Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

PRÉFET DE LA ZONE DE DÉFENSE ET DE SÉCURITÉ SUD

PRÉFET
DE LA ZONE
DE DÉFENSE
ET DE SÉCURITÉ
SUD

Cahier des Clauses Techniques Particulières.
Création / modification d'un système de mise en sûreté

ANNEXE 5 :
Principes d'exploitation du système de mise en sûreté 2020

Les principes de déploiement des équipements ci-dessous servent de référence aux particularités du site décrites dans le document principal

CCTP SURETE – DESCRIPTIF DU PROJET

Table des matières

1. Gestion du Système....3
2. Gestion des droits opérateurs....3
3. Gestion des journaux....5
4. Gestion des accès....6
4.1. Gestion des badges....6
4.1.1. Personnalisation des badges utilisateurs....6
4.1.2. Gestion des profils....6
4.1.3. Type de badge (CAM)....7
4.1.4. Invalidation des badges....7
4.1.5. État d'un badge....7
4.2. Gestion des rapports....8
5. Exploitation locale....9
5.1. Gestion TYPE PC Sécurité (PCS)....9
5.1.1. Aménagement du PCS....9
5.1.2. Gestion des enquêtes....9
5.1.3. Gestion de la cartographie....9
5.1.4. Gestion des alarmes....10
5.1.5. Gestion du système vidéo et scénarii....11
5.1.6. Gestion des caméras....12
5.1.7. Pilotage des caméras....12
5.2. Principe de gestion des réactions aux événements....12
6. Exploitation distante....13
6.1. Gestion du contrôle d'accès....14
6.2. Gestion du système de vidéo-protection....14
6.3. Gestion de l'intrusion....14
7. Exploitation distante à partir d'une DDSP....15
7.1. Gestion du contrôle d'accès....15
7.2. Gestion du système de vidéo-protection....15
7.3. Gestion de l'intrusion....16

1. GESTION DU SYSTÈME

La solution doit permettre de gérer plusieurs types de profils :

- Le profil « **Administrateur système** » permettant à un agent clairement désigné et habilité de vérifier le bon état de fonctionnement du dispositif, d'en administrer l'ensemble (paramétrage, configuration, supervision, sauvegardes, lectures, cartographie…) et d'avoir la visibilité des informations qu'il contient. En aucun cas le profil « Administrateur système » ne doit permettre de lire ni d'extraire des fichiers vidéo.
- Le profil « **Gestionnaire système** » permettant à un agent de gérer les profils, les mots de passe et les droits des opérateurs de chaque système. En aucun cas le profil « Gestionnaire système » ne pourra lire, extraire des fichiers vidéo, ni porter atteinte à l'intégrité des données vidéo enregistrées par le système.
- Le profil « **Opérateur**» permettant à un agent d'exploiter un système. Il peut y avoir plusieurs types d'opérateurs en fonction des systèmes. Les principaux types d'opérateurs sont :
  - Contrôle d'accès : l'opérateur « **Gestionnaire des accès** » administre et gère les profils d'utilisateurs, produit des badges, etc . En aucun cas , le profil « Gestionnaire des accès » ne pourra porter atteinte à l'intégrité des données vidéo enregistrées par le système,
  - Vidéoprotection : l'opérateur « **Opérateur d'extraction** » consulte les images, procède à des recherches de séquences, extrait des images, etc. En aucun cas, le profil « Opérateur d'extraction» ne pourra porter atteinte à l'intégrité des données vidéo enregistrées par le système.
  - Supervision : L'opérateur « **Opérateur poste de contrôle et de sécurité** » surveille la cartographie, consulte les vidéo, gère des alarmes, produit des badges, gère des portes, consulte les fiches réflexe, etc. Le profil « **Opérateur du poste de sécurité** » ne pourra porter atteinte à l'intégrité des données vidéo enregistrées par le système,

L'implantation des différents terminaux d'exploitation se fera en fonction du choix retenu par le maître d'ouvrage.

2. GESTION DES DROITS OPÉRATEURS

Les profils d'utilisateurs permettent de gérer des « droits » ou privilèges sur les objets Équipement/Événement/Alarmes/Actions/Espace de Travail dans tous les applicatifs utilisés.

Toutes les actions sur le système sont réservées et protégées par des droits liés au compte applicatif de l'opérateur. Il y a à minima trois types de droits :

- Le droit de lecture confère à un opérateur le pouvoir de visibilité,
- Le droit d'écriture confère à un opérateur un pouvoir d'action,
- Le droit de modification confère à un opérateur les droits de modification.

Les éléments sont configurés en droits (profil par opérateur), pour permettre à minima les fonctions suivantes :

- Des droits sont gérés pour la création/visualisation/configuration des entités en fonction du système (utilisateur, badge, alarme, actions, fiche de porteur, rapport, équipement),

- Des droits sont gérés par équipement pour permettre la création, la visualisation, la configuration, le changement d'état (actif/inhibé),

- Un équipement (porte, lecteur de badge, détecteur) peut être invisible à un utilisateur,
- Un équipement (porte, lecteur de badge, détecteur) peut être en accès lecture seule. Par exemple, une porte en lecture seule doit permettre la visualisation de son état mais inhibe les droits d'actions (ouverture et fermeture).

- Des droits sont gérés pour les éléments partagés,

- Infériorisation des commandes joystick,
- Priorisation sur l'accès à des écrans et vignettes des murs d'images,
- Accès en lecture seule sur la définition des écrans et vignettes des murs d'images,
- Accès en modification seule sur la définition des écrans et vignettes des murs d'images,

- Des droits sont gérés pour la création, la visualisation, le déclenchement des actions programmées ou natives,

- Des droits sont gérés pour la création, la visualisation, la modification de l'espace de travail,

- Des droits sont gérés pour l'accès aux applications de la solution.

Un opérateur « poste de contrôle et de sécurité » doit pouvoir :

- ✔ Disposer d'un retour type fil de l'eau (historique des évènements notifiés), événement/alarme sur les équipements dont il aura la visibilité,
- ✔ Disposer de droit en écriture sur un accès pour l'ouvrir ou le fermer,
- ✔ Sélectionner une vue dans les listes de caméras pré-définies,
- ✔ Disposer de la lecture de l'historique et de l'acquittement des évènements sur les équipements dont il aura la visibilité.

Un opérateur « gestionnaire du système » doit pouvoir :

- ✔ Personnaliser l'ergonomie de son espace de travail,
- ✔ Créer/modifier des profils des différents opérateurs, autres que l'administrateur,
- ✔ Disposer de la lecture de l'historique des évènements sur les équipements dont il aura la visibilité.

Un opérateur « gestionnaire des accès » doit pouvoir :

- ✔ Personnaliser l'ergonomie de son espace de travail,
- ✔ Créer/modifier des profils, des groupes de porteurs, des porteurs de badge,
- ✔ Enrôler les badges, les plaques d'immatriculation,
- ✔ Disposer d'un droit en écriture pour ouvrir ou fermer les accès,
- ✔ Disposer d'un retour type fil de l'eau (historique des évènements) événement/alarme sur les équipements dont il aura la visibilité,
- ✔ Disposer des droits de lecture/écriture/modification des équipements d'accès,
- ✔ Editer un profil de badge, ou de plaque d'immatriculation, et son historique.

Un opérateur « extraction d'images » doit pouvoir :

- ✔ Configurer son espace de travail,

- ✔ Rechercher des séquences d'images enregistrées sur le stockeur,
- ✔ Faire des extractions d'images (lecture seule)
- ✔ Disposer d'un droit en écriture sur les ports USB de son espace de travail,
- ✔ Disposer d'un retour type fil de l'eau événement/alarme sur les équipements dont il aura la visibilité,

Seuls les opérateurs déclarés avec un profil « administrateur » disposent d'un accès en écriture sur tous les équipements.

Le système de gestion des droits est paramétrable :

- gestion sécurisée des mots de passe des utilisateurs,
- définition des droits relatifs à la modification de l'espace de travail,
- modification des droits des équipements partagés ou des informations partageables, dans le cadre de « raccordements » (fédération, déport, supervision multi-site) ou dans le cadre d'utilisation locale (partage de la motorisation des caméras, des murs d'images).

Le titulaire fournira la documentation détaillée décrivant les possibilités natives offertes par le système de gestion des droits.

3. GESTION DES JOURNAUX

La solution doit permettre la consultation de l'ensemble des actions effectuées sur le système que ce soit au niveau des postes clients ou au niveau des postes serveurs mais selon les droits octroyés à chaque utilisateur.

Les actions tracées sont à minima :

- Système
  - ✔ Arrêt / Lancement des services applicatifs (journalisation incluse),
  - ✔ Arrêt critique sur incident,
  - ✔ Arrêt système par exploitant (identifiant, date/heure),
  - ✔ Démarrage système par exploitant (identifiant, date/heure),
  - ✔ Évènement de ressources systèmes.
- Administration applicative
  - ✔ Ajout/suppression d'équipements,
  - ✔ Gestion des comptes (création/suppression/modification des droits).
- Exploitation courante
  - ✔ Heure de connexion, déconnexion,
  - ✔ Action sur un équipement,
  - ✔ Action sur un badge.

L'accès aux données de traçabilité doit être autorisé uniquement aux personnels habilités.

4. GESTION DES ACCÈS

4.1. Gestion des badges

4.1.1. Personnalisation des badges utilisateurs

La solution doit permettre la gestion de porteurs de badges et de groupes de porteurs de badge. Ces groupes sont des listes créées par direction, service ou site.

La solution doit permettre de paramétrer les propriétés suivantes d'un porteur de carte :

- Nom,
- Prénom,
- Fonction, bâtiment, étage, bureau, service, poste téléphonique, émail,
- Société, service, fonction,
- Adresse (n°, rue, code postal, ville, pays),
- Véhicule (immatriculation),
- Conduite à tenir et observation (255 caractères),
- Dates (remise de badge, début et fin de validité, restitution de badge).

Les champs nominatifs acceptent toutes les lettres donc les caractères accentués et ponctuations utilisés dans la langue française.

La solution doit permettre la gestion de :

- Champs personnalisés (au moins 15),
- Date d'activation/ Date d’expiration,
- Gestion d’une photo capturée à partir d’un périphérique numérique (webcam ou caméra de vidéo surveillance) ou importé par fichier,
- Statut (profil activé ou désactivé, perdu, volé, bloqué, etc..).

Les champs personnalisables sont des entités type :

- Booléen,
- Date,
- Entier,
- Images ou fichiers graphiques,
- Nombres décimaux,
- Texte.

La solution détecte les doublons à partir du nom, prénom, et/ou service, société.
Tous les champs ne sont pas obligatoirement renseignés. Les champs de la fiche de porteurs de badge doivent pouvoir être obligatoires ou non. Elle empêche la création de fiches similaires.
La solution doit permettre :
- d’activer ou d’inhiber un badge ou un groupe de badges manuellement sous réserve des droits utilisateur.
- de gérer des erreurs à l’importation.

4.1.2. Gestion des profils

La solution doit permettre la création de profils à partir de règles d’accès associées à des groupes de points d’accès.

La solution doit permettre :

- l'association de porteurs ou des groupes de porteurs à des règles d'accès et des profils.
- de paramétrer les droits d’accès en fonction des points d’accès et de plages horaires et calendaires.
- de définir des jours fériés :
  - ponctuels,
  - annuels reconductibles, jours fériés calendrier français recalculé automatiquement d'une année sur l'autre.

La solution doit permettre de gérer au minimum 20 profils.

4.1.3. Type de badge (CAM)

LE BADGE DOIT ETRE COMPATIBLE AVEC LA CARTE AGENT DU MINISTERE DE L’INTERIEUR

La solution doit permettre la gestion de différents types de badge portés par des modèles de badge différents. On différenciera naturellement le type de badge, des droits ou profils liés à chaque badge.

Pour simplifier les choses et pour ne pas dévoiler d’informations vitales, il existe au niveau de la personnalisation des badges à minima les catégories suivantes pour les personnes :

- Badge **P** : badge nominatif pour les **permanents** toutes directions confondues,

- Badge **V** : badge non nominatif, journalier, pour des **visiteurs** occasionnels externes. Les droits d’accès associés aux badges V sont définis par le bureau des badges. Ce sont des droits minimaux.

4.1.4. Invalidation des badges

La solution doit permettre de

- rendre automatiquement invalide un badge à la fin de sa période de validité. Cette fonction est particulièrement mise en service pour les badges journaliers.

- bloquer un badge lorsqu’il n’est pas utilisé pendant une durée supérieure à un temps paramétré (de l’ordre de 2 mois). Cette fonctionnalité peut être activée sur certains profils ou badges.

- invalider n’importe quel badge de la solution.

4.1.5. État d’un badge

L'opérateur disposant des droits peut, en recherchant un badge (recherche multicritères à partir d’un nom/numéro d’identifiant) décider de positionner le badge comme :

Actif	Toutes les fonctions prévues
Inactif	Le badge n'ouvre aucun accès. Sa présentation sur un lecteur déclenche une alarme précisant : « Badge inactivé le jj/mm/aa à hh:mn par nom_personne ».
Perdu	Le badge n'ouvre aucun accès. Sa présentation sur un lecteur déclenche une alarme précisant :

	« Badge déclaré perdu le jj/mm/aa à hh:mn par nom_personne »
Volé	Le badge n'ouvre aucun accès. Sa présentation sur un lecteur déclenche une alarme précisant : « Badge déclaré volé le jj/mm/aa à hh:mn par nom_personne ».
Expiré	Le badge n'ouvre aucun accès. Sa présentation sur un lecteur déclenche une alarme précisant : « Badge bloqué le jj/mm/aa à hh:mn par nom_personne ».

4.2. Gestion des rapports

Les rapports standards d'activité courante seront :

- Liste des alarmes,
- Historique des mouvements d'un utilisateur,
- Localisation d’un utilisateur,
- Historique des mouvements de badges,
- Liste des badges non présentés dans telle zone depuis N jours (N paramétrable),
- Historique des événements par type d'objet,
- Taux d'utilisation des lecteurs.

Les rapports d'activité opérateurs seront :

- Historique des login,
- Journal des acquittements trié par date, filtré pour tout ou partie des opérateurs.

Les rapports liés aux utilisateurs seront :

- Liste des badges,
- Etat des badges,
- Liste des badges ayant accès à un ou plusieurs lecteurs,
- Liste des badges venant à expiration à une date donnée,
- Liste des badges appartenant à une série de groupe d'utilisateurs,
- Liste des utilisateurs avec leur fiche d'identification,
- Liste simplifiée des utilisateurs.

5. EXPLOITATION LOCALE

5.1. Gestion TYPE PC Sécurité (PCS)

5.1.1. Aménagement du PCS

Les opérateurs des postes de supervision peuvent être situés dans :

- le local chef de poste d'un commissariat,
- le poste de garde d'un Hôtel de Police,
- le poste de garde d'une préfecture ou sous-préfecture,
- le centre de supervision d'un centre administratif,
- le Centre d'Information et de Commandement (CIC) d'une Direction Départementale de la Sécurité Publique (DDSP).

Chaque poste pourra disposer de plusieurs écrans:

Le premier écran affichera la cartographie sous forme de plan graphique renseigné du site, en 2D ou 3D avec noms des lieux, numéro de l'étage, nom ou numéro de la pièce, type et qualité des moyens, ainsi que la disposition des moyens mis en place tels que caméra, détecteur/contrôleur d'ouverture de porte, détecteur de mouvement, le lancement de commandes directes (mise en/hors service de point d'entrée, activation de sortie, déverrouillage d'accès, etc.). .Sur ce même écran, une fenêtre présentera une fiche « main courante » précisant les événements du jour (prévus, arrivés, en cours, etc.), les incidents types, la conduite à tenir, les mesures prises qui permettent de prévoir, organiser et gérer la sécurité au quotidien en cas d'événement, qu'il soit anodin ou grave. Il sera aussi celui qui permettra l'acquittement et la visualisation des alarmes, la gestion manuelle et automatique des caméras, le pilotage de l'éclairage, l'utilisation des prépositions des caméras sur le plan graphique, l'enregistrement numérique sur disque dur des événements du site).

- le second ou les autres, de grande taille, affichera/afficheront les images de l'ensemble des caméras, en cascade ou en mosaïque au choix de l'opérateur, avec possibilité d'afficher en plein écran l'une ou l'autre des caméras par un simple clic ou de glissement de souris.

Le fonctionnement de ces écrans sera simultané.

5.1.2. Gestion des enquêtes

La solution doit permettre la recherche d'événements-alarmes, mémo, signet, métadonnées et de visualiser la vidéo éventuellement associée à l'événement.

5.1.3. Gestion de la cartographie

Le système dispose d'un outil de cartographie dynamique permettant de localiser tous les équipements de sécurité (caméra, portillon, porte surveillée, contrôle d'accès, lecteur RFID, haut parleur, sirène, détecteur de présence, etc..) sur un plan. Le plan et ses équipements peuvent s'afficher à l'échelle (proportion respectées), par zone, par bâtiment et par étage.

La cartographie accepte les fonctions de zooms avant et arrière à partir de la molette de la souris (par exemple).

Le système doit permettre de zoomer dans le plan, de se déplacer sur 360 degrés.

Le système dispose d'une cartographie multi-sites et multi-niveaux.

La cartographie doit permettre d'exécuter des actions de type glisser/déposer de la cartographie vers toute vignette ou tuile d'affichage pour permettre :

- De visualiser une caméra par dépôt de celle-ci vers une vignette d'affichage,
- De visualiser les événements liés à une porte par dépôt de celle-ci vers une vignette d'affichage,
- De visualiser les photos des titulaires identifiés sur un accès par dépôt de celui-ci vers une vignette d'affichage.

La cartographie doit permettre de proposer une aide contextuelle par équipement. Il devra apparaître un encadré dans lequel devra figurer leur appellation, leur position (étage, zone de sûreté...) et le moyen de détection (détecteur, détecteur/contrôleur, caméra fixe, mobile etc.).

Ce plan graphique, disponible sur les postes d'exploitation, servira en particulier à la visualisation des événements.

Par ailleurs, ces événements entraîneront une animation des éléments graphiques représentant les équipements (barrières infrarouges, détecteurs d'intrusion, caméras etc.) de la zone concernée.

Lorsqu'un événement se produit dans une zone qui est constituée d'une (ou plusieurs) caméra(s) et/ou d'une barrière infrarouge ou autre détecteur de mouvement, chaque équipement de la zone de détection, qui aura déclenché l'alarme, sera automatiquement signalé par un changement de couleur et d'un clignotement sur la cartographie et d'une alerte sonore.

Exemple: la caméra de visualisation passe en rouge de même que le (ou les) faisceau(x) franchi(s) reliant deux barrières infrarouges, etc.).

Par contre, ce changement de couleur sera différent suivant l'état du système, par exemple :

- En rouge lors du déclenchement d'une alarme et restera en rouge clignotant tant que l'alarme ne sera pas acquittée,
- En orange lors du déclenchement d'une panne.

5.1.4. Gestion des alarmes

La solution doit permettre la définition d'une alarme ou d'un événement/alarme à partir de la combinaison d'événements détectés par le système, contact sec, détection d'ouverture, détection d'événements d'identification, d'événement natifs et programmables.

La solution doit permettre de paramétrer la notion d'alarme et d'événement pour pouvoir, sous réserve de ses possibilités, définir une alarme et un événement et éventuellement convertir une alarme en événement (et réciproquement).

Le système doit permettre une hiérarchisation des alarmes par niveau et une hiérarchisation des événements. La solution doit permettre la gestion de plusieurs niveaux d'alarmes et d'événements distincts. Les niveaux d'alarmes doivent pouvoir être filtrés sur la console opérateur et affichés par des signes distinctifs (couleur, etc..). Le terme alarme prioritaire utilisé dans ce document est une alarme de niveau 1.

Chaque alarme doit pouvoir être déclarée dans un champ de 1 à 255 caractères.

Le système doit permettre d'afficher une procédure à suivre en « alarme ».

Le système doit permettre de gérer des alarmes notifiées par l'opérateur.

Le système doit permettre une gestion des alarmes en cascades.

Bien que le système ne sera pas relié à une messagerie ou un serveur de SMS local ou distant, il devra néanmoins garder la possibilité d'émettre des alarmes techniques (perte de l'archiveur, perte service, etc…)

par Email/SMS pour une utilisation ultérieure.

5.1.5. Gestion du système vidéo et scénarii

La solution doit disposer d'une interface simple pour créer des scénarii d'actions. Ces scénarii sont déclenchés soit par un ou une association d'événements (alarme/calendaire), soit manuellement par l'opérateur.

L'opérateur peut pour un scénario nommé :

- Définir des actions sur des portes, passages, équipements,
- Définir des actions sur des caméras.

Le système de vidéo-détection fera l'objet d'un fonctionnement particulier intégrant les informations ci-après :

- D'une prise en compte de plages horaires,
- D'un déclenchement d'alarme selon la zone de détection,
- D'une localisation sur un plan graphique.

Le système d'acquisition et de visualisation numérique des images doit pouvoir s'activer automatiquement dès le déclenchement de la caméra couplée à la détection de la zone traversée ou de mouvement particulier ou d'objet identifié ou d'interprétation et d'analyse d'images.

Il faut pouvoir créer et gérer pour chaque caméra des scenarii préprogrammés (rondes dans le temps ou rotation dynamique cyclique et cycles d'images pour différents groupes de caméras).

Les caméras peuvent être individuellement programmées sur un scénario qui s'appliquera par défaut, au bout d'un laps de temps sans action (rondes, repositionnements).

- Portes et Points d'Accès :

  Les actions natives pour les équipements portes/points d'accès sont : Ouvrir, Fermer, Inhiber, Verrouiller.

- Visiophonie :

  Les actions natives pour les équipements de visiophonie sont : Ouvrir, Fermer, Inhiber, mettre en attente ou transférer une communication.

- Point Alarme :

  Les actions natives pour les équipements d'alarmes sont : Armer, Désarmer, Inhiber.

- Mur image :

  Adapter l'affichage du mur d'image dans une configuration personnalisée.

L'utilisateur peut pour un scénario nommé :

- Définir des actions sur des portes, passages, équipements de détection d'intrusion,
- Définir des actions sur des caméras.

Exemples de scénarii modifiables :

Scénario 1 : Exploitation « normale de jour »,
Scénario 2 : Exploitation « normale de nuit »,
Scénario 3 : Exploitation « normale de week-end et de jours fériés »,

Scénario 4 : Exploitation en situation normale exceptionnelle prévisible (exemple élections, visites de personnalités etc.),

Scénario 5 : Situation de crise.

Pour chaque scénario il sera possible de programmer les fonctions de chaque caméra, les enregistrements à effectuer, les consignes à appliquer en cas d'alarme, etc.

Le passage d'un scénario à l'autre pourra indifféremment se faire automatiquement selon un programme horaire ou une action manuelle par un opérateur autorisé.

5.1.6. Gestion des caméras

Les actions natives sont à minima:

- Déclencher les prépositions d'une caméra motorisée,
- Afficher une caméra / un groupe de caméra sur une (des) vignette(s) du mur d'image,par cliquer/glisser
- Déclencher un scénario identifié par un nom,
- Déclencher une ronde vidéo,
- Déclencher/Arrêter un enregistrement,
- Ajouter un signet et/ou une métadonnée jointe,
- Déclencher l'asservissement du lecteur vidéo pour rejouer une séquence,
- Automatiser la production d'un rapport,
- Accéder aux caméras en Https.

Le système doit permettre de déclencher une action programmée.

Il doit pouvoir, lors d'une alarme, afficher dans une vignette d'un écran local ou distant la vue d'une caméra de la zone concernée.

Le système doit permettre de déclencher une action à distance sur un autre sous système dans le cas de raccordement ou d'utilisation multi-site.

5.1.7. Pilotage des caméras

Le système doit pouvoir piloter les caméras PTZ par simple clic de souris.

Un joystick unique doit permettre de gérer l'ensemble des caméras motorisées.

La solution doit permettre d'attribuer aux opérateurs différents niveaux de priorité sur la prise en main des caméras.

Le pilotage de la télémétrie (motorisation) au poste de sécurité sera toujours prioritaire par rapport aux autres opérateurs de la solution. Dans ce cas, ces opérateurs seront informés par un message indiquant que la caméra est pilotée par une autorité supérieure. La caméra revient ensuite dans sa position initiale après une temporisation réglable ou une action de l'autorité.

La solution doit permettre de gérer plusieurs joysticks répartis sur différents postes-opérateur.

5.2. Principe de gestion des réactions aux événements

Les actions natives sont :

- Acquitter une alarme,
- Afficher un objet du système (fiche carte, fiche utilisateur/voiture, photo d'un identifiant),
- Afficher le signal d’une caméra / les signaux d’un groupe paramétrable de caméras sur une vignette du mur d’image,
- Ajouter un signet et/ou une métadonnée jointe au système vidéo,
- Automatiser la production d'un rapport,
- Déclencher l'asservissement du lecteur vidéo pour rejouer une séquence,
- Déclencher un scénario identifié par un nom,
- Déclencher une ronde vidéo,
- Déclencher/Arrêter un enregistrement,
- Diffuser un message audio depuis un fichier ou un micro,
- Envoyer un message, email, SMS,
- Ouvrir ou fermer la sortie relais d'un contrôleur,
- Accéder aux caméras en Https.

Le système doit permettre :

- d’adresser des actions natives,
- de configurer des actions « dédiées »,
- d’associer une action à partir d’une liste d’actions,
- de déclencher une action calendaire,
- de déclencher une action programmée,
- de gérer manuellement et automatiquement (via les actions) le mur d’image,
- de déclencher une action à distance sur un autre sous-système dans le cas de raccordement ou d’utilisation multi-sites.

La solution doit permettre à un utilisateur, par une action simple et sous réserve de ses droits, de n’importe quel poste client de :

- Activer / Désactiver un équipement,
- Consulter l’état d’un équipement,
- Créer/Supprimer un équipement,
- Inhiber les alarmes associées à un équipement,
- Ouvrir/Fermer un accès.

Ces actions peuvent être faites directement au niveau cartographique et simplement par l’intermédiaire de menu déroulant.

6. EXPLOITATION DISTANTE

Elle a pour finalité de pouvoir se substituer, à partir d’un site principal, à une gestion locale des systèmes de sûreté locaux de sites secondaires.

Les possibilités d’exploitation distante, par des opérateurs, seront implémentées sur le site principal.

Le site principal sera équipé d'un client léger permettant la gestion distante. Les fonctionnalités seront

différentes de la gestion locale. Les gestionnaires multi-sites du site principal auront la visibilité et les droits d'exploitation de tous les composants des solutions de mise en sûreté de tous les sites distants.

Ce **poste d'exploitation** sera constitué d'un PC et d'un écran 24 " ou supérieur.

6.1. Gestion du contrôle d'accès

La solution de gestion du contrôle d'accès sera hébergée sur le site principal. Les sites secondaires ne comporteront que les UTL qui seront mises à jour par les gestionnaires multi-sites du site principal.

Le système « Multi-sites » doit permettre à l'exploitant du site principal de gérer tous les accès, de tous les sites, afin d'ouvrir ou fermer un accès à distance.

Le système « Multi-sites » doit aussi permettre aux opérateurs locaux d'exécuter en toute autonomie, depuis un poste client, les opérations d'exploitation de la solution pour le périmètre local. Il doit permettre à l'exploitant local de gérer uniquement les accès de son ou ses sites, ainsi que la gestion d'accès communs à plusieurs sites. Certains accès pourront en effet être gérés par plusieurs opérateurs d'exploitation locaux.

La capacité de la solution sera spécifiée dans le document CCTP « descriptif du projet ».

6.2. Gestion du système de vidéo-protection

La solution de gestion du système de vidéo-protection sera hébergée sur le site secondaire. Le site principal ne comportera qu'un affichage des caméras les plus pertinentes à exploiter par les opérateurs d'exploitation multi-sites du site principal.

Le soumissionnaire indiquera dans son offre le nombre de flux et la bande passante nécessaires au bon fonctionnement de sa solution. Celle-ci devra permettre la limitation du flux transmis par chaque caméra, afin de cantonner la bande passante globale à la capacité du réseau de renvoi défini. Celui-ci sera spécifié dans le document CCTP « descriptif du projet ».

Dans le cas du renvoi vers un site équipé d'un mur d'images, selon l'installation et les consignes du service utilisateur du site principal, les flux vidéo seront transmis et interfacés avec la matrice vidéo. Les vues seront ainsi reproduites sur le mur d'images.

Pour assurer cette faculté, chaque flux sera relié sur la matrice par l'intermédiaire :

- soit d'un convertisseur VGA-BNC composite. Un câble coaxial 75 Ohms de liaison sera installé entre le PC et la matrice,

- soit d'un câble HDMI

Les opérateurs disposeront alors de l'interface de la matrice pour afficher les images sur les écrans mis à leur disposition.

La capacité de la solution sera spécifiée dans le document CCTP « descriptif du projet ».

6.3. Gestion de l'intrusion

Les fiches réflexes des actions à mener en cas d'événement détecté sur un site secondaire, seront fournies par l'administration.

Elles seront exploitées par les opérateurs du site principal après réception d'une alarme (vidéo-détection ou renvoi téléphonique d'une détection d'intrusion par le système d'alarme).

Suite au déclenchement d'alarme sur le système distant, le système mis à disposition sur le site principal permettra, entre autres, de :

- établir une levée de doute au moyen des images transmises par les caméras

- acquitter une alarme

- afficher une liste d'actions proposées

- ouvrir/fermer un accès (par exemple, à un personnel venu effectuer une levée de doute physique).

7. EXPLOITATION DISTANTE À PARTIR D'UNE DDSP

Elle a pour finalité de pouvoir se substituer, à partir de la Direction Départementale de la Sécurité Publique (DDSP), site principal, à une gestion locale des systèmes de sûreté locaux de sites distants (Commissariat, Bureau de Police, Préfecture, sous-Préfecture, etc...).

Les possibilités d'exploitation distante, par des opérateurs, seront implémentées sur le site principal.

Les possibilités d'exploitation distante des opérateurs du Centre d'Information et de Commandement (CIC) de la DDSP seront à minima celles décrites aux points suivants.

Le CIC sera équipé d'un client léger. Les fonctionnalités seront différentes de la gestion locale. Les équipements de visualisation seront installés au CIC.

Le **poste d'exploitation** sera constitué d'un PC et d'un écran 24 " ou supérieur.

7.1. Gestion du contrôle d'accès

La solution de gestion du contrôle d'accès sera hébergée sur le site principal. Les sites secondaires ne comporteront que les UTL qui seront mises à jour par les gestionnaires multi-sites du site principal.

Le système « Multi-sites » doit permettre à l'exploitant du site principal de gérer tous les accès, de tous les sites afin d'ouvrir ou fermer un accès à distance.

Le système « Multi-sites » doit aussi permettre aux opérateurs locaux d'exécuter en toute autonomie, depuis un poste client, les opérations d'exploitation de la solution pour le périmètre local. Il doit permettre à l'exploitant local de gérer uniquement les accès de son ou ses sites, ainsi que la gestion d'accès communs à plusieurs sites. Certains accès pourront en effet être gérés par plusieurs opérateurs d'exploitation locaux.

La capacité de la solution sera spécifiée dans le document CCTP « descriptif du projet ».

7.2. Gestion du système de vidéo-protection

La solution de gestion du système de vidéo-protection sera hébergée sur le site secondaire. Le site principal ne comportera qu'un affichage des caméras les plus pertinentes à exploiter par les opérateurs d'exploitation multi-sites du site principal.

Le prestataire indiquera dans son offre le nombre de flux nécessaires au bon fonctionnement de la solution. Celle-ci devra permettre la limitation du flux transmis par chaque caméra, afin de cantonner la bande passante globale à la capacité du réseau de renvoi défini. Celui-ci sera spécifié dans le document CCTP « descriptif du projet ».

Le cas échéant, selon l'installation et les consignes du CIC, le ou les flux vidéo transmis à la DDSP pourront être interfacés avec la matrice vidéo utilisée par le système MCIC (Interfaçage en fonction des caractéristiques du site).

Les images seront reproduites sur le mur d'image au travers de la matrice située dans le local technique.

Pour assurer cette faculté, chaque flux sera relié sur la matrice par l'intermédiaire :

- soit d'un convertisseur VGA-BNC composite. Un câble coaxial 75 Ohms de liaison sera installé entre le PC et la matrice,
- soit d'un câble HDMI.

Les opérateurs disposeront alors de l'interface de la matrice pour afficher les images sur les écrans mis à leur disposition.

7.3. Gestion de l'intrusion

Les fiches réflexes des actions à mener en cas d'événement détecté sur site seront établies avec la DDSP.

Elles seront gérées par le superviseur du CIC DDSP après réception d'une alarme RAMSES.

Le système mis à disposition permettra, entre autres :

- d'établir une levée de doute au moyen des images transmises par les caméras,
- d'acquitter une alarme,
- d'afficher une liste d'actions proposées,
- d'ouvrir ou fermer un accès (par exemple, à un équipage de Police venu effectuer une levée de doute physique).