Dossier technique de projet

Remplacement de la technique de sécurité vidéo à l'exemple d'une banque

Version 1.2.

milestone

AXIS COMMUNICATIONS

Table des matières

1. Définition de la mission

Dans une banque, la technique de sécurité vidéo existante doit être remplacée
> suite à l'expiration des contrats de location
> et de mesures de rénovation.

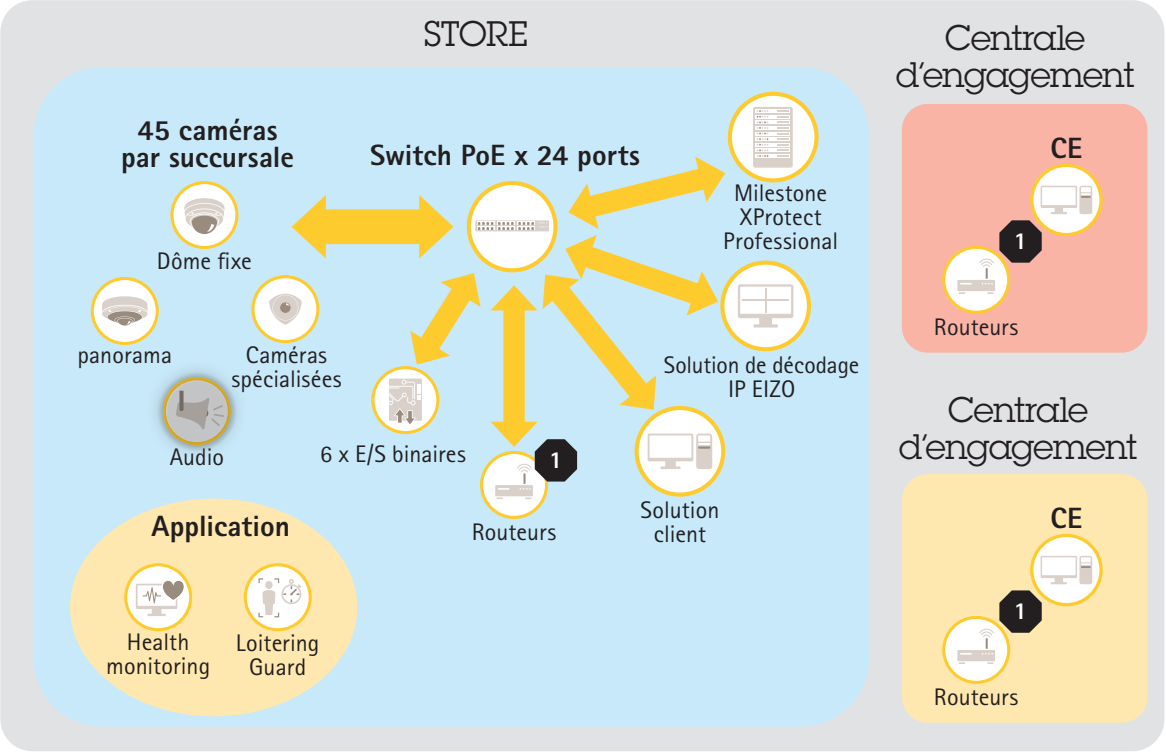
Le câblage réseau existant doit être réutilisé.

Objectifs du projet :
- Surveillance vidéo à la pointe de la technologie
- Gestion centralisée de la technologie vidéo

Cela permet une sécurisation axée sur les objectifs de protection. La nouvelle technique est planifiée de manière à ce qu'elle soit considérée comme sûre sur le plan opérationnel et qu'elle soit à l'abri des pannes conformément aux directives.

Le cahier des charges fonctionnel est basé sur les discussions et les documents du projet avec le/la responsable de la sécurité.

Ce document aborde par la suite les détails de la mise en œuvre technique.
Le but de ce document est de permettre aux fournisseurs d'installations de vidéoprotection d'élaborer une offre concrète qui tienne compte des coûts sur 5 ans pour la maintenance et l'exploitation de l'installation.



1 *Exigence minimale DSL 16000 au moins 2 Mbit/s up*

2. CSR - Corporate Social Responsibility / Code of Conduct

Extrait de globalcompact.de :
Le Pacte mondial des Nations Unies est la plus grande et la plus importante initiative mondiale en matière de gouvernance d'entreprise responsable. Sur la base de 10 principes universels et des objectifs de développement durable (Sustainable Development Goals), il poursuit la vision d'une économie mondiale inclusive et durable au bénéfice de tous les individus, communautés et marchés, aujourd'hui et demain. En y adhérant, plus de 13.000 entreprises et organisations de la société civile, du monde politique et scientifique de 161 pays montrent déjà leur volonté de concrétiser cette vision.

En tant qu'initiative des Nations unies, le Pacte mondial des Nations unies offre un cadre unique pour discuter, au-delà des secteurs et des frontières, d'une conception équitable de la mondialisation et pour concrétiser cette vision par des stratégies et des activités appropriées. Dans ce contexte, l'initiative ne se conçoit pas comme une norme certifiable ou un instrument de régulation, mais comme un forum ouvert permettant d'initier des processus de changement et de partager des idées. Au sein de réseaux nationaux, les participants développent des solutions concrètes et contribuent ainsi à la vision globale du Pacte mondial des Nations unies.

Les fournisseurs d'équipements techniques dans le domaine de la vidéosurveillance sont censés être également des membres actifs du Pacte mondial des Nations unies et publier des rapports de durabilité correspondants depuis au moins 5 ans.

3. Principes de planification

L'exigence posée à la nouvelle installation de sécurité vidéo est d'une part le respect des lois actuellement en vigueur et des normes applicables à la technique de sécurité vidéo et d'autre part une réalisation de la technique de sécurité vidéo conforme aux règles techniques généralement reconnues. Ci-dessous, une sélection des documents pris en compte (liste non exhaustive) :

> DIN EN 62676-1-1
> DIN EN 62676-1-2
> DIN EN 62676-4
> DIN EN 50518
> RGPD (Règlement général sur la protection des données)

Toute la planification est basée sur une documentation existante, des concertations, des photos, des informations écrites et des documents fournis par le client et sur les conclusions d'une visite des lieux effectuée.

4. Le RGPD et la protection des données à caractère personnel

Afin de pouvoir garantir la protection des données à caractère personnel, les bases suivantes doivent être mises à disposition ou élaborées en collaboration avec l'exploitant et l'utilisateur du système de vidéosurveillance :

1. Modèle de directives pour la vidéosurveillance
2. Instructions pour le durcissement du système (robustesse, hardening guide)
3. Guide sur le RGPD
4. Liste de contrôle pour assurer l'intégrité et la confidentialité
5. Formulaire de notification à court terme
6. Formulaire de demande de renseignements de la part des personnes concernées
7. Formulaire de notification de violation de la vie privée
8. Formulaire relatif à la responsabilité du responsable du traitement des données
9. Formulaire d'enregistrement des activités de traitement
10. VMS.
11. Formation sur la protection des données
12. Security by Design
13. Security by Default

Chaque fournisseur doit confirmer, pour chaque composant de réseau actif, c'est-à-dire chaque appareil doté d'un port réseau et, le cas échéant, d'une adresse IP, que la conception de cet appareil relève entièrement de la responsabilité du fabricant sous la marque duquel le produit est vendu sur le marché et qu'il ne s'agit pas de l'achat d'appareils commercialisés sous une autre marque que celle du fabricant d'origine.

Les appareils dits OEM (Original Equipment Manufacturer) ou ODM (Original Design Manufacturer) ne sont pas autorisés, car l'utilisateur ne veut prendre aucun risque en ce qui concerne le support à long terme de ces appareils.

Il en va de même pour le micrologiciel (firmware) des modèles de caméras proposés, qui doit également être de la responsabilité du fabricant sous la marque duquel les modèles sont proposés.

Afin de répondre aux diverses exigences en matière de protection de la vie privée, les caméras doivent offrir de nombreuses possibilités de masquage des zones.

1. Zones privées
   Au moins 30 zones différentes doivent pouvoir être masquées individuellement. Au choix, les masquages peuvent prendre la forme d'une pixellisation ou d'un masquage :

   a. Pixellisation (grossière) :

   b. Pixellisation (fine) :

   c. Masquage complet :

   d. Masquage par superposition :

Au moyen d'Overlays (graphiques superposés à l'image vidéo), il est également possible de masquer différentes zones de l'image.

5. Logiciel de gestion des équipements

Pour pouvoir exploiter le système en toute sécurité, il est indispensable d'utiliser un logiciel de gestion des équipements (GDA) efficace.
Les exigences suivantes doivent au moins être remplies :

a) Information sur les mises à jour de micrologiciel disponibles
Tous les équipements figurant dans la base de données du GVS sont contrôlés plusieurs fois par jour afin de vérifier la disponibilité de mises à jour du micrologiciel. Les mises à jour disponibles doivent être signalées en conséquence.
L'indication doit être facilement reconnaissable pour l'utilisateur.

b) Mise à jour individuelle et de groupe
Les équipements dans le GVS doivent pouvoir être regroupés logiquement, par ex. par secteur, étage, etc. Cela doit permettre de garantir que les mises à jour éventuellement nécessaires puissent être effectuées séparément par groupe.

Cela permet d'une part d'assurer la vidéosurveillance 24h/24 et 7j/7 et d'autre part de ne pas surcharger l'infrastructure réseau.
Les mises à jour doivent pouvoir être exécutées en parallèle ou de manière séquentielle.

c) Hardening Guide
Toutes les étapes recommandées dans le Hardening Guide du fabricant de l'appareil pour assurer le renforcement de la sécurité de l'appareil doivent être supportées par le GVS. Ici aussi, une méthode efficace doit être mise à disposition, par ex. l'utilisation de fichiers de configuration, etc., afin qu'un grand nombre d'appareils (voir mise à jour des groupes) puissent être configurés simultanément.

d) Mise à jour du logiciel et licences
Tous les coûts uniques ou autres occasionnés par les mises à jour, etc. doivent être justifiés en conséquence. Les coûts des mises à jour du logiciel pendant les 5 premières années doivent être inclus dans le prix de la solution GVS, dans les coûts d'acquisition.

Les coûts d'une licence d'équipements doivent être indiqués. S'il existe des bundles de licences, par ex. pour 50 appareils, il faut les indiquer en conséquence. S'il y a plus de deux bundles de licences, ceux-ci doivent être enregistrés dans un document séparé. Le donneur d'ordre se réserve le droit de recourir, le cas échéant, à la possibilité des bundles de licences, pour autant qu'ils soient économiquement raisonnables.

6. Structure

Pour rappeler les objectifs de protection selon la norme EN 62676-4, voici un aperçu :

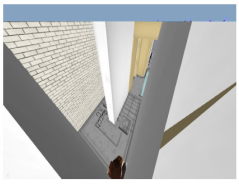
EN 62676- (juillet 2016)						
	Surveiller	Détecter	Observer	Reconnaître	Identifier	Évaluer
Largeur de scène (mm/px)	80	40	16	8	4	1
Pixel/mètre*	12.5	25	62.5	125	250	1 000

Pour la tâche Identifier, il faut faire attention à l'angle de vue de la caméra dans la scène.
Pour éviter les distorsions optiques, les angles horizontaux et verticaux entre la caméra et le panneau de test doivent être inférieurs à 22,5°. Le but devrait être de monter la caméra à hauteur du visage ou légèrement plus haut.

La première étape a consisté à développer une structure des scènes qui articule et catégorise les différentes zones de sécurité et les tâches. Les domaines suivants ont été constitués :

1. Zone de couloir / voie de circulation
   a. Clients

Onboard 1080p/3MP dome camera with WDR Dynamic Capture and AXIS Zipstream

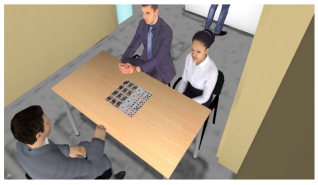


Résolution: 2016x1512
Diagonale du Capteur: 1/3 ; 4:3
Longueur de la Focale: 1.8
Hauteur de la Caméra: 3 m
Inclinaison: 41.2°
Angles de Vue °: 130°; 95°
Distance: 2.1 m
Largeur CDV: 6.1 m
Pixels sur la cible: 132 px/m
Zone aveugle: 0.07 m (Largeur: 0.19 m)

La tâche consiste à reconnaître des personnes

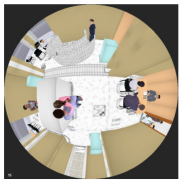
   b. Les employés et la réception des marchandises (courrier, colis)

Vandal resistant indoor 1080p/2MP dome camera with WDR Forensic Capture, AXIS Zipstream and Lightfinder



Résolution: 1920x1080
Diagonale du Capteur: 1/3 ; 16:9
Longueur de la Focale: 4.25
Hauteur de la Caméra: 2.5 m
Inclinaison: 45.3°
Angles de Vue °: 71.4°; 39.3°
Distance: 3.4 m
Largeur CDV: 5.1 m
Pixels sur la cible: 321 px/m

Indoor 1080p/12MP dome camera with WDR Forensic Capture and AXIS Zipstream



Résolution: 2880x2880
Diagonale du Capteur: 1/1.7 ; 1:1
Longueur de la Focale: 1.65
Hauteur de la Caméra: 2.5 m
Inclinaison: -12.3°
Angles de Vue °: 360°; 180°
Distance: 2.3 m
Largeur CDV: 5.3 m
Pixels sur la cible: 270 px/m
Zone aveugle: 0 m (Largeur: 0 m)

Le but est d'avoir une résolution >> 250 px/m dans le parcours, pour la documentation afin de pouvoir suivre les processus.

2. Entrée du personnel
Les personnes à l'entrée du personnel ou dans le sas doivent pouvoir être identifiées.

3. Couloir (employés avec ou sans clients)
Détecter les mouvements des personnes afin de pouvoir suivre les procédures.

Vandal resistant indoor 1080p/2MP dome camera with WDR Forensic Capture, AXIS Zipstream and Lightfinder

Résolution: 1080x1920
Diagonale du Capteur: 1/3 ; 9:16
Longueur de la Focale: 5.69
Hauteur de la Caméra: 3 m
Inclinaison: 26.5°
Angles de Vue °: 30.7°; 54.8°
Distance: 8.2 m
Largeur CDV: 4 m
Pixels sur la cible: 226 px/m
Zone aveugle: 2.19 m (Largeur: 1.07 m)

4. Entrée de la banque – Accès client

Vandal resistant indoor 1080p/2MP dome camera with WDR Forensic Capture, AXIS Zipstream and Lightfinder

Résolution: 1920x1080
Diagonale du Capteur: 1/3 ; 16:9
Longueur de la Focale: 6.8
Hauteur de la Caméra: 3 m
Inclinaison: 21.4°
Angles de Vue °: 48.8°; 27.7°
Distance: 7.5 m
Largeur CDV: 6.7 m
Pixels sur la cible: 262 px/m
Zone aveugle: 4.24 m (Largeur: 3.92 m)

Les clients doivent pouvoir être identifiés via cette zone de la caméra. Sous l'aspect actuel du port du masque, la sécurité demande à ce que le masque soit retiré dans la zone d'entrée afin de pouvoir identifier le client.

5. Réception des marchandises/table d'emballage

Streamlined 4K dome for any light

Résolution: 2160x3840
Diagonale du Capteur: 1/1.8 ; 9:16
Longueur de la Focale: 8.6
Hauteur de la Caméra: 2 m
Inclinaison: 18.2°
Angles de Vue °: 30°; 53°
Distance: 3 m
Largeur CDV: 1.5 m
Pixels sur la cible: 1160 px/m
Zone aveugle: 2.02 m (Largeur: 0.98 m)

La résolution dans la scène doit avoir la qualité d'image Évaluer dans la zone de déplacement des marchandises.
> Les bons de livraison doivent être lisibles lors de la recherche ou
> le produit doit pouvoir être clairement identifié.
Il en va de même pour l'emballage. A cet effet, des emplacements fixes doivent être définis dans la procédure d'exploitation pour
a. le positionnement du bon de livraison et du
b. poste de travail.

6. Bureau/administration

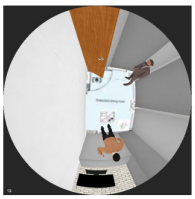
Vandal resistant indoor 1080p/2MP dome camera with WDR Forensic Capture, AXIS Zipstream and Lightfinder

Résolution: 1920x1080
Diagonale du Capteur: 1/3 ; 16:9
Longueur de la Focale: 4.62
Hauteur de la Caméra: 2.5 m
Inclinaison: 28.1°
Angles de Vue °: 66.9°; 37°
Distance: 2 m
Largeur CDV: 2.5 m
Pixels sur la cible: 494 px/m

Dans le domaine BoH (Back of House), il s'agit de reconnaître les processus commerciaux. Les livraisons (par ex. des entreprises de transport ou de la poste) sont saisies et enregistrées ici dans le système.

7. Coffre

Vandal resistant outdoor/indoor 1080p/12MP dome camera with WDR Forensic Capture, AXIS Zipstream and Lightfinder



Résolution: 2992x2992
Diagonale du Capteur: 1/1.7 ; 1:1
Longueur de la Focale: 1.3
Hauteur de la Caméra: 2.5 m
Inclinaison: -10.9°
Angles de Vue °: 360°; 180°
Distance: 2.6 m
Largeur CDV: 5.7 m
Pixels sur la cible: 264 px/m

Documentation complète des processus. Les marchandises et les employés doivent être très facilement identifiables. La résolution dans la scène doit avoir la qualité d'image Évaluer dans la zone de déplacement des marchandises.

8. Locaux techniques

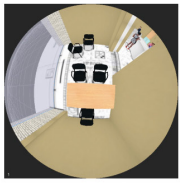
Vandal resistant indoor 1080p/2MP dome camera with WDR Forensic Capture, AXIS Zipstream and Lightfinder

Résolution: 1080x1920
Diagonale du Capteur: 1/3 ; 9:16
Longueur de la Focale: 6.17
Hauteur de la Caméra: 3 m
Inclinaison: 37°
Angles de Vue °: 28.9°; 51.3°
Distance: 5 m
Largeur CDV: 2.4 m
Pixels sur la cible: 361 px/m

L'objectif est que l'accès au local technique soit documenté au moyen du VSS (Video Surveillance System / système de surveillance vidéo) afin de pouvoir établir un profil de mouvement. La tâche de reconnaissance est requise.

9. Salles de consultation

Indoor 1080p/12MP dome camera with WDR Forensic Capture and AXIS Zipstream



Résolution: 2880x2880
Diagonale du Capteur: 1/1.7 ; 1:1
Longueur de la Focale: 1.65
Hauteur de la Caméra: 2.5 m
Inclinaison: -12°
Angles de Vue °: 360°; 180°
Distance: 2.3 m
Largeur CDV: 5.3 m
Pixels sur la cible: 270 px/m

Vandal resistant indoor 1080p/2MP dome camera with WDR Forensic Capture, AXIS Zipstream and Lightfinder

Résolution: 1920x1080
Diagonale du Capteur: 1/3 ; 16:9
Longueur de la Focale: 4.05
Hauteur de la Caméra: 3 m
Inclinaison: 42.2°
Angles de Vue °: 74.1°; 40.7°
Distance: 2.5 m
Largeur CDV: 3.8 m
Pixels sur la cible: 329 px/m
Zone aveugle: 1.56 m (Largeur: 2.76 m)

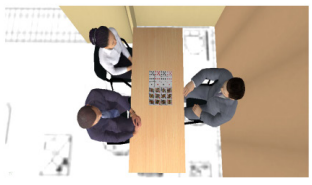
Vandal resistant indoor 1080p/2MP dome camera with WDR Forensic Capture, AXIS Zipstream and Lightfinder

Résolution: 1920x1080
Diagonale du Capteur: 1/3 ; 16:9
Longueur de la Focale: 4.45
Hauteur de la Caméra: 3 m
Inclinaison: 41.9°
Angles de Vue °: 68.9°; 38°
Distance: 3.7 m
Largeur CDV: 5.2 m
Pixels sur la cible: 294 px/m
Zone aveugle: 1.67 m (Largeur: 3.13 m)

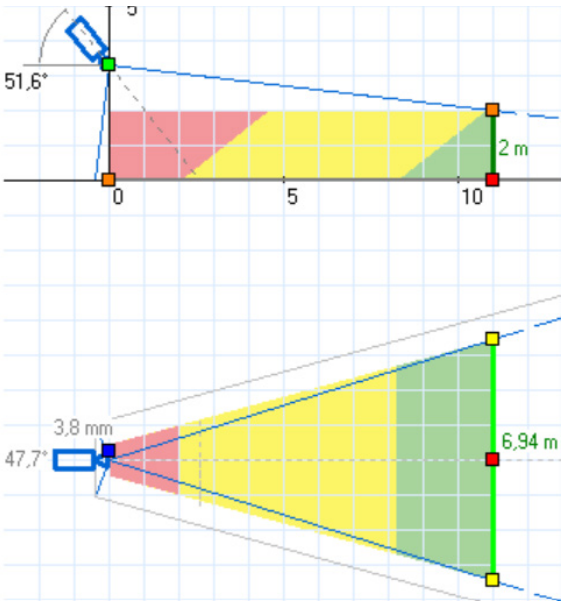
Tous les mouvements des clients doivent pouvoir être suivis depuis différentes perspectives, la caméra située à l'entrée peut être utilisée pour identifier les clients.

10. Guichet de banque/caisse

Complete, extremely discreet HDTV 1080p pinhole camera



Auflösung: 1920x1080
Sensorformat: 1/2.9 ; 16:9
Brennweite (mm): 3.7
Kamera Höhe: 3 m
Neigung: 78.8°
Blickwinkel [Grad]: 91°; 45°
Objekt Entfernung: 0.8 m
Objekt Breite: 2.8 m
Pixel/m am Objekt: 304 px/m
Totzone: -0.25 m (Breite: 2.38 m)



Les processus doivent être clairement identifiés, par ex. pour le comptage des billets de banque.

11. Vitrine/façade espace public

Streamlined outdoor-ready HDTV 1080p fixed dome for any light conditions

Résolution: 1080x1920
Diagonale du Capteur: 1/2.8 ; 9:16
Longueur de la Focale: 6.15
Hauteur de la Caméra: 4 m
Inclinaison: 30.3°
Angles de Vue °: 29.6°; 54.5°
Distance: 10.9 m
Largeur CDV: 5.1 m
Pixels sur la cible: 179 px/m
Zone aveugle: 2.54 m (Largeur: 1.31 m)

Les processus doivent être clairement identifiés. En cas de présence en dehors des heures de bureau de plus de 5 minutes, une notification automatique doit être envoyée aux centrales d'engagement (CE).

7. Exigences d'exploitation selon EN 62676-4

La norme EN 62676 a été utilisée comme base de planification déterminante. La norme EN 62676-4, la norme EN 62676-1-1 et la norme EN 62676-1-2 de cette série de normes ont été prises en compte pour cette planification.

> La norme DIN EN 62676-4 décrit les règles d'application qui correspondent aux règles généralement reconnues de la technique.
> La norme DIN EN 62676-1-1 décrit les exigences du système en général et
> la norme DIN EN 62676-1-1 décrit les exigences en matière de transmission vidéo.

La série de normes DIN EN 62676-1 regroupe les exigences issues de l'analyse des risques en 4 domaines, qui sont identifiés séparément par la suite en fonction des exigences.

Un élément important de la norme DIN EN 62676-4 est le développement et la documentation des exigences d'exploitation. Il s'agit d'une déclaration écrite formelle de la nécessité, de la justification et du but de l'installation de sécurité vidéo prévue ici.

En amont de la planification, les points suivants doivent être clarifiés et décrits plus en détail :

1. Objectifs/fonctionnalités de base
2. Définition des restrictions de surveillance
3. Détermination du ou des sites à surveiller
4. Détermination des activités à enregistrer
5. Qualité du système/de l'image
6. Durée de fonctionnement
7. Conditions sur le site
8. Capacité de charge
9. Surveillance et stockage d'images
10. Exportation d'images
11. Mesures de routine
12. Mesures d'exploitation
13. Charge de travail du personnel
14. formation
15. Extensions
16. Liste de tous les autres facteurs particuliers et non couverts ci-dessus

7.1 Objectifs/fonctionnalités de base

1. Destination du système
   a. Surveillance de l'objet
   b. Détection/surveillance d'attaques
   c. Enregistrement des attaques
   d. Attaques contre des individus
   e. Attaques contre la propriété
   f. Vol
   g. Vols à main armée
   h. Dommages
   i. Escroquerie
   j. Fraude à la carte de crédit
   k. Autres menaces telles que le transport d'objets de valeur de ou vers la banque

En premier lieu, le système de vidéosurveillance sert à protéger le personnel et les produits. Ensuite, il s'agit de documenter les délits et de les élucider.

2. Grade de sécurité du système (selon DIN EN 62676)
   a. 3 ou 4

7.2 Définition des restrictions de surveillance

Les zones suivantes seront exclues de la visualisation de la scène en définissant l'angle de vue ou en utilisant un masquage électronique dans l'image de la caméra :

1. Panneau tactile du distributeur automatique de billets
2. Panneau tactile des coffres-forts
3. Poste de travail conseiller bancaire
4. Poste de travail de conseiller à la clientèle
5. Abords de l'entrée principale max. 50 cm dans la zone publique.

6. En outre, la restriction de surveillance suivante a lieu dans le cadre du RGPD :
   a. Espaces sociaux, ceux-ci en détail :
      i. Salle de pause,
      ii. Cabines d'essayage
      iii. Toilettes

7.3 Détermination du ou des sites à surveiller

L'exemple ci-dessous est adapté individuellement à chaque site sur la base de l'analyse des risques. Cette procédure est également un processus dynamique et peut encore être modifiée pendant la phase d'utilisation.
La banque est un objet à deux étages avec accès latéral pour les employés et les fournisseurs et une entrée principale au rez-de-chaussée. Outre la surface de conseil ainsi que les locaux sociaux, la cage d'escalier en partie publique est le point central de la vidéosurveillance.

1. Bâtiment
2. Zones intérieures
3. Enveloppe extérieure
4. Cage d'escalier

7.4 Détermination des activités à enregistrer

Les activités définies suivantes doivent être couvertes

1. Les objectifs de protection dans chaque partie du site.
2. la vitesse attendue de la cible
3. la catégorie d'observation des cibles du point de vue de l'opérateur
4. La détection externe est-elle nécessaire ?

Les mouvements de personnes doivent être documentés pendant les heures de bureau. En outre, le personnel de la banque et, si nécessaire, le personnel de sécurité doivent pouvoir se faire une idée de la situation aux entrées et devant la banque.

N° en cours	Domaines	IPS	24/7	LTS	SL	ST	Résolution	IP/IK
1	Caméra extérieure du personnel	15	X	X	**D/C**	X	I	>IP 65 >IK9
2	Entrée du personnel	12	X	X		X	I	>IP 65 >IK9
3	Guichet de nuit	12	X	X		X	I	>IP 65 >IK9
4	Entrée/Sortie client	12	X	X		X	B	>IP 65 >IK9
5	Locaux techniques	12	X	X		X	E	
6	Locaux de consultation / vente	25	X	X		X	E	
7	Coffre-fort (non public)	25	X	X		X	Év.	
8	Entrée du coffre-fort	12	X	X		X	E	

Ce tableau doit être considéré comme un exemple et doit être adapté individuellement.

> FPS Enregistrement en images par seconde
> Fonctionnement 24h/24 et 7j/7 (caméra y compris LED IR)
> LTS long-term support firmware track
> SL Surveillance contre le sabotage
- Déformer (D)
- Couvrir (C)
- Out of Focus (O)

> ST Message d'anomalie
  - Au-dessus ou en dessous de la température de fonctionnement
  - Dans les limites de la température de fonctionnement

Détection de sabotage				
Le système doit pouvoir détecter ce qui suit :	**Grade de sécurité**			
	1	**2**	**3**	**4**
Perte de communication		X	X	X
Si un dispositif d'acquisition d'images à champ fixe ne contient plus la totalité du champ défini, la caméra doit le signaler au VMS et faire l'objet d'une notification.			X	X
L'obstruction ou l'éblouissement intentionnel de l'appareil de prise de vue doit être signalé par la caméra au VMS et faire l'objet d'une plainte.			X	X
Le remplacement des données vidéo à la source de l'image, aux connexions ou à la manipulation de l'image.				X
Une réduction significative du contraste de l'image doit être signalée par la caméra au VMS et faire l'objet d'une notification.				X

7.5 Qualité du système/de l'image

Dans les zones d'entrée, les personnes doivent être identifiées conformément à la norme DIN EN 62676-4 ; aux guichets et aux distributeurs de billets de banque, les procédures doivent être clairement identifiées.

Les activités définies suivantes doivent être couvertes

1. Les principales caractéristiques de performance du système et de ses images affichées
2. Le niveau de détail de l'image nécessaire à l'objectif observé dans chaque image en direct, enregistrée et exportée.
3. Une définition de toute fonctionnalité d'analyse d'image, ainsi que la précision attendue, et si celle-ci est obtenue par l'opérateur ou automatiquement par le système.

Journaux système				
Le système doit consigner les activités suivantes avec l'horodatage (date et heure), l'événement et la source :	**Grade de sécurité**			
	1	**2**	**3**	**4**
Alarmes		X	X	X
Sabotage			X	X
Perte vidéo et reprise à partir d'une perte vidéo (en association avec UPS & possibilité de messages UPS via TCP/UDP)			X	X
Perte d'alimentation		X	X	X
Défaillance de fonction essentielle et reprise après défaillance			X	X
Messages de défaut affichés à l'utilisateur			X	X
Réinitialisation du système (Reset), démarrage du système, arrêt du système		X	X	X
* Actions de diagnostic (vérification de l'état)			X	X
Exportation, impression, y compris identification de la source de l'image et plage temporelle		X	X	X
Connexion et déconnexion de l'utilisateur au poste de travail avec horodatage, connexions réussies et refusées (locales/distantes), y compris la raison du refus (mot de passe incorrect, utilisateur inconnu, compte d'accès expiré)		X	X	X
Modifications des codes d'autorisation/du mot de passe de l'utilisateur			X	X
Contrôle des caméras fonctionnelles				X
Recherche et lecture d'images			X	X
Modifications manuelles des paramètres d'enregistrement			X	X
Confirmation (accusé réception) et réinitialisation des alarmes			X	X
Modifications de la configuration du système			X	X
Définition et modification de la date et de l'heure, y compris l'heure actuelle et la nouvelle heure			X	X

** System Monitor pour l'affichage des données pertinentes des composants système connectés – Sur VMS, uniquement possible avec Expert et Corporate*

7.6 Durée de fonctionnement

24 heures sur 24, 7 jours sur 7 et 365 jours par an
Définition de la durée de fonctionnement du système

1. jours ouvrables
2. Dimanche
3. Jours fériés légaux
4. Congés d'usine
5. Les coûts sur 5 ans pour l'inspection et l'exploitation du système de sécurité vidéo doivent être indiqués. Cela inclut également une garantie du fabricant sur 5 ans et un concept élaboré pour l'inspection. Une attention particulière doit être accordée au logiciel de gestion des appareils et à ses fonctions.

7.7 Conditions sur le site

Définition des conditions environnementales qui s'appliquent et/ou varient pendant la période de surveillance et qui sont déterminantes pour la conception du système.

1. Intensité lumineuse minimale (lux) Intérieur
   Doit être déterminée individuellement.
2. Intensité lumineuse minimale (lux) Extérieur
   Doit être déterminée individuellement.
3. Obstacles potentiels Vue de la caméra
   Doit être déterminée individuellement.
4. Plage de température intérieure
   Entre 19 et 22 degrés Celsius
5. Plage de température extérieure
   Entre -40 et +50 degrés Celsius
6. Autres conditions environnementales ayant une influence ?

7.8 Capacité de charge

1. Alimentation de secours :
   Une alimentation de secours de 30 minutes de tous les composants de la vidéosurveillance doit être prévue.

7.9 Surveillance et stockage d'images

Il faut s'assurer que les images, les séquences vidéo sont enregistrées à tout moment sans perte. Toute perturbation qui empêcherait l'enregistrement doit être protégée par un « système de secours ».

Les paramètres de stockage suivants doivent être couverts

1. Déterminer où et par qui le système doit être surveillé et exploité
2. Déterminer ce qui doit être enregistré.
3. Déterminer la durée de conservation des enregistrements et les circonstances dans lesquelles cette durée peut être modifiée
4. Définition de sites (distants) supplémentaires où les images doivent être disponibles
5. Définir les procédures à suivre pour l'extraction, le stockage et le traitement des images et des données du système

Stockage				
Le VSS doit disposer des fonctions suivantes	**Grade de sécurité**			
	1	**2**	**3**	**4**
Sauvegarde des données via RAID ou enregistrement redondant			X	X
Fonctionnement d'un stockage à sécurité intégrée (par ex. RAID 5 ou mise en miroir continue des données) ou basculement automatique d'un support de stockage vers un autre en cas de défaillance de stockage.				X
Réaction à un signal de commande avec un temps de latence maximal de		1 s	500 ms	250 ms
Lecture d'une image enregistrée dans la mémoire avec un temps maximum après l'incident ou l'enregistrement en cours de			2 s	1 s

Archivage et sauvegarde				
L'archivage doit fournir les fonctions suivantes	**Grade de sécurité**			
	1	**2**	**3**	**4**
L'authentification de chaque image individuelle et de chaque séquence d'images				X
Une sauvegarde automatique et programmée des données d'images d'alarme (développement spécial, plug-in)				X
Une sauvegarde des données d'images d'alarme sur demande manuelle (Evidence Lock)			X	X
Vérification manuelle de la réussite de la sauvegarde de l'image			X	X

7.10 Exportation d'images

Les données vidéo doivent pouvoir être consultées à tout moment par le responsable de la filiale ou une personne prévenue. La sauvegarde des données sur un support de stockage externe incombe au responsable de la sécurité ou à son adjoint. Les données doivent pouvoir être utilisées par les tribunaux et être stockées sans être altérables.

Les paramètres de stockage suivants doivent être couverts

1. Déterminer comment les images sont exportées pour les séquences courtes
2. Déterminer comment les images sont exportées pour les séquences longues
3. Définition de la compatibilité requise du média exporté.

7.11 Mesures de routine

Le système de vidéoprotection est contrôlé chaque matin par le directeur du magasin ou son adjoint pour vérifier qu'il fonctionne en direct et qu'il enregistre bien. En outre, il 's'auto-contrôle' en permanence et signale tout dysfonctionnement à la centrale d'engagement.

Détermination des mesures à prendre dans le cadre de la routine prévue

1. Mesures nécessaires dans le cadre de la routine.

Surveillance des connexions				
Le système doit :	**Degré de sécurité**			
	1	**2**	**3**	**4**
vérifier les connexions de manière répétée à intervalles réguliers, avec un intervalle de temps maximal de			30 s	< 10 s
essayer de se reconnecter avec le nombre de fois suivant avant de déclencher une notification			5	2
respecter le délai maximal autorisé à partir du moment où un opérateur est informé d'une interruption de connexion			180 s	30 s

7.12 Mesures d'exploitation

Les mesures de réponse suivantes doivent être couvertes :

> Détermination de la personne responsable de la réponse
Déterminée par le service de sécurité de la banque

> Définition du type de réponse requis pour un événement potentiel.
Déterminé par le service de sécurité de la Banque

> Définition des délais cibles pour chaque réponse
Déterminé par le service de sécurité de la Banque

7.13 Charge de travail du personnel

On peut supposer qu'il n'y a pas d'autres opérateurs que le contrôle avant l'ouverture de la banque et une recherche par trimestre.

7.14 des formations

Le directeur de la succursale et son adjoint doivent être formés de manière à ce que le système de vidéosurveillance puisse être utilisé en toute sécurité à tout moment. Des documents de formation appropriés ainsi qu'un *Quick Guide* doivent être mis à leur disposition.

Définition de la formation nécessaire pour chaque rôle impliqué dans la gestion et l'exploitation de l'installation.

7.15 Extension

Les extensions de système suivantes doivent être couvertes :

> Une extension prévue du système de 10% doit être prise en compte dans la planification.

7.16 Liste de tous les autres facteurs particuliers et non couverts ci-dessus

Si les exigences opérationnelles ne peuvent pas être satisfaites avec la technologie ou les ressources actuelles, cela doit être indiqué séparément dans l'offre de l'intégrateur/professionnel.

Niveaux d'accès

Fonctionnement	Niveaux d'accès			
	1	2	3	4
Configuration du système	NA	NA	A	A
Modification des codes d'autorisation individuels	NA	A	A	A
Attribution et suppression d'utilisateurs de niveau d'accès 2 et de codes d'autorisation	NA	NA	A	A
Remise en paramètres d'usine	NA	NA	A	A
Mise à niveau du système	NA	NA	A	A
Démarrage/arrêt du VSS ou de composants individuels	NA	NA	A	A

Légende
A Autorisé
NA Non autorisé

Complément aux niveaux d'accès :
Les définitions de rôles d'utilisateur permettent d'appliquer des droits d'utilisateur stricts et granulaires à des rôles spécifiques (utilisateurs individuels ou groupes d'utilisateurs) en ce qui concerne :

> les interfaces client que l'utilisateur peut utiliser
> les caméras et autres
> les dispositifs de sécurité
> les fonctions de l'appareil auxquelles l'utilisateur peut accéder
> fonctions du système que l'utilisateur est autorisé à utiliser
> données de configuration du système que l'utilisateur peut consulter/modifier

Les droits de l'utilisateur peuvent être définis de manière statique ou pour une plage temporelle donnée. Ainsi, il est par ex. possible de bloquer l'accès d'un utilisateur au système en dehors des heures de travail normales ou de restreindre les droits d'accès aux caméras et aux fonctions pendant certaines périodes. Avec les droits d'utilisateur basés sur le temps, il est également possible de bloquer l'accès à des enregistrements plus anciens.

Exigences relatives au code d'autorisation

Exigences relatives au code d'autorisation	Grade de sécurité			
	1	2	3	4
Nombre de clés d'autorisation logiques possibles		> 10 000	> 100 000	> 1 000 000
Nombre de clés d'autorisation physiques possibles		> 3 000	> 15 000	> 50 000

Accès aux données

Fonctionnement	Niveaux d'accès			
	1	2	3	4
Affichage d'images en direct et de données	A	A	A	A
Affichage des images et des données enregistrées lorsque des enregistrements sont disponibles	NA	A	A	A
Affichage d'informations de la mémoire lorsqu'une mémoire fait partie du VSS	NA	A	A	A
Impression et enregistrement de données vidéo	NA	A	A	A
Exportation d'images et de données	NA	A	A	A
Suppression d'images et de données (uniquement avec confirmation)	NA	NA	NA	NA
Légende A Autorisé NA Non autorisé				

Accès aux protocoles du système

Fonctionnement	Niveaux d'accès			
	1	2	3	4
Affichage des protocoles du système	NA	A	A	A
Exportation des protocoles	NA	NA	A	A
Suppression de protocoles	NA	NA	NA	NA
Légende A Autorisé NA Non autorisé				

Accès à la configuration du système

Protection de l'accès à la configuration du système	Niveaux d'accès			
	1	2	3	4
Configuration et installation	NA	NA	A	A
Récupération après une panne du système	NA	A	A	A
Remise en service après un sabotage	NA	A	A	A

Légende
A Autorisé
NA Non autorisé

Identification des données

Le VSS doit identifier clairement les données par les éléments suivants	Grade de sécurisation			
	1	2	3	4
Lieu de stockage (par ex. nom du site)		X	X	X
Source (par ex. appareil de prise de vue avec numéro de caméra comme identification)		X	X	X
Date et heure	X	X	X	X
Date et heure en temps universel coordonné (UTC), y compris le décalage pour l'heure locale				X

Précision du service de temps pour le flux de transport vidéo

Classe	T1	T2	T3	T4
Précision du service horaire pour le flux de transport via NTP	80 ms	40 ms	5 ms	1 ms

Connexions - exigences temporelles

Les équipements de transmission vidéo ne doivent pas dépasser	Classe			
	I1	I2	I3	I4
un temps de connexion initial pour chaque nouvelle demande de flux de données vidéo de	2 000 ms	1 000 ms	500 ms	250 ms

Exigences relatives au réseau de transmission vidéo

Les équipements de transmission vidéo sur un réseau partagé doivent fournir des moyens pour la configuration	Classe			
	C1	C2	C3	C4
du débit maximal des flux de données vidéo pour chaque canal vidéo			X	X
du débit de données maximal pour tous les flux de données vidéo disponibles d'un seul appareil			X	X
du débit maximal ou du nombre de flux de données vidéo pour tous les périphériques clients du réseau			X	X

Exigences relatives au réseau de transmission vidéo

Les équipements de transmission vidéo sur un réseau partagé doivent fournir des moyens pour	Classe			
	P1	P2	P3	P4
la priorisation de certains flux de données par rapport à d'autres, par ex. : les flux de données pour l'enregistrement ou les messages d'alarme par rapport aux flux de données d'images en direct			X	X *
la priorité de certains utilisateurs par rapport à d'autres, par ex. pour le contrôle PTZ			X	X

** Pas de priorisation des flux de données, car un seul flux vidéo est récupéré*

Exigences de performance pour le streaming vidéo et la lecture du flux de données vidéo				
Classe	**S1**	**S2**	**S3**	**S4**
Perte maximale	240 ppm	120 ppm	60 ppm	30 ppm
Temps de latence unidirectionnel maximal du flux de données vidéo en direct (y compris encodage, maillage, décodage, lecture)	600 ms	400 ms	200 ms	100 ms
Temps de réponse maximum en mode lecture (pause, pas à pas, etc.)	400 ms	200 ms	200 ms	100 ms
Latence d'aller et retour incluant visualisation et contrôle, par exemple PTZ (Panoramique/inclinaison/zoom)	700 ms	500 ms	300 ms	200 ms
*Latence d'aller et retour incluant visualisation et contrôle, par exemple PTZ lorsque le déplacement d'objets doit être surveillé et suivi	650 ms	450 ms	250 ms	150 ms

** ne s'applique pas, car seules des caméras fixes sont installées*

Gigue des paquets du flux de données vidéo sur le réseau					
Classe	**M0 ms**	**M1 ms**	**M2 ms**	**M3 ms**	**M4 ms**
Gigue maximale du paquet crête à crête	-	160	80	40	<20

Surveillance des connexions				
Le système doit garantir	**Degré de sécurité**			
	1	**2**	**3**	**4**
une durée maximale autorisée d'indisponibilité de l'appareil			180 s	30 s
un temps maximal pour la détection de la perte du signal en direct		8 s	4 s	2 s
L'exigence ci-dessus permet de déterminer si une communication est possible en surveillant la transmission vidéo afin de s'assurer qu'elle est disponible pour la transmission d'un signal ou d'un message. La surveillance peut prendre la forme d'une recherche d'interférences lorsque le dispositif de transmission vidéo communique avec d'autres dispositifs ou applications via des connexions partagées.				

8. Réglages dans les caméras

Selon l'application et le domaine d'utilisation, différents réglages sont nécessaires ou possibles dans les caméras. Les réglages mentionnés ici sont des recommandations et leur utilité doit être vérifiée sur place dans les différentes filiales.

8.1 Temps d'obturation (shutter)

Les vitesses d'obturation des caméras doivent s'adapter de manière entièrement automatique aux conditions de luminosité du magasin. Les vitesses d'obturation fixes ne sont pas autorisées.

Dans les zones où l'on peut s'attendre à des mouvements rapides à courte distance de la caméra, il est recommandé de limiter le temps d'obturation.

Les valeurs exactes nécessaires sont déterminées en fonction de

- la luminosité dans la succursale
- la densité de pixels par mètre et
- la finalité de la surveillance.

Plus les détails sont importants et plus la résolution en pixels/mètre est élevée, plus le temps d'obturation sélectionné doit être adapté dans les paramètres de la caméra.

8.2 WDR (Wide Dynamic Range)

La performance des propriétés WDR des caméras dépend d'un grand nombre de facteurs et diffère parfois sensiblement entre les différents types de caméras.

Il convient de vérifier en conséquence si la fonction WDR offre une valeur ajoutée pour l'utilisation prévue.

Afin d'éviter/de minimiser les artefacts de mouvement, il peut être nécessaire d'adapter la vitesse d'obturation.

9. Prescription des switchs :

Afin de pouvoir garantir un service sans faille du réseau, les fonctions suivantes doivent être assurées :

- Protection par mot de passe
- Filtrage d'adresse IP
- Chiffrement HTTPS
- Contrôle d'accès au réseau IEEE 802.1X
- ACL
- VLAN privés
- Snooping DHCP

ainsi que les protocoles suivants sont pris en charge :
IPv4, IPv6, HTTP, HTTPS, QoS, Bonjour, UPnP, SNMP v1/v2c/v3, DNS, NTP, TCP, UDP, IGMP, ICMP, DHCP, ARP, SSH, STP, RSTP, MSTP, LLDP, LLDP-MED, TFTP, SMTP, BPDU.

Lors de l'affectation des commutateurs, il convient de tenir compte du calcul de la puissance en fonction des composants connectés et à alimenter. L'objectif devrait être une utilisation symétrique et une répartition des risques des appareils connectés.

10. Prescription des routeurs

Afin de pouvoir garantir un service sans faille du réseau, seuls des Cisco Integrated Services Router sont intégrés dans le réseau.
Actuellement, les composants suivants ont été testés et approuvés :

- ISR4351/K9*
- ISR4451-X/K9*

**ou le modèle successeur*

11. Connexion/accès VPN du siège social selon la protection informatique de base du BSI (Bundesamt für Sicherheit in der Informationstechnik)

Exigences de base
Les exigences suivantes DOIVENT être mises en œuvre en priorité pour le module VPN (Virtual Private Network) :

11.1 Exigences standard

Conjointement avec les exigences de base, les exigences suivantes correspondent à l'état de l'art pour le module VPN. Elles DOIVENT être mises en œuvre.

11.1.1 Planification du déploiement du VPN

Le déploiement d'un VPN DOIT être soigneusement planifié. A cette occasion, les responsabilités pour l'exploitation du VPN DOIVENT être définies. Des groupes d'utilisateurs et leurs autorisations DOIVENT également être planifiés pour le VPN. Il est également IMPÉRIEUX de définir la manière dont les droits d'accès accordés, modifiés ou retirés doivent être documentés.

11.1.2 Sélection d'un fournisseur de services VPN [Responsable de la sécurité de l'information (RSSI)]

Des accords de niveau de service (SLA) DOIVENT être négociés et documentés par écrit avec un fournisseur de services VPN. Il DOIT y avoir des contrôles réguliers pour vérifier que le fournisseur de services VPN respecte les SLA convenus.

11.1.3 Installation sécurisée de terminaux VPN

Le système d'exploitation sous-jacent de la plateforme VPN DOIT être configuré de manière sécurisée. Si un appareil est utilisé, il DOIT faire l'objet d'un contrat de maintenance valide. Il DOIT être garanti que seul un personnel qualifié installe les composants VPN. L'installation des composants VPN et tout écart par rapport aux spécifications de planification DOIVENT être documentés. La fonctionnalité et les mécanismes de sécurité choisis pour le VPN DOIVENT être testés avant la mise en service.

11.1.4 Configuration sécurisée d'un VPN

Une configuration sécurisée DOIT être définie pour tous les composants du VPN. Celle-ci DOIT être documentée de manière appropriée. L'administrateur responsable DOIT également contrôler régulièrement si la configuration est encore sûre et éventuellement l'adapter pour tous les systèmes informatiques.

11.1.5 Verrouillage des accès VPN qui ne sont plus nécessaires

Il DOIT être vérifié régulièrement que seuls les systèmes informatiques et les utilisateurs autorisés peuvent accéder au VPN. Les accès VPN qui ne sont plus nécessaires DOIVENT être désactivés rapidement. L'accès au VPN DOIT être limité aux heures d'utilisation nécessaires.

11.1.6 Réalisation d'une analyse des besoins VPN

Une analyse des exigences DOIT être effectuée afin de déterminer les scénarios d'utilisation pour le VPN concerné et de pouvoir en déduire les exigences relatives aux composants matériels et logiciels nécessaires. Les points suivants DOIVENT être considérés dans l'analyse des exigences :

- Processus d'affaires ou tâches spécialisées
- Voies d'accès
- Procédures d'identification et d'authentification
- Utilisateurs et autorisations d'utilisation
- Responsabilités et voies de notification

11.1.7 Planification de la réalisation technique VPN

Outre la planification générale (voir NET.3.3.A1 Planification du déploiement du VPN), les aspects techniques d'un VPN DOIVENT être soigneusement planifiés. Ainsi, les méthodes de cryptage, les points de terminaison VPN, les protocoles d'accès autorisés, les services et les ressources doivent être définis pour le VPN. En outre, les sous-réseaux accessibles via le VPN DOIVENT être définis (voir NET.1.1 Architecture et conception du réseau).

11.1.8 Création d'une politique de sécurité pour l'utilisation du VPN

Une politique de sécurité concernant l'utilisation du VPN DOIT être créée. Elle DOIT être communiquée à tous les employés. Les mesures de sécurité décrites dans la politique de sécurité DOIVENT être expliquées dans le cadre de la formation. Si un accès VPN est mis en place pour un employé, il DOIT recevoir une fiche d'information sur les principaux mécanismes de sécurité VPN. Tous les utilisateurs de VPN DOIVENT être tenus de respecter les directives de sécurité.

11.1.9 Choix approprié de produits VPN

Lors de la sélection des produits VPN, il DOIT être tenu compte des besoins des institutions en matière d'interconnexion de différents sites et de connexion des employés mobiles ou des télétravailleurs.

11.1.10 Fonctionnement sécurisé d'un VPN

Un concept d'exploitation DOIT être établi pour les VPN. Celui-ci DOIT prendre en compte les aspects de gestion de la qualité, de surveillance, de maintenance, de formation et d'autorisation.

11.1.11 Connexion sécurisée d'un réseau externe

Si un VPN est utilisé pour se connecter à un réseau externe, les procédures d'authentification et de cryptage considérées comme sûres DOIVENT être mises en œuvre. La méthode choisie pour l'échange de clés DOIT également être considérée comme sûre. Il DOIT être garanti que les connexions VPN sont établies UNIQUEMENT entre les systèmes informatiques et les services prévus à cet effet. Les protocoles de tunnel utilisés à cet effet DOIVENT être adaptés à l'utilisation.

11.1.12 Gestion des utilisateurs et des accès pour les VPN d'accès à distance

Pour les VPN d'accès à distance, une gestion centralisée et cohérente des utilisateurs et des accès DOIT être assurée. Les méthodes d'authentification utilisées DOIVENT satisfaire aux exigences du module ORP.4 Gestion des identités et des autorisations.

Si des serveurs autonomes sont utilisés pour la gestion des utilisateurs et des accès, il DOIT être garanti que ces serveurs sont configurés et exploités de manière sûre et cohérente par rapport aux exigences du module ORP.4 Gestion des identités et des autorisations. En outre, les serveurs utilisés DOIVENT être protégés contre les accès non autorisés.

11.1.13 Intégration de composants VPN dans un pare-feu

Les composants VPN DOIVENT être intégrés dans le pare-feu. La manière dont les composants VPN sont intégrés dans le pare-feu DOIT être documentée.

11.1.14 Exigences en cas de besoin de protection accru

Des propositions d'exigences allant au-delà du niveau de protection correspondant à l'état de la et qui DOIVENT être prises en considération EN CAS DE BESOINS DE PROTECTION ACCRUS sont présentées ci-dessous à titre d'exemple pour le composant VPN. La définition concrète se fait dans le cadre d'une analyse des risques. Les lettres entre parenthèses indiquent les valeurs fondamentales qui sont protégées en priorité par l'exigence (C = confidentialité, I = intégrité, A = disponibilité).

12. Autres exigences

1. Il doit être possible de repeindre les caméras dans la couleur RAL souhaitée sans perdre la garantie.

Il doit s'agir d'un processus standardisé par le fournisseur du fabricant de la caméra.

2. L'intégrateur doit pouvoir justifier d'au moins un projet comparable, en termes d'envergure et de tâches.

Les valeurs marquées en vert correspondent aux exigences de ce projet.

FR/R1/2202

À propos d'Axis Communications

En concevant des solutions réseau qui améliorent la sécurité et permettent le développement de nouvelles façons de travailler, Axis contribue à un monde plus sûr et plus clairvoyant. Leader technologique de la vidéo sur IP, Axis propose des produits et services axés sur la vidéosurveillance, l'analyse vidéo, le contrôle d'accès, l'interphonie et les systèmes audio. L'entreprise emploie plus de 3800 personnes dans plus de 50 pays et collabore avec des partenaires du monde entier pour fournir des solutions clients adaptées. Axis a été fondée en 1984, son siège est situé à Lund en Suède.

Pour en savoir plus, visitez notre site web www.axis.com