**PROGRAMME SURETE**

**ANNEXE AU PROGRAMME TECHNIQUE DETAILLE**

(Retours d’expériences d’opérations analogues)

**SOMMAIRE**

Contenu

[1/ GENERALITES 3](#_Toc85472443)

[2/ TYPES DE RISQUES 4](#_Toc85472444)

[2.1/ Risques « extérieurs » 4](#_Toc85472445)

[2.2/ Risques « intérieurs » 4](#_Toc85472446)

[3/ PRECONISATIONS 5](#_Toc85472447)

[3.1/ SURETE PERIPHERIQUE DU BATIMENT 5](#_Toc85472448)

[3.1.1/ Façades sur rue / espaces mitoyens (logements, établissements scolaires, terrains de sport…) 5](#_Toc85472449)

[3.1.2/ Façades sur cour 6](#_Toc85472450)

[3.2/ GESTION DES ACCES PUBLIC / PERSONNEL AUTORISE, ET PIETON / VEHICULE 7](#_Toc85472451)

[3.2.1/ Entrée du public piéton 8](#_Toc85472452)

[3.2.2/ Sortie du public piéton 9](#_Toc85472453)

[3.2.3/ Accès piéton (entrée et sortie) du personnel de la PP 9](#_Toc85472454)

[3.2.4/ Accès des véhicules personnels et de service 9](#_Toc85472455)

[3.3/ COUVERTURE VIDEO 10](#_Toc85472456)

[3.4/ LECTEURS DE BADGES 10](#_Toc85472457)

[3.4.1/ Portes et Menuiseries des locaux / espaces sous contrôle d’accès 10](#_Toc85472458)

[3.4.2/ Portes et Menuiseries des locaux sensibles 11](#_Toc85472459)

[3.4.3/ Contacts sur portes servant au contrôle d’accès 11](#_Toc85472460)

[3.4.4/ Portes d’issues de secours 11](#_Toc85472461)

[3.5/ VISIOPHONIE 11](#_Toc85472462)

[3.6/ APPELS D’URGENCE 12](#_Toc85472463)

[3.7/ TRAITEMENT DES GUICHET / BANQUE D’ACCUEIL 13](#_Toc85472464)

[3.7.1/ Banque d’accueil 13](#_Toc85472465)

[3.7.2/ Guichet d’armurerie 13](#_Toc85472466)

# 1/ GENERALITES

Les objectifs en termes de sûreté impliquent des techniques et corps d’état divers. Si le corps d’état Electricité – Courants faibles prédomine, la cohérence de l’ensemble des corps d’état techniques impliqués doit être pilotée par un spécialiste sûreté à travers le suivi des études (élaboration d’un diagnostic suivi d’une notice sûreté globale du projet) et des travaux.

L’objectif du présent programme de sûreté est donc une conception aboutie incluant l’identification des risques et leurs implications, ainsi que le développement de réponses adaptées et performantes, notamment en termes d’exploitation. La présence de zones spécifiques telles que les garde-à-vue ajoute un facteur de complexité à la gestion des flux, des accès différenciés, entrant parfois en opposition aux règles de sécurité incendie et d’accessibilité PSH.

L’ensemble des contraintes devra donc être mis en cohérence par le pilote sûreté.

Certains corps d’état techniques sont traités dans des référentiels spécifiques ; c’est le cas de la vidéo protection qui est traitée dans l’annexe « VDI Vidéo Radio ».

En cas de contradiction entre les différentes pièces du programme, les plus contraignantes seront prises en compte et la MOE devra interroger la MOA. Les services spécialisés internes à la Préfecture de Police (DILT, DIE/DE, SOPS…) seront consultés pour lever toute ambiguïté.

Il est à noter que, depuis les attentats de 2015 et l’utilisation d’armes de guerre par les terroristes, les besoins sûreté ont évolué par rapport au référentiel « 50/500 » des commissariats de Police. Hormis la nécessité de renforcer les protections balistiques (vitrage pare-balles, sas avec effet de chicane, protection anti-bélier…), une approche plus contextuelle des besoins sûreté de chaque site doit être menée.

Par exemple, le mitraillage d’une façade de commissariat depuis la rue est un risque identifié. Des vitrages pare-balles en partie basse de l’immeuble sur rue sont donc nécessaires, tandis que dans les étages supérieurs, on peut supposer que les balles atteindront le faux plafond en raison de l’angle de tir réduit.

Le présent document constitue donc une base de réflexion à la MOE sans l’exonérer d’une analyse et d’une étude approfondie de la sûreté en adéquation avec son projet architectural et son insertion dans le site.

Praticité d’usage et pérennité devront également guider la MOE dans sa conception. La facilité d’usage des dispositifs de sûreté mis en place permettra de limiter les points de faiblesse dus au facteur humain (négligence, fatigue, habitude…) et par là-même d’éviter des tentatives d’évasion ou des intrusions.

Une vigilance des concepteurs est également requise en termes de cohérence entre les divers types de dispositifs de sûreté mis en place et leur environnement. Par retour d’expérience, on peut citer les exemples suivants :

* Une porte et sa serrure ayant un classement anti-effraction certifié par PV d’essai ne disposent pas automatiquement d’un PV coupe-feu ;
* Une porte anti-effraction sans serrure coordonnée, ou encore intégrée dans une cloison sans degré anti-effraction ne remplit pas son rôle.

Enfin, les concepteurs devront intégrer des types d’équipements ou de logiciels préconisés par la Préfecture de Police ; la cohérence de ces derniers lui permettant un suivi et une maintenance facilités de l’ensemble de ses sites (cylindres de portes, logiciel de gestion du contrôle d’accès, types de caméras de vidéosurveillance…).

# 2/ TYPES DE RISQUES

Les risques « intérieurs » soit à l’échelle du bâtiment, sont distingués des risques « extérieurs » soit à l’échelle du site. Cette liste n’est pas exhaustive mais constitue une amorce à la réflexion des concepteurs.

## 2.1/ Risques « extérieurs »

* Les tirs depuis l’extérieur en direction du commissariat : tirs ciblés depuis l’espace public ou bâtiments avoisinants, ou mitraillage depuis les voies publiques, les éventuels transports en commun aériens surplombant le site...
* Les attaques à la voiture bélier : elles sont particulièrement dévastatrices lorsque les aménagements de voierie permettent aux véhicules d’arriver à pleine vitesse sur les façades. Des plots spécifiques (rétractables lorsque nécessaire) disposés en amont peuvent limiter ce risque.
* Les attaques par charge explosive. En cas de véhicule explosif, un traitement en amont doit également être étudié.
* Le vandalisme (caillassage, projection de peinture…) et les intrusions malveillantes visant le sabotage de la vidéosurveillance, du contrôle d’accès…
* Les rassemblements et manifestions sur la voie publique avec les débordements potentiels que cela suppose.

## 2.2/ Risques « intérieurs »

* Mouvements de foule depuis l’intérieur, évasion de gardés-à-vue : la première étape consiste à bien circonscrire les zones spécifiques au sein du commissariat.
* Vols de documents ou de scellés dans les bureaux des enquêteurs, les salles d’audition, les boxes de plaintes et les locaux dédiés fréquentés par le public, les convoqués, les gardés à vue…
* Vandalisme : cela concerne tous les locaux / espaces fréquentés par le public, convoqués, gardés à vue… restant un instant hors de vue des moyens de surveillance. Il s’agit des espaces d’attente du public, des cellules de garde à vue, du local de visioconférence, des circulations, des sanitaires…
* Détournement ou vol de données informatisées.
* Agression des agents d’accueil et des Policiers dans les locaux de la zone de sûreté, les salles d’audition…

Ce panel de risques, de l’acte de malveillance à l’attaque terroriste, doit être appréhendé de manière globale afin que le bâtiment dispose des moyens passifs (enveloppe, structure, architecture…) et actifs (contrôle d’accès, vidéosurveillance, anti-intrusion, anti-agression…) offrant les dispositions de sûreté et de sécurité optimale à ses fonctionnaires et à ses usagers.

# 3/ PRECONISATIONS

## 3.1/ SURETE PERIPHERIQUE DU BATIMENT

### 3.1.1/ Façades sur rue / espaces mitoyens (logements, établissements scolaires, terrains de sport…)

**Pare-vue diurne :**

Vitrage réfléchissant (25% minimum) sur tous les niveaux si absence de dispositif architectural alternatif.

**Pare-vue nocturne :**

Stores intérieurs (les stores extérieurs devant être relevés par temps forts) si absence de dispositif architectural alternatif.

**Pare-balles :**

Selon norme **EN 1063**.

RDC : niveau de protection des vitrages : **BR6**, soit :

**- BR6 NS SG2 FB6** pour les ensembles vitrés fixes,

**- BR5 NS SG2 FB5** pour les portes.

R+1 : niveau de protection équivalent au RDC sauf si étude de sûreté spécifique au projet architectural confirme l’absence de nécessité selon angles de tirs (balle perdue en faux plafond ?)

A partir du R+2 : sans propriété balistique ni anti-vandalisme (à confirmer selon projet architectural)

Il s’agit de classements minimum.

Les vitrages pare-balles ne devront pas être de teinte ou d’aspect qui les différencieraient des autres vitrages du bâtiment. Leur identification devra être rendue la plus difficile possible pour des raisons évidentes de sécurité. Les types de vitrages tiendront compte des besoins en apport de lumière naturelle.

**Anti-vandalisme et anti-effraction :**

Selon normes **EN 356 (verres) et EN 1627 (menuiseries)**.

Les classements antivandalisme et anti-effraction de l’ensemble des éléments vitrés et menuisés (portes…) en façade extérieure seront au minimum les suivants :

RDC : vitrages classés pare-balles (voir ci-dessus) et grilles de ventilation des sous-sols (le cas échéant) et autres ouvertures potentielles placées en partie basse de la façade => classés résistant à l‘effraction **CR4** (éléments menuisés) et **P6B** (vitrages).

R+1 : vitrages classés pare-balles (voir ci-dessus) => classés résistant à l’effraction **CR3** (éléments menuisés) et **P5A** (vitrages).

A partir du R+2 : néant hormis accès locaux techniques en terrasse.

**Anti-caillassage :**

Protection des vitrages contre les projections de pierres par mise en place de volet roulant métallique, système fixe de grillage, ou tout autre dispositif architectural alternatif.

**Anti-intrusion :**

Mise en place de dispositifs anti-escalade au niveau des éléments verticaux de façade, ornements architecturaux éventuels accessibles depuis la voie publique (type descentes d’eaux pluviales), clôture, portails.

Portes sur alarmes anti-intrusion.

Clôture et portails de 3m de haut, sans possibilité d’escalade.

**Contrôle d’accès :**

En préalable, dissocier les flux suivants :

- entrées et sorties,

- véhicules et piétons,

- public, convoqués, agents de Police et gardés à vue, prestataires extérieurs, personnel technique de la Préfecture de Police, avocats, médecins… (Étant entendu que les convoqués, les prestataires extérieurs, les avocats et médecins utiliseront l’entrée publique, les gardés à vue seront amenés sur site par les agents de Police, et le personnel de la PP empruntera la même entrée que les agents de Police).

Seuls les agents de Police, le personnel technique de la PP et parfois les prestataires extérieurs (après vérification préalable de leur casier et demande justifiée) pourront pénétrer sur site au moyen d’un véhicule. Tous les autres usagers pénètreront dans le commissariat par la voie piétonne.

Des lecteurs de badges seront disposés aux entrées et sorties des agents de Police / personnel PP, qu’ils soient piétons ou véhiculés.

Des visiophones reliés à la banque d’accueil et au poste de Police (potentiellement doublés de caméras), seront disposés à l’entrée publique ainsi qu’à la sortie.

Un dispositif de sas d’entrée (de préférence en chicane) et de sortie du public (de type anti retour) sera mis en œuvre (voir référentiel « Sas type »), avec portique de sécurité et convoyeur à rayons X. Ces sas seront asservis de porte à porte et munis de bouton de fermeture d’urgence et bouton d’alarme. L’ensemble du sas sera pare-balles et anti-effraction.

Un dispositif de sas véhicules sera mis en œuvre à l’entrée / sortie de la cour de service, et ce, également lorsqu’il existe un second accès au site (issue de secours en cas de blocage de l’accès principal).

**Vidéosurveillance :**

Couverture vidéo de l’ensemble des façades, et en particulier des points de pénétration du site, y compris du stationnement Police sur voie publique le cas échéant.

Si nécessaire, étudier la possibilité d’installer des caméras sur du mobilier urbain dans le cadre du PZVP (autorisation à demander à la Ville).

**Portail, rideau métallique :**

Protection contre les émeutes, manifestations ou autre évènement sur voie publique des parties vitrées au RDC par des dispositifs de type portail ou rideau métallique.

### 3.1.2/ Façades sur cour

**Pare-vue diurne :** dito façades sur rue.

**Pare-vue nocturne :** dito façades sur rue.

**Pare-balles :** dito façades sur rue.

**Anti-vandalisme et anti-effraction :**

Selon normes **EN 356 (verres) et EN 1627 (menuiseries)**.

Les classements antivandalisme et anti-effraction de l’ensemble des éléments vitrés et menuisés (portes…) en façade extérieure jusqu’au R+1 inclus seront **CR3** (éléments menuisés) et **P5A** (vitrages).

En cas de disposition architecturale qui offrirait un point de faiblesse au R+2, ces dispositions devraient être étendues également à ce niveau.

**Anti-caillassage :**

Sans objet si façade non atteignable depuis les espaces mitoyens (logements, établissement scolaire, terrain de sport…). La clôture d’une hauteur minimale de 3m (demande de dérogation à prévoir) devra permettre d’éviter ce risque. En cas contraire : dito façades sur rue.

**Anti-intrusion :**

Alarme anti-intrusion à prévoir sur l’ensemble des points d’accès au bâtiment depuis la cour.

Clôture et portails de 3m de haut, sans possibilité d’escalade.

**Contrôle d’accès :**

Lecteurs de badges pour tous les accès agents et personnel technique de la PP.

**Vidéosurveillance :**

Couverture vidéo de toute la cour extérieure, espaces végétalisés et stationnement compris, de tous ses accès périphériques, et de tous les accès au bâtiment (sous-sol compris) depuis cette cour. Prévoir les masques programmés sur les fenêtres privées le cas échéant.

La vidéosurveillance devra détecter une intrusion avec un taux de fausse alerte le plus bas possible.

## 3.2/ GESTION DES ACCES PUBLIC / PERSONNEL AUTORISE, ET PIETON / VEHICULE

Rappel des types de flux à distinguer :

- entrées et sorties,

- véhicules et piétons,

- personnes autorisées ou non à pénétrer librement sur le site (public, convoqués, agents de Police, gardés à vue, prestataires extérieurs, personnel technique de la Préfecture de Police, avocats, médecins…)

Parmi ces usagers, on recense quatre catégories :

* Le personnel autorisé à pénétrer sur site grâce à leur badge : agents de Police, personnel technique de la Préfecture de Police.
* Les personnes autorisées à pénétrer ponctuellement sur site, (sous condition d’avoir formulé une demande en amont, 48h minimum, et d’avoir reçu l’accord des services de Police qui auront vérifié le casier judiciaire des intervenants) : prestataires de maintenance, entreprises de travaux… Un badge « visiteur » pourra leur être remis à l’arrivée sur site.
* Les personnes non autorisées à pénétrer librement sur site : public, convoqués, avocats, médecins… Ces personnes seront accompagnées par un agent de Police, lorsque hors zones accessibles public (après avoir été autorisées à y pénétrer).
* Les gardés à vue. Ces derniers seront accompagnés par les agents de Police lorsque hors cellules.

De cette distinction découle 4 types d’accès :

* **Entrée du public piéton :** directement en façade sur rue, au moyen d’un sas ;
* **Accès du personnel piéton :** de préférence non accessible directement depuis la façade sur rue mais depuis la cour avant de pénétrer dans le bâtiment. Cet accès fonctionne en entrée et en sortie ;
* **Accès des véhicules personnels et de service :** cet accès fonctionne en entrée et en sortie. Un sas est à créer à chaque accès à la cour (comprendre le second accès de secours le cas échéant) ;
* **Sortie du public piéton :** directement en façade sur rue, au moyen d’un sas avec dispositif anti-retour.

L’ensemble de ces accès devra être équipé des dispositifs de sûreté et de sécurité, tout en étant conformes à la réglementation incendie et PSH.

### 3.2.1/ Entrée du public piéton

Se reporter au référentiel « Sas type » pour les schémas d’implantation, mais prévoir en sus l’implantation d’un convoyeur à rayons X (dimensions : 2082(L)x1380(H)x840(l)mm).

**Fonctionnement de jour (scénario à confirmer avec les utilisateurs au cours des études) :**

1. Une personne sonne au visiophone localisé en façade de l’entrée sur rue (l’appel aboutit à la banque d’accueil). Une caméra permettra d’identifier la personne qui demande à entrer.
2. L’agent d’accueil s’entretient avec elle et commande l’ouverture de la 1ère porte du sas.
3. La personne entre, dépose ses affaires dans le convoyeur à rayons X, puis passe le portique de sécurité, sous le contrôle d’un agent de Police présent dans le sas.
4. Une fois le contrôle effectué, l’agent de Police commande l’ouverture de la seconde porte du sas. (La commande d’ouverture doit également être possible depuis la banque d’accueil et depuis le poste de Police.)
5. La personne se dirige vers la banque d’accueil pour être orientée et accompagnée dans les services adéquats.

**Fonctionnement de nuit (scénario à confirmer avec les utilisateurs au cours des études) :**

1. La personne publique sonne au visiophone localisé en façade de l’entrée sur rue ; l’appel aboutit au poste de Police (les agents d’accueil n’étant pas présents de nuit). Une caméra permettra d’identifier la personne qui demande à rentrer (conditions de nuit).
2. Le chef de poste se déplace vers le sas après entretien avec la personne, et pénètre à l’intérieur du sas.
3. Le chef de Poste libère l’ouverture de la 1ère porte du sas (sur rue).
4. La personne entre, dépose ses affaires dans le convoyeur à rayons X, puis passe le portique de sécurité, sous le contrôle du chef de poste.
5. Le chef de poste libère l’ouverture de la seconde porte puis accompagne la personne dans le bâtiment.

### 3.2.2/ Sortie du public piéton

1. La personne publique appuie sur un bouton de commande du sas.
2. Après ouverture de la porte, la personne entre dans le sas.
3. Seulement après fermeture de la 1ère porte du sas, la personne peut commander l’ouverture de la seconde porte puis sortir. (Dispositif anti retour à prévoir).

### 3.2.3/ Accès piéton (entrée et sortie) du personnel de la PP

Le fonctionnement sera le même de jour comme de nuit.

Un lecteur de badges et un visiophone seront disposés en entrée comme en sortie.

Des caméras surveilleront tous les accès et permettront d’identifier les personnes de jour comme de nuit.

### 3.2.4/ Accès des véhicules personnels et de service

Le fonctionnement sera le même de jour comme de nuit.

En amont du portail, seront disposés des plots anti bélier rétractables, un road-blocker ou tout autre dispositif de sécurité devant empêcher une voiture bélier de forcer l’entrée, selon l’étude de sécurité qui aura été élaborée par les concepteurs.

**Fonctionnement en entrée pour un véhicule Police ou PP :**

1. L’agent de Police ouvre le portail au moyen du lecteur de badges disposé en façade / clôture.
2. Après ouverture du portail, le véhicule s’avance dans le sas.
3. Pendant que le portail sur rue se referme, l’agent passe son badge sur le second lecteur de badges.
4. La barrière levante munie d’une jupe se relève tandis que la herse s’abaisse pour laisser passer le véhicule, (ou autre dispositif proposé par les concepteurs). La barrière (ou rideau métallique ou autre selon étude de sûreté) est asservie au portail afin de garantir l’effet de sas.

Ce dispositif de sas fonctionnera en plan Vigipirate. Un mode convoi sera prévu pour les interventions urgentes des Policiers.

**Fonctionnement pour un véhicule prestataire ayant reçu une autorisation préalable :**

1. Le prestataire appelle le chef de poste (à confirmer par les utilisateurs) et se présente via le visiophone.
2. Le chef de poste fait une première vérification de l’immatriculation du véhicule et du prestataire grâce à la caméra de surveillance et envoit un agent de Police vérifier l’identité du prestataire (il récupère sa CNI ou titre de séjour).
3. Une fois ce contrôle réalisé, l’agent de Police fait signe au chef de poste de commander l’ouverture du portail, ou utilise son badge.
4. Le véhicule s’avance dans le sas.
5. Une fois le portail refermé, le chef de poste lance l’ouverture de la barrière levante avec abaissement de la herse (ou du rideau métallique ou autre selon étude de sûreté), ou l’agent de Police utilise son badge.
6. L’agent de Police indique au véhicule une place de stationnement dans la cour ou l’accompagne au parking en sous-sol. Là encore, il utilise son badge pour commander la porte du parking qui est également munie d’un visiophone.

La présence de vidéosurveillance au niveau de tous les accès permettra d’identifier les visages des personnes dans leur véhicule, de jour comme de nuit.

L’éclairage des accès sur détecteur est donc à prévoir, ainsi que le marquage au sol et tout dispositif permettant aux véhicules de se croiser sans encombre (feux, miroirs, signalétique…).

Les concepteurs devront également prévoir un dispositif d’identification des balises RFID fixées sous les véhicules.

## 3.3/ COUVERTURE VIDEO

L’installation de caméras est à prévoir dans (liste non exhaustive):

* Les sas d’entrée et de sortie, piétons et véhicules, du bâtiment et de la cour ;
* Les zones d’accueil, d’attente du public et tous les cheminements qui lui sont accessibles;
* Les zones de livraison ;
* La cour, comprenant les zones végétalisées et les zones de stationnement ;
* Les locaux sensibles tels que la zone de sûreté, les locaux scellés, les armureries…
* Au droit des rampes de parking.

## 3.4/ LECTEURS DE BADGES

L’installation de lecteurs de badges est à prévoir dans (liste non exhaustive):

* Les sas d’entrée et de sortie, piétons et véhicules, du bâtiment et de la cour ;
* Les passages entre les zones accessibles au public et les zones réservées aux agents;
* Les passages entre les zones dédiées au commissariat et les zones dédiées à la CSI ;
* A l’entrée des différents niveaux (lecteurs de badges au niveau des paliers et non pas dans l’ascenseur), voire à l’entrée de certains services comme l’Etat-major, y compris depuis le sous-sol ;
* Les locaux sensibles tels que la zone de sûreté, les locaux scellés, les armureries…,
* Les locaux techniques tels que les locaux serveurs, ACROPOL, poste HT, TGBT, onduleurs, GE, locaux chaufferie/ ventilation / climatisation…

### 3.4.1/ Portes et Menuiseries des locaux / espaces sous contrôle d’accès

Hormis les locaux sensibles, les locaux et zones sous contrôle d’accès seront à équiper de **portes renforcées** comme suit :

* **Bloc-porte** en bois plein et pourvu d’un renforcement par feuille d’acier. Porte conforme au classement anti-effraction Classe de résistance **CR3**, résistante à l’effraction de 5 minutes selon norme EN1627.
* **Serrure électromécanique** avec certification **Label A2P\*,** soit A2P BP1 pour la correspondance avec les assurances. Les gâches électriques seront prohibées.
* En cas de présence d’un oculus, celui-ci sera en **vitrage** sécurisé de la **Classe P5A**, selon la norme EN 356, soit une protection renforcée par vitrage du niveau 1, résistant à 3 impacts d’une bille d’acier (4,11kg) chutant d’une hauteur de 6m et dégageant une énergie d’impact de 240 joules.
* Ancrage de l’huisserie et type de cloisonnement assortis au niveau de protection demandé.

Les concepteurs veilleront à la cohérence technique entre les exigences sûreté et de sécurité incendie. En cas d’incompatibilité des caractéristiques techniques des composants des blocs portes pour assurer ces deux types de contraintes, les concepteurs devront traiter les deux sujets séparément ou devront obtenir des avis de chantier.

### 3.4.2/ Portes et Menuiseries des locaux sensibles

Les locaux sensibles devront être pourvus de **portes blindées métalliques**, comme suit :

* Bloc porte blindé métallique de la **Classe de résistance CR4**, résistance à l’effraction de 10 minutes selon la norme EN 1627.
* **Serrure 3 points motorisée** avec certification **Label A2P\*\***, soit A2P BP2 pour la correspondance avec les assurances.
* En cas de présence d’un oculus, celui-ci aura un **vitrage sécurisé de la Classe P6B** selon la norme EN 356, soit une protection renforcée par vitrage du **niveau 2.**
* Ancrage de l’huisserie et type de cloisonnement assortis au niveau de protection demandé.

Les concepteurs veilleront à la cohérence technique entre les exigences sûreté et de sécurité incendie. En cas d’incompatibilité des caractéristiques techniques des composants des blocs portes pour assurer ces deux types de contraintes, les concepteurs devront traiter les deux sujets séparément ou devront obtenir des avis de chantier.

### 3.4.3/ Contacts sur portes servant au contrôle d’accès

Toutes les portes sous contrôle d’accès et les issues de secours seront munies de contacts de portes permettant de connaître leur état en temps réel (ouverture, fermeture, ouverture anormalement longue…) ; ces contacts peuvent être des contacts de fond de gâche si le fabricant garantit leur pérennité.

Les états de position et les alarmes correspondantes seront reportées sur le superviseur au moyen d’une cartographie des portes et des fenêtres.

Prescription générale concernant le câblage : aucun câble ne devra être apparent. Tout devra cheminer à l’intérieur des portes et / ou des huisseries.

### 3.4.4/ Portes d’issues de secours

Les portes d’issues de secours seront toutes équipées, quelle que soit leur implantation, de dispositifs identiques :

* Verrouillage électrique homologué par serrure multipoints et barre de poussée, asservi au SSI,
* Temporisation de l’ouverture,
* Contact de porte et report des informations de position de porte, état du DAS (verrouillé / déverrouillé), appui de barre, position du pêne et anomalie moteur,
* Détecteurs de présence,
* Caméras de surveillance en entrée et en sortie.

L’ouverture sera déclenchée depuis le poste de garde (demande de dérogation) à joindre à la notice de sécurité).

## 3.5/ VISIOPHONIE

Un système local totalement « cloisonné » sera déployé pour permettre un dialogue et une visualisation depuis les accès en direction du poste de Police, et / ou de la banque d’accueil.

Pour ce faire, chaque accès contrôlé sera équipé d’un visiophone 3 directions traité anti-vandale.

Le câblage sera direct entre les platines et les 3 postes d’exploitation sans aucun lien Lan avec le réseau global de sécurité du site.

L’installation de visiophones est à prévoir dans (liste non exhaustive):

Au droit des accès extérieurs du site :

* Accès piéton public au hall d’accueil,
* Accès piéton du personnel Police au bâtiment (au niveau du portail + bâtiment),
* Accès véhicule du site (au niveau du portail, doublé à l’intérieur du sas véhicule, et à l’entrée du parking en sous-sol), y compris accès de secours,
* Autre selon le projet architectural.

A l’intérieur du bâtiment :

- à l’intérieur du sas public accédant au hall,

- à l’entrée du poste de Police,

- à l’entrée de la zone GAV,

- à l’entrée des armureries,

- à l’entrée de certains services (exemple Etat-major) à affiner avec utilisateurs.

## 3.6/ APPELS D’URGENCE

Des boutons d’appel d’urgence, placés de manière discrète sont à implanter dans les locaux suivants (liste non exhaustive) :

Dans la zone de GAV :

- locaux d’audition,

- local médecin,

- local fouille,

- local avocat,

- local visioconférence,

- dans chaque cellule de garde à vue, y compris l’attente surveillée,

- dans les circulations.

En dehors de la zone de sûreté :

* Dans les sas d’entrée et de sortie,
* Au niveau de la banque d’accueil,
* Dans les bureaux de prise de plaintes,
* Dans le bureau de l’intervenant social,
* Dans les armureries.

Ces boutons seront encastrés avec dispositif anti-vandale et auto-protégé (platine métallique et visserie). Ils seront protégés contre les déclenchements intempestifs (collerettes périphériques par exemple qui empêcheront le déclenchement d’un simple coup).

Les boutons seront en lien avec l’alarme et reportés au poste de Police.

L’implantation devra tenir compte des usages dont certains exigent une implantation discrète (sous face de bureau ou de guichet…)

L’implantation des boutons dans les cellules de GAV devront permettre une maintenance depuis l’extérieur de la cellule soit depuis la gaine technique située entre deux cellules par exemple (voir référentiel GAV).

## 3.7/ TRAITEMENT DES GUICHET / BANQUE D’ACCUEIL

### 3.7.1/ Banque d’accueil

L’accueil du public se fera après contrôle de ce dernier dans le sas d’accès.

La banque d’accueil ne sera donc pas cloisonnée hermétiquement mais appartiendra au volume du hall.

En revanche, les agents devront être sécurisés contre les comportements agressifs potentiels de certains publics. La configuration de la banque, la largeur de plateau et une partie vitrée, l’ensemble demeurant accessible aux PSH, sont des dispositions à étudier par les concepteurs afin de prévenir les tentatives d’agression.

### 3.7.2/ Guichet d’armurerie

Pour la disposition des locaux d’armurerie, les concepteurs se réfèreront au référentiel zone de sûreté.

Pour mémoire, un sas sécurisé donne accès à un Local de Neutralisation des Armes (LNA) et au guichet passe-armes donnant sur le local aux armes.

Ce guichet est en réalité une façade de serrurerie comportant une porte sécurisée avec un dispositif permettant de passer les armes et équipements lourds (gilets pare-balles par exemple) en partie basse, et une partie sur allège permettant le dialogue avec l’armurier, et l’échange des armes de poing.

Ce guichet accueillera un ordinateur sur plan de travail côté armurier, et une tablette avec écran de visualisation fixé au mur côté agent de Police (pour signature électronique de remise de l’arme).

La sécurisation se fait donc au niveau de la porte du sas (porte blindée CR4 avec oculus, visiophone, contrôle d’accès, anti-intrusion et vidéosurveillance), au niveau de l’accès au local aux armes (même dispositif sans visiophone), puis entre le local aux armes et la soute à munitions (même dispositif sans visiophone).

L’enceinte de l’armurerie sera en béton ou parpaing plein de 15cm d’épaisseur.

## 3.8/ ALARME ANTI-INTRUSION

### 3.8.1/ Au niveau du périmètre du bâtiment

La protection périmétrique passive du bâtiment sera assurée par :

* Grilles et autres protections mécaniques sur accès et mitoyenneté avec bâtiments voisins le cas échéant,
* Classement anti-effraction des ouvertures en façades et toitures.

Sujets déjà traités plus haut.

La protection périmétrique active du bâtiment sera assurée par :

* Vidéo protection,
* Lecteurs de badges,

Sujets déjà traités plus haut.

* Et par l’anti intrusion, pour :

. Les locaux donnant sur rue, non barreaudés et non occupés en permanence des RDC et 1er étages

. la toiture, la détection sera assurée au niveau de la clôture de 3 mètres de haut,

. les locaux sensibles (armurerie, scellés, locaux techniques…)

Cohérence et cohésion devront être garanties pour assurer accessibilité des locaux pour leur maintenance.

NB : les contacts et câblages servant à la sûreté devront être auto-protégés et ne devront pas être confondus avec les contacts servant la domotique comme par exemple la coupure de la CVC lors de l’ouverture d’une fenêtre afin de réduire les pertes énergétiques.

### 3.8.2/ Au niveau du périmètre des locaux et zones concernés

Les équipements à prévoir pour les dispositifs d’alarme anti intrusion seront au moins les suivants :

* Contacts d’ouverture des portes et fenêtres, incorporés avec la filerie dans les bâtis,
* Détecteurs volumétriques couvrant tout le local ou toute la zone concernée pour les locaux sensibles,
* Boîtiers de type digicode pour mise en action et programmation,
* Alarme sonore par haut-parleurs dans zones concernées,
* Alarme sonore type buzzer assortis de voyants lumineux et d’une console dans les lcoaux du personnel de garde dont le chef de poste.

Toute la câblerie sera auto-protégée.

Le matériel préconisé par la Préfecture de Police est de type ARITEC, HONEYWELL ou équivalent.

Localisation (liste non exhaustive) :

* Zone de garde à vue,
* Armurerie
* Scellés
* Locaux ACROPOL,
* Locaux serveurs …

Report au chef de poste.