

## SECURISATION

La Région Occitanie a acté à l'**Assemblée Plénière du 19 novembre 2020** un plan régional de prévention, de sensibilisation et de protection vis-à-vis des violences dans les lycées et les transports régionaux. La Région mobilisera un budget de 30M€ en 2021 et 2022.

Le référentiel suivant indique les points principaux de la sécurisation d'un lycée.

### 1. Niveaux de sécurisation

Niveau 1 : Clôture périphérique / PPMS

Niveau 2 : Vidéo Protection / Contrôle d'accès / Tourniquet

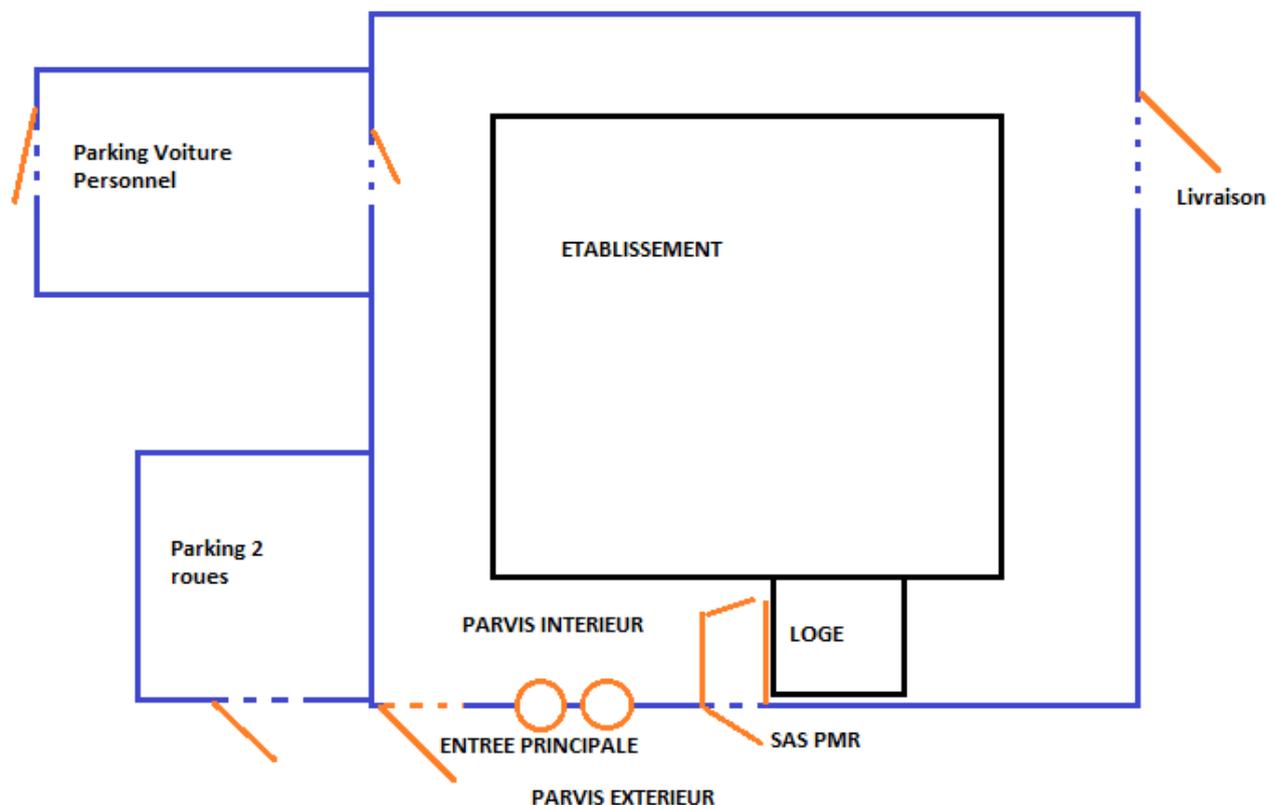
Niveau 3 : Alarme Intrusion

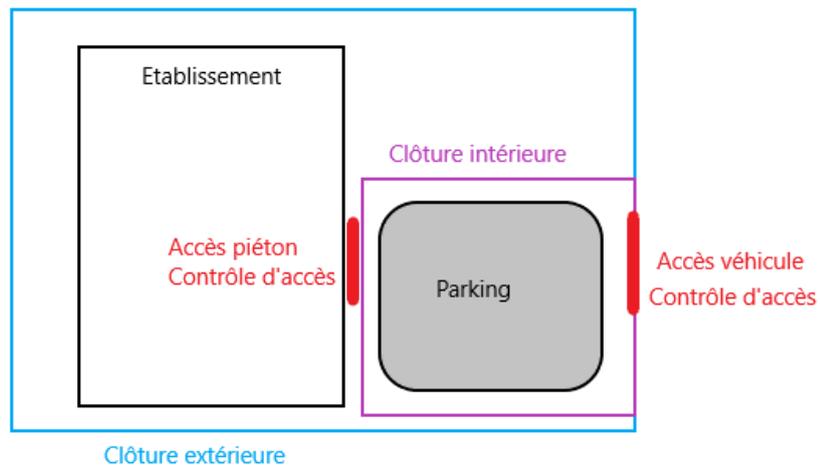
### 2. Clôture

La clôture doit être installée sur le pourtour de la parcelle du lycée sur une hauteur de 2m. Elle doit être fermée et homogène sans facilitateur d'escalade.

Il ne doit pas y avoir de visibilité depuis les voies publiques vers la cour ou dans l'établissement (pour les bâtiments en limite de propriété).

Les parkings intérieurs seront également sécurisés par une clôture intérieure.





### 3. Accès

Le nombre d'accès à l'établissement doit être limité. Dans l'idéal, il faut réaliser un seul accès par typologie de flux (véhicule, piéton, 2 roues). Les accès piétons doivent être séparés des accès véhicules et des accès vélo/2 roues.

Tous les accès à l'établissement doivent être équipés de portail, barrière ou tourniquet afin d'éviter l'intrusion des personnes non autorisées. Ils doivent tous être visibles et contrôlés depuis la loge soit :

- Directement pour l'entrée principale
- Par visiophone et caméra de surveillance pour les accès plus éloignés comme ceux des livraisons, véhicules personnels

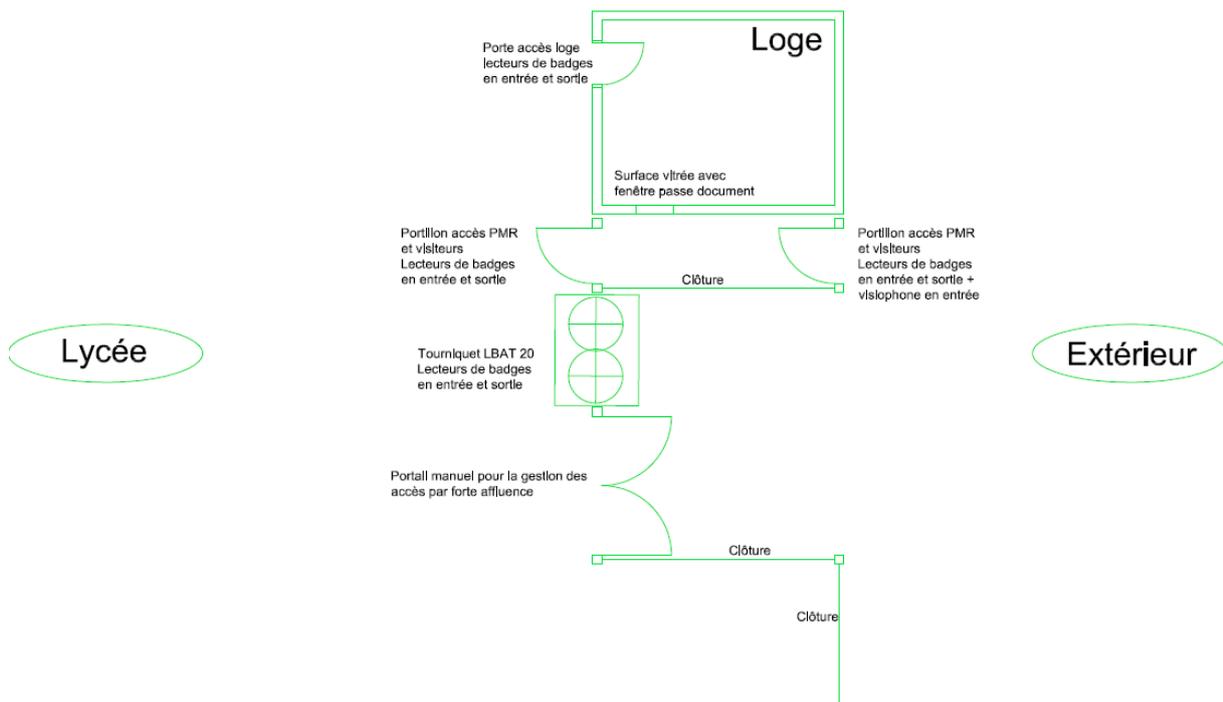
L'entrée principale élève sera équipée :

- d'un portail manuel grand flux pour les entrées sorties aux heures de pointe
- de tourniquets permettant d'accéder aux lycées par contrôle d'accès avec la carte jeune
- de 2 portails électriques (SAS) passant devant la loge pour les accès handicapés et visiteurs

Les entrées secondaires élèves seront équipées uniquement de tourniquets avec contrôle d'accès.

Les entrées voitures/livraison seront équipées de portail ou barrière avec fermeture rapide pour éviter l'intrusion de plusieurs véhicules en même temps, et de dispositif évitant l'intrusion humaine par-dessus (ou dessous).

Pour les bâtiments en limite de propriété, des tourniquets ou portails type accès métro pourront être installés dans le hall. Un travail doit être réalisé sur le niveau sonore des équipements.



#### 4. PPMS

Le Plan Particulier de Mise en Service permet à l'établissement d'alerter les occupants de risques divers (Attentat, intrusion extérieure, feu de forêt, inondation, tempête, séisme, accident industriel, ...) grâce à 3 types de son d'alarmes distincts de l'alerte incendie et des messages parlés indiquant les procédures à suivre (confinement, évacuation, autre, ...) :

- Risque majeur (confinement)
- Attentat-intrusion (confinement - avec possibilité d'alerte silencieuse via téléphone)
- Fin d'alerte
- Evacuation (correspondant au son de l'alerte incendie)

Le système doit être équipé de :

- Hauts parleurs dans tous les espaces permettant la diffusion de messages intelligible partout
- Déclencheurs équipés de micros dans minimum 2 points de déclenchement (loge et proviseur a minima)
- Déclencheur boîtier à code réparti dans l'établissement
- Flash ou gyrophare distinct du rouge (SSI) dans les locaux bruyants ou isolés (sanitaires)

Les équipements du système PPMS peuvent être utilisés également pour la sonnerie intercourts.

Sur certains sites et en accord avec les pompiers, les équipements du SSI (hauts parleurs) peuvent être utilisés par le système PPMS → Système SSS

En annexe les différentes technologies utilisées.

## 5. Contrôle d'accès

Le contrôle d'accès permet d'ouvrir des portes, portails, tourniquet à l'aide d'un badge ou d'une clé électronique.

Le contrôle d'accès par digicode est proscrit sur tout l'établissement.

Le contrôle d'accès doit être déployé a minima sur :

- Tous les accès extérieurs (tourniquet, portails, barrières) permettant d'accéder à l'enceinte du lycée. Un visio phone sera également installée sur les accès parking et livraison.
- Toutes les portes de l'établissement donnant sur l'extérieur
- Les locaux à risque et nécessitant une surveillance particulière à identifier avec l'établissement (local serveur, chaufferie bureaux gestionnaire, proviseur, ...)

Pour les élèves, l'accès se fera grâce à la carte jeune en lecture seule (pas d'écritures sur le badge).

Les contrôle d'accès des portes extérieures seront raccordées en filaire.

## 6. Vidéo Protection

La vidéo protection permet de surveiller les accès de l'établissement. Elles doivent être correctement positionner pour ne filmer que les accès et non les extérieurs. Les points à visionner a minima sont :

- Accès livraison
- Entrée principale en favorisant la vision sur les tourniquets et le SAS handicapé
- Parking professeur
- Parking 2 roues

L'écran de surveillance sera positionné à la loge afin de visualiser l'ensemble des accès sur un même écran.

Un déclaration de la Commission Nationale de l'Information et des Liberté (CNIL) est à fournir par le prestataire.

## 7. Alarme Intrusion

L'alarme intrusion permet de déclencher une alarme en cas d'intrusion d'une personne non autorisée.

Cette alarme pourra être connectée envoyée à une société spécialisée dans l'intervention de sécurité ou non.

L'ensemble des composantes du système anti-intrusion devra être conforme à la norme NF A2P type 3 (3 boucliers) et ou à la norme EN50131 Grade 3.

L'alarme doit être associée à des zones de protection. La constitution de ces zones doit être réalisée en concertation avec l'établissement. Privilégier les zones physiques (bâtiment A) aux zones fonctionnelles (Administration). Le nombre de zone doit être limité de 2 à 4.

La quantité de détecteur et d'alarme devra être correctement étudiée afin de limiter leur nombre à l'essentiel. Aussi, cette protection anti-intrusion se fera principalement :

- Dans les locaux du rez-de-chaussée à proximité des ouvertures donnant sur l'extérieur,
- Dans les étages directement accessibles de l'extérieur (accès depuis toit terrasse ou accès depuis escalier).
- Certains locaux sensibles pourront également être sous alarme (bureau intendant, bureau proviseur, locaux techniques, etc.).

Il faut privilégier les détecteurs volumétriques aux détecteurs d'ouvertures sur les portes d'accès qui peuvent se détériorer plus facilement avec l'usage intense des portes. Ces derniers peuvent être au niveau des portes d'entrées du rez de chaussé.

Les internats devront eux être équipés de détecteurs de porte pour pouvoir la mettre en fonctionnement la nuit.

Les boitiers à code et/ou lecteur de badge doivent se situés à l'entrée de chaque zone (hors champs élèves) et dans la loge.

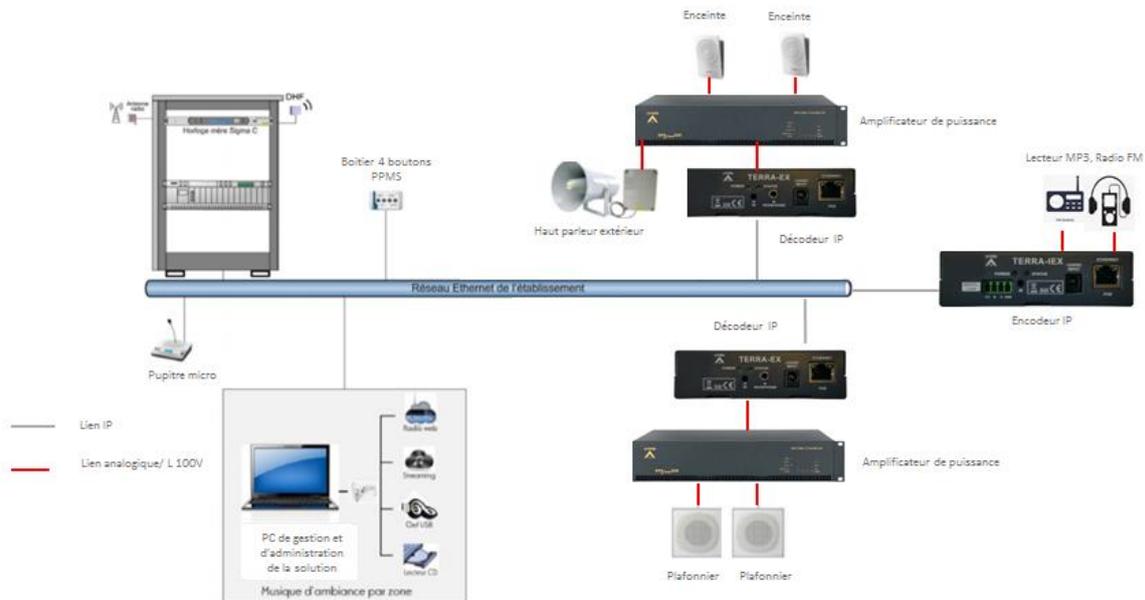
Les détails techniques sur les différents équipements sont présentés en Annexe 2.



PPMS

1. Technologie Hybride

Branchement IP du déclencheur aux switches sur le réseau ethernet (ou à travers un réseau dédié). Puis un décodeur transforme le message IP en signal électrique. Un amplificateur transforme le signal électrique en signal son analogique. Les hauts parleurs sont raccordés en série à l'amplificateur.

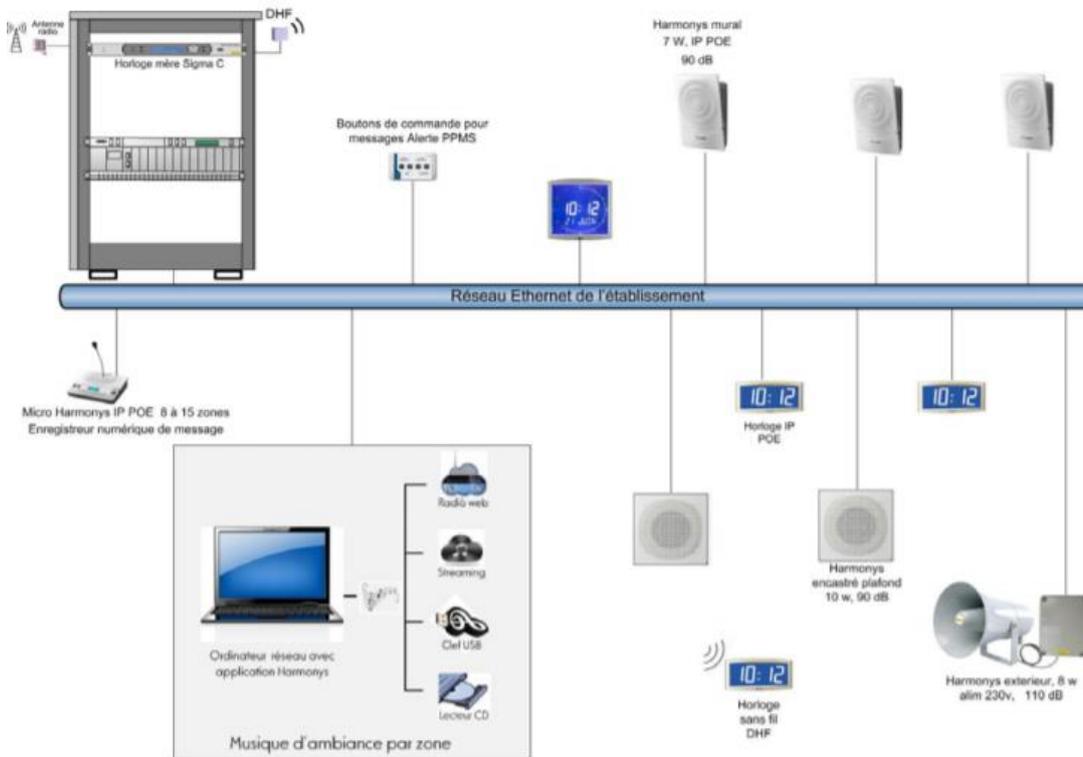


Préférer cette solution si :

- le budget ne permet pas la mise en place d'une technologie Full IP
- il y a des switches POE existants (pour le réseau WIFI notamment) mais qui ne sont pas encore raccordés au réseau (et le seront prochainement)

## 2. Technologie Full IP

Branchement IP du déclencheur aux switches POE sur le réseau ethernet (ou à travers un réseau dédié). Puis branchement IP des switches POE aux hauts parleurs. Chaque Haut Parleur est adressé par une adresse IP (et donc programmable individuellement).



Préférer cette solution si :

- il n'y a pas de switch POE et donc possibilité de les installer
- les switch POE existant sont déjà raccordés au réseau
- le budget permet la mise en place de cette technologie (2 à 3 fois plus cher qu'une solution hybride)

## 3. Technologie Radio

Transfert des données du déclencheur aux Hauts Parleur par radio.

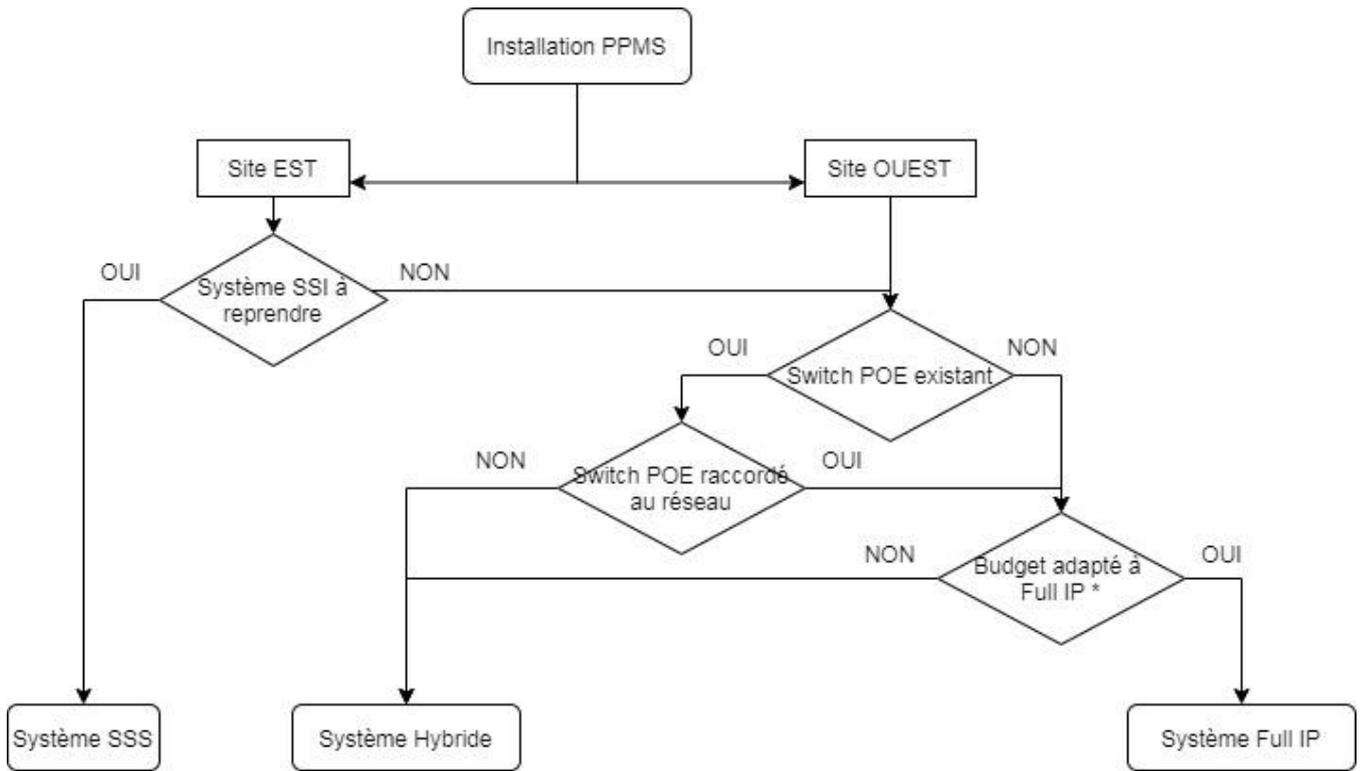
Préférer cette solution si :

- Pendant une période de travaux pour maintenir la continuité de sécurité de l'établissement
- En cas d'urgence
- Si la structure du bâtiment ne permet pas de faire circuler des câbles

## 4. Technologie analogique

Branchement en analogique du déclencheur aux Hauts Parleurs.

Préférer cette solution si le réseau ethernet actuel du site ne permet pas de supporter un système PPMS.



## 5. Equipements

### **Pupitre d'appel**

Le pupitre d'appel doit diffuser des appels généraux sur tout un site ou dans des lieux précis.

Il sera équipé d'un écran tactile pour visualiser le nom des zones d'appels.

Branchement IP.



### **Boitier de déclenchement**

Le bouton doit permettre de :

- ▶ Déclencher/Arrêter la restitution de messages audio standard ou d'alerte.
- ▶ Activer/désactiver la programmation de sonneries.
- ▶ Le boitier sera équipé de 4 boutons.

### **Amplificateur de puissance**

L'amplificateur de puissance est un boitier rackable qui s'intègre dans les baies 19". Il a une puissance variable. Il est le relais entre l'encodeur et les hauts parleurs

### **Encodeur**

L'encodeur permet de transformer un analogique (signaux électrique) en IP. Uniquement présent sur les technologies hybrides, il fait le lien entre les boitiers ou pupitres analogiques au réseau IP.

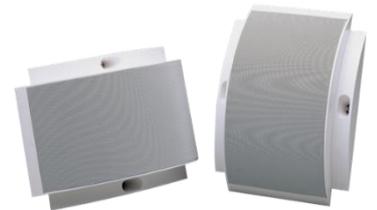
### **Décodeur**

L'encodeur permet de transformer un message IP en message analogique. Uniquement présent sur les technologies hybrides, il fait le lien entre les connexions IP et les connexions électriques.

### **Haut-parleur**

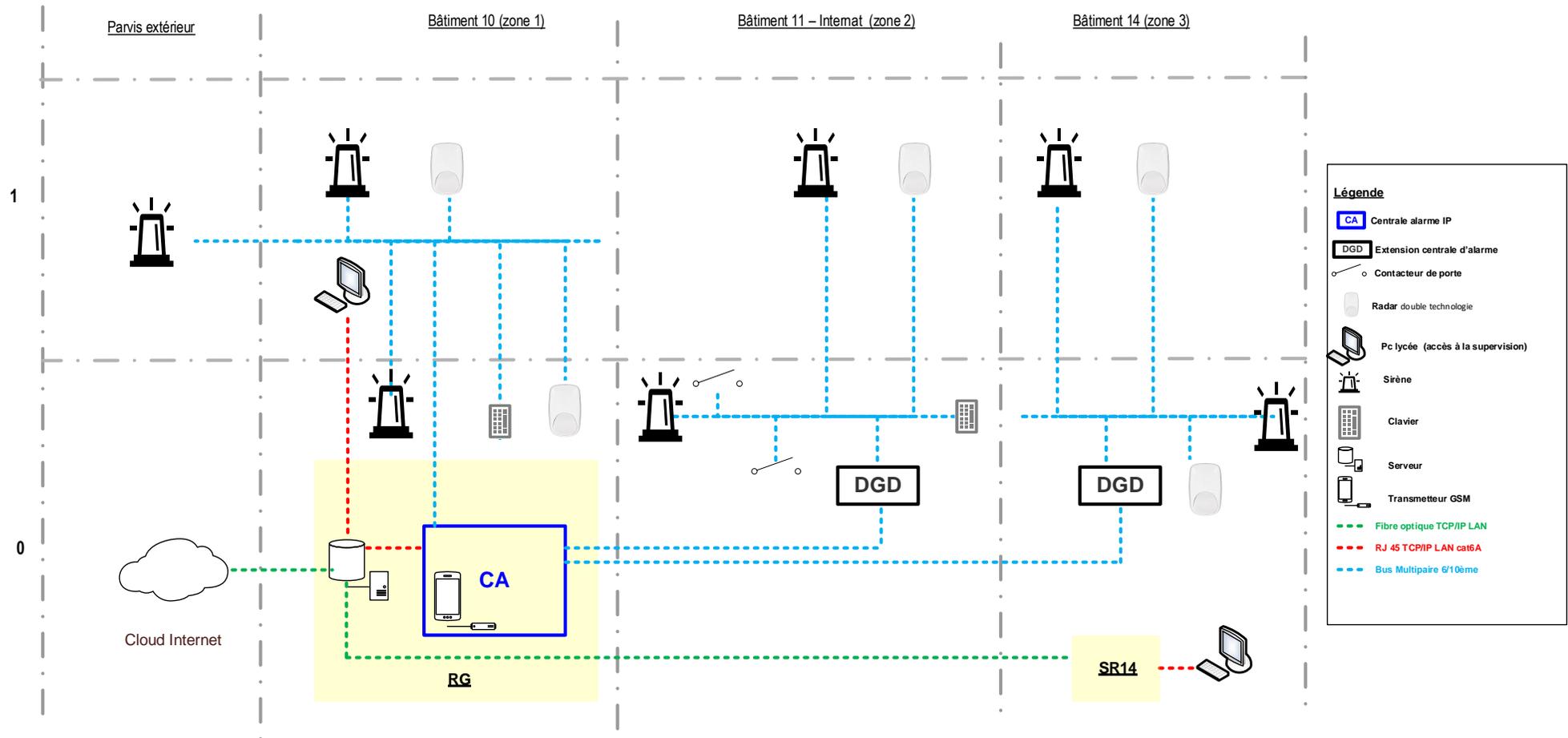
Les haut-parleurs seront Ip ou analogique en fonction de la technologie choisie.

Le haut-parleur IP devra permettre de stocker les sons afin que seul l'impulsion de déclenchement du son soit envoyé et non le son en entier dans les bandes passantes.



ALARME INTRUSION

1. Synoptique de la solution anti-intrusion cible



Afin de faciliter la gestion quotidienne du système, un zoning simple sera déployé, correspondant principalement à 1 zone = 1 bâtiment-ensemble de bâtiment. La gestion des zones précitées devra être possible depuis la centrale, et depuis les postes informatiques ayant accès à la supervision.

## 2. Les composantes

### Les détecteurs

Détecteur volumétrique :

Intégrés uniquement en intérieur : Circulation, entrée-hall, salle de cours avec matériel de valeur (salle informatique), bureaux administratifs, CDI, salles des enseignants, locaux techniques. Il sera fait principalement usage de détecteurs de mouvement double technologie (infrarouge + hyperfréquence) grand angle.

Détecteur d'ouverture de porte :

Intégrés uniquement en intérieur : porte d'accès extérieure en rez de chaussée, zone dortoir internat. Le nombre de ces détecteurs doit être minimisé au maximum, ils sont sensibles aux chocs et génèrent, avec le temps, de nombreux déclenchements intempestifs. (**A ne pas généraliser et à intégrer au cas par cas**)

### Les claviers de commandes

Intégrés uniquement à l'intérieur, en nombre limités de 2 à 4 en fonction de la taille du lycée, positionnés au niveau des accès principaux (**hors champs d'élèves**). Ils intégreront un lecteur de Tag-badge (possibilité de couplage avec une solution de contrôle d'accès via carte Région).

Ces équipements pourront être tactile ou manuel.

### Les sirènes

Intégrées en intérieures, elles seront principalement posées en circulation tous les 20 à 50m (fonction de la configuration du lycée), puissance sonore de 110 dB minimum à 1 mètre.

Intégrées en extérieures, elles seront souvent positionnées sur la façade au niveau de l'accès principal du lycée, avec Flash lumineux, puissance sonore de 105dB minimum à 1 mètre. (En règle générale 1 à 2 sirènes extérieures par établissement)

Elles seront auto-protégées contre l'ouverture et l'arrachement et sécurisées électriquement via une batterie permettant d'avoir une autonomie en alarme > 30min.

### La centrale intrusion

Intégrée dans le local serveur principal (Répartiteur général), local sécurisé et rafraîchi. Elle sera secourue et régulée électriquement (électricité non soumise à des pics de tension), positionnée au mur, auto-protégée contre l'ouverture et l'arrachement. Elle doit intégrer un certain nombre d'entrée/ sortie, de différents types, permettant de connecter l'ensemble des composantes. (A dimensionner en fonction de la taille du lycée, une réserve de 30% à la livraison est demandé pour les éventuelles extensions)

Elle doit intégrer un transmetteur GSM pour la transmission des alarmes ; ce boîtier transmetteur doit être positionné à l'intérieur du boîtier d'alarme et doit permettre l'envoi de message type SMS et messages vocaux. Elle doit également disposer à minima de 1 port Ethernet LAN compatible avec le protocole TCP/IP. (Possibilité d'intégrer la centrale au réseau informatique du lycée et/ou à un réseau IP externe Régional)

### L'outil de supervision et d'administration

Intégré en local sur un poste ou, sur un serveur (physique ou virtuel).

L'outil doit permettre, en fonction du login - mot de passe, d'avoir accès à plusieurs niveaux de fonctionnalité pour éviter des manipulations non autorisées :

- Code utilisateur (plusieurs codes devront être possibles) : accès au module simple d'utilisation
- Code gestionnaire de site : accès à des fonctionnalités avancées de programmation (gestion de code temporaire, de zoning, etc.)

- Code personnel de maintenance : accès à l'ensemble des modules d'administration et de supervision

Il devra permettre entre autres de :

- Configurer les différentes composantes
- Etablir des diagnostics en temps réel du système
- Suivre l'historique des évènements (défaillance, mise en et hors alarme, date et heure des déclenchements, etc.)

Cet outil doit pouvoir être disponible en ligne **via un navigateur internet et ou sur une application mobile** (fonction limitée). Il doit être le plus ouvert possible pour être **interopérable avec d'autres solutions de sécurisation** du bâtiment (contrôle d'accès, PPMS et vidéo-protection).

### 3. Les liens physiques d'interconnexion et câblage associé

Pour minimiser les différents types de câblage distribués dans les bâtiments, les liaisons entre les PC du lycée, la centrale intrusion et le serveur seront réalisées en utilisant le câblage banalisé (VDI) du lycée, au travers d'un câble 4 paires catégorie 6A F/FTP ou éventuellement d'un lien optique (lien inter-bâtiment).

Le câblage entre les différents composantes-interfaces et la centrale sera réalisé au travers d'un Bus, câblé en 6/10ème multipaires. Il devra cheminer sur des chemins de câbles courants faibles, tube IRL et sous gaine ICT. En aucun cas, les câbles seront posés sans support.

Le raccordement de chaque composante sera réalisé sur bornier vissé, intégré aux différentes composantes. Aucun câblage - raccordement ne sera laissé en apparent ou accessible dans les plafonds.

### 4. Les services attendus

Le prestataire devra une formation par profils de personnels (minimum 3 profils) sur le système et l'outil de supervision-administration :

- Personne de maintenance : recherche de panne, gestion complète de la solution
- Personne administratif : paramétrages simples du système (activation de zone spécifique, création de code temporaire, etc.), analyse des événements dans l'historique
- Personnel de loge-gardien : mise en et hors alarme, gestion quotidienne de la solution

Cette formation devra être accompagnée pour chaque module, d'un guide utilisateurs/fascicule spécifique pour chacun des 3 profils dictés ci-avant.

La documentation à fournir dans le cadre du dossier des ouvrages exécutés devra à minima intégrée :

- Les plans d'implantation avec notamment, la localisation, le repérage, numéro d'identification de chacune des composantes du système
- Les documentations techniques des équipements
- Les codes et mots de passe du système afin d'assurer une réversibilité en cas de changement de mainteneur