CAHIER DE PRESCRIPTIONS SECURITE

Projets de construction, rénovation et restructuration

5 juin 2018

ASSISTANCE PUBLIQUE HÔPITAUX DE PARIS

CAHIER DE PRESCRIPTIONS SECURITE POUR TOUT PROJET DE CONSTRUCTION, RENOVATION ET RESTRUCTURATION

(Ce cahier ne traite pas de la sécurité incendie)

Ce guide a une vocation évolutive notamment à partir des expériences des sites et des évolutions technologiques.

Il constitue une synthèse des documents traitant de la sécurité des projets de construction, rénovation et restructuration, des retours d'expérience de l'AP-HP et des exigences du plan d'action sécurité de l'AP-HP.

SOMMAIRE

Le présent cahier a vocation à mieux intégrer la sécurité dans **tous** les projets de construction, restructuration et rénovation conformément à la mesure n°6 du plan d'action « sécurité » de l'AP-HP. Le chargé de sécurité localement compétent, comme le conseiller sécurité et défense de l'AP-HP peuvent vous aider dans ce cadre.

L'intégration de la sécurité dès l'origine de tous les projets de construction, restructuration et rénovation est une **source d'économie et d'efficacité**. La sécurité ne doit pas être vue comme une priorité, mais comme un fil rouge.

Propos liminaires

Les prescriptions du présent document sont à prendre en compte impérativement dans tous les projets de construction/rénovation/restructuration de l'AP-HP. Elles constituent des prescriptions fortes. Si des dérogations sont envisagées, elles se feront en lien avec le chef de projet, le chargé de sécurité, les réglementations spécifiques du projet et le contexte local. L'appui du conseiller sécurité et défense de l'AP-HP pourra être apporté.

I – MESURES GENERALES DE SECURITE A L'HOPITAL :

L'introduction récente de la sécurité dans les opérations de construction, d'urbanisme ou d'aménagement s'appuie sur des mesures qui doivent :

- rendre le passage à l'acte plus long et plus difficile (ex : le contrôle d'accès qui interdit le passage aux personnes non autorisées),
- engendrer des situations plus rassurantes et moins risquées (ex : la vidéo protection et la surveillance naturelle des utilisateurs qui peuvent confondre une personne malveillante),
- répondre aux besoins de surveillance qu'exigent le plan Vigipirate (sécurité renforcée – risque attentats) et le plan de sécurité d'établissement (PSE),
- assurer la sécurité des personnes (personnels, usagers, étudiants & prestataires), des biens (mobiliers et immobiliers) et des informations (informatiques ou papiers) en situation normale et en situation de crise (réception d'un grand nombre de victimes dans des délais très courts par exemple).
- utiliser les compétences externes pour améliorer la prise en compte des problématiques de sécurité (par exemple SOPS du cabinet du préfet de police pour les grands projets, SPPAD de la DSPAP, MPC des commissariats pour les autres projets). Faire réaliser une Etude de Sûreté et de Sécurité Publique (ESSP) lorsque celle-ci est prévue par les textes. Cette ESSP sera engagée par le MOA conformément à la réglementation et notamment au Décret n° 2011-324 du 24 mars 2011 relatif aux études de sûreté et de sécurité publique. Les concepteurs devront prendre en compte les résultats de cette étude qui sera soumise lors de la sous-commission pour la sécurité publique. Les remarques de la sous-commission intégrées aux attendus du permis de construire seront analysées et prises en compte par les concepteurs.

II– MESURES GENERALES DE SECURITE D'UN PROJET :

Trois sortes de mesures permettent d'assurer la sécurité :

1. Les mesures bâtimentaires intégrant les préconisations du présent cahier, du SOPS, du SPPAD et des MPC des commissariats : c'est le « bien construire ».
2. Les contrôles d'accès conformes notamment aux prescriptions de l'ANSSI (Agence Nationale de Sécurité des Systèmes d' Information), aux exigences de la DSI de l'AP-HP et, sans restriction, aux badges professionnels de l'AP-HP (CPx) avec différenciation du niveau de sécurité en fonction de la sensibilité des locaux. Ces systèmes doivent être supervisables.
3. La vidéo protection, conforme aux prescriptions de l'ANSSI, de la CNIL et de l'AP-HP, en privilégiant les caméras numériques fixes, haute définition, grand-angle, compatibles avec les logiciels d'analyse intelligente d'images et interconnectable avec les systèmes de l'AP-HP. Elle doit être supervisable et interconnectable. Le flux vidéo en sortie de caméra ainsi que les enregistrements sur serveurs ne doivent pas être en format propriétaire.

Les mesures de sécurité sont déterminées sur la base de l'analyse des flux des personnes, des biens et des informations pour sécuriser les espaces. Les équipements de sécurité devront ainsi être adaptés au niveau de sécurité nécessaire (organe central type cœur de réseau…), à la fréquence d'utilisation (nombreux passages…) et à la particularité du flux (matières dangereuses, fluides médicaux, etc.).

L'établissement/l'espace sera plus généralement organisé à partir des méthodes de prévention situationnelles tout en respectant le projet de soin.

La fréquentation des espaces, le changement de type d'usager, déterminent les positionnements des points de contrôle d'accès : séparation contrôlée des espaces intérieurs et extérieurs, séparation des espaces accessibles librement au public, des espaces à public restreint, des espaces réservés aux personnels, des espaces réservés à certains personnels, des espaces exceptionnellement accessibles (zones SAIV, locaux techniques sensibles…). Pour chaque point sur contrôle d'accès, on doit s'interroger sur la nécessité de mise en place d'un dispositif de visiophonie.

Le site doit être conçu de telle manière qu'il puisse fonctionner fermé. C'est-à-dire qu'en cas de crise interne ou externe, le site doit être en mesure d'exercer ses activités essentielles en mettant en œuvre des mesures de sécurité strictes et individuelles. En cas de crise majeure, le bâtiment doit permettre de renforcer le contrôle des accès et la sécurité de l'établissement, de renforcer le dispositif opérationnel de veille, d'orienter le champ d'investigation vers les agents susceptibles de constituer une menace, de garantir le fonctionnement des chaînes de production et de distribution des produits de santé essentiels ou concernés par la menace.

Au-delà des obligations réglementaires, il s'agit de protéger les ouvrages contre la dégradation volontaire, le vol des biens du site (notamment les matières les plus sensibles), le vol des biens des personnels et des usagers ainsi que la protection des personnes contre les actes de malveillance de tout type ; notamment par le choix judicieux des matériaux et matériels et par la limitation des accès et la surveillance.

Les prescriptions du présent guide conduisent à favoriser la conception d'un site entièrement clôturé et dont les bâtiments sont construits à l'intérieur de l'espace ainsi délimité, sans contact direct avec la voie publique. Cela permet de réduire strictement le nombre des accès, de maîtriser et contrôler les flux et de réduire les frais de fonctionnement tout en facilitant les flux internes.

III - ANALYSE DU PROJET AU REGARD DES RISQUES DE SECURITE :

Faire l'analyse de ces risques permettra d'une part d'identifier les vecteurs malveillants, issus de l'environnement, susceptibles d'impacter le futur établissement ou projet d'aménagement et, d'autre part, de prendre en compte les risques générés par le futur projet.

Elle ciblera également les problématiques de sûreté en rapport avec l'intervention des services d'ordre ou d'urgence.

Enfin, les vulnérabilités du site, identifiées par espace, pourront être collectées.

A - Analyse des risques malveillants :

- L'analyse doit prendre en compte l'ensemble du panel des risques susceptibles d'impacter le projet de construction ou d'aménagement, qui sont liés à l'environnement même du site et qui donc préexistent à l'implantation du projet.

- Elle doit également mettre en évidence les infractions qui risquent d'impacter la zone en raison de la création du projet ainsi que les risques qui découlent de son architecture, de son activité, ceux qui sont susceptibles d'être générés par son mode de fonctionnement, par ses horaires d'ouverture, ceux qui sont liés au public reçu ou à la concentration de personnes en un même lieu.

- Elle doit envisager l'arrivée ou le départ (tardif) isolé de nuit d'un (ou d'une) employé(e). Cela permet bien souvent d'identifier un certain nombre de risques et de vulnérabilités auxquels des réponses devront être apportées.

- L'échelle des risques à retenir doit couvrir les faits mineurs, mais particulièrement gênants que représentent les incivilités (tags, regroupement habituel de personnes, détournement d'espaces...), jusqu'aux infractions les plus graves (infractions contre les biens et celles contre les personnes jusqu'à l'action terroriste).

- Il s'agit bien d'analyser les faits de délinquance et d'incivilités et non d'en dresser une liste, ou d'en fournir les statistiques. Il convient donc de bien mettre en évidence les risques qui pourraient impacter l'établissement ou la zone afin de pouvoir déterminer l'importance des mesures de protection à adopter.

B - Analyse des risques relevant de l'ordre public :

Il convient également de prendre en compte les risques liés à la gestion de l'ordre public qui peuvent être modifiés sur la zone du fait de la réalisation du projet (en se basant sur la situation actuelle ainsi que sur la situation future après réalisation). De façon plus générale, il importe d'évoquer toutes les difficultés d'intervention que pourraient rencontrer les services de secours ou d'urgence.

Ex. : manifestations, problématique du stationnement, lieux accidentogènes, absence d'itinéraire de délestage, embarras de la circulation, occupation de l'espace public, éventuelles difficultés à mettre en place un service d'ordre, etc.

C - Les vulnérabilités du site :

Les items listés infra n'ont pas vocation à être limitatifs, mais plutôt à illustrer cette partie avec des aspects concrets. Pour permettre de faire le lien avec les recommandations, les items sont classés par espace :

- **l'espace périphérique**
  - S'assurer que la configuration de la voirie ne fait pas obstacle aux forces de sécurité intérieure : accessibilité insuffisante des véhicules d'intervention, difficulté pour manœuvrer, pas de vue sur certaines façades depuis la voie publique,
  - L'éclairage doit être suffisant et vérifié régulièrement,
  - Optimiser les conditions de desserte en transport en commun et cheminement pour se rendre aux stations ou arrêts,
  - Les espaces doivent être bien conçus puis entretenus régulièrement (végétation exubérante par exemple) afin de ne pas générer de problème de sécurité,
  - La signalétique doit être suffisante, claire et ne pas faire l'objet d'une mauvaise compréhension du statut des espaces (publics, privés),
  - Tous les lieux sensibles en périphérie doivent être identifiés (usine Seveso, lieu de culte, école…).

- **l'espace périmétrique**
  - S'assurer que la clôture est homogène, que la protection mécanique des ouvrants et façades est adaptée et/ou égale en termes de résistance à l'intrusion ou à l'effraction,
  - Identifier les espaces sous structure, aisément accessibles, pouvant faciliter les détournements d'espaces (espace masqué occupé illicitement…),
  - Repérer et protéger les points hauts qui pourraient favoriser les jets de projectiles, les repérages, l'affichage de revendications,
  - Identifier et gérer les issues ne permettant pas une bonne visualisation des arrivants et rendant difficile toute anticipation d'un envahissement,
  - Organiser les flux d'entrées et de sorties, des personnels et du public, en évitant les mixités afin de réduire leur perméabilité entre eux et facilité leur maîtrise,

- Durcir la sécurité des abords les plus sensibles (exposition de stockage de matières dangereuses…) contre les agressions les plus importantes (véhicules béliers par exemple),
- Identifier les configurations accidentogènes susceptibles d'être détournées de leur usage (accessibilité sur des terrasses – détournement d'installations extérieures pour des sports à risques type sport de glisse dans des volées d'escaliers - grandes lignes droites sans dispositif limitant la vitesse), afin d'en supprimer ou limiter les risques
- Protéger les piliers porteurs de la structure pouvant faire l'objet d'une attaque terroriste (par limitation d'accès ou de stationnement par exemple),
- Recenser les lieux nécessitant l'installation ou le renforcement de la vidéoprotection,

- **les volumes intérieurs**

Il s'agit d'identifier tous les lieux qui fragilisent la sécurité et d'y remédier par des mesures adaptées, par exemple :

- Absence de détermination des espaces différenciés et de contrôle d'accès,
- Insuffisance d'implantation de la vidéo protection,
- Mauvaise implantation du PCS,
- Organisation des entités sans logique induisant un croisement de flux,
- Implantation rendant les prises d'air neuf trop accessibles,
- Etc.

Les mesures envisagées doivent non seulement permettre de prévenir et de réduire les risques identifiés, mais elles doivent aussi faciliter les missions des forces de l'ordre et des secours (Art. R 114-2 3° b du code de l'urbanisme).

IV - CONTROLE DES ACCES :

Lorsqu'un dispositif de contrôle d'accès est mis en place, son usage ne doit pas pouvoir être contourné. Ainsi, si un système d'accès par tourniquet ou porte à effacement est prévu, il doit être suffisamment haut pour ne pas être enjambé, suffisamment large pour ne pas être contourné et descendre jusqu'au sol afin de ne pas être franchi par dessous.

A - De l'espace périphérique

Le site est conçu fermé avec une enceinte périphérique. Il est strictement isolé des autres entités juridiques.

- Gérer les flux de circulation et de stationnement induits par le site, liaison parking intérieur et voie publique : estimer, analyser et prévoir des mesures, par exemple :
  - Pour les piétons : il est possible de protéger les abords en surélevant les trottoirs… ;
  - Contre les véhicules lancés (véhicules béliers) : mettre en place une protection ex : emmarchement - bornes, jardinières ou mobilier urbain d'un niveau de résistance adapté (voir aussi norme européenne NF CEN TR 14383-8). Les obstacles (bornes…) télescopiques sont bien plus résistants que les barrières et peuvent stopper un véhicule lancé. En revanche, elles peuvent être parfois contournées par les deux roues (ou par des manifestants), elles sont dans ce cas complétées par une barrière classique et une grille ou tout autre dispositif d'entrave de l'ensemble de la voie. La densité et le type de flux déterminent les matériels à déployer. Par exemple, pour des raisons de maintenance, un obstacle escamotable ne pourra être activé qu'en cas de rupture d'une barrière ou sur déclenchement manuel. La nature de l'entrée et des flux prévus déterminent les choix en fonction des risques encourus ;
  - Le type de végétation en périphérie du site doit être déterminé ainsi que l'entretien qui en est ou qui en sera réalisé. De même, il faut s'assurer qu'il n'y a pas de masque végétal et que la surveillance naturelle du site est satisfaisante ;
  - Si besoin l'éclairage public sera amélioré pour obtenir un éclairage compatible avec les impératifs de sûreté.
- Prendre en compte les cheminements depuis les transports en commun : estimation, analyse – mesures envisagées.

- La hauteur de l'enceinte périphérique doit mesurer au minimum 3m00 dans un but d'antifranchissement (recommandation de la préfecture de police). Si le PLU ne permet pas de retenir la hauteur souhaitée, l'enceinte doit avoir la hauteur maximale autorisée par le PLU. Toutefois, il est recommandé de solliciter une dérogation au PLU afin d'obtenir une enceinte d'une hauteur homogène de 3m00. Aucun mobilier urbain implanté ne doit faciliter l'escalade (par exemple : compteurs électriques, bancs publics, etc.). La hauteur sera adaptée au risque et au besoin surélevé ponctuellement.

B - De l'espace périmétrique

De manière générale, toutes les entrées sur le périmètre sont contrôlées : par agent ou badge CPx, ouvertures contrôlées à distance et caméras. Il convient de maintenir fermés les accès surnuméraires ou dont on ne peut pas assurer la surveillance et *a fortiori* le contrôle. Toutefois, leur condamnation définitive ne doit être envisagée qu'avec prudence et après appréciation de leur utilité en cas de catastrophe importante ou nécessitée d'évacuation d'urgence.

- Différencier et gérer les flux : estimation, analyse – mesures envisagées :

    - Différencier les flux :

    - Le nombre de points d'entrées/sorties du site est restreint aux stricts besoins ;
    - Les flux entrées/sorties, piétons/véhicules, personnels/visiteurs doivent être différenciés ;
    - Les flux de livraisons sont distingués des flux de visiteurs et des flux des personnels ;
    - Les accès sont configurés en fonction des véhicules et du type de protection envisagée ;
    - Les accès livraisons doivent être conçus pour faciliter l'application des différentes législations des matières livrées (matières dangereuses…) et permettre l'application des procédures de l'AP-HP ;
    - La gestion des accès en cas de situation dégradée doit être prévue ainsi que les mesures de protection contre les menaces imminentes d'envahissement (fermeture rapide des accès). Notamment, les points d'accueil et de sécurité seront dotés d'un bouton d'urgence de fermeture des accès qu'ils accueillent
    - Eventuellement, mettre en œuvre une procédure « VIP » (accueil – cheminement dédié - réservation stationnement) ;
    - La circulation de certaines catégories de patients (dispositif anti-enlèvement de nourrissons, système anti-errance des personnes désorientées…) est sécurisée ;
    - Certaines zones de soins seront limitées aux seuls patients et soignants ;
    - Des circuits spécifiques d'accueil et de sécurisation des détenus, des transports de fonds, de certaines matières dangereuses, etc. doivent être prévus ;

- Les conditions de circulation sur la zone sont définies : voie traversante, circulation périphérique uniquement, sens de circulation, largeur des voies, leur statut (public ou privé)…. Privilégier les sens uniques de circulation ;
- Des voiries spécifiques pour les circulations douces sont créées, complètement séparées ou placées à côté des voies véhicules – avec séparatif ;
- La zone aux dispositifs de transports en commun est prise en compte, y compris pour les véhicules de transport de fonds, de livraisons et les deux roues. Anticiper les besoins et les dimensionnements ;
- La circulation des déchets et des entreprises extérieures (éventuellement une zone de stationnement dédiée), MADA (Matières Dangereuses), pompes funèbres, est prévue ;
- Les conditions d'accessibilité des secours et d'évacuation ainsi que les dépose-minute sont définis ;
- Il convient de ne pas opposer les espaces piétonniers à l'accessibilité des secours (gestion de bornes et barrières à anticiper) ;
- Des dispositifs (visuels, infrastructures…) doivent permettre de maîtriser la vitesse des véhicules ;
- Le contrôle d'accès des véhicules est dimensionné afin de limiter les risques d'embouteillage sur la voie publique. Les dispositifs d'accès piéton devront également être adaptés afin de ne pas générer de regroupement sur la voie publique. Prévoir un itinéraire d'échappement pour les véhicules engagés, mais non autorisés à rentrer ;
- Le cas des taxis et des véhicules de transport sanitaire hors urgences doit faire l'objet d'un traitement particulier (système de gestion des places de stationnement et de dépose avec temporisation…). La menace constituée par ces véhicules, souvent nombreux et de gabarit important, ne doit pas être sous-estimée, car ils peuvent s'approcher au plus près d'installations critiques. Contrôler leurs mouvements participe aussi à la sécurisation globale du site ;

    - Gérer les flux :

- Les accès sont contrôlés. L'emplacement et le raccordement de portiques détecteurs sont prévus pour les accès publics périmétriques afin de pouvoir les installer sans travaux supplémentaires en cas de besoin ;
- Les effets transportés sont contrôlés :
    - ouverture des sacs. L'emplacement et le raccordement de tunnels radioscopiques doivent être prévus pour les accès publics afin de pouvoir les installer sans travaux supplémentaires en cas de besoin ;
    - les personnels d'accueil doivent être en mesure de demander aux visiteurs la production d'une pièce d'identité et de la conserver, ainsi que de distribuer un badge d'accès ;
- Le contenu des véhicules peut être contrôlé visuellement (coffres, intérieur des véhicules, etc.). La configuration de l'accès doit le permettre ;
- Eventuellement, selon la sensibilité, un contrôle radioscopique des plis et colis, détection d'explosif peut être prévu. Si ce choix n'est pas retenu, le circuit courrier et les locaux recevant les courriers et colis doivent être conçus afin de recevoir les appareils de contrôle sans nécessité de travaux d'adaptation des locaux ;

A prévoir des équipements mobiles de Protection du travail isolé (PTI) pour les agents de sécurité et d'intervention ainsi que des moyens de liaison adaptés.

- Envisager dans la conception d'éventuels mouvements de foule (particulièrement sur des espaces sensibles en terme de sécurité comme des passerelles, les passages sur des points hauts...). Les points hauts (passerelle, escalier en cage ouverte…) seront évités. Sinon ils seront sécurisés afin qu'aucune personne ne puisse chuter ni se jeter volontairement dans le vide. Ainsi, les cages d'escalier ne seront pas vides en partie centrale ;
- Les issues de secours sont contrôlées : protection - placement sous UGCIS (unité de gestion centralisée des issues de secours) avec vidéoprotection ;
- Les conditions de stationnement sont définis (autorisé sur les voies ou seulement dans les parkings), type de parking (aérien, souterrain), nombre de places de stationnement souhaité. Le contrôle d'accès par badge CPx est prévu pour les parkings réservés. Les emplacements non autorisés seront physiquement conçus pour empêcher le stationnement irrégulier (surélévation des trottoirs…) et la circulation ;

    - Points de vigilance pour ne pas faire obstacle aux flux :

- La hauteur, le positionnement et la densité de la végétation ne devront pas nuire à la visibilité ni à la diffusion de la luminosité ou à l'éventuelle couverture de la vidéoprotection. Il est recommandé de limiter la hauteur des arbustes et des bosquets à une hauteur maximale de 80 cm afin d'offrir un maximum de visibilité. Dans le même ordre d'idées, les arbres devront être élagués et présenter un tronc lisse sur une hauteur de 2 mètres.
- Un éclairage adapté à la sûreté (en termes de résistance et de luminosité) devra être mis en place sur l'ensemble des voies et cheminements, une luminosité homogène minimum devra être assurée conformément aux textes et normes en vigueur ;
- Sur l'ensemble des sites, il conviendra de se conformer *a minima* au niveau d'éclairement réglementaire en vigueur, notamment concernant la circulation des personnes en situation de handicap (PSH) ;
- De plus, pour éviter les zones d'ombre, l'espacement des points d'éclairage doit être régulier (maximum 25 mètres). L'éclairage doit produire une puissance minimale au sol de 22 lux (recommandation formulée par l'Association Française de l'Eclairage (A.F.E.) – celle-ci sera adaptée à la législation en vigueur et aux particularités des zones ;
- Les façades des bâtiments situés au droit des voies publiques seront alignées et jointives pour éviter les recoins propices aux délinquants.

Le système de filtrage différenciera les accès piétons et conducteurs de véhicules dotés d'un badge professionnel de ceux non dotés ; aussi bien en entrées qu'en sorties. Les entrées véhicules et piétons sont automatisées pour les détenteurs d'un badge CPx, mais elles ne doivent permettre l'accès que d'un véhicule ou d'un piéton à la fois. Dans ces conditions, ces accès sécurisés dédiés aux personnels peuvent être multipliés autour du site afin de permettre un meilleur fonctionnement du site. Les personnes et véhicules non dotés d'un badge professionnel, accèdent par un minimum d'ouvertures sécurisées par des agents. Chaque entrée automatisée doit

être couverte par une caméra de vidéoprotection permettant en toute circonstance d'identifier un individu et son véhicule. Si un dispositif LAPI (lecture automatique de plaque d'immatriculation) est envisagé, il ne pourra servir que pour la gestion du parking ou en faciliter sa sortie (et non pour du contrôle d'accès) ; il ne constitue pas un dispositif de sécurité (une simple copie de plaque permet un accès).

- La détection et les accès :

Les ouvrants contrôlant des zones non ouvertes au public (espace administratif, services d'hospitalisation en dehors des heures de visites, les issues de secours, etc.), seront équipés de contacteurs permettant de connaître leur position ainsi que leur état (ouvert, fermé, forcé). Des systèmes couplant les fonctions de sécurité incendie et de sécurité existent sur le marché pour éviter toute incompatibilité et répondre aux exigences des services d'incendie et de secours. Les ouvrants seront contrôlés par des lecteurs de badges.

Les portes installées dans les lieux de passages professionnels (circulation des brancards, matériels…) pourront être équipées de portiques de détection RFID qui permettront leur ouverture automatique. L'implantation des portiques devra être disposée (en amont) en prenant en compte au minimum la longueur d'un brancard ou d'un lit et la vitesse d'arrivée du flux.

Le déploiement des portiques de détections aux accès des services ou des secteurs communs d'activités pourra déceler la sortie de matériels onéreux ou imposants (endoscope, informatique...) qui auront été préalablement « pucés » (technologie RFID de type antivol par exemple). Une alerte sera renvoyée au PC sécurité avec ou non le déclenchement d'une alarme sonore ou lumineuse localement. Le dispositif pourra éventuellement permettre de faire un inventaire instantané du matériel présent dans une zone et la gestion de la vie de l'appareil (contrôle technique, entretien…). Il est possible d'utiliser le dispositif de sonorisation du site afin d'émettre un message de rappel au cas où une personne sortirait avec du matériel sans autorisation. En dernier recours, des portiques pourront être implantés au niveau des sorties du site et les agents de sécurité pourraient être dotés de détecteurs RFID volumétrique.

ATTENTION : il est recommandé qu'au sein d'un même site (idéalement d'un même GH), tous les systèmes de sécurité soient gérés par un même et unique logiciel de gestion. En cas de rénovation partielle, l'unification des systèmes devra être prévue.

Tous les systèmes de portes formant sas doivent fonctionner en mode libre, mode sas et mode fermé. Des commandes sont prévues depuis le poste d'accueil immédiatement concerné et depuis le PC sécurité.

Les conditions de travail des agents en entrée doivent être prises en compte. Les contrôles d'accès se faisant depuis la voie publique, ces points doivent être conçus sécurisés et conformes aux exigences du droit du travail.

Certains accès périmétriques peuvent être automatisés notamment afin de réduire les frais de gardiennage ou de faciliter les flux du personnel. Ces accès sont alors conçus afin de ne pas pouvoir être utilisés par d'autres personnes :

- installation de tourniquets pleine hauteur (le nombre est adapté au flux),

- passage sécurisé d'une personne à la fois,
- le contrôle d'accès doit être par badge CPx en entrée comme en sortie (pas de sortie libre). Une personne non badgée ne doit pas sortir par ce lieu,
- le lieu doit disposer d'au moins une caméra permettant d'identifier les personnes utilisatrices en entrée comme en sortie,
- cette caméra doit être accompagnée d'un micro pour détecter une anomalie sonore comme des coups, des hurlements, une détonation ou une explosion (avec image pop-up apparaissant automatiquement au PC sécurité),
- le système doit pouvoir être verrouillé depuis le PC sécurité,
- il ne doit pas être déverrouillable (pas de mode libre),
- il doit être en sécurité positive (si coupure de courant, le système est verrouillé) et donc ne pas constituer une issue de secours,
- il peut être ajouté un écran de contrôle à l'intérieur des locaux des principaux utilisateurs (CRRA SAMU par exemple) afin d'accentuer le contrôle du flux).

Les personnels doivent accéder par une entrée automatisée afin de soulager les contrôles effectués par les agents de sécurité sur les entrées prévues pour les personnes non badgées. Elles peuvent être situées à proximité les unes des autres.

Contrôle d'accès

Le système doit être de type IP.

Les lecteurs de badges sont de type de proximité (mains libres), et installés en pose murale (sauf exception explicitées ci-après).

En complément pour certaines zones les plus sensibles, il doit être installé des lecteurs biométriques.

Les ascenseurs, monte-malades et monte-charge sont tous sous badge avec programmation possible pour chaque étage et fonction (libre ou sous contrôle d'accès).

Les accès sont classés selon trois niveaux de sécurité :

- **Niveau 1** (portes nécessitant un filtrage des accès) :

  Serrures électromécaniques à béquille contrôlée sur badge.

  Les serrures à axe et entraxe au standard français donnent l'information sur l'état (ouverte/ fermée) de la porte et l'état du verrouillage de la porte. Tout produit type gâche est proscrit.

- **Niveau 2** (portes à sécuriser ou à fort trafic) :

  Serrures reliées de manière filaire au système de contrôle d'accès centralisé. Signalisation des anomalies de fonctionnement par renvoi vers la centrale d'alarme intrusion. Alarme sonore au PCS si porte ouverte.

  Les serrures à axe et entraxe au standard français donnent l'information sur l'état (ouverte/ fermée) de la porte et l'état du verrouillage de la porte. Tout produit type gâche est proscrit.

- **Niveau 3** (portes pour locaux sensibles type pharmacie, stupéfiants...) :

  Pour les locaux sensibles la serrure avec demi-tour est de type 3 ou 5 points selon les risques à protéger. Le montage est de type applique motorisée avec double détection de fermeture par capteur magnétique et/ou infrarouge.

  Fonction demi-tour anti-rebond. Signalisation des anomalies de fonctionnement par renvoi vers la centrale d'alarme intrusion. Alarme sonore au PCS si porte ouverte.

  Les issues de secours donnant sur l'extérieur et les locaux à risques importants doivent disposer de barre antipanique électromécanique contrôlée, modèle DAS avec fonction « dogging », permettant l'installation de contrôle d'accès. Elles sont sous UGCIS. Les barres antipaniques à pression seront privilégiées par rapport aux barres à basculement, plus fragile à l'effraction.

Les autres issues de secours contrôlées en sortie disposent :

- d'organe de verrouillage en partie haute de porte avec voyant lumineux d'état verrouillé/déverrouillé (conformes à la norme NFS 61937 fiche XIV),
- de boîtier de décondamnation (couleur verte) ou autre dispositif conforme à la réglementation (DAS), et sont également asservies à la détection incendie.

  Une porte ouverte provoquera une alarme sonore au PC Sécurité et le déclenchement de la vidéosurveillance la plus proche (affichage de l'écran vidéo en pop-up). Les portes sous UGCIS doivent être équipées de la même manière.

  Tous les accès peuvent être programmés individuellement suivant les programmes horaires. Les autres accès possèdent des sorties libres par bouton poussoir.

  Les UTL (unité de traitement local) sont toujours installées en local technique LT-SR ou en gaines techniques courants faibles. L'installation est conforme aux recommandations de l'ANSSI.

  La totalité de l'installation est secourue et alimentée par le réseau HQ (serrures, UGCIS, UTL,…).

  Le serveur est redondant, installé en salle informatique générale et équipé de logiciels d'exploitation, de paramétrage.

  Le poste d'exploitation (écran de supervision) sera installé au PC Sûreté.

Alarme intrusion

Certains services et locaux cités dans les fiches de spécifications techniques du PTD doivent être dotés d'une alarme intrusion.

La supervision des alarmes est centralisée au PC Sûreté, serveurs redondants en zone protégée.

Des plans de localisation seront prévus sur écran avec icônes actives des points d'alarme.

Le système d'alarme intrusion qui sera proposé doit être interfacé au réseau IP, et aussi interfacé avec le contrôle d'accès. Chaque zone surveillée doit être dotée d'un ou plusieurs lecteurs de badges ou/et claviers M/A permettant l'activation ou la désactivation d'une zone sous surveillance.

La gestion de chaque point de détection (et zones) doit être réalisée à partir du PCS selon programme horaire et commande manuelle de mise en/hors service manuelle.

Les alarmes intrusions enclenchent un enregistrement des caméras de vidéosurveillance concernées de bonne qualité pour exploitation. L'enregistrement débute (1 minute avant l'évènement).

PM : Les services et locaux sous surveillance intrusion implique un contrôle d'accès par lecteur de badges sur les accès.

Les contacts anti-intrusion sont encastrés.

Les détecteurs volumétriques utilisent la bande K, éloignée des bandes radio utilisées par le WiFi.

Les dispositifs anti intrusion devront être précisés dans les fiches de spécifications techniques.

Sont sous surveillance particulière les locaux suivants (liste non exhaustive) :

- la pharmacie (détection volumétrique et périmétrique),
- le service mortuaire,
- les services ambulatoires qui sont non utilisés le week-end ou la nuit (détection périmétrique),
- les services contenant des appareils médicaux (détection périmétrique),
- les ouvrants et portes des niveaux accessibles (détection périmétrique),
- les locaux informatiques (LT-SR, cœurs, salles informatiques) (détection volumétrique et périmétrique),
- les magasins principaux (détection volumétrique et périmétrique),
- les locaux NRBC,
- les locaux contenant des appareils de maintenance technique,
- les locaux de la maintenance biomédicale,
- les locaux accessibles depuis l'extérieur des zones non contrôlées et fermées la nuit (détection volumétrique et périmétrique),
- Tous les locaux techniques sensibles (locaux électriques, locaux groupe, chaufferie, locaux eaux,….)
- Le cas échéant, toutes les galeries techniques donnant sur l'extérieur de la parcelle.

Appel d'alerte – Appel à l'aide

Cette installation est à considérer comme un sous-système de l'alarme anti intrusion.

Certains services doivent être équipés de bouton d'appel à l'aide à installer sous les banques d'accueil, type bouton-poussoir ou appel au pied (via la centrale intrusion) avec renvoi d'appel sur le PC Sécurité, il s'agit :

- des postes d'accueil,
- des postes des admissions,
- les box des urgences.

Ce système est couplé à la vidéoprotection.

V - MESURES BATIMENTAIRES :

Pour toute construction, la hauteur maximum et /ou la longueur des bâtiments envisagés, l'écartement minimum des bâtiments entre eux en fonction de la configuration géographique seront définis.

Dans tous les cas, les caractéristiques et niveaux de résistance des matériaux de construction employés sont définis.

A- Les ouvrants – les façades :

Les rideaux métalliques (hauteur, nature…), la résistance des ouvrants (qualité des serrures - ouvrants - produits verriers) doivent respecter les normes en vigueur.

Les ouvrants doivent être suffisamment durcis pour pouvoir contenir une foule régulée qui a subi un évènement grave.

Les portails, portillons, lisses, doivent être d'un niveau de résistance suffisant et l'ouverture doit être adaptée à la nature des lieux, au moment de la journée et à la fréquentation.

L'accès aux façades doit être protégé des personnes malveillantes. Eviter les passerelles et autres structures métalliques accessibles ; si elles existent, il convient de les sécuriser. Par exemple, les colonnes d'eau descendantes extérieures doivent être sécurisées afin de ne pas permettre leur escalade (ceint de piques par exemple).

L'accès aux bâtiments doit être impossible depuis les fenêtres du rez-de-chaussée et du premier étage (barreaudage, blocage des fenêtres hors activité…).

Les ouvrants doivent être conçus pour rendre impossible la défenestration et disposeront d'une serrure ou d'un système d'entrebâillement antichute non facilement démontable. Il n'y aura pas d'ouvrant dans les secteurs suivants (sauf contraintes réglementaires) : interventionnel, soins critiques, urgences, imagerie et médecine nucléaire, plateau de biologie, logistique médicale, logistique hôtelière, stérilisation, etc..

Les terrasses accessibles aux personnels (hors personnels d'entretien-maintenance), voire au public : le cas échéant, les terrasses contiguës à la cafétéria, au self du personnel, aux soins critiques et aux blocs opératoires (pour la détente du personnel), etc., doivent être sécurisées par des dispositifs fixes (protections physiques en périphérie) afin qu'une personne ne puisse ni chuter si se projeter dans le vide. Elles doivent être strictement limitées.

Il est indispensable de rendre sûres les toitures autorisées (terrasse ou en pente).

Il est nécessaire de verrouiller les accès inutiles tout en maintenant les issues de secours fonctionnelles. Des dispositifs permettent de centraliser au PC de sécurité l'ouverture de tout ou partie des issues de secours (unités de gestion des issues de secours – UGIS). La relative fragilité de ces dispositifs doit conduire à prévoir leur maintenance dès le départ.

Des « zones fumeurs » devront être prévues, clairement identifiées et accessibles, y compris la nuit, afin que les issues de secours ne soient pas utilisées à cette fin et maintenues ouvertes (il en va de même des accès verrouillés la nuit qui restent dans les faits ouverts « à la crémone »…).

D'une manière générale, qu'il s'agisse d'accès de secours maintenus ouverts ou de l'utilisation d'accès réservés comme « raccourcis », les détournements d'usage doivent être strictement interdits.

B - Les portes et issues de secours :

Les portes d'issues de secours au niveau extérieur doivent être de qualité suffisante pour résister à une tentative d'effraction importante et équipées de systèmes de temporisation d'ouverture de type UGIS, de détection d'effraction et de position. Les issues de secours doivent aboutir à l'intérieur du site.

Les issues de secours donnant sur l'extérieur ne devront pas présenter de poignées (ou d'autres prises) et seront dotées de ferme-porte efficaces régulièrement contrôlés (rôle du SSIAP lors de sa ronde de sécurité). Il est préférable que le système de fermeture soit constitué d'une « barre poussoir » plutôt que tout autre type de crémone aisément manœuvrable. Un contact de fond de gâche installé, permettra de déclencher localement une alarme sonore pour dissuader d'un détournement d'usage et connaître l'état de la porte (ouvert, fermé ou forcé) depuis le PC sûreté.

Les issues de secours intérieures devront être verrouillées dans le sens inverse de l'évacuation au moyen d'un contrôle d'accès de type serrure ou lecteur de badges. Pour les issues de secours les plus sensibles, on pourra installer un système UGCIS (incluant la vidéoprotection). Il est également recommandé de placer ces accès sous vidéoprotection.

L'ensemble des portes du bâtiment devra pouvoir être fermé (hors cabines WC, déshabilloirs). La volonté du maître d'ouvrage sera de passer sur un système tout badge compatible avec les badges CPx. Il n'est pas exigé pour toutes les portes une alimentation filaire et le maître d'œuvre travaillera sur des systèmes sans fil. Le choix se fera par rapport au flux et à la sensibilité du local. A minima, les entrées des zones seront sous contrôle d'accès par badge CPx. En fonction des besoins, certaines seront équipées de visiophone. La réception de l'appel par visiophone sera adaptée à l'activité du service afin de limiter strictement sa perturbation (appel du visiophone arrivant sur DECT par exemple).

Le sens d'ouverture des portes doit être pensé pour qu'elles résistent le mieux possible à une tentative d'effraction (sauf chambres qui s'ouvriront vers l'intérieur). Cependant, la sécurité incendie prime sur la sécurité anti-malveillance.

Sur les circulations horizontales, il est conseillé d'installer des portes de sectionnement en certains points stratégiques des couloirs de circulation pour isoler les bâtiments les uns des autres ou en fonction de services homologues. Cette mesure peut notamment être mise en place dans les couloirs de dessertes en sous-sol.

Les circulations verticales (escaliers et ascenseurs) :

Tous les paliers devront être dotés idéalement de lecteurs de badges dans le sens inverse de l'évacuation ou d'un simple dispositif de verrouillage mécanique. Le système de fermeture devra permettre de connaître la position de l'ouvrant et l'état de la serrure (fermé, ouvert ou forcé). L'alarme ou le fil de l'eau sera reporté au PC de sécurité.

Il conviendra de mettre les ascenseurs du personnel sous lecteurs de badges (en intérieur ou sur les paliers) et de prévoir une priorisation d'appel pour les services de sécurité afin de permettre une intervention rapide.

Au niveau du croisement des circulations verticales et horizontales (paliers), un affichage clair devra être apposé. Il devra indiquer :

- L'étage, le secteur, le nom du bâtiment
- La liste et la direction des services d'hospitalisation, administratif,
- Le numéro des chambres,
- Le nom du chef de service,
- Horaires de visites et de consultations.

C - Les volumes internes :

Il est nécessaire de :

⇒ prévoir l'éclairage et la signalétique des lieux ;
⇒ prévoir la sonorisation complète de l'immeuble (messages d'alertes parlés ou signal sonore clairement audible depuis n'importe quel point). La sonorisation est différenciée par ensembles cohérents. Elle est pilotée depuis le PC sécurité ;
⇒ définir le zoning de sûreté (détermination des zones à accès libre, des zones à accès contrôlé et des zones à accès réservé) ;
⇒ les espaces susceptibles d'être soumis aux intempéries ou à leurs conséquences (hall d'entrée, escaliers, fortes pentes, etc.) doivent être constitués d'un revêtement antidérapant y compris lorsqu'ils sont mouillés.

Des clôtures ou une végétation particulière peuvent servir à séparer les différentes parcelles (ou à l'inverse, les interdire), ou clore la zone dans son ensemble. La rehausse de rambardes ou leur retrait est nécessaire lorsqu'elles empêchent de voir en contrebas.

Un éclairage supplémentaire puissant et spécifique asservi à une détection de présence pourra être envisagé pour certaines zones particulières (entrée d'une pharmacie, aux abords d'une zone de stockage de matières dangereuses, etc.).

L'entretien et l'éclairage des zones extérieures doivent être surveillés, particulièrement les zones de stationnement et de cheminement piétons. Veiller à la visibilité des espaces extérieurs (végétation trop haute et non entretenue).

La signalétique interne à l'établissement doit être revue et adaptée. Cette signalétique doit être claire et suffisante pour faciliter les déplacements sur la zone. Seules les zones publiques sont identifiées nommément. Les autres zones peuvent être numérotées.

Des affichages dissuasifs doivent être installés (site gardienné, site vidéo protégé, dépôt de plainte systématique, etc.).

Tous les éléments susceptibles d'être utilisés à des fins malveillantes (pierres, éléments métalliques, mobiliers, etc.) sont à protéger. Notamment, les extincteurs seront placés dans des alcôves dans toutes les zones à accès du public.

Les poubelles publiques seront de type Vigipirate (supports de sacs transparents) mais compatible avec une éventuelle législation particulière à certains lieux.

L'utilisation de revêtements de chaussée différents (couleurs, nature) permet de matérialiser le passage d'un espace à l'autre (privé/public).

Il convient de choisir des revêtements de chaussée non roulants dans les lieux qui ne sont pas destinés aux cycles, rollers à l'exception des zones permettant le passage des personnes à mobilité réduite.

Il est important de définir des types de matériaux particuliers ou de mobiliers urbains en fonction des espaces pour aider à en identifier la fonction.

D - Détermination des volumes dits sensibles :

La nature de l'activité conduira à identifier un certain nombre de locaux sensibles comme notamment :

- les pièces où seront stockées des valeurs,
- les bureaux de la direction,
- les locaux techniques ou informatiques,
- les espaces VIP (accès dédié, dispositifs de protection particuliers, exfiltration...) ;
- certains locaux doivent faire l'objet d'une attention particulière : locaux poubelles, toilettes accessibles au public, locaux à vélos ;
- les zones SAIV,
- les blocs opératoires,
- les pharmacies
- les crèches
- les laboratoires
- les parkings souterrains sous structure : Dans la mesure où l'analyse de risque a retenu le risque terroriste, il conviendra de s'interroger sur :

- la nature des contrôles effectués à l'entrée ?
- en cas de menace sérieuse, sa condamnation a-t-elle été prévue?
- où se trouvent les piliers porteurs ?
- quels sont les dispositifs prévus pour leur protection ex : renforcement de ces piliers, gestion du stationnement des deux roues autour, stationnement réservé aux personnels du site, aménagement d'un système amovible permettant la neutralisation des places autour de ceux-ci en cas d'élévation de la menace...),.
- Etc.

E - Protection des valeurs :

Il convient de :

- mesurer le niveau de résistance à l'effraction des locaux où seront entreposées les valeurs (structure, ouvrants) ;
- porter une attention particulière à la qualité du mobilier pour remiser ces valeurs (armoire forte – coffre-fort) ;
- prévoir une protection électronique de la pièce (structure et volume) et du meuble de stockage.

F - Prises d'air neuf :

La circulaire DGS/DGUHC/DDSC du n° 2003-114 du 7 mars 2003 prévoit pour les ERP de 1re et 2e catégorie de :

- procéder à un état des vulnérabilités des risques liés à la présence de ces éléments ainsi que des conduits de ventilation,

- mettre en œuvre des mesures de sécurité et de sûreté afin de contrer ce risque (accessibilité restreinte, protection tant mécanique qu'optoélectronique). Une caméra de surveillance des toits, grand-angle, pourra en outre surveiller les prises d'air neuf par détection de mouvement. La porte d'accès au toit sera sous alarme anti effraction reliée au PC sécurité.

Il s'agit donc de réduire au maximum les possibilités d'introduction d'agents R.B.C. dans le système de traitement d'air. L'élément incontournable de cette protection est l'inaccessibilité immédiate par le public de ces prises d'air neuf. En effet il n'existe à ce jour aucun dispositif efficace de protection. La stratégie de base reposera donc sur la difficulté d'accès de ces prises d'air neuf. Leur positionnement, couplé à une détection associée à la vidéoprotection permettra d'anticiper toute action malveillante, et laissera donc le temps aux agents de procéder à une coupure de la centrale de traitement d'air. Une prise d'air neuf accessible depuis la voirie est à proscrire.

G - Transports de fonds :

- les articles L613-10 et D613-60 à D613-75 du code de la sécurité intérieure (CSI) imposent des aménagements dédiés (notamment sas ou trappon) pour les convoyeurs de fonds.
- si eu égard aux caractéristiques intrinsèques du site, cela s'avère impossible, il convient de posséder une dérogation à la loi qui émane, après saisine, de la commission départementale de sécurité des transports de fonds (à Paris, secrétariat assuré par la direction de la police générale). Dans ce cas un cheminement sécurisé ou un local sécurisé accessible depuis l'extérieur devra être mis en place, protégé par un dispositif de vidéoprotection ou un système d'alarme ou de communication.
- pour les constructions neuves, insister sur la nécessité de ne pas recourir au système dérogatoire.

H - Communication radioélectrique des services de secours en opération au sein de certaines catégories d'établissements recevant du public :

- L'article R732-9 du CSI relatif aux communications radioélectriques des services de secours en opération dans les ouvrages routiers, ferroviaires ou fluviaux ou dans certaines catégories d'établissements recevant du public. Il oblige les ERP situés même partiellement en infrastructure à garantir la couverture radioélectrique des services de secours en tout point de l'établissement
- Se référer également à l'arrêté du 26 juin 2008 portant diverses dispositions relatives à la sécurité contre les risques d'incendie et de panique dans les établissements recevant du public.

VI– LES BADGES :

Au regard des difficultés présentées par les diverses solutions de contrôle d'accès (codes, clés, etc.), le contrôle d'accès par badge réunit un maximum d'avantage et le moins d'inconvénients. Pour l'AP-HP il s'agit de la carte professionnelle nationale CPx distribuée par l'ASIP Santé et personnalisée à l'aide d'une photo, du logo de l'AP-HP et d'un film inviolable.

Ce badge d'identité professionnelle permet l'accès piéton, véhicule et l'accès à différents services dont les accès informatiques. Il est unique pour plusieurs fonctionnalités (identification du porteur avec photo, gestion des paiements de restauration, des horaires de présence, de l'habillement pour le personnel soignant…).

Une version spécifique peut être fournie aux partenaires extérieurs (livreurs, ambulances, taxis, maintenance, etc.) pour leur permettre d'œuvrer au sein des locaux.

Ce contrôle d'accès par badge doit être complété par un deuxième système de contrôle d'accès pour les lieux les plus sensibles (salle cœur de réseau, Centre de réception et de régulation des appels du SAMU, PC sécurité…). Il s'agit de l'authentification à deux facteurs. La deuxième authentification peut être réalisée par un code individuel ou par un autre dispositif sécurisé (biométrie par exemple). Pour les lieux très sensibles ayant une activité 24/7 comme les CRRA & les PC sécurité, il doit être prévu, en interne, un dispositif mécanique solide de fermeture de la porte afin qu'une personne ne puisse pas rentrer avec un badge subtilisé ou en contraignant le titulaire d'un badge (confinement en cas d'attaque armée par exemple).

Pour des lieux spécifiques ou l'identification par badge CPx n'est pas possible (pour des raisons d'hygiène comme à l'entrée des blocs opératoires par exemple), un dispositif d'accès alternatif peut être envisagé (biométrie par exemple). La biométrie fonctionne alors en parallèle du lecteur de badge et non comme dans le cas précédent en complément.

De préférence, les personnes ayant un badge, en flux piéton et/ou voiture, ont un accès automatique mais contrôlé ; une seule personne peut accéder à chaque ouverture. L'ouverture libérée par le badge ne doit pas permettre le passage de plusieurs personnes ou véhicules : sas, obstacle barrière puis obstacle amovible en mode sas par exemple pour les véhicules. Pour les accès piétons et véhicules avec badge CPx, le contrôle d'accès se fait en entrée et en sortie.

Les personnes n'ayant pas de badges (flux piéton ou véhicule) doivent avoir des entrées identifiées réduites au strict minimum (idéalement un seul point) qui sont contrôlées humainement : entrée piétonne Vigipirate avec agent.

L'accès des personnels par une voie dédiée permet de soulager les contrôles humains sur les autres points. En outre, un hôpital peut améliorer son ouverture sur la ville en multipliant les ouvertures piétonnes automatisées (CPx) pour les personnels.

Il est possible de délivrer à l'accueil en échange d'une pièce d'identité restituée au visiteur contre le badge lors de son départ. Des solutions permettent de désactiver certains badges à partir d'une heure déterminée.

Dans tous les cas, le badge doit être porté par tous en permanence et de manière apparente (règlement intérieur de l'AP-HP). La décision de doter les usagers et les visiteurs de badges (un marché est prévu) est subordonnée aux contraintes de fonctionnement des différents services.

Les systèmes de contrôles d'accès par badge dorénavant acquis doivent être compatibles sans restriction avec la carte CPx (document prescriptif ASIP Santé). La carte CPx intègre plusieurs dispositifs de sécurité (numéro d'identifiant unique et numéro IAS avec possibilité de certificat ou de mise à la clef - la mise à la clef nécessite une carte CPx inscriptible distribuée à partir de juillet 2017 par l'ASIP Santé).

Si pour des locaux sans particularité, il est possible de retenir un niveau de sécurité relativement faible, pour les locaux sensibles (laboratoires L3, salles serveurs, locaux NRBC…), il y a lieu de déployer une technologie davantage sécurisée comme un certificat d'authentification du numéro IAS. Dans des cas bien particuliers de haute sécurité, il vous est possible de déployer un dispositif authentifiant le certificat d'authentification du numéro IAS. Ces niveaux de sécurité améliorés évitent la copie frauduleuse d'une carte CPx. Cette amélioration du niveau de sécurité est cumulative avec l'authentification à deux niveaux évoquée préalablement.

Dans tous les cas, il est recommandé l'achat de matériels compatibles avec toutes les technologies de la carte CPx ainsi que les principales technologies en service actuellement (Norme 14443 A dont le Mifare Desfire par exemple) afin de n'avoir qu'une simple mise à jour logicielle à effectuer lorsque vous souhaiterez rehausser le niveau de sécurité du système. L'ASIP Santé travaille à l'évolution des dispositifs de sécurité de la carte CPx en la rendant multitechnologie, mais rétro compatible avec les technologies de la carte actuelle. Le système MIFARE Classic, technologie la plus répandue actuellement, présente des failles et est amené à être de moins en moins utilisé.

Les équipements de contrôle d'accès doivent être pilotables au travers d'un logiciel interopérable avec le système d'information de l'AP-HP : ce logiciel de gestion doit être nativement et sans coût supplémentaire en capacité d'intégrer des données en provenance du SI de l'AP-HP, telles que les informations relatives aux identités des agents (entrants et sortants) ou relatives à leur affectation en provenance de la solution GAIAP – IAM Evidian Suite 9 ou supérieure.

De même, ce logiciel de gestion doit être nativement et sans coût supplémentaire en capacité d'accepter et de répercuter un message énonçant un ordre de révocation des droits d'accès applicables dans un délai réduit.

Plus généralement, la possibilité d'intégrer un message de demande d'attribution d'accès pour une identité avec précision de date et de fin de validité doit pouvoir

être implémentée moyennant communication par les équipementiers retenus des spécifications, des mécanismes et formats implémentant ces dispositifs d'interfaçage afin de pouvoir être rendus interopérables avec la solution GAIAP – IAM Evidian Suite 9 ou supérieure.

En outre, le logiciel de gestion des droits d'accès et des alarmes doit afficher les informations d'accès et d'alarme (notamment d'effraction) dans une liste extractible en format standard (de type csv, xls…) et directement sur une carte des locaux afin de permettre une levée de doute et une intervention immédiate sans avoir à interpréter les données. Le logiciel est supervisable et compatible avec le couplage d'alarme associée à un média (activation d'une caméra sur un écran suite à la détection d'une anomalie sonore ou visuelle).

Lorsqu'une rénovation partielle est effectuée, un seul et même logiciel doit piloter tous les systèmes de contrôle d'accès du site.

Concernant les normes de sécurité de tous ces dispositifs, ils doivent intégrer les préconisations de l'ANSSI[1] en matière de sécurité des systèmes d'information (SI) et notamment leur déclinaison au sein de l'AP-HP :

- Règles de sécurité du SI applicables aux titulaires de marché de l'AP-HP daté de février 2017[2],
- Le cadre de cohérence technique destiné à faciliter l'intégration des nouveaux systèmes dans le SI existant[3]

S'ils ne les respectent pas, il doit en être fait mention très clairement. Une ou plusieurs solutions palliatives seront proposées pour atteindre un niveau de sécurité équivalent.

Aussi, comme tout système d'information, les dispositifs de contrôle d'accès doivent être sécurisés et maintenus en condition de sécurité tout le temps de leur usage. La télémaintenance de ces appareils, lorsqu'elle est prévue, doit être conforme aux exigences de la DSI de l'AP-HP et respecter les CCTP.

Le candidat au marché garantit, sous peine de non-conformité, qu'à la date du dépôt de son offre, les logiciels et matériels qu'il propose dans son offre ne comportent aucune vulnérabilité qui permettrait de prendre leur contrôle à distance sans identification et authentification préalable. Le candidat doit disposer d'une politique de maintien en condition de sécurité des systèmes d'information qu'il présente.

[1] https://www.ssi.gouv.fr/
[2] http://dsi.aphp.fr/wp-content/uploads/2016/04/14DI-CharteTitulaireMarché-20170203V12.pdf
[3] http://dsi.aphp.fr/wp-content/uploads/2017/01/CCT-APHP-v3.3_Janvier-2017.pdf

VII – VIDEOPROTECTION :

Un système de vidéoprotection peut poursuivre trois objectifs distincts ou complémentaires :

- La vidéo dissuasion par l'implantation de caméras visibles qui a pour objectif d'empêcher le passage à l'acte délictuel,
- La vidéo protection intervient dès la détection d'une anomalie par un opérateur distant ou par un Détecteur Automatique d'Anomalie (DAA) et peut apporter un soutien aux personnels intervenants. Cette étape peut également être utilisée en exploitation,
- La vidéo élucidation est utilisée uniquement en post traitement dans, par exemple, un cadre d'enquête judiciaire,

Les caméras selon leurs implantations pourront répondre à deux buts :

- Soit les caméras visionnent des champs larges comme les extérieurs et sont utilisées en détection,

- Soit les caméras visionnent des champs étroits comme des accès ou des couloirs et sont utilisées en identification.

Le choix du matériel devra être en adéquation avec le but recherché. Ainsi, les caméras extérieures devront posséder une sensibilité à la lumière importante et être placées dans des caissons anti-vandales et thermostatés. Celles installées dans des locaux non éclairés seront soit, très sensibles à la lumière, soit couplées à des projecteurs infrarouges. Dans tous les cas, une attention particulière devra être apportée à la maintenance du système de vidéoprotection. Sans un entretien régulier, le dispositif pourrait rapidement se dégrader ou devenir inopérant.

Les systèmes de vidéoprotection doivent être numériques et compatibles avec une analyse intelligente des images. Les systèmes de vidéoprotection doivent être interopérables, notamment avec le système d'information de l'AP-HP, et pouvoir être pilotés par des logiciels/matériels génériques sans coût supplémentaire d'intégration. Le format de la vidéo en sortie de caméra ne doit pas être propriétaire. En outre, le format d'enregistrement sur serveur ne doit pas être propriétaire ; il est de type standard (H265). Le système est au moins conforme à l'arrêté de prescriptions étatiques encadrant les dispositifs de vidéoprotection.

Pour certaines zones très sensibles comme les accès, les halls, les accueils et les urgences, la caméra sera complétée par un micro de détection d'anomalies sonores (coup de feu, éclat de voix…) qui génèrent une alarme automatique par image pop-up de cette caméra au PC sécurité.

Sauf pour des raisons de maintenance ponctuelle explicitées dans les cahiers des charges CCTP, il ne doit plus être envisagé d'achat de systèmes de vidéoprotection non interconnectables.

Concernant les normes de sécurité de tous ces dispositifs, ils doivent intégrer les préconisations de l'ANSSI[4] en matière de sécurité des systèmes d'information (SI) et notamment leur déclinaison au sein de l'AP-HP :

- Règles de sécurité du SI applicables aux titulaires de marché de l'AP-HP daté de février 2017[5],
- Le cadre de cohérence technique destiné à faciliter l'intégration des nouveaux systèmes dans le SI existant[6]

S'ils ne les respectent pas, il doit en être fait mention très clairement. Une ou plusieurs solutions palliatives seront proposées pour atteindre un niveau de sécurité équivalent.

Aussi, comme tout système d'information, les dispositifs de contrôle d'accès et de vidéoprotection doivent être achetés, sécurisés et maintenus en condition de sécurité tout le temps de leur usage. La télémaintenance de ces appareils, lorsqu'elle est prévue, doit être conforme aux exigences de la DSI de l'AP-HP et respecter les CCTP.

Le candidat au marché garantit, sous peine de non-conformité, qu'à la date du dépôt de son offre, les logiciels et matériels qu'il propose dans son offre ne comportent aucune vulnérabilité qui permettrait de prendre leur contrôle à distance sans identification et authentification préalable. Le candidat doit disposer d'une politique de maintien en condition de sécurité des systèmes d'information qu'il présente.

Mesures concrètes :

Caractéristiques générales des caméras de vidéoprotection recommandées :

- Caméra numérique (non analogique)
- Fixe (non motorisée)
- Grand-angle
- Full HD minimum. Cette qualité peut-être supérieure pour des lieux spécifiques afin de réduire le nombre des caméras nécessaires à la couverture du site (par exemple un grand hall, un parking…). Au minimum, il doit y avoir 100 pixels par mètre pour les caméras implantées afin de permettre une levée de doute et de 400 pixels par mètre pour les caméras devant permettre une identification (caméras filmant les accès…)
- 25 images par seconde minimum
- Lorsqu'un projecteur infrarouge est prévu :
    - sa portée théorique doit être de 50 % supérieure à la portée réelle souhaitée pour la caméra. Sauf cas exceptionnel, une portée réelle du champ de vision de la caméra supérieure à 100m n'est pas nécessaire
    - il doit être séparé de l'œil de la caméra afin de ne pas attirer les insectes sur l'objectif de la caméra

[4] https://www.ssi.gouv.fr/
[5] http://dsi.aphp.fr/wp-content/uploads/2016/04/14DI-CharteTitulaireMarché-20170203V12.pdf
[6] http://dsi.aphp.fr/wp-content/uploads/2017/01/CCT-APHP-v3.3_Janvier-2017.pdf

- Le WDR ou équivalent (filtre qui permet de réduire le contre-jour) doit être au moins de 120db
- La caméra doit être dotée de la technologie Starlight ou équivalent afin d'être performante de jour comme de nuit
- Le format de sortie de la caméra doit être de type H265 afin de, notamment, réduire la taille des flux vidéo.

La qualité de l'enregistrement vidéo doit être proche de celle du format de sortie de la caméra. La qualité du visionnage des images issues des enregistrements doit tendre vers la même qualité que le visionnage en direct.

Les unités ou services accessibles à des usagers doivent être équipés d'un visiophone et d'une ouverture à distance sur IP permettant le transfert de l'appel et image sur poste fixe ou mobile type DECT.

Le choix des zones couvertes par les caméras pourra être fait en lien avec les signalements de violences et les zones sensibles identifiées.

Concernant les grandes règles à prendre en compte dans le choix des emplacements des caméras :

⇒ L'absence d'angle mort,
⇒ La vision de nuit (notamment ne pas être neutralisée par l'éclairage éblouissant d'un lampadaire par exemple),
⇒ La reconnaissance des individus en toutes circonstances,
⇒ Le traitement de la totalité d'un flux de son entrée jusqu'à sa sortie de l'enceinte afin de pouvoir anticiper, réagir et apporter les preuves utiles (cependant des exceptions peuvent être prévues, par exemple dans les zones de soins où les soignants peuvent souhaiter une confidentialité absolue),
⇒ Les caméras, dans la mesure du possible, devront se couvrir mutuellement,
⇒ L'absence de neutralisation par une évolution (construction, feuilles des arbres en été, pousse d'arbre, développement de la végétation, etc.),
⇒ La couverture de chaque caméra par une autre afin de suivre sans discontinuer un flux et d'éviter la neutralisation d'une caméra,
⇒ L'enregistrement sur une période suffisamment longue, en lien avec les procédures d'alerte de l'établissement, afin que les images soient utilisables comme élément de preuve (le délai de 30 jours, délai maximal légal, est fortement recommandé),
⇒ L'enregistrement doit permettre de rechercher un patient ayant quitté le service à l'insu des soignants par analyse des caractéristiques physiques (par exemple par reconnaissance du visage),
⇒ L'enregistrement des caméras se fait par détection de mouvement avec un début d'enregistrement qui débute cinq secondes avant l'évènement,
⇒ assurer une traçabilité par des caméras fixes mégapixel afin de permettre une identification a posteriori de toute personne entrant sur site ;
⇒ privilégier un asservissement à une détection d'intrusion ou un mode sensor (à ne pas utiliser en extérieur) pour les heures creuses afin d'assurer une gestion confortable de la vidéoprotection ;
⇒ limiter l'usage des caméras motorisées, celles-ci nécessitant un opérateur pour un usage optimal, n'assurant qu'une traçabilité partielle et étant incompatibles avec une analyse intelligente des images ;
⇒ relier le système vidéo sur le courant secouru quand cela est possible ;

- ⇒ privilégier un renvoi de nuit vers le télésurveilleur (si le site n'est pas armé H24) pour une levée de doute facilitée ;
- ⇒ enregistrer systématiquement en pleine définition.
- ⇒ prendre en compte des vulnérabilités architecturales et description des mesures de protection envisagées : protection des points hauts, des prises d'air neuf, des espaces sous structures, des recoins, des lieux susceptibles d'être détournés de leur usage (marches d'escalier – allées extérieures en lignes droites).

Un logiciel d'analyse intelligente des images pour détecter des situations anormales peut être prévu. Ce système génère automatiquement des alertes sur un écran vidéo et permet de passer de la réaction à la prévention en limitant les opérateurs nécessaires au traitement des images. Par exemple, ces caméras sont capables d'alerter sur l'ouverture d'une porte après une certaine heure ou encore un certain laps de seconde, si une personne reste à un même endroit très longtemps, si un individu a des gestes brusques (bagarre, etc.), s'il y a une chute dans un escalator, si un corps est en position allongée et immobile, si un colis a été abandonné, si un véhicule est stationné de manière irrégulière (devant une zone où sont stockés des matières dangereuses, devant un accès pompier, etc.), une circulation à contre sens, un franchissement d'une ligne virtuelle. Le franchissement de ligne est particulièrement adapté à une banque d'accueil afin de détecter un individu qui la franchirait pour agresser le personnel. A cette fin, une caméra doit être dans l'axe de la banque d'accueil.

De manière générale lors d'une alarme de tout type, les caméras du secteur concerné devront se déclencher automatiquement pour une levée de doute (affichage prioritaire sur écrans de contrôle). L'affichage des écrans de contrôle est suffisamment dimensionné afin qu'une image affichée suite à détection ne soit pas occultée par une autre image issue d'une autre détection. Le constructeur s'engage à régler le système d'analyse intelligente des images dans l'hôpital en pleine activité et jusqu'à ce que le nombre de fausses alarmes soit réduit au minimum. Un dernier ajustement est prévu dans les 6 mois de la mise en route définitive.

Les caméras de contrôle des issues doivent se déclencher sur l'alarme d'effraction.

S'agissant de la vidéoprotection dans une zone de soins ou dans un cabinet médical, pour des raisons du respect du secret médical et de l'intimité due aux patients, des professionnels de santé ne souhaitent pas forcément l'implantation de caméras dans ces zones. S'ils le souhaitent, une solution intermédiaire est envisageable, à savoir la mise en place de caméras qui ne s'activent qu'en cas de déclenchement par le professionnel par bouton PTI par exemple. Cette caméra n'est pas positionnée en direction de l'espace de soin du patient, mais vers le reste de l'espace où se situe notamment le bureau de travail du professionnel, lieu du conflit potentiel. Si un évènement intervient, le professionnel déclenche la caméra ; les évènements sont alors filmés. Ces caméras peuvent aussi se déclencher en cas de bruit intempestif ou anormal (plus de X décibels) ou d'agitation (mouvance des pixels). De préférence, cette caméra est dotée d'une diode. Eteinte, la caméra n'enregistre pas, allumée, la caméra enregistre.

En parallèle, déployer des systèmes de détection permettant de déclencher une alarme (barrières immatérielles, contacts d'ouvertures, détecteur de chocs ou bris de vitres ...).

Le dossier « CNIL » devra être complété techniquement (schéma, zone, portée des caméras) par la Maîtrise d'œuvre.

Le système de vidéoprotection doit être conforme aux arrêtés portant définition des normes techniques des systèmes de vidéosurveillance (réglementation française) ou de leur dernière version en vigueur.

Le système sera de type tout IP. Le stockage et les serveurs associés devront être hébergés en salle informatique générale.

La capacité du système doit permettre une durée de stockage de minimum 3 semaines. Dans l'idéal le délai maximal de 30 jours est retenu.

Les caméras seront disposées dans des dômes fixes anti-vandales ou des caissons thermostatés, suivant leur localisation et les besoins. Les dispositifs de vidéosurveillance seront dotés de reports d'alarmes en cas de vandalisme ou d'effraction (masquage, déconnexion…).

Les espaces/accès suivants seront couverts par de la vidéoprotection :

- tous les espaces extérieurs (accès au site, portails et barrières…),
- les circulations (voies d'accès des véhicules VL, PL, les voies engins…)
- Les halls,
- Les accès tant périmétriques qu'intérieurs,
- les portes d'accès au bâtiment coté intérieur, à tous les niveaux,
- les zones publiques accessibles aux usagers : parkings (urgences, dépose-minute, malades couchés), hall principal (plusieurs caméras), locaux de détente, presse, salles d'attente, principaux couloirs (vidéo protection fixe, adaptée à la zone concernée), etc.
- l'hélistation (images renvoyées vers le PC sécurité),
- les salles informatiques générales (à l'intérieur et à l'extérieur),
- les salles cœurs de réseau (à l'intérieur et à l'extérieur),
- les locaux électriques (TG de tout type, poste HT/BT, onduleurs…),
- les postes de paiements,
- les noyaux centraux ascenseurs à tous les étages,
- les halls secondaires intégrant une banque d'accueil ou un service d'entrées sorties des patients,
- les paliers ascenseurs et monte-charge annexes, les paliers de tous les étages de manière à contrôler les circulations verticales. Dans tous les escaliers, installation de la caméra au niveau d'évacuation, pour visualisation de la personne,
- tous les espaces dotés de détecteurs ou de Bouton d'Appel d'Urgence (BAU),
- les circulations horizontales en rez-de-chaussée et notamment au niveau des accès.
- les circulations au niveau de la logistique,
- les zones extérieures de livraison logistique ; surveillance totale de la surface, les quais logistiques, gares de chargement/déchargement et les parcours des transports automatisés lourds ou pas,
- les galeries techniques,
- la pharmacie,

- la zone de délivrance des médicaments de la pharmacie,
- les urgences (accueil, salles d'attente, attentes couchées),
- les portes sous UGCIS,
- les postes de distribution électrique (poste HT, etc.),
- les combles et vides sanitaires,
- les locaux à risques dans l'établissement (réserves, production de chaud, de froid, distribution d'électricité),
- Les régulations de SAMU et leurs accès avec un retour de l'image par écran à l'intérieur du CRRA,
- …

VIII – POINTS PARTICULIERS DE SURETE :

Sécurité et assistance aux forces de l'ordre et services d'urgence :

- matérialiser les cheminements possibles des forces de l'ordre et des secours pour entrer dans le site en indiquant :
  - les difficultés que pourraient rencontrer ces moyens de secours pour cheminer vers leurs accès (stationnements abusifs qu'il convient de prévenir) ;
  - les points dominants qui pourraient être utilisés aux fins de jets de projectiles sur ces personnels.
- extraction facilitée d'une ou plusieurs personnes interpellées :
  - y aura-t-il des possibilités d'approcher le plus possible du cœur du site à l'aide des véhicules de police ou de gendarmerie ?
  - un local de rétention sera-t-il prévu ? Dans l'affirmative, il convient qu'il soit positionné près d'un accès véhicules ou d'un cheminement sécurisé en dehors des lieux accueillant du public. Les chambres sécurisées sont dotées d'un espace sas permettant aux forces de l'ordre d'être positionné de manière sécurisée. Un téléphone est prévu comme les équipements nécessaires aux besoins de la mission (table, chaise…) ;
  - la vidéoprotection pourra-t-elle intervenir en soutien de l'intervention des forces de l'ordre ?

Prévoir les mesures telles que :

- la diffusion d'un signal sonore spécifique à l'alerte des personnels dans l'établissement. Ce signal étant distinct de l'alarme générale sélective prévue par le règlement de prévention des risques d'incendie et de panique.

- Tous les téléphones et DECT doivent avoir une touche d'alarme (appui long par exemple) reportée au PC sécurité. Il en sera de même des boutons d'alarme des banques et caisses.

Ces mesures peuvent se traduire par :

- La fermeture partielle ou totale des accès de l'établissement. Sous le contrôle d'agents de sécurité ou des agents de police ou gendarmerie : seuls les patients et les ambulances à destination des soins urgents seraient autorisés à entrer sur le site hospitalier, ainsi que les personnels rappelés,

- L'instauration d'un périmètre de sécurisation par filtrage des accès aux lieux critiques de l'établissement (SAMU, services des urgences, pharmacies à usage intérieur, etc.),
- Une gestion des flux afin d'éviter un attroupement excessif aux portes ou un blocage des ambulances sur le site des urgences,
- Mise en alerte des personnels en charge des SI (renforcement de la surveillance, restriction ou fermeture préventive de certaines connexions, pré activation du plan de continuité informatique…).

IX – FOCUS SUR :

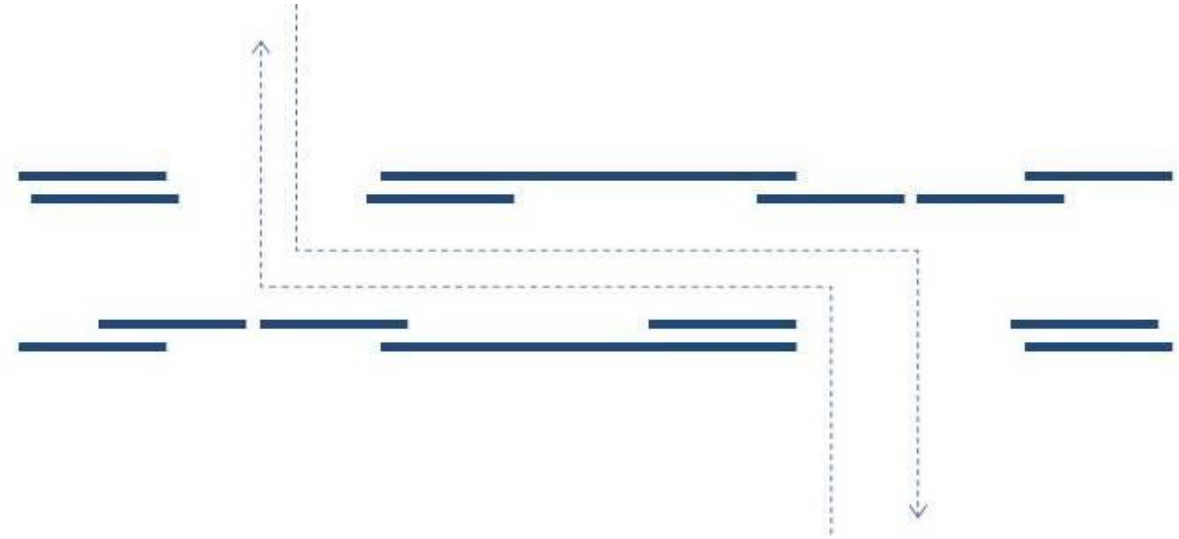
Concernant la signalétique et les plans indicateurs, si pour des locaux ouverts au public, il y a lieu d'être clair sur l'identité du service et leur fléchage ; pour les locaux non ouverts au public, il est préférable de les représenter par des numéros ; autant sur les plans que sur la signalétique. L'objectif est de faciliter l'orientation des patients tout en rendant l'accès aux zones non publiques plus difficile.

A - L'entrée de l'hôpital :

Le contrôle d'accès au site se fait depuis le premier point d'accès depuis la voie publique. Distinguer les entrées avec carte professionnelle (personnels) des entrées sans carte professionnelle. Ces dernières sont contrôlées obligatoirement par un agent de sécurité. Des dispositions sont à prévoir :

- guérite adaptée aux dispositions du Code de Travail, aux normes de sécurité (verre antieffraction, glaces sans tain, etc.) et à la mission confiée,
- systèmes de communication et d'alertes avec le PC Sûreté,
- possibilité pour l'agent de fermer les portes depuis sa position,
- les accès piétons sont à dimensionner en fonction du flux. Un accès automatisé pour les personnels est sous contrôle d'accès en entrée comme en sortie (afin de ne pas être utilisé par une personne non badgée ; s'agissant d'un lieu sans contrôle humain) et surveillée par une caméra (cf paragraphe IV),
- accès véhicules équipés pour fonctionner en « sas de sécurité » avec obstacle télescopique, barrière à jupe et grilles automatiques,
- les accès doivent être sécurisés pour contenir une foule, empêcher la pénétration en force d'un véhicule deux roues ou quatre roues. Les accès véhicules ne doivent pas permettre l'entrée illicite d'un piéton. Les entrées véhicules doivent pouvoir fonctionner en mode sas afin qu'un seul véhicule ne puisse accéder. Un dispositif LAPI est souhaitable pour la gestion du parking et pour faciliter la sortie. Il n'est pas utilisé pour autoriser l'entrée d'un véhicule,
- tous les accès sont dotés d'un dispositif de détection sonore d'une agression (hurlement, claquement, détonation…) et déclenchant une caméra pour une levée de doute depuis le PC sécurité.

Si l'accès se fait par plusieurs portes pour une même entrée, celles-ci doivent pouvoir être individuellement désactivées en entrée afin de créer une entrée en sas décalée et faciliter ainsi le contrôle du flux :

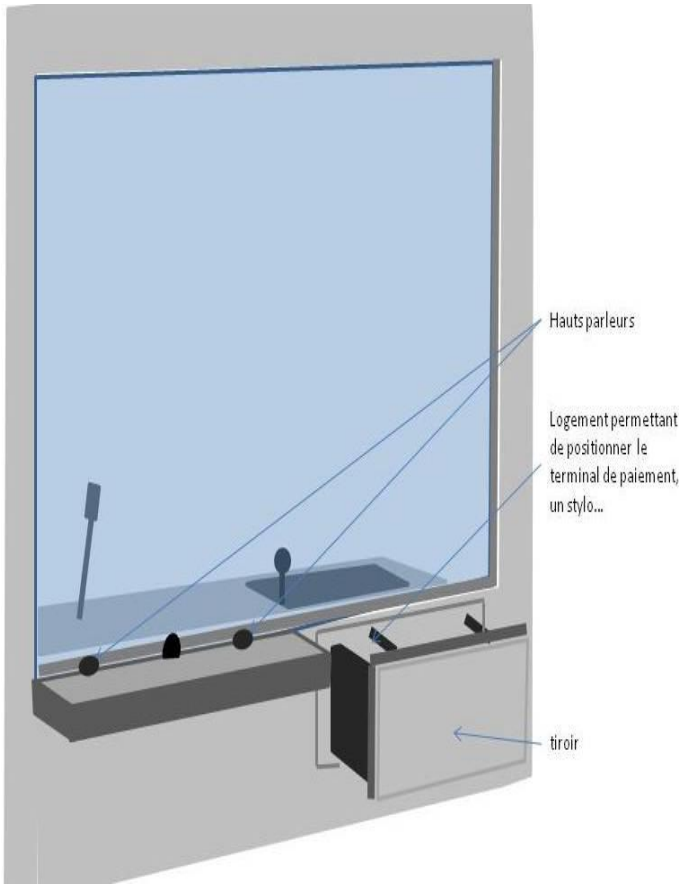


B - La banque d'accueil :

Trois grands types d'accueil prennent en compte le paramètre sécurité. En fonction des contraintes, les solutions proposées ci-après peuvent être mixées.

1- Le guichet de sécurité (vitre blindée) entièrement fermé protège le personnel des coups (schéma ci-dessous). En revanche, il est fréquemment constaté une hausse des injures due à l'absence de contact entre les personnes (hausse du niveau sonore pour se comprendre).

Si le passe-son est simplement ajouré, il évite les coups, mais pas la diffusion du gaz lacrymogène : si telle est la solution retenue, une sortie de secours arrière sécurisée doit être prévue pour le personnel gazé afin qu'il puisse s'extraire des lieux sans être en contact avec l'agresseur. Le gaz ne doit pas pouvoir se diffuser dans la zone de soin. Un passe-son électronique évite cet inconvénient, mais augmente encore la distance avec le patient et nécessite la création d'un passe-document ou passe-colis répondant aux mêmes normes que le guichet. La confidentialité et l'ouverture ne sont pas les atouts de ce type de guichet qui peut être réservé aux lieux de trésorerie ou aux lieux signalant le plus de faits violents. Plus la surface vitrée est haute et moins le sentiment de bunker se fait ressentir. Ce type de guichet est habituellement réservé aux lieux qui voient des transferts d'argent.



2 - Le guichet ouvert : Il est possible d'ajouter une vitre sécurisée au-dessus du comptoir (schéma ci-dessous) afin de maintenir un accueil ouvert et de limiter les risques d'agression physique.

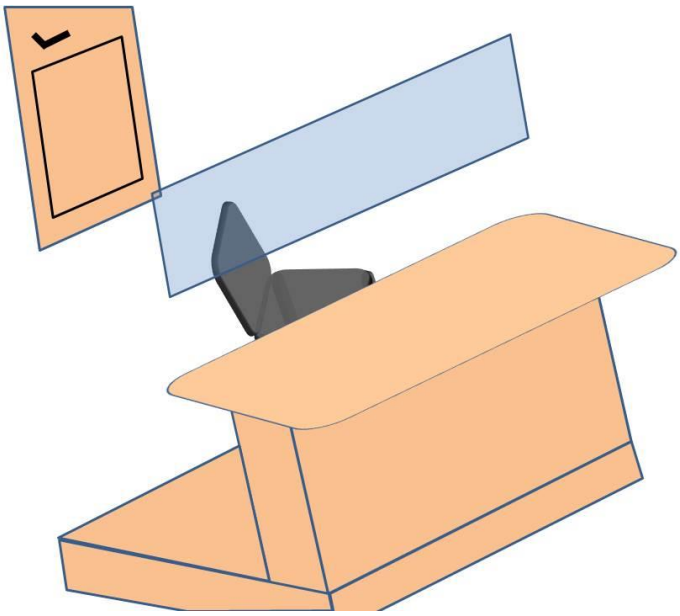
L'espace situé entre le comptoir et la vitre blindée doit être relativement étroit afin de rendre difficile le franchissement. La vitre doit être suffisamment haute pour ne pas être franchissable. L'ensemble de la structure doit pouvoir supporter des coups le temps que l'accueillant s'échappe. Les couleurs sont claires.

Comme dans les autres solutions, pour fuir une agression, une sortie de secours sécurisée est à envisager ; le personnel doit alors pouvoir s'enfermer par un simple mouvement de loquet. Le sens de fermeture de la porte lui permet de résister par l'ensemble de son chambranle et non uniquement par le pêne.

Au minimum, l'accueillant est en hauteur, sur une estrade, mettant son visage en léger surplomb de la personne accueillie (y compris dans une zone plus basse éventuellement réservée aux personnes à mobilité réduite. Celle-ci est alors sécurisée par une vitre supérieure de manière à rendre difficile le franchissement). Cette configuration doit être prévue que l'agent d'accueil soit prévu debout ou assis. Le comptoir de la banque d'accueil est profond afin de limiter la portée d'un coup lancé. Un bouton d'alarme est présent. La seule sortie de cette banque d'accueil est située vers une zone privée. Le matériel ne dépasse pas afin de ne pas être utilisé comme projectile. Les matériels sont enfermables afin d'assurer leur

intégrité en l'absence de l'accueillant. Un bouton de fermeture d'urgence des portes principales doit être prévu pour réagir à une attaque subite.

La conception doit interdire au public de se situer dans le dos de l'agent.



3- Le guichet ouvert afin de favoriser l'accueil (schéma ci-dessous)

La banque d'accueil du hall général, au strict minimum, doit être suffisamment profonde pour limiter l'effet d'un coup porté. L'agent d'accueil assis doit avoir sa tête en léger surplomb de la personne accueillie (estrade). Aucun accès direct ne doit être prévu sur la zone publique et l'accès arrière sur la zone privée doit être fermable rapidement pour faciliter la fuite (loquet). Le matériel d'accueil (informatique) est sécurisé. Un bouton d'alarme doit être prévu et un bouton de fermeture d'urgence des portes principales doit être prévu pour réagir à une attaque subite. Aucun matériel ne doit être accessible directement par la personne accueillie. Si une zone adaptée aux personnes handicapées est nécessaire, elle peut être positionnée sur le côté et sécurisée par une vitre (schéma 2) afin d'éviter un franchissement aisé par un agresseur.

Toutefois, une solution ouverte et sécurisée peut être adaptée au service d'admission (schéma 3). Les deux blocs sur les côtés, contenant le matériel de l'accueil, sont hauts et difficilement franchissables. La partie centrale est étroite et ne peut être franchie qu'en plongeant (avantage supplémentaire, cette étroitesse guide le son et améliore la confidentialité). La table d'accueil est suffisamment profonde pour qu'un coup porté soit en bout de course. Il développe peu d'énergie (il blesse peu).

La table est constituée d'une plaque en verre et l'écran d'ordinateur est situé sous cette plaque de verre. Le clavier est dans un tiroir coulissant sous la table en verre.

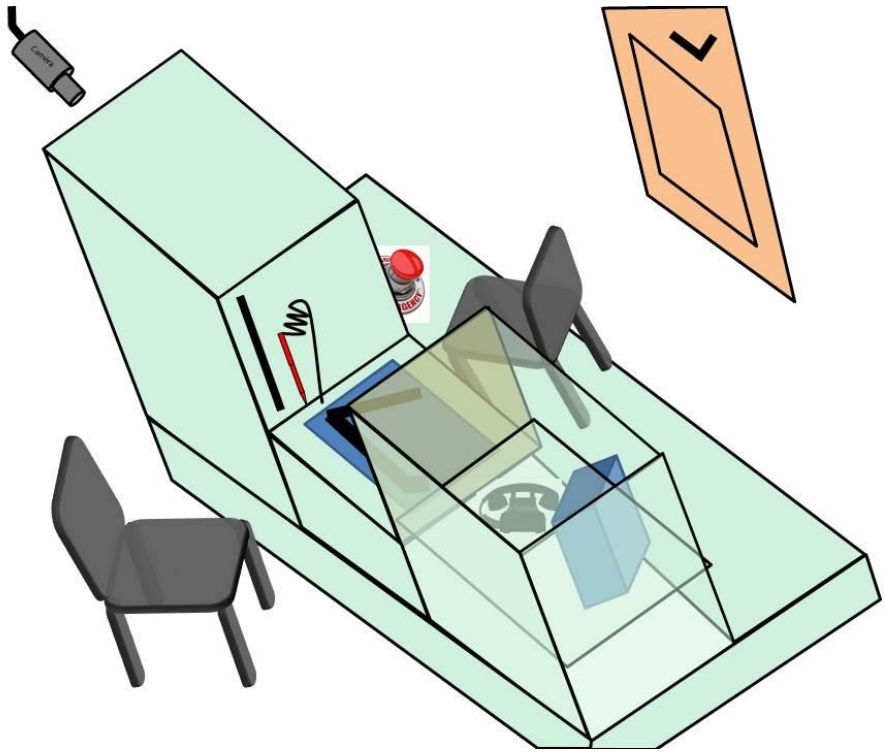
Aucun objet n'est posé entre le personnel et le patient/résident. Aucun élément pouvant servir de projectile ne doit être ajouté sans avoir été sécurisé (terminal de

paiement carte bancaire, lecteur de carte Vitale, crayon pour signer les formulaires, éclairage, etc.).

L'accueillant est monté sur une petite estrade qui surhausse sa position et créer ainsi un rapport de force en signaux faibles qui ne génère pas de violence, mais au contraire retarde le passage à la violence. Les chaises ont plutôt des angles ronds afin de minimiser les dégâts qu'elles pourraient faire subir si elles étaient utilisées comme projectile.

Un ou des systèmes d'alarme sont à disposition en cas de danger potentiel ou avéré. Une caméra analyse la situation afin de détecter par intelligence artificielle une anomalie (cf. paragraphe vidéoprotection). Elle peut détecter le franchissement du guichet par le patient/résident ; elle crée automatiquement une alerte au PC sécurité. Une porte de secours est disponible pour l'agent en cas d'agression. À l'intérieur la serrure doit être munie d'un loquet de fermeture pouvant être manipulé dans l'urgence. La couleur du guichet est claire afin d'améliorer l'accueil.

La conception doit interdire au public de se situer dans le dos de l'agent.



Le personnel d'accueil des principaux accès doit pouvoir réagir en cas de grave menace (risque terroriste) : commande de neutralisation des portes d'accès déclenchement de l'alerte.

Pour chaque point d'accès public, l'agent de contrôle doit pouvoir être en mesure de fermer rapidement depuis sa position, fermer l'accès et de donner tous types d'alertes.

Sur les entrées publiques (accueil principal, urgences), la banque d'accueil devra intégrer un renvoi de la vidéoprotection extérieure et intérieure pour permettre l'anticipation par l'agent des flux qu'il reçoit. Il doit pouvoir également déclencher

tous les types d'alertes et fermer depuis la banque les accès du flux entrant. Le dispositif crée une alerte automatique au PC sécurité. Le personnel d'accueil doit ensuite pouvoir s'échapper en assurant sa sécurité.

C'est pourquoi l'unique accès des banques d'accueil est prévu par une zone non publique située à l'arrière. Une alarme agression est renvoyée au PC de sûreté.

C - Les urgences

Lieu de passage, d'accueil permanent et ouvert à toutes les souffrances, crises, stress et frustrations, les services d'urgence sont par nature pourvoyeurs d'un nombre important de signalements. Le personnel hospitalier en est la principale victime, mais l'agression n'est pas toujours le fait du seul patient : interfèrent également les accompagnateurs et intrus, étrangers à la demande de soins.

Les raisons conduisant à ces violences sont variées. Parfois la conception architecturale inadaptée est un facteur de stress des patients.

L'accès au service des urgences doit se composer d'un accès public/valide ainsi qu'un second accès dédié aux véhicules de secours et/ou aux malades alités. Il est possible d'équiper le second accès d'un sas véhicule si celui-ci est doté d'une boucle de détection magnétique. Une signalétique claire doit être apposée pour différencier les fonctions.

Les issues seront équipées d'un système de fermeture contrôlable à distance depuis l'accueil par exemple. Ce dispositif permettra le fonctionnement de ce service en sécurité positive dans les périodes de faibles affluences ou si une situation à risque est détectée à l'extérieur. Un vidéophone portier et/ou une caméra sera installé pour permettre l'identification du demandeur.

Chaque box de soins dispose d'un bouton d'alarme anti agression relié à l'accueil des urgences et au PC sécurité. L'alarme doit identifier immédiatement le lieu afin de réduire le délai d'intervention. Le bouton d'alarme est positionné discrètement afin que les patients impatients n'utilisent pas ce moyen pour perturber le fonctionnement du service. Cependant, sa forme ne doit pas le confondre avec un autre dispositif.

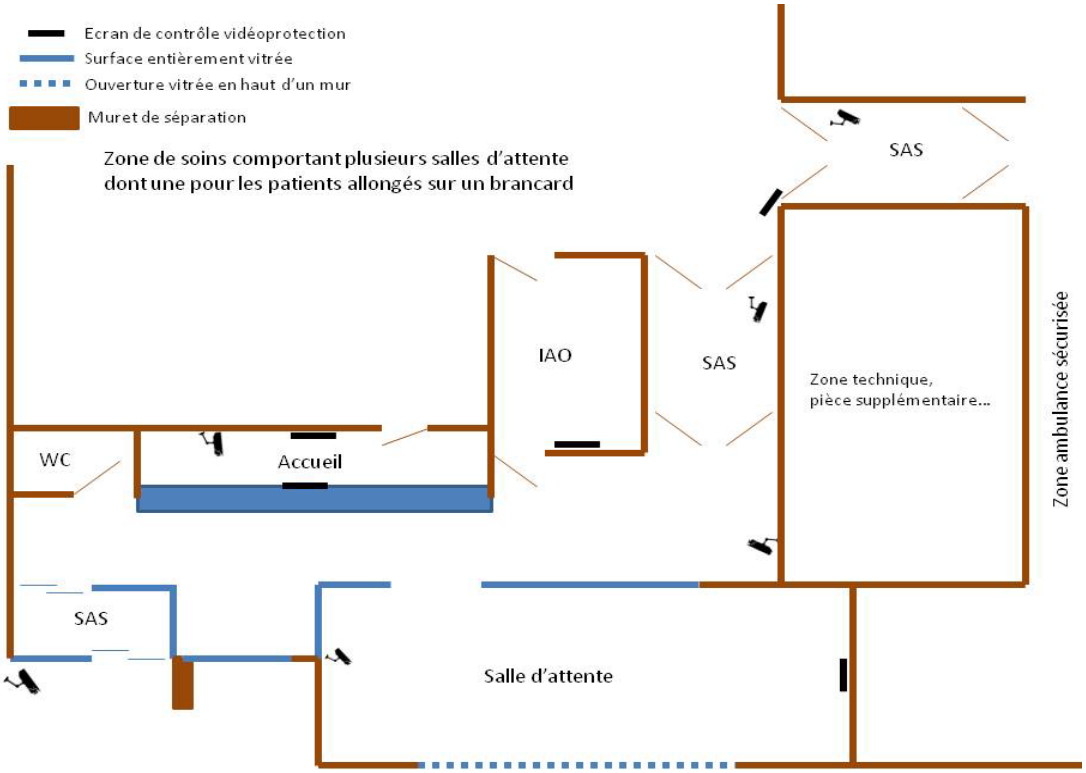
Des cheminements distincts et séparés de l'accès des urgences devront être prévus et clairement identifiés par une signalétique afin de rejoindre les services situés à proximité (radiologie…). Les urgences ne doivent pas être considérées comme un lieu de passage.

Ainsi, il est possible d'envisager la structure comme suit :

Tous les accès peuvent fonctionner en mode accès simple (badge CPx ou détecteur en fonction de la zone), en mode sas (une porte ne peut être ouverte que si la deuxième est fermée) ou en mode blockhaus (les soignants constatent une situation dangereuse, appuient sur un bouton qui passe le système en mode de fermeture complète). L'accès aux urgences doit aussi pouvoir fonctionner en mode fermé (notamment la nuit). L'accès est ouvert uniquement sur déclenchement d'un bouton depuis le poste d'accueil. La sonnette est de type visiophone.

L'entrée en sas décalé et inversé par rapport au sens normal de circulation ralentit le flux d'entrée et de sortie (schéma ci-après). Les patients sont obligés de cheminer par le sas puis devant le comptoir d'accueil (v. la rubrique banque d'accueil ci-dessus) pour toutes les entrées et sorties. Un contrôle naturel du flux est ainsi effectué.

Les surfaces sont entièrement vitrées pour faire rentrer la lumière et permettre le contrôle visuel le plus en amont possible. Cela permet d'anticiper et de passer en mode blockhaus si nécessaire par pression d'un simple bouton. L'agent à l'accueil doit pouvoir directement surveiller les flux entrants et sortants (ou par écran de contrôle si la vue est impossible) pour détecter le plus tôt possible une anomalie et réagir selon la procédure adéquate, notamment déclencher une procédure d'urgence (bouton) et passer le bâtiment/l'entrée en mode blockhaus.



La salle d'attente principale est vitrée vers l'intérieur pour amener de la lumière et un contrôle naturel (v. les aménagements intérieurs possibles de la salle d'attente). Cependant, ce vitrage ne doit pas permettre d'avoir une vue directe sur la zone de soins lorsque le sas d'accès est ouvert, pour des raisons de confidentialité. Le mur extérieur est vitré dans sa partie supérieure afin d'apporter de la lumière sans pour autant rendre visible la salle d'attente depuis l'extérieur (voir le nombre de personnes en attente depuis l'extérieur avant même une prise de contact avec l'accueil augmente le stress inutilement avant d'avoir pu prendre en charge le patient).

Les deux sas d'accès à la zone de soins (piétons et véhicules) sont profonds afin de ne pas pouvoir les franchir rapidement en profitant de la sortie d'un soignant. Ils sont sous contrôle d'accès. Pour les sas d'accès à la zone de soins, il est recommandé de disposer de portes motorisées afin d'éviter les manipulations nombreuses qui réduisent fortement la durée de vie des systèmes (quelques mois

dans les faits). Le sens d'ouverture des portes détermine leur résistance à l'effraction. Aussi, les portes doivent-elles s'ouvrir vers l'extérieur. Les portes peuvent comporter une partie vitrée sans tain afin de voir l'extérieur avant de sortir. Une fermeture deux points est recommandée.

Des écrans de contrôle vidéo complémentaires peuvent être ajoutés à l'accueil, dans la zone de soins (notamment à l'entrée des sas) pour un contrôle naturel par les soignants, mais aussi dans la zone publique (salle d'attente, banque d'accueil…) dans un but de transparence. Au-delà de l'occupation que peut représenter la vision d'un écran de retour caméras en cas d'attente, cela montre un suivi par l'établissement de toutes les actions et peut dissuader de passer à l'acte. Le positionnement des écrans doit conduire à leur visionnage naturel par les personnels.

L'accueil devra être constitué d'espaces semi-privatifs pour le patient et aménagé conformément aux recommandations du chapitre « aménagement possible de la salle d'attente ». Un grand écran tourné vers la salle d'attente diffusera non seulement l'ordre de passage mais également des messages de préventions et différentes informations utiles (parcours aux urgences, inscription, etc.).

Les assises seront orientées vers l'accueil permettant une surveillance naturelle et une meilleure réception des messages vidéo. Elles devront être ancrées au sol pour éviter d'être transformées en éventuels projectiles en cas de heurts.

La salle d'attente sera clairement séparée de l'espace de soins par des portes automatiques (ferme-porte motorisé), équipées d'un lecteur de badges.

Un personnel hospitalier viendra chercher uniquement le patient, les accompagnants n'étant pas autorisés en salle de soins si nécessaire. Un autre personnel informera régulièrement les proches de l'avancée des soins. L'un des critères parfois retenus pour laisser rentrer un accompagnant est l'utilité médicale pour le patient.

Le parcours entre les services mitoyens et le service d'urgence sera équipé d'un vidéophone portier pour identifier tous les demandeurs et filtrer les indésirables.

Pour compléter l'ambiancement de la salle d'attente, une musique douce pourra être diffusée et des chargeurs de téléphones anti-vandales installés. Pour respecter les normes Vigipirate, cette borne permettra de voir le contenu des éventuels casiers à tout moment (porte grillagée, plexiglas…).

La sortie de la salle d'attente est située devant le comptoir d'accueil afin de créer un contrôle naturel de l'accès. Il est recommandé d'éloigner les commodités (toilettes, distributeurs automatiques de restauration…) de la salle d'attente afin d'obliger des mouvements d'usagers réguliers devant le comptoir d'accueil et accentuer naturellement les contacts entre les personnels d'accueil et les usagers. L'IAO (infirmière d'accueil et d'orientation) est attenante à l'accueil afin de mieux faire circuler l'information et l'alerte. Le sens d'ouverture des portes de l'IAO permet une extraction rapide et une résistance à l'effraction optimale. Les portes sont dotées d'un groom automatique et d'un loquet pour permettre la fermeture rapide. Le comptoir d'accueil n'a pas d'ouverture directe sur la zone publique afin de ne pas créer une faiblesse de sécurité. L'accès arrière limite fortement la diffusion d'un gaz afin de ne pas indisposer les patients en cas d'utilisation d'un gaz en zone publique.

La partie « zone technique, pièce supplémentaire » permet la mise en place de zones supplémentaires nécessaires par exemple à des entretiens spécifiques ou des publics spécifiques (mineurs, patients alcooliques, personnes socialement déstructurées, toxicomanes ou présentant des signes d'agressivité d'ordre psychiatrique). En fonction du public visé, la pièce est plus ou moins ouverte et plus ou moins à la vue du public. Cette zone ne doit pas constituer une faiblesse du dispositif global. S'il s'agit de patients agités, un équipement spécifique est à prévoir afin qu'il ne puisse pas se faire mal, ni faire mal. Une seconde porte d'accès peut être prévue afin de permettre une intervention plus aisée de manière simultanée. Chaque porte (hors sas) doit pouvoir être fermée de l'intérieur par un dispositif rapide (loquet…) afin de pouvoir être fermée en urgence.

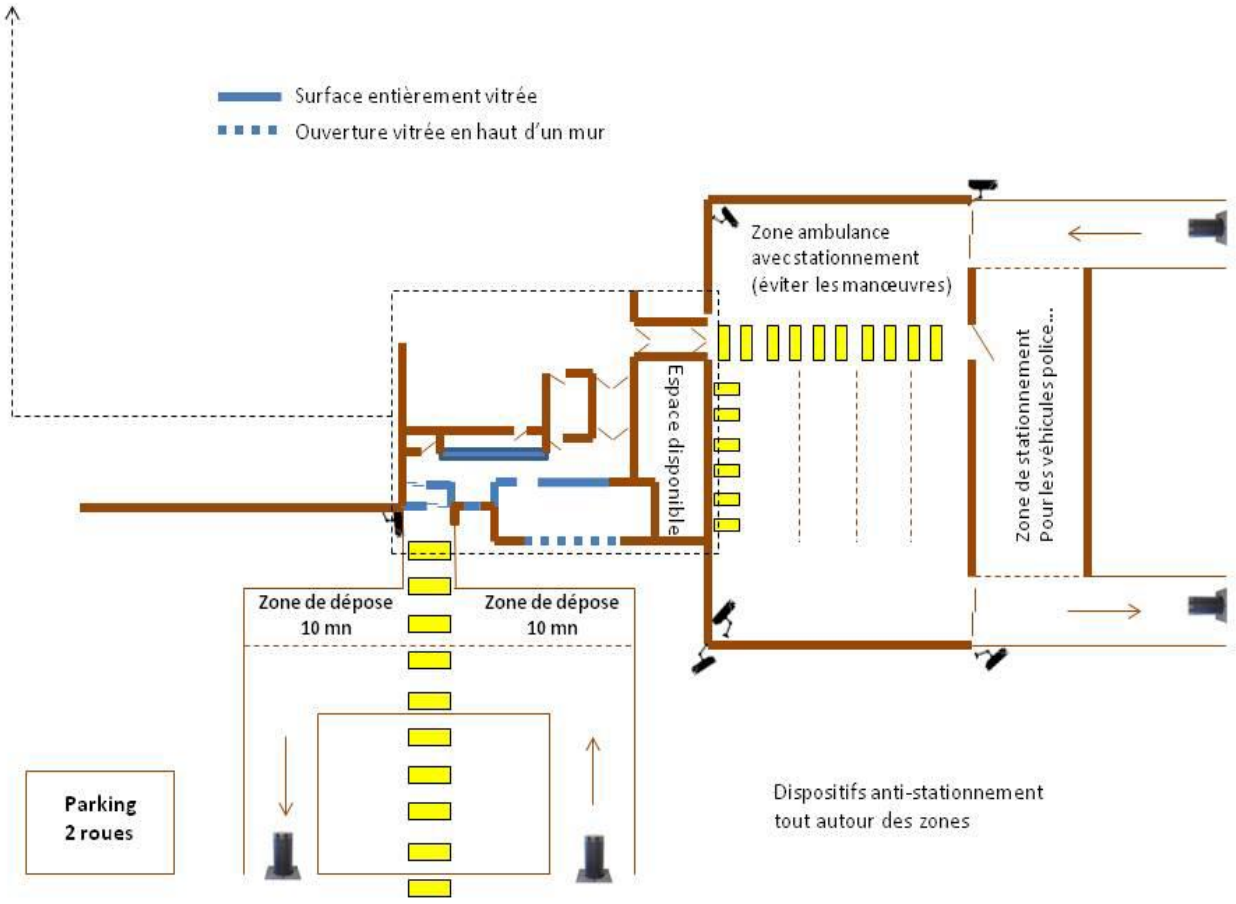
Une salle d'attente isolée et non visible des patients sera réservée aux forces de l'ordre en particulier pour les BNA (Bulletin de Non Admission) et les GAV (Garde A Vue). Du mobilier fixe devra être présent et vidéo protégé.

À l'extérieur, les zones de circulation réservées doivent être également sécurisées par du contrôle d'accès. La zone de réserve des brancards vides s'ouvre par badge, mais également à partir de l'accueil afin d'y donner accès aux ambulanciers après validation du service. La partie publique est sous contrôle par vidéoprotection. La zone de soins peut être également équipée en matière de vidéoprotection.

À l'extérieur, un schéma d'accueil des urgences pourrait être pensé ainsi (schéma ci-après) :

- toutes les zones sont sous vidéoprotection, sans angle mort,

- l'accès public (piétons et véhicules) se fait par une zone sanctuarisée à l'aide d'obstacles télescopiques complétés par des barrières et avec un unique sens de circulation. La largeur de la voie ne doit pas permettre le stationnement anarchique. Des dispositifs anti stationnement doivent être mis en place (surélévation des trottoirs par exemple). Le temps est limité à la dépose du patient (par exemple avec une temporisation sur LAPI (lecture automatique de plaque d'immatriculation) ou un ticket : au-delà de 15 minutes, le stationnement devient payant – une affiche doit être prévue). Une zone de stationnement des deux roues est à prévoir. Elle doit être éloignée de la porte d'accès (Vigipirate). L'accès piéton doit être direct et sécurisé.



- l'accès ambulance est effectué par une voie différente sous contrôle d'accès,

- la zone de stationnement ambulance doit permettre la circulation et le stationnement sans manœuvre (y compris l'entrée et la sortie) et prendre en compte les différents flux,

- à proximité, doit être prévue une zone de stationnement pour les véhicules des forces de l'ordre et de l'administration pénitentiaire,

- une porte piétonne sécurisée entre le hall ambulance et la zone «police» permet l'accès piéton (elle est également indispensable aux ambulanciers et professionnels de santé fumeurs). L'absence de porte piétonne conduit les fumeurs à utiliser les portes d'accès ambulances qui sont souvent neutralisées ou endommagées en raison de cet usage trop fréquent. Cet accès permet aussi un cheminement des patients détenus à l'abri du regard des usagers (prescription du contrôleur général des lieux de privation de liberté).

Les zones qui ne sont pas prévues pour la circulation ou le stationnement doivent être conçues avec des dispositifs physiques de protection de type anti-circulation ou anti-stationnement.

Par ailleurs, les chambres sécurisées sont à placer plutôt dans la zone de soins des urgences afin de ne pas être à la vue du public (exigence du contrôleur général des

lieux de privation de liberté) et être accessible par le sas véhicule. L'accès des véhicules de police, de gendarmerie et de l'administration pénitentiaire est à prendre en compte plutôt dans la zone ambulance toujours pour des questions de confidentialité. Cela leur permet également de recentrer les flux de patients accompagnés par les forces de l'ordre et d'accentuer le passage et la présence de ces derniers dans les urgences pour une sécurité accrue. Ces chambres sécurisées peuvent être précédées d'un espace sécurisé dédié aux forces de l'ordre pour leur permettre de réaliser leurs opérations spécifiques et obligatoires. Cet espace peut être équipé d'un dispositif de vidéoprotection des chambres et de l'extérieur, de casiers pour réunir les objets personnels dangereux des patients, d'un téléphone leur permettant de communiquer y compris avec l'extérieur. Ils doivent pouvoir effectuer un contrôle d'accès des personnes se présentant. Des sanitaires différenciés sont souhaitables pour les patients et les gardiens. Chaque chambre dispose idéalement de deux accès afin de permettre une intervention.

D - Les aménagements possibles de la salle d'attente et gestion des files d'attente :

Quelques pistes d'aménagements permettent de rendre plus agréable le moment passé par les patients/résidents et les accompagnants.

Ainsi, opter pour :

- l'ajout d'un aquarium, pour son rôle apaisant. L'intégration de l'aquarium dans un dispositif aménagement sécurisé permet de protéger les animaux,

- mettre au moins deux écrans :

  - pour éventuellement passer un film expliquant le déroulement d'une prise en charge. Par exemple, un film est présenté dans les bonnes pratiques du site internet de l'ONVS. Ce film est diffusé sur des écrans en alternance avec une présentation des points clefs d'une prise en charge, afin de mieux faire comprendre les délais d'attente et la priorité de passage,
  - la diffusion d'un média distrayant.

- la présence de plantes est reconnue par les soignants comme participant au bon accueil. Les pots les contenant ne doivent pas pouvoir servir de projectile ou de bélier,

- il est possible d'alterner la diffusion des messages d'information avec l'affichage des images issues des caméras des zones publiques des urgences à destination des patients (salle d'attente, extérieurs…),

- la lumière et les couleurs doivent éviter le sentiment d'oppression des endroits confinés,

- les bancs peuvent être dotés d'accoudoirs réguliers ou les sièges peuvent être suffisamment espacés afin de ne pas permettre à une seule personne de s'allonger sur les sièges et ainsi réduire les places disponibles, de générer

des incivilités. Le haut du dossier ne doit pas permettre de s'y asseoir afin d'éviter qu'une personne s'assoie sur le dossier en mettant les pieds sur le siège (la tranche supérieure du dossier est rendue inconfortable – fine, irrégulière, proche d'un mur),

- Le mobilier est scellé au sol dans les zones où le risque d'utiliser l'objet est important, comme la salle d'attente des urgences,

- des distributeurs automatiques de boissons et denrées alimentaires peuvent aider à patienter, ainsi que des bornes de rechargement des téléphones et tablettes (ces bornes sont conformes aux exigences du plan Vigipirate : si elles sont constituées de casiers fermables, le contenu doit pouvoir être vérifié depuis l'extérieur en permanence (grille, plexiglas…).

Gestion des files d'attente

Toutes les zones d'attentes et d'accueil physique (zones de paiements avancés, consultations, d'admissions et sorties, …) doivent être équipées d'un système de gestion de files d'attente qui peut être réalisé au moyen de panneaux d'affichages, de distributeur automatique de tickets en libre-service, de consoles d'appel depuis les guichets et d'une sonorisation d'appel.

Les écrans (type écran TV) doivent permettre d'identifier le poste appelant et sont couplés à une synthèse vocale.

Le système doit être doté d'un superviseur d'exploitation permettant de gérer en temps réel les files d'attente.

Le système sera du type tout IP et interfaçable avec le Système d'Information.

Le serveur est installé en salle informatique générale.

E – Sécurisation des bâtiments :

Chambres d'hospitalisation et des services de médecine :

L'accès principal du service devra être équipé d'un vidéophone portier dont le report s'effectuera dans la salle de garde ou dans le bureau du cadre hospitalier ou sur DECT. Afin de simplifier le travail du personnel et obtenir l'adhésion au dispositif, un ferme-porte motorisé pourra également être mis en place si le service devait fonctionner en sécurité positive en période de visites. La mise en place d'un fonctionnement en sécurité positive pourra se faire dans plusieurs cas :

- en période nocturne, lorsque le personnel est en nombre restreint,
- lors de l'hospitalisation de personnes blessées pendant une rixe entre bandes ou suite à des violences conjugales,
- en cas d'hospitalisation de personnes gardées à vue ou incarcérées.

Les issues de secours, dans toutes les configurations, ne seront pas utilisables dans le sens inverse de l'évacuation.

La salle de garde et/ou le bureau du cadre seront placés au niveau de l'accès principal de manière à permettre une vigilance naturelle et donner le plus en amont possible l'alerte en cas de problèmes. Ces deux locaux pourront également être dotés d'un BAU ou le personnel hospitalier équipé d'un PTI/DATI. Au moins un de ces deux lieux devra présenter une partie vitrée de type anti-vandalisme donnant sur l'entrée du service. Il devra également pouvoir être verrouillable depuis l'intérieur afin de servir de refuge pour le personnel en cas d'agression. Idéalement, cet espace fonctionnera en sécurité positive et disposera d'un lecteur de badge et d'un ferme-porte motorisé dans un souci d'hygiène et de facilité d'usage.

La pharmacie déportée ne devra pas être visible depuis les circulations ouvertes au public. Les produits stupéfiants devront être stockés dans une armoire ou un coffre conformément à la législation et au document de l'APHP intitulé « gestion des stupéfiants dans les unités de soins » (selon l'article 5 de l'arrêté du 12 mars 2013).

Conformément à la législation incendie, tous les services sont équipés de portes de cloisonnement, habituellement maintenues ouvertes à l'aide de ventouses électromagnétiques. Une fermeture programmée sur l'heure des visites sera instaurée de manière à sécuriser les lieux en périodes de faible activité (équipe restreinte). Les ouvrants seront équipés d'un système de verrouillage.

Appel malade – Appel d'urgence :

Le système d'appel malade doit être prévu avec phonie Full duplex. Il doit être décentralisé par service avec possibilité de communication paramétrable interservices ; dans les unités d'hébergement, il est possible d'associer une chambre à telle ou telle unité sans modification de câblages.

Le système d'appel malade doit permettre la traçabilité de tous les événements, sur PC de supervision. Il doit être interconnecté en IP à l'ensemble du SIH afin de permettre de sérialiser les appels vers des terminaux ou téléphones de personnels en fonction du type d'appels. Le logiciel constructeur de traçabilité doit être simple à utiliser par l'utilisateur final.

Le système appel-malade peut être sous IP en fonction des matériels proposés et de l'état de l'art.

Les équipements suivants sont à prévoir :

- en salle de soins par service, un pupitre constructeur permettant de connaître l'état des appels et du système ; il permet de visualiser les appels, d'identifier le patient, avec phonie incluse,
- les écrans de renvoi dans les salles de détente et offices du service,
- les hublots de signalisations 4 feux dans les circulations,
- les terminaux avec phonie dans les chambres et caméras IP asservies aux appels,
- les manipulateurs d'appel en tête de lit, type auto arrachable. Il est précisé que les commandes domotiques de proximité sont indépendantes du système d'appel malade. Les manipulateurs comprennent plusieurs boutons de couleurs différentes selon le type d'appel.

- les tirettes dans les sanitaires communs accessibles au public, les salles de bains et les salles d'eau, (compatibles avec le confort hôtelier voulu par le maître d'ouvrage).
- les tirettes dans les salles de bains des chambres, adaptées dans les chambres PMR (compatibles avec le confort hôtelier voulu par le maître d'ouvrage).

Une source autonome de sécurité d'une autonomie de 2h doit alimenter le système d'appel-malades.

Localisation :

Les services suivants sont à équiper (liste non exhaustive, se référer également aux fiches de spécifications techniques) :

- les unités d'hospitalisation,
- les unités ambulatoires,
- les attentes couchées,
- les services de consultations,
- le service des urgences,
- les unités de soins critiques,
- d'une manière générale tout lieu où un patient est susceptible d'être seul.

Le système d'appel doit être placé dans chaque chambre, box, cabinet de toilette, dans les salles de soins et les salles de bains.

Pour le cabinet de toilette des chambres des patients, doit être prévu un appel par tirette.

Dans les services suivants, doit être prévu un bouton d'appel d'urgence clairement identifiable, mais positionné de manière discrète ([7]), permettant d'alerter les personnels situés dans d'autres locaux du service (box, salles, postes de surveillance, bureaux de surveillance du service), avec couplage sur téléphone mobile IP :

- Salles du bloc opératoire, et endoscopie,
- Salle de réveil au droit de chaque lit,
- Salle déchocage et salle d'examen des urgences,
- Chambres des soins critiques,
- les attentes couchées.

<u>Le bâtiment d'hospitalisation</u> :

En journée, le point d'accueil devra être en capacité de visualiser l'entrée du bâtiment pour anticiper tout incident. Un report de commande de fermeture de l'accès principal pourra être utilisé.

En dehors des heures de visites, tous les ouvrants seront verrouillés et une signalétique indiquera les horaires d'ouverture au public et le protocole d'accès en

[7] L'alarme doit identifier immédiatement le lieu afin de réduire le délai d'intervention. Le bouton d'alarme est positionné discrètement afin que les patients impatients n'utilisent pas ce moyen pour perturber le fonctionnement du service.

cas de nécessité. Un vidéophone sera installé au niveau de l'accès principal et reporté dans le service.

Bâtiments de consultations et administratifs :

Ces bâtiments ne sont habituellement ouverts qu'en journée et donc désert en dehors des heures de bureau. En l'absence de personnel, la sécurisation de ces lieux devra être prise en compte par les mesures suivantes :

- un dispositif technique de validation des passages de ronde afin de s'assurer que tous ouvrants seront contrôlés et la vacuité des lieux,
- Une alarme anti-intrusion sera installée, idéalement couplée à la vidéoprotection afin de permettre une levée de doute rapide,
- Les produits verrière du rez-de-chaussée seront opacifiés pour ne pas permettre une vue depuis l'extérieur et équipés d'un limitateur d'ouverture ou barreaudés,
- Les locaux sensibles (régie, local coffre…) seront dotés de deux dispositifs de détections,
- Tous les services et bureaux seront fermables.
- La sécurisation doit être conçue afin de ne pas attirer l'attention par une visibilité excessive de la sursécurisation d'un site.

Pour des questions relatives au plan Vigipirate, les dispositifs mis à la disposition du public (type consignes ou placards de recharge de téléphone portable), la porte de fermeture doit avoir une transparence suffisante afin de visualiser le contenu depuis l'extérieur et ainsi s'assurer qu'il ne représente pas un danger.

F - Les parkings public et personnel :

La circulation sur les parkings des établissements est parfois complexe et source de tensions voir d'accidents. Certains établissements choisissent de sous-traiter le parking ; d'autres choisissent de rester ouverts avec des mesures de circulation adaptées.

Parfois, des établissements choisissent des solutions mixtes. Certains retiennent la solution du péage, gratuit pour les personnels, les livraisons et les déposes rapides, payant pour les autres usagers (les tarifs peuvent être adaptés notamment en fonction des besoins de fréquentation de l'établissement). Rappelons qu'un parking, même privé, ouvert au public, sans distinction de public, voit le Code de la route s'appliquer, même s'il dispose de barrières pour permettre le paiement du péage. Un arrêté municipal et des panneaux peuvent compléter le dispositif. S'ils ne sont pas indispensables dans tous les cas, ils sont recommandés, l'application des règles en sera facilitée. Le règlement intérieur doit prévoir la réglementation du stationnement et de la circulation. En revanche, le Code de la route ne s'applique pas dans un hôpital qui a mis en place des barrières pour ne laisser rentrer qu'un certain public.

Une seule entrée et une seule sortie des véhicules sur un même point sont à privilégier afin de fluidifier et maîtriser la circulation. Il y a lieu également d'éviter les croisements de flux. Un accès supplémentaire sous contrôle peut exister pour les zones techniques. Des miroirs d'angle sont mis dans tous les angles aveugles afin de voir les véhicules/piétons arrivant à contresens. On peut prévoir d'autres miroirs pour qu'un automobiliste s'assure de ne pas être suivi en entrant dans le parking.

Concernant les zones de stationnement, au-delà du cas particulier des urgences, il y a lieu de distinguer les zones publiques, les zones réservées aux professionnels et les zones réservées aux personnels. Elles ont des destinations et des contraintes différentes.

Par exemple, pour désengorger les parkings, un partenariat avec une société de covoiturage peut permettre aux personnels d'effectuer leur trajet domicile travail à moindres frais, de développer une politique éco responsable et de ramener de la fluidité sur les parkings.

Un ou plusieurs parkings deux roues avec accroches de type U inversé devront être prévus. Ils ne sont pas placés immédiatement devant l'entrée (Vigipirate), mais à proximité. Ils seront sécurisés, éclairés et vidéo protégés. L'espacement des U inversés déterminera le type de deux roues qui pourra être accepté.

Là où le stationnement n'est pas autorisé, des dispositifs doivent empêcher physiquement le stationnement illicite (surélévation de trottoirs par exemple). Le dispositif anti-stationnement ne doit pas permettre l'attache d'un deux roues (exemple : un dispositif anti-stationnement en U métallique verra inévitablement les usagers attacher leurs vélos en ce lieu).

Parcs et parkings souterrains :

Les accès véhicules sont d'abord mis en sécurité par l'installation d'un accès pouvant fonctionner en sas (barrière + porte par exemple). Cette zone sera vidéoprotégée, munie d'un lecteur de badge et d'un dispositif de visiophone. La rampe doit être recouverte d'un revêtement clair, bien éclairée et également vidéoprotégée. L'accès parking est fermé par une porte solide basculante ou coulissante conforme à la réglementation en vigueur et est asservi à un lecteur de badge.

Il peut être muni d'un anti pass-back (Un dispositif anti-pass back est une fonction particulière du dispositif permettant de s'assurer d'une entrée pour une sortie avec un même badge, il empêche ainsi l'utilisation de l'accréditif pour faire entrer ou sortir plusieurs véhicules).

Afin d'éviter l'entrée d'un piéton ou d'un autre véhicule derrière un véhicule accrédité, il y a lieu d'installer :

- une alarme de détection (optique, analyse intelligente des images, etc.),
- une barrière haute avec jupe rendant difficile le franchissement par un piéton,
- une boucle magnétique (l'utilisation du badge sans détection magnétique ne permet pas les ouvertures).

Les sas utilisant des rampes monovoie seront équipés de feux alternatifs.

Toutes les issues doivent être d'un niveau de sécurité équivalent à l'entrée principale. L'accès au parking depuis l'intérieur du bâtiment doit être protégé de la façon suivante : asservir la commande pour l'accès au sous-sol par les ascenseurs contrôle d'accès, la montée disposant d'une rupture au niveau 0. Les portes donnant accès aux plateaux doivent être également sous contrôle. La porte de l'escalier située au rez-de-chaussée du bâtiment et menant aux parkings sera elle aussi sous contrôle d'accès.

Parc de stationnement :

Les plateaux doivent offrir un visuel aussi large que possible. Les emplacements doivent être matérialisés au sol et numérotés afin d'être individualisés.

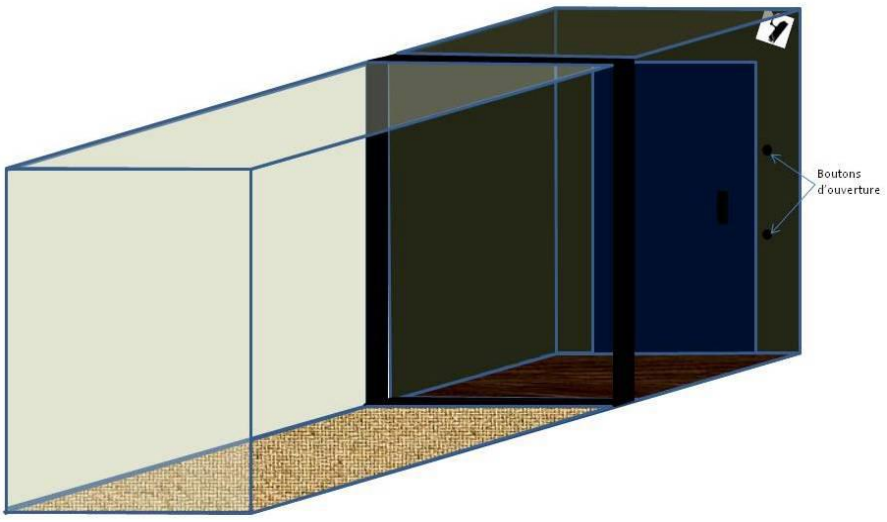
Un éclairage puissant pourra être installé afin de garantir qu'aucune zone d'ombre ne persiste dans le parking. Une peinture claire sera appliquée sur les murs et éventuellement au plafond.

Des caméras devront être installées de manière à couvrir les accès ainsi que les espaces de circulation.

En complément de ces mesures, une musique d'ambiance pourra être diffusée afin de participer au sentiment de sécurité.

G - La gériatrie :

Une des difficultés rencontrées dans les services de gériatrie est la fuite des patients fortement atteints par une malade les désorientant. Pour limiter les sorties présentant un danger pour le patient ou autrui (patients les plus gravement atteints) tout en maintenant les locaux ouverts, il est possible d'aménager les accès pour limiter les sorties dangereuses à leur strict minimum sans avoir besoin de mettre en place une surveillance humaine permanente. Un dispositif de géolocalisation des patients sera prévu.



Le principe qui peut être retenu est de rendre très sombre la dernière partie du couloir de sortie (sur trois mètres environ) afin d'inciter les patients les plus gravement atteints à ne pas se rendre dans ce secteur. Les couleurs des murs, du plafond et du sol sont les mêmes que dans le couloir, mais, dans la dernière partie, elles sont bien plus sombres, de plusieurs teintes. La luminosité est basse. Aucun objet ne doit présenter un risque de chute dans cette partie. L'ajout d'une bande noire de séparation des deux zones de 30 cm sur les murs, le plafond et le sol accentue le phénomène en marquant la césure. Ainsi, les personnes les plus désorientées, celles pour lesquelles la fuite constitue un risque réel pour leur santé, sont dissuadées de franchir cette zone. Elle ne retire pas la nécessité d'une surveillance humaine, mais réduit considérablement le risque pour les patients les plus fragiles.

Il est aussi possible de mettre en place une porte d'accès à serrure ventouse dont l'ouverture est commandée par l'appui simultané sur deux boutons distants verticalement d'environ 50 cm. Ainsi, les locaux restent ouverts à la sortie, mais sont davantage sécurisés pour le public le plus fragile. Le dispositif est accompagné d'une caméra avec un logiciel capable de détecter une stagnation devant ou dans cette zone sombre.

Afin de limiter les fuites des patients les plus fragiles, des dispositifs de localisation sont également employés sous forme de bracelet (cependant, parfois, des patients tentent de les enlever avec acharnement en s'occasionnant des blessures légères), de pastilles insérées dans une poche, une pantoufle ou tout autre objet. Ces dispositifs peuvent générer une alerte si le patient entre dans une zone qui peut être dangereuse pour lui. Le dispositif doit être conforme aux recommandations de l'AP-HP.

H - La Psychiatrie :

Afin d'éviter les incendies, il est possible de mettre en place des briquets muraux (gros boîtier briquet fixé au mur). Ils sont généralement fixés en extérieur, dans la zone fumeurs, près d'un cendrier, sous un auvent. Ils permettent de ne plus devoir gérer les briquets des patients. Parfois l'interdiction des briquets est prévue dans le contrat de soins que le patient signe. Ce dispositif permet de limiter les départs de feu rencontrés fréquemment dans ce secteur.

Certains patients utilisent les angles des couloirs pour se cacher puis surprendre et agresser. Des miroirs d'angle de type « sortie de parking » peuvent limiter ce phénomène et permettre une meilleure appropriation de l'espace. Dans certains cas ce choix ne sera pas retenu par crainte d'aggravation de la paranoïa de certains patients.

Concernant les chambres d'isolement, il semble qu'un accès double soit indispensable en cas de crise du patient afin de pouvoir délivrer les soins en toute sécurité. Bien évidemment, aucun objet ne doit être accessible au patient en toute circonstance.

En revanche, en ce qui concerne le positionnement des sanitaires, douches, observation par caméra, œilleton, fenêtre de surveillance, équipements

(téléviseurs, etc.) les avis sont très partagés sur les effets induits en terme de sécurité.

La mise en place de plusieurs salles de pause collectives pour les patients réduit les tensions en permettant de satisfaire la diversité de leurs besoins.

A l'image de la gériatrie, il est possible de mettre en place une prise de photographie des patients susceptibles de fuguer afin de pouvoir les retrouver plus facilement, notamment en diffusant la photo aux forces de l'ordre. Ce dispositif doit être conforme aux recommandations de l'AP-HP (avis/décision médical, avis/décision famille…).

I - La Maternité :

Il est recommandé de mettre en place :

- un système anti-rapt du nourrisson : par exemple les nouveau-nés portent à la cheville un bracelet (émetteur miniature inviolable) déclenchant une alarme ou la fermeture automatique des issues (y compris le blocage des ascenseurs si l'enfant est emmené hors de la zone surveillée par une personne autre que l'un des membres du personnel autorisé (port du badge obligatoire),
- un circuit du patient et du personnel en dehors des heures d'ouverture,
- la liste du personnel autorisé pour le déplacement du nourrisson.

La mise en place de ce système s'accompagne d'une communication importante (signalétique, livret d'accueil, affiches, etc.) et d'une formation du personnel.

Les sorties de secours sont sous UGCIS (Unité de Gestion Centralisée des Issues de Secours).

La porte d'accès, unique, est accessible uniquement sur contrôle d'accès et dispose d'un visiophone. Les appels sont reportés sur les DECT (ou équivalent) des personnels pour permettre l'ouverture à distance. Une caméra filme l'accès. Elle est couplée à une détection sonore d'anomalie.

J - La crèche des enfants du personnel :

De préférence, l'accès se fait par un sas (s'il est vitré, les vitres doivent être blindées), le sas doit pouvoir fonctionner en mode normal, en mode sas, en mode fermé ; aussi bien en entrée qu'en sortie.

A l'extérieur, il doit être positionné un visiophone : on doit pouvoir répondre au visiophone et déclencher les différents modes de l'accès du sas, fermé, sas, ouvert depuis les bureaux administratifs, un accueil.

Une caméra est positionnée à l'intérieur et filme les entrées et sorties ; elle est suffisamment définie pour pouvoir identifier une personne en toute circonstance

(jour, nuit). Comme pour tous les accès, la caméra est asservie à une détection sonore d'incident.

Les salles des crèches étant vitrées pour des raisons de transparence, elles ne peuvent servir de salle de confinement en cas d'attaque armée. Aussi, une pièce/zone durcie, capable de résister à une attaque armée, et permettant de contenir tous les enfants, doit être envisagée pour les confinements.

Il est recommandé d'occulter à la vue des voisins les espaces extérieurs.

Par ailleurs, la mention « crèche » ne doit plus apparaître tant sur les panneaux que sur les plans. La numérotation chiffrée, comme sur toutes les zones sensibles non ouvertes au public, est recommandée.

K - La Chambre mortuaire :

Les flux de patients décédés depuis les unités de soins doit être discret, ils ne doivent en aucun cas croiser les flux patients ou visiteurs.

La chambre mortuaire dispose de 2 accès extérieurs réservés :

- aux familles : l'accès est direct par l'extérieur avec parking associé
- aux professionnels partenaires (Pompes Funèbres Générales, thanatopracteur, ministres du Culte, etc.).

Les effets des défunts peuvent, selon les possibilités de l'hôpital, être divisés en deux parties distinctes :

Les biens de valeurs et d'importance (bijoux, moyens de paiement, téléphone portable, tablette…). Ils seront stockés obligatoirement dans un coffre avec inscription et détail sur un registre dédié. Ces biens ne seront remis qu'aux proches légitimes, après vérification des identités et contre signature.

Les biens de faible valeur (vêtements, trousse de toilette…) seront recensés et stockés dans un local fermant à clef.

La sécurisation des chambres mortuaires peut engager la responsabilité de l'établissement, notamment s'il est porté atteinte à l'intégrité du corps du défunt ou si une tentative de subtilisation quelconque intervient. L'accès à la chambre froide (contrôle d'accès) doit être strictement réglementé pour le personnel qui y est dédié (les personnes extérieures ne doivent pas y avoir accès seules – mêmes munies d'une autorisation de l'hôpital). Aussi, la ou les chambre(s) froide(s) doivent être sécurisée(s).

L'ONVS recense des violences en ces lieux notamment en raison des particularités des différentes cultures ou pratiques religieuses qui génèrent des comportements ou souhaits parfois contradictoires avec la légalité de certaines situations. Aussi, c'est un endroit qui doit être sécurisé afin d'assurer tant la sécurité des personnels, que des familles, du défunt et des locaux. Aussi, les accès seront renforcés et les principes généraux de zonage avec contrôle d'accès strictement respectés.

L - Points névralgiques et lieux sensibles :

On entend par locaux sensibles les lieux, pouvant présenter des risques particuliers (oxygène, acides, produits stupéfiants…), abritant des installations indispensables au bon fonctionnement du site (serveurs informatiques, onduleurs, groupes électrogènes…) ou vitaux pour les secours à la population.

Ceux-ci devront être *a minima* sous contrôle d'accès de niveau supérieur (authentification forte et/ou à deux niveaux), dotés d'ouvrants résistants et d'alarme intrusion. Ils sont protégés par caméras.

Lorsque le lieu sensible est extérieur (stockage de gaz médicaux par exemple), l'enceinte doit être d'une hauteur minimum de 3 mètres. Elle est close dans ses trois dimensions (grillage dans sa partie plafond par exemple). Le plafond est alors situé au minimum à un mètre au-dessus du sommet du dispositif protégé. Ces prescriptions seront adaptées en fonction des normes spécifiques s'imposant au matériel protégé. Le dispositif sensible protégé n'est pas visible depuis la voie publique (mur opaque…).

Les mesures de sécurité des points névralgiques et des lieux sensibles doivent être renforcées par :

- La protection et la résistance de tous les ouvrants (portes, fenêtres),
- Le niveau de verrouillage,
- Les systèmes de filtrage, SAS de sécurité,
- La supervision des contrôles (délais, alertes…)
- La vidéoprotection,
- La détection intrusion (à l'ouverture, volumétrique, etc.) / conditions d'intervention.

Des zones sont identifiées comme zones névralgiques, car elles entrent dans le dispositif de Sécurité des Activités d'Importance Vitale (SAIV) du code la défense et sont identifiées dans le plan de sécurité de l'opérateur de l'AP-HP.

Les dispositifs prévus dans le plan Vigipirate doivent être pris en compte. Ces zones sont notamment :

- Le local plan blanc
- L'unité d'hospitalisation infection à très haut risque,
- Les urgences (toute la chaîne de fonctionnement des urgences),
- Les trauma-centers,
- Les locaux pour la prise en charge NRBCE,
- Les laboratoires L3,
- Les salles informatiques générales et salles « cœur de réseaux »,
- Les locaux techniques principaux : les livraisons concessionnaires (électricité, eau, chauffage), la centrale GE, les aires de fluides médicaux, les locaux techniques de production/distribution des primaires.

Les conditions d'accès sont durcies conformément au paragraphe « contrôle d'accès ». Une couverture par vidéoprotection de l'accès extérieur des locaux et une couverture totale de l'intérieur des locaux hors chambre REB et zones de soins doivent être prévues.

Cependant, toutes les vulnérabilités doivent être prises en compte :

- les accès (piétons et véhicules),
- les enceintes,
- les fluides (stocks et flux),
- les stocks particuliers,
- les matières dangereuses (NRBC et autres comme les DASRI) et leurs déchets ainsi que les flux les gérant,
- les matières dangereuses,
- les DZ,
- les circuits logistiques,
- les circuits/stocks des denrées alimentaires,
- eau potable,
- eau osmosée,
- air,
- génie climatique,
- les produits médicaux (stocks et flux),
- les appareils biomédicaux ou dispositifs techniques indispensables aux soins des patients,
- les réseaux téléphoniques et informatiques vulnérables,
- les dispositifs électriques et de secours,
- ne pas oublier de prendre en compte les risques liés à la 3e dimension (notamment pour les sites qui reçoivent des VIP qui pourraient être exposés à des prises de vue depuis l'extérieur).

Ces différenciations doivent prendre en compte la temporalité : la situation peut être différente, la nuit (une alarme ?), le jour, le week-end… Ceci permet de différencier les espaces et de prévoir les différents lieux de contrôle d'accès. Chaque changement de zone doit être assuré par un contrôle d'accès.

Les besoins d'investissement de tous les espaces identifiés se déterminent notamment à partir de l'analyse des flux.

Les activités infectieuses (de bactériologie, de mycologie, de parasitologie, de virologie et d'hygiène) peuvent être éventuellement rassemblées dans un ensemble cohérent qui permettra de maîtriser les conditions environnementales inhérentes à ces activités. De nombreuses complémentarités techniques existent ce qui permet d'envisager des mutualisations de moyens et de favoriser les échanges de compétences.

Des caméras doivent être installées sur les lieux de livraison d'électricité, de carburants et autres.

La sécurisation des réseaux doit être assurée sur toute leur longueur (eau, électricité, production calorifique, génie climatique, fluides médicaux, distribution capillaire de réseau de tous types…). L'accès direct à tous les réseaux est interdit sauf dans les locaux techniques, gaines techniques ou autres espaces réservés aux personnels de maintenance habilités.

Les issues de secours de la galerie CPCU doivent être sécurisées pour éviter toutes intrusions ainsi que les accès souterrains qui pourraient exister (réseau d'égouts, passages de câbles).

M – La pharmacie centrale :

L'accès à la pharmacie devra être muni d'un contrôle d'accès à distance de type vidéophone portier. Il devra fonctionner *a minima* en sécurité positive de nuit.

Un comptoir dédié au personnel non autorisé et aux patients munis d'ordonnance devra être constitué, le cas échéant. Afin d'éviter tout contact direct, ce comptoir sera surmonté d'un plexiglas ou un vitrage de type anti-vandalisme et d'une trappe à volet pour échanger les ordonnances et les médicaments requis.

Le local sera muni d'un bouton d'appel d'urgence ou le personnel doté d'un PTI. Le local est placé sous vidéoprotection.

Afficher le rappel de la réglementation sur la gestion des produits stupéfiants (ou assimilés).

La caméra située en zone d'accueil du public est couplée à un micro capable de déclencher l'affichage automatique de la caméra au PC sécurité en fonction de l'anomalie sonore détectée (cris…).

Le local sera conçu pour faciliter la gestion et le contrôle des stocks.

Gestion des produits stupéfiants

Les produits stupéfiants devront être stockés dans une armoire ou un coffre conformément à la législation et au document de l'AP-HP intitulé « gestion des stupéfiants dans les unités de soins »

Arrêté du 12 mars 2013

Relatif aux substances, préparations, médicaments classés comme stupéfiants ou soumis à la réglementation des stupéfiants dans les établissements de santé.

Article 5

Les substances, préparations et médicaments classés comme stupéfiants sont détenus séparément dans une armoire ou un compartiment spécial banalisé réservé à cet usage et lui-même fermé à clef ou disposant d'un mode de fermeture assurant la même sécurité, dans les locaux, armoires ou autres dispositifs de rangement fermés à clef ou disposant d'un mode de fermeture assurant la même sécurité, réservés au stockage des médicaments.

Tout vol ou détournement est signalé sans délai aux autorités de police, à l'agence régionale de santé et à l'Agence nationale de sécurité du médicament et des produits de santé. Les quantités volées ou détournées sont portées sur le registre prévu à l'article R. 5132-36 du code de la santé publique.

N – Les blocs opératoires :

Deux accès sont prévus dans les blocs opératoires, l'un pour les patients alités et un second pour les seuls personnels, configurés en sas de manière à conserver l'environnement stérile. Les accès sont équipés d'un lecteur de badges CPx et d'un moyen d'identification biométrique sans contact (iris par exemple) fonctionnant en parallèle du lecteur de badge et de fermes portes motorisés. Ces équipements permettent l'accès en toutes circonstances notamment lorsque l'hygiène ne permet pas l'utilisation d'une carte d'accès.

Afin d'obtenir l'adhésion du personnel et de faciliter les flux, des portiques de détection RFID seront installés de part et d'autre des portes, qui devront être automatisées ; notamment pour permettre le passage des patients alités et du matériel médical. Ce dispositif évitera la détérioration des ventaux avec des brancards par exemple.

Par manque de place, les chariots de stockage de matériels médicaux, propres ou ayant servi, sont stockés dans les couloirs de circulations en amont des blocs et laissés ouverts. *A minima*, les chariots seront fixés aux murs et verrouillés. Une autre solution consiste à placer les chariots dans des espaces adaptés et pourvus de portes à ouverture automatique avec des lecteurs de badges.

Les locaux de stockage et les accès seront placés sous vidéoprotection. Si les locaux ne sont pas utilisés en H24, les lieux seront placés sous alarme avec une levée de doute par vidéoprotection. Les équipements onéreux (endoscopes par exemple) seront mis sous clef et obligatoirement sous alarme.

O - Accès pour les personnes à mobilité réduite :

La réglementation en matière d'accessibilité aux personnes à mobilité réduite doit être respectée.

P – Sécurisation des chambres d'hospitalisation et coffres forts :

Les chambres d'hospitalisation seront équipées d'un coffre-fort.

Afin de réduire les vols d'opportunité, il est important de revoir la disposition des emplacements sécurisés offerts aux patients. Ces dispositifs pourront être de deux types :

- fermeture du tiroir à portée de main du lit au moyen d'une serrure à code individualisable,
- ou positionnement du coffre-fort dans la table de chevet ou au mur à portée de main.

Si l'ouverture du coffre doit être effectuée par le personnel (lors d'un décès ou d'un transfert par exemple), celle-ci doit impérativement se faire à deux pour éviter toute contestation. Si le personnel s'aperçoit que des biens de valeurs sont laissés seuls à proximité d'une personne dans l'incapacité de pouvoir les gérer elle-même, un process interne doit être mis en place pour éviter tout problème. Dans l'absolu,

ces biens doivent être consignés dans un registre avant d'être stockés dans un coffre de l'hôpital. Cette opération doit se faire également à deux personnes.

Des coffres forts doivent être présents :

- dans les chambres de patients et de dimension suffisante pour contenir une sacoche, un sac à main ou une tablette,
- dans les chambres des hôtels hospitaliers (mêmes caractéristiques que pour les chambres des patients),
- dans les services de soins (stupéfiants) et autres produits dangereux,
- aux urgences : coffre-fort tampon ou de délestage,
- dans les régies
- dans les PC sécurité
- dans les bureaux des chargés de sécurité antimalveillance.

Lorsque le patient arrive aux urgences ou s'il est inconscient : il est impératif de faire un inventaire des objets et valeurs qu'il a à son arrivée.

Q - Le poste de sécurité :

Si les conditions réglementaires ne permettent pas de créer un PC sécurité unique intégré réunissant l'incendie et l'antimalveillance, il y a lieu de privilégier leur création dos-à-dos, séparés par une cloison vitrée et une porte de communication afin de faciliter les échanges et le travail collaboratif.

L'équipement du poste de sécurité central devra être équipé :

1/ d'une alimentation électrique (220 volts) sur une ligne d'alimentation séparée, dédiée, avec courant secouru par des onduleurs pendant 4 heures au moins. Prévoir également deux éclairages halogènes d'appoint et un éclairage (ampoules) de qualité « lumière du jour », avec variateur d'intensité,

2/ d'un chauffage principal + un chauffage autonome en cas de panne, avec une réversibilité climatisation pour les périodes de forte chaleur,

3/ de prises et connexions : sur plot central courant sur les postes de travail, rétractable et sécurisés (résistance à l'arrachage) avec plusieurs RJ 45, plusieurs prises téléphoniques réseau classique, chargeurs de téléphone intégrés, prises libres pour PC, tablettes, imprimantes portables, etc. Prévoir un kit de rallonges multiprises (racks sécurisés) stocké,

4/ de postes de travail avec plan de travail plat, tiroir coulissant dessous pour claviers, rack de rangement de fournitures de bureau et accessoires, coulissant lui aussi, chaises de bureau à roulettes, avec repose-bras et appuie-tête pour usage intensif. Prévoir un kit de chaises pliantes, stockées sur un chariot à roulettes, facilement accessibles et déployables,

5/ d'un dispositif empêchant de voir l'intérieur du PC sécurité depuis l'extérieur (par exemple par vitre/film sans tain, fenêtres avec survitrage mercure…) et stores coulissants électriques pour « isoler » totalement la pièce. Les vitres sont de type antiblast,

6/ d'un grand tableau mural connecté et interactif + un second plus petit dans un autre endroit mural,

7/ d'un tableau d'affichage type « Velléda » mural et tableau électrique coulissant escamotable (vertical),

8/ d'écrans plats de réception vidéo et tous supports (télévision notamment). Le nombre est à définir, mais une pluralité d'écrans est recommandée en raison des fonctions diverses et partagées (communication, suivi de la main courante, report d'images vidéo, lien Skype, etc.). Voir la partie vidéoprotection pour davantage de détails,

9/ d'un accès sécurisé par sas (pas de mode libre) à la salle par lecteur de carte CPx avec authentification à deux niveaux (cf paragraphe contrôle d'accès). Prévoir un verrou intérieur pour confinement (blocage physique de la porte pour neutraliser l'accès par carte CPx et 2^{e} niveau de contrôle). Prévoir aussi un visiophone connecté avec l'extérieur de la salle et deux ou trois autres lieux stratégiques (bureau de repli, bureau du DG si besoin), bureau sécurisé de la sécurité générale, etc.. Plus globalement, les locaux doivent être compatibles aux exigences d'une zone réservée,

10/ de la téléphonie : une ou plusieurs liaisons cryptées : de et vers le Ministère de la Santé, de et vers la préfecture de police, de et vers le Samu de zone, etc. Batteries de téléphones connectées sur l'autocom. Prévoir deux lignes sécurisées séparées de l'autocom,

11/ de petit(s) coffre(s) de sécurité pour stocker le matériel sensible : coffre(s) fixé(s) sur support inamovible avec un clavier digital,

12/ d'une porte d'accès sécurisée (voir ci-dessus 9/), mais aussi rendue étanche : renforcée par une plaque de kevlar (pare-éclats et pare-balles de calibre usuel) et un isolant phonique. Pour des raisons de sécurité, ne prévoir qu'une porte d'accès à ces lieux. Mais possibilité et souhait fort de prévoir une sorte de « passe-plats » sécurisé (verre et matériaux), étanche, pour des approvisionnements/désapprovisionnements réguliers. Cela évite d'ouvrir la porte sécurisée,

13/ d'une zone de repos avec réfrigérateur de moyenne capacité intégré dans le mobilier, un four à micro-ondes, une cafetière/théière, un meuble de stockage de vaisselles et de consommables à usage unique : verres, gobelets, couverts, serviettes, papier linge type « sopalin », produits nettoyants, sacs-poubelle, contenants divers, etc. et d'une poubelle étanche pour résidus alimentaire,

15/ d'une signalétique : prévoir une signalétique (panneaux, visuel, écran électronique mural) pour avant et aussi pendant (salle occupée, merci de ne pas pénétrer sans autorisation, etc.). Attention : faire le lien avec 9/ ci-dessus,

16/ des horloges murales, au moins deux pour temps universel GMT, heure réelle GMT + 1 ou + 2,

17/ un meuble vestiaire (pour éviter que les vestes et gilets traînent sur les chaises),

18/ un second meuble avec des chasubles d'identification (chef de poste, chef d'intervention, COS, etc.) et des brassards,

19/ du matériel technique d'éclairage portable (torche grande puissance, projecteur sur accumulateur) en cas de coupure volontaire ou accidentelle de courant.

Enfin il faut prévoir une organisation de fonctionnement sécurisée pour l'entretien (ménage, poubelles), la maintenance (heures, présence d'un responsable ?), l'approvisionnement courant (présence d'un responsable aussi ?).

Afin de fluidifier la gestion de crise, le PC sécurité anti-malveillance est adossé au PC sécurité incendie. La séparation des deux sera en grande partie vitrée avec porte de communication verrouillable et de résistance supérieure.

Depuis le PC sécurité, l'ensemble des systèmes de sécurité de l'immeuble doit être pilotable y compris les différents modes de portes d'accès.

De plus, le système qui reçoit les alarmes doit être capable dans l'instant (et sans possibilité d'interprétation) de localiser le lieu où se déclenche une alarme, par exemple sur un plan.

R - Moyens à mettre en place pour limiter les actes de violence au travail (directives générales en santé du Bureau International du Travail - BIT) :

- Environnement physique :

Les caractéristiques physiques d'un lieu de travail contribuent de façon déterminante à désamorcer ou éventuellement déclencher la violence. On accordera donc une importance particulière au niveau d'exposition et à la manière dont les travailleurs, les malades et les visiteurs sont exposés à ces facteurs et à l'adoption de solutions adéquates, conformes aux lois et aux pratiques existantes, pour réduire ou éliminer tout effet négatif. Plus particulièrement :

- réduire au maximum les niveaux sonores pour éviter l'irritation et la tension parmi les travailleurs, les visiteurs et les malades,
- les couleurs utilisées seront reposantes et attrayantes,
- les odeurs nauséabondes seront éliminées
- assurer une bonne luminosité pour améliorer la visibilité dans toutes les zones, en particulier les accès, les parkings et les zones de stockage, spécialement la nuit,
- prendre des mesures pour assurer une température / hygrométrie / aération adéquates en particulier dans les zones de fortes affluences et dans les périodes les plus chaudes,
- veiller au bon entretien de toutes les structures et installations physiques,

- Accès :
  - la sécurité de l'accès au lieu de travail doit être assurée pour ceux qui arrivent et ceux qui partent,
  - réduire au minimum les zones d'accès publiques aux établissements de soins de santé,
  - placer les services de sécurité à l'entrée principale, près du passage qu'empruntent les visiteurs et les services des urgences,

- envisager avec beaucoup de précautions la recherche d'armes et effectuer des contrôles, si besoin, dans le respect des lois et pratiques locales, le but prioritaire étant d'éviter tout risque superflu,
- la réception doit être facilement reconnaissable par les malades/visiteurs, facilement accessible et visible pour les autres membres du personnel
- l'accès public au principal établissement de soins de santé doit être réglementé conformément à des protocoles convenus,
- l'accès aux salles du personnel (vestiaires, salle de repos) doit être réservé au personnel de l'établissement,
- les aires de parking du personnel doivent être situées à proximité du lieu de travail.

➢ Espace :
- l'espace entre les visiteurs et les malades doit être suffisant pour réduire les interférences personnelles et la création de tensions,
- l'espace de travail doit être suffisant pour faciliter la prestation des services,
- un espace de détente suffisant doit être prévu pour le personnel de soins de santé,
- des aires de réception spacieuses et tranquilles, avec suffisamment d'espace pour le personnel, doivent être prévues,
- des barrières de protection doivent être utilisées pour les travailleurs particulièrement exposés, et pour séparer les malades dangereux des autres malades et du public.

➢ Zones d'attente :
- des sièges confortables devront être prévus, en particulier pour les attentes prolongées,
- pour éviter l'ennui, on proposera des activités (par exemple, de la lecture, un poste de télévision, des jouets pour les enfants).

➢ Aménagements :
- le mobilier devra être disposé de façon à ce que le personnel ne se sente pas pris au piège
- dans les salles réservées aux entretiens et les zones où sont administrés les traitements de crise, le mobilier devra être réduit au minimum, léger, sans arêtes, ni angles vifs et, le cas échéant, être fixé au sol.

➢ Locaux :
- les salles de soins devront avoir deux portes de sortie ou, à défaut, être disposées de façon à permettre d'en sortir facilement,
- les salles de soins des urgences doivent être séparées des zones publiques. Sauf en psychiatrie ou lorsque les consignes des soignants sont autres, les patients sont positionnés plutôt vers le fond de la pièce et le soignant vers la porte de sortie. De manière plus globale, le trajet du soignant doit être plus court pour s'échapper que celui du patient. Un obstacle peut permettre cette différenciation

- on étudiera attentivement la possibilité de réserver une salle pour les malades caractériels, les malades ivres, les bandes rivales et les cas analogues, compte tenu cependant du fait que, dans certaines circonstances, le recours à ce moyen peut être perçu comme discriminatoire et, par conséquent, exacerber encore la situation,
- les toilettes et les zones de restauration devront être signalées par des panneaux, facilement accessibles et convenablement entretenues,
- les zones non-fumeurs et fumeurs devront être clairement reconnaissables,
- l'intimité devra être respectée autant que possible.

➢ Systèmes d'alarme et caméras de surveillance :

- des caméras de surveillance seront installées dans les zones potentiellement dangereuses,
- des systèmes d'alarme – téléphone, alphapage, radio à ondes courtes – devront être fournis aux travailleurs là où les risques sont apparents ou prévisibles pour qu'ils puissent prévenir des collègues en cas de problème,
- il est conseillé d'utiliser des systèmes silencieux pour éviter la réaction de l'agresseur. En l'absence de système silencieux, la victime évitera d'utiliser les systèmes existants avant le départ de l'agresseur pour éviter qu'il se retourne contre elle,
- un système d'intervention fiable en cas de déclenchement d'une alarme devra être prévu,
- le type de système d'alarme dépendra de l'évaluation des risques pour la zone particulière.

S – Les mesures d'alerte - attaque armée :

L'alerte

Donner l'alerte permet d'avertir le personnel, les usagers et les prestataires le plus tôt possible. Le facteur temps en cas d'attaque est primordial.

Le premier maillon de l'alerte doit se situer au niveau des accès (bâtiments, paliers et services) et notamment aux points d'entrées de l'enceinte. Les ADS, en charge du filtrage, les agents des accueils seront dotés d'un moyen d'alerte rapide (PTI/DATI/moyens de communication…), même s'il est impossible de passer un message clair. Tous les téléphones de l'hôpital disposeront d'une touche d'alerte rapide (par exemple en appui long), reliée au PC sécurité. Le logiciel recevant l'alerte devra indiquer immédiatement sur un plan le lieu de l'alerte. La personne recevant l'alerte ne doit pas avoir besoin d'interpréter l'information pour agir.

Ces zones devront être sous vidéoprotection de type « ambiancement » pour effectuer une levée de doute et se rendre compte de la situation, quel que soit le cas.

Le cas échéant, une collaboration étroite devra être mise en place entre les services de sécurité antimalveillance et incendie pour la chaîne d'alerte et de réactions (évacuation générale…). La configuration des PC préconisée plus haut permet cette organisation.

T - Electricité courants faibles, autres spécificités :

Tous les réseaux courants faibles doivent être de type IP sauf

- le réseau des systèmes de sécurité incendie,

Ce sont :

- les réseaux de communication pour la voix, l'image et les données issus de tous les systèmes numériques en capacité à se raccorder à un réseau (SIH, biomédical, domotique, contrôles de processus et de supervision, automates…) ; (cf chapitre système Voix Données),
- les bornes WiFi (étude de couverture à la charge du maître d'oeuvre),
- la gestion des files d'attente,
- l'appel malade, appel d'urgence,
- la téléphonie sans fil (WiFi)
- la géolocalisation
- les systèmes anti-rapt ou anti-fugue
- le contrôle d'accès,
- l'alarme intrusion et anti-agression,
- la vidéo surveillance,
- l'interphonie,
- la télévision,
- les horloges,
- la sonorisation,
- la gestion des salles de réunions et des salles de consultations,
- la téléphonie IPBX et postes téléphoniques
- les équipements visioconférence et de téléconférence
- la vidéo sur IP
- tous les paramétrages et programmations des équipements à charge de la MOE (cf paragraphe « limites de prestations courants faibles »).

Généralités

Protection de licence matérielle et/ou logicielle

Les systèmes de protection de licences logicielles par « dongle » sont à proscrire ; ainsi que l'usage de clés de licences indexées sur des adresses IP, adresses Mac…. Dans tous les cas les éventuelles protections de licences logicielles permettent au minimum une continuité de fonctionnement totale de 30 jours en cas d'absence de « protection de licence » sur les matériels en production, peu importe la raison.

Sonorisation

L'ensemble du bâtiment dispose de haut-parleurs permettant de diffuser en tout point, depuis le PC sécurité, un message parlé diffusé par micro ou par un fichier préenregistré. Le dispositif devra être activable par zone ; un bâtiment constituant une zone.

Orientation et traçabilité du patient IP

Ce système permet de localiser, en temps réel, le parcours de soins du patient (tags RFID), de la personne en fugue, de la personne désorientée et d'un enfant sur l'ensemble du bâtiment.

La détection est réalisée à travers le système RTLS global du site ou grâce au réseau WiFi.

L'alarme et la localisation du patient s'effectuent sur le PC de l'unité de soins du service concerné, ainsi que vers le PC Sécurité. Ce type d'alarme enclenche un enregistrement (de bonne qualité) des caméras de vidéosurveillance concernées pour l'exploitation des images.

Les données de localisation du patient doivent être aussi transmises en temps réel au SIH pour mettre à jour son dossier (positionnement en chambre, etc.).

L'architecture prévue est hébergée sur le réseau IP.

Le serveur redondant est installé en salle informatique générale.

En complément de la géolocalisation des patients, le maître d'œuvre doit intégrer un système permettant de géolocaliser les équipements appartenant au centre hospitalier. Ces équipements pourront être de tout type : équipements médicaux, lits, fauteuils roulants, TV, …).

PTI / DATI / Rondier (Protection du Travailleur Isolé/Dispositif d'alarme pour Travailleur Isolé)

Le système PTI/DATI permet de localiser les personnes travaillant seules ou en secteur particulier au travers d'un système dédié. Il est couplé au réseau WiFi (téléphonie IP, géolocalisation), avec localisation extérieure par GPS (et géolocalisation WiFi), localisation intérieure par géolocalisation WiFi 3D. Compatible avec les services de télésurveillance.

Ce système permet également d'assurer les rondes des agents de sécurité et de sûreté. Le tag de reconnaissance rondier doit être intégré aux terminaux IP multiservices, équipés de tag RFID. Les puces de contrôles infalsifiables sont du type sans contact, elles sont installées après étude par le maître d'œuvre des cheminements sûreté / sécurité du bâtiment.

L'alarme et la localisation du travailleur s'effectuent sur la base des plans du bâtiment visualisés sur le PC du PC Sécurité et renvoyés à un télésurveilleur. Il en est de même pour le rondier qui est exploité sur le même poste.

Détection :

Secteur non sensible sera de 5 mètres près sur l'ensemble du bâtiment,

- Pour le secteur sensible, le PTI sera associé à des récepteurs RFID WiFi implantés dans chaque local et interconnectés sur le réseau WiFi,

L'ensemble des alarmes remonte sur les postes téléphoniques IP (fixes et mobiles).

Zones sous PTI secteurs sensibles permettant une localisation fine par local :

- les services logistiques,
- la stérilisation, la pharmacie, le plateau de biologie médicale, l'EFS
- les urgences,
- le hall principal,
- les salles informatiques générales et cœurs de réseaux,
- Tous les locaux techniques électriques, fluides,
- Les groupes électrogènes,
- Les vides sanitaires et galeries techniques.

Les terminaux IP multiservices doivent permettre la gestion de l'appel d'urgence, la perte de verticalité, l'absence d'acquittement et l'arrachement. Ils sont adaptés aux travaux des personnels les possédant (personnels hospitaliers, agents de sûreté) (IP, IK) et sont munis d'un système d'accrochage. Ils sont équipés d'accumulateurs rechargeables.

L'embase principale multicanal de communications avec microphone de table est prévue au PC Sûreté.

Des postes avec phonie sont réservés aux sapeurs-pompiers.

La couverture devra être de 100 % des bâtiments et des extérieurs.

Le serveur redondant est installé en salle informatique générale.

Systèmes de communications

Téléphonique

Les cabines des appareils élévateurs sont équipées de système de communication et d'alarme avec l'intercommunication cabine / poste de sécurité en phonie tout IP et de remontée d'alarmes. Les protocoles à utiliser doivent être de type SIP normalisé.

X – BIBLIOGRAPHIE :

- Guide méthodologique « La prévention des atteintes aux personnes et aux biens en milieu de santé » - ministère chargé de la Santé – DGOS.
- Guide de déclinaison des mesures de sécurisation périmétriques et bâtimentaires – Les Ministères sociaux.
- Projet de construction de l'Hôpital Universitaire du Grand Paris Nord – Tome 1 et 2.
- Directive générale du Bureau international du travail (BIT) sur la violence au travail dans le secteur de la santé – 2002.
- Guide d'aide à la réalisation d'une ESSP.
- Instruction N° SG/HFDS/2016/340 du 4 novembre 2016 relative aux mesures de sécurisation dans les établissements de santé du 16 novembre 2016.
- Prescriptions de sûreté de la Préfecture de Police.

GLOSSAIRE

ANSSI : Agence Nationale de Sécurité des Systèmes d'Information

CNIL : Commission Nationale de l'Informatique et des Libertés

CPS/CPE :

CPx :

CQP-APS : Certificat de Qualification Professionnelle – Agent de Prévention et de Sécurité

ESSP : Etude de Sûreté et de Sécurité

MADA : Matières Dangereuses

MOA : Maître Ouvrage A

PCS : Poste Central de Sécurité

PSE : Plan de Sécurité Etablissement

PTI : Protection du Travail Isolé

RBC :

SAIV : Sécurité des Activités d'Importance Vitale

SOPS de la PP : de la Préfecture de Police

SPPAD de la PP : de la Préfecture de Police

UGCIS : Unité de Gestion Centralisée des Issues de Secours

VIP : Very important person (personne très importante)