

Notes sur les dispositifs techniques sûreté

1 Périphérie du bâtiment :

Si un espace de type parvis piétons est créé, il faudra prévoir des protections pour protéger les piétons contre les véhicules lancés.

Ces protections peuvent être de type bornes anti véhicule béliers, ou la mise en place de mobilier urbain avec un fort niveau de résistance.

Les abords du bâtiment devront être équipés d'éclairage public de type détection automatique et ceux jusqu'au parking le plus proche.

L'éclairage extérieur couvrant une zone équipée de caméra devra être d'une puissance de 20 lux minimum.

L'accès au bâtiment depuis les fenêtres du rdc doit être impossible (barreaudage, blocage des fenêtres), le vitrage devra être aux normes anti vandale.

L'accès aux terrasses et toitures devront être sécurisées.

Ne pas prévoir d'empierrement qui pourrait être utilisé comme projectile dans des espaces verts, parvis extérieurs.

Si des locaux techniques extérieurs sont créés (centrale gaz médicaux, etc..), prendre en compte la menace liée au sabotage des installations et mettre des dispositifs techniques de protection.

2 – Gestion des accès et organigramme des clés

Tous les accès périmétriques du bâtiment seront équipés de contrôle d'accès, y compris les accès liés à la liaison de communication vers le BMC.

Le système de contrôle d'accès par badge (carte CPS 3- Mifare -Desfire) devra être compatible avec le logiciel existant : VAUBAN

Un visiophone devra être prévu à l'entrée principale du bâtiment, il devra comporter autant de bouton d'appel que de service (à voir la nécessité de maintenir ce dispositif suivant le fonctionnement du bâtiment, peut-être les prévoir aux entrées de service à chaque étage si celles-ci sont sécurisées).

En complément de l'ensemble des accès périmétriques du bâtiment, chaque entrée des différents services, l'ascenseur et les locaux sensibles et abritant des valeurs (pharmacie, locaux de soins, informatique, matériel médical...) devront eux aussi être équipé de contrôle d'accès par lecteur de badge.

Pour les locaux sensibles, les vestiaires, le contrôle d'accès se fera en entrée et en sortie.

Le système proposé devra obtenir l'aval du service informatique concernant la sécurité du SI.

Un organigramme des clés définissant les autorisations d'accès en fonction des catégories de personnel, des différents services et de l'affectation des locaux et du nombre de personnes habilitées à y pénétrer devra être réalisé.

Cet organigramme devra prendre en compte les organisations en place (locaux techniques sur les cylindres « BCHK 05 » et les issues de secours sur les cylindres « SECURIT » existants)

Les locaux identifiés avec contrôle d'accès et équipés d'une serrure devront avoir une variure spécifique (cylindre « SECURIT » existant au sein du CH).

Les serrures auront la certification A2P dans tous les cas.

Précision : les portes permettant de sécuriser le bâtiment ou les services, mais qui sont aussi des issues de secours ou qui se trouvent dans les circulations seront asservies à la détection incendie, ce qui ne sera pas le cas des locaux (principe à retenir dans le cahier des charges SSI)

3 – Alarme intrusion

Il conviendra de mettre en place des moyens qui permettent d'éviter des intrusions lorsque le bâtiment est fermé. Pour ces derniers, l'objectif étant d'éviter l'intrusion de personnes extérieures.

Si le dispositif choisi est une alarme intrusion celle-ci devra être compatible avec le système de contrôle d'accès.

La supervision des alarmes devra être centralisée au PC sécurité du site, les plans de localisation étage par étage devront être inclus dans le logiciel afin d'apparaître sur écran en cas d'alarme.

Nota : l'alarme intrusion est utile uniquement si le bâtiment n'a pas d'activité la nuit, dans le cas contraire, elle sera inutile.

4 – Vidéoprotection

Conformément à l'étude de sureté du PSE du bâtiment, les accès au bâtiment seront équipés de caméra de vidéoprotection anti vandale sur chaque entrée, ces caméras visionneront en champ étroit pour privilégier l'identification.

L'arrière du bâtiment donnant sur la cours logistique de l'Allurad devra être équipé de caméras qui visionneront en champ large, idem si un espace de type parvis piétons ou parking sont créés.

L'extension vidéo devra tenir compte du système existant du CH (marque Millestone) et une étude devra être réalisée afin de vérifier le matériel d'extension nécessaire (serveur, licence, etc..).

Ne pas prévoir de végétation pouvant dans un futur réduire la visibilité du champ de vision des caméras.

5 – Protection contre les intrusions et attentats et le risque Agression

Dans le cadre des mesures nationales du plan VIGIPIRATE, et du PSE (Plan de sécurisation de l'établissement) chaque niveau doit comporter au minimum un local sécurisé par contrôle d'accès et doublé d'une serrure mécanique, ce local sera précisé avec le maître d'ouvrage.

Un système de diffusion de l'alerte attentat sera prévu, le fonctionnement du système sera conforme aux prescriptions du PSE, la diffusion sera de préférence par signaux visuels lumineux couvrant la

totalité des locaux et actionné par déclencheurs manuels accessible rapidement par le personnel du bâtiment.

Le système choisi devra permettre un retour d'information au PC sécurité.

Concernant le risque d'agression du personnel, il faudra envisager d'équiper l'accueil du bâtiment d'un bouton d'appel urgence Agression reporté au PC sécurité du CH (il faudra reprendre ce dispositif sur le système existant au CH – Logiciel de marque DMR Alert - marque AXIANS)