

**DEMANDE DE FINANCEMENT GRACE AU FONDS SPECIAL  
DU CONSEIL DE DIRECTION :  
B. MISES A NIVEAU DES SYSTEMES DE SECURITE DES LOCAUX DU CIRC**

## **CONTEXTE**

1. Au cours de 2015, l'attaque de Charlie Hebdo à Paris en janvier puis les attaques coordonnées dans la ville le 13 novembre ont eu un retentissement international. On a accordé moins d'attention à ce qui s'est passé à seulement 30 km du CIRC, sur le site de l'entreprise de notre fournisseur d'azote liquide, à savoir l'explosion d'un véhicule et une exécution de type terroriste. Depuis ces événements, la France a sensiblement relevé ses mesures de sécurité dans tout le pays et tout particulièrement dans les lieux considérés comme des cibles potentielles.

2. Même si les autorités françaises n'ont pas identifié les locaux de l'Organisation des Nations Unies (ONU) comme des zones à haut risque, en 2015 l'Equipe de coordination du dispositif de sécurité de l'ONU pour la France a établi quatre priorités pour toutes les Agences de l'ONU en France :

- 1) Revoir le contrôle de l'accès aux locaux des agences de l'ONU et renforcer la sécurité ;
- 2) Mettre en place un système efficace permettant de contacter tous les membres du personnel dans chaque Agence, de façon à pouvoir les dénombrier en situation d'urgence ;
- 3) Définir clairement un point focal pour la sécurité au sein de chaque Agence ;
- 4) Rappeler à tous les membres du personnel qu'ils sont responsables de leur propre sécurité et de celle de leur famille, et leur fournir des informations dans la mesure du possible.

3. Le CIRC a suivi ces recommandations à la lettre, et renforcé la sécurité de son siège à Lyon. Le CIRC s'est signalé auprès des Services de sécurité de la Préfecture et des autorités locales de police et a déjà travaillé étroitement avec eux tout au long de l'année 2015, ce qui a permis d'établir des contacts directs et adaptés. Les mesures de sécurité ont été renforcées, notamment par le contrôle de tous les visiteurs et l'inspection de leurs effets personnels.

4. A la suite des attaques terroristes de novembre, le contrôle des accès a été renforcé avec la mise en place de nouvelles règles d'accès dans l'enceinte du CIRC pour les piétons et les véhicules. Le système d'alarme par SMS existant a également été amélioré pour permettre au personnel de répondre aux messages d'alerte, dans les situations d'urgence, en donnant des indications sur l'endroit où ils se trouvent et sur leur niveau de sécurité, pour eux-mêmes ainsi que les personnes reconnues à leur charge.

5. Parallèlement, pour pouvoir établir un plan efficace d'amélioration de la sécurité, le Secrétariat du CIRC a décidé de faire procéder à plusieurs audits pour déterminer le statut effectif de la sécurité physique du CIRC :

- Audit interne du niveau global de sûreté et de sécurité des locaux du CIRC et des politiques et procédures en matière de sécurité ;
- Audit interne de tous les systèmes de gestion du bâtiment en temps réel, notamment des systèmes de contrôle de la sécurité (Annexe 1) ;
- Audit externe de la sûreté et de la sécurité, mené par la Police française et sa branche spéciale chargée de la sécurité publique (les conclusions de l'audit sont présentées dans l'Annexe 2).

6. Le Département de la sûreté et de la sécurité de l'Organisation des Nations Unies (UNDSS) a reconnu, dans son bulletin d'information du 28 janvier 2016, que les agences des Nations Unies s'étaient peu préoccupées des mesures de sécurité en Europe, à la différence des autres pays ou régions où l'ONU avait été la cible d'attaques terroristes. Cela explique peut-être l'excès de confiance ou le manque de sensibilisation aux problèmes de sécurité, qui s'est traduit par une vulnérabilité tangible des locaux de l'ONU. Le bulletin de l'UNDSS détaillait certaines des mesures de sécurité à mettre en place sur tous les sites européens de l'ONU dans les domaines suivants :

- Protection du périmètre ;
- Contrôles de sécurité et encadrement des visiteurs ;
- Systèmes de détection d'intrusion, alarmes et vidéosurveillance ;
- Formation des forces de sécurité et opérations de riposte ;
- Détection d'activités de reconnaissance et de surveillance hostiles ;
- Coordination avec le pays hôte ;
- Espaces sécurisés et compartimentage ;
- Communication ;
- Sécurité, sécurité incendie et préparation aux situations d'urgence ;
- Formation du personnel.

## **VULNERABILITE DU SYSTEME DE SECURITE DU CIRC ET PLAN D'AMELIORATION**

7. Les audits ont révélé plusieurs secteurs de vulnérabilité du système de sécurité physique du CIRC, notamment des éléments architecturaux, technologiques, procéduraux et humains. Ces points critiques, assortis des recommandations de l'UNDSS, ont été cartographiés pour élaborer un plan d'amélioration de la sécurité physique dans le but de renforcer la sécurité au CIRC. La Direction du CIRC a revu le plan et établi des priorités en fonction de leur faisabilité.

8. Ce plan est présenté dans le tableau ci-dessous, qui indique les mesures déjà en place et celles qui restent à prendre pour réduire la vulnérabilité. Pour pouvoir mettre en place les actions d'amélioration nécessaires et obligatoires, le Secrétariat du CIRC prie le Conseil de Direction d'allouer la somme de 120 000€ à partir du Fonds spécial du Conseil de Direction, selon les propositions détaillées et le budget figurant dans le tableau.

Zones de sécurité physique	Points de vulnérabilité du CIRC	Mesures déjà en place ou déjà lancées	Mesures additionnelles à mettre en place	Budget requis
Protection du périmètre	Les barrières légères et bornes escamotables à l'entrée et la sortie de la zone de livraison n'empêchent pas l'entrée des piétons.		Remplacer les barrières par des portails électriques, plus dissuasifs envers les intrus.	14 000€
	Si les portails et les barrières d'entrée et de sortie du parking, une fois ouverts, restent sans surveillance, des piétons ou des véhicules non autorisés peuvent facilement pénétrer sur le site.	Réduction du nombre de barrières pouvant s'ouvrir en même temps, restriction des heures d'ouverture des barrières, renforcement des contrôles en augmentant le nombre des agents de sécurité durant les heures d'ouverture des barrières et formation des agents de sécurité à mieux contrôler l'accès et les sorties.		
	Trop peu de panneaux "défense d'entrer".	Mise en place de panneaux supplémentaires sur les clôtures.		
Contrôles de sécurité et encadrement des visiteurs	Interphones obsolètes.	Remplacement de tous les interphones.		
	La configuration de l'entrée principale ne se prête pas à un contrôle de sécurité pratique et efficace.		Revoir la configuration de la réception et du bureau des agents de sécurité pour améliorer la vue sur l'entrée principale et faciliter les mouvements des agents de sécurité.	15 000€
	Les badges ne sont pas toujours portés de façon visible.	Rappel régulier des procédures de sûreté et de sécurité à tous les membres du personnel et à tous les visiteurs.		
	Les visiteurs ne sont pas toujours accompagnés une fois arrivés sur les lieux.	Rappel régulier des procédures de sûreté et de sécurité à tous les membres du personnel.		
	Système de contrôle des accès obsolète.		Migrer le système de contrôle des accès vers un nouveau serveur.	4 500€
	Pas de contrôle des livraisons.		Ajouter un nouveau poste de garde pour que l'agent de sécurité soit protégé des intempéries et d'éventuels assaillants.	5 000€

Zones de sécurité physique	Points de vulnérabilité du CIRC	Mesures déjà en place ou déjà lancées	Mesures additionnelles à mettre en place	Budget requis
Systèmes de détection d'intrusion, alarmes et vidéosurveillance	Caméras obsolètes.		Remplacer les caméras obsolètes.	10 000€
	Zones non couvertes par les caméras.		Ajouter des caméras là où cela s'avère nécessaire.	10 000€
	Pas de système de détection d'intrusion sur le périmètre.		Pour compenser la vulnérabilité due à la faible hauteur de la clôture et pour améliorer la détection précoce de la présence de personnes non autorisées, mettre en place un nouveau système de détection des intrusions.	45 000€
	Système de gestion technique du bâtiment (GTB) obsolète.	Migrer la GTB vers un nouveau serveur.		
	Zones d'ombre et éclairage obsolète.		Rajouter des éclairages appropriés là où cela s'avère nécessaire.	6 500€
Formation des forces de sécurité et opérations de riposte	Les agents de sécurité ne suivent pas toujours les instructions et les procédures.	Rappel régulier des procédures, entraînement en situation pour les agents de sécurité (scénarios de situations d'urgence).		
Détection d'activités de reconnaissance et de surveillance hostiles	Faible sensibilisation.	<ul style="list-style-type: none"> <li>- Actions régulières de sensibilisation à la sécurité.</li> <li>- Page sur intranet dédiée à la sécurité pour informer sur les procédures et permettre l'accès à des informations et des conseils en matière de sécurité et de détection d'activités de reconnaissance et de surveillance hostiles.</li> </ul>		
Coordination avec le pays hôte	Manque d'information de la part des autorités du pays hôte.	Réunions et échanges réguliers, contacts avec les autorités locales et centrales.		
Espaces sécurisés et compartimentage	Evènements publics dans le Grand Hall, exposé à tous les visiteurs et risque d'entrées non autorisées.		Rajouter une sécurité supplémentaire et un compartiment de sécurité avec un système de verrouillage des portes du sas.	10 000€

Zones de sécurité physique	Points de vulnérabilité du CIRC	Mesures déjà en place ou déjà lancées	Mesures additionnelles à mettre en place	Budget requis
Communication		Système renforcé d'envoi en masse de SMS, testé régulièrement et amélioré.		
Sécurité, sécurité incendie et préparation aux situations d'urgence		<ul style="list-style-type: none"> <li>- Formation annuelle en sécurité incendie obligatoire pour tous les membres du personnel, accompagnée de la diffusion d'informations supplémentaires sur la sécurité.</li> <li>- Exercice annuel d'évacuation.</li> <li>- Système de sécurité incendie bien entretenu et testé régulièrement ; échanges réguliers avec le Service départemental-métropolitain d'incendie.</li> </ul>		
Formation du personnel	Formation de l'UNDSS à la sécurité des déplacements assurée régulièrement mais pas de formation particulière relative aux attaques à main armée.	Rappel aux membres du personnel qu'ils doivent suivre régulièrement les formations de l'UNDSS à la sécurité des déplacements.		
		Formation à la sécurité spécifique pour les femmes.		
		Diffusion des instructions et conseils en matière de sécurité.		
				120 000€

Annexe 1 – Audit interne de tous les systèmes de gestion du bâtiment en temps réel

<b>I.</b>	<b>Introduction</b>	<b>2</b>
<b>a.</b>	<b>Les serveurs dédiés à la Gestion du Bâtiment</b>	<b>2</b>
<b>b.</b>	<b>Récapitulatif des serveurs</b>	<b>2</b>
<b>1.</b>	<b>Serveur XBS / Honeywell</b>	<b>3</b>
<b>2.</b>	<b>Serveur Contrôle d'accès Delta</b>	<b>3</b>
<b>II.</b>	<b>Risques, probabilités et Impact sur le Centre avec Recommandations</b>	<b>4</b>
<b>1.</b>	<b>Serveurs XBS et EBI/Honeywell</b>	<b>4</b>
<b>i.</b>	<b>Risques Pannes Electriques</b>	<b>4</b>
<b>ii.</b>	<b>Risque Panne Informatique</b>	<b>4</b>
<b>iii.</b>	<b>Panne Routeurs BNA ou automate étage</b>	<b>4</b>
<b>iv.</b>	<b>Panne Pc Client Monitoring</b>	<b>4</b>
<b>v.</b>	<b>Recommandations pour XBS et EBI / Honeywell</b>	<b>4</b>
<b>2.</b>	<b>Serveur Contrôle d'accès</b>	<b>5</b>
<b>i.</b>	<b>Risque Panne Electrique</b>	<b>5</b>
<b>ii.</b>	<b>Risque Pannes informatiques</b>	<b>5</b>
<b>iii.</b>	<b>Pannes Electroniques sur Contrôleurs de Lecteurs d'accès Delta</b>	<b>6</b>
<b>iv.</b>	<b>Recommandations pour Contrôleur d'accès Delta = 5000€</b>	<b>6</b>
<b>3.</b>	<b>Serveur VideoSurveillance</b>	<b>6</b>
<b>i.</b>	<b>Risque Panne Electrique</b>	<b>6</b>
<b>ii.</b>	<b>Risques Panne Informatique</b>	<b>6</b>
<b>iii.</b>	<b>Risque Panne Caméra</b>	<b>6</b>
<b>iv.</b>	<b>Recommandation Serveur VideoSurveillance = environ 10000€</b>	<b>6</b>
<b>4.</b>	<b>Serveur PABX</b>	<b>7</b>
<b>i.</b>	<b>Risque Panne Electrique</b>	<b>7</b>
<b>ii.</b>	<b>Risque Panne Electronique PABX</b>	<b>7</b>
<b>iii.</b>	<b>Risque Panne Informatique Système OmniPCX</b>	<b>7</b>
<b>iv.</b>	<b>Recommandation Serveur PABX = environ 25000€</b>	<b>7</b>
<b>III.</b>	<b>Description des Serveurs</b>	<b>8</b>
<b>1.</b>	<b>Serveur XBS HoneyWell</b>	<b>8</b>
<b>2.</b>	<b>GTC via Honeywell EBI – Entreprise Building Integrator</b>	<b>10</b>
<b>3.</b>	<b>Serveur de Contrôle d'accès Delta</b>	<b>12</b>
<b>4.</b>	<b>Système Vidéosurveillance</b>	<b>14</b>
<b>5.</b>	<b>Infrastructure de Téléphonie Alcatel</b>	<b>15</b>

## **I. Introduction**

### **a. Les serveurs dédiés à la Gestion du Bâtiment**

Nous possédons plusieurs serveurs dédiés à la Gestion du Bâtiment. Ces serveurs nous aident à superviser l'ensemble des équipements sensibles et critiques du Centre.

Ce rapport a pour but de faire un Audit de ce matériel, estimer les risques et la probabilité de coupures de services sur ces serveurs, et de faire des préconisations et recommandations pour assurer la pérennité de fonctionnement de tous ces matériels.

Voici la Liste des 6 serveurs dédiés à la Gestion des Bâtiments :

- Serveur XBS/Honeywell : Gestion Technique de La Tour (Electricité, Climatisation, Congélateurs ...)
- Serveur EBI/Honeywell : Gestion Technique Latarjet (Electricité, Climatisation, ...)
- Serveur Delta : Contrôle d'accès CIRC
- Serveur Videosurveillance : Caméras de surveillance
- OmniPCX PABX : Téléphonie du CIRC
- Serveur Sirius : Monitoring Congélateurs SMHS1, S18, S15, 13ème

### **b. Récapitulatif des serveurs**

- **Serveur XBS/HoneyWell**
  - o Age :
    - Automate de Régulation : entre 1980 et 2000
    - Serveur de Supervision : Dernier update 1998
  - o Localisé : Comptoir de l'Accueil
  - o Machine Dell Optiplex GX270 Windows 2000 Pro
    - Connexion sur BUS Honeywell analogique (une seule arrivée)
    - Plateforme XBS
  - o Constructeur : Honeywell
- **Serveur EBI/HoneyWell**
  - o Age :
    - Automate de Régulation : Après 2000
    - Serveur de Supervision : 2010.
  - o Localisé : Comptoir de l'accueil
  - o Machine Dell Precision 380
    - Connexion Sur Bus Ethernet
    - Plateforme EBI
  - o Constructeur HoneyWell
- **Serveur Delta**
  - o Age : 1988
  - o Localisé : Salle Opus S/Sol
  - o Machine Dell Precision 380 Windows 2000 Pro
  - o Constructeur : Delta 2S, Système BeWator
- **Serveur de VideoSurveillance**
  - o Age :
    - Caméras : 1991 à maintenant
    - Serveur : 2009
  - o Localisé en S02
  - o Machine Logidom Assemblée
  - o Constructeur : Logidom, Système AverDigi

- **Serveur PABX**
  - o Age : Dernier Update 2007
  - o Localisé : Salle Opus
  - o Constructeur : Alcatel
- **Serveur Sirius**
  - o Age : 2010
  - o Localisé : VM salle Serveur Tour
  - o Constructeur : JRI

Avant de commencer l'audit et le détail serveur par serveur, voici un aperçu des recommandations primordial pour le fonctionnement de certains éléments du CIRC.

**Priorités :**

**1. Serveur XBS / Honeywell**

a. 1<sup>ère</sup> Phase = 3600€ + 2750€

- Mettre en place un routeur CBUS Ethernet (routeur BNA)
- Remplacer la machine serveur par plus récent

b. 2<sup>ème</sup> Phase = environ 35 000€ (ou contrat de maintenance évolutif)
- Migrer XBS vers une plateforme EBI/IP
- Migrer EBI Total vers VMware
  - o Problème de sauvegarde manuelle résolu
  - o Problème de reprise d'activité résolu car beaucoup plus rapide et indépendant du matériel
  - o Panne électrique sur Serveur résolue car Salle Serveur sécurisée.

**2. Serveur Contrôle d'accès Delta**

- **Migrer la plateforme vers une solution IP = environ 20 000€**
  - o Ajouter une carte d'extension IP au niveau des contrôleurs
  - o Migrer vers un logiciel SiPass
  - o Apport :
    - Plus de souplesse d'administration du serveur
    - Reprise d'activité plus rapide en cas de perte du serveur
    - Synchronisation des informations avec une base de données LDAP possible
    - Reprise d'activité rapide en cas de pannes des Clients.
  - o Contrat de Maintenance sur contrôleurs.

## **II. Risques, probabilités et Impact sur le Centre avec Recommandations**

### **1. Serveurs XBS et EBI/Honeywell**

#### **i. Risques Pannes Electriques**

- Générale : Comme tous les éléments de la Tour, les appareils sont connectés sur le groupe électrogène.
- Serveur : Aucun Onduleur sur Serveur situé à l'Accueil
- Probabilités des coupures électriques du CIRC
  - o 2 coupures le mois dernier
- Impact :
  - o Aucun Monitoring Congélateurs, Chambres Froides
  - o Aucun contrôle sur éléments techniques (climatisation, chauffage, ...)
  - o Aucune remontée des alarmes Incendie

#### **ii. Risque Panne Informatique**

- Matériel Obsolète, pas de Spare du GX270 pour le XBS
- Système d'exploitation Windows 2000 Pro sur XBS, aucune mise à jour Microsoft
- Lien Analogique CBUS pour XBS arrivant à l'accueil, impossible de déplacer le serveur.
- Probabilités :
  - o Durant les 3 dernières années, il y a eu 4 pannes informatiques. Chaque panne a duré de ½ journée à 4 jours.
- Impact :
  - o Aucun moyen de contrôler certains éléments très importants : Climatisation, chaufferie ...
  - o Aucun Monitoring Congélateurs, Chambres Froides
  - o Aucun poste client ne peut accéder aux informations.

#### **iii. Panne Routeurs BNA ou automate étage**

- Aucune remontée d'informations et aucun contrôle entre les automates et les serveurs.
- Probabilités :
  - o 5 Pannes depuis 2010 sur Automates
  - o 1 panne sur Bus Analogiques carte de communication Serveur
- Impact :
  - o Aucune communication entre Automates et le serveur
  - o Aucun Monitoring
  - o Aucun contrôle

#### **iv. Panne Pc Client Monitoring**

- Pas de possibilités de contrôler/gérer le système
- Matériel Obsolète, besoin du port parallèle pour Dongle Honeywell

#### **v. Recommandations pour XBS et EBI / Honeywell**

- a. **1<sup>ère</sup> Phase = 3600€ + 2750€**
- Mettre en place un routeur CBUS Ethernet
- Remplacer la machine serveur par plus récent
- b. **2<sup>ème</sup> Phase**
- **Migrer XBS vers une plateforme EBI/IP = 35 000€ ou contrat de maintenance évolutif**
- Migrer EBI Total vers VMware
  - o Problème de sauvegarde manuelle résolu
  - o Problème de reprise d'activité résolu car beaucoup plus rapide et indépendant du matériel
  - o Panne électrique sur Serveur résolue car Salle Serveur sécurisée.
- Contrat de Maintenance/Evolution pour problème sur les Automates

- Si panne d'un automate, Chercher dans le stock fournisseur si par chance il existe encore un automate similaire. Ce type de matériel devient très difficile à trouver.
  - Renouvellement du matériel pour qu'il soit compatible avec la plateforme EBI
  - Prestation de reconfiguration sur l'EBI pour les automates dont nous n'avons pas les Codes Sources.
- Contrat de Maintenance avec Intervention J+1 recommandé

## **2. Serveur Contrôle d'accès**

### **i. Risque Panne Electrique**

#### **Coupures Electriques Générales sur Contrôleurs de Lecteurs et Gâches électriques**

- Coffrets des contrôleurs avec alimentation de secours par Groupe Electrogène
- Coffrets Alimenté par Onduleur en S02
  - Tous les lecteurs de Badges continuent de fonctionner
  - Toutes les gâches électriques sont alimentées (sauf les barrières automatiques Cours Albert Thomas et AFL sur alimentation générale)
- Probabilités : 2 coupures le mois dernier
- Impact : Les portes d'accès fonctionnent normalement

#### **Coupures Electriques du Serveur Salle Opus**

- Alimenter par Onduleur Salle Opus (Charges +3h)
- Après 3h coupure d'alimentation
  - Aucun contrôle des entrées sorties
- Probabilité : aucune recensée
- Impact : Aucun contrôle sur les lecteurs et badges

### **ii. Risque Pannes informatiques**

#### **Crash Serveur Contrôle d'accès situé en Salle Opus**

- Probabilité : 1 fois depuis 2010
- Impact :
  - Contrôleurs et Lecteurs de badges continuent de fonctionner
  - Plus aucun historique d'accès
  - Plus aucun contrôle sur les badges et les niveaux d'accès
  - Aucune machine en Backup
  - Machine Obsolète en Windows 2000 Pro
  - Licence Serveur sur Dongle Port Parallèle
  - Reprise d'activité Longue et difficile

#### **Crash Pc Clients Accueil et Aso**

- Probabilité : 3 fois depuis 2010 pour Accueil / 1 fois pour ASO
- Impact :
  - Aucunes incidences sur le contrôle d'accès
  - Perte du monitoring
  - Machine Obsolète en Windows 2000 Pro
  - Client Lourd avec Dongle sur Port Parallèle
  - Reprise d'activité longue et difficile

**iii. Pannes Electroniques sur Contrôleurs de Lecteurs d'accès Delta**

- o Probabilité : 1 fois depuis 2010
- o Impact :
  - Tous les Lecteurs de Badges et Gâches Electriques connectés sur le contrôleur HS ne fonctionnent plus. Position Ouverte.

**iv. Recommandations pour Contrôleur d'accès Delta = 5000€**

- **Changer les Interphones Accès = 5000€**

- o Interphone portillon CAT
- o Interphone Parking CAT
- o Interphone Portillon AFL
- o Interphone Parking AFL
- o Interphone Quai AFL
- o Interphone Entrée Quai
- o Interphone Entrée Latarjet

**3. Serveur VideoSurveillance**

**i. Risque Panne Electrique**

- Générale : Comme tous les éléments de la Tour, les appareils sont connectés sur le groupe électrogène.
- Serveur : Relié à l'onduleur en S02
- Probabilités des coupures électriques du CIRC
  - o 2 coupures le mois dernier
- Impact :
  - o Aucun Monitoring du Site pour les agents de Sécurité
  - o Aucun enregistrement

**ii. Risques Panne Informatique**

- Matériel assemblé : Pas de support matériel
- Aucune machine en Spare
- Reprise de service longue en cas de changement de matériel
- Probabilité : 1 panne en 2014 pendant le Conseil de Direction
- Impact :
  - o Aucun Monitoring du Site pour les agents de Sécurité
  - o Aucun enregistrement

**iii. Risque Panne Caméra**

- Alimentation Electrique Générale du CIRC
- Panne Electronique de la Caméra
- Probabilité : Quasi nul depuis 5 ans
- Impact : Perte de la caméra sur le monitoring de l'accueil

**iv. Recommandation Serveur VideoSurveillance = environ 10 000€**

- Upgrade Machine vers Windows 7
- Mettre en Spare pour répondre rapidement aux pannes :
  - o Alimentation
  - o Mémoire
  - o HDD
- Remonter d'alerte sur la machine et/ou sur la RAID
- Contrat de maintenance sur Caméras
- Ajouter plusieurs Caméras Infra-rouge
  - o Pour Parking
  - o Accès Quai
  - o Jardin coté Audito

- Garage à Vélo
- Cuve Azote Parking
- Changer les prises de vues de plusieurs Caméras
  - Un audit des caméras va être fait par un expert de la Sécurité
- Ajouter des clients monitoring pour le magasinier Quai
  - Meilleure visibilité de tous les espaces du Quai pour le Magasinier
- Changer le Système de Détection vers système de détection informatisé
  - Affichage uniquement des caméras avec activité à surveiller
  - Agents de sécurité plus vigilants car moins d'écrans à surveiller
  - Alléger le nombre d'écrans au Poste Accueil

#### **4. Serveur PABX**

##### **i. Risque Panne Electrique**

- Générale : Comme tous les éléments de la Tour, les appareils sont connectés sur le groupe électrogène.
- Salle Opus : Onduleur avec Charge 3h+
- Probabilité : Nul depuis 5 ans
- Impact : Aucun Appel Entrant/Sortant

##### **ii. Risque Panne Electronique PABX**

- 2 CPU Redonder
  - Si un CPU tombe en panne, le 2<sup>ème</sup> prend le relais.
  - Problème : Pas de contrat de Supervision, si un CPU tombe en panne aucun moyen d'alerte.
  - Contrat de Maintenance Bouygues Energie J+1 pour remplacement tout matériel dans OmniPCX
- 2 CPU dans le même Rack (même endroit physique)
  - Solution : Délocaliser les 2 CPU, mais besoin d'une 2<sup>ème</sup> arrivée FT
- Probabilité : Aucun depuis 2010
- Impact : Aucun Appel Entrant/Sortant

##### **iii. Risque Panne Informatique Système OmniPCX**

- Machine de Contrôle et Monitoring du PABX sous Windows XP Pro
  - Aucune Maj Windows
  - Aucun Spare identique en cas de panne ou de restore
- Probabilité : Aucune depuis 2010
- Impact :
  - Téléphones continuent de fonctionner
  - Aucun moyen de contrôle et modification sur les téléphones

##### **iv. Recommandation Serveur PABX = environ 25 000€**

- Upgrader le PABX vers version up to date
- Délocaliser les 2 CPU dans 2 bâtiments différents, mais besoin d'une 2<sup>ème</sup> arrivée FT
- Migrer le serveur de monitoring vers une VM

### III. Description des Serveurs.

#### 1. Serveur XBS HoneyWell

La GTC nous permet de gérer différents éléments techniques tels que le chauffage, la ventilation et la climatisation du CIRC.

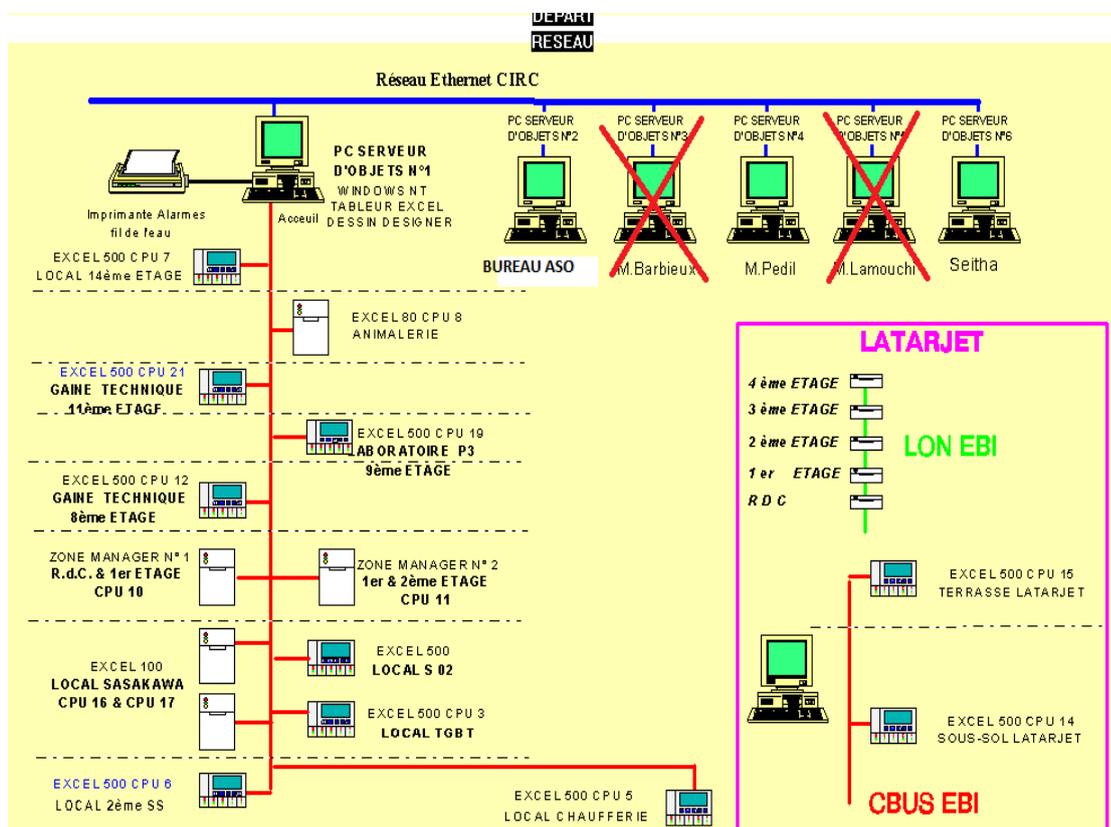
XBS de Honeywell est un outil de supervision qui nous permet de contrôler différents éléments à distance (Congélateurs, ...).

Cet outil nous permet de :

- Réaliser des économies d'énergie en adaptant les consommations d'énergie
- Apporter des solutions de confort aux occupants
- Sécuriser le bâtiment

#### Notre installation au CIRC

Nous avons une architecture de base suivante :



Dans notre XBS, nous pouvons gérer les éléments suivants :

LOCAL 906	EPIC	SASAKAWA
CLIMATISATION DES LOCAUX	ELECTRICITE	CLIMATISATION
SECURITE	CONGELATEURS	CHAMBRES FROIDES
CHAUFFERIE	BIP	ISOLEMENT
Synthèse Générale Alarme	DIVERS	HONEYWELL

### Les problèmes et limites actuels niveau informatique :

- Administration niveau informatique très compliquée car :
  - o Matériel obsolète (+ 10 ans)
  - o Système d'exploitation obsolète (Windows 2000 Pro)
  - o Reprise d'activité suite à un crash très difficile car il faut restaurer sur une machine identique.
  - o Mise à niveau vers machine récente impossible car il faut garder un port parallèle pour la clé serial du logiciel.
- Niveau plateforme XBS
  - o Plateforme XBS très complexe
  - o Plusieurs prestataires ont travaillé dessus (ESSAM, Seitha, Cofely ...), chacun a fait des configurations avec des codes sources impossible à retrouver. Historique des modifications introuvables.
  - o Evolution impossible car plateforme obsolète et incompatible avec les nouveaux éléments de contrôle (automates, etc.)
  - o Architecture très instable.
- Maintenance Honeywell
  - o La maintenance proposée par Honeywell a été interrompu en 2012.

#### **Améliorations à apporter :**

- Une migration vers la plateforme EBI
  - o Changement des automates vers un échange de données via IP.
  - o Migration de tous les points de contrôle XBS vers EBI existant.
  - o Prestation lourde en temps de configuration.

Le but est de sécuriser en cas de panne le serveur actuel qui pose quelques problèmes.

## Les problèmes et limites actuels niveau élément actifs Honeywell :

- Tout le matériel situé dans les gaines techniques est obsolète. Les automates (Excel 80, Excel 100 et Excel 500) qui nous permettent de gérer et de transférer les informations techniques provenant des éléments de chaufferie, climatisation ou autres ne sont plus ni maintenus ni fabriqués par Honeywell depuis de nombreuses années.
- La plupart des pannes sur ces automates sont réparées avec de l'appareillage d'occasion. Ce stock d'occasion s'écoule au fur et à mesure du temps et il est maintenant très difficile de retrouver ce type de matériel en stock chez les fournisseurs.
- Le matériel fabriqué aujourd'hui n'est pas compatible avec la plateforme XBS.

### 2. GTC via Honeywell EBI – Enterprise Building Integrator

L'EBI est une version plus évoluée que la XBS pour de la Gestion de Bâtiment proposée par Honeywell.

Nous possédons la version R410, qui est la version commercialisée pendant les années 2008 à 2010. Honeywell est maintenant à la version R430 avec des fonctionnalités évoluées par rapport à notre version.

La solution EBI est bâtie autour d'une architecture IP.

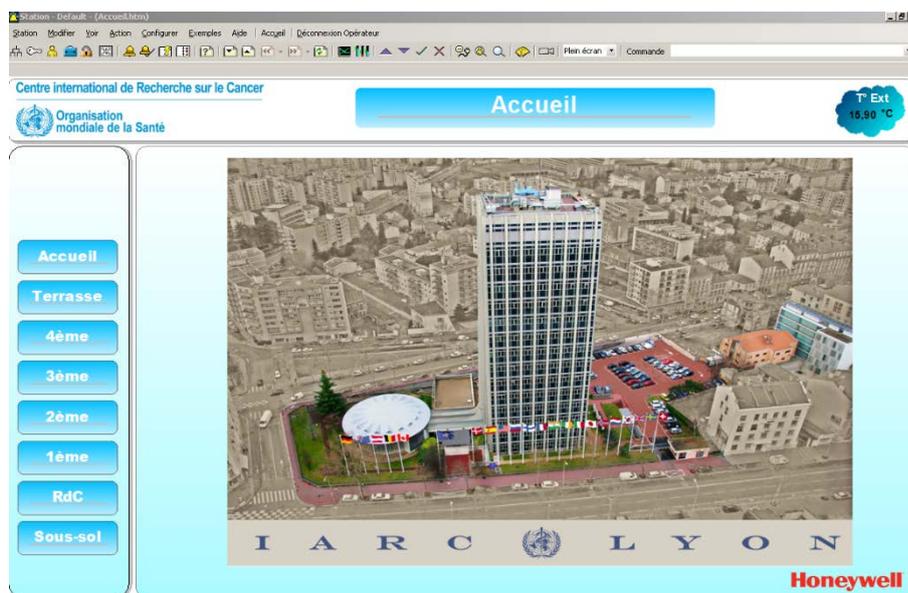
Cela rend l'administration informatique beaucoup plus facile à gérer.

Notre Solution EBI nous permet de gérer le bâtiment LATARJET.

Ce bâtiment est équipé d'automate, de Zone Manager et de routeur BNA permettant de communiquer avec un serveur EBI Honeywell où qu'il soit sur le réseau.

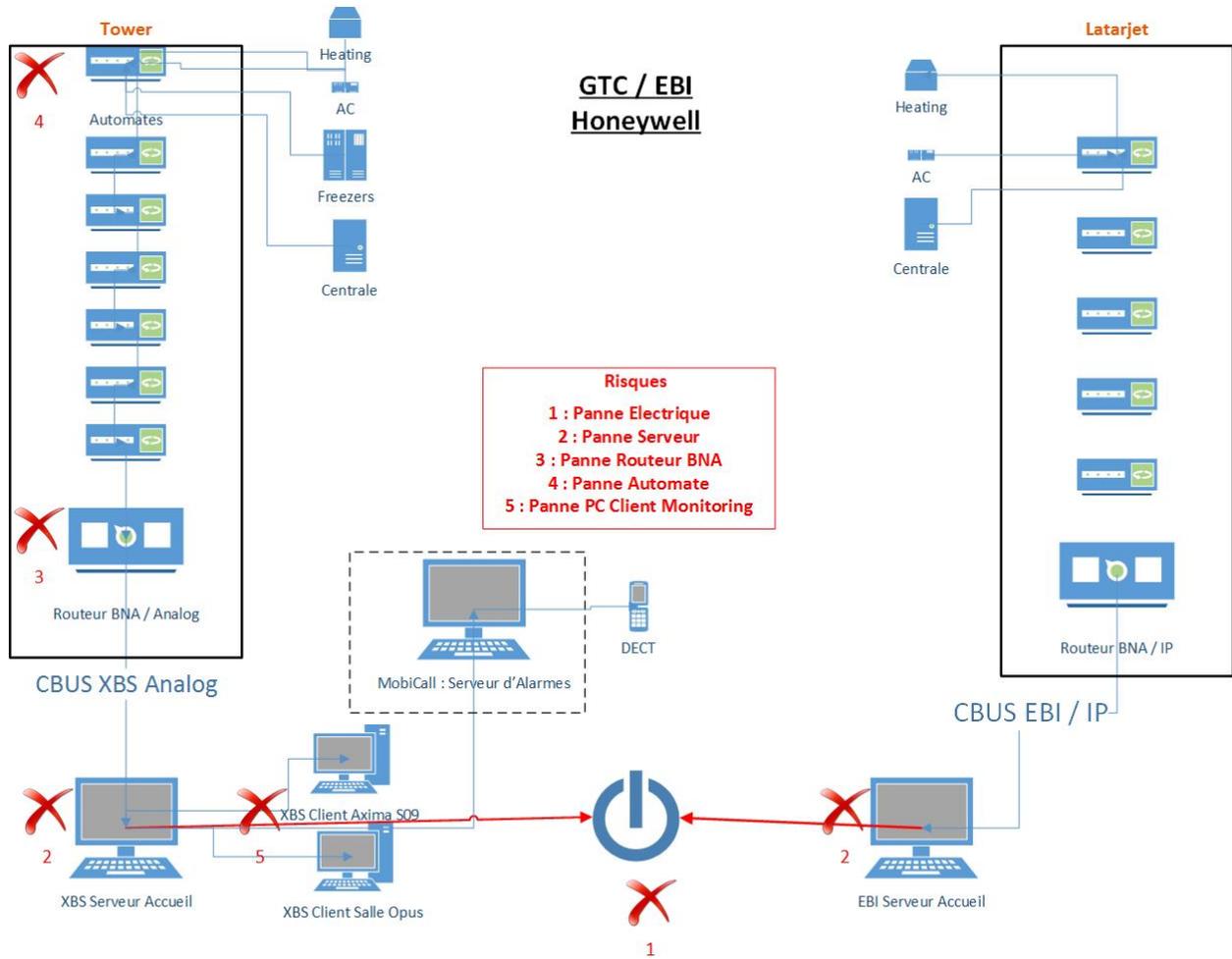
Ce serveur est physiquement situé à l'accueil.

Aucun poste client n'est connecté avec ce serveur. Toutes les manipulations se font depuis ce poste serveur.



Améliorations possibles :

- Migrer la machine vers une VM
- Installer plusieurs clients



### **3. Serveur de Contrôle d'accès Delta** **BEWATOR – Granta 4.2.95 – Carte COTAG**

L'implantation du Contrôleur d'accès par DELTA PROTECTION au CIRC date de 1988.

Au fur et à mesure différentes extensions de lecteurs de cartes et de cartes d'extension sont venues s'ajouter à l'existant.

Le cœur du réseau du contrôleur d'accès se situe dans le local courant faible du 1<sup>er</sup> S/Sol, pièce S18.  
Le disjoncteur du contrôleur d'accès se trouve dans le local technique en S02.

Le cœur est composé de 4 Contrôleurs servant à gérer les lecteurs de cartes.

Une liaison RS232 vers la vidéosurveillance permet le déclenchement des caméras sur certains lecteurs de cartes.

Les informations qui apparaissent pour chaque passage chez les gardiens de l'accueil :

- i. Le numéro du badge
- ii. Le lieu de passage
- iii. L'heure
- iv. Le nom de la personne affecté au badge

Le cœur du réseau est un élément vital du CIRC, s'il tombe en panne plus aucun accès au CIRC ne fonctionne. Des alimentations auxiliaires sont disponibles dans la gaine technique pour répondre à des éventuelles coupures de courant. Si ces alimentations de secours viennent à s'épuiser, les gâches électriques ne fonctionneraient plus.

#### **Architecture informatique.**

Le contrôle d'accès est administré via la solution GRANTA 4.2.95.

Ce logiciel permet de configurer les badges et de leur affecter un niveau d'accès.

Cet outil permet aussi de gérer les lecteurs de badges et les niveaux d'accès.

Il existe au CIRC 3 postes avec le logiciel GRANTA.

Delta01 situé à l'accueil

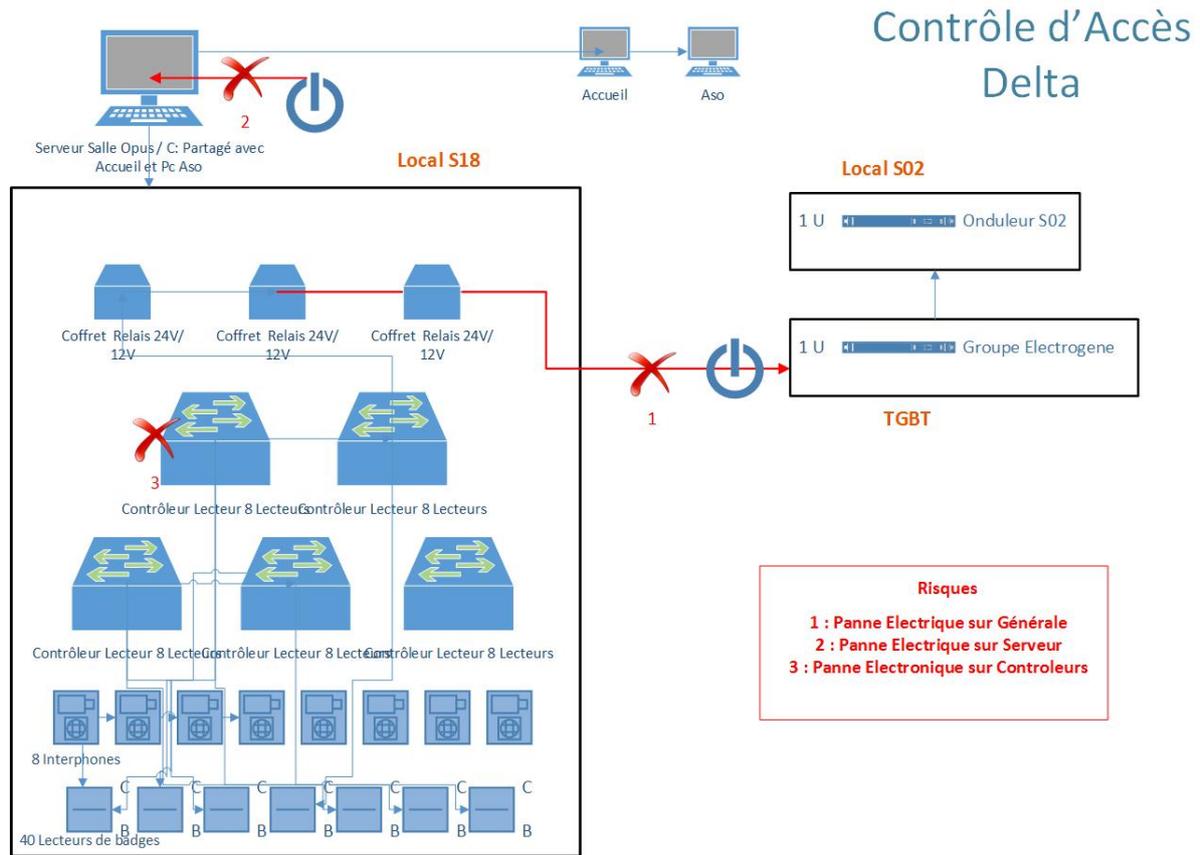
Badgeur ASO situé à en R04.

Delta02 (serveur et stockage de la base de données) situé en Salle Opus S17

La base de données n'est synchronisée avec aucune autre base de données du CIRC, ce qui rend difficile la mise à jour automatique des données.

Chacun de ces postes possède des droits d'accès différents.

Ces 3 machines sont hors domaine iarc.



#### 4. Système Vidéosurveillance

La vidéosurveillance a été mise en place au CIRC en 1991.

Elle a été mise en place initialement afin d'assurer la surveillance des accès :

- Du Parking
- Du Bâtiment Tour
- Des Bâtiments BRC et Latarjet

Suite aux différents ajouts de caméra et extension de Bâtiment, nous avons aujourd'hui :

- 22 Caméras fixes autour des bâtiments
- 6 portiers sur lecteur de badges
- 1 Dôme pour le parking
- 4 Caméras fixes sur la tourelle

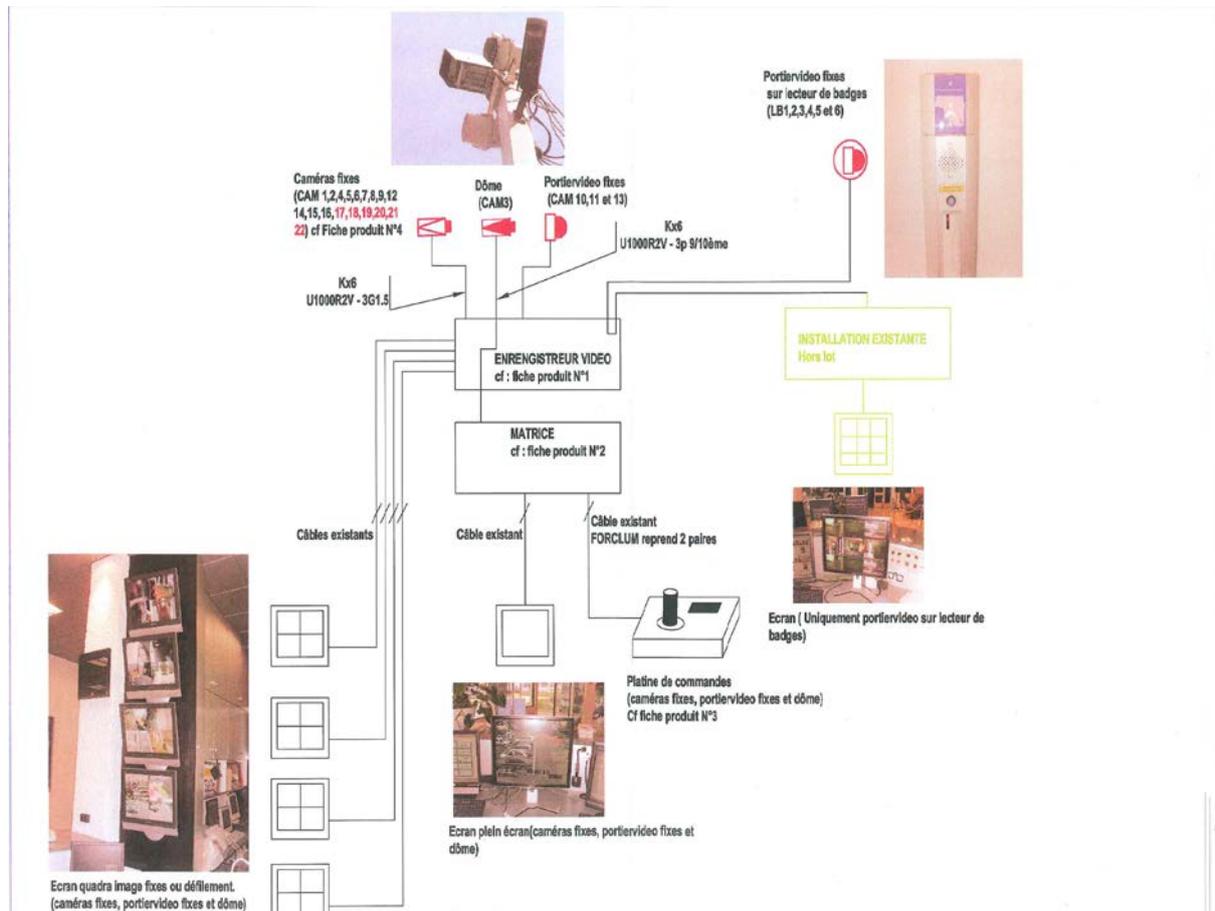
Le cœur du réseau de caméras se situe dans la baie de vidéosurveillance en S02.

Dans cette baie sont rangés :

- Enregistreur numérique (fourni par LOGIDOM)
  - o Logiciel de vidéosurveillance AverDigi
  - o Equipé de 3 HDD avec 15 jours de rétention
- Matrice vidéo 32 voies

Alimentation Electrique :

- Alimentation Générale
- Onduleurs S02

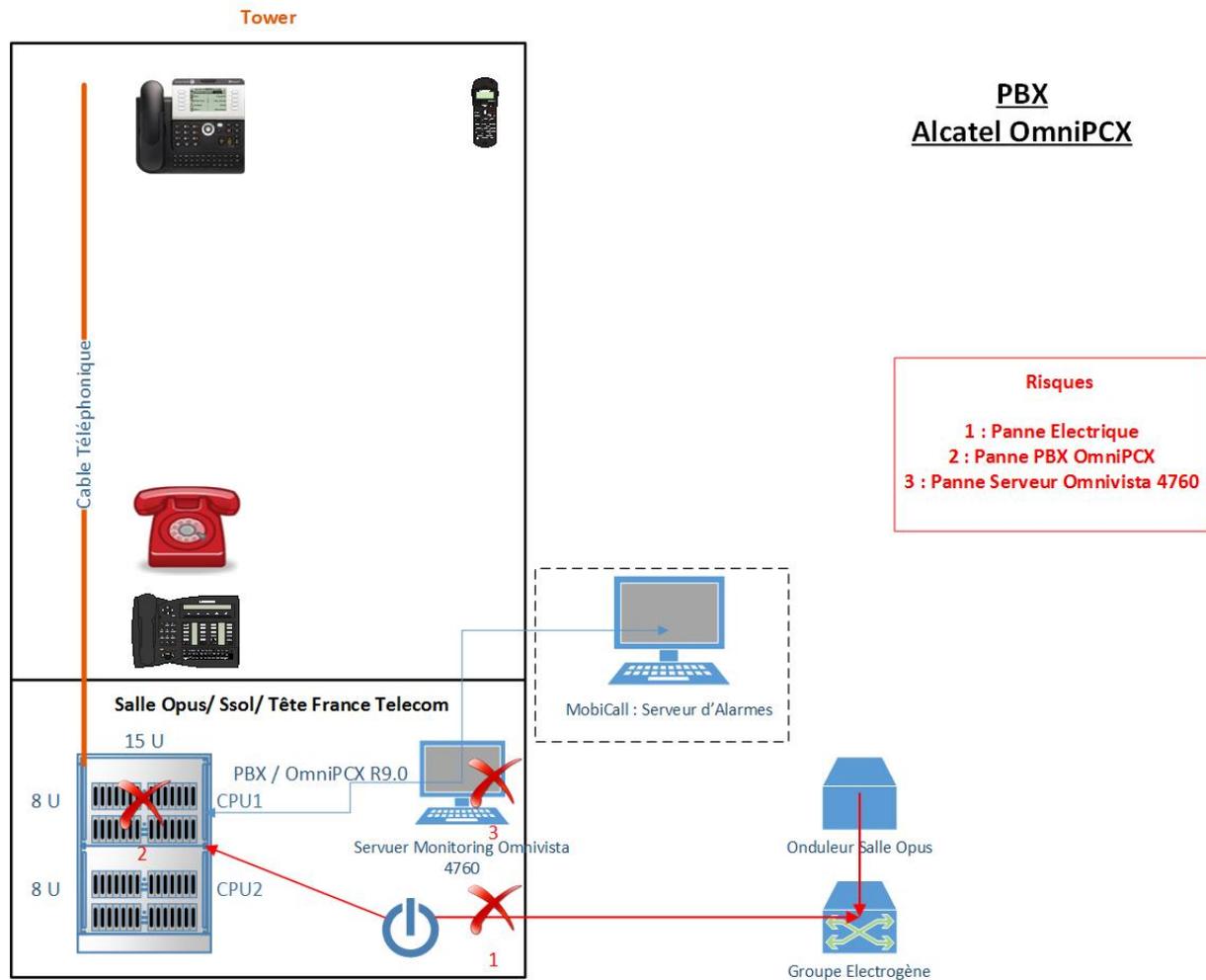


### 5. Infrastructure de Téléphonie Alcatel

Le CIRC possède :

- Un PABX OmniPCX R9
- Une messagerie vocale 4635J
- Un outil d'administration Omnivista 4760 R5.1
- 1 PO PC 4059

La dernière mise à jour du PABX date de 2008 où une grosse opération de migration de carte de communication analogique vers numérique avait été réalisée.





MINISTÈRE DE L'INTÉRIEUR

Direction Générale  
de la Police Nationale

Direction Centrale  
de la Sécurité Publique

Direction Départementale  
de la Sécurité Publique  
du Rhône

Etat-Major/PPPPV/CPS

Lyon, le 01 février 2016

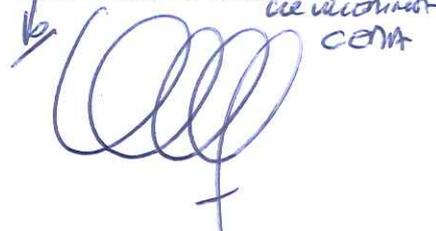
**SOIT TRANSMIS A**

**Madame FRANÇON,  
Administrateur des Services Intérieurs  
de l'Organisation Mondiale de la Santé.**

**OBJET :** Consultation de sûreté du Centre International de Recherche sur le Cancer, situé  
150 cours Albert Thomas à Lyon 8ème.

Le Commissaire Divisionnaire  
Chef d'Etat-Major

Claire MAZOYER





MINISTÈRE DE L'INTÉRIEUR

DIRECTION GÉNÉRALE  
DE LA POLICE NATIONALE

Lyon, le 01 Février 2016

-----  
DIRECTION DÉPARTEMENTALE  
DE LA SÉCURITÉ PUBLIQUE  
DU RHÔNE

Le Major de Police Joël BENMOYAL  
Matricule 431 855  
en fonction à l'État-Major / PPPPV / CPS

-----  
État-Major / P.P.P.P.V.

à

-----  
C.P.S.

Madame le Commissaire Divisionnaire  
Chef d'État-Major  
Claire MAZOYER

S/C de la Voie Hiérarchique

**OBJET :** Consultation du Centre International de Recherche sur le Cancer (CIRC) rattaché à l'Organisation Mondiale de la Santé (OMS) à Lyon 8ème.



CIRC

J'ai l'honneur de vous rendre compte de la visite du CIRC situé 150 cours Albert Thomas à Lyon 8ème, accompagné du Capitaine Fabrice LARGE du service.

----

La mise en sûreté d'un site n'est efficace que si la démarche et l'analyse de risque sont appréhendées de façon systémique ou globale. Les préconisations qui en découlent ont pour objet de prévenir tout acte malveillant.

Ce document est diffusé de manière restreinte. En aucun cas il ne saurait engager la responsabilité du service relevant de la Direction Départementale de la Sécurité Publique du Rhône.

----

Cette étude a été effectuée en totale concertation, s'agissant d'une approche globale et commune de l'analyse du risque, de l'identification et de l'examen des problématiques rencontrées et d'une adaptation des préconisations à mettre en œuvre aux particularités et caractéristiques du site et de sa fréquentation.

Notre intervention est consécutive à une demande de Mme Elisabeth FRANCON, Administrateur des Service Intérieurs. Nous avons été reçus par M. PEPIL, responsable sécurité/sûreté du site. Dans le contexte actuel, lié aux risques de terrorisme et eu égard au rôle emblématique que joue cet organisme sur la scène international, les dirigeants souhaitent avoir un conseil sur la cohérence des dispositifs de sûreté dont ce site dispose et le cas échéant, dégager des préconisations.

Le Centre international de recherche sur le cancer (**CIRC**), est une agence intergouvernementale de recherche sur le cancer, créée en 1965 par l'Organisation mondiale de la santé (OMS) des Nations Unies. Ses bureaux sont situés à Lyon, en France. Il fait partie depuis 2003 du cancérpôle Lyon Auvergne Rhône-Alpes (CLARA). Il est le siège de l'organisation à laquelle sont rattachés 21 pays membres à travers le monde.

Le rôle du CIRC est de diriger et de coordonner la recherche sur les causes du cancer (il n'est en principe pas impliqué dans la recherche sur des traitements sur le cancer). Il effectue également des études épidémiologiques sur l'incidence du cancer à travers le monde. Il publie une série de monographies sur les risques cancérigènes pour l'homme constitués par divers agents, mélanges et expositions.

Les locaux sont situés 150 cours Albert Thomas à Lyon 8ème. C'est une tour « IGH » de 13 étages (R+13-2). Il y a un amphithéâtre situé à l'extérieur (R+1) ainsi que des bureaux côté rue feuillat (R+4-1).

320 personnes (scientifiques, chercheurs en visite, étudiants) sont employées au sein de cet organisme qui fonctionne en continue 24/24 heures. Un poste de sécurité est opérationnel 24/24 heures.

## **I – PERIPHERIE – Les abords ou zone urbaine**

Le site est ceinturé au Nord par le cours Albert Thomas, au Sud par l'avenue des Frères Lumière, à l'Est par la rue Professeur Rochaix et à l'Ouest par la rue Feuillat.

Les axes probables de fuite pourraient être par les avenues Rockefeller et Franklin Roosevelt pour atteindre le boulevard périphérique Laurent Bonnevey et les autoroutes.

La circulation est à double sens, une voie à sens unique réservée aux véhicules et un couloir à contresens dédié aux autobus et cycles. Le stationnement est autorisé de chaque côté de la chaussée.

Il y a de la vidéo-protection urbaine à proximité du site, l'éclairage urbain est de bonne qualité. La végétation sur l'espace urbain est maîtrisée.

## II – PERIMETRIE - de la clôture à la façade et ouvrants inclus

### La clôture

Le bâtiment est ceinturé sur sa périmétrie par une clôture homogène de faible hauteur, aisément franchissable.



### Préconisations :

- *Réhausser la clôture afin de dissuader son franchissement.*
- *L'implantation d'une barrière infrarouge en périmétrie, en fonctionnement la nuit et le week-end, pourrait permettre la détection d'une intrusion bien en amont.*

### Les ouvrants dans la clôture

On distingue une entrée principale (portail et portillon piétons) et trois autres portails destinés à l'entrée et sortie des véhicules du personnel, respectivement cours Albert Thomas et rue Feuillat, et aux véhicules d'intervention et de secours.



Un agent est présent de 8h30 à 9h30, pour l'entrée des véhicules du personnel. Durant ce laps de temps, le portail est ouvert, une barrière automatique fait office de sas. Les piétons disposent d'un badge d'accès pour l'ouverture du portillon à l'entrée principale.

Une rampe d'accès permet aussi les livraisons d'une part et l'accès des transports de fonds d'autre part.



### Livraisons et transports de fonds

Une rampe d'accès souterraine rue feuillat est dédiée aux livraisons qui s'effectuent de 8h à 12h00. Une fiche d'enregistrement est renseignée avant le déchargement, toutefois, le contenu n'est pas vérifié et les véhicules accèdent directement au quai de déchargement. On notera la présence d'une barrière d'accès à la rampe qui est toutefois en position ouverte. En revanche les colis livrés aux particuliers sont acheminés à l'entrée principale et systématiquement vérifiés.

#### **Préconisations :**

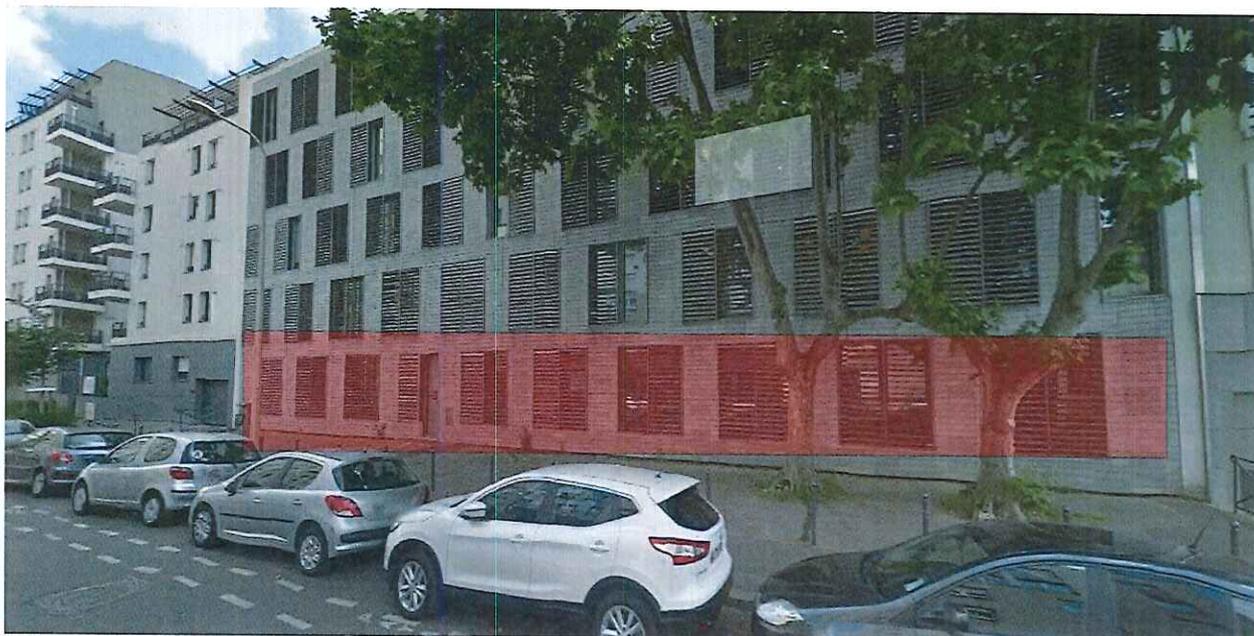
- ***Fermer la barrière d'accès en permanence. Procéder aux vérifications d'usages relatives au transporteur et au chargement.***
- ***Mettre à disposition au PC la liste des livraisons prévues au quotidien.***

L'organisme dispose de fonds importants nécessitant l'intervention d'une société privée. Le véhicule stationne devant le quai de déchargement et les agents qui sont les seuls à détenir les clés, accèdent au coffre implanté à même le quai.

#### **Préconisations :**

- ***Faire en sorte que le fourgon puisse accéder à la zone sécurisée. Refermer le sas durant toute l'opération qui doit s'effectuer hors de la vue du public.***
- ***Dégager la zone de cheminement des agents de transports de fonds de tout encombrant.***

Un immeuble de bureaux, dont la façade se situe rue feuillat, a de nombreux accès (fenêtres et porte), qui donnent directement sur la voie publique. Ses accès ne sont pas sécurisés tant au niveau de la résistance des matériaux que de la levée de doute en cas d'intrusion.



### **Préconisations :**

*La norme, dans le cas d'ouvrants accessibles donnant sur la voie publique, est pour les fenêtres, un vitrage retardateur à l'effraction de norme « P6B », soit l'ancrage d'un barreaudage installé dans les règles de l'art, soit des volets pleins. pour les portes d'un bloc norme EN 1627.*

*- Placer tous les accès, porte et fenêtres sous alarme intrusion.*

*- Placer un film sur les vitres, à opacification commandée*

Certains vitrages sont capables de s'opacifier lorsqu'ils sont mis sous tension électrique. Avec un simple interrupteur, on peut commander l'opacification d'une surface vitrée permettant de créer ainsi un écran totalement opaque à la vue mais laissant passer la lumière.

Cette nouvelle technologie appliquée à la sûreté permet :

- de rendre confidentiels à la demande des espaces vitrés (salle de réunion),
- de créer des masques (lorsqu'une personne sensible se trouve à son bureau),
- de concevoir un compartimentage visuel des espaces (canalisation de flux),
- d'assurer un complément à la protection de devantures sensibles contre l'effraction.

### **Prise d'air neuf**

Des appareils de climatisation sont accessibles au pied du bâtiment de la rue feuillat.

### Préconisations :

*- L'activité exercée dans ce bâtiment est sensible et nécessite d'une part, de sécuriser les blocs de climatisation qui seront placés hors de portée, et, d'autre part, un renforcement des vitrages et ouvrants principaux.*

#### La cour intérieure

Un auditorium en R+1 est implanté à proximité de l'entrée. Il dispose d'une entrée principale et d'une sortie de secours. Le bâtiment est sous alarme reliée au poste de garde.

La végétation n'est pas maîtrisée et occulte la vision.

Des assises (tables et bancs), prévues pour le personnel, sont implantés en bordure de clôture.



### Préconisations :

*- La végétation doit être régulièrement entretenue et taillée à hauteur d'homme, afin de ne pas occulter la vision naturelle et celle des caméras extérieures de vidéoprotection.*

*- Durant la période estivale, des personnes s'introduisent sur le site pour profiter des assises réservées au personnel. Planter une signalétique claire interdisant l'accès du site aux personnes non autorisées et surélever la clôture existante.*

#### L'auditorium

En dehors de son mode de fonctionnement, l'auditorium doit être fermé en permanence et examiné avant et après son occupation par des personnes extérieures.

## L'éclairage

Un éclairage public **fiable et performant** est indispensable sur l'ensemble du site pour accroître la sûreté et contribuer notamment à :

- dissuader un éventuel malfaiteur
- assurer une meilleure visibilité notamment dans le cas de la vidéoprotection
- faciliter le travail des forces de l'ordre à l'occasion de leurs patrouilles
- lutter contre le sentiment d'insécurité

Pour éviter les zones d'ombres, l'espacement des points d'éclairage doit être régulier (maximum 25 mètres) produire une puissance minimale de 22 lux (recommandations formulées par l'Association Française de l'Éclairage (A.F.E.) et couvrir toutes les zones de circulation.

Pour garantir un éclairage performant, divers composants doivent être pris en considération :

- les ampoules : adaptées et d'un modèle courant pour être facilement remplacées,
- les luminaires : en nombre suffisant, installés hors d'atteinte et résistants au vandalisme et aux intempéries.

Afin de minimaliser la pollution lumineuse (*cf. schéma 1*), il convient de s'assurer que la lumière soit dirigée vers la zone désirée. Ces zones doivent être éclairées avec des luminaires qui maintiennent l'émission de lumière en dessous d'un plan horizontal (*cf. schéma 2*).



Schéma 1



Schéma 2

DDSP 69 / EM / CPS

### Préconisations :

- *L'éclairage du site est peu performant, au besoin faire placer des projecteurs automatiques à déclenchement de présence.*

## Parking

73 places en surface sont prévues pour le personnel.

### **Préconisations :**

*- Une vigilance doit être apportée envers les véhicules « tampons » ou suspects en stationnement prolongé sur le parking.*

## Zones d'ombres

Il y a sur le site des zones d'insécurité, qui ne sont pas couvertes par la vidéoprotection (locaux EDF à l'entrée des véhicules, arrière du bâtiment « EPIC »). *Il est recommandé d'éclairer ces zones et de les placer sous couverture vidéo reliée au poste de garde.*

## Les ouvrants dans la clôture

L'entrée principale : elle est constituée d'un sas à ouverture alternative. Le personnel dispose d'un badge lui permettant d'ouvrir la seconde porte, une fois que la première est refermée.

Les visiteurs sonnent au vidéophone avant d'être réceptionnés par le personnel d'accueil.

### **Préconisations :**

*- Sensibiliser le personnel à la vigilance notamment lors des accès au bâtiment.*

*- Il est souhaitable que les visiteurs soient pris en charge par les services concernés.*

## Sorties de secours

6 sorties de secours disposent de contacteurs de position de porte.

## **III – VOLUMETRIE – Les volumes intérieurs**

La majorité des personnels présents déambulent librement au sein du bâtiment principal. Il n'y a pas de traçabilité des badges dont ils disposent (sauf l'accès à un laboratoire P3).

Certaines zones doivent être particulièrement protégées comme l'accès au groupe électrogène qui nous semble vulnérable.

### **Préconisations :**

*- Il est conseillé de prévoir une traçabilité des badges affectés au personnel, tant au niveau de la gestion des accès que de la présence du personnel sur site en temps réel. Une programmation des badges pour hiérarchiser les zones est aussi souhaitable.*

*- Renforcer les accès aux zones techniques (ouvrants) qui seront placées sous alarme et vidéoprotection reliées au poste de sécurité.*

### Préconisations :

- *Il est conseillé de placer l'accueil face à l'entrée principale.*
- *Créer un PCS sécurisé :*

*1 - en fermant la banque existante avec un vitrage résistant et une porte sécurisée par badge.  
2 – conception d'une structure indépendante dans un local fermé, dédiée à la sécurité/sûreté. Réception des alarmes sécurité/sûreté, gestion des caméras de vidéoprotection et fonctions annexes citées supra.*

*Le PCS doit être informé en temps réel de tout déclenchement d'alarme intrusion et devra être à même d'effectuer une levée de doute vidéo et audio.*

- *Vérifier ou faire vérifier périodiquement et de manière minutieuse l'état des serrures, des ouvrants et des rideaux.*
- *Tester régulièrement les différents dispositifs de sûreté du site et faire assurer la maintenance du matériel défectueux le plus rapidement possible.*
- *Il est primordial que les agents dédiés à la sûreté puissent se sentir investis des missions qui leur sont confiées. Cette tâche sensible ne peut être menée à bien que par la fidélisation du personnel.*
- *Le service de sûreté doit travailler de concert avec les services de police, notamment en ce qui concerne les modalités d'alerte et d'intervention.*

### III – LES DISPOSITIFS TECHNIQUES

#### La vidéoprotection

Son but est de rappeler les finalités d'un système de vidéoprotection, de souligner les éléments à prendre préalablement en compte et de formuler un certain nombre de conseils techniques destinés à améliorer les conditions de sécurité sur votre site.

Un système de vidéoprotection n'est utile que :

- ➔ s'il est installé d'une manière efficace,
- ➔ s'il est exploité d'une manière optimale,
- ➔ et si, le cas échéant, le personnel qui gère son exploitation est formé à cette tâche.

La vidéoprotection remplit un double but :

- d'une part, elle est dissuasive,
- d'autre part, elle est informative (en temps réel pour la levée de doute ou en différé).

Parallèlement, un dispositif de vidéoprotection peut :

- dissuader un acte de malveillance par une présence ostensible des caméras et d'une information substantielle,
- faire diminuer le nombre de faits commis,
- renforcer le sentiment de sécurité,

- localiser avec précision les lieux de l'infraction ou du trouble, faciliter la levée de doute,
- permettre une intervention plus efficace des services d'intervention,
- faciliter l'identification des auteurs d'infractions et l'administration de la preuve.

Le nombre de caméras nécessaires et leur implantation sont déterminés par les champs de vision des caméras, par leur résolution, ainsi que par la nature des secteurs visualisés, le dimensionnement des objets ou cibles à visualiser et le but de la vidéo-protection dans ces secteurs.

Les dimensions d'un objet ou d'une personne (cible) sur l'écran de contrôle correspondent à l'objectif recherché dans l'application du rôle de la caméra par exemple : l'identification, la reconnaissance, la détection ou le contrôle selon les recommandations suivantes :

- pour identifier la cible, celle-ci doit représenter au moins 120 % du champ de vision de la caméra, à la distance maximale d'observation souhaitée; pour une caméra numérique, le visage d'un individu doit représenter au minimum 90 × 60 pixels ;
- pour reconnaître une cible, celle-ci doit représenter au moins 50 % du champ de vision de la caméra à la distance maximale d'observation souhaitée ;
- pour l'effraction d'une cible, celle-ci doit représenter au moins 10 % du champ de vision de la caméra à la distance maximale d'observation souhaitée.

#### Dispositif de l'O.M.S.

Le site dispose de **32 caméras**, 2 dans le bâtiment principal, 2 dans le bâtiment situé rue Feuillat, 3 au niveau du quai de livraison (transport de fonds) et 25 à l'extérieur. Un nouveau projet est en cours.

Il y a des zones d'ombre qui ne sont pas couvertes par les caméras, créant de ce fait des zones pouvant, soit générer de l'insécurité, soit favoriser la dissimulation d'individus ou d'objets.

Le stockeur est placé au sous-sol dans un endroit sécurisé, 3 personnes sont habilitées à visionner les images enregistrées sur 15 jours.

#### Préconisations :

- *La qualité des images doit permettre l'identification*
- *Les caméras tant à l'extérieur qu'à l'intérieur doivent être placées sur des points de passage obligés*
- *Filmer tous les accès aux bâtiments et aux entrées sensibles*
- *Opter pour certaines caméras « intelligentes » placées dans des endroits stratégiques et qui se déclencheront à la présence avec report d'alarme au PCS.*

Les alarmes

Des alarmes sont placées en volumétrie au rez-de-chaussée des bâtiments avec report au PCS.

**Préconisations :**

*- Il est conseillé de placer tous les accès sous alarme intrusion reportée au PCS. En effet, il est préférable de détecter une intrusion le plus en amont possible.*

P0 | Vu et transmis

Le Chef du P.P.P.V

Capitaine Fabrice LARGE

Le Major de Police

