

CENTRE HOSPITALIER UNIVERSITAIRE GRENOBLE
ALPES

DIRECTION DES SERVICES TECHNIQUES



REGLES DE REALISATIONS
DES
INSTALLATIONS COURANT FAIBLE
Vidéosurveillance et Systèmes anti-intrusion

1 Table des matières

1	DESCRIPTION DU SYSTEME DE DETECTION INTRUSION	1
1.1	PRINCIPE DE FONCTIONNEMENT	1
1.2	MATERIELS.....	1
1.2.1	<i>Les Détecteurs volumétriques</i>	<i>1</i>
1.2.2	<i>Les Détecteurs d'ouverture.....</i>	<i>1</i>
1.2.3	<i>Les Détecteurs Bris de glace</i>	<i>1</i>
1.2.4	<i>Les Barrières à infrarouge actif</i>	<i>1</i>
1.2.5	<i>Exploitation de l'alarme intrusion</i>	<i>2</i>
1.3	DEUX TYPE DE CENTRALE INTRUSION SONT UTILISE SUR LE CHU DE GRENOBLE	2
2	DESCRIPTION DU SYSTEME DE VIDEOSURVEILLANCE	3
2.1	PRINCIPE DE FONCTIONNEMENT	3
2.2	MATERIELS.....	3
2.2.1	<i>Enregistreur Numérique</i>	<i>3</i>
2.2.2	<i>Les Licences</i>	<i>4</i>
2.2.3	<i>Les caméras.....</i>	<i>4</i>
2.2.4	<i>Les caissons extérieurs et support</i>	<i>5</i>
2.2.5	<i>Les écrans</i>	<i>5</i>
2.2.6	<i>Convertisseur de média</i>	<i>5</i>
2.2.7	<i>Les Décodeurs.....</i>	<i>5</i>
2.2.8	<i>Le logiciel d'exploitation.....</i>	<i>6</i>
2.2.9	<i>Stockage numérique.....</i>	<i>6</i>

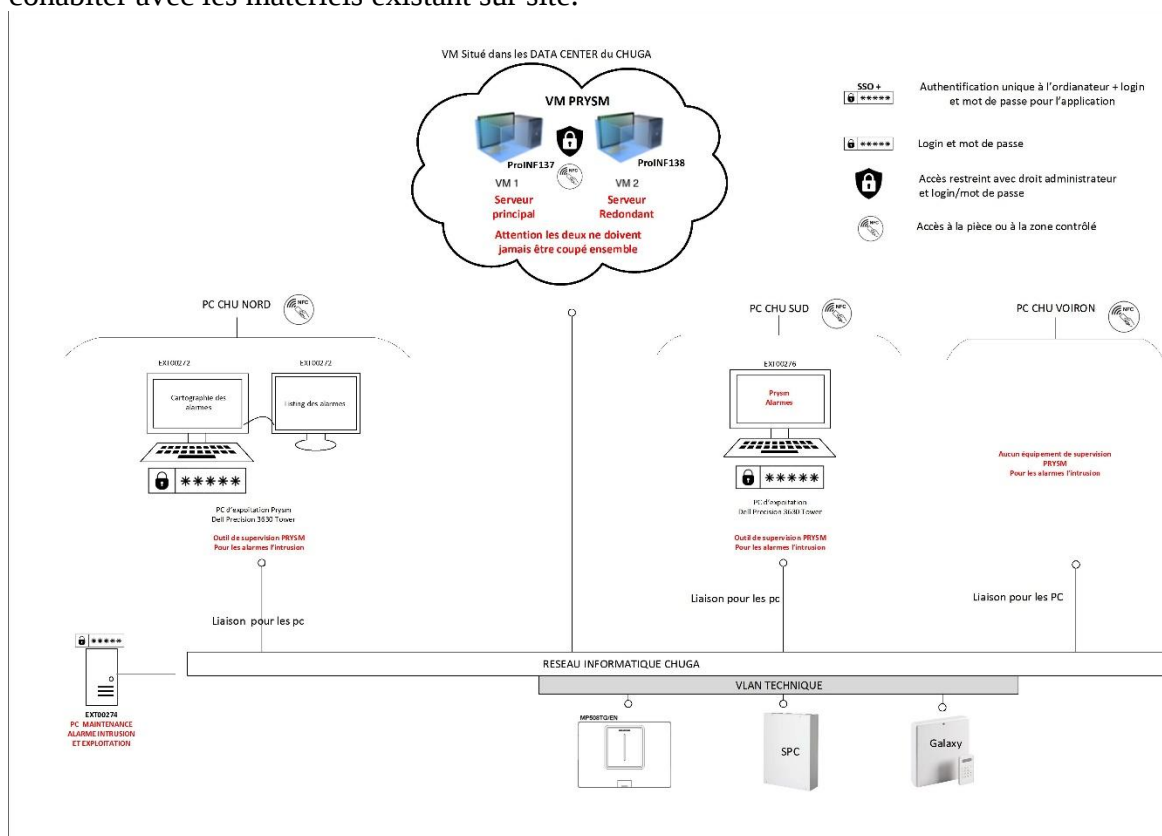
Tableau de révision historique

Indice	Date	Nom	Détail
V0	16/06/22	LGU / LLAV	Document initial
V1	20/03/2026	LLAV	Modification architecture vidéo et intrusion

1 DESCRIPTION DU SYSTEME DE DETECTION INTRUSION

1.1 Principe de fonctionnement

Le système de Détection Intrusion sera de type installation filaire sauf dérogation du CHU permettant l'utilisation de l'ensemble des périphérique d'alarme filaire « Détecteur volumétrique, contact d'ouverture, choc, bris de vitre, etc Le système devra être communiquant et administrable à distance, afin d'avoir une gestion plus simple pour l'exploitant dans un souci d'économie de matériel et de simplicité d'utilisation. Il devra cohabiter avec les matériels existant sur site.



1.2 Matériels

1.2.1 Les Détecteurs volumétriques

-Les détecteurs devront être adapté au risque et à l'environnement (animaux domestique, long couloir, grand espace. Une technologie devra permettre de parer au fausse alarme.

1.2.2 Les Détecteurs d'ouverture

- Les détecteurs seront de type magnétique.

1.2.3 Les Détecteurs Bris de glace

- Les détecteurs seront de type choc.

1.2.4 Les Barrières à infrarouge actif

- Les barrières à infrarouge actif sont constituées de cellules émettrices qui génèrent des faisceaux de lumière infrarouge invisibles. Des cellules réceptrices détectent et analysent la bonne réception des faisceaux. À la coupure d'un ou plusieurs faisceaux, le système transmet une information d'alarme.

1.3 Exploitation de l'alarme intrusion

A. Généralités

Les zones de contrôle pourront être configurables depuis un PC, par un module permettant de connecter la centrale sur un réseau informatique de type LAN / WAN (sous protocole TCP/IP).

Fonctionnalités

- Transmissions aux protocoles intrusion sur réseaux LAN / WAN (TCP/IP).
- Compatible avec le logiciel de télémaintenance et de programmation du fabricant.

B. Armement et désarmement de zones d'intrusion

L'opérateur pourra définir les méthodes d'armement et de désarmement à utiliser dans la zone d'intrusion pour en modifier l'état.

a. Méthodes d'armement et désarmement d'une zone d'intrusion marche total par code confidentiel

b. Méthodes d'armement et désarmement d'une zone d'intrusion marche Partiel par code confidentiel

Possibilité d'éjection d'une zone en cas de dysfonctionnement.

1.4 Type de Centrale intrusion sont utilisé sur le CHU de Grenoble

Vanderbilt gamme spc

Ces centrales seront paramétrées par ordinateur et le programme sauvegardé et remis à l'exploitant (CHU DE GRENOBLE). La centrale devra être évolutive. Elle sera toujours dimensionnée avec une réserve de 20% permettant son évolution dans le temps.

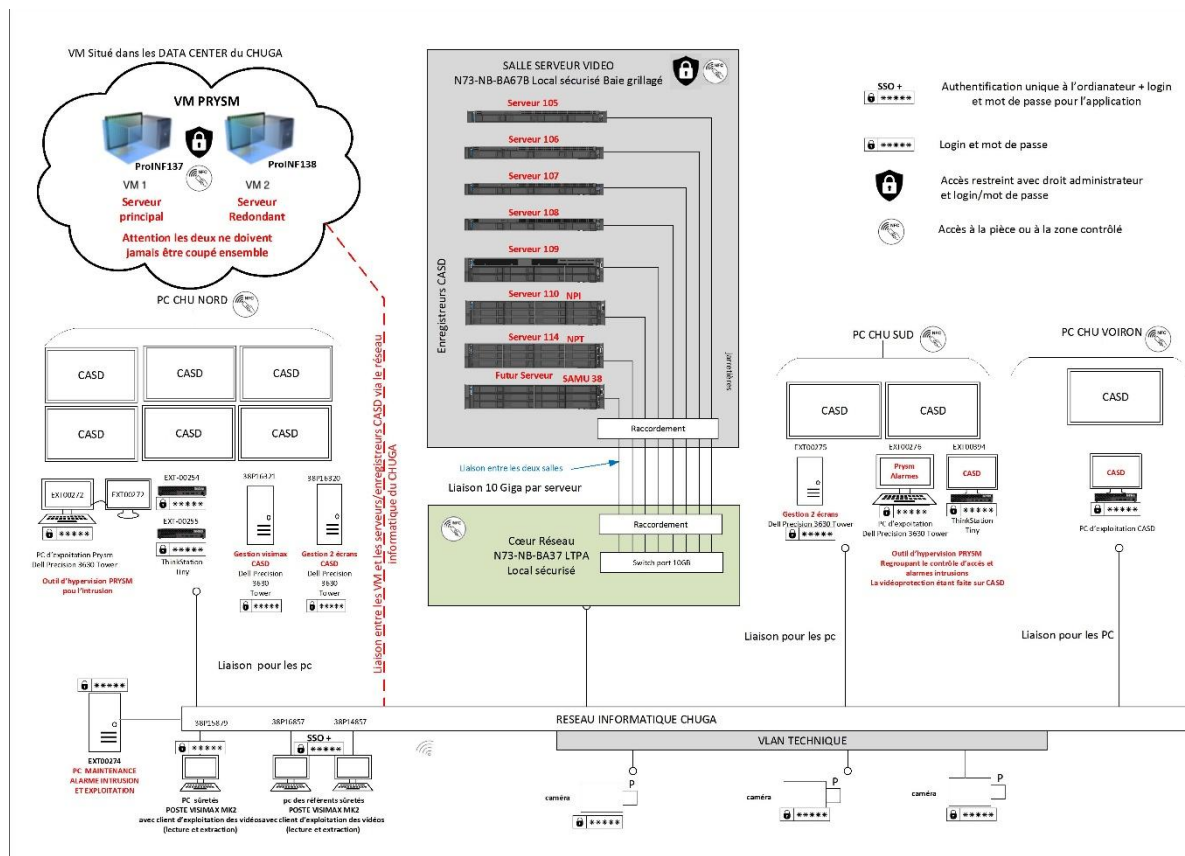
Elle intégrera en plus un serveur WEB et une interface IP native, lui permettant de transmettre ses alarmes vers des destinataires IP.

Elle devra pouvoir donner un accès web sécurisé à l'utilisateur via internet (accès protégé HTTPS), pour l'utilisation quotidienne via un PC et pouvoir donner un accès web sécurisé à l'installateur via internet (accès protégé HTTPS), pour le paramétrage et la maintenance de ce système.

2 Description du système de Vidéosurveillance

2.1 Principe de fonctionnement

Le système de vidéosurveillance devra être intégré au réseau ETHERNET afin de centraliser le cœur système dans un seul et même lieu dans un souci d'économie de matériel et de simplicité d'utilisation. La visualisation s'effectuera des moniteurs de contrôle situés les deux PC de surveillance. Le système de vidéo devra pouvoir transmettre via le réseau Ethernet, avec accès sous mot de passe les images aux administrateurs déclarées en préfecture. Conservation des images sur 30 jours.



2.2 Matériels

2.2.1 Enregistreur Numérique

Les enregistreurs numériques de marque CASD (ZA Actipôle - 296, rue de la Béalière - Bâtiment E - 38113 VEUREY-VOROIZE). Le NVR VisiMAX permet la gestion en simultané de l'enregistrement de 96 caméras IP mégapixels ainsi que de 96 canaux audio. Un nombre illimité de NVR peuvent être empilés afin de permettre le déploiement d'une solution multi-sites ou pour prendre en charge des systèmes nécessitant l'enregistrement et la gestion d'un nombre illimité de caméras. Un contrôle centralisé de systèmes NVR et DVR est possible grâce au logiciel multi-site VisiMAX Supervision.

Le NVR VisiMAX est compatible avec de nombreux formats de compression : MPEG4 et H.264, ainsi qu'avec une grande variété de modèles de caméras IP, fixes, mobiles, HD, et d'encodeurs.

Marques compatibles : Acti, Arecont, Arlotto, Axis, Bosch, COE, Dallmeier, Dynacolor, Eneo, Evibox, HIK, NKF, Panasonic, Pelco, Samsung, Sanyo, Siquira, Sony, Traficon, UDP, UTC, Verint, Vivotek, ZTE.

Les enregistreurs seront dotés d'un processeur puissant et d'une technologie de gestion de la mémoire permettant plusieurs opérations simultanées enregistrement, relecture, extraction, consultation distante, rediffusion de flux.

La face avant permet d'accéder facilement au lecteur de DVD-RW, à deux port USB v2.0, d'une sortie **VGA**, et aux disques durs amovibles. Les ingénieurs système disposent ainsi d'une méthode rapide et pratique leur permettant d'augmenter la capacité de stockage NVR sur le terrain et d'intervenir facilement pour des opérations de maintenance.

- 5 x Serveur VisiMAX et 1 serveur de spairedynamique

2.2.2 Les Licences

ENREGISTREMENT :

- Licence VisiMAX permettant l'acquisition et l'enregistrement de caméra IP, pilotage des dômes, 40 marques compatibles, résolution CIF à 4K, gestion unicast ou multicast, serveur Web et 3G. Gestion jusqu'à 96 caméras par serveurs, 4000 caméras par site. Licence nécessaire pour chaque serveur
- Ajout d'une voie IP supplémentaire (caméra)
Tout rajout de voie après la période de maintenance nécessite une mise à jour

2.2.3 Les caméras

Les caméras devront être adapté à l'environnement à filmer. Elles devront être au minimum :

- Résolution 4MP avec 30 i/s et la norme H.264
- Mode jour/nuit authentique (filtre IR-Cut) plus éclairage IR si besoin
- Caméra indice de protection (IP66) pour l'extérieur ou anti vandalisme.
- alimentation PoE+ (Power over Ethernet PoE IEEE802.af)
- Zoom/focale réglables par navigateur
- Accès simultané et contrôle des images individuellement.
- Fonction multicast intégrée pour les vidéos MPEG-4 H.264 et H265..
- Filtre IP limitation de l'accès à la caméra à un ou plusieurs utilisateurs.
- Protection par mot de passe pour permettre l'accès. L'administrateur détient le plus haut niveau d'accès et de contrôle sur la caméra.
- Conforme au standard **ONVIF PROFILE S**
- Nombre minimum de fenêtres de masquage de vie privée : 8 masques floutés quadrangulaires dynamiques et paramétrables par caméra
- Température de fonctionnement : - 20°C à + 50°
- Selon le besoin des caméras motorisé (PTZ) type dôme IP jour/nuit d'extérieur FullHD à très haute résolution avec objectif à zoom motorisé x30 peuvent être demandé. Rotation sans butée : azimut : 360°

Le CHU de Grenoble possédant les outils de contrôle au niveau du PC SURETE NORD, SUD et VOIRON

Masquage dynamique des zones de vie privée

Afin de respecter la loi du 21 janvier 1995 et son décret d'application du 17 octobre 1996 en matière de

protection de la vie privée, les caméras extérieures intégreront un dispositif de masquage dynamique de la partie d'image concernée, sans occulter systématiquement la totalité de l'image visualisée.

La partie masquée sera dynamiquement ajustée aux mouvements des caméras et du zoom et sera activée à partir d'une valeur de zoom paramétrable pour chaque zone de masquage.

Les caméras dômes seront équipées d'un minimum de 8 zones de masquage privatif par caméra. Les masques seront de type masques floutés (masque mosaïque floutés).

Les masques seront des formes quadrangulaires paramétrables indépendamment en hauteur et en largeur afin de définir précisément les contours des fenêtres et blocs de fenêtre à masquer.

Il est obligatoire que le paramétrage et la définition des masques de zones de vie privée soient réalisés depuis le poste d'exploitation via l'interface graphique du logiciel, par une personne autorisée

en présence d'un responsable d'exploitation (confidentialité). Les opérateurs d'exploitation ne pourront en aucun cas dévalider ce masquage.

Les paramètres de ces fenêtres de masquage doivent être sauvegardés dans la caméra, y compris en cas de coupure prolongée de l'alimentation électrique de celle-ci.

2.2.4 Les caissons extérieurs et support

Les caissons extérieurs devront être équipés d'un pare soleil, également chauffés et thermo statés et devront avoir leur indice de protection = IP66.

2.2.5 Les écrans

Les écrans permettant la visualisation des caméras seront installés dans le local PC SURETE. Ces écrans devront être de type : Ecran plat taille selon bordereau et demande à technologie LED.

MONITEURS

L'affichage des caméras se fera en fixe, cyclique ou mosaïque sur moniteur ou écran plat TFT- LED 42" muni d'une sortie informatique et d'une sortie vidéo, à fixer au mur.

Il doit au minimum avoir les caractéristiques suivantes :

- Écran de surveillance 42 minimum
- Format 16:9
- Norme HDTV 1080P
- Résolution 1920x1080
- Rétroéclairage LED
- Balayage 100HZ mini
- Luminosité 500 cd / m2 mini
- Contraste élevé 1500 :1
- Angle de vision 178° vertical et horizontal
- Temps de réponse 8 ms
- Ecran anti-rayure et anti- reflet
- Connectique HDMI

2.2.6 Convertisseur de média

Le convertisseur de média PoE (Power over Ethernet) permet d'alimenter les appareils réseau via la connexion de données CAT5 existante. Le convertisseur de PoE Ethernet à Fibre 10/100/1000M fournit une solution économique pour augmenter la distance d'un réseau existant avec un câblage fibre. En même temps, ils fonctionnent comme des injecteurs PoE pour alimenter des appareils tels que des téléphones IP, des équipements de vidéo conférence, des caméras IP et des appareils Wi-Fi sur câbles UTP en cuivre. Une alimentation personnalisée est également disponible pour ce genre de convertisseur de média PoE.



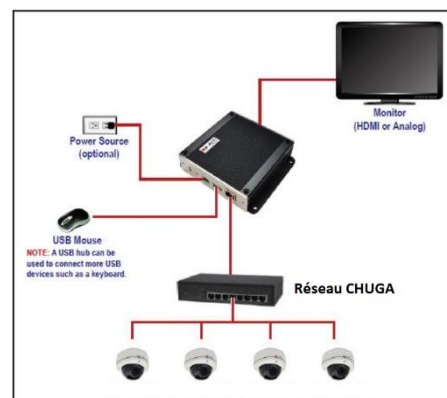
2.2.7 Les Décodeurs

Les décodeurs permettront de remonter des caméras uniquement en visualisation.

Ils seront raccorder sur des moniteurs en HDMI.

Ces décodeurs devront répondre aux caractéristiques suivantes :

- Transmetteur vidéo IP (Décodeur).
- Max 16 voie Vidéo.
- 1 port RS485/422, Jusqu'à 30ips en 4 CIF.
- Alimentation PoE norme IEEE 802.3af.
- Définition 4CIF 25 ips.
- Résolution 640 X 480, 704 X 576, 720 X 480, 1920 X 1080
- Compression H.264, MPG4



- Protocole ARP, HTTP, ICMP, IP, RTP, RTSP, TCP, UDP, UPnP
- Connecteur RJ-45 , BNC
- Signal NTSC, PAL sortie HDMI
- Ethernet (10/100 Base-T)

2.2.8 Le logiciel d'exploitation

Le logiciel permettant la visualisation, le stockage et la saisie simultanés de services vidéo, audio et de données de qualité supérieure, à haute résolution.

Le logiciel devra obligatoirement présenter une évolutivité, pouvant prendre en charge un nombre important de caméras vidéo et de sources audio.

Accessibilité des Utilisateurs par mots de passe et droits d'accès, et historisation des logs des actions faites.

2.2.9 Stockage numérique

Attention à chaque rajout de caméra il sera nécessaire de recalculer le temps de sauvegarde réel.

Ce temps devra être maintenu conforme aux déclarations préfectoral du CHUGA à avoir 30 jours de profondeur d'enregistrement.