International Agency for Research on Cancer

World Health Organization

Governing Council **GC/58/18B**
Fifty-eighth Session 12/04/2016

Lyon, 19–20 May 2016
Auditorium

REQUEST FOR USE OF FUNDS FROM THE GOVERNING COUNCIL SPECIAL FUND: B. UPGRADES TO IARC PREMISES SECURITY SYSTEMS – PHYSICAL SECURITY IMPROVEMENT PLAN

CONTEXT

1. During 2015 the attacks in Paris in January at the Charlie Hebdo Magazine and the coordinated attacks across the city on 13 November drew mass international coverage. Less attention was given to an incident which occurred only 30 km from IARC at the premises of our liquid nitrogen supplier which involved a vehicle explosion and a terrorist themed execution. Since these events, France has substantially escalated security preparedness across the country with specific attention to places it sees as likely targets.

2. While the French authorities have not singled out United Nations (UN) premises among the highest at-risk locations, during 2015 the UN Security Management Team for France agreed upon four priorities for all UN Agencies in France:

1) UN premises access control needs to be reviewed, and the posture strengthened;
2) A robust system for contacting all personnel must be set up within each Agency in order to account for all during an emergency;
3) Clear focal points for security information must be clearly communicated within Agencies;
4) All personnel should be reminded about their responsibility for their personal security and that of their family, and provided with information as possible.

3. IARC followed these recommendations closely, heightening its security posture for its Headquarters in Lyon. Already IARC had been working closely with the Prefecture Security service and the local police authorities throughout 2015 in order to ensure appropriate and direct contacts and attention to IARC's presence in Lyon, which are now well in place. Heightened security procedures including screening of all visitors and packages were also implemented.

4. Following the November attacks access control was enhanced by implementing revised rules on pedestrian and vehicular access to the compound. The existing emergency "sms" system was also improved to allow personnel to respond to a broadcast message with their and their recognized dependent's location and level of safety in the event of an emergency.

5. In parallel, in order to build and develop a cost effective security improvement plan, the IARC Secretariat decided to go through several security reviews in order to assess and determine the status and effectiveness of the physical security at IARC:

- An internal assessment of the overall security and safety level of IARC premises and the review of security policies and procedures;
- An internal review of all building management real time systems, including security monitoring systems (Annex 1);
- An external global security review, led by the French Police and its specific branch for public safety (Annex 2 includes recommendations).

6. The United Nations Department of Safety and Security (UNDSS) issued an information bulletin on 28 January 2016 which recognized that security arrangements for the UN in Europe have not been of major concern, unlike in other countries/regions where the UN has been targeted by terrorists. This may have led to a lack of security awareness or complacency, translating into significant vulnerability for UN premises. The UNDSS bulletin thus detailed some of the security measures that must be implemented in all European UN premises in the following areas:

- Perimeter Protection;
- Security screening and visitor management;
- Intrusion detection systems, alarms and CCTV;
- Security force training and response operations;
- Hostile surveillance and reconnaissance detection (HSRD);
- Host country coordination;
- Safe havens and compartmentalization;
- Communications;
- Safety, fire safety and emergency preparedness;
- Staff training.

VULNERABILITIES OF IARC SECURITY SYSTEM AND IMPROVEMENT PLAN

7. The security reviews highlighted several vulnerabilities of IARC's physical security system, including architectural, technological, procedural and human elements. These areas of concern were mapped with the recommendations made by UNDSS in order to put together a consolidated physical security improvement plan to enhance IARC's security risk mitigation posture. IARC management reviewed the plan and prioritized actions according to their feasibility.

8. The resulting plan is set out in the table below, indicating actions already taken and those still required in order to limit vulnerability. In order to be able to implement the remaining mandatory improvement actions, the IARC Secretariat requests the Governing Council to consider allocating €120 000 from the Governing Council Special Fund according to the following table which details the plan, proposed actions and the proposed budget to fund additional and necessary features.

Physical security Areas	Vulnerabilities at IARC	Actions already done or launched	Further actions	Budget Requested
Perimeter protection	Light barriers and bollards at the delivery area entrance and exit do not prevent pedestrian entrance.		Replace the barriers by motorized gates, which would constitute a better deterrent against intruders.	€14 000
	Once gates and barriers at the parking entrance and exits are open, and when unguarded, other unauthorized pedestrians or vehicles can easily penetrate into the compound.	Reduce the number of gates that can be open at the same time, restrict the time slots when the gates can be open, reinforce the control with additional security guards during the time slots and train security guards to better control the access and exits.		
	Too few "no trespassing" signs.	Additional signs are being put in place on the fence.		
Security screening and visitor management	Obsolete interphones.	Replace all interphones.		
	Set up of the main entrance not suitable for comfortable and effective security control.		Redesign the reception desk and security guard desk in order to have a better view of the main entrance of the compound and to enhance the security guards movements.	€15 000
	ID cards not always worn visibly.	Regular reminder of security and safety procedures to all staff and all visitors.		
	Visitors not always escorted once in the premises.	Regular reminder of security and safety procedures to all staff.		
	Obsolete access control system.		Migrate the access control system to a new server.	€4 500
	No screening for deliveries.		Add a new warden station for the guard to be protected against changes of the weather and potential assailants.	€5 000

Physical security Areas	Vulnerabilities at IARC	Actions already done or launched	Further actions	Budget Requested
Intrusion detection systems, alarms and cameras (CCTV)	Obsolete cameras.		Replace obsolete cameras.	€10 000
	Zones not covered by cameras.		Add cameras where necessary.	€10 000
	No intrusion detection on the perimeter.		In order to balance the low fence vulnerability and to increase the early detection of unauthorized persons, set up of a new intrusion detection system.	€45 000
	Obsolete BMS (building management system).	Migrate BMS to a new server.		
	Dark zones and obsolete lightning.		Set up additional lights where adequate and necessary.	€6 500
Security force training and response operations	Security guards not always following instructions and procedures.	Regular reminder of procedures, training with emergency scenarios were made for the security guards.		
Hostile surveillance and reconnaissance detection	Low awareness.	- Regular reminder of security awareness. - Security page on intranet launched to inform on procedures and give access to tips and information regarding security and on HSRD.		
Host country coordination	Lack of information from the host country authorities.	Regular liaison and meetings, contacts with local and central authorities.		
Safe havens and compartmentalization	Public events in Grand Hall exposed to all visitors and potential unauthorized entries.		Add a layer and security compartment with interlocking system of the sas doors.	€10 000

Physical security Areas	Vulnerabilities at IARC	Actions already done or launched	Further actions	Budget Requested
Communications		Mass SMS already in place enhanced, regularly tested and improved upon.		
Safety, fire safety and emergency preparedness		- Yearly fire safety training mandatory to all staff, when additional security information is also disseminated. - Yearly evacuation exercise. - Fire safety system well maintained and well and regularly tested; regular liaison with the local Fire Department.		
Staff training	UNDSS travel security training done regularly but no specific training regarding active shooter scenarios.	Remind staff to follow UNDSS travel security training regularly.		
		Specific training security for women.		
		Security instructions and advice disseminated.		
				€120 000

Annex 1 – Internal review of all building management real time systems

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

- **Serveur PABX**
  - Age : Dernier Update 2007
  - Localisé : Salle Opus
  - Constructeur : Alcatel
- **Serveur Sirius**
  - Age : 2010
  - Localisé : VM salle Serveur Tour
  - 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. 1ère Phase = 3600€ + 2750€

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

   b. 2ème Phase = environ 35 000€ (ou contrat de maintenance évolutif)

- Migrer XBS vers une plateforme EBI/IP
- Migrer EBI Total vers VMware
  - Problème de sauvegarde manuelle résolu
  - Problème de reprise d'activité résolu car beaucoup plus rapide et indépendant du matériel
  - 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€
  - Ajouter une carte d'extension IP au niveau des controleurs
  - Migrer vers un logiciel SiPass
  - 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.
  - Contrat de Maintenance sur controleurs.

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
  - 2 coupures le mois dernier
- Impact :
  - Aucun Monitoring Congélateurs, Chambres Froides
  - Aucun contrôle sur éléments techniques (climatisation, chauffage, …)
  - 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 :
  - Durant les 3 dernières années, il y a eu 4 pannes informatiques. Chaque panne a duré de ½ journée à 4 jours.
- Impact :
  - Aucun moyen de contrôler certains éléments très importants : Climatisation, chaufferie …
  - Aucun Monitoring Congélateurs, Chambres Froides
  - 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 :
  - 5 Pannes depuis 2010 sur Automates
  - 1 panne sur Bus Analogiques carte de communication Serveur
- Impact :
  - Aucune communication entre Automates et le serveur
  - Aucun Monitoring
  - 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. 1ère Phase = 3600€ + 2750€

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

b. 2ème Phase

- Migrer XBS vers une plateforme EBI/IP = 35 000€ ou contrat de maintenance évolutif
- Migrer EBI Total vers VMware
  - Problème de sauvegarde manuelle résolu
  - Problème de reprise d'activité résolu car beaucoup plus rapide et indépendant du matériel
  - 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

- Probabilité : 1 fois depuis 2010
- 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€
  - Interphone portillon CAT
  - Interphone Parking CAT
  - Interphone Portillon AFL
  - Interphone Parking AFL
  - Interphone Quai AFL
  - Interphone Entrée Quai
  - 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
  - 2 coupures le mois dernier
- Impact :
  - Aucun Monitoring du Site pour les agents de Sécurité
  - 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 :
  - Aucun Monitoring du Site pour les agents de Sécurité
  - 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 :
  - Alimentation
  - Mémoire
  - HDD
- Remonter d'alerte sur la machine et/ou sur la RAID
- Contrat de maintenance sur Caméras
- Ajouter plusieurs Caméras Infra-rouge
  - Pour Parking
  - Accès Quai
  - 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
  - Meilleur 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 2ème 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 2ème 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 2ème 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.

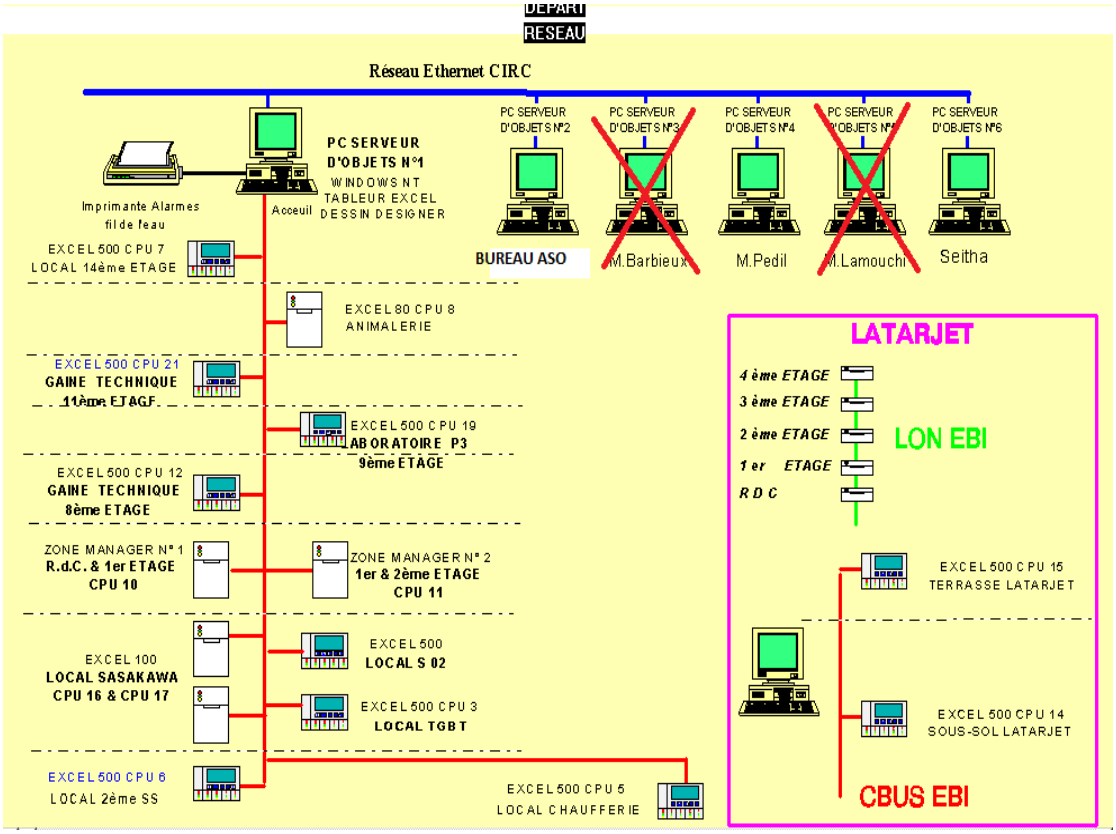
XBS de Honeywell est un outil de supervision qui nous permet de contrôler différents éléments à distance (Congélateurs, …).

Cet outil nous permet de :

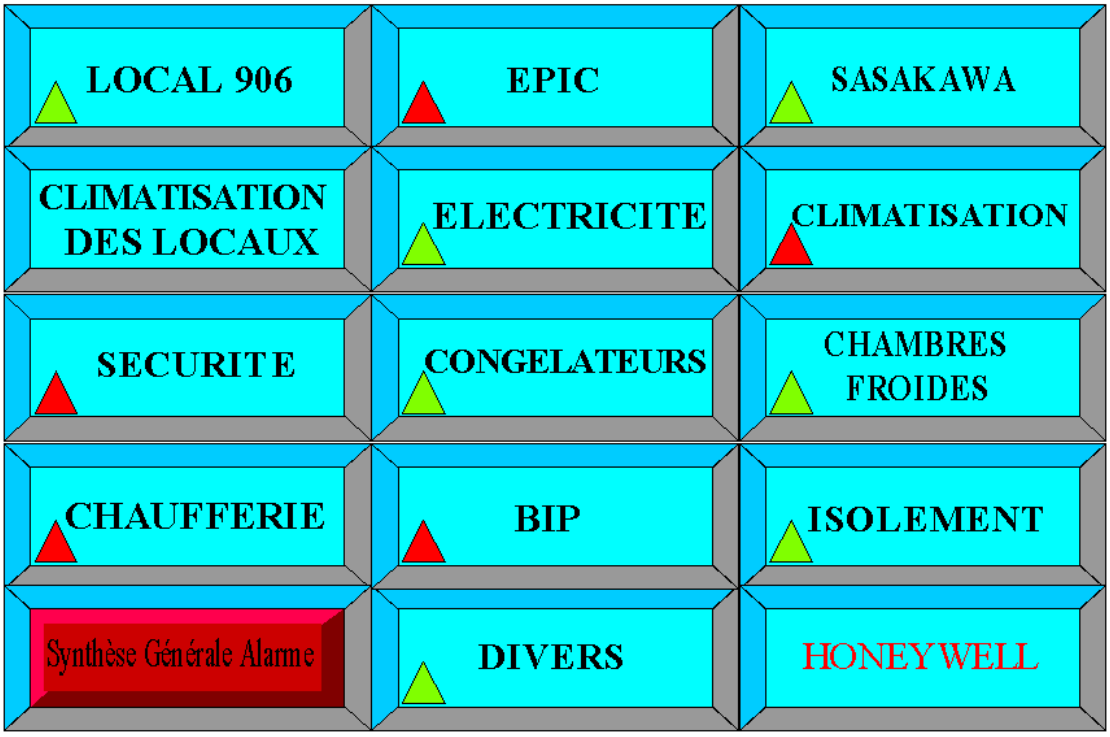
- Réaliser des économies d'énergie en adaptant les consommations d'énergie
- Apporter des solutions de confort aux occupants
- Sécuriser le bâtiment

Notre installation au CIRC

Nous avons une architecture de base suivante :



Dans notre XBS, nous pouvons gérer les éléments suivants :



Les problèmes et limites actuels niveau informatique :

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

Améliorations à apporter :

- Une migration vers la plateforme EBI
  - Changement des automates vers un échange de données via IP.
  - Migration de tous les points de contrôle XBS vers EBI existant.
  - 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 – Entreprise 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.

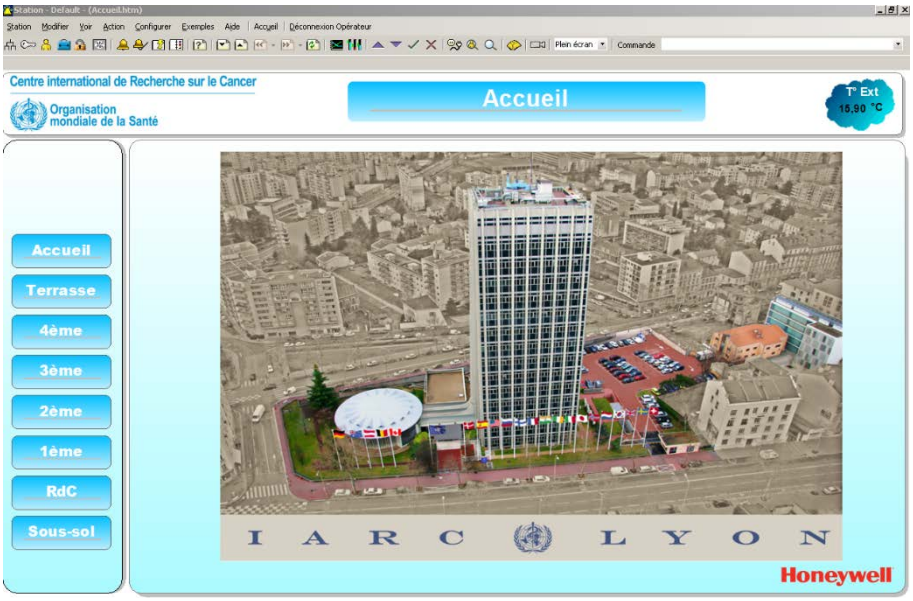
Cela rend l'administration informatique beaucoup plus facile à gérer.

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.

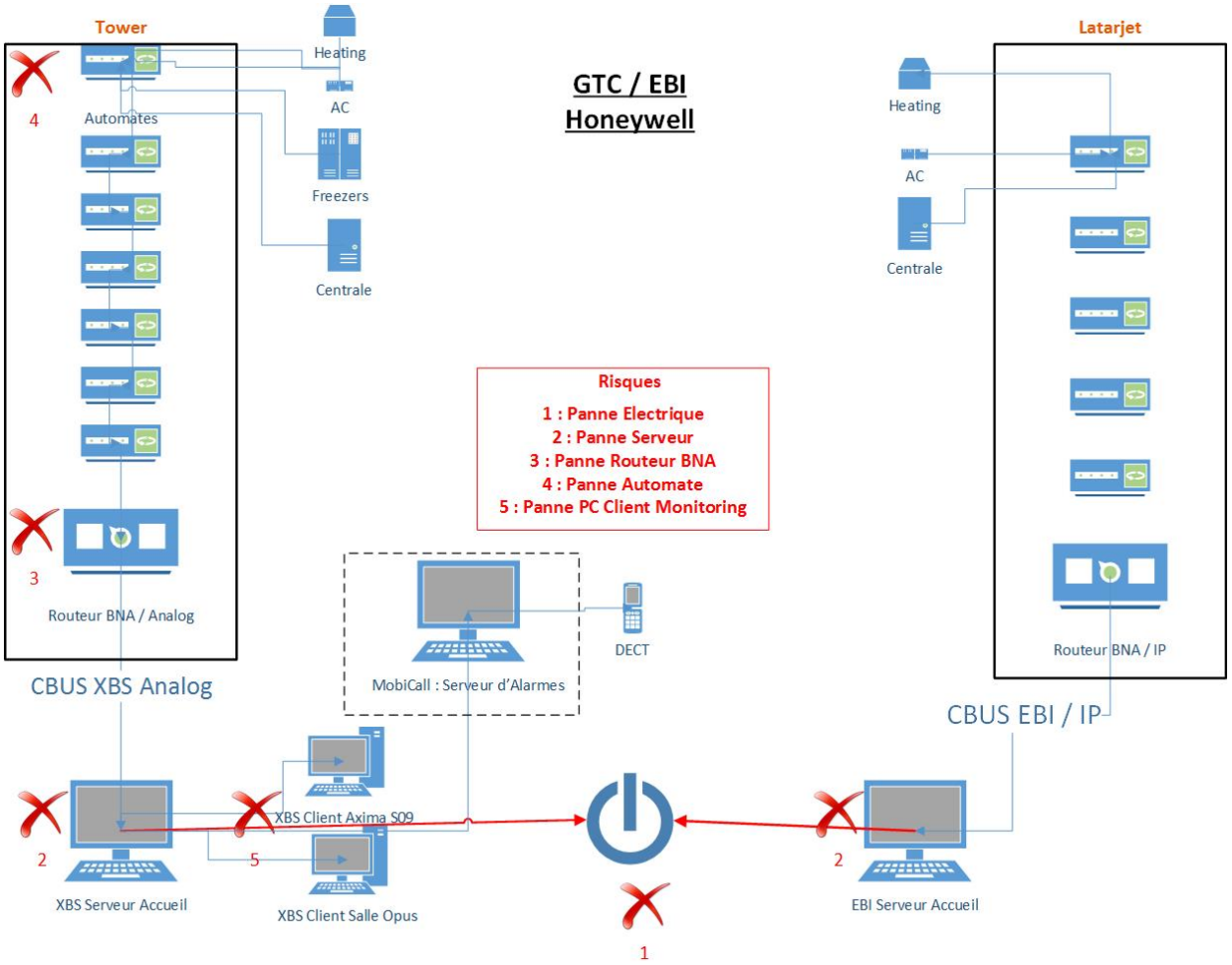
Ce serveur est physiquement situé à l'accueil.

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


Tower
Heating
AC
Freezers
Centrale
4
Automates
3
Routeur BNA / Analog
CBUS XBS Analog
GTC / EBI
Honeywell
Risques
1 : Panne Electrique
2 : Panne Serveur
3 : Panne Routeur BNA
4 : Panne Automate
5 : Panne PC Client Monitoring
MobiCall : Serveur d'Alarmes
DECT
Latarjet
Heating
AC
Centrale
Routeur BNA / IP
CBUS EBI / IP
2
XBS Serveur Accueil
5
XBS Client Axima S09
XBS Client Salle Opus
1
2
EBI Serveur Accueil

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 1er 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

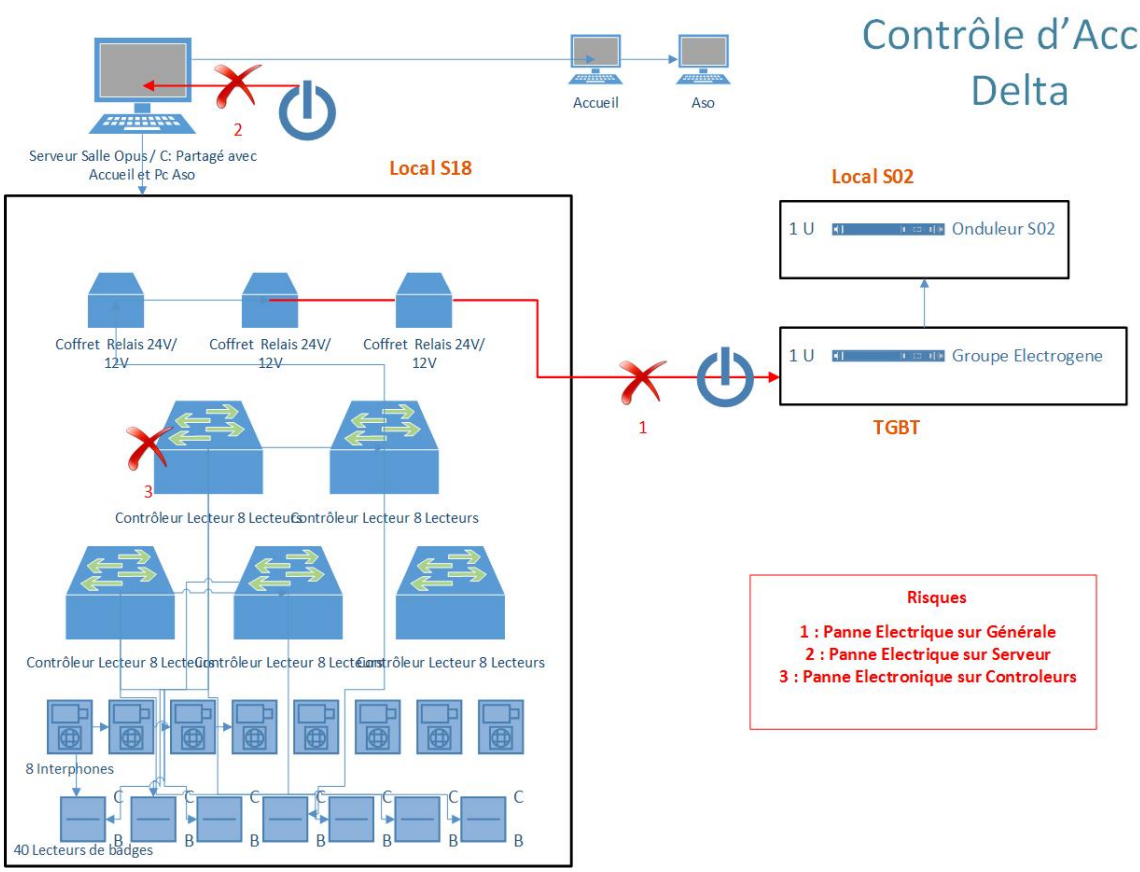
Badgeur ASO situé à en R04.

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.


Contrôle d'Accès Delta
Accueil
Aso
2
Serveur Salle Opus / C: Partagé avec Accueil et Pc Aso
Local S18
Local S02
1 U
Onduleur S02
1 U
Groupe Electrogene
TGBT
1
Coffret Relais 24V/ 12V
Coffret Relais 24V/ 12V
Coffret Relais 24V/ 12V
3
Contrôleur Lecteur 8 Lecteurs
Contrôleur Lecteur 8 Lecteurs
Contrôleur Lecteur 8 Lecteurs
Contrôleur Lecteur 8 Lecteurs
Contrôleur Lecteur 8 Lecteurs
8 Interphones
40 Lecteurs de badges
Risques
1 : Panne Electrique sur Générale
2 : Panne Electrique sur Serveur
3 : Panne Electronique sur Controleurs

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

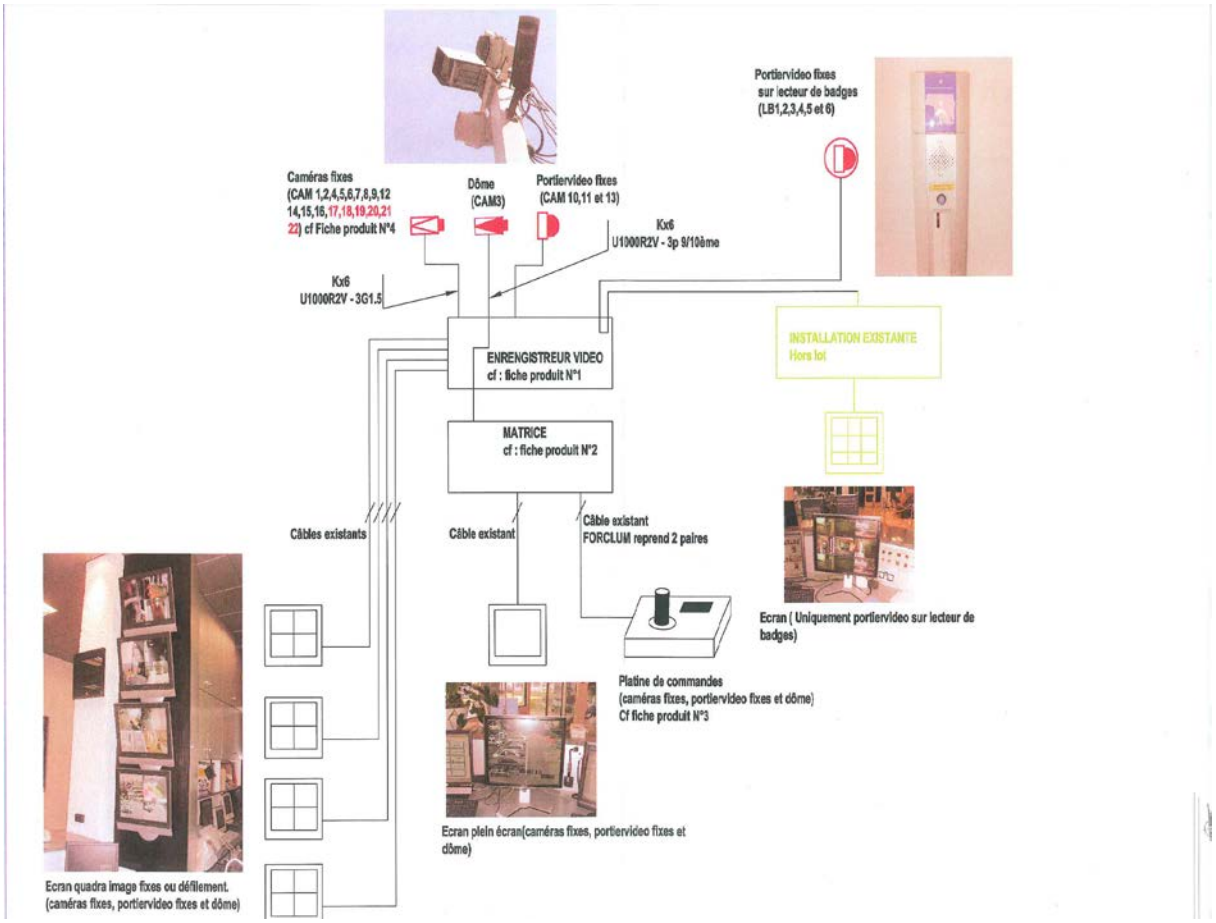
Le cœur du réseau de caméras se situe dans la baie de vidéosurveillance en S02.

Dans cette baie sont rangés :

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

Alimentation Electrique :

- Alimentation Générale
- Onduleurs S02

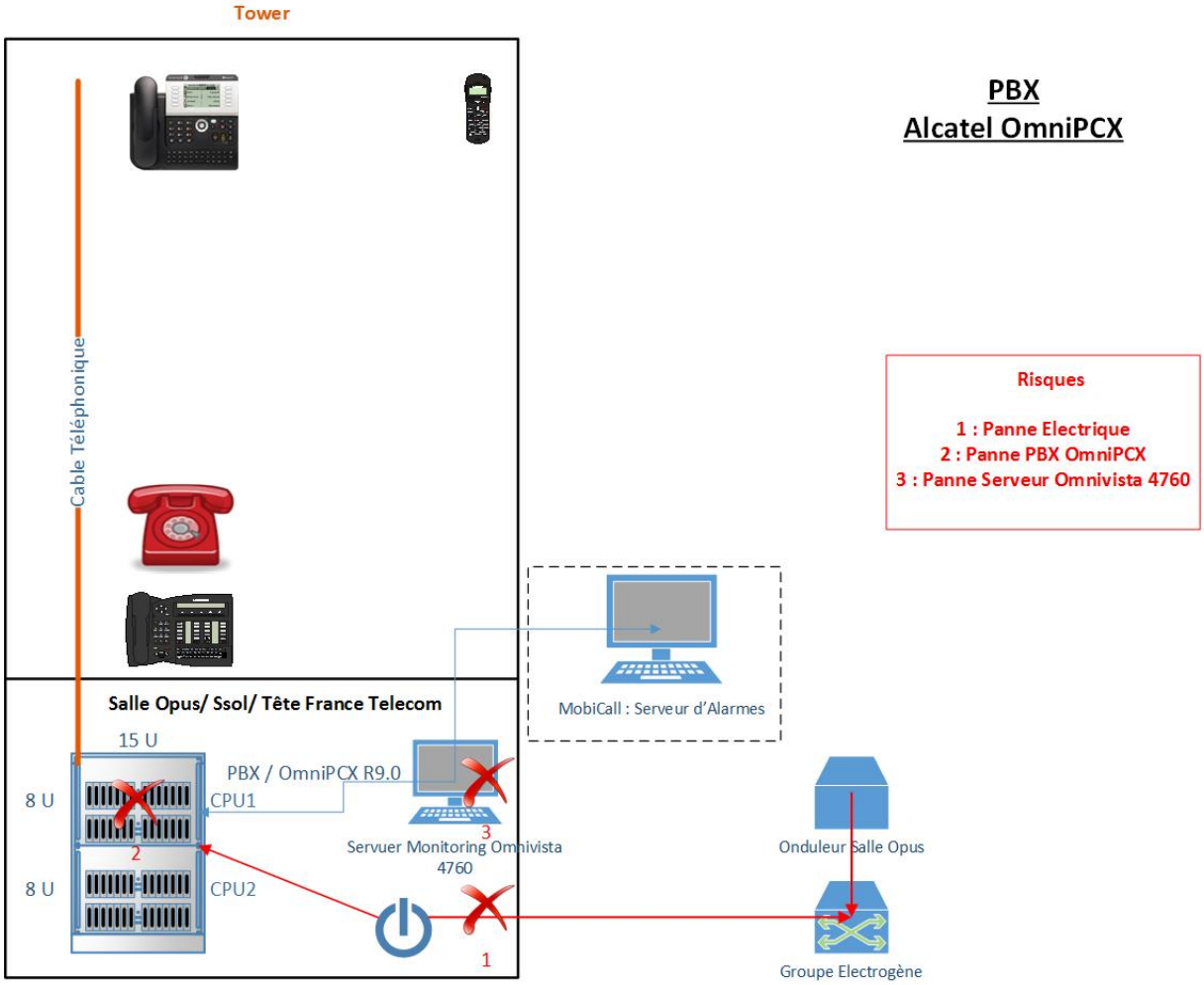


5. Infrastructure de Téléphonie Alcatel

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.



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

MINISTERE DE L'INTERIEUR

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

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

MINISTERE DE L'INTERIEUR

DIRECTION GENERALE
DE LA POLICE NATIONALE

DIRECTION DEPARTEMENTALE
DE LA SECURITE PUBLIQUE
DU RHONE

État-Major / P.P.P.P.V.

C.P.S.

Lyon, le 01 Février 2016

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

à

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 cancéropôle 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 cancérogènes 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 amphitéatre 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 – <u>PERIPHERIE</u> – <u>Les abords ou zone urbaine</u>

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 Bonnevay 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.

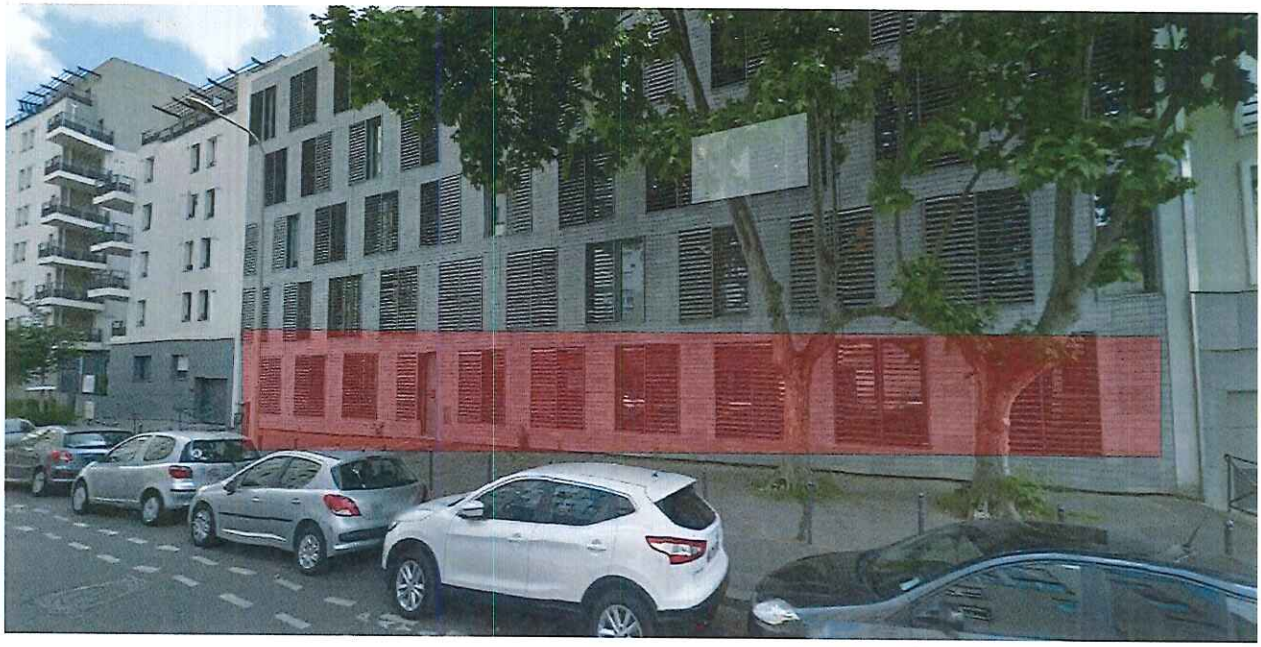
L'organisme dispose de fonds importants nécessitant l'intervention d'une société privée. Le véhicule stationne devant le quai de déchargement et les agents qui sont les seuls à détenir les clés, accèdent au coffre implanté à même le quai.

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. Implanter 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

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 véhicule, 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 déclencherons 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.

PO Vu et transmis

Le Chef du P.P.P.P.V

Capitaine Fabrice LARGE

Le Major de Police