en continu à partir d'un système de caméra modulaire à quatre canaux dans un bus.



À gauche, une caméra modulaire à sténopé dans une application de guichet automatique. À droite, une unité de capteur montée sur un mur et un panneau de verre.

Une large gamme d'unités de capteurs avec différents facteurs de forme et différents types d'objectifs, tels que standard, focale variable, mini dôme et à sténopé, sont disponibles.



Conçu pour être placé à proximité de la sortie des bâtiments, un boîtier avec jauge de hauteur permet une installation extrêmement discrète de capteurs à sténopé. La caméra est positionnée et orientée face au visage de la personne pour une identification plus fiable.

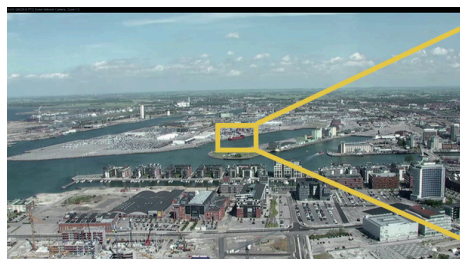
2.4.5 Caméras PTZ



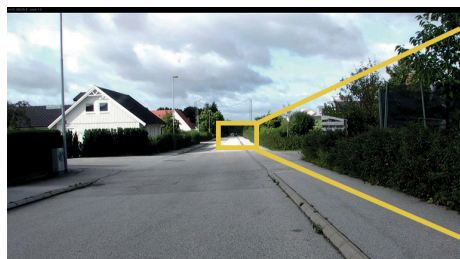
Modèles de caméras PTZ avec des caractéristiques telles que : (à partir de la gauche) résolution HDTV 1080p avec technologie Sharpdome, refroidissement actif, une solution combinant une caméra multi-capteur et une caméra PTZ, et (tout à droite) une caméra visuelle et une caméra thermique associées dans une même unité.

Une caméra PTZ offre des fonctions de panoramique, d'inclinaison et de zoom (à l'aide d'une commande manuelle ou automatique), ce qui active la couverture d'une zone étendue et permet d'obtenir un niveau de détail élevé lors d'un zoom. Les caméras PTZ Axis ont généralement la capacité d'effectuer un panoramique sur 360°, de s'incliner sur 180° ou 220°, et sont souvent équipées d'un objectif zoom. Un véritable objectif zoom fournit un zoom optique qui maintient la résolution de l'image, contrairement au zoom numérique, qui agrandit l'image au détriment de la qualité de l'image.

Dans les opérations avec surveillance en direct, les caméras PTZ peuvent être utilisées pour suivre un objet et effectuer un zoom avant pour une inspection plus approfondie. Dans les opérations non surveillées par un opérateur, des tours de garde automatiques peuvent être utilisés pour surveiller différentes zones d'une scène. En mode tour de garde, une caméra PTZ peut parvenir à couvrir une zone que seules de nombreuses caméras fixes pourraient couvrir en temps normal.



Vue large (gauche) et vue agrandie (droite) sur une caméra PTZ HDTV 1080p, rendant le texte sur le cargo lisible à une distance de 1,6 km (1 mile).



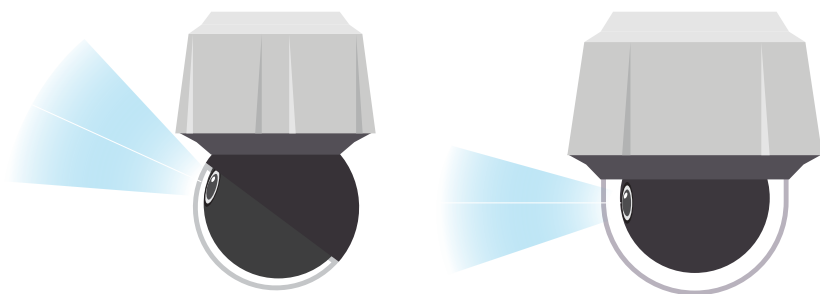
Vue large (gauche) et vue agrandie (droite) sur une caméra PTZ HDTV 1080p, permettant de lire la plaque d'immatriculation à une distance de 275 m (900 pieds).

Les caméras PTZ Axis peuvent être équipées de diverses fonctionnalités intelligentes, par exemple :

- > **Ronde de contrôle (positions prédéfinies).** Les caméras PTZ permettent généralement de programmer plusieurs positions prédéfinies (jusqu'à 100). Une fois que ces positions ont été définies dans la caméra, l'opérateur peut rapidement passer d'une position à l'autre en sélectionnant simplement une position. En mode tour de garde, la caméra peut être programmée pour passer automatiquement d'une position prédéfinie à la suivante dans un ordre prédéterminé ou aléatoire. Jusqu'à 20 tours de garde peuvent être configurés et activés à différents moments de la journée.
- > **Ronde de contrôle (enregistrée).** La fonctionnalité d'enregistrement de tour des caméras PTZ permet de configurer facilement un tour automatique à l'aide d'un dispositif, comme un joystick, pour enregistrer les mouvements panoramique-inclinaison-zoom d'un opérateur et le temps passé dans chaque position. Le tour enregistré peut ensuite être activé par simple pression d'un bouton ou à une heure spécifique.
- > **Suivi automatique.** Cette application d'analyse détectera automatiquement une personne ou un véhicule en mouvement et le ou la suivra dans la zone de couverture de la caméra. Le suivi automatique est particulièrement utile pour la vidéosurveillance sans opérateur où la présence occasionnelle de personnes ou de véhicules nécessite une attention particulière. Cette fonctionnalité permet de réduire considérablement le coût du système de surveillance, car il faut moins de caméras pour couvrir une même scène. Cela rend également la solution plus efficace, puisque la caméra PTZ peut enregistrer les parties d'une scène où il y a de l'activité.
- > **AXIS Radar Autotracking for PTZ.** Cette application logicielle utilise les données de mouvement provenant des dispositifs radar Axis pour trouver les objets d'intérêt sur un site, et contrôle automatiquement la direction et le niveau de zoom d'une ou de plusieurs caméras PTZ. Le dispositif radar agit en complément de la caméra PTZ, et l'application permet une confirmation visuelle des objets détectés même en dehors du champ de vision actuel de la caméra. AXIS Radar Autotracking pour caméra PTZ permet également de moins souvent contrôler la caméra au joystick.
- > **AXIS Perimeter Defender PTZ Autotracking.** Lorsqu'elle est installée sur une caméra PTZ, cette application permet à une caméra thermique fixe ou à une caméra visuelle fixe prenant en charge les outils d'analyse AXIS Perimeter Defender de diriger automatiquement la caméra PTZ pour obtenir une vue rapprochée des objets déclencheurs de l'alarme dans la zone de détection de la caméra fixe. La caméra PTZ règle automatiquement le niveau d'agrandissement pour conserver tous les objets de l'alarme dans la scène, y compris les nouveaux qui apparaissent dans la zone de détection de la caméra fixe.
- > **Portier actif/avancé.** Le portier avancé permet aux caméras PTZ de pivoter, d'incliner et de zoomer dans une position prédéfinie lorsqu'un mouvement est détecté dans une zone prédéfinie, puis de revenir à la position initiale après un délai spécifique. Le portier devient un portier actif lorsqu'il peut continuer à suivre l'objet détecté.

2.4.5.1 Technologie Sharpdome

Avec la technologie Axis Sharpdome, une caméra PTZ peut voir au-dessus de son horizon. La mécanique Sharpdome permet au dôme de pivoter complètement, contrairement à un dôme conventionnel où la caméra tourne à l'intérieur du dôme. La mécanique et le positionnement du module caméra ainsi que la conception unique du dôme extérieur permettent d'obtenir la même netteté d'image optimale et de reproduire une scène complète avec la même fidélité, quelles que soient les positions de panoramique et d'inclinaison. Cela permet une identification claire des objets jusqu'à 20° au-dessus de l'horizon de la caméra.



Une caméra avec Sharpdome (à gauche) et une caméra à dôme classique (à droite)

Le Sharpdome inclut une fonction de séchage rapide, pour fournir des images nettes par temps pluvieux. Lorsque des gouttes d'eau recouvrent le dôme, la fonction de séchage rapide fait tourner le dôme en alternance à grande vitesse, se débarrassant ainsi efficacement de l'eau.



Deux instantanés de la même scène pluvieuse, avant de secouer (à gauche) et après avoir secoué (à droite) le dôme en utilisant la fonction de séchage rapide.

2.4.6 Caméras thermiques



Caméras thermiques cylindriques (à gauche) et boîtier fixe monté sur une unité de positionnement (au centre). La caméra PTZ bispectrale (à droite) associe une caméra visuelle et une caméra thermique en une seule unité pour les scénarios de surveillance critiques.

Les caméras thermiques détectent le rayonnement thermique (chaleur) que tous les objets émettent à température supérieure au zéro absolu. Capables de sélectionner de petites différences de températures et de les convertir en une image visuelle, ces caméras peuvent distinguer des personnes et des véhicules à de grandes distances. Elles sont performantes même dans l'obscurité complète et quelles que soient les conditions d'éclairage, les camouflages, la végétation, les conditions météorologiques difficiles ou d'autres conditions où une caméra visuelle peut s'avérer insuffisante.

Les caméras thermiques sont souvent employées dans les systèmes de protection périmétrique. La vidéo en direct provenant d'une caméra thermique peut détecter de l'activité autour d'emplacements critiques bien avant qu'une caméra visuelle n'ait vu quelque chose d'inhabituel. Les images thermiques sont analysées automatiquement, directement sur la caméra, et le système de sécurité peut être configuré de manière à proposer diverses réponses. Il peut déclencher des alertes audio automatiques en utilisant des haut-parleurs pour dissuader activement les intrus, envoyer des alertes par e-mail au personnel de sécurité, et effectuer un panoramique et zoomer les caméras visuelles du système de manière à capturer et enregistrer des séquences vidéo permettant d'identifier les intrus. Les images thermiques seules ne suffisent généralement pas pour identifier les individus. Cela fait des caméras thermiques une option précieuse pour la surveillance dans des endroits où la confidentialité est particulièrement importante. Les caméras thermiques peuvent également servir à surveiller la température de procédés industriels. Elles permettent, par exemple, de détecter des fuites thermiques dans les bâtiments ou de déterminer si un véhicule a récemment été utilisé.

Une caméra thermométrique est une caméra thermique conçue pour surveiller des objets ou des processus afin de détecter si la température dépasse ou tombe en dessous d'un ensemble de limites

définies par l'utilisateur. Ce type de caméra est utilisé pour prévenir les dommages, les pannes, les incendies ou d'autres situations dangereuses.

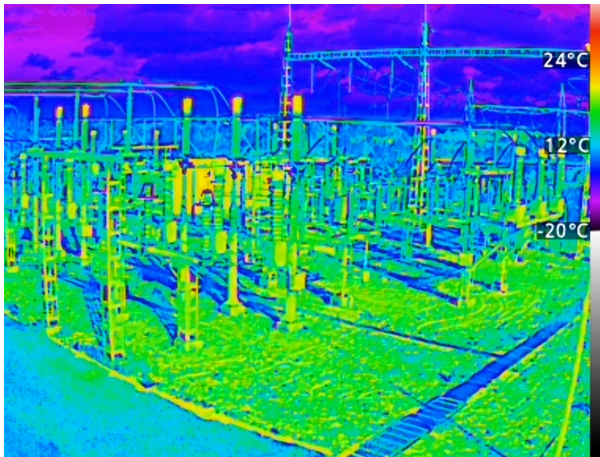


Image provenant d'une caméra thermométrique. Différentes températures sont visualisées à l'aide d'une palette de couleurs.

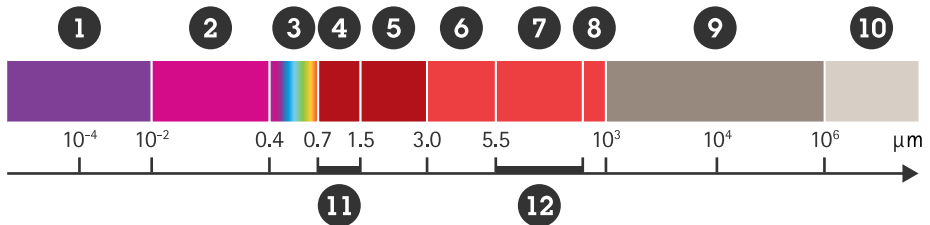
Les caméras thermiques nécessitent des optiques spéciales, car le verre standard bloque le rayonnement thermique. La plupart des objectifs de caméras thermiques sont fabriqués en germanium, ce qui permet à la lumière infrarouge et au rayonnement thermique de passer. L'objectif influe sur la capacité de vision de la caméra thermique. Un objectif grand angle donne à une caméra thermique un champ de vision plus large, mais une plage de détection plus courte qu'avec un téléobjectif, qui offre une plage de détection plus longue avec un champ de vision plus étroit.

Les caméras thermiques nécessitent également un capteur d'image spécial. Les capteurs pour l'imagerie thermique peuvent être répartis en deux types :

Les **capteurs d'image thermique non refroidis** fonctionnent à la température ambiante ou une température proche de celle-ci, à 8–14 μm dans la plage infrarouge à ondes longues. Les capteurs non refroidis sont souvent basés sur la technologie du microbolomètre et sont plus petits et moins chers que les capteurs d'image refroidis.

Les **capteurs d'image thermique refroidis** sont généralement contenus dans un boîtier scellé sous vide et refroidis à des températures allant jusqu'à $-210\text{ }^{\circ}\text{C}$ ($-346\text{ }^{\circ}\text{F}$) pour réduire le bruit créé par leur propre rayonnement thermique à des températures plus élevées. Cela permet aux capteurs de

fonctionner dans la bande infrarouge à ondes moyennes, d'environ 3 à 5 μm , qui offre une meilleure résolution spatiale et un contraste thermique plus élevé, car ces capteurs peuvent distinguer des différences de température plus petites et produire des images nettes et de haute résolution. Malheureusement, ces détecteurs sont volumineux, coûteux, énergivores et les refroidisseurs doivent être reconstruits toutes les 8 000 à 10 000 heures.



Spectre des rayonnements électromagnétiques. Les caméras thermiques Axis fonctionnent dans la plage LWIR (infrarouge à ondes longues) (7) à environ 8 à 14 μm .

1. Rayons X
2. Lumière ultraviolette
3. Lumière visible
4. Rayonnement infrarouge proche (NIR) (entre 0,75 et 1,4 μm environ)
5. Rayonnement infrarouge à longueur d'onde courte (SWIR) (entre 1,4 et 3 μm)
6. Rayonnement infrarouge à longueur d'onde moyenne (MWIR) (entre 3 et 5 μm)
7. Rayonnement infrarouge à grande longueur d'onde (LWIR) (entre 8 et 14 μm) – utilisé par les caméras thermiques Axis
8. Rayonnement infrarouge lointain (FIR), entre 15 et 1000 μm environ
9. Rayonnement micro-ondes
10. Ondes radio/TV
11. Éclairage IR
12. Caméras thermiques Axis

La capacité d'un capteur thermique à détecter de très petites différences de rayonnement thermique peut être caractérisée par sa valeur NETD (Noise Equivalent Temperature Difference). En règle générale, plus le NETD est petit, plus le capteur est performant. Cependant, il vaut mieux ne pas se représenter les performances d'une caméra thermique uniquement par sa valeur NETD, car il n'existe pas de protocole de mesure normalisé.

Les produits et technologies qui peuvent être utilisés à des fins militaires et commerciales sont appelés biens à double usage. Les exportations de ces biens sont réglementées dans le cadre de l'Arrangement international de Wassenaar de 1996, qui vise, entre autres, à promouvoir la transparence et une responsabilité accrue dans les transferts d'armes conventionnelles, ainsi que

des biens et technologies à double usage. Pour qu'une caméra thermique puisse être exportée librement, sa fréquence d'image maximale ne doit pas dépasser 9 images par seconde (ips). Les caméras thermiques dont la fréquence d'image va jusqu'à 60 ips peuvent être vendues dans la plupart des 42 pays membres de l'Arrangement de Wassenaar, à condition que l'acheteur soit enregistré et puisse être tracé et que le vendeur réponde à toutes les exigences en matière d'exportation propres à chaque pays, y compris les licences ou les exceptions de licence. Les caméras thermiques ne peuvent jamais être vendues à un pays sous embargo ou faisant l'objet de sanctions.

2.4.7 Caméras avec boîtiers antidéflagrants



Caméras avec boîtiers antidéflagrants.

Photos de gauche et du milieu : caméras fixes et PTZ conçues et certifiées pour les zones/divisions de type 1 (zones dangereuses).

Droite : caméra fixe conçue et certifiée pour les zones/divisions de type 2, moins potentiellement combustibles, situées dans des lieux dangereux.

Les caméras avec boîtier antidéflagrant sont idéales pour les applications de santé et de sécurité et pour gagner en efficacité opérationnelle. Elles permettent de surveiller vos opérations et processus critiques avec la vérification visuelle à distance des jauges et capteurs implantés sur vos sites. Elles permettent aussi de renforcer l'efficacité, de maintenir un niveau d'opérabilité maximale et d'optimiser le temps de disponibilité. Les caméras utilisées dans les endroits dangereux peuvent être intégrées à un système de capteurs et de caméras de zone de sécurité déjà en place sur un réseau existant. Les caméras thermométriques peuvent surveiller les surchauffes potentielles de l'équipement, ce qui permet de prendre des décisions informées sur le processus en cours, afin d'assurer le bon fonctionnement de la production et d'être aussi efficace que possible.

Grâce aux caméras avec boîtier antidéflagrant, vous pouvez améliorer la sécurité des employés et réduire l'exposition humaine inutile dans les zones dangereuses. Vous pouvez utiliser des outils d'analyse qui contrôlent l'utilisation d'équipements de protection personnels, tels que des casques

rigides, ou qui détectent la présence de signes de fumée ou d'incendie dans des environnements potentiellement combustibles.



Les équipements avec boîtier antidéflagrant sont généralement utilisés dans les industries de transformation, les installations pétrolières et gazières, et la manutention et le stockage des grains. Mais des zones dangereuses sont toutefois présentes dans une large gamme de secteurs variés, notamment les usines chimiques et pharmaceutiques, les sites de mines, de traitement de l'eau et des déchets.

Les caméras réseau protégées contre les explosions offrent de nombreux avantages par rapport aux versions analogiques, dont l'intelligence intégrée, l'analyse, les possibilités d'enregistrement et de stockage, une qualité d'image supérieure et une technologie de caméra moderne et évolutive.

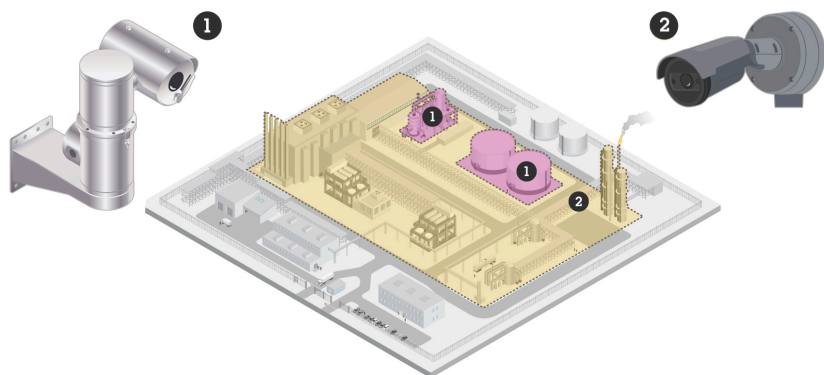
Lorsqu'un appareil électrique est installé dans un environnement potentiellement combustible, tel qu'une usine de traitement chimiques ou à proximité de vannes ou d'événements de gaz par exemple, il doit répondre à des normes de sécurité très spécifiques. Ce sont les environnements potentiellement combustibles qui doivent être protégés contre les sources d'ignition.

Conçues dans le respect des méthodes de protection contre les explosions, qui peuvent être, par exemple, le confinement ou la prévention, les caméras avec boîtier antidéflagrant sont certifiées pour une utilisation dans des endroits dangereux. L'utilisation d'un boîtier antidéflagrant **n'implique pas** que la caméra elle-même supporte une explosion externe.

- > **Confinement** : Ces caméras utilisent un boîtier robuste pour confiner l'énergie issue d'un éventuelle combustion interne. Une explosion provoquée par des étincelles ou des températures élevées dans ces caméras sera limitée à l'enceinte du boîtier et ne se propagera pas à l'atmosphère potentiellement inflammable à l'extérieur. Ce type de caméra avec boîtier antidéflagrant peut être certifié pour une utilisation dans les *zones/divisions dangereuses de type 1*, où la probabilité que l'atmosphère soit inflammable en raison de la concentration de vapeurs, de gaz, de poussières ou de fibres explosives est relativement élevée.
- > **Prévention** : Ces caméras sont conçues de telle sorte que l'énergie fournie n'est pas suffisante pour enflammer une atmosphère inflammable. Elles peuvent être certifiées pour une utilisation

dans les *zones/divisions dangereuses de type 2*, qui sont potentiellement moins combustibles dans un lieu dangereux.

Dans les endroits dangereux, les secteurs Zone/Division 2 sont généralement beaucoup plus grands que les secteurs Zone/Division 1. Les caméras certifiées pour les zones/divisions de type 1 peuvent également être utilisées dans les zones/divisions de type 2, mais les caméras dédiées et certifiées pour les zones/divisions de type 2 sont une alternative plus rentable dans ces zones.



La caméra adaptée au bon type de zone dangereuse.

1. Dans les zones/divisions de type 1, vous devez utiliser une caméra spécifiquement certifiée pour les zones/divisions de type 1.
2. Dans les zones étendues et potentiellement moins combustibles (zones/divisions de type 2) d'un site dangereux, il est également possible d'utiliser une caméra beaucoup plus légère et économique certifiée pour les zones/divisions de type 2.

Les caméras avec boîtier antidéflagrant doivent être certifiées selon les normes industrielles applicables dans le pays où elle doivent être utilisées.

3. Paramètres d'une caméra

La qualité de l'image et le champ de vision sont probablement les aspects les plus importants de la caméra. Ils sont affectés par divers éléments de la caméra, notamment la sensibilité à la lumière, l'objectif utilisé, le capteur d'image, ainsi que les fonctionnalités de traitement d'image.

3.1 Sensibilité à la lumière

La sensibilité à la lumière d'une caméra, souvent spécifiée en lux, est le niveau d'éclairage le plus bas auquel la caméra produit une image acceptable. L'éclairage est le quotient du flux lumineux reçu par unité de surface. La sensibilité à la lumière dépend principalement de l'objectif et du capteur d'image, et plus la valeur lux spécifiée est faible, plus la sensibilité à la lumière de la caméra est élevée.

Éclairage (lux)	Condition d'éclairage
100,000	Plein soleil
10,000	Plein jour
500	Lumière intérieure d'un bureau
100	Salon familial
10	Bougie à une distance de 30 cm
0,1	Pleine lune avec ciel dégagé
0.01	Quartier de lune

tableau 3.1a Exemples de niveaux d'illumination dans différentes conditions d'éclairage.

De nombreuses scènes naturelles offrent un éclairage assez complexe, avec à la fois des ombres et des reflets qui donnent différentes lectures de lux dans différentes parties de la scène. Il faut donc

garder à l'esprit qu'une seule lecture de lux n'indique pas la condition de lumière pour la scène dans son ensemble.

De nombreux fabricants spécifient le niveau minimum d'éclairement nécessaire pour qu'une caméra réseau produise une image acceptable. Bien que ces spécifications soient utiles pour effectuer des comparaisons de sensibilité à la lumière entre les caméras produites par le même fabricant, il n'en est pas de même lors de la comparaison entre les caméras de différents fabricants. En effet, chaque fabricant utilise des méthodes de mesure différentes et n'a pas la même définition d'une image acceptable. Pour comparer correctement les performances de luminosité faible de deux caméras différentes, les caméras doivent être placées côte à côte et voir un objet en mouvement dans une luminosité faible.

Pour capturer des images de bonne qualité dans des conditions de faible luminosité ou la nuit, Axis propose une variété de solutions telles que des caméras avec fonctionnalité jour/nuit, ou des caméras jour/nuit avec la technologie Axis Lightfinder ou avec LED infrarouge (IR) intégrée. Les caméras avec fonctionnalité jour/nuit tirent parti de la lumière infrarouge proche pour produire des vidéos de qualité en noir et blanc, et les caméras jour/nuit activent la vidéo couleur dans des conditions de faible luminosité. Les éclairages infrarouges externes améliorent la qualité de la vidéo en noir et blanc dans des conditions de lumière faible ou dans l'obscurité complète. Les caméras thermiques qui utilisent le rayonnement infrarouge (à des longueurs d'onde plus grandes que la lumière visible) émanant d'objets sont les outils les plus fiables pour détecter les incidents, 24h/24 et 7j/7.

Pour plus d'informations sur la technologie Axis Lightfinder, les caméras avec voyants infrarouges intégrés et les caméras thermiques, voir le chapitre . Pour plus d'informations sur la fonctionnalité jour/nuit et les éclairages, voir la section .

3.2 Objectifs

Un objectif sur une caméra remplit plusieurs fonctions.

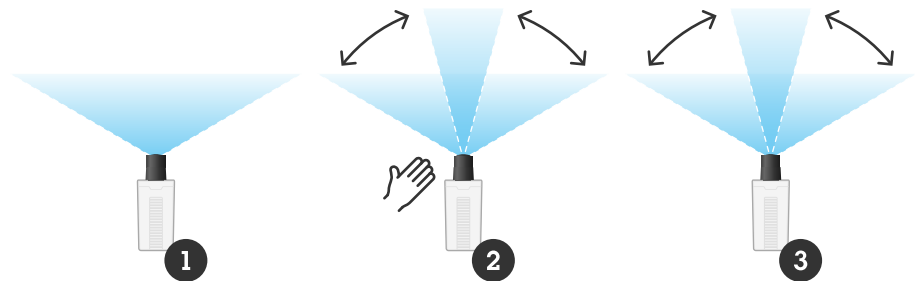
- > Il définit le champ de vision, qui détermine la quantité de scène qui peut être vue dans l'image.
- > Il préserve les détails de la scène en faisant correspondre la résolution de l'objectif à la résolution du capteur.
- > Il contrôle la quantité de lumière atteignant le capteur d'image de sorte que l'image soit correctement exposée.
- > Il effectue une mise au point de l'image en ajustant soit les éléments intérieur de l'objectif lui-même ou en modifiant la distance entre l'objectif et le capteur d'image.

L'objectif est l'œil de la caméra et ses capacités et fonctionnalités sont donc très importantes. Le champ de vision, la résolution, la sensibilité à la lumière et la profondeur de champ doivent être soigneusement pris en compte et correspondre à vos besoins lors du choix de la caméra.

3.2.1 Types d'objectifs

Selon l'utilisation, il existe différents types d'objectifs :

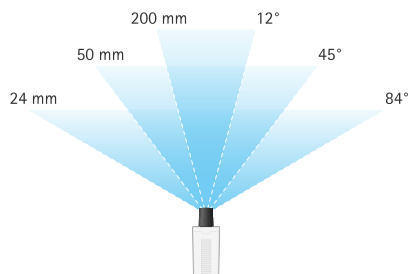
- > **Objectifs fixes de distance focale.** Également appelé objectif fixe. La distance focale est fixe et offre un seul champ de vision.
- > **Objectif à focale variable.** Offre une distance focale variable et donc différents champs de vision. Le champ de vision peut être réglé sur l'objectif ou via l'interface Web de la caméra. Le réglage de la distance focale dans un objectif à focale variable nécessite également une mise au point de l'objectif.
- > **Objectif à zoom.** Il s'agit d'un objectif de type focale variable qui offre un champ de vision réglable, mais ici, il n'est pas nécessaire de resserrer la mise au point si le champ de vision est modifié. La mise au point est conservée lors du changement de la distance focale. Ce type d'objectif est peu courant dans le secteur de la sécurité, mais la fonction peut être imitée par des objectifs motorisés.



Caméra avec objectif fixe (1), objectif à focale variable (2) et objectif zoom (3).

3.2.2 Champ de vision

Le champ de vision décrit l'angle que la caméra peut capturer. Il est déterminé par la distance focale de l'objectif et la taille du capteur d'image. Plus la distance focale est grande, plus le champ de vision est étroit. Le champ de vision est parfois étiqueté HFoV, VFoV ou DFoV, qui représentent le champ de vision horizontal, vertical ou diagonal.



Une distance focale plus importante (en mm) offre un champ de vision plus étroit (en degrés). Un objectif peut être classé dans l'une des trois catégories ci-après, selon les angles que l'objectif peut reproduire.

- > **Objectif grand angle.** Donne un champ de vision beaucoup plus large que ce qui est normal pour l'œil humain. Fournit généralement une grande profondeur de champ.
- > **Objectif à vue normale.** Offre un champ de vision similaire au champ de vision central de l'œil humain.
- > **Téléobjectif.** Donne un champ de vision plus étroit et fournit un effet d'agrandissement par rapport à la vision humaine. Peut parfois entraîner une petite profondeur de champ.



1



2



3



Champ de vision avec objectif grand angle (1), objectif de vue normale (2) et téléobjectif (3).

Le meilleur moyen de trouver la distance focale requise pour un champ de vision spécifique est d'utiliser les outils Axis en ligne *Calculateur d'objectif* ou *Sélecteur de produit*, tous deux disponibles à l'adresse www.axis.com/tools.

3.2.3 Chiffre F et exposition

La capacité de collecte de lumière d'une caméra est spécifiée par la valeur f de l'objectif. La valeur f définit la quantité de lumière qui peut traverser l'objectif et atteindre le capteur d'image. Il s'agit du rapport entre la distance focale de l'objectif et le diamètre de la pupille d'entrée de l'objectif.

Plus la valeur f est petite, meilleure est la capacité de collecte de lumière, c'est-à-dire plus la lumière peut passer au capteur d'image. Dans les situations de faible luminosité, une valeur f faible fournit généralement une image de meilleure qualité alors qu'une valeur f élevée augmente la profondeur de champ. Un objectif avec une valeur f faible est généralement plus cher qu'un objectif avec une valeur f élevée.

Dans certains objectifs, la taille de l'ouverture peut être modifiée. Pour ce faire, le diaphragme peut être manuel ou contrôlé par la caméra. Avec un objectif à focale variable ou un objectif zoom, la valeur f change lorsque la distance focale est modifiée. Plus la distance focale est longue, plus la valeur f est élevée. La valeur f imprimée sur l'objectif est normalement valide uniquement pour le réglage large.



La capacité de collecte de lumière d'une caméra est plus élevée lorsque la valeur f est plus faible.

3.2.4 Types de diaphragme

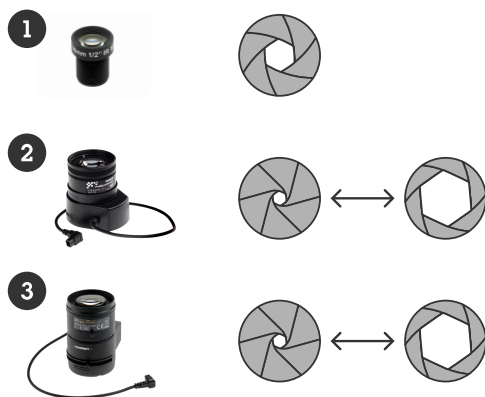
Le diaphragme d'un objectif fonctionne de la même façon que l'iris de l'œil humain. Il contrôle la quantité de lumière qui traverse de sorte que l'image de la caméra soit correctement exposée. Il peut également être utilisé pour optimiser différents aspects de la qualité d'image, tels que la résolution, le contraste et la profondeur de champ.

Trois types de diaphragme sont couramment utilisés dans le secteur de la sécurité :

- > Dans un objectif à **diaphragme fixe**, la taille de l'ouverture du diaphragme ne peut pas être modifiée. Ce diaphragme est utilisé par l'objectif M12 (monture S). Les objectifs avec ce type

de diaphragme sont principalement utilisés dans les environnements à niveaux de lumière contrôlés, généralement en intérieur.

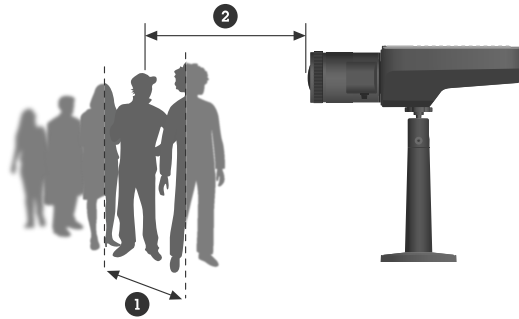
- > Avec un objectif à **diaphragme DC**, la caméra peut automatiquement modifier la taille de l'ouverture du diaphragme en fonction du niveau d'éclairage et ainsi contrôler la quantité de lumière qui atteint le capteur d'image. Les objectifs avec ce type de diaphragme peuvent être utilisés dans des environnements avec des conditions d'éclairage plus difficiles, généralement en extérieur.
- > Avec un objectif **P-Iris**, la caméra peut contrôler la taille de l'ouverture du diaphragme beaucoup plus précisément qu'un objectif à diaphragme DC. La caméra peut non seulement optimiser la quantité de lumière qui atteint le capteur d'image, mais également s'ajuster pour une meilleure netteté, un meilleur contraste et une profondeur de champ plus adaptée.



Types d'iris courants dans le secteur de la sécurité : fixe (1), diaphragme DC (2), P-Iris (3).

3.2.5 Profondeur de champ

La profondeur de champ fait référence à la distance entre les objets les plus proches et les plus éloignés qui apparaissent nets simultanément. Cette constante est importante dans les applications telles que la surveillance d'un parking, où vous devrez peut-être lire les plaques d'immatriculation à des distances de 20, 30 et 50 mètres (60, 90 et 150 pieds).



Cette illustration marque la profondeur de champ (1) et la distance focale (2), c'est-à-dire la distance entre la caméra et son point focal. Avec une plus grande profondeur de champ, les objets apparaissent nets à une plus longue portée autour du point focal.

La profondeur de champ est influencée par quatre facteurs : la distance focale, la valeur f , la distance entre la caméra et le sujet et la façon dont l'image est visionnée. La façon dont l'image est vue concerne des aspects tels que la taille des pixels, la distance entre le moniteur et l'observateur, la vue de l'observateur, etc.

Une distance focale plus longue, une valeur f inférieure, une distance plus courte entre la caméra et le sujet et une distance plus courte entre le moniteur et l'observateur diminuent tous la profondeur de champ.



*À gauche : photo avec une petite profondeur de champ – seuls les stylos au premier plan sont nets.
À droite : photo avec une plus grande profondeur de champ – tous les stylos sont d'une netteté acceptable.*

3.2.6 Adaptation de l'objectif et du capteur

Lors de l'échange d'objectifs, il est important d'assortir le nouvel objectif au capteur d'image de la caméra. Si l'objectif est destiné à un capteur plus petit que celui de la caméra, les angles de l'image

seront noircis. Si l'objectif est destiné à un capteur plus grand que celui de la caméra, le champ de vision sera plus petit que la capacité de l'objectif, car une partie des informations en dehors du capteur d'image seront perdues. Cette situation crée un effet de téléobjectif et l'image paraît zoomée.



Effet des différents objectifs sur un capteur 1/1,8". À droite : un objectif de 1/2,7" est trop petit pour le capteur et l'image comporte des angles noirs. Au centre : un objectif de 1/1,8" correspond à la taille du capteur. À gauche : un objectif de 1/1,2" est trop grand pour le capteur et les informations en dehors du capteur d'image seront perdues.

Les pages produit de l'objectif sur axis.com fournissent généralement des informations sur les tailles de capteurs pris en charge et les caméras compatibles avec chaque objectif.

3.2.7 Types d'objectifs de surveillance

	Un objectif bloc utilise des moteurs pour régler la mise au point et le zoom à distance tout en offrant quelques possibilités pour une qualité d'image optimisée. Il est couramment utilisé pour les caméras PTZ, dômes et caméras cylindriques. Ce type d'objectif est intégré à la caméra et ne peut pas être échangé.
	Généralement, un objectif M12 a une distance focale fixe et n'a pas de contrôle du diaphragme. De par son petit format, il est utilisé dans les caméras modulaires, certaines caméras dômes, les caméras-piétons et les interphones. Dans certaines caméras, cet objectif est échangeable. Cet objectif est également connu sous le nom d'objectif à monture S.



Un objectif C/CS a un filetage de montage spécifique, qui facilite l'échange de l'objectif. Ce type d'objectif est utilisé dans les caméras à boîtier. Il existe dans une grande variété de longueurs de varifocale avec contrôle CC ou P-Iris. Cet objectif offre une grande flexibilité et convient à diverses applications de surveillance.



Un objectif i-CS a le même filetage qu'un objectif C/CS, mais avec une intelligence supplémentaire grâce à ses moteurs intégrés pour ajuster le zoom et la mise au point à distance. Il offre des avantages similaires à l'objectif bloc, mais il est échangeable. Il est compatible avec les caméras à boîtier compatibles i-CS.

3.2.8 Mise au point

La mise au point d'une caméra réseau nécessite souvent des réglages fins de l'objectif. Avec les objectifs à diaphragme automatique moins sophistiqués, il est préférable d'ajuster la mise au point dans des conditions de faible luminosité ou en utilisant un filtre assombrissant tel qu'un filtre de densité neutre. Dans des conditions de faible luminosité, le diaphragme s'ouvre automatiquement, ce qui réduit la profondeur de champ et aide l'utilisateur à effectuer une mise au point plus précise.

Mise au point automatique

La mise au point automatique permet à la caméra d'ajuster automatiquement l'objectif de manière mécanique afin que l'image soit mise au point. La fonction de mise au point automatique est incontournable dans les caméras panoramiques où la direction de la caméra change constamment. Certaines caméras fixes ont également l'autofocus, mais puisque la mise au point d'une caméra fixe n'est normalement nécessaire qu'à l'installation, il est difficile de justifier le coût supplémentaire.

Certaines caméras intègrent des fonctions de mise au point à distance, éliminant ainsi le besoin d'un réglage manuel sur site. Le logiciel donne des retours en direct pour que l'utilisateur voit que l'objectif est correct. Avec un compteur de pixels intégré, il est également possible de s'assurer d'obtenir suffisamment de pixels sur le sujet pour pouvoir l'identifier, qu'il s'agisse du visage d'une personne ou d'une plaque d'immatriculation.

La fonction de mise au point automatique ne nécessite ni réglage, ni programmation pour fonctionner. Dans les caméras PTZ Axis, elle est activée par défaut et commence à fonctionner dès que la caméra est allumée.

Dans les scènes avec une luminosité ou un contraste faible, ou dont le niveau de bruit est élevé, la mise au point automatique peut prendre un certain temps pour être effectuée, et parfois même se

mettre au point sur le mauvais objet. Lorsque la scène change, la netteté peut être perdue pendant un moment, jusqu'à ce que la fonction de mise au point automatique la retrouve. Cela peut donner l'impression que la mise au point de la caméra est constamment en action.

Rappel de mise au point

Une zone de rappel de mise au point est un moyen rapide et simple de retrouver immédiatement une image nette dans la vue souhaitée. Contrairement au rappel de mise au point, la mise au point automatique règle la netteté à chaque changement de scène. Pour sa part, le rappel de mise au point mémorise une zone dont la mise au point est fixe, évitant ainsi les réglages répétés.

La zone de rappel de mise au point est définie en cliquant sur le bouton de rappel de mise au point dans l'interface utilisateur de la caméra lorsque la vue a la mise au point souhaitée. La caméra sauvegarde le réglage de sa mise au point. Le rappel de mise au point est alors activé dès que l'utilisateur effectue un panoramique ou une inclinaison dans la zone de rappel de mise au point à l'aide du joystick, et la caméra effectue automatiquement la mise au point en utilisant le réglage enregistré.

Mise au point laser

Certaines conditions d'éclairage peuvent constituer un défi pour la fonction autofocus. Il peut être difficile de trouver la mise au point dans les scènes à faible luminosité ou contraste, et dans les scènes avec des réflexions ou des sources lumineuses ponctuelles.

La fonction de mise au point laser permet de faire la mise au point sur des objets brillants et qui reflètent beaucoup de lumière, par exemple des vitres de fenêtres. La mise au point automatique peut s'avérer difficile car la lumière réfléchie brouille ou masque les bords nets que l'autofocus doit pouvoir mettre au point. Avec des objets en mouvement et des scènes qui changent rapidement, la mise au point laser agit immédiatement, ce qui permet de faire la mise au point sur la plaque d'immatriculation d'un véhicule en mouvement, par exemple.



Mise au point laser focalisée sur une plaque d'immatriculation dans des conditions de faible luminosité avec des sources lumineuses ponctuelles

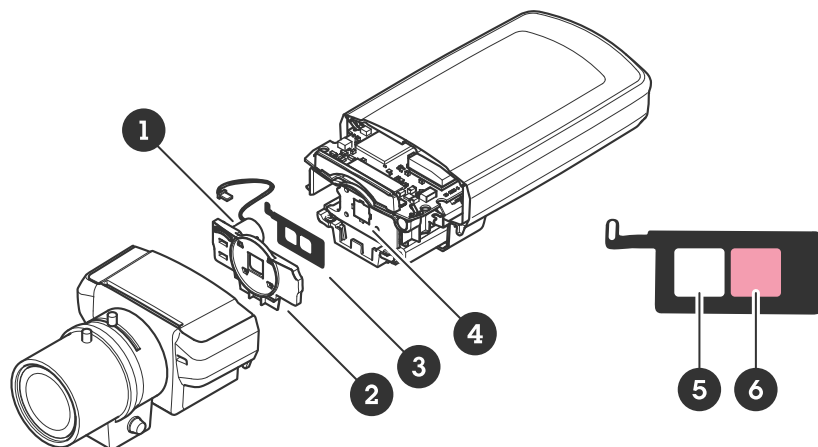
La mise au point laser est particulièrement utile pour les caméras PTZ, car la vue change de manière dynamique lorsque la fonction PTZ est utilisée.

3.2.9 Précision PTRZ

La fonction PTRZ à distance (panoramique-inclinaison-roulement-zoom) est une fonction qui permet d'ajuster la vue de la caméra à distance, sans interrompre l'enregistrement. La caméra peut pivoter autour de ses axes verticaux (de haut en bas), latéraux (d'un côté à l'autre) et longitudinaux (d'avant en arrière), et changer également sa distance focale pour obtenir un champ de vision plus étroit (zoom avant) ou plus large (zoom arrière).

3.3 Filtre infrarouge amovible (fonctionnalité jour / nuit)

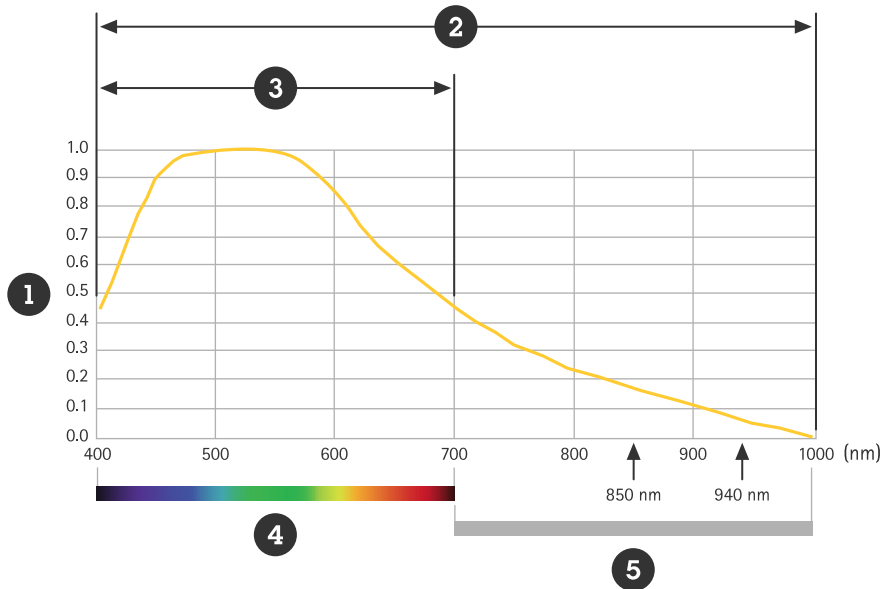
De nombreuses caméras possèdent un filtre infrarouge à retrait automatique entre l'objectif et le capteur d'image. Ce filtre bloque la lumière infrarouge (IR), pour permettre à la caméra de produire les couleurs perceptibles par l'œil humain. Cependant, lorsque le filtre est retiré par luminosité faible ou la nuit, le capteur de la caméra peut alors tirer parti de la lumière ambiante proche infrarouge (NIR) et est capable de fournir des images en noir et blanc dans des scènes où la lumière visible est insuffisante.



Filtre infrarouge (jour/nuit) sur support optique qui, dans cette caméra, glisse latéralement. Le filtre rouge est utilisé pendant la journée et la partie transparente pendant la nuit.

1. Solénoïde
2. Cache avant
3. Support optique
4. Capteur d'image
5. Filtre nocturne
6. Filtre diurne

L'œil humain ne peut pas voir la lumière proche infrarouge, qui se trouve dans la plage approximative de 700 à 1000 nanomètres (nm), mais la plupart des capteurs de la caméra peuvent la détecter et l'utiliser.



Le graphique montre la manière dont un capteur d'images répond à la lumière visible et à la lumière infrarouge proche.

1. Sensibilité relative du capteur
2. Longueurs d'onde utilisées en mode nocturne
3. Longueurs d'onde utilisées en mode jour
4. Lumière visible
5. Lumière infrarouge proche

Les caméras dotées d'un filtre infrarouge à retrait automatique disposent d'une fonctionnalité jour / nuit, car elles diffusent des vidéos couleur pendant la journée et des vidéos en noir et blanc pendant la nuit. Elles sont utiles dans les situations de luminosité faible, de surveillance cachée et dans des environnements qui restreignent l'utilisation de la lumière artificielle.

Les projecteurs infrarouges qui fournissent une lumière proche infrarouge peuvent être utilisés avec des caméras jour / nuit pour améliorer davantage la capacité de la caméra à produire des vidéos de haute qualité dans des conditions de luminosité faible ou dans l'obscurité totale. Certaines caméras jour/nuit disposent d'un éclairage IR intégré utilisant des LED IR. L'éclairage IR fournit normalement une lumière IR d'une longueur d'onde de 850 nm ou 940 nm.



Illuminateurs infrarouges externes et caméra avec illuminateurs infrarouges intégrés.

Les voyants infrarouges intégrés aux caméras Axis peuvent être ajustés pour correspondre à l'angle de vue et activés automatiquement dans l'obscurité, sur événement ou sur demande des utilisateurs. Les caméras Axis avec voyants DEL IR intégrés simplifient l'installation et constituent une option économique par rapport à l'utilisation d'éclairages infrarouges externes. Des éclairages externes, d'autre part, permettent aux installateurs de choisir librement le modèle qui leur convient, comme un modèle longue portée. Ils peuvent placer la lumière là où elle est nécessaire, pas nécessairement au même endroit que la caméra.

3.4 Capteurs d'image

Le capteur d'image constitue un élément clé de toute caméra numérique. Le capteur d'image enregistre la lumière qui passe à travers l'objectif depuis toutes les parties de la scène et la convertit en signaux électriques. Ces signaux fournissent les informations nécessaires à la caméra pour reproduire une image numérique de la scène, après une amplification et un traitement supplémentaires.

Le capteur d'image de la caméra est composé de millions de détecteurs optiques (diodes photosensibles), communément appelés pixels. Chaque pixel capture la lumière (photons) pendant une période de temps définie, qui est le temps d'exposition de la caméra, ou l'intervalle d'exposition. Après cet intervalle de temps, le pixel est lu et sa charge est mesurée. Un nouvel intervalle d'exposition commence et le pixel peut capturer de nouveaux photons.

La qualité des capteurs a été améliorée de manière spectaculaire. Les capteurs mégapixels, HDTV et 4K sont largement disponibles. Mais même si l'industrie de la surveillance ne cesse d'évoluer vers des résolutions plus élevées, les fabricants ont cherché à conserver une taille de capteur identique dans le but d'éviter l'augmentation du coût d'un capteur plus grand. Autrement dit, ils doivent intégrer plus de détecteurs optiques dans la même zone de capteur, ce qui rend chaque pixel plus petit et capable de capturer une quantité de lumière moindre. La charge après chaque intervalle d'exposition sera par conséquent plus faible et le signal électrique de chaque pixel exigera davantage d'amplification, avec un bruit plus présent.

Il suffit donc d'augmenter le nombre de pixels dans un capteur de même taille pour obtenir une meilleure résolution, mais vous pourrez également obtenir des images de qualité moindre. Cela s'avère particulièrement vrai dans les scènes à faible luminosité, pour lesquelles le bruit de l'image a tendance à être plus perturbant. Si vous augmentez plutôt la taille du capteur, chaque détecteur optique peut capturer davantage de photons et générer un signal plus intense avec moins de bruit.

Axis propose des caméras avec des tailles de capteurs variées, dont plusieurs alliant une résolution 4K avec un grand capteur. Avec des pixels plus de quatre fois plus gros que ceux de la plupart des autres caméras 4K, ces caméras dotées de grands capteurs réalisent naturellement des images claires et nettes en haute résolution, même dans des conditions de faible luminosité.

3.5 Contrôle d'exposition

Les deux principaux éléments qui contrôlent la quantité de lumière reçu par un capteur d'image sont la capacité de l'objectif à collecter la lumière (valeur *f*) et le temps d'exposition. Le troisième élément, le gain, est un amplificateur de niveau d'image qui est utilisé pour rendre l'image plus lumineuse. Cependant, l'augmentation du gain augmente également le niveau de bruit (granulation) d'une image, c'est pourquoi le réglage du temps d'exposition ou de l'ouverture du diaphragme est préférable.

Le temps d'exposition aura toujours un effet sur les images, et les réglages liés à l'exposition peuvent être modifiés de plusieurs façons. Les plus importants, la priorité d'exposition, les zones d'exposition, le WDR et la plage dynamique, ainsi que la compensation de contre-jour sont expliqués dans cette section.

3.5.1 Priorité de l'exposition

Les environnements lumineux nécessitent des expositions plus courtes. Les conditions de faible luminosité nécessitent des expositions plus longues afin que le capteur d'image puisse capter plus de lumière et ainsi améliorer la qualité de l'image. Cependant, l'augmentation du temps d'exposition augmente également le flou de mouvement et abaisse la fréquence d'images totale, car il faut plus de temps pour exposer chaque image.

Dans des conditions de faible luminosité, les caméras Axis permettent aux utilisateurs de donner la priorité à la qualité vidéo en termes de mouvement ou de niveau de bruit faible (grain). Pour un mouvement rapide ou lorsqu'une vitesse d'image élevée est requise, une exposition plus courte / une vitesse d'obturation plus rapide est recommandée, mais la qualité de l'image peut être réduite.

Lorsque le niveau de bruit est prioritaire, le gain (amplification) doit être maintenu aussi bas que possible pour améliorer la qualité de l'image, mais la fréquence d'images peut être réduite en

conséquence. N'oubliez pas que dans des conditions de luminosité faible, un faible gain peut entraîner une image très sombre. Une valeur de gain élevée permet d'afficher une scène sombre, mais avec un niveau de bruit accru.

3.5.2 Zones d'exposition

L'exposition automatique d'une caméra doit décider de la partie de l'image qui doit déterminer la valeur d'exposition. Dans de nombreuses caméras Axis, l'utilisateur peut également utiliser des zones d'exposition pour s'assurer que la partie la plus importante de la scène est exposée de manière optimale.

3.5.3 Compensation de contre-jour

Les caméras réseau avec compensation de contre-jour s'efforcent d'ignorer les zones limitées d'un éclairage élevé (généralement, le ciel), comme si elles n'étaient pas présentes. La compensation de contre-jour permet de voir les objets au premier plan, mais les zones lumineuses sont surexposées.



Fort contre-jour, sans compensation de contre-jour (à gauche). Avec la compensation de contre-jour, le premier plan est plus visible (à droite).

3.5.4 Plage dynamique

En termes de lumière, la plage dynamique est le rapport entre les valeurs d'éclairement les plus élevées et les plus faibles dans une image. De nombreuses scènes ont une plage dynamique élevée, avec des zones très lumineuses et très sombres. Il s'agit d'un problème pour les caméras standard, qui ne peuvent gérer qu'une plage dynamique limitée. Dans ces scènes, ou dans des situations de contre-jour où une personne placée devant une fenêtre lumineuse, une caméra standard produira une image dans laquelle les objets se trouvant dans les zones sombres seront difficilement visibles. Diverses techniques peuvent être appliquées pour augmenter la capacité de plage dynamique d'une caméra et permettre la visualisation d'objets se trouvant dans les zones sombres et claires.

L'exposition peut être contrôlée et la cartographie de tonalité peut être utilisée pour augmenter le gain dans les zones sombres.



Deux images de la même scène. L'image à droite gère mieux la gamme dynamique de la scène, et les détails sont aussi bien visibles dans les zones claires que sombres.

3.5.5 Imagerie WDR

L'imagerie à plage dynamique étendue (WDR) permet de recréer la plage dynamique complète d'une scène WDR dans une seule image. Par exemple, la scène du garage de stationnement ci-dessous. Une caméra conventionnelle ne peut pas capturer toute sa gamme dynamique, et la visibilité doit être sacrifiée dans les zones sombres ou lumineuses.



Garage de stationnement avec des conditions lumineuses difficiles. À gauche, l'image est surexposée. À droite, l'image est sous-exposée.

Avec une caméra WDR, toutes les zones peuvent être rendues visibles dans une seule image.



Parking couvert avec des conditions lumineuses difficiles, capturé par une caméra de surveillance WDR.

Axis propose plusieurs solutions pour l'imagerie WDR :

- > **Forensic WDR** associe une méthode de double exposition et une méthode locale d'amélioration du contraste. Cette fonction produit des images optimisées pour un usage à des fins d'enquête. Cette technologie, basée sur la dernière génération d'algorithmes de traitement d'image, réduit efficacement le niveau de bruit et les anomalies. Forensic WDR convient également pour les scènes comportant du mouvement et les caméras à ultra-haute résolution.
- > **WDR – forensic capture** combine la double exposition et une méthode d'amélioration locale du contraste. Cette fonction produit des images optimisées pour un usage à des fins d'enquête.
- > **WDR – dynamic capture** applique une méthode de double exposition, qui fusionne les images capturées à des temps d'exposition différents. La plage dynamique est limitée par des anomalies visuelles, par exemple celles liées aux mouvementx et aux scintillements dans la scène.
- > **WDR – Dynamic Contrast** utilise une méthode d'amélioration du contraste avec une gamme dynamique assez limitée mais avec très peu d'anomalies visuelles. Comme les images sont prises avec un temps d'exposition fixe, cette solution est à privilégier dans les scènes comportant beaucoup d'objets mobiles.

La capacité de plage dynamique d'une caméra est généralement spécifiée en dB. Cependant, les performances réelles du WDR ne sont pas faciles à mesurer, car elles dépendent de nombreux facteurs comme la complexité de la scène, les mouvements de la scène et la capacité de traitement de l'image de la caméra. Pour Axis, ce qui compte c'est de donner la priorité aux enquêtes judiciaires et à une qualité d'image élevée plutôt qu'à une valeur dB élevée. Par conséquent, une caméra Axis dont la plage dynamique est définie par une valeur donnée peut très bien surpasser une caméra concurrente dont la valeur en dB est supérieure.

3.6 Alarme de détérioration

L'alarme de sabotage active alerte automatiquement l'opérateur lorsqu'une caméra est sabotée ou interrompue, ce qui permet au personnel de sécurité de détecter toute interruption du fonctionnement de la caméra. Cela s'avère particulièrement utile lorsqu'il y a des risques de vandalisme, comme dans les écoles, les prisons, les transports publics et dans les environnements difficiles où les conditions météorologiques, les vibrations ou la saleté peuvent affecter les performances de la caméra. L'alarme de sabotage active détecte les incidents tels que la redirection, le blocage ou la défocalisation des caméras, et se déclenche lorsque la caméra est sabotée, peinte à la bombe ou intentionnellement couverte.

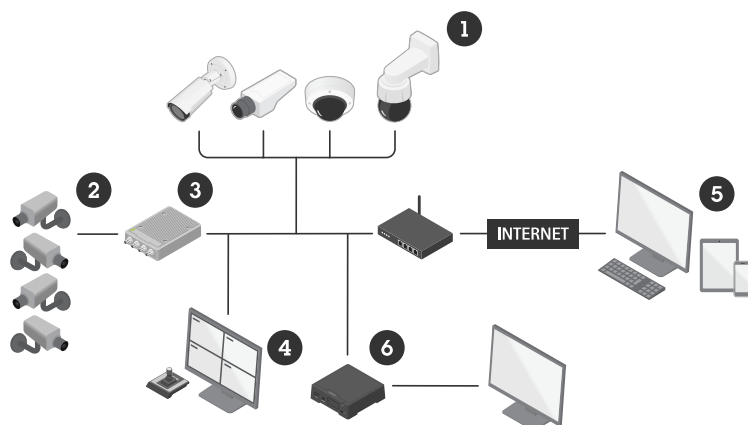
3.7 Détection sonore

La détection sonore peut être utilisée pour détecter des bruits, tels que des voix ou l'effraction d'une fenêtre, et déclencher la transmission et l'enregistrement de vidéos ou d'audio ou alerter les opérateurs en cas d'activités suspectes. La détection audio est un puissant complément à la vidéo, car elle peut détecter une activité dépassant le champ de vision de la caméra ou dans des zones trop sombres pour la détection de mouvement vidéo. Pour que la détection audio fonctionne, la caméra doit inclure une prise en charge de l'audio et être équipée d'un microphone intégré ou externe.

4. Encodeurs vidéo

Les encodeurs vidéo permettent d'intégrer un système de vidéosurveillance analogique existant à un système de vidéo sur IP. Les encodeurs vidéo jouent un rôle important dans les installations comportant de nombreuses caméras analogiques.

4.1 Qu'est-ce qu'un encodeur vidéo ?



Les encodeurs et les décodeurs vidéo peuvent être utilisés pour intégrer les caméras vidéo analogiques et les moniteurs de vidéo en direct dans un système de vidéo sur IP. Les caméras réseau (1) sont ici complétées par des caméras analogiques (2) et un encodeur vidéo (3). Le système est géré via un système de gestion vidéo (4) et accessible à distance depuis un ordinateur ou un périphérique mobile (5). Un décodeur (6) permet l'utilisation de moniteurs pour afficher une vidéo en direct sans ordinateur.

Les encodeurs vidéo permettent aux responsables de la sécurité de continuer à utiliser leurs caméras de vidéosurveillance analogiques tout en construisant un système de vidéosurveillance offrant les avantages de la vidéo sur IP. Si un encodeur vidéo est inclus dans le système, les caméras analogiques peuvent être contrôlées et accessibles via un réseau IP, tel qu'un réseau local ou Internet. Cela signifie également que les anciens appareils d'enregistrement vidéo tels que les enregistreurs vidéo numériques et les moniteurs peuvent être remplacés par des moniteurs d'ordinateur et des serveurs standard.

4.1.1 Composants d'encodeur vidéo et considérations

Les encodeurs vidéo Axis et les les caméras réseau offrent pratiquement les mêmes fonctions. Lors de la sélection d'un encodeur vidéo et la construction des systèmes professionnels, la fiabilité et la qualité sont les facteurs les plus importants. Il faut aussi tenir compte du nombre de canaux analogiques pris en charge, de la qualité d'image, des formats de compression, de la fréquence d'image et de la résolution. Certains encodeurs prennent en charge des caméras analogiques HD, ainsi que des caméras analogiques de résolution standard. Des fonctionnalités telles que la prise en charge PTZ, l'audio, la gestion d'événements, l'analyse, l'alimentation Power over Ethernet et les fonctionnalités de sécurité peuvent également être cruciales.

Si l'encodeur vidéo doit résister à des conditions telles que les vibrations, les chocs et les températures extrêmes, un modèle robuste ou un boîtier de protection doit être privilégié.



Encodeurs vidéo prenant en charge quatre canaux et 16 canaux.

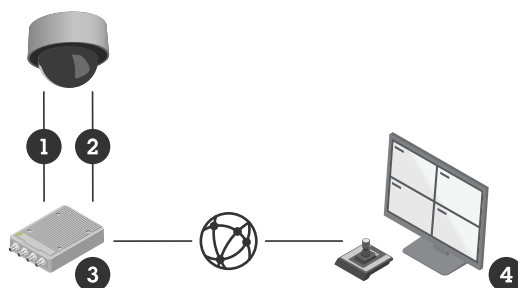
Grâce à un encodeur vidéo multicanaux, les signaux vidéo provenant des caméras distantes peuvent alors partager le même câblage réseau, réduisant ainsi les coûts liés au câblage. Si des investissements ont été réalisés dans des caméras analogiques mais que des câbles coaxiaux n'ont pas encore été installés, il est préférable d'utiliser et de positionner des encodeurs vidéo à proximité des caméras analogiques. Cela réduit les coûts d'installation en évitant de faire passer de nouveaux câbles coaxiaux vers un site central, car la vidéo peut être envoyée plutôt sur un réseau Ethernet.

4.1.2 Gestion des événements et analyse vidéo

Les encodeurs vidéo Axis ont pour principal avantage de pouvoir fournir la gestion d'événements et l'analyse, sachant que ces capacités ne peuvent pas être fournies par un système vidéo analogique. Des fonctions d'analyse intégrées telles que la détection de mouvement vidéo multi-fenêtres, la détection audio et l'alarme de sabotage active, ainsi que des ports d'entrée pour les capteurs externes, permettent au système de vidéosurveillance de rester constamment en alerte. Une fois qu'un événement est détecté, le système peut intervenir automatiquement en lançant diverses actions, comme l'enregistrement vidéo, l'envoi d'alertes par e-mail, l'activation des lumières, l'ouverture/la fermeture des portes et des alarmes sonores.

4.2 Encodeurs vidéo avec caméras PTZ analogiques

Dans un système de vidéo sur IP, les commandes PTZ d'un tableau de contrôle sont transmises sur le même réseau IP que la transmission vidéo, et sont transmises à la caméra PTZ analogique via le port série de l'encodeur vidéo (RS-422 / RS-485). Les encodeurs vidéo permettent ainsi de contrôler des caméras PTZ analogiques sur de longues distances, même sur Internet.



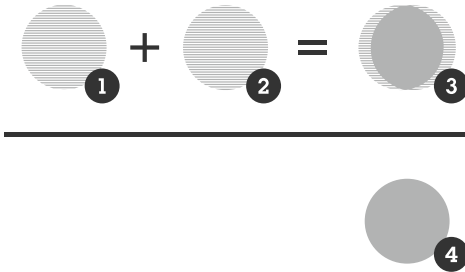
Une caméra à dôme analogique PTZ peut être commandée via le port série de l'encodeur vidéo (RS-485, par exemple), ce qui permet de la contrôler à distance sur un réseau IP.

1. Câble à paires torsadées RS-485
2. Câble coaxial
3. Encodeur vidéo
4. Poste de travail avec joystick

4.3 Techniques de désentrelacement

Les caméras analogiques utilisent le balayage entrelacé pour former une image. Cela signifie que deux champs de lignes sont générés : un champ affichant les lignes impaires et un second champ affichant les lignes paires. Lors de la transmission d'une image entrelacée, les lignes impaires et

paires de l'image sont transmises en alternance, ce qui réduit de moitié l'utilisation de la bande passante. Les caméras réseau utilisent plutôt le balayage progressif (progressive scan), dans lequel toutes les lignes de l'image sont capturées, transmises et affichées dans une seule image.



En haut : une image à balayage entrelacé, avec les lignes impaires et paires transmises en alternance, et son apparence sur un moniteur d'ordinateur. En bas : apparence d'une image à balayage progressif sur le même moniteur.

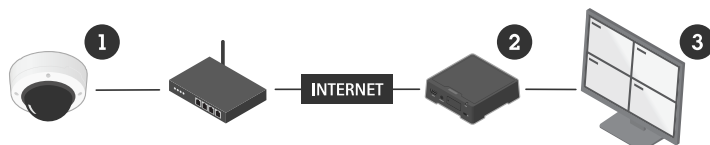
1. 1er champ : lignes impaires.
2. Second champ : lignes paires, 17/20 (NTSC/PAL) millisecondes plus tard.
3. Arrêt sur image sur un point en mouvement avec balayage entrelacé.
4. Arrêt sur image sur un point en mouvement avec balayage progressif.

La vidéo des caméras analogiques est conçue pour être visionnée sur des moniteurs analogiques tels que les téléviseurs traditionnels, qui utilisent le balayage entrelacé. Lorsque ce type de vidéo est affiché sur un écran d'ordinateur, qui utilise le balayage progressif, des effets d'entrelacement (un effet de peigne) provenant d'objets en mouvement peuvent être vus. Différentes techniques de désentrelacement peuvent être utilisées pour réduire les effets d'entrelacement indésirables. Dans les encodeurs vidéo Axis avancés, les utilisateurs peuvent choisir l'une des deux techniques de désentrelacement suivantes : l'interpolation adaptative ou le mixage.

L'interpolation adaptative offre la meilleure qualité d'image et implique l'utilisation d'un seul des deux champs consécutifs et de l'interpolation pour créer l'autre champ de lignes et former une image complète. Le mélange consiste à fusionner deux champs consécutifs et à les afficher comme une seule image, de sorte que tous les champs sont présents. L'image est ensuite filtrée afin d'éliminer les artéfacts de mouvement (ou l'effet peigne) dus à l'écart de temps dans la capture des deux trames. La technique de mélange n'est pas aussi gourmande que l'interpolation adaptative en termes de sollicitation du processeur.

4.4 Décodeurs vidéo

Les décodeurs vidéo Axis permettent aux moniteurs numériques de se connecter aux caméras Axis et de les afficher en direct. Il s'agit d'une solution économique de vidéosurveillance dans laquelle plusieurs flux vidéo en direct peuvent être affichés sur un moniteur de visionnage public ou un moniteur de sécurité sans recourir à une connexion via un PC.



Un décodeur vidéo (2) permet d'afficher une vidéo en direct depuis une caméra Axis (1) sur un moniteur (3) sans utiliser d'ordinateur.

5. Résolutions vidéo

Plus le capteur a de pixels, plus il peut capturer des détails plus fins et produire une image de meilleure qualité. Plusieurs nouvelles résolutions issues de l'industrie de l'informatique et de la télévision numérique ont été introduites sur le marché.

5.1 Résolutions mégapixels

Un capteur mégapixel produit une image qui contient des millions de pixels (un million ou plus). Les caméras mégapixels sont utilisées dans la surveillance où les détails sont essentiels, par exemple lorsque des personnes et des objets doivent être identifiés ou qu'une grande zone doit être surveillée.

Conformément aux meilleures pratiques de vidéosurveillance, une vue d'ensemble a besoin d'environ 70 à 100 pixels pour représenter 1 m (20 à 30 pixels par pied). Pour les situations qui nécessitent des images détaillées, telles que l'identification des personnes, vous pouvez avoir besoin jusqu'à 250 pixels par mètre (80 pixels par pied). Cela signifie que s'il est nécessaire d'identifier les personnes qui traversent une zone de 4 m de large et de 4 m de haut, la caméra doit être capable de fournir une résolution d'au moins 1 mégapixel (1000 × 1000 pixels). Pour plus de détails sur les densités de pixels recommandées, voir le chapitre .

5.2 Résolutions de télévision haute définition (TVHD)

Les deux normes HDTV les plus importantes sont SMPTE 296M, qui définit le format HDTV 720p et SMPTE 274M, qui définit le format HDTV 1080.

Une caméra conforme aux normes SMPTE indique le respect de la qualité TVHD et doit offrir tous les avantages de la HDTV en termes de résolution, de fidélité des couleurs et de fréquence d'images. La norme TVHD est basée sur des pixels carrés, semblables aux écrans d'ordinateur, de sorte que la vidéo TVHD des produits de vidéo sur IP peut être affichée sur des écrans TVHD ou des écrans d'ordinateur standard. Avec la vidéo TVHD à balayage progressif, aucune technique de conversion

ou de désentrelacement ne doit être appliquée lorsque la vidéo doit être traitée par un ordinateur ou affichée sur un écran d'ordinateur.

Taille	Format d'image	Balayage	Fréquence d'image (ips/Hz)	Étiquettes
1280 × 720	16:9	Progressive	50	720p50
1920 × 1080	16:9	Entrelacé	25 ^a	1080i50
1920 × 1080	16:9	Progressive	25	1080p25
1920 × 1080	16:9	Progressive	50	1080p50

tableau 5.2a *Tailles d'image TVHD de base dans l'Union européenne de radiodiffusion.* ^a Taux de champ de 50 Hz. Notez que d'autres fréquences d'images peuvent être utilisées. Les plus courantes sont 24, 25, 30, 50 et 60 ips.

Taille	Format d'image	Balayage	Fréquence d'image (ips/Hz)	Étiquettes
1280 × 720	16:9	Progressive	60	720p60
1920 × 1080	16:9	Entrelacé	30 ^a	1080i60
1920 × 1080	16:9	Progressive	30	1080p30
1920 × 1080	16:9	Progressive	60	1080p60

tableau 5.2b *Les tailles d'image HDTV de base dans les pays du Comité du système de télévision national.* ^a Taux de champ de 60 Hz. Notez que d'autres fréquences d'images peuvent être utilisées. Les plus courantes sont 24, 25, 30, 50 et 60 ips.

5.3 Résolutions Ultra-HD

Comme la TVHD, l'Ultra-HD est une norme qui garantit une certaine qualité vidéo, alors que le mégapixel sert simplement à faire état de la résolution de la caméra. La télévision Ultra-HD (TVUHD) a deux formats vidéo numériques :

- > Ultra-HD 2160p est communément appelé 4K, avec une résolution de 3840 x 2160 pixels donnant 8,3 mégapixels, quatre fois plus que HDTV 1080p.
- > Ultra-HD 4320p est communément appelé 8K, avec une résolution de 7680 x 4320 pixels donnant 33,2 mégapixels, seize fois plus que HDTV 1080p.

Les deux formats offrent une fidélité des couleurs très élevée, une numérisation progressive, jusqu'à 100/120 images par seconde et une compression H.265.

En vidéosurveillance, cette résolution inégalée Ultra-HD permet d'avoir des capacités de zoom numérique exceptionnelles et un champ de vision étendu. Les caméras Ultra-HD sont ainsi idéales pour capturer les traits du visage et d'autres détails. Néanmoins, l'Ultra-HD exige des objectifs de haute qualité, beaucoup de pixels et de grands capteurs capables de capter suffisamment de lumière, ainsi que des augmentations significatives de la bande passante et de la capacité de stockage. En d'autres termes, l'augmentation de la résolution peut se faire à des coûts très élevés.

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

Ultra-HD 4320p (8K) a 16 fois la résolution de HDTV 1080p. Ultra-HD 2160p (4K) a 4 fois la résolution de HDTV 1080p.

5.4 Rapports

Le rapport d'aspect est le rapport entre la largeur de l'image et sa hauteur. Un moniteur de télévision à l'ancienne, traditionnellement utilisé pour visionner des vidéosurveillance analogiques, affiche une image avec un rapport d'aspect de 4:3. La vidéo sur réseau peut offrir le même rapport mais aussi d'autres rapports tels que 16:9.

L'avantage d'un rapport d'aspect 16: 9 est que les détails sans importance habituellement situés dans les parties supérieure et inférieure de la scène ne font pas partie de l'image. Par conséquent, les besoins en bande passante et en stockage peuvent être réduits.

Le rapport d'aspect 9:16 est simplement une image 16:9 pivotée de 90°. Le rapport d'aspect 9:16 est très utilisé dans la vidéosurveillance, car la vue complète de la caméra peut être utilisée pour surveiller des scènes étroites comme les allées des magasins, les routes, les couloirs scolaires et les quais des gares. Ce rapport d'aspect est parfois appelé format de couloir.



Rapports d'aspect 4:3 et 16:9



Le format de couloir est souvent utilisé dans les environnements de vente au détail.

6. Compression vidéo

La plupart des fournisseurs de vidéo sur IP utilisent aujourd'hui des techniques de compression normalisées qui garantissent la compatibilité et l'interopérabilité. Les normes de l'industrie sont très utiles pour la surveillance vidéo car le matériel vidéo peut être utilisé à un grand nombre de fins différentes et, dans certains cas, doit être visionnable plusieurs années après la date d'enregistrement. Grâce à des technologies comme Axis Zipstream, un système de surveillance peut combiner l'utilisation de caméras haute résolution et des coûts système raisonnables, tout en préservant la valeur légale de la vidéo. En effet, les données inutiles sont supprimées, tout en maintenant les exigences de stockage au plus bas, tandis que les détails importants et les mouvements sont conservés.

6.1 Bases de compression

Les technologies de compression vidéo consistent à réduire et à supprimer les données vidéo redondantes afin que la vidéo numérique puisse être efficacement visualisée sur un réseau et stockée sur des disques d'ordinateur. Avec des techniques de compression efficaces, des réductions significatives de la taille du fichier peuvent être réalisées, entraînant peu ou pas d'effet négatif sur la qualité vidéo. Cependant, si le niveau de compression d'une technique de compression donnée est trop élevé, il peut avoir des effets négatifs sur la qualité.

6.1.1 Codec vidéo

Le processus de compression implique l'application d'un algorithme à la vidéo source pour créer un fichier compressé prêt à être transmis ou stocké. Pour lire le fichier compressé, un algorithme inverse est appliqué pour décompresser la vidéo et produire pratiquement le même contenu que la vidéo source d'origine. Le temps nécessaire pour compresser, envoyer, décompresser et afficher un fichier s'appelle la latence. Plus l'algorithme de compression est avancé, plus la latence est élevée. Une paire d'algorithmes qui fonctionnent ensemble s'appelle un codec vidéo (encodeur/décodeur).

Les codecs vidéo de différentes normes ne sont normalement pas compatibles entre eux ; autrement dit, le contenu vidéo compressé à l'aide d'une norme ne peut pas être décompressé avec

une autre norme. Par exemple, un décodeur H.264 ne fonctionnera pas avec un encodeur H.265. En effet, un algorithme ne peut pas décoder correctement la vidéo d'un autre algorithme, mais il est possible d'implémenter de nombreux algorithmes différents dans le même logiciel ou matériel, afin de permettre à plusieurs formats de coexister.

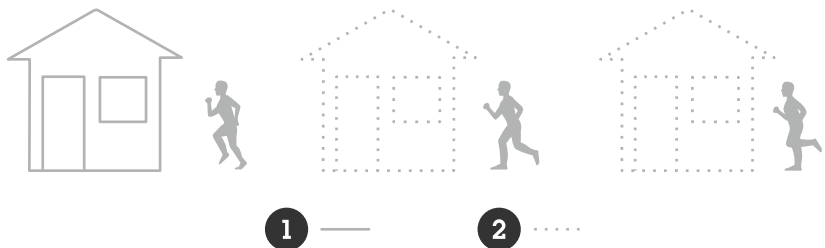
6.1.2 Différence entre compression d'image et compression vidéo

Chaque norme de compression utilise des méthodes différentes pour réduire les données. Par conséquent, les résultats diffèrent en termes de débit, de qualité et de latence. Les algorithmes de compression se divisent en deux types : la compression d'images et la compression vidéo. La compression d'image utilise la technologie de codage « intraframe ». Les données sont réduites dans une trame d'image en supprimant simplement les informations inutiles qui pourraient ne pas être perçus par l'œil humain. Motion JPEG est l'une des ces normes de compression. Les images d'une séquence Motion JPEG sont codées ou compressées en tant qu'images JPEG individuelles.



Dans le format Motion JPEG, les trois images de la séquence ci-dessus sont codées et envoyées en tant qu'images uniques distinctes, sans dépendance vis-à-vis de l'une ou de l'autre.

Les algorithmes de compression vidéo tels que H.264, H.265 et AV1 utilisent la prédiction intertrame pour réduire les données vidéo sur une série de trames. Des techniques spécifiques sont ainsi utilisées, telles que l'encodage différentiel, où une trame est comparée à une trame de référence envoyée plus tôt et seuls les pixels qui ont changé par rapport à la trame de référence sont codés. De cette manière, la valeur de pixel codée et envoyée est réduite. Lorsque cette séquence codée est affichée, les images apparaissent comme dans la séquence vidéo d'origine.



Avec l'encodage différentiel, seule la première image (trame I) est codée dans son intégralité. Dans les deux images suivantes (trames P), des références sont faites dans la première image pour les éléments statiques, c'est-à-dire la maison. Seules les parties mobiles, c'est-à-dire la personne qui court, sont codées, ce qui réduit la quantité d'informations envoyées et stockées.

1. Transmis

2. Non transmis

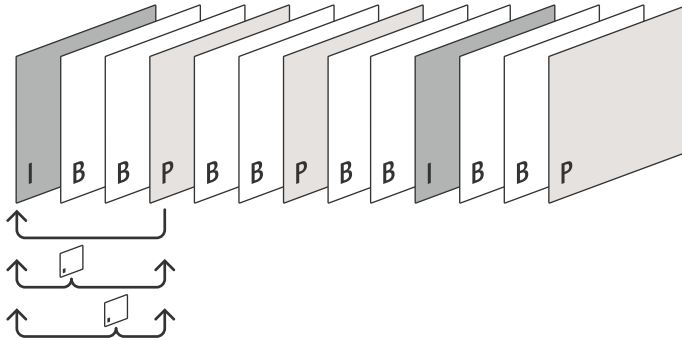
D'autres techniques peuvent être appliquées pour réduire davantage les données. La compensation de mouvement basée sur blocs, par exemple, prend en compte le fait qu'une grande partie de ce qui constitue une nouvelle image dans une séquence vidéo peut être trouvée dans une trame précédente, mais peut-être au dans un autre emplacement. Cette technique divise la trame en une série de macroblocs (blocs de pixels). Bloc par bloc, une nouvelle trame peut être composée ou « prédite » en recherchant un bloc correspondant dans une trame de référence. Si une correspondance est trouvée, l'encodeur code la position où le bloc correspondant doit être trouvé dans la trame de référence. L'encodage du vecteur de mouvement, comme on l'appelle, utilise moins de bits que si le contenu réel d'un bloc devait être codé.

Dans la prédiction intertrame, chaque trame d'une séquence d'images est classée comme un certain type de trame, telle qu'une trame I, une trame P ou une trame B.

Une trame I (intraframe), est une image autonome qui peut être décodée indépendamment sans référence à d'autres trames. La première image d'une séquence vidéo est toujours une image I. Elle sert de point de départ pour les nouveaux spectateurs ou de point d'accès à la synchronisation si le flux de données est endommagé. Les images I peuvent être utilisées pour mettre en œuvre l'avance rapide, le retour en arrière et d'autres fonctions d'accès aléatoire. L'encodeur insère automatiquement les trames I à intervalles réguliers ou à la demande lorsque les nouveaux clients commencent à voir le flux. Les trames I ont pour inconvénient de consommer beaucoup plus de bits. D'un autre côté, elles ne génèrent pas beaucoup d'artefacts, qui sont causés par des données manquantes.

Une image P est une inter-image prédictive qui fait référence aux parties des images I ou P antérieures. Les images P nécessitent généralement moins de bits que les images I, mais elles sont généralement très sensibles aux erreurs de transmission, en raison de la complexité de leur dépendance des images P et/ou I antérieures.

Une trame B (intertrame bi-prédictive) fait référence à la fois à une trame de référence antérieure et à une trame future. L'utilisation de trames B augmente la latence.



Séquence type d'images I, B et P. Une image P peut uniquement faire référence aux images I ou P précédentes, alors qu'une image B peut faire référence aux images I ou P précédentes et suivantes.

Lorsqu'un décodeur restaure une vidéo en décodant le flux de bits trame par trame, le décodage doit toujours commencer par une trame I. Si elles sont utilisées, les trames P et B doivent être décodées avec le(s) cadre(s) de référence.

Les produits vidéo Axis permettent de définir la longueur GOP (groupe d'images), qui détermine le nombre de trames P à envoyer avant qu'une autre trame I ne soit envoyée. Le débit peut être réduit en abaissant la fréquence des trames I (un GOP plus long). Toutefois, en cas de congestion du réseau, la qualité de la vidéo peut diminuer en raison d'une perte de paquets réseau.

Outre le codage par différence et la compensation de mouvement, d'autres méthodes avancées peuvent être employées pour réduire davantage les données et améliorer la qualité vidéo. H.264 et les autres normes de compression vidéo prennent en charge des techniques avancées qui incluent des schémas de prédiction pour l'encodage des images I, une compensation de mouvement améliorée avec une précision inférieure au pixel, et un filtre de déblocage en boucle pour lisser les bords des blocs (artefacts).

6.2 Formats de compression

Axis utilise quatre normes de compression vidéo : H.264, H.265, AV1 et Motion JPEG. AV1 est la norme de compression vidéo la plus récente et la plus avancée, avec un débit binaire très attractif. MPEG-4 Part 2 (simplement appelé MPEG-4) a été progressivement abandonné.

6.2.1 H.264

La norme H.264, également connue sous le nom de MPEG-4 Part 10 ou ISO/IEC 14496-10 Advanced Video Coding, est la norme de codage vidéo MPEG. Elle a été définie conjointement par des organismes de normalisation dans le secteur des télécommunications (Video Coding Experts Group de l'UIT-T) et des technologies de l'information (Moving Picture Experts Group de l'ISO/CEI).

H.264 est la norme la plus largement adoptée et elle est compatible avec un grand nombre de systèmes d'exploitation, de logiciels et de clients mobiles. H.264 a contribué à accélérer le fonctionnement des caméras mégapixel/HDTV, car la technologie de compression très efficace permet de réduire la taille des fichiers et les débits binaires générés sans compromettre la qualité de l'image.

Bien qu'elle reste un choix fiable pour la compression vidéo, la norme H.264 a été introduite il y a plus de vingt ans et n'est plus la norme offrant le meilleur débit. Sa technologie vieillissante peine à répondre aux demandes croissantes de transmission et de stockage de vidéos en haute résolution et H.264 ne prend pas en charge les vidéos d'une taille supérieure à 8K.

Le profil de base pour H.264 utilise uniquement des trames I et P, tandis que le profil principal peut également utiliser des trames B en plus des trames I et P. Sans trames B, la latence est plus faible. Les produits vidéo Axis utilisent le profil de base H.264 ou le profil principal. Dans les produits de vidéo avec des processeurs plus puissants, Axis utilise le profil principal sans trames B pour permettre une compression plus élevée, tout en maintenant une faible latence et la qualité de la vidéo.

6.2.2 H.265

H.265 est la norme de codage vidéo à haute efficacité approuvée par l'UIT, ISO/IEC 23008-5. Par rapport à H.264, H.265 améliore la compression de 15 à 40 % pour la même qualité vidéo. La norme est réglée pour des résolutions vidéo plus élevées, des fréquences d'images plus élevées et plus de mouvement.

L'encodage H.265 ne répond pas encore entièrement aux exigences des vidéos de type surveillance. La plupart des équipements de surveillance prennent en charge l'encodage H.265, mais la prise en charge du décodeur et des navigateurs est limitée. De nombreux utilisateurs doivent continuer à utiliser H.264 pour pouvoir visionner des vidéos sur leurs clients préférés, mais cela ne devrait pas poser de problème car Zipstream avec H.264 est très efficace en termes de débit. La norme AV1, plus récente, est susceptible de concurrencer la norme H.265 en tant que successeur privilégié de la norme H.264, étant donné les performances supérieures et le large soutien de l'industrie à la norme AV1 par rapport à la norme H.265.

6.2.3 AV1

AV1 est une norme d'encodage vidéo moderne optimisée pour la transmission de vidéos sur Internet. AV1 permet un flux et un stockage vidéo de haute résolution, sans problème et à moindre coût.

AV1 devrait devenir le codec dominant dans l'industrie de la vidéosurveillance grâce à son faible débit, à ses nouvelles fonctionnalités et à la prise en charge d'un grand nombre de décodeurs clients. Il est déjà pris en charge par les principaux navigateurs, systèmes d'exploitation, plateformes cloud et périphériques mobiles.

AV1 a été normalisé par l'Alliance for Open Media (AOM) en tant que codage vidéo *AOMedia Video 1* selon *AV1 Bitstream & Decoding Process Specification v1.0.0* par aomedia.org. AOM a été fondée par les principales sociétés informatiques du monde et AV1 est librement accessible sans frais de licence à AOM.

AV1 a bénéficié d'un large soutien dans l'industrie des technologies de l'information. Il est largement utilisé dans les technologies de flux cloud, telles que WebRTC, permettant une communication efficace en temps réel et un flux vidéo. L'intégration transparente dans le cloud permet aux développeurs d'utiliser directement la vidéo de sécurité dans les applications informatiques, telles que les systèmes logistiques, afin d'améliorer l'intelligence économique et l'efficacité opérationnelle.

6.2.4 Zipstream pour H.264, H.265 et AV1

Optimisée pour la vidéosurveillance, la technologie Axis Zipstream est une implémentation de codeur vidéo radicalement plus efficace, qui réduit encore plus les besoins en bande passante et en stockage, avec une réduction de 50 % minimum. Zipstream n'est en aucun cas un remplacement de H.264, H.265 ou AV1. C'est une amélioration 100% conforme à la norme.

Zipstream fonctionne en incluant un module dans le moteur de compression vidéo de la caméra pour s'assurer que les détails importants de l'image (régions d'intérêt) reçoivent suffisamment d'attention, tandis que les données inutiles sont supprimées. Zipstream réduit les exigences en matière de stockage sans aucune intégration compliquée, et aucun changement coûteux n'est requis dans le reste du système de surveillance. Les détails intéressants et les mouvements sont conservés avec la qualité vidéo spécifiée, tandis que le module Axis compresse davantage les autres zones, afin d'utiliser au mieux la bande passante disponible. Zipstream est pris en charge par les caméras Axis les plus récentes, y compris les caméras PTZ et les caméras Ultra HD 4K.

La solution utilisée pour compresser la vidéo selon les encodages H.264, H.265 et AV1 ne fait pas partie des normes, puisque seule la syntaxe et la méthode utilisées pour effectuer la lecture sont

standardisées. Cela permet de créer des encodeurs H.264 / H.265 / AV1 compatibles améliorés, tels que Zipstream, tout en préservant le format de fichier à des fins d'interopérabilité (compatibilité du décodeur).

Zipstream regroupe plusieurs algorithmes différents qui réduisent la bande passante :

- > **Algorithme dynamique de région d'intérêt (ROI).** Méthode de fréquence d'images complète automatique pour sélectionner les zones importantes afin de réduire la taille de toutes les images.
- > **Algorithme dynamique d'images par seconde (FPS).** Méthode supplémentaire pour réduire la fréquence d'images afin de réduire le stockage nécessaire pour les images P.
- > **Algorithme dynamique de groupe d'images (GOP).** Méthode supplémentaire pour modifier la longueur du GOP afin de réduire la quantité de stockage nécessaire pour les images I.

Zipstream adapte le flux vidéo compressé en fonction du mouvement de la scène, du contenu de la scène, du niveau d'éclairage ambiant et des options de configuration, telles que les paramètres de compression, la fréquence d'images et le paramètre de force définissant le niveau d'effort.

Paramètre de force	Niveau d'effort	Effet visible
Désactivé	Désactivé	Aucun
10	Faible	Pas d'effet visible dans la plupart des scènes
20	Moyen	Effet visible dans certaines scènes : moins de bruit et niveau de détail légèrement inférieur dans des régions de faible intérêt
30	Élevé	Effet visible dans de nombreuses scènes : moins de bruit et niveau de détail inférieur dans des régions de faible intérêt
40	Plus élevé	Effet visible dans encore plus de scènes : moins de bruit et niveau de détail inférieur dans des régions de faible intérêt
50	Extrême	Effet visible dans la majorité des scènes : moins de bruit et niveau de détail inférieur dans des régions de faible intérêt

tableau 6.2a *Valeurs du paramètre de force Zipstream et niveaux d'effort.*

Vous pouvez configurer individuellement les différentes parties de l'algorithme Zipstream ou utiliser le profil de stockage, qui configure automatiquement Zipstream à des fins d'optimisation de la vidéo pour le stockage.

- > **Profil classique** : Profil par défaut, qui permet de gérer individuellement les éléments majeurs de l'algorithme Zipstream. Au départ, le paramètre de force est réglé sur 10, et le groupe dynamique d'image et l'IPS dynamique sont désactivés. Ce paramètre est compatible avec toutes les applications existantes, tout en réduisant le débit binaire. Pour un débit binaire encore plus faible, vous pouvez choisir un paramètre de force supérieur et activer le groupe dynamique d'image et/ou l'IPS dynamique.
- > **Profil de stockage** : Ce profil configure Zipstream de sorte que la vidéo est optimisée pour le stockage et l'accès ultérieur, ce qui correspond au principal cas d'utilisation des produits vidéo Axis. Le profil de stockage minimise le débit binaire tout en maximisant la nature probante de la vidéo pour ce scénario. Avec le profil de stockage, la caméra active automatiquement l'algorithme Zipstream le plus adapté à ce type de caméra et utilise des outils d'encodage vidéo plus évolués. Le profil varie en fonction des caméras et de leurs fonctionnalités, et le résultat peut varier selon les types de caméra.

6.2.5 Motion JPEG

Motion JPEG ou M-JPEG est une séquence vidéo numérique constituée d'une série d'images JPEG individuelles. Comme il n'y a pas de dépendance entre les images, une vidéo Motion JPEG est robuste : si une image est supprimée pendant la transmission, le reste de la vidéo ne sera pas affecté. Motion JPEG est une norme sans licence. Elle présente une large compatibilité et peut être nécessaire lors de l'intégration avec des systèmes qui ne prennent en charge que le Motion JPEG. Elle est également populaire dans les applications où des images individuelles dans une séquence vidéo sont nécessaires, par exemple dans les analyses, et où des fréquences d'image faibles sont utilisées, par exemple dans un aperçu VMS.

Comme il s'agit d'une série d'images fixes et complètes, Motion JPEG ne peut pas utiliser de techniques de compression vidéo pour réduire les données. Cela conduit à un débit binaire relativement élevé ou à un taux de compression faible pour la qualité fournie par rapport à d'autres normes de compression vidéo.

Motion JPEG peut être déconseillé pour les produits vidéo dont la résolution est supérieure à 1080p, car les images peuvent être trop volumineuses à transférer sur un réseau de 100 Mbits/s en fréquence d'image complète. La mise à niveau vers un réseau gigabit ne fera que déplacer le goulot d'étranglement vers les étapes de traitement d'image sur la caméra avant et après le transport sur

IP, et rendra l'utilisation beaucoup plus compliquée. Si des images JPEG sont requises, la fréquence d'images du système doit être réduite en conséquence.

6.2.6 JPEG

Les images fixes suivent la norme JPEG, qui est prise en charge par toutes les caméras. Les images fixes sont parfois utilisées dans les caméras vidéo comme icônes ou comme vue d'ensemble.

6.3 Débits binaires moyens, variables et maximum

H.264, H.265 et AV1 peuvent tous être configurés pour utiliser des flux vidéo codés avec un débit binaire moyen, variable ou maximal. La sélection la mieux adaptée dépend de l'application et de l'infrastructure réseau.

Avec ABR (débit binaire moyen), un espace de stockage spécifié est utilisé sur une période donnée. Un certain espace de stockage est attribué à un flux vidéo et le contrôleur ABR de la caméra adapte la qualité vidéo pour s'assurer que la vidéo de toute la période respecte le budget de débit binaire. Le stockage inutilisé lors de périodes précédentes moins actives peut être utilisé pour maintenir une haute qualité de vidéo lors de périodes ultérieures plus actives et le budget de débit binaire est conservé. Cela permet d'améliorer la qualité vidéo tout en évitant de dépasser les limites de stockage du système. ABR est optimal pour les flux enregistrés en continu, sans périodes de pause programmées.

Avec VBR (débit binaire variable), une qualité d'image prédéfinie est maintenue, que la scène contienne ou non des mouvements. Cela signifie que l'utilisation de la bande passante augmentera quand il y aura beaucoup d'activité dans une scène et diminuera quand il y aura moins de mouvements. C'est utile pour les scénarios de vidéosurveillance où une haute qualité est requise, particulièrement s'il y a du mouvement dans la scène. Comme le débit peut varier, même lorsqu'une moyenne est définie, l'infrastructure de réseau (bande passante disponible) doit pouvoir accepter des débits élevés.

Avec une bande passante limitée disponible, le mode recommandé est normalement MBR (débit maximal), définissant une limite maximale sur le débit. Il faut cependant noter que quand il y a beaucoup d'activité dans une scène, cela entraîne un débit supérieur au débit cible, et la restriction sur le débit binaire conduit à une qualité d'image et à une fréquence d'images plus basses. Les produits vidéo Axis permettent à l'utilisateur de donner la priorité à la qualité d'image ou à la fréquence d'images si et quand le débit dépasse le taux cible.

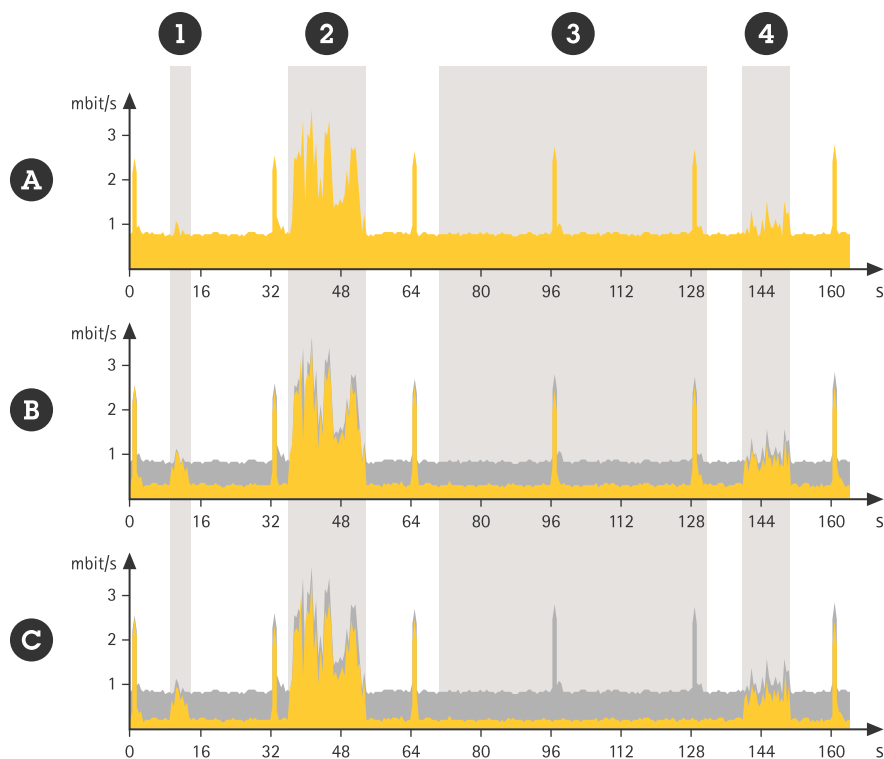
6.4 Comparaison des normes

Lorsque l'on compare la performance des normes de compression vidéo, il est important de noter que les résultats peuvent varier entre les encodeurs qui utilisent la même norme, car différents sous-ensembles peuvent être implémentés. Tant que la sortie d'un encodeur est conforme au format d'une norme et au décodeur, il est possible de réaliser des implémentations différentes. Cela permet d'optimiser la technologie et de réduire la complexité des implémentations.

Cependant, cela signifie également qu'une norme ne peut garantir un débit ou une qualité donné(e) et que les comparaisons ne peuvent pas être effectuées correctement sans d'abord définir la manière dont les normes sont implémentées dans un encodeur.

Contrairement à un encodeur, un décodeur doit implémenter toutes les parties requises d'une norme pour décoder un flux binaire conforme. Cela signifie que seul le décodeur est réellement normalisé. La norme spécifie exactement la manière dont un algorithme de décompression doit restaurer chaque bit d'une vidéo compressée. Quand la qualité de la vidéo entre en jeu, l'utilisateur doit tester quelques produits pour s'assurer que la qualité correspond à l'objectif.

Étant donné le même niveau de qualité d'image, la figure ci-dessous montre une comparaison de débit binaire entre H.264 et Axis H.264 amélioré (technologie Axis Zipstream) à des niveaux d'effort faible et élevé.



Le débit binaire instantané dans quatre scénarios différents (1, 2, 3, 4) pour différents niveaux d'effort de Zipstream (A : Zipstream désactivé, B : faible, C : élevé). La réduction du débit binaire est représentée par les zones grisées. Chaque mise à jour de l'image I est clairement visible sous la forme d'une pointe dans le débit binaire, qui peut être lue sur les axes verticaux. Tous les flux sont de type VBR (débit binaire variable) avec une longueur de groupe d'images de 32.

Les périodes de la figure mettent en évidence le comportement de Zipstream dans différentes conditions :

1. Période avec de brefs et petits mouvements. Les petits mouvements sont détectés et l'ajout de bits dans cette région peut conserver la partie en mouvement de la vidéo.
2. Une période plus longue avec un mouvement plus important nécessite plus d'espace, mais il est toujours possible d'économiser du stockage, dans la mesure où l'algorithme de région d'intérêt dynamique (ROI) détecte les zones dans lesquelles les informations non prioritaires peuvent être supprimées.

3. Les périodes sans mouvement sont détectées et l'algorithme GOP dynamique supprime les mises à jour d'images I inutiles.
4. Périodes avec petit mouvement de longue durée.

AXIS Site Designer peut être utilisé pour estimer les débits binaires pour différents types de scènes.

7. Audio

Les fonctionnalités audio associées à un système de vidéosurveillance offrent des possibilités inestimables de détection et d'interprétation des événements et des urgences. L'analyse audio permet de surveiller les flux audio et de réagir lorsqu'un événement se démarque. En associant le système à des haut-parleurs réseau, vous pouvez facilement communiquer avec les visiteurs ou émettre des avertissements à l'intention des intrus.

7.1 Détection sonore

La détection audio peut être déployée en tant que technologie autonome, ce qui permet plusieurs cas d'utilisation dans les domaines de la prévention des crimes et délits, de la protection et des enquêtes judiciaires. Par exemple, la surveillance audio avec interaction directe avec l'opérateur renforce la perception de la scène. Dans un hôpital ou un centre de soins, la détection audio peut vous aider à percevoir si un patient est en détresse et a besoin d'une infirmière. En matière de détection audio, il peut également s'agir de détecter si un son inattendu vient de la droite ou de la gauche et de diriger une caméra PTZ vers la source sonore.

En cas d'utilisation combinée de la vidéosurveillance, l'audio ajoute une nouvelle dimension d'information pour la prise de décision et optimise potentiellement la majorité des cas de vidéosurveillance existants. Par exemple, les opérateurs de sécurité peuvent avoir un bien meilleur aperçu des événements d'une scène si leur flux vidéo est complété par un flux audio.

7.1.1 Périphériques et technologie de connectivité audio

La fonctionnalité de détection audio d'une caméra peut être mise en œuvre de plusieurs manières.



Une caméra avec microphones intégrés pour une détection audio de haute qualité, un microphone numérique autonome doté d'un connecteur 3,5 mm (1/8 pouce) et une interface audio et E/S qui utilise la technologie de conversion des ports pour ajouter en toute transparence la fonctionnalité de détection audio à une caméra.

Microphone intégré : Grâce aux microphones intégrés, les fonctions audio telles que l'amplificateur de voix peuvent être adaptées au modèle de caméra spécifique et à l'usage auquel elle est destinée. Avec deux microphones intégrés, une caméra peut fournir un son stéréo qui permet de distinguer de quelle direction viennent les sons. Avec au moins trois microphones intégrés, la caméra reçoit également des informations spatiales plus détaillées. Cela permet de localiser automatiquement la source audio ou la formation de faisceau, ce qui permet de « zoomer vers l'avant » sur le son provenant d'une direction spécifique.

Prise en charge intégrée de l' audio et microphone autonome : Souvent, les caméras sont équipées d'une prise micro/entrée de ligne de 3,5 mm (1/8 po) pour connecter, par exemple, un microphone séparé. Des microphones séparés peuvent être placés dans les meilleurs emplacements stratégiques et capturer un son clair et pertinent. Si une caméra doit être placée en hauteur sur un mur ou au plafond pour fournir une vue d'ensemble, un petit microphone séparé peut être discrètement placé à un niveau inférieur, plus proche de là où les personnes se trouvent. En cas de connexion à l'aide d'un kit d'extension audio numérique, un microphone numérique peut transporter le signal audio avec un câble réseau pouvant atteindre 100 m (358 pieds) sans perte.

Technologie bord à bord : l'appairage de microphones, via la technologie bord à bord, est possible si les deux périphériques sont connectés au même réseau et qu'ils prennent en charge le bord à bord dans leur logiciel. Après l'appairage, les paramètres audio du microphone peuvent être contrôlés à partir de l'interface utilisateur de la caméra, même si, initialement, la caméra n'était pas configurée pour prendre en charge l'audio.

Interface audio et E/S avec conversion des ports : la technologie de conversion des ports est un concept unique d'Axis, qui repose sur l'utilisation d'un périphérique d'interface audio et E/S connecté physiquement directement à la caméra à l'aide d'un câble réseau. Une fonction audio

bidirectionnelle peut être ajoutée aux caméras qui ne prennent pas en charge l'audio intrinsèquement. Le dispositif de conversion des ports utilise l'adresse IP de la caméra, est contrôlé depuis la caméra et permet à la caméra de fournir une connectivité audio intégrée à la caméra, avec l'audio et la vidéo dans un même flux sur le réseau. Certains dispositifs de conversion des ports sont équipés d'un microphone intégré.

Connectivity Hub : ce périphérique ajoute une fonction d'entrée audio à votre système, y compris des fonctions de communication bidirectionnelles et une compatibilité étendue du microphone. Le Connectivity Hub a sa propre adresse IP et dispose de plusieurs E/S et ports pour intégrer divers capteurs non visuels.

7.1.2 Amélioration de la détection audio

Les périphériques dotés de fonctionnalités de détection audio bénéficient de différentes améliorations pour générer un son de qualité optimale.

- > **Amplificateur vocal** : amplifie les contenus vocaux par rapport à d'autres sons dans le but de rendre la voix plus audible.
- > **Contrôle automatique du gain** : adapte dynamiquement le gain aux changements apportés au son.
- > **Suppression de l'écho** : reconnaît et supprime les sons générés par le haut-parleur intégré.
- > **Égaliseur graphique** : permet aux utilisateurs avancés de filtrer des fréquences sonores spécifiques.

7.1.3 Analyse audio

Tout comme plusieurs types d'analyses vidéo peuvent être employés pour le lancement automatique d'alarme basé sur la détection visuelle, les analyses audio peuvent surveiller les flux audio et réagir lorsqu'un événement se démarque. Les analyses audio peuvent être configurées pour déclencher des alarmes automatiques et d'autres actions lorsqu'un microphone détecte des sons associés au cri de personnes, à du bris de verre ou à d'autres sons anormaux. Cet avertissement rapide permet des réponses et une intervention rapides. L'analyse audio peut également être utilisée pour rediriger automatiquement une caméra PTZ vers un incident audible ou pour mesurer le SPL (niveau de pression sonore) afin de donner des indications sur la pollution sonore.

En général, les analyses audio n'enregistrent pas le son en continu. Elles le mettent temporairement en mémoire tampon et traitent l'audio afin de rechercher des modèles, niveaux ou fréquences spécifiques. Mais les systèmes peuvent être configurés pour enregistrer ce qui a été mis en mémoire tampon juste avant ou après une détection afin de permettre à la sécurité de vérifier la détection et éventuellement, conserver l'audio dans le cadre d'une enquête judiciaire.

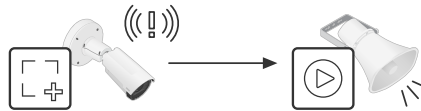
7.2 Sortie audio

L'ajout de haut-parleurs sur IP à un système de vidéosurveillance permet de dissuader proactivement les actes criminels par une réponse immédiate et une intervention à distance avec des messages préenregistrés ou en direct. Les haut-parleurs sont également adaptés aux systèmes audio multi-usages qui permettent de dissuader, d'informer, de diffuser des messages de sécurité et de la musique en arrière-plan, le tout dans le cadre d'une installation unique.

7.2.1 Sortie audio en vidéosurveillance

De nombreuses caméras disposent d'une fonction audio intégrée et d'un connecteur de sortie audio permettant de connecter un haut-parleur. En outre, une caméra qui prend en charge la technologie bord à bord peut également être appairée à un haut-parleur même si elle n'est pas équipée de sortie audio ou de sortie de ligne. Une fois l'appairage effectué, les paramètres audio peuvent être contrôlés à partir de l'interface utilisateur de la caméra. De nombreux modèles de caméra peuvent également se connecter à des haut-parleurs via un Connectivity Hub ou une interface audio et E/S.

Une solution de sécurité avec audio et vidéo peut être surveillée ou non surveillée, avec différents niveaux d'intégration des caméras.



Solution non surveillée : une caméra dotée d'outils d'analyse détecte les accès non autorisés ou d'autres événements dans une zone à accès restreint et envoie une commande à un haut-parleur pour lire un message audio préenregistré.



Solution surveillée : une caméra dotée d'outils d'analyse détecte les accès non autorisés ou d'autres événements et envoie une notification à un opérateur. L'opérateur peut parler en direct ou diffuser un message audio préenregistré.

Les caméras peuvent également être connectées à des avertisseurs audiovisuels (une sirène stroboscopique, par exemple). Ce type de dispositif entièrement connecté en réseau peut être

utilisé pour dissuader des intrus ou améliorer l'efficacité opérationnelle grâce à un éclairage stroboscope et des alarmes sirène. Il peut être personnalisé via l'utilisation de différentes séquences lumineuses blanches et RGBA et de sons préconfigurés. Une sirène stroboscopique est particulièrement utile lorsqu'elle est connectée à une caméra avec une protection périmétrique ou une fonction de reconnaissance de plaque d'immatriculation.

7.2.2 Systèmes audio sur IP pour la sonorisation

Les haut-parleurs et d'autres périphériques audio en réseau peuvent être combinés à un système de sonorisation (PA) sur IP pour diffuser des annonces en direct et préenregistrées, des messages de sécurité et de la musique en arrière-plan. Grâce à la technologie IP, le système devient flexible et évolutif. Elle simplifie également l'intégration avec d'autres systèmes, car les haut-parleurs peuvent être intégrés directement à un système de téléphonie VMS ou VoIP (Voice over IP).

Les haut-parleurs réseau Axis sont des systèmes audio complets de haute qualité, avec un amplificateur et un processeur de signal numérique intégrés pour disposer de son préconfiguré. Ils disposent également d'un microphone intégré qui permet une communication bidirectionnelle et des auto-vérifications automatiques pour garantir une qualité sonore optimale.



Les formes, pressions sonores et possibilités de montage des haut-parleurs d'Axis varient et correspondent à différents cas d'utilisation.

Le logiciel de gestion audio permet de gérer le contenu audio et les périphériques. Tous les matériels audio Axis sont livrés avec des logiciels intégrés adaptés aux cas d'utilisation de base sur les petits systèmes et les systèmes de taille moyenne. Axis propose également des options logicielles convenant à des systèmes plus importants et plus avancés, notamment les environnements multisites qui incluent des milliers de sites. Grâce au logiciel de gestion audio, chaque haut-parleur est adressable individuellement. Les haut-parleurs peuvent également être regroupés en zones, ce qui vous permet de cibler des annonces vers des publics spécifiques dans les zones pertinentes d'un site, sans répéter le message sur l'ensemble du réseau de locuteurs. Les zones peuvent être facilement reconfigurées en un instant, sans utiliser de nouveaux câbles. Des messages préenregistrés et de la musique en arrière-plan peuvent être programmés et la fonctionnalité du système est automatiquement contrôlée.

Pour en savoir plus sur les systèmes audio sur IP, consultez le Guide technique de l'audio sur IP, disponible en téléchargement sur axis.com/learning/technical-guides.

7.3 Modes de communication audio

Selon l'application, il peut être nécessaire d'envoyer de l'audio dans une seule direction ou dans les deux directions. Cela correspond à trois modes de base de communication audio :

- > **Simplex** signifie que l'audio peut être envoyé dans une seule direction. Dans l'audio sur IP, le son est généralement envoyé par un opérateur à un haut-parleur, par exemple pour communiquer des avertissements ou des annonces via le haut-parleur. Mais l'audio en mode simplex peut également être envoyé depuis le haut-parleur à l'opérateur, par exemple dans des applications de surveillance à distance où l'audio en direct provenant d'un site surveillé est envoyé sur un réseau.
- > **Semi-duplex** signifie que l'audio peut être envoyé et reçu dans les deux directions, mais seulement dans une direction à la fois. La direction est contrôlée soit par l'intermédiaire d'un bouton poussoir physique, soit par le biais d'un logiciel de détection de la voix. Ce mode de communication est similaire à une conversation par talkie-walkie. Dans la mesure où le haut-parleur et le microphone ne sont jamais actifs en même temps, le half-duplex ne présente aucun risque de problèmes d'écho.
- > **Duplex intégral** signifie que les utilisateurs peuvent envoyer et recevoir de l'audio (parler et écouter) en même temps. Ce mode de communication est similaire à une conversation téléphonique. Le full-duplex nécessite que le client (PC, microphone SIP ou téléphone VoIP) et le haut-parleur prennent en charge l'audio full-duplex. Lors de la mise en œuvre, la suppression de l'écho acoustique (AEC) doit également être prise en charge afin d'éviter les effets d'écho.

Les périphériques audio Axis fonctionnent en half-duplex ou en full-duplex pour un audio bidirectionnel.

7.4 Codecs audio

Un codec (encodeur-décodeur) audio est un système logiciel capable de numériser et de compresser les données pour la transmission et de décompresser les données reçues. Les produits Axis prennent en charge différents codecs audio :

AAC-LC (Advanced Audio Coding – Low Complexity), également connu sous le nom de MPEG-4 AAC, qui nécessite une licence. AAC-LC, en particulier à un taux d'échantillonnage de 16 kHz ou plus et à un débit binaire de 64 kbit/s ou plus, est le codec qu'il est recommandé d'utiliser lorsque la meilleure qualité audio possible est requise.

G.711 et **G.726**, sont des normes ITU-T sans licence. Ils ont une latence plus faible et nécessitent moins de puissance de calcul que l'AAC-LC. G.711 et G.726 sont des codecs vocaux qui sont principalement utilisés dans la téléphonie et qui ont une faible qualité audio. Tous deux ont un taux d'échantillonnage de 8 kHz. G.711 a un débit binaire de 64 kbit/s. La mise en œuvre du G.726 d'Axis prend en charge 24 et 32 kbit/s. Avec G.711, les produits Axis ne prennent en charge que la loi μ , qui est l'un des deux algorithmes de compression du son dans la norme G.711. Lorsque G.711 est utilisé, il est important que le client utilise également la compression μ -law.

Les caméras Axis prennent également en charge LPCM. En outre, les produits Axis qui prennent en charge SIP peuvent également utiliser Opus, L16/16000, L16/8000, speex/8000, speex/16000 et G.726-32.

7.5 Synchronisation de l'audio et de la vidéo

La synchronisation des données audio et vidéo est assurée par un lecteur multimédia ou par un framework multimédia tel que WebRTC.

L'audio et la vidéo sont envoyés sur un réseau sous la forme de deux flux de paquets distincts. Pour que le client ou le lecteur synchronise parfaitement les flux audio et vidéo, les paquets audio et vidéo doivent être horodatés. L'horodatage des paquets vidéo utilisant la compression Motion JPEG n'est pas toujours pris en charge dans une caméra réseau. Si c'est le cas et s'il faut que la vidéo et l'audio soient synchronisés, le format vidéo qui s'impose est H.264, H.265 ou AV1 puisque ces flux vidéo, ainsi que le flux audio, sont envoyés en RTP (Transport en Temps Réel Protocole), qui horodate les paquets vidéo et audio. Cependant, il arrive très souvent que l'audio synchronisé soit

moins important ou même indésirable ; par exemple, si l'audio doit être contrôlé mais pas enregistré.

8. Radar

Les radars conviennent idéalement à la protection de vastes espaces ou à la surveillance du trafic. Ils peuvent être utilisés en mode autonome, par exemple lorsque des réglementations en lien avec le respect de la vie privée limitent l'utilisation des caméras, mais ils sont aussi facilement intégrables aux systèmes de surveillance.

8.1 Une technologie non visuelle qui complète la vidéosurveillance

Le radar est une technologie non visuelle qui offre des résultats fiables dans de nombreuses situations où les autres technologies de surveillance sont inappropriées. Il utilise les ondes électromagnétiques pour détecter les mouvements et n'est pas sensible aux éléments qui déclenchent habituellement de fausses alarmes (ombres ou faisceaux lumineux en mouvement, gouttes de pluie ou insectes, par exemple). Il est précis quelles que soient les conditions de luminosité, 24 heures sur 24.

En outre, à l'inverse des caméras vidéo, il fournit également des informations essentielles sur les objets détectés comme la position exacte, la vitesse et la direction du mouvement. Des fonctions d'analyses pour la détection, le suivi et la classification des objets sont intégrées dans le radar.

8.2 Dispositifs radar



Deux radars utilisés pour la surveillance d'une zone et la surveillance du trafic, et une caméra de fusion radar-vidéo permettant une collecte d'informations optimale sur une scène.

Doté d'une fonction d'analyse intégrée, un radar Axis peut détecter, classer et suivre avec précision les personnes et les véhicules. Il est fourni avec deux profils de détection optimisés pour différents scénarios.

Le profil de surveillance de zone permet de détecter les personnes et les véhicules circulant à faible vitesse. Lorsque ce profil est activé, le radar assure la protection d'une zone étendue 24 heures sur 24 et 7 jours sur 7, avec un faible taux de fausses alarmes. Il est parfait pour les zones extérieures ouvertes où l'activité est modérée, par exemple, les sites industriels ou les parkings et les quais de chargement après les heures de bureau/travail.

Le profil de surveillance routière permet de détecter les véhicules circulant à des vitesses plus élevées. Lorsque ce profil est activé, le radar suit et mesure la vitesse des véhicules dans le cadre de la surveillance des flux de circulation. Si AXIS Speed Monitor est installé sur le radar ou sur une caméra connectée, il est facile d'extraire des statistiques permettant d'optimiser la prise de décision. En outre, le flux vidéo du radar ou de la caméra permet de visualiser les vitesses en direct.

Une caméra de fusion radar-vidéo combine deux périphériques en un : une caméra qui offre une excellente utilisation des images et un radar entièrement intégré. Le radar détecte des objets sur de larges zones avec peu ou pas de lumière, et visualise la vitesse et la distance des objets en mouvement directement dans la vue de l'application. Les analyses vidéo et radar combinées fournissent des données plus complètes, avec une collecte d'informations optimale sur la scène, associée à la valeur légale de la vidéo. Vous pouvez déclencher des actions basées sur la détection par le radar uniquement, par la caméra uniquement, ou par les deux dispositifs, selon les besoins.

8.3 Radars intégrés à un système de surveillance

Les radars Axis sont alimentés par PoE et s'intègrent facilement à d'autres périphériques et systèmes de gestion vidéo.

En plus de déclencher une alarme lorsqu'il détecte un intrus, le radar peut également déclencher un enregistrement vidéo pour la vérification visuelle. L'association de radars et de caméras est particulièrement efficace avec des caméras PTZ (panoramique-inclinaison-zoom), qui peuvent suivre et identifier des personnes ou des véhicules en fonction de leur position géographique exacte fournie par le radar.

En ce qui concerne la protection périmétrique, la zone de détection étendue d'un radar complète la zone de détection étroite mais plus étendue d'une caméra thermique. Vous pouvez, par exemple, installer le radar sur une clôture orientée vers l'extérieur, afin de créer une zone tampon et de détecter les intrus potentiels avant même qu'ils n'atteignent la ligne de clôture. Les radars peuvent également être utilisés avec des haut-parleurs dans des situations où l'identification visuelle n'est pas autorisée ou prioritaire. L'utilisation d'un message audio est un moyen efficace de dissuader les intrus détectés par le radar.

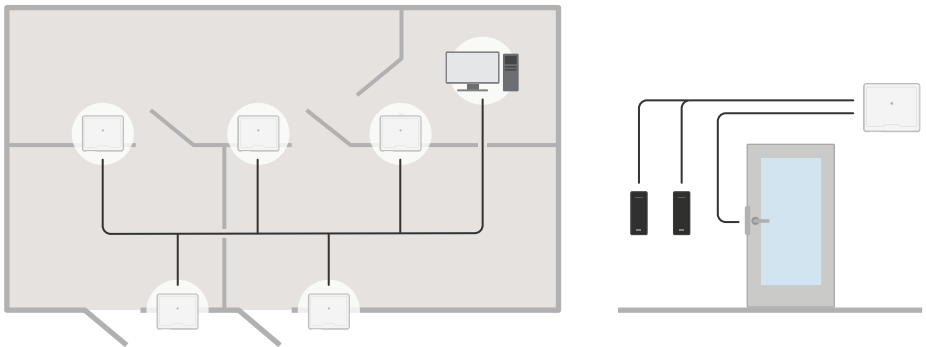
Un radar intégré dans un système de surveillance génère également des économies d'énergie car il peut « voir » dans l'obscurité. Par exemple, vous pouvez définir des déclencheurs dédiés à l'allumage de lumières infrarouges ou de projecteurs en cas de détection d'objet par le radar, ce qui est utile sur les sites à faible activité après les heures de travail. Vous pouvez également économiser de l'espace de stockage si vous choisissez de ne déclencher des enregistrements que dans certaines situations. En outre, le faible taux de fausses notifications permet au personnel de sécurité d'agir uniquement sur les menaces réelles, ce qui lui permet de gérer davantage de caméras et de vous faire gagner ainsi du temps et de l'argent.

9. Contrôle d'accès

Les systèmes de contrôle d'accès physiques sont omniprésents dans les usines, les hôpitaux, les magasins et de nombreux autres secteurs dans le monde. Actuellement, le contrôle d'accès passe des solutions traditionnelles et propriétaires (fermées) à la technologie ouverte IP, qui apporte des améliorations majeures en termes de performance des produits et de la gestion. Le contrôle d'accès IP peut être utilisé comme système de sécurité autonome, mais aussi comme complément à la surveillance vidéo sur IP ou intégré à d'autres types de systèmes.

9.1 Qu'est-ce que le contrôle d'accès ?

Dans un système dédié au contrôle d'accès physique, des dispositifs tels que des contrôleurs de porte, des lecteurs de carte et des modules de relais d'E/S sont installés à proximité des portes et des points d'entrée. Avec un logiciel de gestion d'accès, ils permettent de gérer l'accès du personnel et des visiteurs dans des zones spécifiques.



Système de contrôle d'accès avec des contrôleurs de porte, un logiciel de gestion d'accès et des lecteurs de carte.

Un exemple : Que se passe-t-il lorsqu'un employé présente sa carte d'accès devant le lecteur de carte à l'entrée de son bureau ? Le lecteur envoie les informations de la carte au contrôleur de porte (connecté au verrou électronique de la porte) qui vérifie dans la liste d'accès (dans le système de gestion d'accès intégré au contrôleur de porte ou sur un serveur) si la carte permet d'accéder à la porte. Si les identifiants correspondent à un élément de la liste, le contrôleur de porte envoie au verrou électronique un signal de déverrouillage de la porte.

Le contrôle d'accès peut également être intégré à des interphones réseau pour autoriser l'accès aux visiteurs de manière contrôlée et sécurisée, avec une identification vidéo et une communication bidirectionnelle. L'intégration des systèmes de contrôle d'accès avec la surveillance vidéo ajoute également de nouvelles dimensions à la solution de sécurité, en autorisant des fonctions telles que la surveillance, l'investigation et l'assistance.

9.2 Pourquoi IP dans le contrôle d'accès ?

Un système de contrôle d'accès classique est un système fermé, conçu par des fournisseurs qui développent l'ensemble du produit, depuis les contrôleurs et les identifiants jusqu'au logiciel. Cela garantit le fonctionnement du système mais implique également un manque de flexibilité pour l'utilisateur. Lorsqu'une société se développe ou lorsque ses besoins en matière de contrôle d'accès évoluent, il peut être nécessaire d'installer un système entièrement nouveau et de supprimer complètement l'ancien. Et il peut être nécessaire de le refaire quelques années plus tard, en cas de nouvelle évolution des besoins.

Un système de contrôle d'accès basé sur IP est flexible dès le début, et il est facile de l'étendre ou d'y ajouter une nouvelle fonctionnalité. Son intelligence s'étend jusqu'à la porte ; il est donc possible de prendre des décisions d'accès localement et de manière centralisée. Le contrôleur de porte utilise des règles distribuées et mises à jour sur le réseau IP. Il peut être connecté et alimenté via PoE.

Les principaux avantages peuvent être résumés comme suit :

- > **Une sécurité renforcée grâce au cryptage.** Un contrôleur de porte edge-based intelligent peut garantir le stockage sécurisé des clés cryptographiques à l'aide d'un module de calcul embarqué certifié EAL6+. Une certification de canal sécurisé OSDP garantit le cryptage et la protection de la communication avec le lecteur dans son intégralité. Ce type de système est également capable de sécuriser la communication avec le logiciel de gestion de contrôle d'accès.
- > **Intégration facile et évolutive.** En adoptant des normes et des interfaces ouvertes, le contrôle d'accès IP peut être intégré à d'autres systèmes, notamment des solutions de surveillance, d'analyse, d'interphones, de son ou de gestion du temps de présence. Les possibilités sont

illimitées si la technologie est considérée comme une solution IoT (Internet des objets), plutôt qu'un contrôle d'accès seulement.

- > **Rentabilité.** Les solutions de contrôle d'accès IP peuvent être facilement connectées et alimentées par un réseau IP existant, sans nécessiter de câblage particulier. IP permet également la gestion à distance et la surveillance de l'état du système, ce qui contribue à réduire le coût total de possession.
- > **Évolutivité.** Avec IP, vous pouvez commencer par la solution dont vous avez besoin aujourd'hui, puis évoluer facilement au fur et à mesure de l'évolution des besoins de l'entreprise.
- > **Souplesse.** Les produits de contrôle d'accès IP sont basés sur une architecture API ouverte et ne sont pas propriétaires. Cela signifie qu'il est possible d'utiliser et de combiner des composants à norme ouverte proposés par n'importe quel fournisseur.

9.3 Composants d'un système de contrôle d'accès

Les composants d'un système de contrôle d'accès englobent tout, du logiciel et du matériel de gestion de contrôle d'accès le plus élémentaire aux options les plus avancées.



Produits de contrôle d'accès comprenant (à partir de la gauche) : un interphone réseau, un lecteur, un contrôleur de porte, un module de relais E/S, et des informations d'identification : porte-clés, cartes d'accès et informations d'identification mobiles.

9.3.1 Contrôleurs de porte réseau

Un contrôleur de porte en réseau peut être considéré comme le cerveau d'un système de contrôle d'accès. Il déverrouille la porte et stocke également le logiciel de contrôle d'accès.

Quelle que soit la taille du système, un contrôleur de porte en réseau peut être installé pour chaque porte. Pour les installations ayant des conditions d'accès de base, la gestion peut être assurée par un logiciel intégré, tandis qu'un système plus complexe nécessitera un logiciel tiers.

Le contrôleur de porte peut être intégré avec d'autres systèmes tels que la vidéosurveillance, la détection d'intrusion, le pointage et la présence. Par exemple, lorsqu'une personne entre ou sort par une porte, le contrôleur de porte peut déclencher le début d'enregistrement d'une caméra. Ou, s'il est couplé à un système de CVC (chauffage, ventilation et climatisation), les informations d'un contrôleur de porte sur l'occupation du bâtiment peuvent être utilisées pour adapter le chauffage et la climatisation des locaux. Les contrôleurs de porte peuvent également être intégrés avec des interphones réseau pour des possibilités de communication vidéo et audio.

9.3.2 Lecteurs

Les lecteurs de carte constituent le moyen le plus courant pour permettre aux utilisateurs de s'identifier dans un système de contrôle d'accès. Cependant, les types d'identifiants ne doivent pas être limités aux cartes, en particulier lorsque des caméras et des stations de porte vidéo sur IP sont intégrées dans une solution de contrôle d'accès. L'accès peut être accordé en fonction de différents facteurs :

- > **Un objet détenu par l'utilisateur**, par exemple une carte à puce, un code QR, un porte-clé ou un téléphone portable.
- > **Un élément connu par l'utilisateur**, par exemple un code PIN ou la réponse à une question de sécurité.
- > **Des facteurs biométriques**, tels que les empreintes digitales ou les traits du visage.
- > **Une personne qui vérifie l'utilisateur**, par exemple un réceptionniste qui reconnaît l'image de l'utilisateur à la caméra.

La sécurité est renforcée lorsque plusieurs types de facteurs doivent être combinés pour autoriser l'accès.

9.3.3 Modules de relais d'E/S réseau

Un module de relais d'E/S réseau constitue un moyen simple et économique d'étendre les fonctionnalités des produits Axis. Ceci est particulièrement utile pour intégrer un contrôleur de

porte en réseau avec d'autres systèmes dans un bâtiment, mais peut également être utilisé avec d'autres systèmes de l'installation. Le module déclenche des actions lorsqu'il réagit aux entrées, telles que les signaux des détecteurs de mouvement PIR (capteur infrarouge passif) ou des interrupteurs de position de porte. Le module peut également fonctionner de manière autonome et planifiée, par exemple si vous voulez qu'une porte se déverrouille à une certaine heure tous les jours ou si vous voulez des règles spécifiques d'identification pour réguler l'accès d'un ascenseur à certains étages d'un bâtiment.

9.3.4 Systèmes de gestion d'accès

En matière de surveillance d'un système de contrôle d'accès, il y a différentes solutions logicielles. AXIS Camera Station Secure Entry offre une gestion intuitive des accès pour tous les besoins. Pour une solution basée sur l'accès des véhicules, il existe AXIS License Plate Verifier qui capture et valide automatiquement les plaques d'immatriculation pour une gestion simplifiée des portails. Il existe également toute une série de logiciels tiers pour la gestion du contrôle d'accès.

10. Visiophones réseau

Les interphones réseau sont utilisés en tant qu'outils de communication pour les visiteurs aux entrées, mais également en tant que points d'information ou téléphones d'urgence locaux. Il s'agit de périphériques fiables et faciles à installer qui augmentent la sécurité globale. Les interphones réseau sont basés sur une technologie IP ouverte normalisée qui simplifie l'intégration avec les autres systèmes, tels que le contrôle d'accès, la vidéosurveillance et les systèmes de communication basée sur IP (VoIP).

10.1 Dispositifs de communication multifonctions pour une sécurité accrue

Les interphones vidéo sur IP combinent la vidéosurveillance, la communication bidirectionnelle et le contrôle des entrées à distance dans un seul dispositif. Ils peuvent être placés au niveau des entrées et des sorties pour un grand nombre de visiteurs connus et inconnus, où ils autorisent les appels vidéo et vous permettent de contrôler à distance les accès via un ordinateur, un téléphone de bureau, un dispositif mobile ou une unité de réponse désignée. Les interphones sont également largement utilisés en tant que points d'aide ou téléphones d'urgence dans des zones plus vastes telles que les villes, les parcs ou les campus universitaires. Les interphones réseau peuvent facilement être connectés et alimentés par un réseau IP existant, afin de ne pas nécessiter de câblage spécial.



Interphones vidéo sur IP.

Les fonctions des interphones vidéo sur IP Axis comprennent :

- > **Vidéo de haute qualité.** Une caméra vidéo sur IP intégrée de haute qualité permet de bien visualiser la personne qui appelle au niveau des yeux. Avec des fonctions de caméra avancées telles que WDR (plage dynamique étendue), l'appelant est clairement visible, même dans de mauvaises conditions d'éclairage. L'analyse intégrée de la détection de mouvement vidéo peut être définie pour déclencher différents types d'alarmes, ainsi que des enregistrements vidéo. La prise en charge d'AXIS Camera Application Platform (ACAP) permet l'installation d'applications d'analyse supplémentaires.
- > **Audio bidirectionnel clair.** La communication est claire, ininterrompue et sans écho grâce au flux audio full-duplex avec réduction du bruit et suppression de l'écho. Les interphones peuvent également comporter des fonctions d'accessibilité pour les personnes malentendantes, telles qu'une boucle d'induction pour les appareils auditifs. Et grâce à l'analyse audio, les interphones peuvent déclencher des avertissements ou des enregistrements audio lorsque par exemple, une personne approche, ou si un coup de feu ou un comportement agressif est détecté.
- > **Contrôle des entrées.** Certains interphones peuvent fonctionner en tant que lecteur de carte et de code PIN pour l'admission des employés et d'autres personnes autorisées sans autre intervention. Les visiteurs inconnus peuvent utiliser le clavier de l'interphone pour faire une demande d'accès en appelant la réception, la personne à laquelle ils rendent visite ou le personnel de sécurité. Les destinataires de l'appel peuvent alors voir, parler et ouvrir la porte aux visiteurs, directement ou à distance depuis un téléphone portable, un téléphone IP ou un système de gestion vidéo.
- > **Intégration.** En tant que périphériques IP, les interphones réseau s'intègrent facilement à d'autres systèmes. La prise en charge du protocole SIP permet l'intégration à la téléphonie IP, ce qui permet de transmettre la vidéo et le son depuis l'interphone et de répondre aux appels à partir d'un téléphone de bureau ou d'un périphérique mobile. Les appels peuvent également être reçus via la plupart des systèmes de gestion vidéo sur IP, permettant au client d'exploiter la solution système qu'il préfère. Dans les systèmes plus complexes, par exemple dans les centres logistiques ou les aéroports, les interphones sont un complément utile dans une solution intégrée avec des caméras réseau, des systèmes de contrôle d'accès, des alarmes anti-intrusion et d'autres applications de sécurité. Les interphones peuvent disposer d'un grand nombre de ports, de relais et de protocoles pris en charge qui vous permettent de connecter des capteurs externes, d'activer des éclairages, d'ouvrir des portes, de déclencher des caméras externes ou d'émettre des alarmes.

11. Dispositifs portables

Les caméras-piétons documentent les événements et capturent des preuves précieuses. Elles sont également un moyen efficace de dissuader les mauvais comportements et d'avoir une influence positive sur les actions des porteurs de caméra et du public. Les caméras-piétons Axis offrent une qualité vidéo et audio supérieure, et fournissent ainsi des preuves faciles à comprendre et à interpréter qui seront jugées acceptables par les tribunaux. Le système de caméras-piétons Axis repose sur des normes ouvertes de flexibilité et d'évolutivité. Il peut être utilisé avec différentes destinations de contenu et utilise un cryptage de bout en bout pour la cybersécurité. AXIS Body Worn Live permet de diffuser en direct des vidéos, du son et des métadonnées à partir des caméras-piétons Axis. Sécurisée et fiable, la solution favorise les prises de décisions éclairées des opérateurs et renforce le sentiment de sécurité des porteurs des caméras.

11.1 Objectif des caméras-piétons

Avec une caméra-piéton, il est possible d'enregistrer les incidents partout où ils surviennent. Fixée sur le corps, par exemple, d'un livreur, d'un conducteur de train, d'un employé de gare ou d'un agent de sécurité, la caméra est présente à l'endroit où elle est requise et elle peut capturer des événements qui n'auraient jamais été capturés par des caméras postées à un endroit fixe.

Un enregistrement produit par une caméra-piéton comprend des éléments de preuve fiables et sécurisés, montrant objectivement ce qui s'est passé sur la scène d'un incident. Les séquences peuvent être utilisées dans des enquêtes internes et au cours de procédures judiciaires, mais également dans le cadre de discussions et d'analyses lors de la formation du personnel de surveillance sur la manière de réagir aux situations qu'ils sont susceptibles de rencontrer. Une caméra-piéton facilite également la documentation des livraisons ou autres tâches, qui ont été gérées conformément aux procédures appropriées.

L'utilisation de caméras-piétons a une incidence sur le comportement des porteurs de caméra et des personnes avec lesquelles ils interagissent. La conscience d'être filmé semble donner aux

personnes l'impression de la présence d'un témoin numérique à leur actes, qui sont ainsi moins enclines à mal se comporter, alors que les personnes qui portent la caméra ont davantage propension à rester calmes et à se conformer aux réglementations.



L'utilisation de caméras-piétons peut aider à garder le contrôle de certaines situations lorsque le porteur de la caméra et le public sont tous deux au courant que leur comportement et leurs décisions peuvent avoir pour témoin un tiers.

11.2 Caméras-piétons



Les caméras-piétons Axis existent en noir, en blanc ou en gris, ce qui leur permet de se fondre dans l'environnement ou de se démarquer des vêtements. Ces modèles sont adaptés à une utilisation dans tout type de secteur d'activité.

Les caméras-piétons d'Axis offrent des images nettes et un son clair. Elles sont légères, robustes et résistantes à l'eau. Elles démarrent et s'arrêtent d'un simple toucher et bénéficient d'une mémoire

tampon jusqu'à 120 secondes avant le début d'un enregistrement. La longue durée de vie des batteries, la charge USB et le rechargement rapide les rendent encore plus faciles à utiliser.

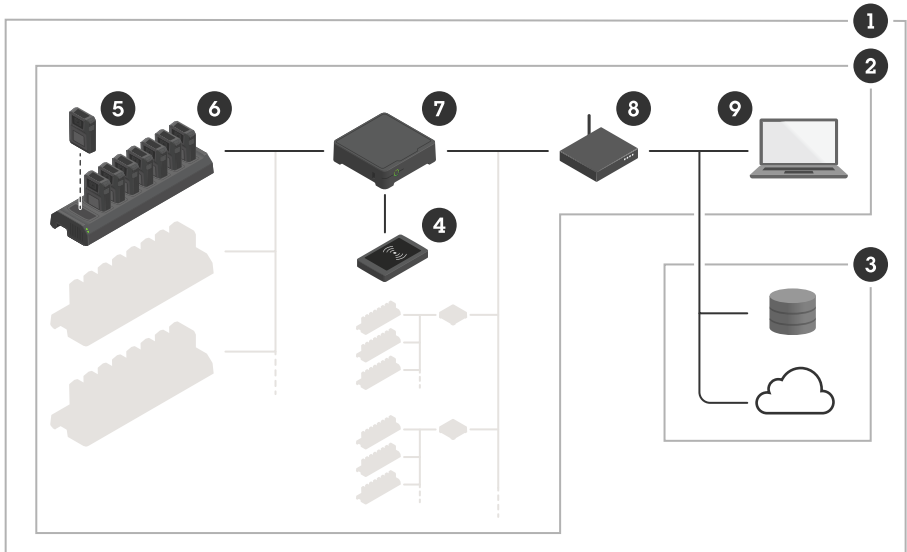
Choisissez un modèle noir ou blanc, selon que vous souhaitez ou non utiliser une caméra qui se démarque des vêtements à des fins de dissuasion. Les mini-capteurs peuvent être fixés à la caméra et être montés sur un casque ou sur des vêtements avec des fixations standard, ce qui permet filmer de manière pratique et discrètement.

Les caméras-piétons stockent les données de localisation récupérées auprès des satellites de navigation dans leurs enregistrements. Le matériel vidéo étant relié aux coordonnées géographiques où il a été filmé, le suivi de l'emplacement peut être activé et la valeur probante des enregistrements peut être accrue de manière significative. Les caméras-piétons Axis bénéficient également de la technologie Axis Zipstream qui vous permet de stocker une grande quantité de séquences vidéo sans avoir à compromettre la qualité vidéo.

Avec AXIS Body Worn Live, l'utilisateur qui démarre un enregistrement peut également activer immédiatement un flux audio et vidéo en direct depuis sa caméra vers l'opérateur, lequel peut ensuite suivre les événements en temps réel. Pour une solution sans intervention, les sociétés peuvent choisir la version hébergée par Axis, basée sur le cloud. Elles peuvent également héberger elles-mêmes AXIS Body Worn Live si les règles en vigueur excluent l'hébergement sur le cloud. L'opérateur peut prendre des décisions éclairées telles que l'envoi de renforts, et les coordonnées GPS indiquent où l'envoyer. L'opérateur peut envoyer une notification à l'utilisateur, qui est alors informé qu'il dispose d'un soutien et qu'il peut se concentrer sur l'incident plutôt que sur la communication avec le siège. Les notifications peuvent prendre la forme de bip ou, sur certains modèles, de symbole sur l'écran LCD de la caméra.

11.3 Solution de caméra-piéton Axis

Après utilisation de la caméra-piéton, vous la placez dans sa station d'amarrage. Le contrôleur système commence instantanément à transférer les données de la caméra vers la destination du contenu de votre choix, et la batterie de la caméra démarre en charge. Le contrôleur système maintient également les caméras à jour avec la dernière version d'AXIS OS et d'autres paramètres, tout en surveillant l'intégrité globale de la solution de caméras-piétons Axis.



Composants d'une solution caméra-piéton Axis.

La solution de caméras-piétons Axis (1) se compose d'un ou de plusieurs systèmes de caméras-piétons Axis (2) connectés à une destination de contenu (3). Le système de caméras-piétons ne fonctionne que s'il est connecté à une destination de contenu.

Le système de caméra-piéton Axis (2) se compose de caméras-piétons Axis (5), de stations d'accueil Axis (6), de contrôleurs système Axis (7) et d'AXIS Body Worn Manager (9).

Un lecteur RFID optionnel (4) peut être connecté au contrôleur système. Il permet à l'utilisateur de s'attribuer n'importe quelle caméra-piéton disponible, en utilisant son étiquette d'auto-attribution.

AXIS Body Worn Manager (9) est une application Web à partir de laquelle vous pouvez configurer et gérer votre système de caméra-piéton.

Des normes ouvertes et des stations d'amarrage à faible coût, avec un contrôleur système séparé, offrent un moyen simple et économique d'ajouter des caméras et des utilisateurs au système si nécessaire. L'application pour appareils mobiles AXIS Body Worn Assistant, se connecte directement à la caméra-piéton pour, par exemple, regarder la vidéo enregistrée.

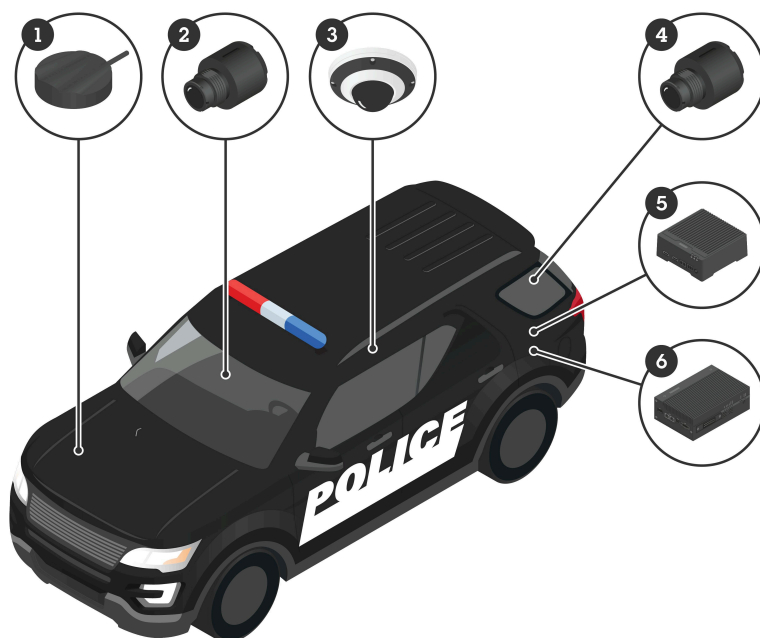
La solution caméra-piéton Axis est prise en charge par différents types de destinations de contenu : systèmes de gestion des preuves (EMS), les systèmes de gestion vidéo (VMS) et les serveurs

multimédia. Vous pouvez utiliser une solution Axis de bout en bout incluant AXIS Camera Station ou Axis Case Insight, ou tout système VMS ou EMS tiers, sur site ou dans le cloud.

Les caméras-piétons Axis prennent en charge les normes officielles de cybersécurité du FBI avec cryptage de bout en bout.

11.4 Solution embarquée

La solution de vidéosurveillance embarquée Axis pour les forces de l'ordre intègre une surveillance embarquée robuste et fiable avec les caméras-piétons Axis. Les caméras et les microphones de cette solution diffusent des vidéos et de l'audio pour une utilisation médico-légale et fournissent une connaissance complète de la situation à l'intérieur des véhicules et à l'extérieur. Tous les documents et informations enregistrés sont protégés par des fonctionnalités de cybersécurité intégrées.



Une installation typique sur un véhicule, incluant : 1) Antenne, 2) Caméra de pare-brise, 3) Caméra à boîtier fixe, 4) Caméra de lunette arrière, 5) Unité principale, 6) Ordinateur robuste.

12. Fonctions d'analyse

Une caméra peut être bien plus qu'une simple source vidéo. Les analyses transforment la vidéo, l'audio et d'autres données en informations utilisables. Et, du fait du développement de l'intelligence artificielle (IA), l'analyse est devenue un élément de différenciation majeur de la vidéosurveillance et la surveillance, ce qui facilite la sécurité, la sûreté et l'efficacité opérationnelle.

12.1 L'analytique au service d'un monde plus sûr et plus intelligent

Les fonctions d'analyse servent à accroître la sécurité et la protection et à optimiser la gestion opérationnelle et l'efficacité. Elles peuvent également être conçues pour protéger activement la confidentialité des personnes dans le cadre d'une surveillance.

Dans la mesure ou l'accès à des données structurées et étiquetées met en évidence les détails essentiels d'une scène, la solution permet d'automatiser les actions et d'orienter les décisions dans la bonne direction. Elle réduit également les ressources nécessaires à l'analyse des données et à l'élaboration de prévisions basées sur les tendances et les schémas.

Les événements ou alertes basés sur des règles que l'utilisateur configure pour déclencher des actions et des alarmes automatisées permettent à la fois de gagner en efficacité opérationnelle et d'améliorer la télésurveillance. L'émission d'une alarme lorsqu'une personne traverse une ligne virtuelle dans une zone à accès restreint ou l'ouverture automatique d'une barrière à chaque arrivée d'un véhicule autorisé permet d'économiser des ressources.

L'analyse peut également fournir des informations sur les objets présents dans la scène et leurs attributs, tels que la présence de chapeaux ou de sacs, et d'autres caractéristiques (couleur, forme ou vitesse, par exemple). Les métadonnées d'événements et les métadonnées de scène sont appelées *métadonnées d'analyse*. Elles sont extrêmement utiles dans le cadre de la recherche d'énormes quantités de vidéos. Elles peuvent également être utilisées pour détecter des modèles et des tendances, générer des statistiques ou fournir des informations exploitables supplémentaires et même prévoir des événements futurs.

Les cas d'utilisation de l'analyse ne cessent de se développer et les possibilités futures sont pratiquement infinies. Ce chapitre présente certains des cas d'utilisation les plus importants aujourd'hui.

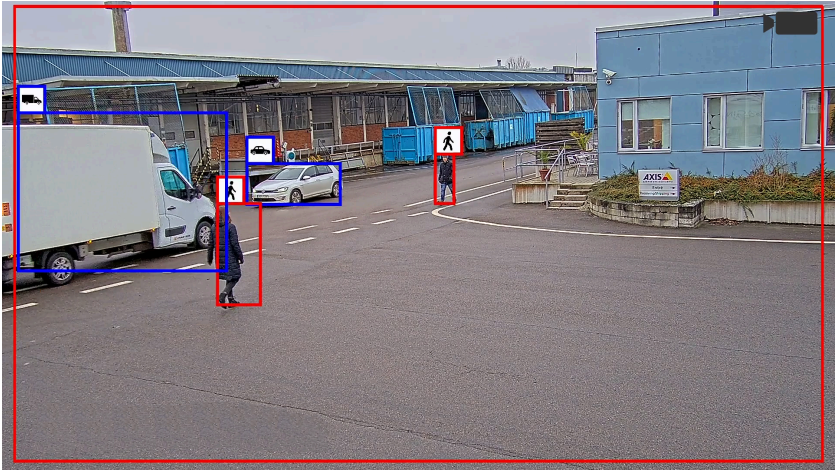
12.2 Avantages des fonctions d'analyse

L'analyse renforce la sécurité, la sûreté et l'efficacité du fonctionnement et peut fournir une intelligence économique précieuse. Cela peut vous aider à :

- > **Réagir plus rapidement aux incidents critiques.** Avec des événements et des notifications en temps réel et une image plus nette de la scène, vous pourrez intervenir plus rapidement dans les moments cruciaux. Les réponses peuvent même être automatisées.
- > **Prendre des décisions plus éclairées.** Il existe des outils d'analyse pour prendre des décisions axées sur les données, optimiser les opérations, éliminer les points à risque et améliorer la rentabilité en utilisant des informations exploitables.
- > **Utiliser au mieux les ressources.** En automatisant les tâches que les machines peuvent réaliser, voire mieux que les humains, les opérateurs pourront se concentrer sur des tâches plus avancées.
- > **Trouver ce que vous recherchez.** Accélérez les enquêtes en permettant une recherche efficace dans plusieurs flux vidéo pour trouver des objets, leurs événements ou des incidents d'intérêt pour une scène.
- > **Empêcher proactivement les événements indésirables.** L'analytique peut favoriser des actions préventives en envoyant des signaux précoces à propos de situations potentiellement à risque, comme une présence suspecte ou un véhicule volé dans la zone.

12.2.1 Surveillance en temps réel

L'analyse implique d'automatiser le visionnage de plusieurs heures de vidéo, d'en extraire les informations utiles et de prendre les mesures appropriées. Des objets tels que les humains et les véhicules peuvent être automatiquement détectés, puis surveillés pour trouver les événements importants que vous souhaitez identifier ou auxquels le système doit réagir automatiquement. Les actions automatiques peuvent, par exemple, consister à informer le personnel, démarrer un enregistrement vidéo, ouvrir une porte ou démarrer une annonce pré-enregistrée.



AXIS Object Analytics offre la détection et la classification d'objets basées sur l'AI.

Dans un environnement commercial ou similaire, l'analyse peut contribuer à rendre la gestion du personnel plus efficace. Par exemple, une longue file d'attente pourrait déclencher une annonce telle que : « Plus de personnel demandé aux caisses, s'il vous plaît ». Le comptage des personnes et des véhicules fournit des informations précieuses qui peuvent vous aider à mieux comprendre les tendances en matière de visiteurs et les schémas de trafic. Ces données vous permettent d'évaluer la performance du site, de surveiller le flux de circulation, d'optimiser la capacité de stationnement et, en fin de compte, d'optimiser vos activités commerciales.

L'analyse peut également être utilisée pour la reconnaissance des plaques d'immatriculation, ce qui la rend très efficace pour le contrôle d'accès, la gestion des parkings, l'application du code de la route, etc. Ces solutions permettent de suivre les véhicules impliqués dans des activités criminelles, des excès de vitesse ou des vols, tout en prenant en charge des tâches quotidiennes telles que l'automatisation de la perception des péages, la surveillance des flux de trafic, un accès sans problème dans les parkings et une planification proactive du trafic grâce à des informations fondées sur des données.



AXIS License Plate Verifier permet la reconnaissance de plaque d'immatriculation en temps réel, optimisée par l'IA, pour un éventail d'applications de circulation, y compris l'accès aux véhicules, la recherche de véhicules et des solutions de stationnement.

12.2.2 Recherche efficace

L'utilisation d'outils d'analyse pour améliorer la recherche est l'un des cas d'utilisation les plus courants et les plus précieux, car il permet de sauvegarder un temps et des ressources considérables. L'analyse accélère divers types de recherches en rationalisant les requêtes portant sur des objets, des attributs et des activités spécifiques. Dans les centres logistiques, par exemple, l'analyse permet de localiser rapidement les colis, ce qui réduit considérablement le temps de recherche manuelle. Dans le commerce, elle peut aider à découvrir les comportements des clients, ce qui permet aux entreprises d'optimiser le fonctionnement, l'optimisation des stratégies de merchandising et l'amélioration de l'expérience globale d'achat. Dans le cadre d'enquêtes judiciaires, l'analyse contribue à la recherche d'indices probants tels que les véhicules ou les individus liés à un incident, et peut même aider les enquêteurs à suivre les mouvements et les activités des suspects. Alimentées par l'IA, ces solutions extraient des informations détaillées, permettant des recherches rapides, précises et efficaces dans un large éventail d'industries. En outre, l'analyse peut s'intégrer aux systèmes et flux de travail existants, tels que les systèmes de surveillance, les bases de données et les outils d'investigation, pour soutenir la recherche et l'analyse.

12.2.3 Repérer les tendances et les schémas

Les analyses peuvent fournir des informations et des statistiques utiles et exploitables pour améliorer les opérations et aider à prendre des décisions plus éclairées, par exemple, dans la gestion des flux de trafic ou des mouvements de visiteurs. Comme les analyses utilisent des métadonnées

pour décrire le contenu d'une scène, elles peuvent vous aider à collecter, organiser et stocker le contenu intéressant pour identifier des tendances et des modèles.

12.2.4 Confidentialité

Grâce au masquage intelligent, vous pouvez brouiller les visages, les corps entiers et les plaques d'immatriculation dans une scène pour plus de confidentialité. Cela signifie que les identités des individus ou des véhicules sont masquées alors que leurs mouvements peuvent toujours être observés. Avec le masquage basé sur l'IA, la vidéo en direct est analysée pour des objets spécifiques et vous pouvez masquer soit les objets, soit l'arrière-plan. Ce type d'analyse est spécifiquement conçu pour protéger la vie privée des personnes, ce qui vous permet de surveiller des activités sans collecter de données personnelles.

12.3 Architecture système : où la vidéo est-elle analysée ?

Lors de la conception d'un système d'analyse vidéo, il est essentiel de savoir où traiter les données d'analyse. Il existe trois options principales : sur la caméra, sur un serveur ou dans le cloud.

> **Sur la caméra.** L'analyse vidéo en périphérie est utile pour de nombreuses raisons :

- **Plus grande précision :** L'exécution d'une analyse sur des données vidéos non compressées permet d'obtenir une meilleure précision car la qualité vidéo n'est pas dégradée.
- **Une réponse et une action rapides :** Les solutions edge-based minimisent la latence en traitant les données près de leur source, évitant ainsi les retards causés par la transmission vers des serveurs distants ou des plateformes cloud. Cela active des alertes en temps réel qui, associées à des déclenchements automatisés, permettent des temps de réponse rapides et une action immédiate.
- **Adaptation facile :** L'exécution d'analyses à la périphérie facilite l'évolutivité en réduisant la charge de traitement des systèmes centralisés. Ceci est particulièrement avantageux car le traitement de toutes les données vidéo dans le cloud peut s'avérer très coûteux. En outre, l'analyse réduit les coûts des serveurs et les besoins de maintenance.
- **Réduction de la charge du réseau et de la pression sur l'infrastructure :** En évitant de transférer des données inutiles, vous réduirez le trafic sur le réseau, les besoins en bande passante et la demande en matériel, ce qui se traduira en fin de compte par d'importantes économies.

- **Confidentialité améliorée** : Avec l'exécution d'analyses en périphérie, vous avez la possibilité d'envoyer uniquement des données anonymisées et/ou des alertes sur le réseau, ce qui peut améliorer la confidentialité.
- > **Sur un serveur**. Lorsque vous avez besoin de beaucoup de puissance de traitement, l'analyse vidéo sur des serveurs dédiés est souvent requise. Les serveurs peuvent aussi analyser simultanément plusieurs flux vidéo issus d'une diversité de sources et rechercher dans les volumes gigantesques d'informations de base de données.
- > **Dans le cloud**. Une autre option consiste à envoyer les vidéos directement des caméras vers le cloud. Mais le traitement de toutes les données vidéo dans le nuage peut entraîner des coûts importants en raison des frais de stockage, de transfert et de traitement des données, ce qui peut limiter sa pertinence pour certaines applications. Le cloud computing nécessite souvent une connexion Internet robuste et fiable, qui n'est pas toujours disponible dans toutes les situations. En revanche, le cloud computing peut traiter plusieurs flux vidéo en même temps. Il est également facile à adapter. Certaines entreprises doivent conserver toutes les données dans leurs locaux en raison de la réglementation et sont donc peu enclines à envisager une solution cloud.
- > **Solution hybride**. Un système hybride qui combine le traitement à la périphérie, dans le cloud et sur des serveurs sur site, est souvent la meilleure approche car il tire parti des atouts de chaque technologie. Dans les systèmes hybrides, la classification des objets peut intervenir dans les caméras, alors que des algorithmes qui nécessitent plus de puissance sont exécutés sur des serveurs ou dans le cloud. La répartition de la charge de traitement entre la périphérie de réseau et les serveurs produit des systèmes beaucoup plus évolutifs. En particulier, l'ajout d'une caméra dotée de capacités d'analyse à la périphérie évite d'avoir à augmenter la puissance de calcul des serveurs.

12.4 Facilité d'utilisation des images : base d'excellentes performances analytiques

Les performances analytiques dépendent de nombreux facteurs, dont la plupart peuvent être optimisés une fois que vous avez pris conscience de leur impact. Ces facteurs sont, par exemple, le matériel de la caméra, la qualité de l'image, la dynamique de la scène et le niveau d'éclairage, ainsi que la configuration, la position et la direction de la caméra.

Les outils d'analyse, quelle que soit leur puissance, s'appuient sur les technologies qui les prennent en charge. Sans des images de qualité et une classification précise (ou un étiquetage) des données, les résultats obtenus ne sont pas acceptables. Des éléments tels que le filtrage du bruit, l'amélioration du contraste et le flou de mouvement ont une incidence sur la précision de l'analyse. Par faible luminosité, la qualité des images peut être problématique. Les technologies de traitement d'image avancées telles que Lightfinder, Forensic WDR et OptimizedIR ont un rôle majeur. Axis

Scene Intelligence a été développé spécifiquement pour améliorer la compréhension de la scène à la périphérie grâce à une qualité d'image supérieure et à une analyse basée sur l'IA pour extraire les détails cruciaux.

Il va presque sans dire que les mises à niveau rapides des logiciels – ou la *maintenance numérique* – sont importantes pour une analyse performante. Il est cependant un aspect qui reçoit souvent moins d'attention, c'est l'*entretien physique*. Or, une vue dégagée de la scène est primordiale pour les fonctions d'analyse. Une qualité d'image médiocre, qu'elle soit due aux conditions environnementales ou à la dégradation de l'équipement, peut compromettre les résultats. Ainsi, pour vous aider à tirer le meilleur parti de votre investissement dans l'analyse, nous recommandons une approche proactive de maintenance des caméras, tant numérique que physique.

Pour aider à maintenir une qualité d'image optimale, AXIS Image Health Analytics surveille et analyse en permanence les images de la caméra, détectant les problèmes susceptibles d'avoir un impact sur les performances d'analyse. Si un problème est détecté, tel qu'une image bloquée, brouillée, sous-exposée ou redirigée, le système envoie une notification, ce qui permet une action corrective rapide.

12.5 Intelligence artificielle

L'intelligence artificielle (IA) est un concept assez vaste appliqué aux machines qui peuvent résoudre des tâches complexes tout en faisant preuve de comportements apparemment intelligents. Contrairement à la programmation traditionnelle, qui repose sur des instructions explicites et des règles définies par l'homme, l'IA permet aux machines de traiter de grandes quantités de données et de s'adapter à de nouvelles situations de manière autonome. Par rapport à la programmation traditionnelle, l'avantage de l'IA est sa capacité à traiter beaucoup plus de données que les humains, ce qui se traduit dans des applications plus précises. Le machine learning et le deep learning sont des sous-catégories de l'IA.

Le machine learning utilise des algorithmes d'apprentissage statistiques pour développer des systèmes qui peuvent apprendre et s'améliorer pendant la phase de formation sans être explicitement programmés, par exemple, pour déterminer ce qui se passe dans les images ou les flux vidéo (vision artificielle). La vision par ordinateur classique repose sur l'extraction manuelle d'éléments, l'homme définissant les caractéristiques à détecter dans les images ou les flux vidéo. L'algorithme apprend à combiner ces fonctionnalités via l'exposition à de grandes quantités de données de formation collectées et annotées par des humains. Les données alimentent le système jusqu'à ce que le programme soit suffisamment formé pour détecter les besoins. Une fois le processus terminé, le programme n'apprendra plus rien de nouveau.

Le deep learning est l'apprentissage des fonctionnalités par les données et de la méthode pour les combiner. Tout comme le cerveau humain, l'algorithme peut apprendre les structures très profondes des combinaisons de fonctionnalités en chaîne, qui sont simulées dans des réseaux neuronaux artificiels (le type d'algorithme le plus courant dans le deep learning). Les algorithmes de deep learning peuvent exploiter un plus grand nombre de combinaisons de caractéristiques, ce qui leur permet de s'attaquer à des tâches plus complexes et d'atteindre une plus grande précision.

Les caméras dotées d'une unité de traitement deep learning (DLPU) offrent une classification plus granulaire des objets détectés. Cette capacité s'avère très utile lorsque le facteur temps est critique, car la classification a lieu directement sur la caméra. Les analyses basées sur le deep learning sont idéales pour les scènes très actives et les exigences plus strictes. Elles offrent également de meilleures capacités de détection et de classification pour les personnes se tenant dans des positions inhabituelles (accroupies, par exemple) ainsi que les objets partiellement visibles. En disposant de données d'entraînement adéquates, les algorithmes de deep learning peuvent détecter avec précision les attributs des objets, notamment la couleur des vêtements, la présence d'un casque de sécurité, la détection d'un sac, et bien plus encore.

12.6 Plateforme d'applications AXIS Camera (ACAP)

La plupart des périphériques Axis prennent en charge notre plateforme d'applications ouverte, AXIS Camera Application Platform (ACAP). Cette puissante plateforme utilise des chaînes d'outils bien connues, des API open-source standard et des langages de programmation de haut niveau pour permettre le développement, le déploiement et l'intégration d'applications en périphérie, ce qui permet d'élaborer des solutions adaptées aux besoins spécifiques des clients. Les applications peuvent donc s'exécuter là où elles optimisent le mieux les performances et minimisent la bande passante. Maximiser l'efficacité du traitement et l'efficacité totale du système est important à la fois pour l'utilisateur final, qui bénéficie d'un système plus puissant et rationalisé, et pour les développeurs, qui peuvent s'axer sur l'application plutôt que sur la plateforme. Cela signifie que les développeurs peuvent véritablement innover sur les périphériques Axis.

13. Technologies réseau

Différentes technologies de réseau sont utilisées pour prendre en charge et fournir les nombreux avantages offerts par un système de vidéo sur IP. Ce chapitre commence par une discussion sur les réseaux locaux, et en particulier le réseau Ethernet et ses composants. L'utilisation de Power over Ethernet est également abordée.

La communication Internet est ensuite traitée, avec des discussions au sujet de l'adressage IP (Internet Protocol), notamment comment les produits vidéo réseau sont accessibles sur Internet. Nous présentons également les réseaux locaux virtuels, la qualité du service, ainsi qu'un aperçu des protocoles de transport de données utilisés dans la vidéo réseau.

13.1 Réseaux locaux et Ethernet

Un réseau local (LAN) est un groupe d'ordinateurs qui sont connectés dans une zone localisée pour communiquer entre eux et partager des ressources telles que des imprimantes. Les données sont envoyées sous forme de paquets, et différentes technologies régulent la transmission des paquets. La technologie LAN la plus répandue est Ethernet, qui est spécifiée dans la norme IEEE 802.3. D'autres types de technologies de réseaux LAN comprennent l'anneau à jeton et FDDI (Fiber Distributed Data Interface).

Aujourd'hui, Ethernet utilise une topologie en étoile dans laquelle les nœuds individuels (périphériques) sont connectés les uns aux autres via des équipements de réseau actifs tels que des commutateurs. Un LAN peut comporter plusieurs milliers de périphériques en réseau.

Il convient de toujours développer un réseau avec une capacité supérieure à celle requise. Pour pérenniser un réseau, vous pouvez le concevoir de sorte qu'il n'utilise que 30 % de la capacité totale lors de la première mise en service. Comme de plus en plus d'applications s'exécutent sur des réseaux, les performances des réseaux devront être de plus en plus élevées. Les commutateurs de

réseau sont faciles à mettre à niveau après quelques années, mais le câblage est généralement beaucoup plus difficile à remplacer.

13.1.1 Types de réseaux Ethernet

Les types de réseaux Ethernet les plus courants dans l'industrie de la vidéosurveillance sont les suivants : Ils peuvent être basés sur des câbles à paires torsadées ou à fibres optiques.

Fast Ethernet. Peut transférer des données à un débit de 100 Mbit/s. L'ancien Ethernet 10 Mbit/s est encore installé et utilisé, mais ces réseaux ne fournissent pas la bande passante nécessaire pour certaines applications de vidéo sur IP. La plupart des appareils sont équipés d'une interface Ethernet 10BASE-T/100BASE-TX, plus communément appelée interface 10/100, qui prend en charge à la fois le débit 10 Mbits/s et Fast Ethernet. Le type de câble à paires torsadées prenant en charge Fast Ethernet est appelé câble Cat-5.

Gigabit Ethernet. Prend en charge un débit de données de 1 000 Mbit/s (1 Gbit/s) et est désormais plus couramment utilisé que Fast Ethernet. Ethernet 1 ou 10 Gbit/s peut être nécessaire pour le réseau de base qui connecte de nombreuses caméras réseau. Le câble à paires torsadées prenant en charge Gigabit Ethernet est de type Cat-5e, dans lequel les quatre paires de fils torsadés sont utilisées pour atteindre les débits de données élevés. Les catégories de câbles Cat-5e ou supérieures sont recommandées pour les systèmes de vidéo sur IP. La plupart des interfaces sont rétrocompatibles avec Ethernet 10 et 100 Mbits/s et sont communément appelées interfaces 10/100/1000. Pour la transmission sur de plus grandes distances, des câbles à fibre optique tels que 1000BASE-SX (jusqu'à 550 m/1804 pi.) et 1000BASE-LX (jusqu'à 550 m avec fibres optiques multimodes et 5 000 m ou 3 miles avec fibres monomodes) peuvent être utilisés.

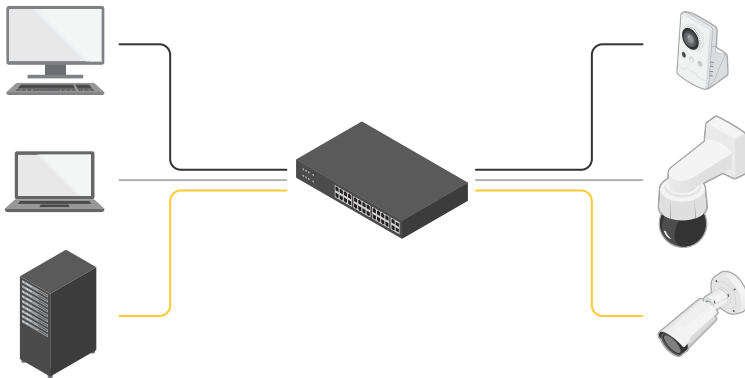
10 Gigabit Ethernet. Prend en charge un débit de 10 Gbit/s (10 000 Mbit/s). 10GBASE-LX4, 10GBASE-ER et 10GBASE-SR basés sur un câble à fibre optique peuvent être utilisés pour couvrir des distances allant jusqu'à 10 km (6 miles). Un câble de très haute qualité (Cat-6a ou Cat-7) est requis pour les solutions à paire torsadée. Ethernet 10 Gbit/s est principalement utilisé pour les réseaux dorsaux dans les applications qui nécessitent des débits de données élevés.

13.1.2 Connexion de périphériques et de commutateurs réseau

La mise en réseau de plusieurs périphériques dans un LAN nécessite un équipement avec des commutateurs réseau. La principale fonction d'un commutateur est de transmettre les données d'un périphérique à l'autre sur le même réseau, ce qu'il fait efficacement en dirigeant les données d'un périphérique directement vers le périphérique cible, sans affecter les autres périphériques du même réseau.

Un commutateur réseau fonctionne en enregistrant l'adresse MAC (Media Access Control) de chaque périphérique qui s'y connecte. Chaque périphérique de mise en réseau possède une adresse MAC unique, composée d'une série de chiffres et de lettres en notation hexadécimale, telle que définie par le fabricant. L'adresse se trouve souvent sur l'étiquette du produit. Lorsqu'un commutateur réseau reçoit des données, il les transmet uniquement au port connecté à l'appareil avec l'adresse MAC destinataire appropriée.

Les commutateurs réseau indiquent généralement leurs performances en débits par port, en débits internes ou en « backplane » (en débit binaire et en paquets par seconde). Les débits de port indiquent les débits maximums sur des ports spécifiques. La vitesse d'un commutateur, par exemple 100 Mbit/s, correspond ainsi souvent à la performance de chaque port.



Dans un commutateur réseau, le transfert de données est géré très efficacement, car le trafic de données peut être dirigé d'un périphérique à un autre sans affecter les autres ports du commutateur.

Un commutateur réseau prend normalement en charge différents débits de données simultanément. Auparavant, les débits les plus courants étaient de 10/100 Mbit/s, prenant en charge les normes 10 Mbit/s et Fast Ethernet. Aujourd'hui, cependant, les commutateurs réseau ont souvent des interfaces 10/100/1000, prenant ainsi en charge 10 Mbit/s, Fast Ethernet et Gigabit Ethernet simultanément. Le débit et le mode de transfert entre le port d'un commutateur et un périphérique connecté sont normalement négociés automatiquement, grâce à quoi le débit de données commun le plus élevé et le meilleur mode de transfert sont utilisés. Le commutateur réseau permet également aux périphériques connectés de fonctionner en mode full-duplex, c'est-à-dire pour envoyer et recevoir des données en même temps, ce qui améliore les performances.

Les commutateurs réseau peuvent avoir des caractéristiques ou des fonctions différentes. Par exemple, certains peuvent inclure la fonctionnalité de routeur et de nombreux modèles prennent en charge l'alimentation Power over Ethernet. Un commutateur incluant la qualité de service peut contrôler la quantité de bande passante utilisée par les différentes applications.

13.1.3 Alimentation par Ethernet

Power over Ethernet (PoE) est utilisé pour alimenter les périphériques connectés à un LAN Ethernet via le même câble que celui utilisé pour la communication de données. PoE est largement utilisé pour alimenter les téléphones IP, les points d'accès sans fil et les périphériques réseau comme une caméra.

PoE a pour principal avantage de réduire les dépenses. Il n'est pas nécessaire d'engager un électricien agréé et d'installer une fréquence d'alimentation séparée pour utiliser le PoE, ce qui est avantageux, en particulier dans les zones difficiles d'accès. Le fait que le câblage électrique ne soit pas nécessaire permet d'économiser potentiellement des centaines d'euros par caméra. PoE facilite également le déplacement d'une caméra vers un nouvel emplacement ou l'ajout de nouvelles caméras à un système de vidéosurveillance existant.

En outre, PoE permet de sécuriser davantage le système de surveillance. Un système avec PoE peut être alimenté à partir de la salle des serveurs, qui est souvent sauvegardée par un onduleur UPS (alimentation continue). Ainsi, le système peut rester opérationnel même pendant une panne d'électricité.

En raison des avantages de PoE, il est recommandé de l'utiliser avec autant de périphériques que possible. L'énergie disponible à partir du commutateur ou de l'injecteur PoE doit être suffisante pour les périphériques connectés, et les périphériques doivent prendre en charge la classification de puissance.

Norme 802.3af, PoE+ et High PoE

La plupart des appareils PoE actuels sont conformes à la norme IEEE 802.3af publiée en 2003. La norme IEEE 802.3af utilise des câbles Cat-5 standard ou supérieurs et garantit que le transfert de données n'est pas affecté. Dans la norme, l'appareil qui fournit l'alimentation est appelé équipement d'alimentation (PSE). Cela peut être un commutateur ou injecteur compatible PoE. L'appareil qui reçoit l'alimentation est appelé appareil alimenté (PD). Souvent, cette fonctionnalité est intégrée au périphérique réseau. Elle peut également être fournie à partir d'un séparateur autonome.

La rétrocompatibilité avec les périphériques réseau non-PoE est garantie. La norme inclut une fonction d'identification automatique de la prise en charge de la technologie PoE par le périphérique, et l'alimentation n'est fournie à l'appareil que lorsque cette prise en charge est confirmée. Cela signifie également que le câble Ethernet connecté à un commutateur PoE ne fournira aucune alimentation s'il n'est pas connecté à un périphérique compatible PoE. Cela élimine le risque d'électrocution lors de l'installation ou de la reconnexion d'un réseau.

Il y a quatre paires de fils torsadés dans un câble à paires torsadées. PoE peut utiliser soit les deux paires de fils « de rechange », soit il peut superposer le courant sur les paires utilisées pour la transmission de données. En général, les commutateurs avec PoE intégré alimentent les deux paires de fils utilisées pour le transfert des données, alors que les injecteurs utilisent habituellement les deux paires de rechange. Un appareil alimenté (PD) prend en charge ces deux options.

Selon IEEE 802.3af, un équipement d'alimentation fournit une tension de 48 V CC avec une puissance maximale de 15,4 W par port. Étant donné qu'il y a une certaine perte de puissance sur un câble à paires torsadées, seuls 12,95 W sont garantis comme étant disponibles pour le DP. La norme IEEE 802.3af spécifie différentes catégories de performances pour les DP.

Les PSE tels que les commutateurs et les injecteurs fournissent normalement une certaine quantité d'énergie, généralement de 300 à 500 W. Sur un commutateur à 48 ports, cela représente 6 à 10 W par port, si tous les ports sont connectés à des périphériques utilisant le PoE. À moins que les PD ne prennent en charge la classification de l'alimentation, 15,4 W doivent être réservés pour chaque port utilisant le PoE, ce qui signifie qu'un commutateur de 300 W ne peut alimenter que 20 des 48 ports. Cependant, si tous les appareils indiquent au commutateur qu'ils sont de classe 1, alors 300 W suffiront pour alimenter les 48 ports.

Classe	Type	Puissance minimale au PSE	Puissance maximale utilisée par le PD
0	Type 1, 802.3af	15,4 W	0,44 W - 12,95 W
1	Type 1, 802.3af	4,0 W	0,44 W - 3,84 W
2	Type 1, 802.3af	7,0 W	3,84 W - 6,49 W
3	Type 1, 802.3af	15,4 W	6,49 W - 12,95 W
4	Type 2, 802.3at	30 W	12,95 W - 25,5 W
6	Type 3, 802.3bt	60 W	51 W
8	Type 4, 802.3bt	90 W	71,3 W

tableau 13.1a *Classifications de puissance selon IEEE 802.3af, IEEE 802.3at et IEEE 802.3bt.*

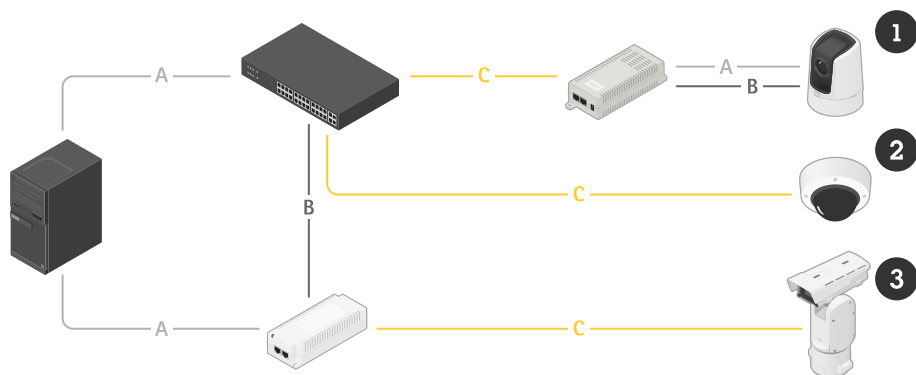
La plupart des caméras réseau fixes peuvent être alimentées via PoE en utilisant la norme IEEE 802.3af et sont normalement identifiées en tant que périphériques de classes 1 ou 2.

D'autres normes PoE sont la norme IEEE 802.3at, également appelée PoE+ et IEEE 802.3bt. Avec PoE+, la puissance limite atteint au moins 30 W fournie par deux paires de fils provenant d'un PSE. Lorsque les besoins en puissance dépassent ce que peut fournir la norme PoE+, Axis utilise le nom de High PoE. Dans cette configuration, la puissance maximale peut atteindre 60 W grâce à quatre paires de fil et 51 W sont garantis pour le PoE.

Les injecteurs et séparateurs PoE+ et High PoE peuvent être utilisés, par exemple, sur les caméras PTZ avec commande de moteur, ainsi que sur les caméras avec fonction de chauffage et de ventilation, qui nécessitent plus de puissance que la norme IEEE 802.3af. Pour PoE+ et High PoE, l'utilisation d'un câble de catégorie Cat-5e ou supérieure est recommandée.

L'injecteur, qui injecte de l'énergie au câble Ethernet, est placé entre le commutateur réseau et les périphériques alimentés. Pour s'assurer que le transfert de données n'est pas affecté, la distance maximale entre la source des données (par exemple, le commutateur) et le périphérique ne doit pas dépasser 100 m (328 pi.). Par conséquent, l'injecteur et le(s) séparateur(s) actif(s) doivent être placés à moins de 100 m.

Un séparateur permet de séparer l'alimentation et les données d'un câble Ethernet en deux câbles distincts, qui peuvent ensuite être raccordés à un périphérique ne prenant pas en charge le PoE. Étant donné que le PoE ou le PoE+ ne fournit que 48 V CC, le séparateur doit aussi réduire la tension au niveau requis par le périphérique, 12 V ou 5 V par exemple.



Avec des injecteurs et séparateurs, vous pouvez combiner des caméras sans PoE (1), des caméras avec PoE (2) et des caméras qui ont besoin de plus de puissance que PoE ne peut fournir (3) sur le même système.

A. Alimentation (de l'onduleur)

B. Ethernet (du commutateur réseau)

C. Alimentation par Ethernet

1. Une caméra sans PoE peut être connectée à l'aide d'un séparateur.

2. Une caméra avec PoE reçoit à la fois de la puissance et une connectivité Ethernet via un câble Ethernet du commutateur.

3. Une caméra qui a besoin de plus de puissance qu'un commutateur PoE standard est capable de fournir peut être connectée à l'aide d'un injecteur, qui fournit un niveau de puissance supérieur à la caméra. L'injecteur reçoit les données du commutateur et lui en transmet, tandis que l'alimentation PoE vers la caméra provient de l'alimentation secteur, via le système d'alimentation sans coupure (UPS) dans cet exemple.

13.2 Envoyer des données sur Internet

Voici les éléments de base de la communication sur Internet :

Routeurs. Les routeurs réseau doivent être utilisés pour transférer des paquets de données d'un LAN à un autre via Internet. Ces périphériques acheminent les informations d'un réseau à un autre en fonction des adresses IP. Un routeur ne transmet que les paquets de données destinés à un autre réseau, et le plus souvent il est utilisé pour connecter un réseau local à Internet. Les routeurs sont parfois nommés passerelles.

Pare-feu. Un pare-feu est conçu pour empêcher tout accès non autorisé à ou depuis un réseau privé. Le pare-feu peut être matériel ou logiciel, voire à la fois matériel et logiciel. Les pare-feu sont fréquemment utilisés pour empêcher les utilisateurs Internet non autorisés d'accéder à des réseaux privés connectés à Internet. Les messages entrant ou sortant d'Internet passent par le pare-feu, qui examine chaque message et bloque ceux qui ne répondent pas aux critères de sécurité spécifiés.

Connexions Internet. Lors de la connexion à Internet, le flux de téléversement (envoi de données) correspond au débit de transfert (bande passante) auquel les données peuvent être téléchargées depuis l'appareil vers Internet (lorsque la vidéo est envoyée à partir d'une caméra réseau, par exemple). Le débit descendant est la vitesse de transfert pour le téléchargement de fichiers ; par exemple, lorsqu'une vidéo est reçue par un PC. Dans la plupart des scénarios, c'est la vitesse de téléchargement qui est la plus importante à prendre en compte. Dans une application vidéo avec une caméra installée sur un site distant, cependant, la vitesse de téléversement (envoi de données) est plus importante, puisque la vidéo de la caméra sera téléchargée vers l'Internet. Les technologies

Internet plus anciennes avec une bande passante asymétrique telle que l'ADSL (Asymmetric Digital Subscriber Line) peuvent ne pas convenir aux applications vidéo en réseau car leur débit d'envoi de données sera probablement trop bas.

L'envoi de données entre deux périphériques situés chacun sur un réseau local différent nécessite une méthode de communication standard, car chaque réseau local peut utiliser des technologies différentes. Cette exigence a conduit au développement de l'adressage IP et de nombreux protocoles IP pour la communication sur Internet.

13.2.1 Adressage IP

Les dispositifs souhaitant communiquer via Internet doit avoir des adresses IP uniques et appropriées, qui identifient les dispositifs expéditeurs et destinataires. Il existe actuellement deux versions d'IP : IP version 4 (IPv4) et IP version 6 (IPv6). La principale différence entre les deux est qu'une adresse IPv6 est plus longue (128 bits contre 32 bits pour une adresse IPv4). Les adresses IPv4 sont les plus couramment utilisées aujourd'hui.

13.2.1.1 Adresses IPv4

Les adresses IPv4 sont regroupées en quatre blocs, chaque bloc étant séparé par un point. Chaque bloc est un nombre compris entre 0 et 255 ; par exemple, 192.168.12.23.

Certains blocs d'adresses IPv4 sont réservés à un usage privé. Ces adresses IP privées sont les suivantes : 10.0.0.0 à 10.255.255.255, 172.16.0.0 à 172.31.255.255 et 192.168.0.0 à 192.168.255.255. Ces adresses ne peuvent être utilisées que sur des réseaux privés et ne sont pas autorisées à être transmises à Internet par l'intermédiaire d'un routeur. Les périphériques souhaitant communiquer sur Internet doivent posséder leur propre adresse IP publique, qui sera attribuée par un fournisseur de services Internet. L'adresse peut être une adresse IP dynamique, qui peut changer au cours d'une session, ou une adresse statique, qui est généralement facturée en sus sur une base mensuelle.

Ports

Un numéro de port définit un service ou une application de sorte que le serveur destinataire (par exemple, une caméra réseau) saura comment traiter les données entrantes. Lorsqu'un ordinateur envoie des données liées à une application spécifique, il ajoute d'ordinaire automatiquement le numéro de port à une adresse IP.

Les numéros de port peuvent être compris entre 0 et 65535. Certaines applications utilisent des numéros de port qui leur sont préattribués par l'IANA (Internet Assigned Numbers Authority). Par exemple, un service Web via HTTP est généralement mappé au port 80 sur une caméra réseau.

Définition des adresses IPv4

Une adresse IP doit être assignée au périphérique pour qu'il puisse fonctionner sur un réseau IP. La définition d'une adresse IPv4 pour un périphérique Axis peut être effectuée automatiquement à l'aide du protocole DHCP (Dynamic Host Configuration Protocol) qui nécessite un serveur DHCP sur le réseau. Il est également possible d'utiliser un outil logiciel de gestion tel qu'AXIS Device Manager. L'adresse peut aussi être définie manuellement. Pour ce faire, il faut utiliser la page Web du périphérique et entrer l'adresse IP statique, le masque de sous-réseau et les adresses IP du routeur par défaut, le serveur DNS (Domain Name System) et le serveur NTP (Network Time Protocol).

Un serveur DHCP gère un pool d'adresses IP, qu'il peut affecter dynamiquement aux périphériques réseau. Souvent, cette fonction est effectuée par un routeur haut débit, qui est généralement connecté à Internet et reçoit sa propre adresse IP publique en provenance d'un fournisseur de services Internet. L'adresse IP d'un périphérique réseau peut changer chaque jour quand elle est dynamique. Avec les adresses IP dynamiques, il est recommandé d'enregistrer un nom de domaine (par exemple, *www.mycamera.com*) pour le périphérique sur un serveur DNS dynamique, qui peut toujours lier le nom de domaine du périphérique à l'une des adresses IP de ce dernier. Un nom de domaine peut être enregistré en utilisant certains sites DNS dynamiques connus tels que *www.dyndns.org*.

L'utilisation de DHCP pour définir une adresse IPv4 fonctionne comme suit : Lorsqu'un périphérique réseau (comme une caméra réseau) est en ligne, il envoie une requête demandant la configuration à partir d'un serveur DHCP. Le serveur DHCP répond avec la configuration demandée par le périphérique. Cela inclut normalement l'adresse IP, le masque de sous-réseau et les adresses IP du routeur, du serveur DNS et du serveur NTP. Le périphérique vérifie d'abord que l'adresse IP proposée n'est pas déjà utilisée sur le réseau local, lui attribue l'adresse et peut mettre à jour un serveur DNS dynamique avec son adresse IP actuelle afin que les utilisateurs puissent accéder au périphérique en utilisant un nom de domaine.

AXIS Device Manager est le logiciel qui peut automatiquement trouver et définir des adresses IP et afficher l'état de la connexion. Il peut également assigner des adresses IP statiques et privées à tous les produits de vidéo sur IP Axis. C'est la procédure recommandée lorsque vous utilisez un logiciel de gestion vidéo pour accéder à des produits vidéo sur IP. Dans un système de vidéo sur IP pouvant comporter des centaines de caméras, un logiciel tel qu'AXIS Device Manager est nécessaire pour gérer efficacement le système.

Traduction d'adresses réseau (NAT)

Lorsqu'un périphérique réseau avec une adresse IP privée souhaite envoyer des informations via Internet, il doit le faire en utilisant un routeur prenant en charge NAT. En utilisant cette technique, le routeur traduit l'adresse IP privée en une adresse IP publique, pour une exposition publique sur Internet.

13.2.1.2 Adresses IPv6

Une adresse IPv6 est écrite en notation hexadécimale avec des deux-points subdivisant l'adresse en huit blocs de 16 bits chacun (par exemple, 2001:0da8:65b4:05d3:1315:7c1f:0461:7847).

IPv6 a pour avantage, mis à part le nombre élevé d'adresses IP qu'il fournit, de permettre à un périphérique de configurer automatiquement son adresse IP à l'aide de son adresse MAC. Pour la communication sur Internet, l'hôte demande au routeur et reçoit de celui-ci le préfixe requis du bloc d'adresse publique, ainsi que toute information supplémentaire. Le préfixe et le suffixe de l'hôte sont alors utilisés, de sorte que le DHCP pour l'attribution des adresses IP et le paramétrage manuel des adresses IP ne sont plus nécessaires avec l'IPv6. Parmi les autres avantages de l'IPv6 figurent la renumérotation pour simplifier le passage de réseaux d'entreprise entiers d'un fournisseur à l'autre, un routage plus rapide, le cryptage point à point selon IPsec, et la connexion en utilisant la même adresse dans des réseaux changeants (Mobile IPv6).

Une adresse IPv6 est placée entre crochets dans une URL et un port spécifique peut être adressé de la façon suivante : `http://[2001:0da8:65b4:05d3:1315:7c1f:0461:7847]:8081/`

Pour définir l'adresse IPv6 d'un périphérique réseau Axis, il suffit de cocher une case pour activer IPv6 dans le périphérique. Le périphérique reçoit ensuite une adresse IPv6 en fonction de la configuration définie dans le routeur réseau.

13.2.2 Protocoles de transport de données pour la vidéo sur IP

Le protocole TCP (Transmission Control Protocol) et le protocole UDP (User Datagram Protocol) sont les protocoles IP utilisés pour l'envoi de données. Ces protocoles de transport font office de transporteurs pour de nombreux autres protocoles. Par exemple, HTTP (Hyper Text Transfer Protocol), qui est utilisé pour parcourir les pages Web, est transporté par TCP.

TCP fournit un canal de transmission fiable basé sur la connexion. Cela garantit que les données envoyées d'un point sont reçues à l'autre point. La fiabilité du TCP grâce à la retransmission peut entraîner des retards importants, mais en général, le TCP est utilisé lorsque la fiabilité de la communication est préférable à la réduction de la latence.

UDP est un protocole sans connexion et ne garantit pas la livraison des données transmises, laissant ainsi l'ensemble du mécanisme de contrôle et de vérification des erreurs à l'application

elle-même. UDP ne retransmet pas les données perdues et, par conséquent, n'introduit pas de délai supplémentaire.

Protocole	Protocole de transfert	Port	Utilisation courante	Utilisation en vidéo sur IP
FTP (protocole de transfert de fichiers)	TCP	21	Transfert de fichiers	Transfert d'images ou de vidéos sur un serveur FTP ou une application
SMTP (Protocole d'envoi de message)	TCP	25	Protocole d'envoi d'e-mail	Le produit de vidéo sur IP envoie des images ou des notifications d'alarme à l'aide d'un client de messagerie intégré.
HTTP (Protocole de transfert hypertexte)	TCP	80	Parcourir le Web, c'est-à-dire obtenir des pages Web à partir de serveurs Web	Le périphérique vidéo fonctionne en tant que serveur Web, permettant à l'utilisateur ou au serveur d'applications d'accéder à la vidéo.
HTTPS (Hypertext Transfer Protocol over Transport Layer Security)	TCP	443	Accès sécurisé aux pages Web à l'aide de la technologie de cryptage	Transmission sécurisée de vidéo à partir de produits de vidéo sur IP.

Protocole	Protocole de transfert	Port	Utilisation courante	Utilisation en vidéo sur IP
RTP (Protocole en temps réel)	UDP/TCP	non défini	Format de paquet normalisé RTP pour la diffusion audio et vidéo sur Internet, souvent utilisé dans les systèmes de diffusion multimédia en continu ou la vidéoconférence	Transmission de vidéo et synchronisation de la vidéo et de l'audio. Le RTP assure la numérotation séquentielle et l'horodatage des paquets de données, permettant ainsi un réassemblage correct. Monodiffusion ou multidiffusion.
RTSP (Protocole d'envoi de flux en temps réel)	TCP	554	Configuration et contrôle des sessions multimédia sur RTP	

tableau 13.2a *Protocoles TCP / IP communs et ports utilisés pour la vidéo sur IP.*

Voir aussi la documentation Axis sur les ports couramment utilisés sur <https://help.axis.com/axis-os#commonly-used-network-ports>

13.2.3 SIP

Session Initiation Protocol (SIP) est un protocole basé sur du texte, similaire à HTTP et SMTP, pour la communication sur les réseaux IP. Il est utilisé pour démarrer, changer et mettre fin à des sessions de flux média, qui peuvent inclure des éléments vocaux et vidéo. SIP est le protocole standard utilisé dans les applications de voix sur IP (VoIP) et les plateformes de communication unifiée, pour la vidéoconférence, le contrôle des appels et la messagerie instantanée. SIP constitue un moyen de connecter, d'intégrer et de contrôler les produits réseau Axis.

Les appels SIP peuvent être configurés de plusieurs façons, mais il existe trois types principaux :

Appels P2P homologues, également appelés appels locaux. Il s'agit d'appels effectués entre deux appareils (tels que des ordinateurs, des haut-parleurs réseau, des téléphones logiciels, des stations de porte, des caméras ou des téléphones de bureau IP) appartenant au même réseau. L'appel est effectué à l'adresse SIP de l'appareil.

Appels de serveur SIP, également appelés appels d'autocommutateur privé (PBX). Pour effectuer des appels de serveur SIP, les périphériques doivent être connectés à un serveur SIP qui gère les échanges d'appels. Un serveur SIP ou un PBX est un concentrateur qui fonctionne comme un standard traditionnel. Il peut être hébergé sur un réseau intranet ou par un fournisseur de services tiers. Les périphériques SIP s'enregistrent auprès du serveur SIP et peuvent se contacter via leurs adresses SIP. Un PBX peut entre autres afficher l'état des appels, autoriser les transferts d'appels, gérer la messagerie vocale et rediriger les appels.

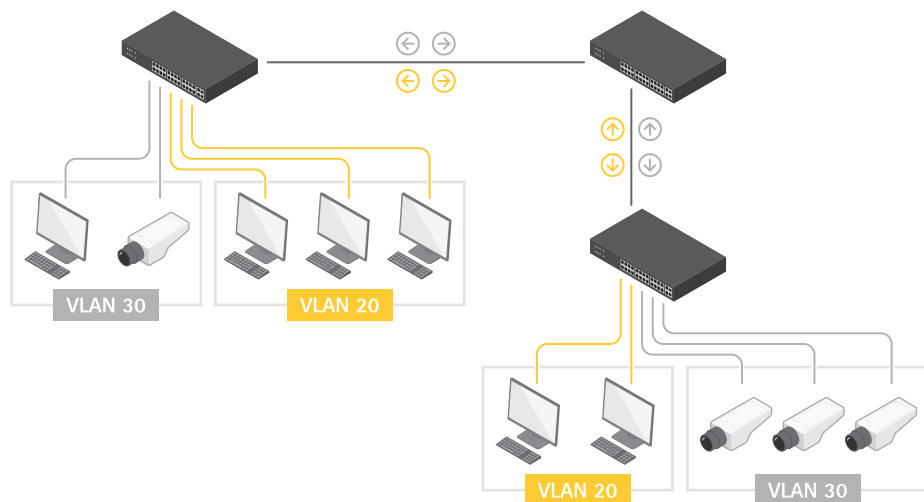
Les adresses SIP, également appelées identificateurs de ressources uniformes (URI) SIP ou numéros SIP, sont utilisées pour identifier les utilisateurs au sein d'un réseau, tout comme les numéros de téléphone ou les adresses e-mail. Comme les adresses e-mail, les adresses SIP sont un type d'URI qui comprend deux parties spécifiques à l'utilisateur, un ID utilisateur ou une extension, et un nom de domaine ou une adresse IP. Avec un préfixe et le symbole @, ils forment une adresse unique. Dans le cas d'un appel P2P, l'adresse SIP inclura l'adresse IP plutôt que le nom de domaine.

Appels de ligne réseau SIP. Avec un fournisseur de services qui propose des lignes groupées SIP, le réseau téléphonique traditionnel peut être utilisé pour effectuer des appels, et les numéros de téléphone traditionnels peuvent être attribués aux dispositifs SIP. De cette manière, les appels peuvent être effectués à partir d'un haut-parleur réseau ou d'une station de porte réseau vers un mobile ou inversement.

13.3 Réseaux locaux virtuels

La mise en place de systèmes de vidéo sur IP entraînent souvent la nécessité de séparer le réseau des autres réseaux, à la fois pour des raisons de sécurité et de performance. À première vue, la meilleure solution serait de construire un réseau distinct. Alors que la conception serait simplifiée, le coût d'achat, d'installation et de maintenance du réseau serait souvent plus élevé que l'utilisation d'un réseau local virtuel (VLAN).

VLAN est une technologie permettant de segmenter virtuellement des réseaux. Cette fonctionnalité est prise en charge par la plupart des commutateurs réseau. Il faut pour ce faire diviser les utilisateurs du réseau en groupes logiques. Seuls les utilisateurs d'un groupe spécifique peuvent échanger des données ou accéder à certaines ressources sur le réseau. Si un système vidéo sur IP est segmenté dans un VLAN, seuls les serveurs situés sur ce VLAN peuvent accéder aux caméras réseau. Les VLAN constituent une solution flexible et plus rentable qu'un réseau séparé. Le protocole principal utilisé lors de la configuration des VLAN est IEEE 802.1Q, qui étiquette chaque trame ou paquet avec des octets supplémentaires pour indiquer à quel réseau virtuel appartient le paquet.



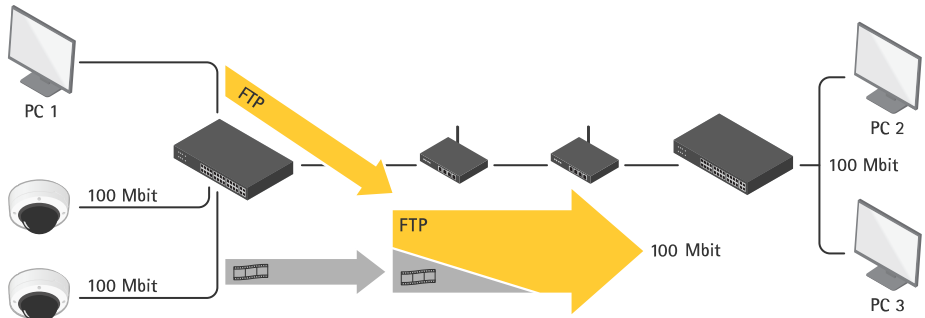
Dans cette illustration, les VLAN sont configurés sur plusieurs commutateurs. Les deux LAN différents sont segmentés en VLAN 20 et VLAN 30. Seuls les membres du même VLAN peuvent échanger des données, soit au sein du même réseau soit sur des réseaux différents.

13.4 Qualité de service

Étant donné que différentes applications (par exemple, le téléphone, l'e-mail et la vidéosurveillance) peuvent toutes utiliser le même réseau IP, il est souvent nécessaire de contrôler la manière dont les ressources réseau sont partagées pour répondre aux besoins de chaque service. Pour ce faire, il est possible de laisser les routeurs et les commutateurs de réseau fonctionner différemment pour différents types de services (voix, données et vidéo) lorsque le trafic passe à travers le réseau. En utilisant la Qualité de Service (QoS), différentes applications réseau peuvent coexister sur le même réseau sans consommer la bande passante des autres.

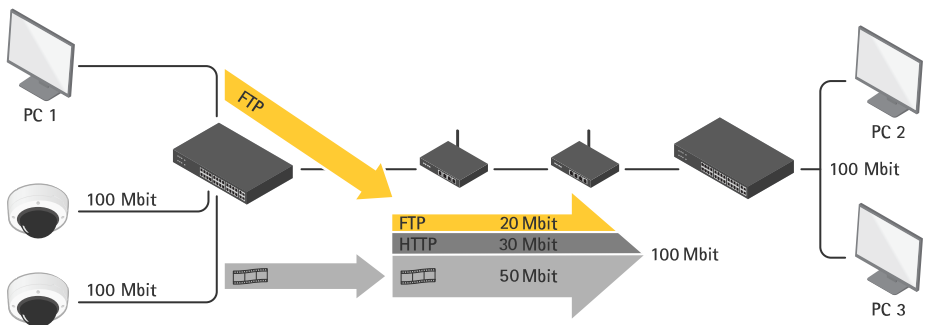
La Qualité de Service fait référence à un certain nombre de technologies, telles que DSCP (Differentiated Services Code Point), qui peuvent identifier le type de données des paquets et diviser ceux-ci en classes de trafic afin de leur attribuer une priorité de transfert. Un réseau compatible QoS a pour avantage de hiérarchiser le trafic pour permettre de diffuser les flux critiques avant les flux ayant une priorité moindre. Il offre aussi une meilleure fiabilité dans le réseau en contrôlant la quantité de bande passante qu'une application peut utiliser et ainsi la concurrence entre les applications. Le QoS peut par exemple être utilisé avec les commandes PTZ pour garantir des réponses rapides de la caméra aux demandes de mouvement. Afin de pouvoir

utiliser la QoS dans un réseau vidéo, il faut que tous les commutateurs, routeurs et périphériques vidéo sur IP prennent en charge la Qualité de Service.



Réseau standard (n'utilisant pas QoS). Dans cet exemple, les flux FTP et vidéo disposent de 100 Mbit/s à partager et la bande passante vidéo ne peut pas être garantie.

Dans cette illustration, le PC 2 regarde deux flux vidéo (provenant des deux caméras), chaque caméra diffusant à 25 Mbit/s. Soudain, le PC 3 lance un transfert de fichier depuis le PC 1. Dans ce scénario, le protocole de transfert de fichiers (FTP) essaiera d'utiliser toute la capacité de 100 Mbit/s entre les deux routeurs, tandis que les flux vidéo essaieront de maintenir leur total de 50 Mbit/s. La quantité de bande passante fournie au système de surveillance ne peut plus être garantie et les flux de données seront probablement réduits. Dans le pire des cas, le trafic FTP consommera toute la bande passante disponible.



Réseau utilisant QoS. Le flux vidéo dispose d'une bande passante garantie jusqu'à 50 Mbit/s.

Dans cette illustration, le premier routeur a été configuré pour utiliser jusqu'à 50 Mbit/s des 100 Mbit/s disponibles pour le flux vidéo. Le trafic FTP peut utiliser 20 Mbit/s, et HTTP et tous les autres trafics peuvent utiliser un maximum de 30 Mbit/s. Cela signifie que les flux vidéo disposeront toujours de la bande passante nécessaire. Les transferts de fichiers sont considérés comme moins importants et ont moins de bande passante, mais la bande passante reste disponible pour la navigation sur le Web et d'autres types de trafic. Notez que ces valeurs maximales ne s'appliquent que lorsqu'il y a congestion du réseau. La bande passante inutilisée peut servir à n'importe quel type de trafic.

14. Protection du système

Les cybermenaces sont généralement associées aux pirates informatiques et aux logiciels malveillants, mais leur impact négatif peut également résulter d'un usage abusif non intentionnel. Lorsque vous déployez un système, il est recommandé de respecter les meilleures pratiques du secteur. Pour être protégé, un système doit être bien configuré et bien maintenu.

14.1 Protection du réseau

Les réseaux ont besoin d'être protégés contre les cyberattaques. Tous les paquets envoyés sur le réseau peuvent être récupérés par d'autres ordinateurs sur le même réseau. Si la charge utile des paquets est envoyée en texte clair, les données peuvent être facilement compromises par ce que l'on appelle le reniflage réseau. Une autre menace concerne l'usurpation de réseau, où ordinateur malveillant tente d'usurper l'identité d'un serveur, d'un ordinateur ou d'un périphérique réseau légitime afin d'accéder au réseau. Les connexions cryptées et les certificats signés par AC assurent une protection.

Pour en savoir plus sur la réduction de l'exposition du réseau aux risques, consultez le manuel *Axis Network Switches Hardening Guide* sur <https://help.axis.com/axis-network-switches-hardening-guide>.

Pour connaître les meilleures pratiques concernant l'intégration et le fonctionnement des périphériques Axis dans les réseaux alimentés par HPE Aruba Networking, consultez le guide d'intégration *HPE Aruba Networking - Integration Guide* à l'adresse help.axis.com/axis-aruba-secure-network-integration. La configuration conforme aux meilleures pratiques utilise des normes et des protocoles de sécurité modernes tels que IEEE 802.1X, IEEE 802.1AR, et HTTPS.

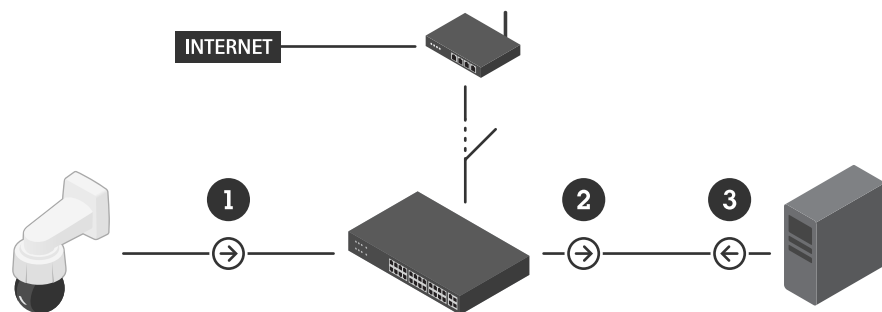
14.1.1 IEEE 802.1X

De nombreux produits Axis prennent en charge la méthode IEEE 802.1X, qui est utilisée pour protéger les réseaux contre les connexions d'appareils non autorisés. IEEE 802.1X établit une connexion point à point, ou empêche l'accès à partir du port LAN si l'authentification échoue.

IEEE 802.1X empêche ce qu'on appelle le piratage de port, c'est-à-dire lorsqu'un périphérique non autorisé accède à un réseau via une connexion physique à un port / une prise réseau. IEEE 802.1X est utile dans les applications vidéo sur IP, car les caméras sont souvent situées dans des espaces publics où une prise accessible peut présenter un risque de sécurité. Dans les réseaux d'entreprise d'aujourd'hui, IEEE 802.1X est une exigence de base pour tout ce qui est connecté à un réseau.

Dans un système de vidéo sur IP, IEEE 802.1X peut fonctionner comme suit :

- 1 Une caméra configurée pour IEEE 802.1X envoie une demande d'accès réseau à un commutateur.
- 2 Le commutateur transmet la requête à un serveur d'authentification, par exemple un serveur RADIUS tel qu'un serveur Microsoft Internet Authentication Service.
- 3 Si l'authentification réussit, le serveur demande au commutateur d'ouvrir son port et de permettre aux données de la caméra réseau de passer à travers le réseau.



IEEE 802.1X permet la sécurité basée sur port.

14.1.2 HTTPS (HTTP sur TLS)

HTTPS (Hypertext Transfer Protocol Secure) est une méthode de communication sécurisée qui envoie HTTP à l'intérieur d'une connexion TLS (Transport Layer Security). La connexion HTTP et les données elles-mêmes sont ainsi cryptées.

De nombreux produits vidéo Axis intègrent le protocole HTTPS, ce qui permet de sécuriser la communication des données. Pour permettre à une caméra ou à un encodeur vidéo Axis de communiquer via HTTPS, un certificat numérique et une paire de clés asymétriques doivent être installés dans le produit. La paire de clés est générée par le produit Axis. Le certificat peut être généré et auto-signé par le produit Axis, ou il peut être émis par une autorité de certification. Dans HTTPS, le certificat est utilisé pour l'authentification et le cryptage, ce qui signifie que le certificat permet à un client de vérifier l'identité du produit et crypte la communication à l'aide de clés générées par la cryptographie à clé publique.

14.1.3 Infrastructure de clé publique (PKI) fiable

Une infrastructure de clé publique (PKI) fiable est constituée d'une autorité de certification (CA) privée ou publique, qui est un service d'émission (signature) de certificats à installer sur les périphériques en réseau. Les certificats sont utilisés pour le cryptage de bout en bout des connexions TLS entre les hôtes d'un réseau. Un certificat signé par une autorité de certification (AC) avec une chaîne de confiance validée permet aux applications, telles qu'un système VMS ou un navigateur Web, de valider l'identité du périphérique en réseau Axis. Généralement, un certificat CA (certificat racine) signe un certificat CA intermédiaire, qui, en retour, signe les certificats client pour les périphériques. Pour que cette validation réussisse, le certificat CA connu publiquement (certificat racine et/ou intermédiaire) doit être installé et utilisé par l'application pour vérifier les certificats clients qui sont transportés par les périphériques en réseau Axis. AXIS Device Manager dispose d'un service d'autorité de certification intégré pouvant émettre et déployer des certificats de serveur sur les périphériques de façon économique.

14.1.4 NTS Network Time Protocol

NTS fournit une sécurité cryptographique pour le mode client-serveur du Network Time Protocol (NTP), permettant aux utilisateurs d'obtenir l'heure de manière authentifiée. Les périphériques d'Axis prennent en charge NTS à partir d'AXIS OS 11.1.

La synchronisation du temps est traditionnellement réalisée par le protocole NTP (Network Time Protocol). NTS garantit que le périphérique ne reçoit l'heure que de sources fiables, chaque synchronisation étant authentifiée et validée jusqu'à ce que les caractéristiques de synchronisation du temps du protocole NTP soient conservées.

14.1.5 Isolement du réseau

L'isolation réseau, ou segmentation réseau, est un moyen de séparer les ressources réseau critiques les unes des autres afin de réduire le risque d'impact négatif qu'elles peuvent avoir les unes sur les autres. Il s'agit d'une tactique particulièrement pertinente si les différentes ressources n'ont pas besoin ou ne doivent pas interagir entre elles. La segmentation réseau peut être virtuelle (VLAN) et nécessiter une infrastructure de commutateurs gérés. Les réseaux peuvent également être séparés avec un câblage et des équipements réseau différents.

14.2 Normes de cybersécurité

14.2.1 ETSI EN 303 645

La norme ETSI EN 303 645 est une norme de cybersécurité pour laquelle les dispositifs Axis fonctionnant avec AXIS OS 11 ou une version plus récente sont certifiés. Elle établit une ligne de base de sécurité pour les produits de consommation connectés à internet et aide les périphériques à mieux se conformer aux réglementations RGDP.

14.2.2 FIPS (Federal Information Processing Standard) 140

FIPS 140 est reconnue comme une norme de sécurité de pointe, à laquelle les agences fédérales américaines et canadiennes et les infrastructures critiques doivent se conformer. FIPS 140-2 et FIPS 140-3 sont des normes de sécurité de l'information pour les modules informatiques cryptographiques, publiées aux États-Unis par le NIST (National Institute of Standards and Technology). FIPS 140-3 a remplacé FIPS 140-2 en 2019 en tant que version mise à jour.

Axis exige que ses modules informatiques cryptographiques matériels incorporés soient certifiés au moins selon les critères communs EAL4 et/ou FIPS 140-2/3 niveau 2. La norme FIPS 140 prévoit quatre niveaux de sécurité, les niveaux 1 à 4. Chaque niveau ajoute des exigences plus restrictives ; ainsi, le niveau 1 présente les exigences les plus faibles et le niveau 4 les exigences les plus élevées.

Vous pouvez consulter des informations concernant ces certification sur la fiche technique d'un périphérique Axis ou dans le sélecteur de produits Axis.

14.2.3 Critères communs (CC)

Critères communs (CC) est une norme internationale (ISO/IEC 15408) pour la certification en matière de sécurité des produits IT. Axis impose à ses modules de calcul cryptographique matériels intégrés d'être au moins certifiés conformément aux Critères communs EAL4 et/ou aux normes 140-2/3 niveau 2.

14.3 Protection des dispositifs

Un périphérique en réseau et ses ressources doivent être dûment protégés. La protection peut dans ce cas se référer à la fois à la protection physique, comme placer les caméras hors de portée, et à la protection du logiciel de la caméra. *AXIS OS Hardening Guide* fournit plus d'informations sur la protection des périphériques.

14.3.1 Plateforme de cybersécurité intégrée

Les périphériques Axis sont protégés par la plate-forme de cybersécurité matérielle Axis Edge Vault. Elle repose sur des bases solides constituées de modules de calcul cryptographique (élément sécurisé et TPM) et d'une sécurité SoC (TEE et démarrage sécurisé), associés au savoir-faire en matière de sécurité des dispositifs périphériques.

Axis Edge Vault limite l'exposition aux risques de cybersécurité et transforme les périphériques en unités sécurisées et fiables au sein du réseau.

- > **Identité du périphérique de confiance** . Être capable de vérifier l'origine du périphérique est essentiel pour instaurer la confiance dans l'identité du périphérique. Pendant la production, avec Axis Edge Vault, un certificat d'identifiant de périphérique Axis unique, provisionné en usine et conforme IEEE 802.1AR est assigné à chaque périphérique. Il est stocké de manière sécurisée et permanente dans le keystore sécurisé et peut être utilisé pour l'intégration automatique de périphériques sécurisés et l'identification sécurisée des périphériques.
- > **Stockage sécurisé des clés** . Le fichier de clés sécurisé fournit un stockage matériel des informations cryptographiques protégé contre le sabotage. Il protège l'identifiant de périphérique Axis ainsi que les informations cryptographiques chargées par le client, et empêche tout accès non autorisé et toute extraction malveillante en cas de faille de sécurité.
- > **Détection de sabotage des vidéos** . Avec la *vidéo signée*, un traçage est possible jusqu'à la caméra d'origine, ce qui permet de vérifier que l'enregistrement n'a pas été saboté une fois qu'il n'est plus dans la caméra. Chaque caméra utilise sa clé de signature de vidéo unique, qui est stockée dans un fichier de clés sécurisé, pour ajouter une signature dans le flux vidéo. À la lecture, le lecteur vidéo indique si la vidéo est intacte.
- > **Protection de la chaîne d'approvisionnement** . Les fonctions de cybersécurité, le *démarrage sécurisé* et le *système d'exploitation signé* contribuent à établir une base sécurisée pour Axis Edge Vault en fournissant une chaîne ininterrompue de logiciels validés par cryptographie. Le *démarrage sécurisé* empêche le sabotage de la chaîne d'approvisionnement physique en garantissant qu'un périphérique ne peut démarrer qu'avec un système d'exploitation signé par Axis. Le *système d'exploitation signé* garantit que le système d'exploitation installé (AXIS OS) est authentiquement signé par Axis et que tout nouveau système d'exploitation installé sur le périphérique est signé par Axis. Si le périphérique détecte que l'intégrité du système d'exploitation est compromise ou s'il n'est pas signé par Axis, la mise à niveau sera rejetée.
- > **MACsec**. De nombreux périphériques Axis prennent également en charge la norme de sécurité IEEE 802.1AE MACsec. MACsec est activé par défaut et crypte automatiquement les données au niveau de la couche 2 Ethernet dans les connexions entre les périphériques Axis et les commutateurs Ethernet compatibles MACsec. Du fait qu'elle est mise en œuvre à ce niveau de base, MACsec peut crypter et protéger des données qui ne pouvaient pas l'être auparavant,

telles que NTP, DHCP pour le fonctionnement général des périphériques et RTP/RTSP pour les flux vidéo.

14.3.2 Gestion des comptes utilisateurs

Les mots de passe des périphériques ont tendance à se généraliser au sein d'une société. Par exemple, lors de la maintenance d'un périphérique, une personne est susceptible de demander le mot de passe pour effectuer un réglage. Quelques jours ou semaines plus tard, une autre personne peut faire la même demande. Rapidement, un grand nombre de nouveaux utilisateurs (ou d'utilisateurs temporaires) connaissent le mot de passe de tous vos périphériques et vous avez perdu le contrôle des personnes qui peuvent y accéder. La complexité du mot de passe ne fait aucune différence dans ce scénario. La gestion des périphériques doit impliquer l'utilisation de plusieurs comptes (en fonction des rôles) et des comptes temporaires doivent être créés pour la maintenance et la recherche de panne occasionnelle.

Pour l'accès aux comptes, vous devez utiliser le principe de moindre privilège. Cela signifie que les privilèges d'accès d'un utilisateur sont limités aux seules ressources nécessaires à l'exécution de ses tâches spécifiques. AXIS Device Manager permet une gestion facile et efficace de plusieurs comptes et mots de passe, aux niveaux de l'utilisateur, de l'opérateur ou de l'administrateur.

14.3.3 Filtrage d'adresses IP

Les produits Axis fournissent un filtrage d'adresse IP, qui autorise ou refuse l'accès à des adresses IP définies. Dans une installation standard, les périphériques en réseau sont configurés de manière à n'autoriser l'accès au produit qu'à l'adresse IP du serveur qui héberge le logiciel de gestion vidéo.

Le filtrage IP agit comme un pare-feu local sur le périphérique en réseau. Les clients vidéo accèdent à la vidéo en direct et enregistrée depuis le VMS, jamais en accédant directement à un périphérique en réseau. Par conséquent, le seul ordinateur ou serveur censé accéder aux périphériques en réseau pendant les opérations normales est le serveur VMS. Les périphériques peuvent être configurés avec un filtre IP pour répondre uniquement aux adresses IP sur liste d'autorisation, généralement le serveur VMS et les clients d'administration. En cas de compromission du mot de passe du périphérique, le filtrage IP permet d'atténuer les risques provenant des périphériques non corrigés ou d'attaques par force brute.

14.3.4 Mise à jour des logiciels des périphériques

L'utilisation de périphériques dotés de la dernière version du système d'exploitation AXIS OS permet de limiter les risques courants. En effet, la dernière version inclut généralement des correctifs de sécurité pour toutes les vulnérabilités connues, notamment celles récemment découvertes. Par conséquent, les cybercriminels ne peuvent ni exploiter les vulnérabilités ni compromettre éventuellement le système, l'application ou les périphériques. Le logiciel de gestion des

périphériques Axis vous aide à gérer les mises à niveau de plusieurs périphériques et sites et vous avertit automatiquement de l'existence de nouvelles versions.

En tant qu'autorité de numérotation CVE (CNA), Axis respecte les meilleures pratiques du secteur en matière de gestion et de réponse aux failles de sécurité découvertes dans ses produits. Les vulnérabilités sont évaluées à l'aide du système d'évaluation CVSS largement utilisé, et corrigées pendant une période déterminée en fonction du score.

Pour une protection contre les menaces spécifiques de sabotage de la chaîne d'approvisionnement, les fonctions de *système d'exploitation signé* et de *démarrage sécurisé* sont largement disponibles sur les dispositifs Axis.

14.4 Protection du VMS

De nombreux principes qui s'appliquent à la protection des périphériques et du réseau s'appliquent également à la protection du VMS. Par exemple, vous devez respecter le principe de moindre privilège au moment de définir les comptes système, et veiller à utiliser la dernière version logicielle du VMS, qui dispose de correctifs de sécurité pour toutes les vulnérabilités récemment découvertes. En outre, il est recommandé de déployer des logiciels antivirus sur tous les serveurs et ordinateurs qui se connectent au serveur VMS. De même, vous ne pouvez exécuter que le logiciel serveur VMS et les intégrations tierces sécurisées sur le matériel hôte.

Pour plus d'informations, voir le Guide de renforcement (Hardening Guide) du système AXIS Camera Station à l'adresse <https://help.axis.com/axis-camera-station-system-hardening-guide>. Il décrit les politiques et procédures de cybersécurité permettant de sécuriser le déploiement et la maintenance des systèmes AXIS Camera Station.

14.5 Protection physique

Même si un périphérique en réseau ne peut jamais être protégé physiquement à 100 %, différents aspects physiques doivent être pris en compte. Pour de nombreux types de périphériques, tels que les caméras et les haut-parleurs, vous pouvez choisir un design et une couleur qui se fondent dans l'environnement, placer le périphérique hors de portée et faire passer le câble directement à travers le mur ou le plafond derrière le périphérique. L'application de cette configuration permet de renforcer la protection contre le vandalisme spontané et les attaques planifiées. Pour les périphériques qui doivent être facilement accessibles (interphones ou contrôleurs de porte, par exemple), il est important de choisir des modèles résistants au vandalisme équipés d'une fonction de détection de vandalisme. Les équipements réseau stratégiques, tels que les routeurs et les

commutateurs, et l'hôte exécutant le logiciel serveur VMS doivent être placés dans un environnement dont les accès physiques et logiques sont restreints.

15. Technologies sans fil

Pour les applications de vidéosurveillance, la technologie sans fil offre un moyen flexible, économique et rapide de déployer des caméras, en particulier sur de vastes zones comme les parkings ou en centre-ville. Dans les bâtiments plus anciens et protégés, la technologie sans fil peut être la seule alternative si l'installation de câbles est interdite.

Axis propose des caméras avec prise en charge sans fil intégrée, mais les caméras qui n'en sont pas dotées peuvent tout de même être intégrées dans un réseau sans fil via l'utilisation d'un pont sans fil.

15.1 Normes WLAN 802.11

La norme la plus répandue pour les réseaux locaux sans fil (WLAN) est IEEE 802.11. Bien qu'il existe d'autres normes, ainsi que des technologies propriétaires, la norme 802.11 a pour avantage de fonctionner dans un spectre sans licence, ce qui signifie qu'aucun frais de licence n'est associé à la configuration et à l'utilisation du réseau. Les modifications des normes les plus pertinentes concernant les produits Axis sont les suivantes :

- > 802.11ac (ou Wi-Fi 5) a été approuvée en 2014. Elle s'appuie sur la norme 802.11n, bien qu'elle fonctionne exclusivement dans la bande des 5 GHz. Selon les conditions d'utilisation, le débit varie entre 1,7 et 2,5 Gbit/s.
- > 802.11n (ou Wi-Fi 4), que la plupart des produits sans fil actuels prennent en charge. Approuvée en 2009, elle fonctionne dans la bande des 2,4 GHz ou 5 GHz. Selon les fonctionnalités implémentées, la norme 802.11n permet un débit maximal de 600 Mbit/s.
- > 802.11g, qui a été approuvée en 2003 et fonctionne dans la bande des 2,4 GHz, fournit des débits de données allant jusqu'à 54 Mbit/s.
- > 802.11b, qui a été approuvé en 1999, fonctionne dans la gamme 2,4 GHz et fournit des débits de données allant jusqu'à 11 Mbit/s.

Les produits désignés 802.11b/g/n/ac sont compatibles avec les quatre extensions.

La capacité de bande passante du point d'accès et les besoins en bande passante des périphériques réseau doivent être pris en compte lors de la configuration d'un réseau sans fil. En général, le débit de données utile pris en charge par une norme WLAN est équivalent à environ la moitié du débit stipulé par la norme, en raison des frais généraux de signalisation et de protocole.

15.2 Sécurité WLAN

Lorsque les données sont transférées sur une connexion sans fil, il faut prendre en compte le fait que la limite fixe du réseau local câblé n'existe pas sur le réseau sans fil. En théorie, toute personne se trouvant à portée d'un WLAN peut attaquer le réseau et intercepter les données qui y transitent, c'est pourquoi il est crucial d'empêcher tout accès non autorisé aux données et au réseau.

Quelques directives concernant la sécurité :

- > Activer la connexion par saisie de l'utilisateur et du mot de passe dans les caméras.
- > Activer le cryptage (HTTPS) dans le routeur/les caméras sans fil. Ce cryptage doit être déployé avant que les clés ou les informations d'identification ne soient définies pour le WLAN afin d'empêcher quiconque de voir ces clés telles qu'elles sont envoyées et configurées dans la caméra.
- > Utilisez WPA2-PSK et une phrase secrète contenant au moins 20 caractères aléatoires dans une combinaison mixte de lettres minuscules et majuscules, de caractères spéciaux et de chiffres. WPA2-PSK peut être utilisé pour sécuriser les petits réseaux qui ne peuvent pas utiliser de serveur d'authentification.
- > WPA2-Enterprise avec EAP-TLS, qui offre le niveau de sécurité le plus élevé, est recommandé pour une utilisation dans les environnements d'entreprise qui nécessitent un puissant mécanisme d'authentification et de cryptage.

15.2.1 WPA2™¹

Le protocole WPA2™ repose sur la norme IEEE 802.11i. Notez que le protocole précédent, WPA™, n'est plus recommandé pour la protection des réseaux sans fil.

WPA2-Personal, également connu sous le nom de WPA2-PSK (clé pré-partagée), est conçu pour les petits réseaux et ne nécessite pas de serveur d'authentification. Avec cette technologie, les caméras sans fil Axis utilisent un PSK pour s'authentifier auprès du point d'accès. La clé peut être entrée sous la forme d'un chiffre 256 bits, exprimé en 64 chiffres hexadécimaux (0-9, A-F) ou d'une phrase secrète comportant 8 à 63 caractères ASCII. Des mots de passe longs doivent être utilisés pour contourner les faiblesses de cette méthode de sécurité.

Conçu pour des réseaux plus grands, le mode WPA2-Entreprise nécessite un serveur d'authentification et l'utilisation de la norme IEEE 802.1X. Voir la section pour plus de détails sur la norme IEEE 802.1X.

¹ WPA et WPA2 sont des marques de Wi-Fi Alliance.

15.3 Ponts sans fil

Certaines solutions peuvent utiliser d'autres normes que la norme IEEE 802.11, offrant des performances accrues et des distances beaucoup plus longues associées à une très haute sécurité. Les micro-ondes et les lasers sont les technologies les plus couramment employées. Elles peuvent relier des bâtiments ou des sites via une liaison de données à haut débit point à point.

15.4 Réseau maillé sans fil

Le réseau maillé sans fil est couramment employé pour les applications de vidéosurveillance des centres-villes où des centaines de caméras peuvent être impliquées, ainsi que des routeurs et passerelles maillés. Ce réseau est caractérisé par plusieurs nœuds de connexion qui reçoivent, envoient et relaient des données, fournissant des chemins de connexion individuels et redondants entre eux. Il est important de minimiser la latence dans certaines applications, telles que la vidéo en direct, surtout lorsque des caméras PTZ sont utilisées.

15.5 Réseaux 4G et 5G

Le système universel de télécommunications mobiles (UMTS) est une norme de communications mobiles qui comprend une série de technologies. La 3G a été la première génération technologique à offrir des débits binaires suffisamment élevés pour le transfert de données et son utilisation est aujourd'hui largement répandue, bien qu'elle soit rapidement remplacée par des normes ultérieures.

La norme 4G offre des débits binaires de pointe allant jusqu'à 100 (Mbit/s) pour les applications mobiles (par exemple, dans les véhicules en mouvement) et jusqu'à 1 Gbit/s pour une utilisation plus ou moins stationnaire. La 4G, sous ses différentes formes, est également largement utilisée.

Le successeur des réseaux 4G actuellement en cours de commercialisation dans de nombreux pays est généralement appelé 5G. En plus d'offrir des débits plus élevés, la 5G dispose également d'une plus grande capacité et peut donc connecter beaucoup plus de périphériques dans une même zone géographique. Les débits de données disponibles actuellement et les évolutions bientôt disponibles rendent les réseaux 5G particulièrement attractifs pour les applications de vidéosurveillance.

Certains dispositifs, tels que les caméras-piétons, intègrent la technologie 4G ou 5G qui permet de diffuser des vidéos en direct sur le réseau mobile.

15.6 Z-Wave®

Z-Wave a d'abord été proposé sur le marché comme système de contrôle d'éclairage destiné au grand public. Aujourd'hui, Z-Wave a évolué pour devenir un système et un protocole de réseau maillé domotique complet, qui permet à 232 périphériques intelligents de se connecter les uns aux autres au sein d'un même réseau. Bien que Z-Wave ne soit pas utilisé pour la vidéo, divers dispositifs Z-Wave, tels que des capteurs IR, des capteurs de porte/fenêtre et des boutons d'alerte sans fil s'avèrent utiles lorsqu'ils sont intégrés à un système de vidéosurveillance. Un réseau Z-Wave comprend également un contrôleur, ou hub (concentrateur) intelligent, qui est normalement le seul appareil connecté directement à Internet. Elle offre des taux de transmission allant jusqu'à 100 kbps pour les petits paquets de données. Z-Wave fonctionne sur la bande basse fréquence 908,42 MHz aux États-Unis et sur la bande 868,42 MHz en Europe. L'utilisation de basses fréquences signifie que Z-wave a une portée de signal et un taux de pénétration des murs supérieurs.

15.7 Zigbee®

Comme Z-Wave, Zigbee est un protocole réseau de proximité à faible consommation d'énergie et à faible débit. Un réseau Zigbee est néanmoins capable de prendre en charge plus de 65 000 périphériques, avec un nombre illimité de sauts entre les appareils. Zigbee, qui utilise plusieurs protocoles et normes ouvertes, ne nécessite pas l'obtention d'une licence. Le protocole fonctionne principalement à la fréquence élevée de 2,4 GHz.

16. Systèmes de gestion vidéo

La gestion de la vidéo pour la visualisation en direct, l'enregistrement, la lecture, la recherche et le stockage, en plus de la gestion des produits de vidéo, est un aspect important des systèmes de surveillance vidéo. Tout cela est géré par un système de gestion vidéo (VMS).

Axis propose VMS pour une utilisation sur site, les systèmes sous Windows, ainsi que des solutions de cloud hybride edge-based, le tout avec un accès distant et une surveillance vidéo en direct des sites, la lecture, le stockage et l'exportation de vidéos, et l'utilisation d'analyses. Les systèmes peuvent également inclure la gestion des accès et d'autres fonctions telles que l'audio pour la sécurité. Les systèmes sont accessibles à l'aide d'un PC ou d'un ordinateur portable ou via des applications sur un appareil portable. De plus, le réseau Axis de partenaires d'intégration technologique propose des solutions pour tout type de système, taille ou complexité.

16.1 Types de systèmes de gestion vidéo

Les systèmes de gestion vidéo impliquent une combinaison de plates-formes matérielles et logicielles pouvant être configurées de différentes manières. L'enregistrement, par exemple, peut être effectué localement à l'emplacement de la caméra, il peut être hébergé ou tout peut être effectué à un emplacement central. Les solutions IP offrent une flexibilité et des performances maximales pour la conception spécifique du système, avec la possibilité d'ajouter des fonctionnalités telles qu'un stockage accru ou externe, des pare-feux, des analyses et d'autres périphériques IP.

Le système à utiliser doit être fonction de vos besoins et de la manière dont vous souhaitez gérer le système. Pour un petit système dont les besoins en matière de gestion vidéo sont modestes, un système basé sur le cloud peut être idéal. Les systèmes de plus grande taille – éventuellement avec plusieurs sites – avec des enregistrements importants qui nécessitent une plus grande capacité de stockage gagneraient à fonctionner sur un réseau privé.

16.1.1 Systèmes basés sur le cloud

La gestion vidéo hébergée dans le cloud signifie que la plupart des services et des logiciels sont hébergés et accessibles via internet. Les seules parties de l'installation qui doivent être présentes sur le site sont les périphériques.

16.1.1.1 AXIS Camera Station Edge

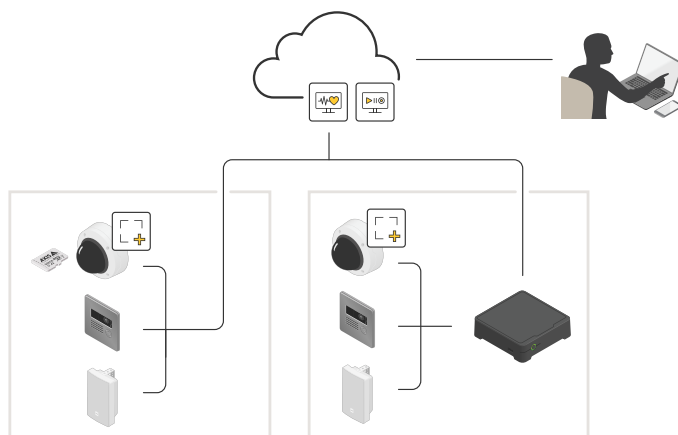
AXIS Camera Station Edge est un système de gestion vidéo (VMS) basé sur le cloud qui ne nécessite qu'une maintenance minimale et aucun serveur.

AXIS Camera Station Edge offre des connexions directes entre les caméras et le cloud, éliminant ainsi le besoin de serveurs locaux. Vous pouvez accéder à des fonctions clés telles que la vidéo en direct, la recherche chronologique et l'exportation de vidéos par le biais d'une interface utilisateur conviviale. Il est évolutif et facile d'ajouter de nouveaux sites ou périphériques aux installations existantes.

AXIS Camera Station Edge est compatible avec les caméras et périphériques Axis. Le système prend en charge le stockage dans le cloud redondant avec AXIS Camera Station Cloud Storage, ce qui garantit que les séquences enregistrées sont toujours accessibles. Les notifications d'alerte en temps réel peuvent être personnalisées à l'aide d'analyses basées sur l'IA, ce qui vous permet de connaître instantanément les activités suspectes. La configuration des périphériques et les mises à jour des logiciels sont automatisées, ce qui réduit la nécessité d'une intervention manuelle.

Vous pouvez également personnaliser les autorisations pour gérer l'accès aux fonctions du système, ce qui vous permet de contrôler qui peut effectuer certaines actions (spectateur, opérateur, administrateur). Les durées de conservation des séquences enregistrées peuvent être facilement gérées, et les périphériques peuvent être redémarrés à distance si nécessaire. La détection audio en direct vous permet de répondre aux alarmes et de communiquer avec les personnes présentes sur le site.

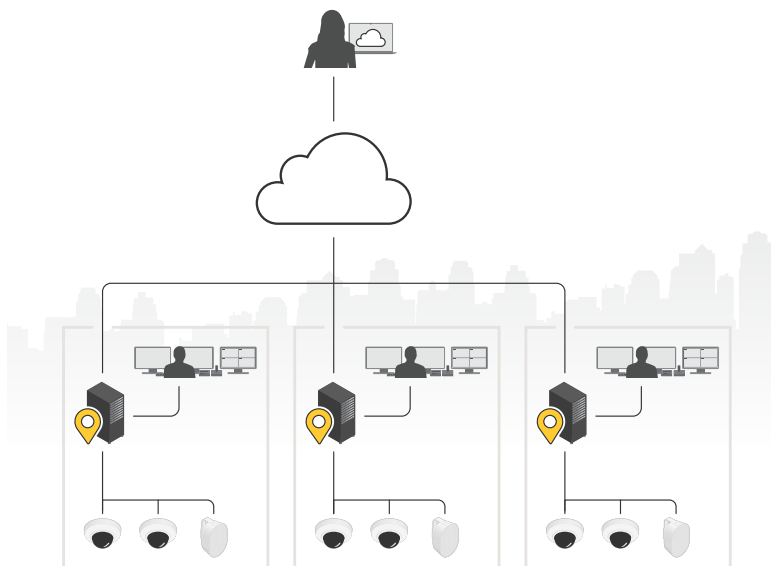
Il existe plusieurs façons d'accéder au système AXIS Camera Station Edge et de le surveiller. Une application mobile dédiée permet d'accéder aux fonctionnalités du système en déplacement, tandis qu'une application client de bureau offre une interface de gestion complète. Une interface web est également disponible, permettant de surveiller les caractéristiques du système depuis n'importe quel lieu.



À gauche : AXIS Camera Station Edge avec stockage sur carte SD. À droite : AXIS Camera Station Edge avec un enregistreur vidéo réseau Axis.

16.1.2 Réseaux privés

Si vous avez des besoins plus importants en termes de capacité ou des exigences plus strictes pour votre système de gestion vidéo, il est fort probable que vous deviez envisager une configuration sur votre propre réseau privé. Les avantages d'une telle démarche peuvent être les suivants : un meilleur contrôle des mesures de sécurité, la conformité aux réglementations qui vous obligent à sauvegarder vos données dans vos propres locaux, et des économies sur les coûts de stockage pour de grandes quantités de vidéos enregistrées. Une solution de réseau privé peut être complétée par l'ajout de capacités cloud en option.

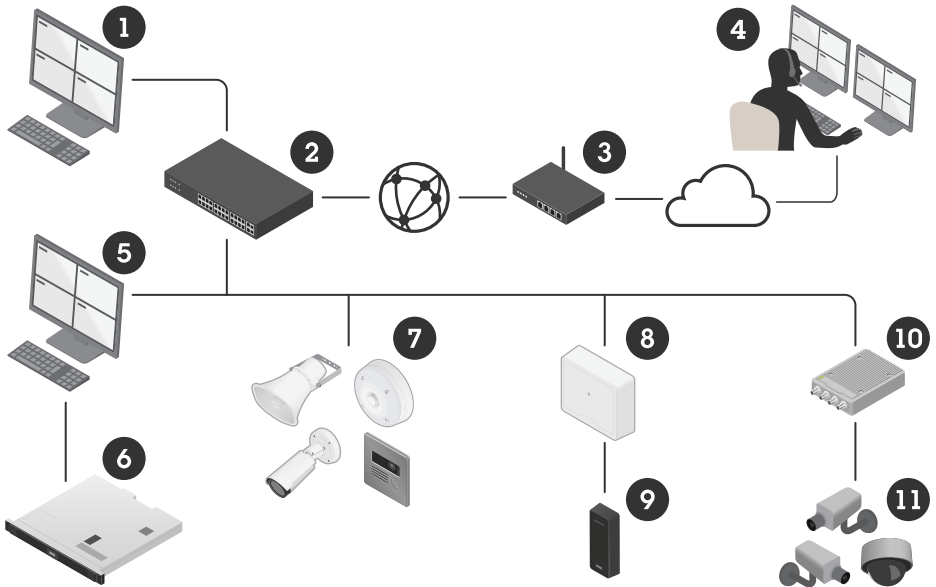


Un exemple de solution de réseau privé, complété par un accès optionnel au cloud.

16.1.2.1 AXIS Camera Station Pro

AXIS Camera Station Pro offre une fonctionnalité avancée de gestion vidéo et un système complet de surveillance et d'enregistrement incluant la gestion du contrôle d'accès. Le logiciel peut être exécuté sur des enregistreurs vidéo réseau AXIS Camera Station validés, sur du matériel tiers et sur des machines virtuelles. Il permet une installation facile et une gestion efficace des caméras Axis et d'autres périphériques. Le logiciel offre un jeu de fonctionnalités très riche qui aide les utilisateurs à gérer les incidents et à exporter les preuves. Cela inclut une configuration flexible de la vidéo en direct, un puissant moteur de règle d'action pour configurer des déclencheurs automatisés, une recherche intelligente pour trouver rapidement du contenu vidéo, une rédaction vidéo pour protéger la confidentialité des tiers et des rapports d'incident pour établir facilement un dossier.

Basée sur une application client-serveur Windows, AXIS Camera Station Pro est une solution centralisée utilisant un logiciel de gestion vidéo qui s'exécute en continu sur un serveur sur site pour les fonctions de gestion et d'enregistrement. Les enregistrements sont effectués sur le réseau privé, soit sur le même ordinateur où AXIS Camera Station Pro est installé, soit sur des périphériques de stockage distincts.



Un système de surveillance basé sur une plateforme de serveur PC ouverte avec le logiciel de gestion vidéo AXIS Camera Station Pro.

1. Logiciel client AXIS Camera Station Pro
2. Commutateur réseau
3. Routeur
4. Accès distant via le logiciel client AXIS Camera Station Pro
5. Logiciel AXIS Camera Station Pro
6. Serveur d'enregistrement
7. Produits vidéo réseau sur IP et audio Axis
8. Contrôle d'accès : contrôleur de porte
9. Contrôle d'accès : lecteur
10. Encodeur vidéo
11. Caméras analogiques

Il existe plusieurs façons de se connecter au système AXIS Camera Station Pro. Pour une expérience complète, une application client peut être installée sur n'importe quel ordinateur pour la visualisation, la lecture et l'administration, qui peuvent toutes être effectuées sur site ou à distance via Internet. La fonctionnalité multisite est prise en charge, permettant aux utilisateurs d'accéder aux caméras connectées aux différents serveurs AXIS Camera Station Pro. Il est ainsi possible de gérer la vidéo sur de nombreux sites distants ou dans un grand système, y compris le

fonctionnement vidéo avancé, le contrôle d'accès, la notification d'alarme, la configuration du système, la gestion des périphériques et la surveillance de l'état du système.

Une application mobile cliente est également fournie, permettant d'accéder à plusieurs systèmes, de recevoir des notifications, de gérer la vidéo et d'effectuer des actions – comme l'ouverture d'une porte à partir d'un interphone. En outre, vous pouvez accéder au système à l'aide d'un navigateur Web au sein de votre réseau privé ou via le cloud, afin de visualiser la vidéo en direct des caméras, de faire fonctionner les caméras PTZ, de rechercher, de rejouer et d'exporter des enregistrements, de gérer les utilisateurs et les périphériques, et de surveiller l'état du système.

AXIS Camera Station Pro constitue une base pour créer une solution avec des produits issus de la large gamme Axis, tels que l'audio, le contrôle d'accès, le suivi radar et les analyses. Grâce à l'utilisation d'API et de modules E/S, il permet également l'intégration avec d'autres systèmes tels que la gestion technique du bâtiment, le contrôle industriel et d'autres systèmes externes.

16.1.3 Solutions personnalisées des partenaires Axis

Axis travaille avec plus de 800 partenaires d'intégration technologique dans le monde entier pour garantir une meilleure intégration des solutions logicielles qui prennent en charge les produits de vidéo sur IP Axis. Ces partenaires offrent une gamme de solutions logicielles personnalisées et peuvent offrir des fonctionnalités optimisées et avancées, des fonctionnalités sur mesure pour des segments spécifiques ou des solutions axées sur les besoins de pays spécifique. Il existe également des solutions qui prennent en charge plus de 1 000 caméras et plusieurs marques de produits vidéo. Pour trouver des applications compatibles, voir www.axis.com/partner.

16.2 Caractéristiques du système

Voici les caractéristiques les plus courantes d'un système de gestion vidéo :

- > **Enregistrement.** L'enregistrement vidéo et audio est une fonction majeure d'un système de gestion vidéo. Elle comprend la mise en place de règles d'enregistrement et des moyens intelligents de rechercher des enregistrements et de les exporter vers d'autres systèmes.
- > **Visionnage.** La plupart des logiciels de gestion vidéo permettent à plusieurs utilisateurs de voir plusieurs caméras différentes en même temps et permettent de lancer les enregistrements simultanément. Avec les autres fonctionnalités disponibles comme la visualisation et la cartographie multi-écrans, les icônes des caméras peuvent être superposées sur une carte du bâtiment ou de la zone, représentant l'emplacement réel de chaque caméra. Il est également possible d'inclure des pages Web externes, permettant l'intégration à des systèmes externes. Cette option peut être utilisée pour la présentation d'interfaces de commutation, de statistiques de comptage de personnes, de rapports météorologiques et plus encore.

- > **Recherche.** Les logiciels de gestion vidéo doivent intégrer une fonction de recherche intelligente qui permet aux utilisateurs de rechercher rapidement dans le matériel vidéo les personnes et les véhicules d'intérêt. AXIS Camera Station dispose d'une fonction de recherche intelligente alimentée par les données sur les objets en mouvement de la caméra. Les données sont ensuite traitées à l'aide d'algorithmes de machine learning et de deep learning pour classer rapidement les objets tels que les personnes, les voitures, les camions et les vélos. C'est compatible avec la plupart des caméras Axis, sans matériel ou logiciel supplémentaire. Les performances peuvent facilement être améliorées en ajoutant une capacité de serveur supplémentaire et en utilisant des caméras Axis avec des capacités de machine learning ou de deep learning.
- > **Gestion des événements et analyse vidéo.** Les logiciels de gestion vidéo peuvent recevoir, traiter et associer des notifications d'événement provenant de différentes sources, tels que des dispositifs de contrôle des accès, des terminaux de point de vente, des analyses et les produits vidéo eux-mêmes. Quand une notification d'événement est déclenchée, le système de gestion vidéo peut l'enregistrer, l'associer à un clip vidéo provenant d'une caméra voisine et alerter un opérateur ou un enquêteur via une fenêtre contextuelle sur le moniteur, ou en envoyant une notification à un smartphone.
- > **Administration et gestion.** Cela comprend l'installation, les mises à niveau des logiciels des périphériques, la sécurité, le journal d'audit et les configurations des paramètres des caméras et d'autres composants, tels que les caisses enregistreuses, les contrôleurs de porte et les stations de porte. Plus le système est grand, plus il faut pouvoir gérer efficacement les périphériques. La surveillance de l'état de santé du système fournit un aperçu du système, notamment du matériel d'enregistrement, et génère des notifications si un périphérique ou le système est hors ligne. Un logiciel de gestion vidéo doit aussi offrir des options pour gérer les utilisateurs autorisés, les mots de passe, les niveaux d'accès des utilisateurs et l'accès différencié à des dispositifs spécifiques. Certains logiciels de gestion vidéo peuvent hériter d'une base de données d'utilisateurs Windows, ce qui évite de configurer et de maintenir une base de données d'utilisateurs distincte.

16.3 Systèmes intégrés

Lorsque la vidéo est intégrée à d'autres systèmes tels que le contrôle d'accès, les points de vente, la gestion des bâtiments, les systèmes d'information de patient, ou les systèmes logistiques, des informations provenant d'autres systèmes peuvent être utilisées pour déclencher des fonctions telles que les enregistrements basés sur des événements dans le système de vidéo sur IP, et vice versa. De plus, une interface commune est disponible pour gérer les différents systèmes.

16.3.1 Contrôle d'accès

Le contrôle d'accès est l'une des intégrations VMS les plus utilisées. AXIS Camera Station Secure Entry fait partie du logiciel AXIS Camera Station Pro et propose une solution unifiée combinant des fonctionnalités de surveillance et de contrôle d'accès. En savoir plus sur le contrôle d'accès dans le chapitre .

16.3.2 Point de vente

L'introduction de la vidéo sur IP dans les magasins a facilité son intégration aux systèmes de point de vente (POS).

Cette intégration permet de lier toutes les transactions de caisse enregistreuse à la vidéo réelle des transactions. Cela permet de détecter et de prévenir la fraude et les vols commis par les employés et les clients. Les exceptions au niveau du point de vente, telles que les retours, les valeurs saisies manuellement, les corrections de ligne, les annulations de transaction, les achats effectués par des collègues, les remises, les articles spécialement étiquetés, les échanges et les remboursements, peuvent être vérifiées visuellement en activant des enregistrements basés sur des événements lorsque ces événements se produisent. Les secondes avant et après un événement peuvent également être capturées à l'aide de tampons d'enregistrement spécifiques. Les enregistrements basés sur des événements augmentent la qualité des documents enregistrés, tout en réduisant les besoins de stockage et le temps nécessaire pour rechercher des incidents.

16.3.3 Gestion des bâtiments

La vidéo peut être intégrée dans un système de gestion des bâtiments qui contrôle un certain nombre de systèmes allant du chauffage, de la ventilation et de la climatisation aux systèmes de sécurité, de sûreté, d'énergie et d'alarme incendie. Voici quelques exemples d'applications :

- > Une alarme de panne d'équipement peut déclencher une caméra pour montrer la vidéo à un opérateur, en plus d'activer les alarmes au système de gestion des bâtiments.
- > Un système d'alarme incendie peut déclencher une caméra pour surveiller les portes de sortie et commencer l'enregistrement à des fins de sécurité. Cela permet aux premiers intervenants et aux gestionnaires d'immeubles d'évaluer la situation à toutes les issues de secours en temps réel et de concentrer leurs efforts aux endroits requis.
- > L'analyse peut être utilisée pour détecter le flux inversé de personnes dans un bâtiment, par exemple lorsqu'une porte est ouverte ou non sécurisée suite à divers événements comme une évacuation de l'immeuble.
- > Des alertes vidéo automatiques peuvent être envoyées lorsque quelqu'un pénètre dans une zone ou une pièce où l'accès est restreint.

- > Les informations de détection de mouvement vidéo provenant d'une caméra située dans une salle de réunion peuvent être utilisées avec des systèmes d'éclairage et de chauffage pour éteindre la lumière et le chauffage d'une pièce une fois que plus personne ne s'y trouve, économisant ainsi de l'énergie.

16.3.4 Systèmes de contrôle industriel

La vérification visuelle à distance est souvent bénéfique et nécessaire dans les systèmes d'automatisation industrielle complexes. En ayant accès à la vidéo en réseau via la même interface que celle utilisée pour surveiller un processus, l'opérateur n'a pas besoin de quitter le panneau de contrôle pour vérifier visuellement une partie du processus. De plus, lorsqu'une opération est défectueuse, la caméra réseau peut être déclenchée pour envoyer des images. Dans certains procédés sensibles en salle blanche ou dans des installations contenant des produits chimiques dangereux, la vidéosurveillance est le seul moyen d'avoir un visuel sur les processus. Il en va de même pour les réseaux électriques avec sous-stations dans des sites distants.

16.3.5 RFID

Les systèmes de suivi qui impliquent la RFID (identification par radiofréquence) ou des méthodes similaires sont utilisés dans de nombreuses applications pour assurer le suivi des articles. Par exemple, les articles avec tag d'un magasin peuvent être suivis avec des séquences vidéo pour éviter le vol ou fournir des preuves. La RFID peut aussi être utilisée dans les aéroports pour le traitement des bagages, afin de les suivre et les diriger vers la bonne destination. Lorsqu'elle est intégrée à la vidéosurveillance, vous disposez de preuves visuelles de la perte ou de l'endommagement des bagages, et pouvez optimiser les procédures routinières de recherche.

17. Technologies cloud

17.1 Passage au cloud

Les technologies cloud ont révolutionné notre approche de la surveillance vidéo sur IP. En s'appuyant sur des services et des solutions basés sur le cloud, les utilisateurs peuvent désormais accéder à leurs flux vidéo à distance, à tout moment et de n'importe où. Cette flexibilité accrue permet une surveillance et des réponses plus efficaces aux incidents de sécurité.

L'utilisation de services et de solutions basés sur le cloud présente de nombreux avantages. Les services gérés dans le cloud peuvent notamment effectuer des mises à jour automatiques des logiciels, ce qui élimine le besoin de maintenance manuelle et réduit le risque de vulnérabilité des systèmes. L'évolutivité est un autre avantage clé, permettant aux utilisateurs d'ajouter ou de supprimer facilement des caméras et des capacités de stockage en fonction de leurs besoins. Le stockage dans le cloud constitue une solution sécurisée et évolutive pour le stockage de grandes quantités de données vidéo. En stockant les séquences hors site, les sociétés peuvent réduire le risque de perte de données due à une défaillance du matériel ou à des dommages physiques.

En outre, les analyses basées sur le cloud permettent des fonctions avancées telles que la détection d'objets, le comptage de personnes et la reconnaissance des plaques d'immatriculation, ce qui renforce la sécurité et l'efficacité de l'entreprise. La solution la plus efficace passe souvent par une configuration hybride qui associe une classification des objets basée sur la caméra à des algorithmes basés sur un serveur ou sur le cloud pour les tâches qui nécessitent une plus grande puissance de calcul.

Dans l'ensemble, l'intégration des technologies cloud dans les systèmes de vidéo sur IP offre une flexibilité, une évolutivité et une sécurité accrues, ce qui en fait une option intéressante pour les entreprises et les organisations qui cherchent à moderniser leur infrastructure de surveillance.

17.2 Installations cloud

Souvent, la gestion de la vidéo et des périphériques sur le cloud repose sur un service hébergé et accessible via Internet. Via des abonnements, vous pouvez payer et utiliser autant (ou aussi peu) de service que vous le souhaitez. Toute définition d'un système basé sur le cloud englobe à la fois les fonctions du système et l'emplacement de ces fonctions. Voici quelques définitions courantes :

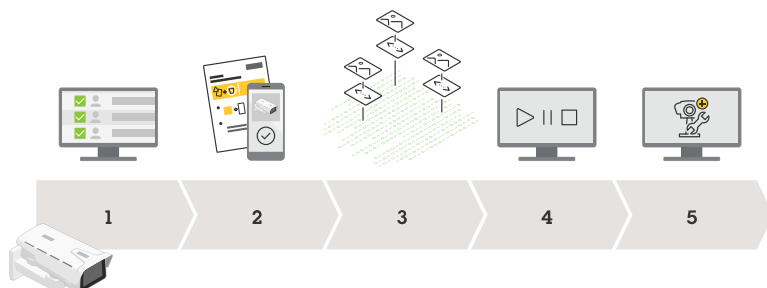
- > **Cloud direct** : Relevant de la technologie « camera-to-cloud » ou « pure cloud », ces solutions ont généralement trois fonctions principales dans le cloud : la visualisation, la gestion et le stockage. Certaines d'entre elles exécutent des outils d'analyse comme applications cloud, bien qu'il soit souvent plus rentable de les utiliser à la périphérie du réseau.
- > **Cloud hybride** : Ce type de solution désigne souvent les systèmes dont certaines fonctions sont exécutées dans le cloud et d'autres en local. C'est le cas par exemple des clouds à la demande, pour lesquels la plupart des fonctions sont théoriquement exécutables dans le cloud, alors que dans la pratique, certaines fonctions ou la totalité sont utilisées en périphérie pour réduire la latence.
- > **Cloud relais** : Ce type de solution n'offre que la visualisation dans le cloud et, éventuellement, certaines fonctions de gestion de base. Toutes les autres fonctions sont locales ou disponibles via d'autres solutions.

La solution optimale dépendra des besoins, des paramètres et de la configuration du système. Pour les sociétés disposant de plusieurs sites de petite taille, une solution basée uniquement sur le cloud peut s'avérer la plus judicieuse, tandis que pour une société disposant d'un site plus important, une solution installée uniquement sur site peut être la bonne option. Pour la plupart des sociétés, la combinaison de puissants dispositifs périphériques connectés, avec le cloud et le réseau privé, constitue la solution idéale.

17.3 Axis Cloud Connect

Axis Cloud Connect est une plateforme cloud hybride ouverte qui, associée aux périphériques Axis, ouvre la voie à des services gérés, comme la gestion des dispositifs et du système, la livraison de contenu vidéo et de données et la sécurité et le support. Les services dont vous bénéficiez sont basés sur les technologies incluses dans la plateforme.

Les solutions utilisant des périphériques Axis et construites avec Axis Cloud Connect, telles que AXIS Camera Station, AXIS Device Manager Edge ou AXIS Device Manager Extend, vous offrent des opérations vidéo, une gestion du cycle de vie des périphériques et un accès aux données plus flexibles et plus efficaces. Elles offrent également de nouvelles possibilités en matière de sécurité, de sûreté, d'efficacité du fonctionnement et d'intelligence économique.



Exemples de services via Axis Cloud Connect : 1) Gestion des utilisateurs et des accès, 2) Intégration sécurisée des périphériques, 3) Média vers le cloud, 4) Fonctionnement en direct, 5) Gestion des périphériques.

18.Considérations de conception du système

L'un des principaux avantages d'un système vidéo sur IP est sa flexibilité et son évolutivité : la liberté de combiner les composants les plus appropriés de différents fournisseurs et la possibilité d'optimiser ou d'étendre le système à n'importe quelle taille.

Il est essentiel de choisir la bonne caméra, de l'installer et de la protéger correctement, de la configurer de manière à ce qu'elle puisse s'adapter aux complexités de la scène, diffuser en temps réel ou enregistrer la vidéo au bon moment, au bon format et dans la qualité la mieux adaptée. Dans le même temps, tout dépend des caméras sélectionnées, des paramètres de celles-ci (tels que la résolution, la compression et la fréquence d'images) et le nombre de caméras déployées pour concevoir la solution réseau et de stockage idéale.

AXIS Site Designer vous aide à sélectionner les caméras adaptées à chaque scénario de surveillance, ainsi qu'à ajouter des accessoires et à choisir une solution d'enregistrement. Lorsque vous avez terminé votre projet de conception, AXIS Site Designer imprime une nomenclature complète comprenant tout ce dont vous avez besoin pour terminer votre installation.

18.1 Sélection d'une caméra

Cette section indique ce qu'il faut garder à l'esprit lors de la sélection d'une caméra.

18.1.1 Types de caméras

Il faut d'abord comprendre la scène et ses conditions pour déterminer quels types de caméras sont adaptées et combien de caméras sont nécessaires pour couvrir une zone. Vous devez également prendre en considération l'objectif de votre surveillance.

- > **Intérieur ou extérieur.** Si vous installez la caméra à l'extérieur, utilisez une caméra conçue pour l'utilisation en extérieur ou installez-la dans un boîtier de protection approprié. Recherchez l'indice IP (IP66 ou plus élevé) ou NEMA (National Electrical Manufacturers Association) (4X ou plus élevé). La caméra doit également avoir une fonctionnalité d'auto-diaphragme.
- > **Caméra panoramique/inclinaison/zoom (PTZ) ou caméra fixe.** Les caméras PTZ dotées d'un zoom optique important peuvent fournir des images très détaillées et couvrir une vaste zone. Gardez à l'esprit que pour tirer pleinement parti des capacités d'une caméra PTZ, un opérateur doit pouvoir contrôler les mouvements ou un tour automatique doit être mis en place. Pour les enregistrements de surveillance sans surveillance en direct, les caméras fixes sont généralement plus rentables.
- > **Exigences en matière de sensibilité à la lumière et d'éclairage.** La sensibilité à la lumière est l'un des facteurs les plus importants d'une caméra. La fonctionnalité jour et nuit vous permet d'obtenir des images dans des conditions naturellement trop sombres. Certaines caméras sont fournies avec des voyants DEM IR intégrés qui fournissent un éclairage efficace et discret, invisible à l'œil nu, mais qui permet d'avoir des images nettes dans l'obscurité.
- > **Obscurité complète et protection périmétrique.** Les caméras thermiques peuvent détecter les mouvements même dans l'obscurité totale et dans d'autres conditions difficiles. Elles peuvent généralement détecter les mouvements à des distances plus élevées que les caméras conventionnelles.
- > **Protection contre le vandalisme et le sabotage et autres exigences spéciales en matière de boîtier.** Une protection adéquate contre l'eau, la poussière, la température et le vandalisme est essentielle.
- > **Surveillance cachée ou très discrète.** Ce cas d'utilisation vous aidera à choisir les caméras qui ont un effet dissuasif ou qui sont installées de manière moins visible.
- > **Zone de couverture.** Pour un lieu donné, vous devez déterminer les zones d'intérêt, le nombre de zones à couvrir, si les zones sont proches ou éloignées les unes des autres. Par exemple, si deux zones d'intérêt relativement petites sont proches l'une de l'autre, vous pouvez éventuellement utiliser une seule caméra haute résolution avec un objectif grand angle à la place de deux caméras de résolution inférieure.
- > **Vue d'ensemble ou images hautement détaillées.** Déterminer le champ de vision ou le type d'image à capturer : un aperçu ou des images très détaillées pour l'identification de personnes ou d'objets, par exemple, la reconnaissance faciale ou de plaques d'immatriculation, ou la surveillance de points de vente (POS).
- > **Analyses Edge-based ou sur serveur.** L'analyse permet une surveillance et des recherches efficaces, et peut fournir des informations précieuses. L'analyse edge-based offre de nombreux

avantages (si la caméra dispose d'une puissance de traitement suffisante), mais l'analyse énergivore peut nécessiter un serveur d'analyse dédié. Pensez à pérenniser votre investissement en achetant des caméras qui prennent en charge des outils d'analyse et offrent les performances nécessaires pour le type d'analyse dont vous pourriez avoir besoin ultérieurement.

18.1.2 Qualité d'image

Bien que la qualité de l'image soit l'un des aspects les plus importants, il peut être difficile de sélectionner la bonne caméra. En réalité, de nombreux aspects de la qualité de l'image ne peuvent être quantifiés ou mesurés. La meilleure façon de déterminer la qualité de l'image est d'installer différentes caméras et de comparer la vidéo produite. Gardez à l'esprit que bien qu'une caméra puisse fournir des images fixes de haute qualité, la qualité de l'image peut se détériorer lorsque des mouvements importants sont introduits dans la scène ou dans des conditions de faible luminosité.

De nombreux facteurs affectent la qualité de l'image. Par exemple, la balance des blancs et la capacité de la caméra à s'adapter à différentes conditions d'éclairage, du sodium haute pression fluorescent à la lumière LED, sont importantes pour garantir la fidélité des couleurs. La faible luminosité, le contre-jour, la lumière dynamique et d'autres conditions d'éclairage extrêmes présentent des défis que la caméra doit pouvoir relever. Généralement, une caméra haute résolution est moins sensible à la lumière qu'une caméra basse résolution. En d'autres termes, vous devrez peut-être envisager de sacrifier la résolution pour une meilleure performance en faible luminosité, ou encore utiliser une caméra avec un capteur et des algorithmes de traitement conçus pour relever ces défis.

18.1.3 Résolution

Lors de la conception d'un système de surveillance, il est important de prendre en compte sa vocation. Vous pouvez consulter les spécifications techniques pour déterminer la caméra qui a la meilleure résolution, mais afin d'optimiser les coûts et les efforts, vous devez vous concentrer sur la caméra et la configuration qui correspondent le mieux à vos besoins opérationnels. Par exemple, avez-vous besoin d'identifier des personnes à partir des séquences vidéo ou avez-vous simplement besoin de détecter qu'une personne est présente ?

Nous pouvons faire la différence entre les besoins suivants : **D**étecter, **O**bserver, **R**econnaître et **I**dentifier. Ces exigences sont parfois désignées dans le cadre de l'acronyme DORI.

Spécification de fonctionnement	Niveau de détail
Détection	Il est possible de déterminer si une personne est présente.
Observation	Il est possible de déterminer le nombre de personnes présentes et de voir les détails caractéristiques, tels que des vêtements distinctifs.
Reconnaissance	Il est possible pour un observateur de déterminer s'il a déjà vu ou non telle ou telle personne.
Identification	Il est possible d'identifier une personne.

tableau 18.1a *Besoins opérationnels courants en vidéosurveillance.*

Les spécifications de ces besoins (pour les caméras visuelles) proviennent de la norme internationale IEC 62676-4 (Systèmes de vidéosurveillance destinés à être utilisés dans les applications de sécurité – Partie 4: Directives d'application)

À noter que les spécifications de ces besoins opérationnels sont valables dans les situations où les images des vidéos sont interprétées par des opérateurs humains. Pour l'analyse ou d'autres systèmes où l'analyse d'image est effectuée par un logiciel, d'autres définitions des besoins opérationnels s'appliqueraient. L'imagerie thermique (l'utilisation de caméras thermiques) utilise également une autre série de spécifications des besoins opérationnels.

La caméra que vous choisissez doit pouvoir fournir le champ de vision adéquat ainsi qu'une densité de pixels adéquate sur les objets prioritaires, comme le visage de personnes.

La base des densités de pixels recommandées est le nombre de pixels nécessaires pour représenter la largeur d'un visage humain, avec ses caractéristiques distinctives d'identification, au niveau de détail requis. Pour obtenir une densité de pixels normalisée, la densité de pixels du visage peut être recalculée en fonction du nombre correspondant de pixels requis par mètre ou par pied, avec l'hypothèse qu'un visage humain moyen a une largeur de 16 cm (6 5/16 pouces). Le tableau répertorie le résultat des densités de pixels pour les différentes catégories de besoins opérationnels.

Spécification de fonctionnement	Densité de pixels requise		
Détection	4 px/visage	25 px/m	8 px/pi
Observation	10 px/visage	63 px/m	20 px/pi

Spécification de fonctionnement	Densité de pixels requise		
Reconnaissance	20 px/visage	125 px/m	40 px/pi
Identification	40 px/visage	250 px/m	80 px/pi

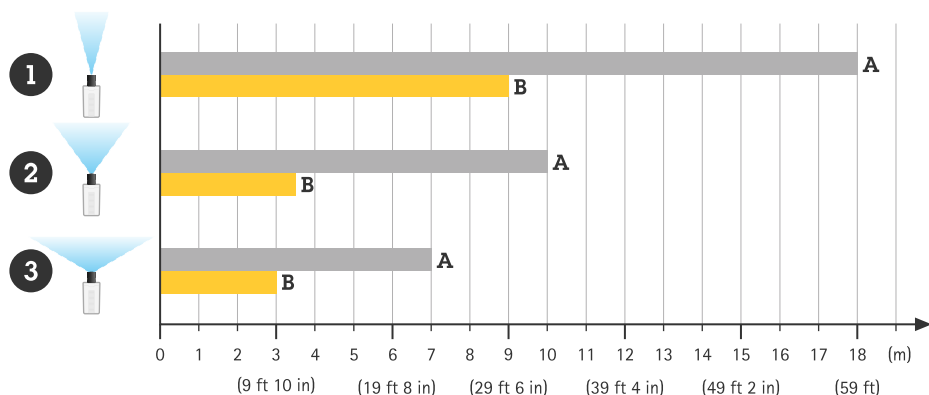
tableau 18.1b *Densités de pixels pour les différents besoins opérationnels.*

Il est généralement recommandé, par exemple dans la norme IEC 62676-4, qu'il y ait au moins 40 pixels sur la largeur d'un visage humain pour permettre l'identification. Des densités de pixels encore plus élevées peuvent être très utiles et offrir une marge de sécurité dans des conditions difficiles, telles qu'un éclairage sous-optimal et les lieux où les personnes ne font pas directement face à la caméra. Si une installation n'est pas conforme aux directives sur la densité de pixels, cela ne signifie pas nécessairement que les besoins opérationnels ne seront pas respectés. En réalité, il existe toujours d'autres facteurs, tels que la direction de la lumière, la qualité de l'optique et la compression de l'image, qui ont des conséquences sur le résultat.

Il faut également noter que si un écran externe est utilisé pour surveiller la scène, la capacité de détecter, d'observer, de reconnaître ou d'identifier des individus dépend en grande partie de la résolution de l'écran.

Les caméras Axis disposent d'une fonction de compteur de pixels pour faciliter le contrôle de la densité de pixels dans l'image. Il s'agit d'une aide visuelle en forme de cadre, avec la largeur et la hauteur du cadre (mesurée en pixels) clairement indiquée.

La densité de pixels d'un objet sous surveillance dépend de la résolution du capteur de la caméra, de la distance de l'objet par rapport à la caméra et du type d'objectif utilisé. Le choix de l'optique est particulièrement important, et c'est une science à part ; c'est pourquoi il est conseillé de travailler avec des fournisseurs qui proposent des caméras testées de bout en bout avec l'objectif inclus. L'illustration fournit un exemple général de la façon dont la distance maximale pour la reconnaissance et l'identification peut changer en fonction des types d'objectifs (à savoir les différents champs de vision).



Exemples de la manière dont les distances maximales pour la reconnaissance (A) et l'identification (B) changent avec le type d'objectif : téléobjectif (1), normal (2), grand angle (3).

Axis propose des outils en ligne pour la conception d'un site de surveillance, en tenant compte à la fois de la densité de pixels et des nombreux autres facteurs. AXIS Site Designer peut aider à calculer la résolution de l'image et le champ de vision en fonction du modèle et de la position de la caméra. L'outil permet de spécifier la densité de pixels requise et d'ajuster la hauteur de montage et le champ de vision de la caméra pour déterminer si la caméra peut ou non répondre aux besoins du cas d'utilisation.

18.1.4 Compression

Les caméras prenant en charge plus d'un type de standard de compression vidéo offrent aux utilisateurs une plus grande flexibilité en matière d'optimisation des besoins de visualisation et d'enregistrement.

La conception du réseau et du système de stockage dépend fortement de la norme de compression sélectionnée. Voici quelques recommandations de base :

- > **AV1.** Cette nouvelle norme est l'option recommandée si votre système la prend en charge. AV1 est optimisée pour la transmission vidéo sur Internet et permet un flux de données et un stockage à haute résolution et à moindre coût.
- > **H.264.** La norme de compression vidéo la plus utilisée en vidéosurveillance. Par rapport à la vidéo AV1, la vidéo H.264 nécessite environ deux fois plus de stockage.
- > **H.265.** L'encodage H.265 ne répond pas encore entièrement aux exigences des vidéos de type surveillance. La plupart des équipements de surveillance prennent en charge l'encodage H.265,

mais la prise en charge du décodeur et des navigateurs est limitée. De nombreux utilisateurs doivent continuer à utiliser H.264 pour visionner des vidéos sur leurs clients préférés, mais cela ne devrait pas poser de problème car Zipstream avec H.264 est très efficace en termes de débit.

- > **Axis Zipstream.** Filtre les zones à faible intérêt et les compresse plus radicalement, tout en enregistrant les détails importants et les mouvements dans une vidéo de qualité supérieure. Cette commutation entre une valeur GOP maximale et une valeur inférieure réduit considérablement le débit et les exigences en matière de stockage et de bande passante.

18.1.5 Fonctions réseau

La fonctionnalité de mise en réseau est tout aussi importante que les images haute qualité. Outre la connectivité Ethernet, une caméra réseau doit également prendre en charge les fonctionnalités suivantes :

- > **Power over Ethernet (PoE)** signifie que la caméra peut recevoir du courant sur le même câble que les données, éliminant la nécessité de faire passer des câbles d'alimentation. Les caméras PTZ extérieures peuvent nécessiter plus de puissance, qui peut être fournie par un injecteur.
- > Le protocole **Dynamic Host Configuration Protocol (DHCP)** est utilisé pour gérer les adresses IP. Un commutateur ou un routeur DHCP attribue automatiquement une adresse IP à chaque périphérique connecté. Cependant, la prévisibilité des adresses IP statiques et la possibilité de faire correspondre les adresses IP aux numéros d'identification des caméras peuvent être préférables.
- > **Cryptage HTTPS** pour une communication sécurisée.
- > Le protocole **SNMP** aide les administrateurs à surveiller l'état du réseau et à déterminer si les périphériques connectés nécessitent une intervention.
- > Le **filtrage d'adresse IP** permet de limiter l'accès à la caméra à certaines adresses IP.
- > Les **fonctions de cybersécurité** sont essentielles pour protéger la caméra et le réseau auquel elle est connectée. Fonctions intégrées de cybersécurité pour neutraliser différents types de cyberattaques, corriger efficacement les vulnérabilités et interdire l'accès non autorisé à votre système. Par exemple, le *démarrage sécurisé* garantit que tout code non authentifié et modifié est bloqué et rejeté pendant le processus de démarrage avant qu'il ne puisse attaquer ou infecter le système. Avec le *système d'exploitation signé*, vous pouvez vérifier l'intégrité du logiciel du périphérique avant d'installer de nouveaux périphériques ou de mettre à niveau des périphériques existants.
- > La **technologie sans fil** est une option intéressante s'il n'est pas pratique ou s'il est coûteux de faire passer un câble vers une caméra réseau. L'accès sans fil peut également être fourni pour une caméra réseau standard en l'équipant d'un pont sans fil ou d'un dongle sans fil.

18.1.6 Autres fonctionnalités

En plus de fournir un flux vidéo, les caméras réseau présentent de nombreuses autres fonctionnalités. Il est également important d'évaluer les capacités de la caméra que vous allez choisir. Voici quelques exemples de fonctionnalités supplémentaires :

- > **Audio pour la communication et la détection.** Les utilisateurs peuvent détecter et classer différents types de sons et communiquer des instructions, des ordres ou des demandes aux visiteurs ou aux intrus. Lorsque les microphones détectent des sons dont le volume dépasse un seuil défini, ils peuvent déclencher des alarmes ou des caméras pour démarrer l'enregistrement. Déterminez si l'audio unidirectionnel ou bidirectionnel est requis.
- > **Outils d'analyse intégrés.** L'intelligence intégrée rend le système plus évolutif et aide à réduire les besoins en bande passante et en stockage, car la caméra peut décider quand envoyer et traiter la vidéo.
- > **Connecteurs d'entrée / sortie (E/S).** En connectant des périphériques d'entrée externes à une caméra (comme un contact de porte, un détecteur de mouvement infrarouge, un détecteur radar, un capteur de bris de verre ou un capteur de choc), celle-ci peut réagir à un événement externe en envoyant et enregistrant des vidéos, par exemple. Les sorties permettent à la caméra ou à un opérateur distant de contrôler des périphériques externes, comme des dispositifs d'alarme, des verrous de porte ou des lumières.
- > **Alerteurs audiovisuels.** Un avertisseur audiovisuel peut être utilisé pour dissuader des intrus ou améliorer l'efficacité opérationnelle grâce à un éclairage stroboscope et des alarmes sirène. Ce périphérique entièrement connecté en réseau est particulièrement utile lorsqu'il est connecté à une caméra avec protection périmétrique ou une analyse des plaques d'immatriculation (LPR).
- > **Connectivité bord à bord.** La technologie bord à bord permet aux périphériques IP de communiquer directement entre eux. Elle offre une fonction d'appairage intelligente entre, par exemple, des caméras Axis et des produits audio ou radar Axis.
- > **Radar.** Un détecteur de mouvement par ondes radar représente le complément précieux d'un système de vidéosurveillance. Outre le fait qu'il déclenche une alarme lorsqu'il détecte un intrus, il peut également déclencher l'enregistrement pour la vérification visuelle. Si le radar est associé à une caméra PTZ, il peut contrôler la caméra automatiquement. Il existe également des caméras combinées avec un radar entièrement intégré. Elles peuvent détecter des objets sur de larges zones quelle que soit la visibilité, puis visualiser la vitesse et la distance des objets en mouvement directement dans la vue de l'application.

- > **Fonctions de gestion des alarmes.** Les caméras évoluées peuvent effectuer des tâches de gestion des alarmes telles que le traitement et la liaison des entrées, des sorties et d'autres événements. Les tampons avant et après alarme dans une caméra peuvent enregistrer de la vidéo avant et après le déclenchement d'une alarme.
- > **Autres dispositifs de sécurité physique.** Lors de l'évaluation d'un système de vidéosurveillance, examinez également d'autres systèmes, tels que le contrôle d'accès, l'intercom, l'audio et la détection d'intrusion, pour déterminer s'il existe un moyen de concevoir un système intégré couvrant tous vos besoins en matière de sécurité physique.
- > **Support multi-applications et facilité d'intégration.** Assurez-vous de sélectionner des caméras disposant d'interfaces de programmation d'application (API) ouvertes qui peuvent s'intégrer à plusieurs applications logicielles de gestion vidéo. Toutes les caméras Axis sont compatibles avec la norme ONVIF, qui assure l'interopérabilité entre les produits de vidéo sur IP, quel que soit le fabricant.

18.2 Installation d'une caméra réseau

L'installation d'une caméra réseau est tout aussi importante que le processus de sélection. Voici quelques recommandations sur la façon de réaliser une vidéosurveillance de haute qualité basée sur le positionnement de la caméra.

18.2.1 Objectif de surveillance

Pour mieux positionner une caméra, vous devez savoir de quel type d'image vous avez besoin. Par exemple, pour suivre des personnes ou des objets en mouvement, depuis et dans diverses directions, vous aurez besoin d'une vue d'ensemble, ce qui vous permettra de mieux repérer ce genre d'événements. Après avoir sélectionné une caméra de vue d'ensemble appropriée, vous pouvez l'installer là où elle vous permettra d'obtenir les images souhaitées.

AXIS Site Designer peut vous aider à trouver la position la mieux adaptée et fournit des plug-ins pour divers diagrammes et logiciels 3D. Ces outils vous aideront à placer les caméras, calculer les angles de vision et la couverture, ainsi qu'à trouver les angles morts et les éléments bloquant la vue.

18.2.2 Gestion de l'éclairage difficile

La performance des caméras traditionnelles est amoindrie lors de scènes peu éclairées, à cause de la lumière directe du soleil ou d'autres types de contre-jour. Les caméras Axis sont équipées de différentes solutions permettant d'obtenir de bonnes images malgré les mauvaises conditions d'éclairage. Il s'agit par exemple de Lightfinder, de LED IR et de Forensic WDR. Si la scène et le lieu

le permettent, vous pouvez ajouter un éclairage externe. Certaines caméras sont équipées de pare-soleil qui aident à réduire l'impact de la lumière directe du soleil et facilitent leur placement.

Même si les réglages automatiques des caméras Axis fournissent généralement les meilleures images, il est également possible de régler les paramètres manuellement (la luminosité, la netteté, la balance des blancs et le WDR, par exemple).

Les caméras thermiques, qui sont une alternative aux caméras visuelles, permettent de surmonter les conditions d'éclairage difficiles.

18.2.3 Choix de l'objectif

Le champ de vision requis doit être défini lors de la sélection de l'objectif. Le champ de vision est déterminé par la distance focale de l'objectif et la taille du capteur d'image. La distance focale d'un objectif est définie comme la distance entre l'objectif d'entrée (ou un point spécifique dans un assemblage d'objectifs complexe) et le point où tous les rayons lumineux convergent (normalement le capteur d'image de la caméra). Plus la focale de l'objectif est longue, plus le champ de vision (FoV) sera étroit.

Le FoV peut être classé en trois types :

- > Vue normale : c'est le même champ de vision que celui de l'œil humain.
- > Téléobjectif : un champ de vision plus étroit, fournissant, en général, des détails plus fins que ceux que l'œil humain peut voir. Un téléobjectif a généralement moins de capacité de collecte de lumière qu'un objectif normal.
- > Grand angle : un champ de vision élargi avec moins de détails par rapport à une vision normale. Un objectif grand angle fournit généralement une bonne profondeur de champ et une performance acceptable en cas de faible luminosité.

AXIS Site Designer et l'outil de sélection de produits peuvent vous aider à choisir la caméra et l'objectif adaptés à vos besoins. Consultez le portail des outils Axis, www.axis.com/tools.

18.3 Protection physique de la caméra

Les caméras de surveillance sont souvent placées dans des environnements très exigeants. Dans les installations extérieures, elles doivent être protégées des conditions météorologiques adverses. Dans les environnements industriels, les caméras peuvent nécessiter une protection contre les dangers tels que la poussière, les acides ou les substances corrosives. Dans les véhicules tels que les bus et les trains, les caméras doivent résister à une forte humidité, à la poussière et aux vibrations.

Certaines caméras peuvent également nécessiter une protection contre le vandalisme et le sabotage.

Les sections ci-dessous traitent de sujets tels que les caractéristiques de protection, les boîtiers externes, le positionnement des caméras fixes dans les boîtiers, les dômes, la protection contre le vandalisme et le sabotage, ainsi que les types de supports.

18.3.1 Protection et classification

Les principales menaces qui pèsent sur l'environnement d'un produit vidéo, en particulier lorsqu'il est installé à l'extérieur, sont le froid, la chaleur, l'eau, la poussière et la neige. Aujourd'hui, de nombreux périphériques Axis pour l'intérieur et l'extérieur sont conçus pour répondre aux défis environnementaux, dès leur déballage, et ne nécessitent pas de boîtiers distincts. Cela se traduit par un périphérique plus compact et une installation simplifiée. Par exemple, les caméras Axis conçues pour fonctionner à des températures allant jusqu'à 75 °C (167 °F) sont très compactes, même avec un système de refroidissement actif intégré.

Une conception de caméra peut également assurer la fiabilité et la maintenance de la durée de vie d'une caméra, en particulier dans des conditions de fonctionnement extrêmes. Par exemple, certaines caméras fixes et PTZ d'Axis intègrent le contrôle de température arctique, qui permet de démarrer les caméras à -40 °C (-40 °F) sans causer d'usure supplémentaire des pièces mécaniques. Certaines caméras dômes Axis sans contrôle de température arctique peuvent également démarrer à -40 °C/-40 °F et envoyer des vidéos immédiatement.

Le niveau de protection des boîtiers, qu'ils soient fournis séparément ou intégrés à l'équipement, est indiqué généralement en référence à des normes, notamment IP, NEMA et IK. La classe IP, acronyme de « Ingress Protection », est connue dans le monde entier. NEMA désigne l'Association nationale des fabricants d'appareils électriques et la norme s'applique aux États-Unis. Les normes IK concernent les chocs mécaniques externes et s'appliquent dans le monde entier.

Les indices environnementaux les plus courants pour les dispositifs intérieurs Axis sont IP42, IP51 et IP52, qui assurent une résistance à la poussière et à l'humidité/l'eau. Les dispositifs extérieurs Axis sont généralement classés IP66 et NEMA 4X. IP66 assure une protection contre la poussière, la pluie et les jets d'eau puissants. NEMA 4X assure une protection non seulement contre la poussière, la pluie et l'eau dirigée par un tuyau, mais aussi contre la neige, la corrosion et les dommages causés par l'accumulation de glace à l'extérieur. Certaines caméras Axis conçues pour les environnements extrêmes sont également conformes à la norme MIL-STD-810G de l'armée américaine pour les hautes températures, les chocs thermiques, les radiations, le brouillard salin et le sable. Pour les produits résistant au vandalisme, IK08 et IK10 sont les indices les plus courants pour la résistance aux chocs.

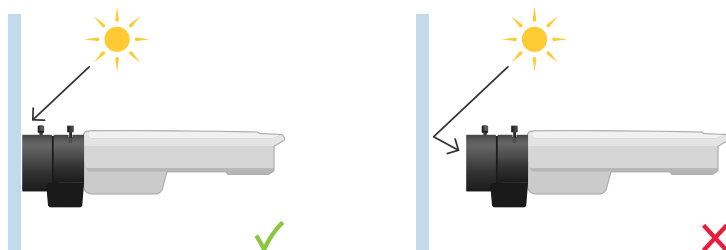
Des boîtiers en acier inoxydable sont nécessaires lorsque les caméras sont exposées à des acides, comme dans l'industrie alimentaire. Des boîtiers spéciaux peuvent également être requis à des fins esthétiques. Certains boîtiers spécialisés peuvent être pressurisés, submersibles ou blindés. Lorsqu'une caméra doit être installée dans un environnement potentiellement explosif, d'autres normes entrent en jeu. Citons par exemple IECEx, une certification mondiale, et ATEX, une certification européenne.

18.3.2 Boîtiers externes

Des boîtiers externes doivent être utilisés lorsque les exigences environnementales dépassent les conditions de fonctionnement d'un produit de vidéo sur IP. La taille, la qualité et les caractéristiques des boîtiers varient. Les boîtiers peuvent intégrer des appareils de chauffage et des ventilateurs (soufflants) pour s'adapter aux changements de température. Certains sont dotés de périphériques tels que des antennes pour des applications sans fil, même si l'utilisation d'une antenne externe n'est requise qu'avec un boîtier métallique.

Dans les installations extérieures, des boîtiers spéciaux peuvent également être nécessaires pour les encodeurs vidéo et accessoires tels que les modules audio E/S et les décodeurs vidéo. Les équipements critiques tels que les alimentations électriques, les centrales et les commutateurs peuvent également nécessiter une protection contre les intempéries et le vandalisme.

18.3.2.1 Mise en boîtier d'une caméra fixe



Lors de l'installation d'une caméra derrière une vitre, il est important de la positionner correctement pour éviter les reflets.

Lors de l'installation d'une caméra fixe dans un boîtier, il est important que l'objectif de la caméra soit positionné contre la fenêtre pour éviter que tout reflet apparaisse sur l'image. Des revêtements spéciaux peuvent également être appliqués sur une vitre placée devant l'objectif pour limiter les reflets. Les caméras fixes d'extérieur Axis sont fournies dans des boîtiers de protection pour utilisation en extérieur, ce qui permet d'économiser du temps d'installation et d'éviter les erreurs.

18.3.3 Dômes transparents

La « fenêtre » ou le dôme transparent d'un boîtier est généralement en acrylique (PMMA) ou en plastique polycarbonate. Comme les fenêtres agissent comme des objectifs optiques, elles doivent être de haute qualité pour ne pas amoindrir la qualité de l'image. Toute imperfection inhérente au matériel est susceptible de compromettre la clarté.

Les dômes des boîtiers des caméras PTZ sont soumis à des exigences plus élevées. Non seulement ils doivent avoir la forme d'une bulle, mais ils doivent aussi offrir une clarté exceptionnelle, puisque les imperfections telles que les particules peuvent être agrandies, en particulier pour les caméras haute résolution et les facteurs de zoom. De plus, si l'épaisseur du dôme est non homogène, une ligne droite peut apparaître incurvée à l'image. Un couvercle de dôme haute qualité devrait avoir très peu d'impact sur la qualité de l'image, quel que soit le niveau de zoom de la caméra et la position de l'objectif.

L'épaisseur d'un dôme peut être augmentée pour résister aux coups puissants, mais plus un dôme est épais, plus le risque d'imperfections est élevé. L'augmentation de l'épaisseur peut également créer des réflexissements et une réfraction de la lumière indésirables. Par conséquent, les dômes plus épais doivent répondre à des exigences plus élevées pour minimiser leur effet sur la qualité de l'image.

Une variété de dômes sont disponibles, y compris en version transparente et fumée. Alors que les versions fumées permettent une installation plus discrète, elles agissent également comme des lunettes de soleil ; elles réduisent la quantité de lumière disponible pour la caméra. Elles vont donc avoir un impact sur la sensibilité à la lumière de la caméra.



Dômes transparents, fumés et partiellement fumés pour caméras PTZ et dômes.

18.3.4 Protection contre le vandalisme et le sabotage

Avec certaines applications de surveillance, les caméras risquent d'être vandalisées. La résistance aux chocs peut être indiquée par l'indice IK d'une caméra ou d'un boîtier. L'indice IK spécifie le degré de protection que les boîtiers d'équipement électrique offrent contre les chocs mécaniques externes. Par exemple, un indice IK10 signifie que le produit peut résister à 20 joules d'impact, ce qui équivaut à un objet de 5 kg tombant d'une hauteur de 40 cm. Les objectifs de la protection contre le vandalisme, indépendamment de la mise en œuvre technique réelle, sont les suivants :

- > **Réduire les possibilités de falsification.** Le sabotage d'une caméra de surveillance vidéo doit être difficile. Plus important encore, leur conception et leur emplacement doivent aussi donner l'apparence d'être des caméras difficiles à saboter.
- > **Créer de l'incertitude.** Si des vandales décident de saboter une caméra, ils ne doivent pas savoir s'ils ont réussi à la détruire ou à interrompre l'enregistrement.
- > **Prolonger et retarder.** Même s'il est impossible de protéger une caméra contre une attaque déterminée, il faut que le sabotage prenne du temps. Chaque seconde gagnée augmente les chances de découverte de l'infraction ou d'abandon par le vandale.
- > **Détection et envoi d'alarmes.** Une caméra dotée d'une analyse intégrée peut détecter tout sabotage et en avertir les opérateurs.

Alors qu'une caméra ou un boîtier ne peut jamais garantir une protection à 100 % contre un sabotage, le vandalisme peut être atténué en prenant en compte divers aspects :

Conception de caméra / boîtier. Un boîtier ou une caméra fixe traditionnelle qui dépasse d'un mur ou plafond est plus vulnérable aux attaques (par exemple, des coups) que ceux plus discrètement conçus pour un dôme ou une caméra PTZ. Le couvercle lisse et arrondi d'une caméra dôme ou PTZ monté au plafond empêche davantage de bloquer la vue de la caméra, par exemple en accrochant un vêtement sur la caméra. Plus un boîtier ou une caméra se fond dans un environnement (par exemple, en lui donnant l'apparence d'une lumière extérieure), plus la protection contre le vandalisme sera appropriée.

Supports. Une caméra qui utilise un support encastré, où seule la fenêtre de la caméra ou du boîtier est visible, est moins vulnérable aux attaques qu'une caméra complètement accessible de l'extérieur. Lorsque vous prévoyez de monter des caméras et de protéger le système contre les vandales, incluez toujours les passages de câble. Faites passer le câble directement à travers le mur ou le plafond derrière la caméra pour offrir le niveau de protection le plus élevé. Un conduit métallique est également une bonne alternative pour protéger les câbles contre les attaques.

Positionnement des caméras. Une caméra montée en hauteur sur un mur ou dans le plafond risque moins d'attirer les tentatives d'attaque incontrôlée. L'inconvénient peut être le champ de vision, qui peut dans une certaine mesure être compensé en choisissant un objectif adapté.

Commutateurs de sabotage. L'ajout de commutateurs de sabotage aux boîtiers et boîtiers de caméra améliore la protection. Au déclenchement de ces accessoires, une alarme ou des notifications peuvent être envoyées aux clients sélectionnés.

Analyses. Des algorithmes intelligents peuvent également détecter si une caméra est redirigée, obscurcie ou altérée, et envoyer des alarmes aux opérateurs dans les salles de contrôle centrales ou

au personnel sur le terrain. Il existe des algorithmes pour détecter : une vue modifiée (sabotage), des sons anormaux (audio), des coups portés à la caméra (chocs), l'ouverture ou l'altération du boîtier et si des câbles sont coupés (E/S supervisées). Plus précisément, AXIS Image Health Analytics vous informe si l'image est bloquée, brouillée, sous-exposée ou redirigée.

18.3.5 Types de supports

Puisque le besoin de surveillance ne se limite pas à un type d'espace spécifique, l'éventail des options de montage proposées doit être vaste. Axis fournit un outil en ligne de sélection d'accessoires qui peut aider les utilisateurs à identifier le boîtier et les accessoires de montage adéquats. Consultez le portail des outils Axis, www.axis.com/tools

Pour minimiser les vibrations, veillez toujours à ce que le support de la caméra soit stable. Étant donné que les caméras PTZ peuvent bouger à l'intérieur de leur boîtier, des interférences peuvent se produire si le support de la caméra n'est pas correctement fixé. En extérieur, un équipement de montage robuste est nécessaire pour éviter les vibrations causées par les vents forts. Si le support n'est pas assez solide ou manque de stabilité, la caméra risque de tomber et de mettre en péril les personnes ou les biens.

Supports de plafond. Les caméras peuvent être montées sur des plafonds en utilisant un des aménagements suivants :

- > Montage en surface : Monté directement sur la surface d'un plafond et donc complètement visible.
- > Montage encastré : Monté à l'intérieur du plafond avec seulement des parties d'une caméra et un boîtier (généralement le dôme) visibles. Ce support est également connu sous le nom de support encastré ou suspendu.
- > Support de kit de suspension : Permet à la caméra d'être accrochée au plafond.
- > Fixation pour rails d'éclairage : Possibilité de fixer la caméra sur un rail d'éclairage existant sans perçage supplémentaire.



Exemples de montage en surface et de montage encastré (en haut) ; kit de suspension et fixation flexible pour rails d'éclairage (bas).

Montages muraux. Les supports muraux sont souvent utilisés pour monter des caméras à l'intérieur ou à l'extérieur d'un bâtiment. Le boîtier est connecté à un bras, qui est monté sur le mur. Les supports avancés disposent d'un presse-étoupe interne pour protéger le câble. Une fixation murale normale, ainsi qu'un adaptateur d'angle supplémentaire, peuvent être utilisés pour installer un boîtier à l'angle d'un bâtiment.

Supports de poteaux. Les supports de poteaux permettent de fixer des caméras PTZ dans de grands espaces extérieurs tels que des parkings, des routes et des parcs. Ce type de support est généralement conçu pour absorber et minimiser les effets des vibrations causées par le vent et le sol, afin de limiter leur impact sur la caméra. Lorsque vous calculez le balancement, tenez compte de la hauteur et du diamètre du poteau, ainsi que du matériau. Les poteaux en béton se balancent moins que les poteaux en métal et en bois. Facteur de poids et dimensions de l'équipement que le poteau doit supporter. Cette considération est particulièrement importante pour les caméras PTZ et les caméras à zoom optique élevé ; si le poteau est sous-dimensionné, le risque de flou de mouvement dans les images sera plus élevé. Les caméras PTZ plus avancées sont dotées d'une fonction de stabilisation d'image électronique intégrée pour limiter les effets du vent et des vibrations. Cependant, les caméras lourdes peuvent causer des blessures graves si elles tombent.

Comme avec les supports muraux, le câble peut généralement être passé à l'intérieur du poteau, et les sorties de câbles et prises doivent être scellées correctement.



Exemples de fixation murale et de fixation sur poteau.

Supports de parapet. Les supports de parapet sont utilisés pour monter des caméras sur les toits ou pour élever la caméra afin d'offrir un meilleur angle de vue. Les supports de parapet permettent d'avoir une caméra qui revient moins cher et est plus facile à entretenir que dans le cadre d'une suspension à une fixation murale. Comme le bras peut pivoter vers l'intérieur, le personnel de maintenance peut accéder à la caméra depuis le toit plutôt que d'utiliser une plate-forme pour y accéder.

Supports très discrets. Les supports très discrets sont généralement utilisés pour monter de minuscules caméras modulaires dans des espaces nécessitant une discrétion totale. Ces supports peuvent être complètement discrets, à peine visibles (montage en sténopé), partiellement visibles (montage encastré) ou entièrement visibles (montage en surface).



Exemples de support de parapet et de montage extrêmement discret (caméra modulaire cachée dans une bande en hauteur).

18.4 Éléments à considérer pour la bande passante et le stockage

La bande passante réseau et les exigences de stockage sont des considérations importantes lors de la conception d'un système de vidéosurveillance. Avec AXIS Site Designer, vous pouvez estimer efficacement les besoins de votre système. Les besoins en bande passante et en stockage dépendent des facteurs suivants :

- > Nombre de caméras
- > Enregistrement continu ou déclenché par un événement
- > Enregistrement en périphérie sur caméra / encodeur vidéo, enregistrement sur serveur ou une combinaison des deux
- > Nombre d'heures d'enregistrement par jour
- > Images par seconde
- > Résolution de l'image
- > Type de compression vidéo : H.264, H.265, AV1 et si Zipstream est utilisé.
- > Complexité de la scène : complexité de l'image, conditions d'éclairage et quantité de mouvements
- > Les données de durée doivent être stockées.

18.4.1 Bits ou octets ?

Il y a souvent confusion quant à la signification des divers termes suivants : bits, octets, Mbit/s, gigaoctets, etc. Lesquels correspondent à la capacité ? Lesquels évoquent la vitesse ?

Tailles de données

La plus petite unité d'informations numériques est un chiffre binaire, plus communément appelé bit (b) ; les deux valeurs possibles sont souvent représentées par 1 ou 0, et parfois par on/off, vrai/faux, oui/non, +/-.

Dans la mesure où les bits sont de très petits incréments de données, on utilise des multiples pour désigner des valeurs plus importantes :

- > 1 000 bits = 1 kilobit (kbit)
- > 1 million de bits = 1 mégabit (Mbit)

Les bits peuvent également être représentés par groupes, en utilisant l'octet. 1 octet (B) = 8 bits (b), ces huit bits étant le minimum requis pour représenter un seul caractère de texte.

Les préfixes des bits s'appliquent également aux octets :

> 1 million d'octets = 1 mégaoctet (Mo)

> 1 milliard d'octets = 1 gigaoctet (Go)

Il est bon à savoir que les ordinateurs sont des systèmes binaires et non décimaux – autrement dit, ils fonctionnent avec la base deux et non avec la base dix. Cela signifie que les totaux exacts des deux systèmes sont différents, même si les divers préfixes (kilo, méga, giga, etc.) sont souvent utilisés à la fois pour les valeurs décimales et binaires.

Par exemple, pour multiplier 1 octet par 1 000 :

> Dans la base 10 (décimale), ce serait $10^3 = 1\,000$

> Dans la base 2 (binaire), l'équivalent le plus proche est $2^{10} = 1\,024$

Bien que légèrement différentes, ces deux valeurs sont généralement indiquées par « 1 kilo-octet », car la plupart des gens trouvent qu'il est beaucoup plus facile de compter en décimal qu'en binaire. Généralement, la capacité des disques durs est exprimée en valeurs décimales ; par exemple, 1 Go est défini comme un milliard d'octets exactement.

Cependant, comme l'ordinateur utilisant le lecteur est un système binaire, un disque de 10 Go sera considéré par l'ordinateur comme n'ayant que 9,31 Go (comme dans un système binaire, $10\text{ Go} = 10\,737\,418\,240$ octets).

Comme 1 octet est constitué de 8 bits, il s'ensuit également que :

> 1 Mo = 0,125 Mo

> 8 Mo = 1 Mo

Pour obtenir d'autres comparaisons de tailles de données, consultez le tableau suivant.

Unité	Taille (binaire)	Taille (décimale)
Kilooctet (Ko)	1 024 octets	1 000 octets
Mégaoctet (Mo)	1 024 kilooctets	1 000 000 octets
Gigaoctet (Go)	1 024 mégaoctets	1 000 000 000 octets
Téraoctet (To)	1 024 gigaoctets	1 000 000 000 000 octets

Pétaoctet (Po)	1 024 téraoctets	1 000 000 000 000 000 octets
Exaoctet (Eo)	1 024 pétaoctets	1 000 000 000 000 000 000 000 octets

tableau 18.4a Comparaisons de tailles de données.

Débits de transfert des données

Les connexions réseau ou Internet sont exprimées en mégabits par seconde (Mbit/s). Bien qu'il s'agisse techniquement d'une mesure de la capacité (nombre de bits déplacés par seconde), les valeurs en Mbit/s sont généralement considérées comme des vitesses, c'est-à-dire qu'une connexion à haut débit est souvent perçue comme étant rapide.

Pour la vidéo sur IP, reprenez que les données sont envoyées sur un réseau « bit par bit » et non en octets. Cela signifie que les Mbit/s peuvent être utiles pour désigner une connexion permettant d'afficher un flux vidéo en direct (c'est-à-dire pas dans le cadre du téléchargement ni de la sauvegarde de la vidéo). Une connexion rapide offre une expérience de visualisation plus fluide (en réduisant la latence) et améliore la diffusion des vidéos haute résolution. Si, au contraire, vous souhaitez simplement télécharger et enregistrer une vidéo, la vitesse de connexion est un critère moins important. Avec une connexion plus lente, le téléchargement d'une vidéo peut durer un peu plus longtemps qu'avec une connexion rapide, mais cela a-t-il vraiment de l'importance ?

Autre critère pertinent : les bits transférés sur un réseau n'arrivent pas toujours dans l'ordre correct et ne proviennent pas nécessairement de la même source. L'application recevant les bits les assemble dans le bon ordre, ce n'est pas un problème, mais cela met en évidence les raisons pour lesquelles les vitesses réseau sont généralement exprimées en Mbit/s plutôt qu'en octets.

Même si les Mbit/s sont le moyen le plus courant de mesurer les vitesses de données, des Mo/s peuvent également être utilisés pour exprimer le temps d'enregistrement d'une vidéo sur disque, par exemple. Ainsi le téléchargement/transfert d'un fichier vidéo de 100 Mo via une connexion de 100 Mbit/s prend 8 secondes, car la vitesse d'écriture convertie en Mo/s est de 12,5 Mo/s (c'est-à-dire que 100 mégaoctets = 800 mégabits).

18.4.2 Exigences en matière de passante

Dans un petit système de surveillance comptant moins de 10 caméras, un commutateur de base de 100 mégabits (Mbits) peut être utilisé sans avoir à tenir compte des limitations de bande passante. La plupart des entreprises peuvent mettre en place un système de surveillance de cette taille en utilisant leur réseau existant. Lors de la mise en œuvre de 10 caméras ou plus, la charge du réseau peut être estimée en suivant quelques règles de base :

- > Une caméra configurée pour fournir des images de haute qualité à des fréquences d'images élevées utilisera environ 2 à 8 Mbit/s de bande passante réseau disponible.
- > Avec plus de 12 à 15 caméras, pensez à utiliser un commutateur avec un backbone gigabit. Si un commutateur gigabit est utilisé, le serveur qui exécute le logiciel de gestion vidéo doit avoir une carte réseau gigabit installée.

Les technologies souffrant une gestion de la consommation de bande passante comprennent l'utilisation d'un VLAN sur un réseau commuté, la Qualité de Service et les enregistrements déclenchés par des événements.

18.4.3 Exigences en matière de stockage

L'un des facteurs influant sur les besoins en stockage est le type de compression vidéo utilisé. H.264 est la norme de compression vidéo dominante dans la vidéosurveillance aujourd'hui, même si les formats AV1 et H.265 sont beaucoup plus efficaces.

Les nouveaux systèmes prennent en charge la norme AV1, qui réduit les besoins en stockage de 50 % par rapport à la norme H.264. La norme H.264 sera prise en charge parallèlement à la norme AV1 pendant de nombreuses années.

H.265 ne répond pas encore entièrement aux exigences des vidéos de type surveillance.

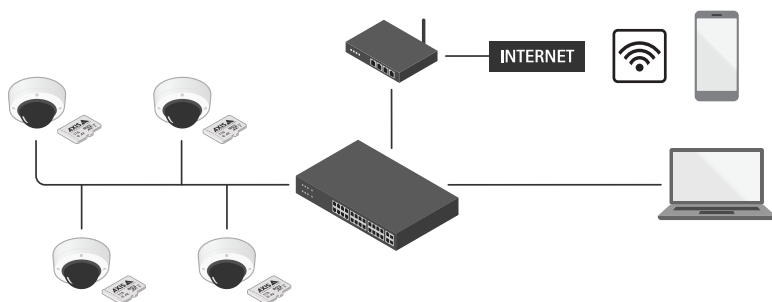
L'activation de Zipstream est recommandée, car elle peut réduire considérablement la taille du stockage système sans compromettre la valeur légale de la vidéo.

AXIS Site Designer constitue le meilleur moyen d'estimer les besoins en matière de stockage sans effectuer de mesures sur site. Cet outil vous aide à choisir les caméras et accessoires adaptés à votre scénario et à votre objectif de surveillance, et à estimer automatiquement les besoins en matière de stockage et de bande passante. Il est important de configurer chaque caméra dans l'outil avec le type de scène, la résolution, la fréquence d'image, la sélection de la qualité et les paramètres d'enregistrement.

18.4.4 Configurations du système

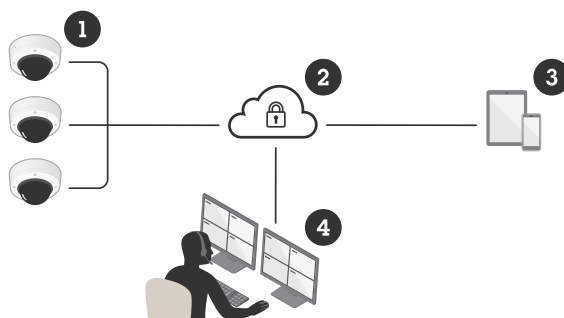
Solution Edge. Une caméra peut être équipée d'une carte SD pour stocker les vidéos et les métadonnées. Axis propose des cartes SD haut de gamme spécialement conçues pour la surveillance. Le stockage edge ou dans le cloud permet de se passer d'un enregistreur vidéo sur réseau ou d'un serveur vidéo. Même l'analyse qui traite la vidéo et/ou les métadonnées peut être exécutée directement dans la caméra. Les systèmes peuvent tirer parti d'une combinaison de composants edge, dans le cloud et sur site dans une configuration hybride. Les composants basés

sur le cloud peuvent offrir une visualisation à distance, le stockage dans le cloud, la surveillance à distance du système et la gestion à distance.



Une solution utilisant un stockage edge et un VMS pour la gestion vidéo.

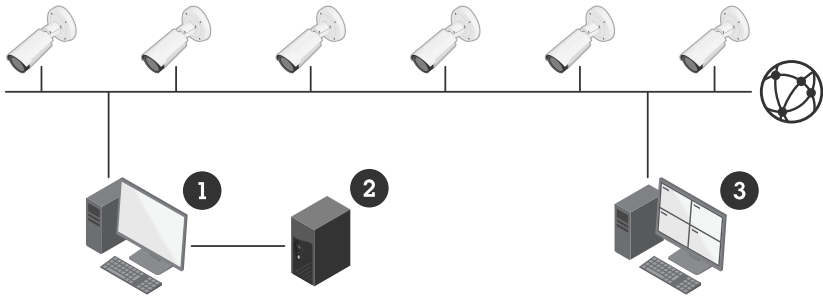
Solution cloud. Dans une configuration vidéo cloud, la plupart des composants du système sont gérés par un fournisseur de services, qui à son tour fournit aux utilisateurs un accès à la vidéo en direct et enregistrée sur internet. Axis Cloud Connect est une plateforme ouverte cloud hybride qui, associée aux périphériques Axis, active les services gérés.



Dans une solution cloud, la vidéo (1) est stockée et gérée dans le cloud (2). Les utilisateurs autorisés peuvent accéder aux vidéos en direct et enregistrées via des périphériques mobiles (3) ou n'importe quel navigateur (4).

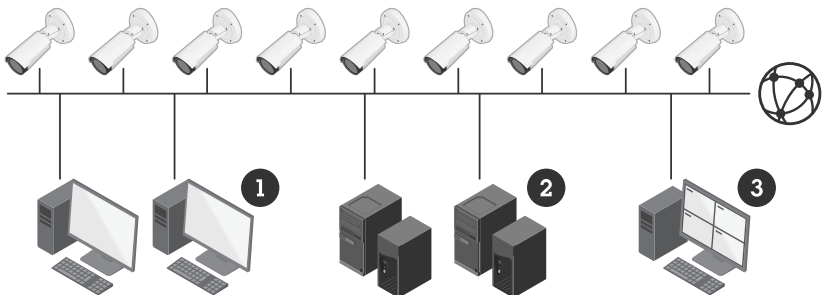
Solution sur site. Dans une installation sur site typique, un serveur est utilisé pour gérer le stockage, la gestion et la maintenance du système, tandis que la visualisation et le fonctionnement des notifications vidéo et d'événement sont gérés à partir d'un client. Généralement, le stockage est

configuré en RAID pour augmenter les performances et la fiabilité. L'analyse peut être edge-based, mais également basée sur un serveur.



Solution sur site avec un serveur (1), stockage RAID (2) en option et client poste de travail.

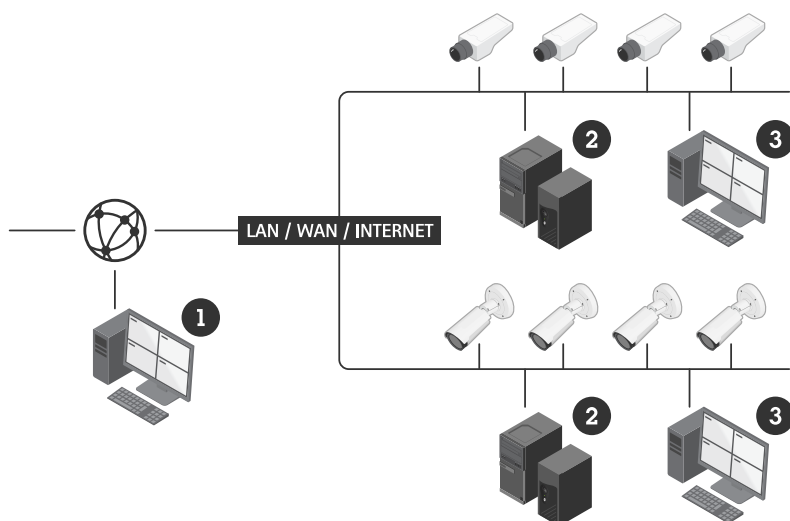
Grand système centralisé. Une installation de grande taille nécessite des performances et une fiabilité élevées pour gérer les importantes quantités de données et la large bande passante. Cela nécessite plusieurs serveurs avec des tâches dédiées. Un serveur principal contrôle le système et décide quel type de vidéo est stocké sur quel serveur de stockage. Comme il existe des serveurs de stockage dédiés, il est également possible de procéder à l'équilibrage de la charge. La configuration permet de faire évoluer le système en ajoutant plus de serveurs de stockage en cas de besoin et d'effectuer la maintenance sans arrêter tout le système.



Un grand système centralisé avec des serveurs principaux (1), des serveurs de stockage (2) et un poste de travail de surveillance (3).

Grand système distribué. Des systèmes d'enregistrement distribués peuvent être utilisés lorsque plusieurs sites nécessitent une surveillance centralisée. Chaque site enregistre et stocke la vidéo à

partir de caméras locales. Le contrôleur principal peut afficher et gérer les enregistrements sur chaque site.



Un grand système distribué avec stations de travail de surveillance (1, 3) et serveurs de stockage avec RAID (2).

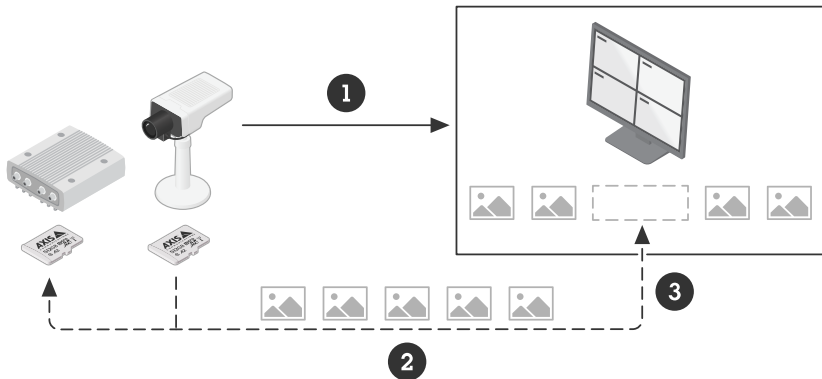
18.4.5 Stockage local

Le stockage edge, parfois appelé stockage local ou enregistrement embarqué, permet aux caméras et aux encodeurs vidéo de créer, contrôler et gérer des enregistrements localement sur une carte mémoire SD (Secure Digital), un stockage connecté au réseau (NAS) ou un serveur de fichiers. Le stockage edge peut être utilisé en tant que stockage principal dans une solution de cloud hybride.

Le stockage edge facilite la conception de solutions d'enregistrement flexibles et fiables. En termes d'avantages, il offre une fiabilité accrue du système, une vidéo haute qualité dans les installations à faible bande passante, un enregistrement pour la surveillance à distance et mobile et l'intégration avec un logiciel de gestion vidéo. L'utilisation de cartes SD comme seul type de support d'enregistrement en fait une solution très rentable.

Le stockage périphérique peut fonctionner en complément du stockage central. Il peut enregistrer des vidéos localement lorsque le système central n'est pas disponible, ou enregistrer en continu en parallèle. Lorsqu'ils sont utilisés avec un logiciel de gestion vidéo tel qu'AXIS Camera Station, les enregistrements de secours peuvent être stockés. Ainsi, les clips vidéo manquants à cause des interruptions du réseau ou de la maintenance du système central peuvent être récupérés à partir de

la caméra et fusionnés avec le stockage central, garantissant des enregistrements vidéo ininterrompus.



Stockage périphérique pour la redondance (enregistrement avec basculement).

- 1 En exploitation normale, la caméra transmet la vidéo au logiciel VMS pour stockage.
- 2 En cas de coupure réseau, les séquences vidéo sont stockées provisoirement sur la carte mémoire SD de la caméra.
- 3 Une fois la connexion réseau rétablie, le logiciel VMS récupère les séquences vidéo manquantes et les fusionne avec l'enregistrement.

De plus, le stockage périphérique peut améliorer l'analyse vidéo pour les systèmes à faible bande passante avec une résolution vidéo amoindrie. En utilisant la surveillance à faible bande passante avec des enregistrements locaux de haute qualité, les utilisateurs peuvent à la fois optimiser les limitations de bande passante et récupérer des vidéos de haute qualité des incidents pour une analyse détaillée.

Le stockage périphérique peut également être utilisé pour gérer les enregistrements de sites distants et d'autres installations où la disponibilité du réseau est intermittente ou inexistante. Sur les trains et autres véhicules à chenilles, le stockage périphérique peut être utilisé pour enregistrer d'abord la vidéo à bord, puis la transférer au système central lorsque le véhicule s'arrête à un dépôt.

Axis propose des cartes de catégorie surveillance, c'est-à-dire des cartes SD spécialement développées pour des performances optimales en vidéosurveillance. Il s'agit de cartes de qualité industrielle qui résistent ainsi aux impacts des températures et des environnements extrêmes. Elles bénéficient également d'une endurance accrue, ce qui correspond au comportement d'enregistrement standard d'une caméra de surveillance. Cela signifie qu'il est possible d'écrire

dessus et de remplacer des données beaucoup plus souvent que sur une carte SD ordinaire. Ainsi, la même carte est utilisable plus longtemps sans phénomène d'usure.

Les cartes de surveillance permettent d'enregistrer la vidéo d'une manière qui optimise l'exploitation de chaque bloc mémoire. Ceci permet non seulement d'économiser de la mémoire, mais également de réduire le nombre de cycles d'écriture/d'effacement, ce qui a pour effet d'augmenter la durée de vie de la carte.

Stockage edge avec cartes SD ou NAS. Les avantages et les inconvénients de l'utilisation de cartes SD ou de NAS pour le stockage edge doivent être pris en compte :

- > Les cartes SD sont plus faciles à déployer et à configurer que les NAS.
- > Les cartes SD peuvent être sabotées si elles sont physiquement accessibles. Les NAS peuvent être placés dans un endroit sûr.
- > Les cartes SD résistent à un point de panne unique. Si le NAS ou sa connexion est interrompu, plusieurs caméras seront touchées.
- > L'unité de stockage réseaux peut avoir une configuration RAID.
- > Le remplacement des cartes SD peut être coûteux si la caméra est montée dans des endroits difficiles d'accès, comme un poteau ou un mur de plus de 4,5 m (15 pi.).

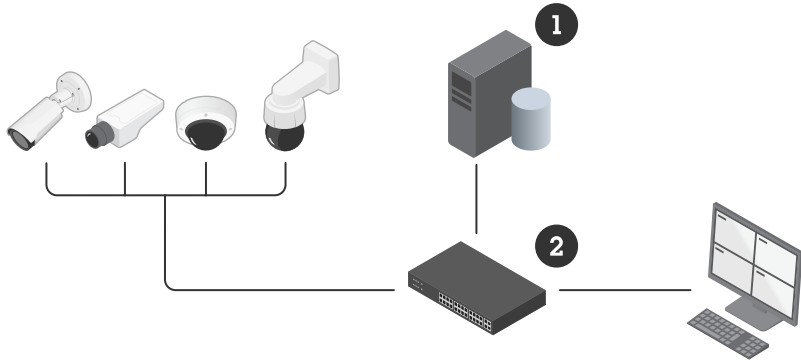
18.4.6 Stockage sur serveur

Le stockage sur serveur implique un serveur connecté localement aux périphériques vidéo sur IP pour la gestion et l'enregistrement vidéo. Le serveur exécute un logiciel de gestion vidéo qui enregistre la vidéo sur le disque dur local (stockage direct) ou sur un NAS. En fonction de l'unité centrale de traitement (CPU), de la carte réseau et de la mémoire vive interne (RAM) du serveur, celui-ci sera en mesure de gérer un certain nombre de cartes, d'images par seconde et de tailles d'image. La plupart des serveurs peuvent contenir plusieurs disques durs.

18.4.7 NAS et SAN

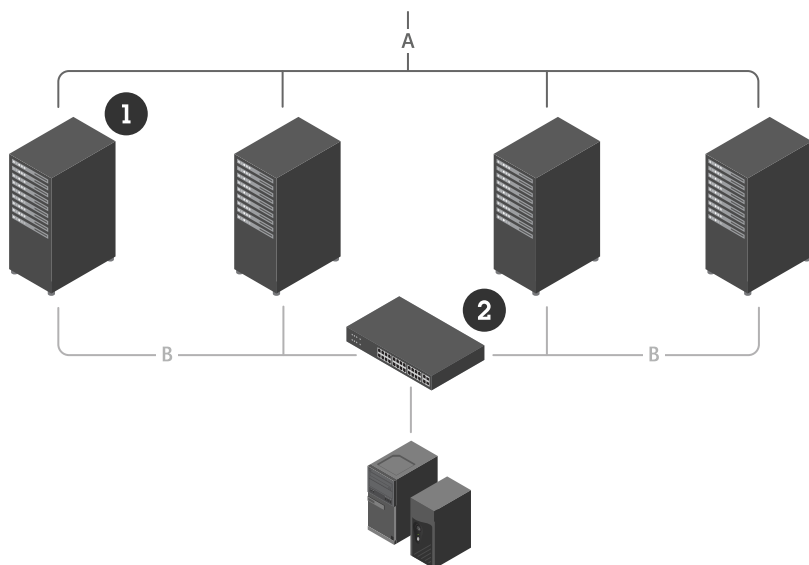
Lorsque la quantité de données stockées et les exigences de gestion dépassent les limites du stockage à connexion directe, le stockage connecté au réseau (NAS) ou le réseau de stockage (SAN) permet d'augmenter l'espace de stockage, la flexibilité et la capacité de restauration.

Le NAS fournit un périphérique de stockage unique directement relié à un réseau local et offre un stockage partagé aux clients du réseau. Le périphérique NAS est simple à installer et à administrer, offrant une solution de stockage à faible coût.



Le stockage connecté au réseau (1) est connecté à un système vidéo sur IP via le commutateur réseau (2), un routeur haut débit ou un pare-feu d'entreprise.

Un réseau SAN est un réseau spécial à grande vitesse pour les dispositifs de stockage. Il est connecté à un ou plusieurs serveurs via un canal fibre. Les utilisateurs peuvent accéder à tous les périphériques de stockage sur le réseau de stockage via les serveurs et la capacité de stockage peut être étendue à des centaines de téraoctets. Le stockage centralisé réduit l'administration et fournit un système de stockage flexible hautes performances pour une utilisation dans des environnements multiserveurs. La technologie Fibre Channel est couramment utilisée pour fournir un transfert de données allant jusqu'à 16 Gbit/s et permettre de stocker de grands volumes de données avec un haut niveau de redondance.



Une architecture SAN où les périphériques de stockage sont liés et partagent la capacité de stockage. Les utilisateurs peuvent accéder à l'un des dispositifs de stockage via les serveurs (1) et un commutateur de canal fibre (2).

A. LAN TCP/IP

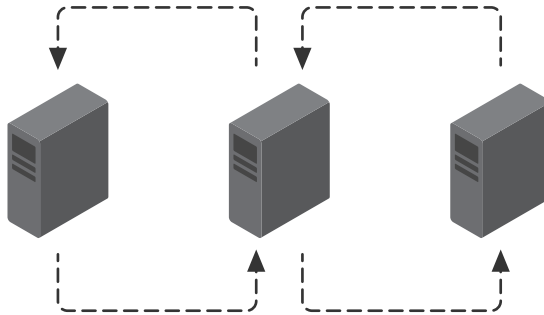
B. Canal à fibres optiques

18.4.8 Stockage redondant

La redondance d'un système de stockage permet d'enregistrer simultanément la vidéo ou d'autres données dans plusieurs emplacements. Cela fournit une sauvegarde pour la récupération de la vidéo si une partie du système de stockage devient illisible. Cette couche de stockage supplémentaire peut être fournie de différentes manières dans un système de surveillance sur IP, y compris via une matrice redondante de disques indépendants (RAID), la réplication de données, le regroupement de serveurs, plusieurs destinataires vidéo, le stockage redondant dans le cloud et les cartes SD.

RAID : le RAID est une méthode d'organisation des disques durs standard, qui permet au système d'exploitation de les considérer comme un grand disque dur unique. La configuration RAID répartit les données sur plusieurs disques durs avec suffisamment de redondance pour que les données puissent être récupérées en cas de défaillance de disque. Il existe différents niveaux de RAID, allant de la quasi-absence de redondance à une solution entièrement en miroir dans laquelle il n'y a aucune perturbation ni perte de données en cas de défaillance de disque dur.

Réplication de données. Cette caractéristique est commune à de nombreux systèmes d'exploitation réseau. Les serveurs de fichiers réseau sont configurés pour répliquer les données entre eux, fournissant une sauvegarde en cas de panne de serveur.



Réplication de données.

Regroupement de serveurs. La méthode de regroupement de serveurs la plus courante consiste à faire fonctionner deux serveurs avec le même périphérique de stockage, tel qu'un système RAID. Lorsqu'un serveur tombe en panne, l'autre serveur configuré de manière identique prend le relais. Ces serveurs peuvent partager la même adresse IP, ce qui rend le basculement complètement transparent pour les utilisateurs.

Plusieurs destinataires vidéo. La méthode la plus courante pour assurer une récupération après sinistre et un stockage hors site consiste à envoyer simultanément la vidéo à deux serveurs différents de sites distincts. Ces serveurs peuvent être équipés de RAID, fonctionner en grappes ou répliquer leurs données avec des serveurs encore plus éloignés. Cette approche est particulièrement utile lorsque les systèmes de surveillance se trouvent dans des zones dangereuses ou difficiles d'accès, telles que les installations de transport en commun ou industrielles.

Carte SD. Le stockage edge utilisant des cartes SD peut fonctionner en complément du stockage central. Il peut enregistrer des vidéos localement lorsque le système central n'est pas disponible, ou enregistrer en continu en parallèle. Lorsqu'ils sont utilisés avec un VMS, les enregistrements de secours peuvent être gérés. Ainsi, les clips vidéo manquants à cause des interruptions du réseau ou de la maintenance du système central peuvent être récupérés à partir de la caméra et fusionnés avec le stockage central, garantissant des enregistrements vidéo ininterrompus.

Stockage dans le cloud. Le stockage dans le cloud consiste à stocker des données sur des systèmes distants, où elles sont gérées et disponibles pour les utilisateurs sur un réseau. Il peut être proposé

dans le cadre d'offres commerciales d'un fournisseur tiers, auquel cas les utilisateurs paient généralement un abonnement. Le stockage dans le cloud privé est géré par l'organisation utilisatrice (et lui appartient généralement), par exemple, lorsque les exigences de sécurité sont élevées. Les solutions hybrides sont utiles lorsqu'une entreprise doit compartimenter le stockage des différents types de données ou lorsqu'elle doit étendre sa capacité de stockage.

19. Outils et ressources

Axis offre de nombreux outils et ressources d'information pour aider à concevoir des systèmes de surveillance sur IP. Nous proposons des outils qui vous permettent de trouver et de comparer des produits, de planifier et de concevoir des sites, d'installer et de gérer des systèmes et d'ajouter des téléchargements et des modules complémentaires. De nombreux outils sont accessibles à partir de www.axis.com/tools. Ce chapitre énumère certains de nos outils les plus utilisés.

19.1 Recherche et comparaison de produits

Sélecteur de produit. Cet outil vous permet de sélectionner les caméras, haut-parleurs, interphones et autres périphériques réseau pour votre projet en fonction des fonctionnalités dont vous avez besoin.

Sélecteur d'accessoires. Cet outil permet de choisir le bon support, boîtier, fixation et accessoire d'alimentation pour les caméras de votre projet.

Calculateur d'objectif. Utilisez le calculateur d'objectif pour connaître les objectifs disponibles pour une caméra spécifique et établir facilement le placement optimal de la caméra et la distance focale requise pour une taille et une résolution de scène spécifiques.

Sélecteur de caméra pour AXIS People Counter. Cet outil vous aide à trouver des modèles de caméras pré-calibrés offrant la meilleure précision possible pour les analyses de comptage de personnes.

19.2 Planification et conception de sites

AXIS Site Designer. Utilisez AXIS Site Designer pour rationaliser la conception du système de surveillance grâce aux workflows d'installation. Que vous souhaitiez créer un système avec des milliers de périphériques Axis ou seulement quelques uns, AXIS Site Designer vous permet de concevoir, d'approuver et d'installer des systèmes de surveillance qui répondent à vos besoins

opérationnels exacts. Les sélecteurs de produits intuitifs facilitent l'identification des caméras et des périphériques idéaux pour chaque situation et choisissent les supports et les accessoires appropriés en fonction de leur emplacement. Le stockage et la bande passante système peuvent également être estimés efficacement. AXIS Site Designer peut être utilisé pour concevoir des systèmes de surveillance intégrant des produits Solution Complète Axis ainsi que des produits proposés par certains partenaires VMS tiers pour des systèmes plus gros.

Plug-in Axis pour Autodesk® Revit® : vous permet de sélectionner et de placer des produits Axis interactifs directement dans votre plan de construction Autodesk Revit et d'intégrer la surveillance dans votre conception. Ce plug-in intègre un sélecteur de produits et vous permet de vérifier le champ de vision et d'ajuster les paramètres pour l'adapter à la scène.

19.3 Installation et gestion des systèmes

AXIS Device Manager. Permet une gestion efficace de l'installation, de la sécurité et de la maintenance des périphériques majeurs. Les fonctions principales comprennent l'attribution d'adresses IP, la gestion des listes de périphériques, la gestion des utilisateurs et des mots de passe, la mise à niveau du logiciel des périphériques, le renouvellement et la gestion des certificats ainsi que le déploiement de contrôles de cybersécurité pour protéger vos dispositifs en réseau et les adapter à une infrastructure de sécurité.

AXIS Device Manager Edge. Offre un aperçu site par site, vous permettant de surveiller à distance le statut de la connectivité des périphériques et d'effectuer des tâches de gestion simples. Il donne un aperçu instantané du statut des périphériques du système tout en activant les mises à niveau automatiques et l'accès distant sécurisé. Cela facilite l'application et la maintenance des mesures de sécurité tout au long du cycle de vie d'un périphérique.

AXIS Device Manager Extend. Idéal pour les opérations multisite, AXIS Device Manager Extend propose une interface unifiée et intuitive vous permettant de gérer activement les périphériques et les sites Axis depuis n'importe quel lieu.

20. Axis Communications Academy

20.1 Développement d'une expertise pour une entreprise plus intelligente

Axis Communications sait que le succès de votre entreprise repose sur votre capacité à développer vos atouts en continu et à proposer le meilleur des solutions et des technologies à vos clients en restant à la pointe de l'innovation.

Axis Communications Academy a pour but de développer tous les aspects de votre entreprise, en fournissant des formations pour vous permettre d'offrir à vos clients toute l'expertise qu'ils attendent de vous, voire plus encore.

En vous tenant à jour des dernières informations sur les solutions Axis, les technologies, les tendances du secteur et les enjeux spécifiques à un secteur, vous pouvez offrir à vos clients des compétences expertes. Des ventes et du commerce et de la conception du système à l'installation et à la configuration.

Choisissez parmi une gamme de formats d'apprentissage - en personne ou en ligne - en fonction de votre style d'apprentissage, de vos préférences et de vos besoins.

- > Vidéos pédagogiques
- > Articles pédagogiques
- > Applications interactives
- > Formation en ligne
- > Formation virtuelle animée par un formateur
- > Formation en salle de cours avec formateur
- > Formation mixte (mélange de formats)
- > Webinaires

Programme de certification Axis

Bénéficiez d'un avantage concurrentiel en validant vos connaissances en vidéo sur IP avec des informations d'identification mondiales reconnues par le secteur.

Pour plus d'informations, visitez Axis Learning Center sur www.axis.com/academy

À propos d'Axis Communications

En améliorant la sûreté, la sécurité, l'efficacité opérationnelle et l'intelligence économique, Axis contribue à un monde plus sûr et plus intelligent. Leader de son secteur dans les technologies sur IP, Axis propose des solutions en vidéosurveillance, contrôle d'accès, visiophonie et systèmes audio. Ces solutions sont enrichies par des applications d'analyse intelligente et soutenues par des formations de haute qualité.

L'entreprise emploie environ 5000 personnes dans plus de 50 pays et collabore avec des partenaires technologiques et intégrateurs de systèmes du monde entier pour fournir des solutions sur mesure à ses clients. Axis a été fondée en 1984, son siège est situé à Lund en Suède.