

7.4.3. COURANTS FAIBLES - SURETE ACTIVE

7.4.3.1. Réseau sûreté

A. Performances générales

Les systèmes de sûreté active utilisent un réseau sûreté dédié, physiquement dissocié des autres réseaux informatiques et courants faibles de l'établissement. Les systèmes de sûreté sont des systèmes ouverts, communiquant via le protocole standard IP.

La conception du réseau sûreté répond aux exigences suivantes :

A.I. Exigences de sécurisation du réseau sûreté

Il est demandé une continuité de service (aucune interruption admissible), sans dégradation de performance, en cas de défaillances suivantes :

- Rupture d'un lien physique (brin de fibre optique ou câble) : le cheminement des informations s'effectue sur un circuit de secours,
- Panne d'un équipement actif : les serveurs et postes clients rattachés à l'équipement actif défectueux sont routés automatiquement sur un équipement actif de secours.

Par ailleurs, la création de VLAN de niveau 2 par applicatifs est exigée :

- VLAN Vidéosurveillance/Archiveurs
- VLAN Supervision sûreté, Gestion des accès, alarmes et contrôle d'accès
- VLAN Interphonie (Cellule, Liaison et sûreté)
- VLAN Système de reconnaissance des personnes détenues
- VLAN GTB
- VLAN Sonorisation
- VLAN Administration-réseau.

Enfin, hors enceinte, un dispositif de reconnaissance est mis en œuvre sur chaque entrée/sortie des équipements actifs de sûreté, de sorte à empêcher toute tentative de connexion au réseau sûreté, via ces terminaux.

A.II. Exigences de supervision du réseau

La mise en place d'un outil de supervision du réseau permet un diagnostic rapide des dysfonctionnements des composants du réseau sûreté. Il fournit une alarme de synthèse à l'hyperviseur de sûreté, pour alerter le surveillant du PCS, au plus tôt. Les postes opérateurs ayant accès au réseau Sûreté sont équipés d'un dispositif de protection mise à jour régulièrement afin de garantir l'intégrité du système et être protégés.

A.III. Exigences de temps de réponse

Le dimensionnement du réseau sûreté permet d'atteindre les temps de réponse exigés au niveau des systèmes de sûreté active décrits ci-après.

B. Prescriptions

B.I. Réserves

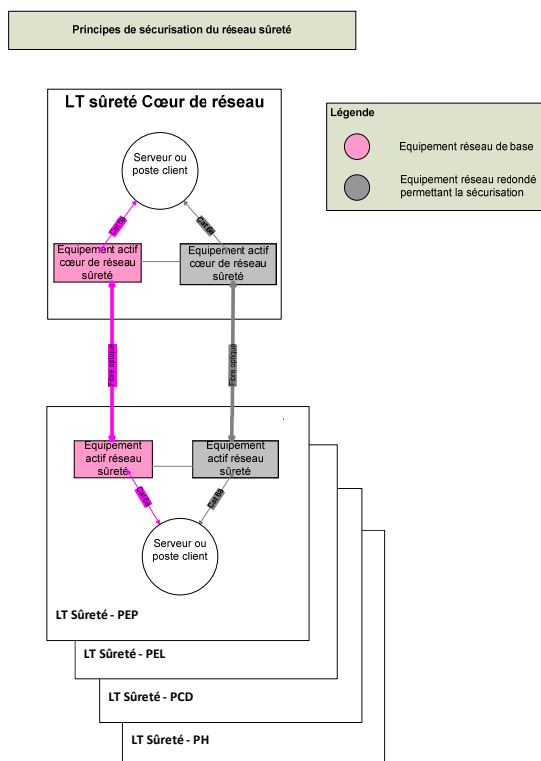
Il est exigé une réserve de 30 % sur tous les câblages réseaux.

B.II. Architecture de réseau sécurisé

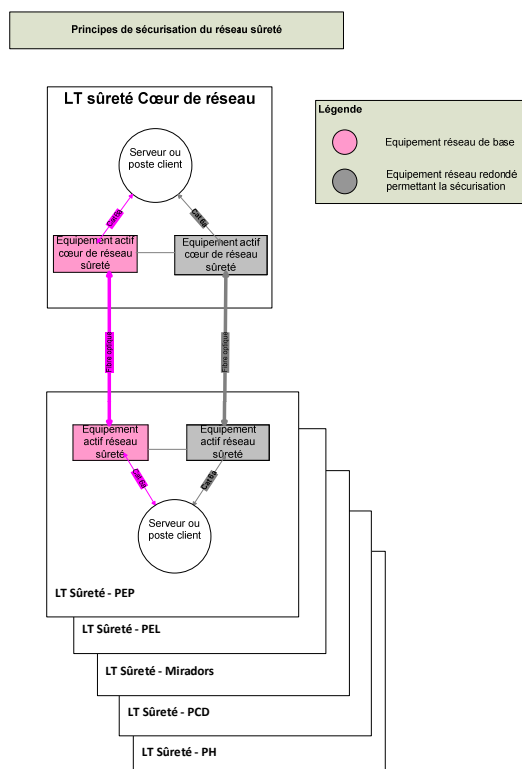
- Mise en œuvre d'un réseau fibre optique redondé, ce qui permet la continuité de service en cas de rupture d'une fibre optique, tout en garantissant un encombrement minimum des flux de données sur les liaisons.
- Double attachement des serveurs et des postes clients sur des équipements actifs distincts du réseau sûreté, ce qui permet la continuité de service en cas de défaillance d'un équipement actif du réseau ou d'un câble de liaison entre l'équipement actif et le serveur / poste client.

Les schémas suivant illustrent l'architecture du réseau prescrit.

Etablissement à sûreté adaptée :



Etablissement à sûreté renforcée :



Les ports libres des équipements actifs devront être désactivés.

B.III. Postes d'exploitations

Les postes d'exploitation des systèmes de sûreté, utilisés par les surveillants et autre personnel de l'établissement, sont dédiés exclusivement à l'exécution des logiciels applicatifs de sûreté.

Les postes d'exploitation des systèmes de sûreté sont sécurisés selon les règles de l'art : protection antivirale, restriction des flux réseaux nécessaires.

Sont notamment rendus impossibles :

- Tout accès à des fonctions Windows ou applications tiers ;
- Les accès débridables aux périphériques d'entrée/sortie.

Les écrans de veille sont monochromes.

Tous les écrans affichent la même heure et la même date le tout synchronisé par un serveur NTP. Le mode d'affichage kiosque (mosaïque) est à mettre en œuvre.

Les unités centrales des postes informatiques du poste protégé sont rackées au sein de la baie sûreté du local technique.

B.IV. Applications

Les applications sont hébergées sur des serveurs situés dans les locaux techniques dédiés à cet effet et accessibles depuis des postes clients déportés. Une gestion des sauvegardes des événements spécifiques à chaque système est mise en œuvre afin de pouvoir assurer la disponibilité des informations en cas de défaillance du système.

Les applications tierces fonctionnent, et les utilisateurs n'ont pas « les droits administrateur » du système d'exploitation.

Les programmes sources des applications développées spécifiquement pour la gestion de la sûreté des établissements sont audités avant d'être installés. Cet audit ne peut pas avoir lieu après la mise en service.

C. Proscriptions

C.I. Postes d'exploitation

- L'affichage de marque de fournisseur est interdit sur les écrans d'affichage vidéo.
- Les publicités sont interdites sur les écrans de veille (marque fournisseur par exemple).
- Les postes informatiques ne seront en aucun cas hébergés dans des baies techniques non prévues à cet effet (baie « VDI », baie « sensible »).

D. Supervision sûreté : périmètre de référence des postes protégés

Le tableau suivant présente de manière générique le périmètre de couverture en termes de supervision sûreté (vidéosurveillance et alarmes de sûreté) de chaque poste protégé par unité fonctionnelle et par zone.

*Les zones s'entendent ainsi :

- Extérieur : espace extérieur rattaché ou interne au fonctionnement d'une UF (ex : cour du greffe pour le Greffe, cour de promenade pour un quartier d'hébergement, patio pour les UVF, etc.)
- Intérieur : au sein du bâtiment accueillant l'UF
- Abords : abords immédiats au niveau de l'entrée à l'UF et zones interstitielles au sein du périmètre de l'UF

**Le poste protégé de référence doit pouvoir accéder à l'ensemble de la supervision sûreté couvrant le périmètre de la zone concernée : accès aux caméras pour affichage vidéo à la demande et information des remontées d'alarmes de la zone.

Un travail sera réalisé en phase études avec l'ergonome de la DAP pour préciser par zone le périmètre et les tâches de chaque poste protégé.

Pour rappel, en tant que poste d'hypervision de la sûreté, le PCS a accès à l'ensemble des systèmes de sûreté du site.