UNIVERSITÉ DE NANTES

DÉLIBÉRATION N°2019-12-20-18
du Conseil d'Administration de l'Université de Nantes

Séance du 20 décembre 2019

POINT 15 – APPROBATION DU SCHEMA DIRECTEUR DE MISE EN SURETE

LE CONSEIL D'ADMINISTRATION

VU le code de l'éducation ;
VU les statuts de l'université de Nantes ;
VU l'avis du comité d'hygiène, de sécurité et des conditions de travail du 25 novembre 2019 ;

APRÈS EN AVOIR DÉLIBÉRÉ,

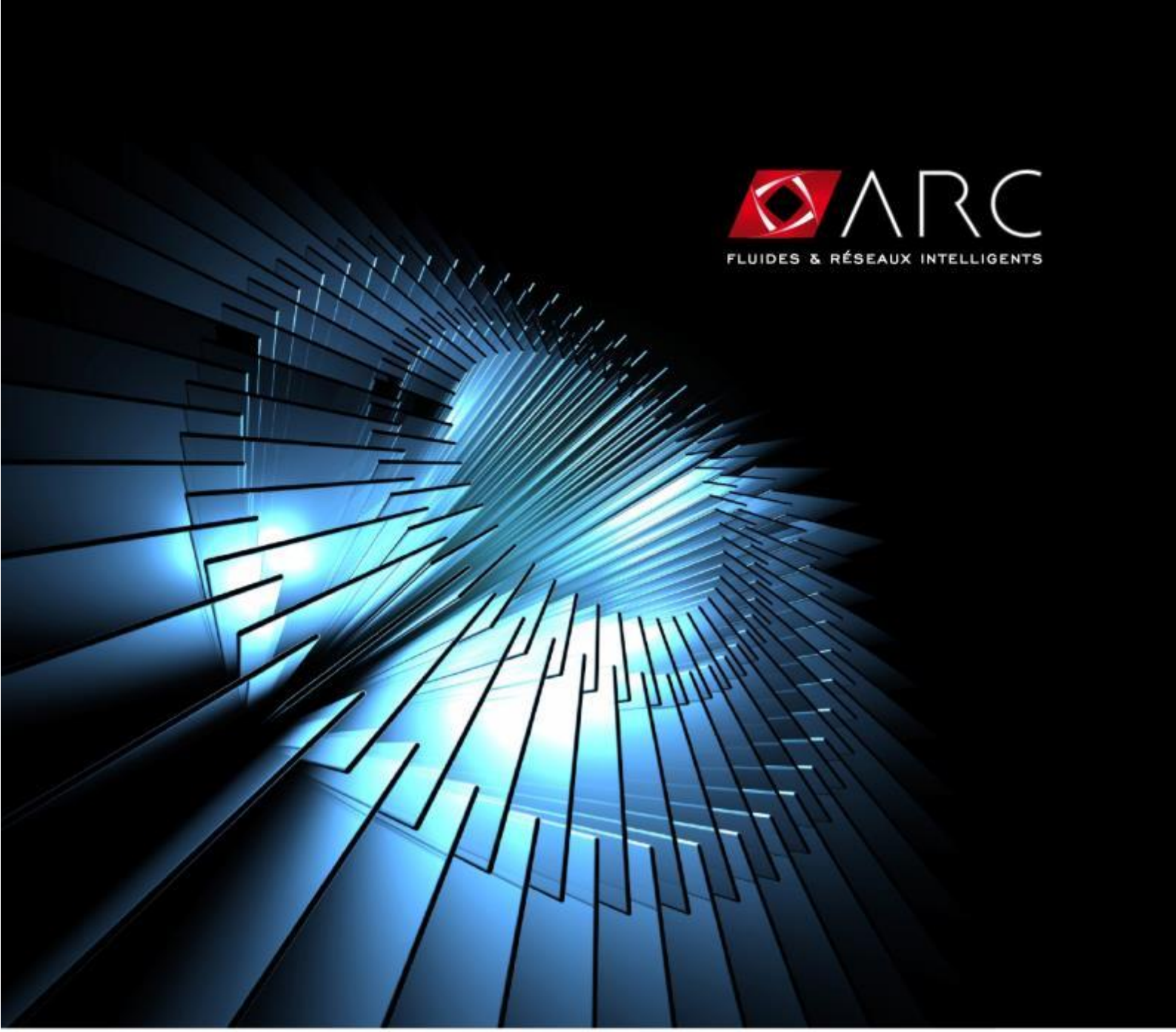
APPROUVE avec 23 voix pour, 4 voix contre et 1abstention, le schéma directeur de mise en sureté de l'Université de Nantes en vue de sa mise en œuvre opérationnelle, tel qu'annexé.

À Nantes, le 20 décembre 2019
Le Président de l'Université de Nantes

Olivier LABOUX

Pour le Président et par délégation
La Première Vice-Présidente
Carine BERNAULT

Extrait transmis au Recteur Chancelier des Universités le : - 7 JAN. 2020
Affiché le : - 7 JAN. 2020



UNIVERSITÉ DE NANTES

UNIVERSITE DE NANTES

SCHEMA DIRECTEUR SÛRETE

CODE OF CONDUCT

AFFAIRE SUIVIE PAR :

SOCIETE : Architecture Réseaux et Communication

NOM : Yoann LEFRILEUX

FONCTION : Consultant Expert

TELEPHONE : +33 (0)7 77 75 66 52

COURRIEL : yoann.lefrileux@arcbe.com

ADRESSE : Siège social
Immeuble Le Cid 10 rue Giboin
83110 Sanary Sur Mer
T +33 (0)4 94 74 54 80
F +33 (0)4 94 74 35 37

SUIVI DU DOCUMENT

INDICE	DATE	AUTEUR	OBJET
A	28/11/2017	Yoann LEFRILEUX	Création
B	12/12/2017	Yoann LEFRILEUX	Modifications suite à la conf call du 11/12/17
C	04/10/2018	Yoann LEFRILEUX	Modifications suite aux zoning sûreté

Sommaire

1. INTRODUCTION - ENJEUX

Pour l'Université de Nantes, les infrastructures techniques de sûreté représentent un enjeu stratégique et se doivent de bénéficier de toutes les avancées technologiques actuelles.

Les objectifs principaux, au regard des besoins exprimés, seront :

- De très hautes performances,
- Une haute disponibilité,
- Le respect des normes actuelles et futures,
- Une grande fiabilité,
- La sécurisation des installations (redondance physique),
- La flexibilité par la faculté d'adaptation des infrastructures techniques,
- L'évolutivité,
- Une grande pérennité,
- L'ergonomie de l'interface homme machine,
- L'optimisation des coûts d'investissement et des coûts d'exploitation,
- La maîtrise de l'exploitation pour les exploitants,
- Des communications performantes et sécurisées.

Un Schéma Directeur Sûreté est nécessaire pour l'Université de Nantes pour assurer la cohérence technique et garantir les performances de ses infrastructures de sûreté.

Il est recommandé de respecter l'ensemble des règles et préconisations décrites dans ce document.

Ce nouveau schéma directeur sûreté s'appuie, en particulier, sur les derniers référentiels et normes en vigueur :

- Référentiel APSAD R81 – Détection d'intrusion – Règle d'installation – Edition de septembre 2015,
- Référentiel APSAD R82 – Vidéosurveillance – Règle d'installation – Edition de février 2016,
- Référentiel APSAD D83 – Contrôle d'accès – Document technique pour la conception et l'installation – Edition de novembre 2012,
- Norme NF EN 50 133-1 portant sur la classification des systèmes de contrôle des accès (identification et accès),
- Norme NF EN 50 131-1 à 6 : Systèmes d'alarme,
- Norme NF EN 50 130-4 : compatibilité électromagnétique – prescriptions relatives à l'immunité des composants des systèmes de détection d'incendie, d'intrusion et d'alarme sonore,
- Norme NF C 48-205 : systèmes d'alarme : règles générales,
- Norme NF C 48-211 : détection d'intrusion - centrales d'alarme : règles,
- Norme NF C 48-212 : détection d'intrusion - transmetteurs téléphoniques d'alarme : règles,
- Norme expérimentale C 48-410 : système d'alarme - paramétrage des centrales d'alarme et transmetteurs téléphoniques d'alarme,

- Norme UTE C 15-411U : installations électriques à basse tension – installations des systèmes d'alarme,
- Norme NF C 15-100 : installations électriques à basse tension.

Ce présent document a pour objectifs principaux suivants :

- Définir les préconisations concernant le contrôle d'accès,
- Définir les préconisations concernant la détection d'intrusion,
- Définir les préconisations concernant la vidéosurveillance,
- Préciser les principes de sûreté applicables à l'Université de Nantes,
- Enumérer les spécifications techniques des matériels de contrôle d'accès, de détection d'intrusion et de vidéosurveillance.

2. PRECONISATIONS CONCERNANT LE CONTRÔLE D'ACCES

Un système de contrôle d'accès a pour objectif de filtrer les flux de circulations, les individus et parfois les véhicules qui souhaitent pénétrer à l'intérieur d'un site, d'un bâtiment ou d'un local.

Il s'agit donc d'accepter ou de refuser les passages aux différentes entrées, après identification, voire authentification, des demandeurs et de contrôler leurs droits d'accès.

Le système de contrôle d'accès doit également, dans certains cas, assurer la traçabilité de ces passages.

Il convient de souligner que la mise en œuvre d'un système de contrôle d'accès sur un site ne peut être efficace que si elle est associée à une protection mécanique des enceintes constituée de dispositifs physiques retardant la pénétration (clôtures, murs, portes, verrous, serrures, volets, grilles, rideaux, barreaux, produits verriers, etc.).

Un élément essentiel du contrôle d'accès est l'adhésion de l'ensemble du personnel dans la préparation, la mise en place, l'utilisation et le suivi de celui-ci.

Les systèmes de contrôle d'accès peuvent nécessiter, selon leur importance, la présence d'opérateurs et de gestionnaires.

2.1 REGLES DE CONCEPTION

2.1.1 PRECONISATIONS GENERALES

Une installation de contrôle d'accès doit posséder la qualité essentielle de sûreté de fonctionnement.

Une telle installation est sûre lorsqu'elle remplit son rôle de façon durable, stable, dans les conditions définies par les constructeurs des matériels constitutifs de l'installation, tout en respectant les normes en vigueur.

Un défaut affectant un organe de l'installation ne doit pas avoir pour conséquence d'entraîner en cascade d'autres défauts (destruction ou défaillance) dans l'ensemble de l'installation.

Afin de réduire le risque d'erreurs de manipulation, il importe que l'utilisation soit simple. Le paramétrage et l'administration du système de contrôle d'accès doivent être réalisés par une personne formée et désignée par l'exploitant.

En cas de défaillance de communication entre les éléments de l'installation, un point d'accès (lecteur et verrou) doit rester fonctionnel et autonome (mode dégradé) pour les autorisations ou les refus d'accès.

Le fonctionnement d'une installation de contrôle d'accès ne doit pas risquer d'être perturbé par tout autre système, associé ou non.

Le projet d'installation doit également tenir compte d'une éventuelle extension du système.

2.1.2 PRECONISATIONS RELATIVES AU NIVEAU DE SÛRETE

Le niveau de sûreté définit la résistance du système de contrôle d'accès à une menace de franchissement par un individu (avec ou sans véhicule) sur un point d'accès contrôlé.

Menaces potentielles			Niveau de sûreté
Qui ?	**Quels moyens ?**	**Quelles connaissances ?**	
Franchissement « naturel » d'un point d'accès			
Pénétrations involontaires ou de curieux (sans préparation)	Pas de matériel ou matériel basique (marteau léger, téléphone portable, etc.)	Pas de connaissance	**I**
Franchissement par attaque mécanique et/ou logique « simple »			
Pénétrations préméditées de personnes faiblement équipées	Matériel et méthode obtenus dans le commerce ou sur internet	Connaissance basique du système acquise au travers de documents publicitaires ou technico - commerciaux émis par le fabricant ou les distributeurs	**II**
Franchissement par attaque mécanique et/ou logique « évoluée »			
Pénétrations préméditées de personnes initiées et équipées	Matériel ou maquette électronique spécifique facilement réalisable	Connaissances recueillies à partir de l'examen d'un dispositif	**III**
Franchissement par attaque mécanique et/ou logique « sophistiquée »			
Pénétrations préméditées de personnes initiées, fortement équipées et renseignées	Matériel comprenant des moyens de cryptanalyse et/ou maquette électronique spécifique conçus spécialement pour neutraliser la sûreté en place	Connaissances sur la conception et l'exploitation du système. Ceci implique d'avoir accès à des informations confidentielles du fabricant	**IV**

Pour l'Université de Nantes, il a été retenu le **niveau de sûreté II** pour son système de contrôle d'accès.

Ce niveau de sûreté se décline suivant 3 classes :

- Classe de reconnaissance,
- Classe du droit d'accès,
- Classe de résistance à la malveillance.

Pour respecter le niveau de sûreté retenu pour les sites de l'Université de Nantes, les préconisations ci-après devront être prises en compte.

2.1.2.1 CLASSE DE RECONNAISSANCE

La classe de reconnaissance des utilisateurs est caractérisée par la précision de l'identification ou de l'authentification nécessaire pour pénétrer dans le secteur contrôlé.

Pour respecter le niveau de sûreté II souhaité par l'Université de Nantes, chaque utilisateur autorisé devra :

- Soit être en possession d'un objet physique permettant l'accès aux zones contrôlées (par exemple un badge),
- Soit avoir la connaissance d'un secret individuel (non partagé) permettant l'accès aux zones contrôlées (par exemple un code 6 chiffres).

L'utilisation de « passes » (badges ou clés) nécessite d'avoir un processus formalisé et précis de gestion permettant l'identification précise des personnes utilisant le passe et ses conditions d'usage.

2.1.2.2 CLASSE DU DROIT D'ACCES

4 classes d'accès sont retenues dans le référentiel APSAD D83 :

- Classe A : pas de grille horaire, ni de traçabilité,
- Classe B : gestion des droits « standard »,
- Classe C : gestion des droits « évolués »,
- Classe D : gestion des droits « évolués », avec une gestion des passages permettant l'unicité de passage.

Pour respecter le niveau de sûreté II souhaité par l'Université de Nantes, la classe du droit d'accès devra être de **type B** et influera au minimum les critères suivants :

- les plages horaires d'accès,
- la durée de l'autorisation d'accès,
- les règles d'accès et de circulation dans les secteurs contrôlés, par exemple les possibilités de passage d'un secteur contrôlé à un autre en fonction des niveaux de sûreté respectifs,
- le cas échéant, l'enregistrement automatique ou manuel des passages,
- les conditions d'accompagnement (par exemple : visiteur),
- la prise en compte des éventuelles obligations d'évacuation du bâtiment (ouverture de points d'accès en cas d'incendie, d'alerte à la bombe, etc.).

2.1.2.3 CLASSE DE RESISTANCE AUX ACTES DE MALVEILLANCE

Les composants et les liaisons équipant les points d'accès d'un système de contrôle d'accès sont classés selon des critères de résistance aux actes de malveillance (fraude).

La résistance aux actes de malveillance est définie pour chaque point d'accès du secteur contrôlé.

Les composants du contrôle d'accès hors lecteurs doivent être placés dans un lieu assurant leur sécurité vis-à-vis de la malveillance (exemple : dans un secteur contrôlé).

Il est nécessaire de tenir compte dans l'étude de la complicité volontaire (exemple : prêt d'un badge) ou involontaire (exemple : blocage d'une porte lors d'une pause « avec oubli de badge »).

Le but recherché d'un système de contrôle d'accès n'est pas la lutte contre la malveillance ou l'intrusion, mais bien le contrôle des flux. Néanmoins, le niveau de résistance aux actes de malveillance doit être cohérent avec le niveau de risque, aux points de passage et sur les plages horaires concernées. Si ce n'est pas le système de contrôle d'accès qui assure la protection contre la malveillance, cela peut être un élément associé.

La résistance aux actes de malveillance d'un système de contrôle d'accès se définit à la fois par la résistance de ce dernier :

- aux attaques logiques (mécaniques et/ou électroniques),
- aux attaques physiques (destructives ou non destructives) portées directement au système de contrôle d'accès.

Pour respecter le niveau de sûreté Il souhaité par l'Université de Nantes, la résistance aux **attaques logiques**, qui passe par une connaissance précise du matériel réalisant le contrôle d'accès, sera au minimum de **type L1** :

- Moyens :

  Matériel et méthode facilement obtenus sur internet ou dans le commerce (les solutions techniques répondant à ces critères sont référencés dans le document de l'Anssi *« Guide sécurité des technologies sans contact pour le contrôle des accès physiques »,*

- Connaissances :

  Connaissance basique du système acquise au travers de documents publics.

Le risque de substitution par création d'un badge valide est pris en compte en tant qu'attaque logique.

Pour respecter le niveau de sûreté Il souhaité par l'Université de Nantes, la résistance aux **attaques physiques destructives**, dans le cas où aucun système associé ne permet la protection aux attaques destructives, respectera au minimum les exigences ci-dessous :

- Temps et moyens :

  5 minutes de résistance minimum avec outillage,

(les préconisations ainsi que l'outillage sont ceux définis par les Règles techniques CNPP T61 - Serrures de bâtiments - Spécifications et méthodes d'essai et le règlement particulier H61 - Règlement particulier de la marque A2P - Serrures de bâtiments),

- Résistance minimum à l'effort sur le pêne d'une serrure mécanique :

  Poussée axiale : 300 daN

  Poussée perpendiculaire : 700 daN.

Dans le cas où un système, associé au système de contrôle d'accès et répondant aux exigences ci-dessus, est prévu, alors les exigences portant sur le système de contrôle d'accès peuvent être réduites :

- Temps et moyens :

  3 minutes de résistance minimum avec outillage,

- Résistance minimum à l'effort sur le pêne d'une serrure mécanique :

  Poussée axiale : 150 daN

  Poussée perpendiculaire : 350 daN.

Enfin, pour respecter le niveau de sûreté II souhaité par l'Université de Nantes, la résistance aux **attaques physiques non destructives** respectera au minimum les exigences ci-dessous :

- Temps et moyens :

  5 minutes de résistance minimum avec outillage,

  (les préconisations ainsi que l'outillage sont ceux définis par les Règles techniques CNPP T61 - Serrures de bâtiments - Spécifications et méthodes d'essai et le règlement particulier H61 - Règlement particulier de la marque A2P - Serrures de bâtiments),

- Nombre minimum de combinaisons pour les serrures mécaniques :

  500.

2.1.3 PRECONISATIONS POUR LA GESTION DES DROITS D'ACCES ET L'ORGANISATION

La gestion d'un système de contrôle d'accès est réalisée selon deux objectifs :

- la gestion des droits d'accès,
- l'organisation et la gestion des évènements.

2.1.3.1 GESTION DES DROITS D'ACCES

Le principe de gestion des droits d'accès doit être dûment formalisé.

L'Université de Nantes doit désigner un ou des responsable(s) chargé(s) de la délivrance des droits d'accès.

Les droits d'accès sont attribués sur la base d'informations recueillies auprès du responsable de chaque secteur contrôlé, ainsi qu'auprès du service du personnel.

Les utilisateurs doivent être formellement informés des conditions d'utilisation du système de contrôle d'accès.

Une sensibilisation doit être réalisée :

- pour les personnes présentes de façon régulière sur le site (personnel et étudiants),
- systématiquement lors de l'accueil des nouveaux arrivants.

Cette sensibilisation intègre notamment les points suivants :

- les dispositions applicables en matière de gestion des accès,
- les rôles et responsabilités des personnes, par exemple l'importance de signaler la perte ou la découverte d'un badge,
- les conséquences d'un non-respect des dispositions applicables (tant pour l'Université qu'au regard de la responsabilité personnelle).

Pour la gestion des badges, l'ensemble des informations concernant les badges en circulation (type, informations présentées, validité, etc.) doivent être recensées.

En cas d'utilisation de badges multi-applications (ce qui est le cas à l'Université de Nantes avec l'utilisation souhaitées des cartes professionnelles CMS, il convient que les droits d'accès relatifs au contrôle d'accès soient indépendants des autres applications (solution de chiffrement robuste).

La gestion des badges devra progressivement migrer vers une solution qui s'appuiera obligatoirement sur ces badges multi-applications (cartes professionnelles CMS). De plus, l'administration des données et des droits d'accès devra reposer sur la relation avec l'annuaire LDAP de l'Université de Nantes.

2.1.3.2 ORGANISATION ET GESTION DES EVENEMENTS

Toute perte d'un badge, d'une clé, etc. doit être signalée. Les actions rendues nécessaires par la perte d'un moyen doivent être préalablement déterminées.

Ces moyens sont délivrés aux utilisateurs en contrepartie de leur adhésion au système.

Le responsable du contrôle d'accès et le personnel d'exploitation doivent avoir conscience de leur mission dans le cadre de la surveillance du site.

Le personnel en charge de l'accueil physique des personnes peut également avoir des missions dans l'organisation du contrôle d'accès, notamment en mode dégradé. Ce personnel doit être informé de sa contribution à cette organisation. Des rappels de consignes réguliers (et au minimum trimestriels) doivent être faits.

L'Université identifie et fait appliquer les consignes nécessaires à l'organisation du contrôle d'accès.

Chaque consigne doit définir l'acteur concerné, l'enchaînement des actions à réaliser, les autres consignes ou documents à utiliser et, si nécessaire, les modalités d'enregistrement des actions engagées.

Le responsable du contrôle d'accès passe en revue quotidiennement (pour les jours ouvrés) le journal des événements associé au système de contrôle d'accès.

L'entreprise doit s'assurer de la conservation dans le temps des journaux d'évènements. A ce titre, la sauvegarde des informations doit être démontrable.

Attention : l'accès au paramétrage des bases de données doit être limité aux seuls responsables de l'exploitation et protégé par un mot de passe. Ce mot de passe doit être changé régulièrement.

2.1.4 PRECONISATIONS POUR LA FIABILITE

2.1.4.1 ALIMENTATION ELECTRIQUE

Afin de respecter le niveau de sûreté II souhaité par l'Université de Nantes, il est conseillé que l'installation de contrôle d'accès soit alimentée par une alimentation principale externe fournie par le réseau basse tension (230 V) et sauvegardée par une alimentation secondaire (batteries d'accumulateurs).

Néanmoins, il peut être, dans certains cas, toléré que l'installation de contrôle d'accès soit alimentée par une alimentation principale interne, dite autonome (piles).

Une ligne d'alimentation principale doit être dédiée exclusivement à l'installation de contrôle d'accès ; le raccordement à une prise n'est pas admis.

Il est primordial que la résistance à la fraude de l'installation soit assurée en permanence. Une coupure seule de l'alimentation principale ne doit pas entraîner la libération d'un point d'accès.

Pour un système à alimentation autonome, un signal sonore ou lumineux doit informer les utilisateurs du niveau bas de l'alimentation, au moins lors d'une demande d'accès.

Pour un système à alimentation externe, l'alimentation secondaire doit assurer, en cas d'absence de l'alimentation principale, le fonctionnement de l'installation de contrôle d'accès pendant une durée minimale de **60 minutes**.

Une signalisation de l'absence d'alimentation principale doit être donnée aux utilisateurs. Cette signalisation est locale au niveau des lecteurs et, éventuellement, centralisée pour des administrateurs d'un système à multiples points d'accès.

L'alimentation secondaire doit assurer au minimum le traitement des données et le déverrouillage / verrouillage des points d'accès.

A l'issue de cette durée d'autonomie (60 minutes), en absence totale d'alimentation, la conservation des données mémorisées doit être assurée par le système pendant au moins 120 h. De plus, cela doit entraîner le verrouillage en entrée du ou des point(s) d'accès concerné(s). En contrepartie le système doit disposer d'un mécanisme

manuel d'urgence pour le déverrouillage en sortie (évacuation) et en entrée (maintenance).

2.1.4.2 RESEAUX ET INTERCONNEXIONS

Les réseaux utilisés et leurs interconnexions devront garantir un niveau minimum de disponibilité du support et de bande passante disponible cohérent avec l'usage du système de contrôle d'accès.

Ils devront également garantir la confidentialité et l'intégrité des données transportées. Ceci implique en particulier l'usage de routeurs de type VPN en cas d'utilisation d'accès Internet (sites distants).

2.1.4.3 SECURITE DES POSTES D'EXPLOITATION

Les postes d'exploitation du système de contrôle d'accès doivent être protégés contre les attaques physiques, logiques et informatiques.

Les organes de gestion technique du contrôle d'accès doivent être placés dans des locaux techniques à accès restreints dont le niveau de protection doit être au minimum égal à celui du point d'accès contrôlé.

Afin de respecter le niveau de sûreté Il souhaité par l'Université de Nantes, le poste d'exploitation avec son interface homme/machine doit **être dans un secteur contrôlé**.

2.1.4.4 CONTINUITE DE SERVICE

En cas de défaillance du système de contrôle d'accès, celui-ci doit pouvoir fonctionner en mode dégradé : il doit être prévu la libération de certains points d'accès pour les problématiques de sécurisation des points névralgiques et de besoins d'évacuations.

En cas de tentative d'attaque sur le système, en particulier en cas d'attaque logique, il doit être prévu le verrouillage et/ou la libération de certains points d'accès.

2.2 REGLES D'INSTALLATION

2.2.1 REGLES GENERALES

Le prestataire de service doit définir dans son offre les moyens pour apporter une réponse adéquate aux besoins exprimés par l'étude conceptuelle en termes de flux, contraintes et niveaux de sûreté.

Les matériels doivent être installés et solidement fixés sur leurs supports par les moyens prévus dans les notices constructeurs. Ils doivent comporter des indications suffisantes pour être identifiés sans risque d'erreur (nom du fabricant, modèle, type, etc.).

Le raccordement doit être effectué selon les règles de l'art et les dispositions de la norme NF C 15-100. Les textes réglementaires en vigueur ainsi que les préconisations des guides UTE C 15-520 et UTE C 15-900 (notamment en matière d'habilitation électrique du personnel) doivent être respectés.

Les matériels doivent comporter le marquage CE, attestant l'engagement du constructeur du respect des directives européennes en vigueur (notamment : CEM et Basse tension).

Le prestataire de service doit choisir l'emplacement des matériels en tenant compte notamment de leur résistance à la fraude face aux tentatives de neutralisation et de leur meilleure commodité d'emploi.

Les phénomènes physiques environnementaux susceptibles d'altérer le fonctionnement des matériels (température, humidité, vibrations, foudre, perturbations électromagnétiques, etc.) doivent être pris en compte.

Tous les matériels constitutifs de l'installation de contrôle d'accès doivent être auto-surveillés à l'ouverture, si leur ouverture permet d'accéder aux borniers de raccordements ou aux alimentations. Ceci concerne aussi les boîtes de raccordement et de dérivation.

Les interventions sur l'installation, autres que celles normalement pratiquées par les différents utilisateurs et pouvant entraîner une modification de celle-ci doivent provoquer le passage à l'état « alarme ».

Chaque point d'accès doit disposer d'un dispositif de fermeture automatique de l'accès après passage de l'utilisateur.

2.2.2 LECTEURS DE BADGES

Un lecteur permet de réaliser la lecture des données introduites dans le système par la composition d'un code sur un clavier et/ou la présentation d'un support identifiant (code, carte, clé, etc.).

Le dispositif est installé à proximité du point d'accès à contrôler. Dans le cas où une menace de vandalisme est identifiée, il est conseillé d'utiliser un lecteur anti-vandale ou de placer les lecteurs sans contact derrière une paroi de protection ou à l'intérieur du secteur contrôlé. Les préconisations des notices des constructeurs doivent être respectées.

Les vis de fixation des lecteurs ne doivent être directement accessibles qu'à l'intérieur du secteur contrôlé.

Afin de respecter le niveau de sûreté Il souhaité par l'Université de Nantes, il est conseillé d'utiliser des lecteurs dotés d'une **auto-surveillance** à l'arrachement s'ils sont placés à l'extérieur du secteur contrôlé.

Par contre, ce niveau de sûreté n'impose pas l'effacement des clés sur arrachement du lecteur.

Le lecteur doit être facilement accessible par l'utilisateur pour permettre les manipulations d'identification.

Aucun code ou identifiant ne doit être laissé à proximité du lecteur.

2.2.3 TRAITEMENT ET COMMANDE

L'unité de traitement et de commande centralisée assure la gestion de toutes les demandes d'accès, les compare à ses bases de données et délivre les commandes de libération des verrouillages.

L'unité de traitement et de commande centralisée doit être mise en place dans le secteur contrôlé du niveau de sûreté le plus élevé.

Des coffrets de traitement et de commande peuvent être déportés près des points d'accès. Ils doivent être mis en place du côté du niveau de sûreté le plus élevé. Ils doivent être fixés sur leurs supports et auto-surveillés à l'ouverture et à l'arrachement.

Les coffrets contenant des éléments vitaux du système (exemple : alimentations) doivent être implantés dans le secteur contrôlé du côté du niveau de sûreté le plus élevé.

Pour assurer le fonctionnement du système et sa bonne utilisation, il est nécessaire de mettre en œuvre des moyens de signalisations des différents états des dispositifs.

Le système doit signaler de façon lumineuse ou sonore à l'utilisateur l'accord et le refus de passage au niveau du lecteur.

Afin de respecter le niveau de sûreté Il souhaité par l'Université de Nantes, il est conseillé de mettre en œuvre des capteurs permettant de signaler à l'unité de traitement :

- la position des points d'accès (ouvert ou fermé),
- la position des pênes des dispositifs de verrouillage (entrés ou sortis) pour les secteurs contrôlés,
- l'ouverture au-delà d'une temporisation des points d'accès (« ouverture trop longue »).

Dans tous les cas, l'unité de traitement doit signaler à l'opérateur les évènements suivants :

- détection d'activation de l'auto-surveillance,

- point d'accès ouvert sans autorisation (« accès forcé »),
- point d'accès ouvert par déverrouillage forcé provenant d'un système extérieur (système incendie, organe de commande mécanique),
- point d'accès ouvert au-delà de la période autorisée (dans le cas de l'utilisation d'une grille horaire ou dans le cas d'une ouverture prolongée au-delà d'une période temporisée),
- défaillance ou niveau bas d'une source d'alimentation.

Le niveau de sûreté souhaitée par l'Université de Nantes n'impose pas au système de contrôle d'accès d'enregistrer de manière horodatée tous les événements suivants :

- transactions avec identification de l'utilisateur et localisation de l'accès,
- accès refusés aux utilisateurs, avec localisation de l'accès,
- détection d'activation de l'auto-surveillance, avec localisation de l'accès,
- point d'accès ouvert sans autorisation,
- point d'accès ouvert par déverrouillage forcé provenant d'un système extérieur (système incendie, organe de commande mécanique)
- point d'accès ouvert au-delà de la période autorisée,
- entrée et sortie du mode de paramétrage,
- défaillance ou niveau bas d'une source d'alimentation.

2.2.4 LIAISONS

D'une manière générale, les câbles circulent à l'intérieur des locaux contrôlés. En cas d'impossibilité, les câbles circulant à l'extérieur doivent être protégés mécaniquement (tubes métalliques, fourreaux, etc.) et auto-surveillés pour détecter les coupures accidentelles ou les tentatives de neutralisation.

En cas d'environnement présentant un risque de détérioration des câbles (atelier, zone d'évolution d'engins de manutention, etc.), il est recommandé de prévoir une protection mécanique des chemins de câbles.

Le choix des câbles doit être défini en fonction des caractéristiques des signaux électriques à transmettre, des courants d'alimentation à fournir et en accord avec les notices d'installation des matériels.

Le raccordement des câbles dans les matériels doit être réalisé sur les borniers ou dans des boîtes de raccordement.

Un système de contrôle d'accès de niveau de sûreté II n'impose pas la surveillance à l'ouverture de ces boîtiers.

Les câbles doivent être correctement repérés, d'un seul tenant, sans épissures ou dominos entre les matériels ou les boîtes de raccordement et de dérivation.

Les câbles ne doivent être ni collés ni agrafés sur leurs supports.

Il faut tenir compte des exigences de sûreté du bâtiment ou du site et définir, pour chaque point d'accès, s'il doit être laissé ouvert ou fermé en cas de défaillance d'une liaison.

La coupure totale d'une liaison entre des matériels de l'installation ou la disparition d'une alimentation doit provoquer une signalisation destinée à l'opérateur.

Le court-circuit total d'une liaison entre les matériels de l'installation doit provoquer une signalisation destinée à l'opérateur. Cette exigence ne concerne pas :

- les câbles de l'alimentation principale fournie par le réseau 230 V de l'installation,
- les câbles téléphoniques.

Attention : les dispositifs de sécurité supplémentaires d'une installation (détecteurs d'intrusion, etc.) ne doivent pas affecter le bon fonctionnement de l'installation. Ces éléments doivent être placés sur des liaisons séparées.

2.2.5 CAS DU DISPOSITIF INTEGRE AUTONOME

Il existe des systèmes de contrôle d'accès implantés directement sur le point d'accès à contrôler, en remplacement des mécanismes standard d'ouverture des portes.

Toutes les fonctions fondamentales d'un système de contrôle d'accès (lecture, traitement et verrouillage) sont alors intégrées dans un seul coffret, y compris l'alimentation interne.

Les vis de fixation du dispositif doivent être placées du côté du secteur contrôlé de niveau de sûreté le plus élevé.

Le coffret du dispositif doit être doté d'une auto-surveillance à l'ouverture et à l'arrachement. Une signalisation sonore interne doit intervenir en cas de manipulation non autorisée.

L'unité de lecture doit être facilement accessible par l'utilisateur pour permettre les manipulations d'identification.

Le dispositif doit être facilement accessible pour le responsable afin de permettre les changements de paramétrage des bases de données.

Le dispositif doit disposer de son alimentation interne autonome. Il doit signaler lorsque cette alimentation est à un état faible.

3. PRECONISATIONS CONCERNANT LA DETECTION D'INTRUSION

Une installation de détection d'intrusion a pour objectif la surveillance des éléments de valeur (mobiliers, fonds et valeurs, ainsi que les produits et documents). Elle est destinée à détecter et à signaler l'approche, la pénétration et/ou le déplacement d'un intrus dans le site, les secteurs sensibles ou les zones de localisation de valeurs et, selon les besoins, permet de déclencher une intervention.

Pour ce faire, elle doit transmettre les alarmes et optionnellement, elle peut déclencher des moyens avertisseurs et/ou dissuasifs (éclairage, générateur de fumée, etc.) dans les limites autorisées par la réglementation.

La mise en sécurité d'un site contre l'intrusion doit d'abord être assurée par une protection mécanique efficace constituée de dispositifs résistants à l'effraction, tels que verrous, serrures, portes, volets, barreaux.

La surveillance par un système électronique de détection d'intrusion vient en complément de la protection mécanique. Plus la durée de l'acte de malveillance est courte, plus la détection doit être précoce ; la résistance des éléments de protection mécanique accroît cette durée.

En cas d'intrusion, des moyens et mesures doivent être prévus pour limiter la durée du passage à l'acte (levée de doute : télésurveillance, télévidéosurveillance, télésécurité, sirène, projecteur ou flash, etc.) et/ou augmenter l'effort à la pénétration et à la circulation (générateur de fumée, etc.).

3.1 REGLES DE CONCEPTION

3.1.1 PRECONISATIONS GENERALES

Une installation de détection d'intrusion doit posséder la qualité essentielle de sûreté de fonctionnement. Une telle installation est sûre lorsqu'elle remplit son rôle de façon durable, stable, dans les conditions et circonstances définies par les constructeurs des matériels constitutifs de l'installation, tout en respectant les normes en vigueur.

L'installation doit être conçue et réalisée de manière à éviter les alarmes injustifiées.

Un défaut affectant un organe de l'installation de détection d'intrusion ne doit pas avoir pour conséquence d'entraîner en cascade d'autres défauts (destruction ou défaillance) dans l'ensemble de l'installation.

Une installation de détection d'intrusion ne doit pas pouvoir être neutralisée, ni totalement ni partiellement, avant que le système n'ait signalé la tentative de neutralisation.

Afin de réduire le risque d'erreurs de manipulation, il importe que l'utilisation du système de détection d'intrusion soit simple et que la commande de l'installation puisse elle-même être effectuée par une manœuvre simple.

Le projet d'installation doit tenir compte d'une éventuelle extension du système de détection. Le choix des éléments en dépend et, principalement, la capacité de la centrale d'alarme, afin d'éviter ultérieurement son remplacement.

L'Université de Nantes a défini deux types de secteur sensible, à savoir :

- Les zones à accès limité dites « rouge » :
  - Salles informatiques (salle serveurs et baie de brassage),
  - Stockage de matériels Informatique ou Vidéo à haute valeur marchande,
  - Archives,
  - Agence comptable et coffre-fort,
  - Stockage de produit chimique, de matières dangereuses,
  - Bureau de la Présidence, bureaux sensibles, autres zones sensibles.
- Les zones à accès restreint dites « orange » :
  - Laboratoires de recherche scientifique et informatique,
  - Locaux administratifs,
  - Stockage de produits intermédiaires à valeur marchande moyenne,
  - Locaux techniques (électriques, traitement de l'air, etc.),
  - Bâtiment à usage non étudiant.
- Les zones accessibles aux étudiants, visiteurs et personnels pendant les heures ouvrées dites « verte » :
  - Tous les autres locaux non listés ci-dessus.

Une catégorie de zone (A, B ou C) est alors définie en fonction du secteur sensible à surveiller et de sa surface :

	< 800 m²	≥ 800 m² et < 3 000 m²	≥ 3 000 m²
Zones « orange »	**A**	**B**	**C**
Zones « rouge »	**B**	**C**	**C**
Zones « verte »	**C**	**C**	**C**

3.1.2 PRECONISATIONS DE SURVEILLANCE

La détection est une combinaison, pour chaque secteur sensible, de deux des trois types de surveillances listés ci-après :

- Surveillance de l'approche (SA) :
  - Franchissement du pourtour du site (SA1),
  - Mouvement entre le pourtour du site et le bâtiment (SA2),

- Surveillance des pénétrations (SP) :
  - Au niveau des issues principales uniquement (SP1),
  - Au niveau des issues principales et secondaires (SP2),
  - Au niveau des issues principales, secondaires et des ouvrants (SP3),
  - Au niveau des issues principales, secondaires, des ouvrants et des PPFR *(Partie de Parois de Faible Résistance)* (SP4).
- Surveillance des mouvements (SM) :
  - Au niveau des passages obligés uniquement (SM1),
  - Au niveau des zones de valeurs uniquement (SM2),
  - Au niveau des passages obligés et des zones de valeurs (SM3),
  - Au niveau des passages obligés, des zones de valeurs et à l'approche des valeurs (SM4).

Pour répondre aux besoins de l'Université de Nantes, la détection sera en fonction de la catégorie de zone à surveiller :

		Catégories		
		A	B	C
Surveillance	Détection	**SP1 + SM1** *par le même équipement (détecteur volumétrique)*	**SP3** *(par détecteur d'ouverture)* + **SM1** *(par détecteur volumétrique)*	**SP3** *(par détecteur d'ouverture)* + **SM1** *(par détecteur volumétrique)*

3.1.3 PRECONISATIONS DE TRAITEMENT DES INFORMATIONS

Le traitement doit être assuré par une centrale d'alarme.

Le besoin de paramétrage (avec les procédures d'accès, les responsabilités associées et le journal des événements) doit être précisé.

La mise en/hors service du système de détection d'intrusion doit se faire suite à une action sur un organe de commande placé à l'extérieur des locaux à surveiller entraînant la mise en/hors service immédiate de la totalité de l'installation.

3.1.3.1 ALIMENTATION ELECTRIQUE

L'alimentation électrique de l'installation de détection d'intrusion doit être assurée en permanence.

Les éléments de l'installation de détection d'intrusion doivent être alimentés :

- soit par une alimentation principale fournie généralement par le réseau 230 V et sauvegardée par une alimentation secondaire (batteries d'accumulateurs),
- soit par une alimentation autonome fournie par une ou plusieurs piles.

Les besoins en alimentation doivent être évalués préalablement à toute installation. Le calcul de ces besoins doit être effectué.

Alimentation principale et alimentation secondaire :

La ligne d'alimentation doit être dédiée exclusivement à l'installation de détection d'intrusion.

Si le site comporte un groupe électrogène, l'installation de détection d'intrusion peut y être raccordée. Dans ce cas, le groupe électrogène doit assurer une reprise effective en énergie, de façon automatique, après la coupure de l'alimentation principale. Il ne se substitue pas à l'alimentation secondaire de l'installation.

L'alimentation secondaire doit assurer, en cas d'absence de l'alimentation principale, le fonctionnement du système.

Alimentation autonome :

Une alimentation autonome (piles) doit être associée à un dispositif qui permet de signaler à l'utilisateur le niveau faible des tensions des piles, au plus tard à la mise en service du système.

3.1.3.2 AUTONOMIE DE L'INSTALLATION DE DETECTION D'INTRUSION

Le constructeur de la centrale d'alarme définit, dans sa notice d'installation, l'intensité maximale de consommation à ne pas dépasser pour respecter l'autonomie requise, en fonction du type de la batterie et du chargeur associé.

Les valeurs mesurées sur l'installation de détection d'intrusion doivent être inférieures ou égales à ces données.

L'alimentation secondaire doit assurer, en cas d'absence de l'alimentation principale, le fonctionnement de l'installation de détection d'intrusion pendant une durée minimale exprimée en heures et, à l'issue de cette période, le fonctionnement des dispositifs de signalisation d'alarme.

Cette durée minimale est exprimée en fonction de la catégorie de zone à surveiller :

		Catégories		
		A	B	C
Traitement	Alimentation secteur + batterie	**Autonomie 12h**	**Autonomie 36h**	**Autonomie 36h**
	Alimentation piles	**Autonomie 1 an**	**Autonomie 2 ans**	**Interdit**

3.1.3.3 TRAÇABILITE DES EVENEMENTS

Le constructeur de la centrale d'alarme peut proposer une fonction de mémorisation des événements, soit sous forme d'un journal des événements ou sous forme de contrôleur enregistreur.

Cette possibilité permet à l'utilisateur et à l'installateur d'assurer une traçabilité des événements, notamment dans le cas de déclenchement d'alarme ou à des fins de maintenance du système de détection d'intrusion.

L'accès à ce journal des événements peut être directement disponible à l'utilisateur ou bien nécessiter l'intervention de l'installateur.

3.1.4 PRECONISATIONS D'ALARME ET DE DISSUASION

L'installation de détection d'intrusion peut comporter des dispositifs d'alarme afin de dissuader l'intrus de poursuivre sa tentative et informer des personnes extérieures de son déclenchement :

- une sirène extérieure dont l'objectif est d'alerter le voisinage,
- une alarme lumineuse intérieure (éclairage de certaines pièces, projecteur ou flash) dont l'objectif est de dissuader l'intrus,
- un ou plusieurs générateurs de fumée dont l'objectif est d'entraver les déplacements de l'intrus,
- une alarme lumineuse extérieure (projecteur ou flash) dont l'objectif est d'indiquer la zone faisant l'objet du déclenchement. Dans le cas de site étendu, il est conseillé d'éclairer le voisinage immédiat du bâtiment,
- une transmission d'alarme (données, audio, vidéo) dont l'objectif est d'informer des personnes situées en dehors du site via un réseau de communication (station de télésurveillance) ou à l'intérieur du site à un poste central de sécurité (avec surveillance humaine).

L'installation de détection d'intrusion comporte au minimum un dispositif d'alarme sonore intérieur dont l'objectif est de dissuader l'intrus.

À l'état hors service, le déclenchement des dispositifs d'alarme audible de la voie publique par la fonction autosurveillance n'est pas obligatoire.

En fonction de la catégorie de zone à surveiller, le système de détection d'intrusion doit être complété par d'autres dispositifs d'alarme et de dissuasion :

<table>
<tr><th colspan="2" rowspan="2"></th><th colspan="3">Catégories</th></tr>
<tr><th>A</th><th>B</th><th>C</th></tr>
<tr><td rowspan="10">Alarme et dissuasion</td><td>Sirène intérieur</td><td>Oui</td><td>Oui</td><td>Oui</td></tr>
<tr><td>Sirène extérieure</td><td rowspan="5">Pas d'exigence</td><td rowspan="3">Pas d'exigence</td><td rowspan="3">1 au choix</td></tr>
<tr><td>Alarme lumineuse</td></tr>
<tr><td>Générateur de fumée</td></tr>
<tr><td>Transmission des alarmes au télésurveilleur</td><td rowspan="2">1 au choix</td><td rowspan="2">1 au choix</td></tr>
<tr><td>Transmission des alarmes au PC Sécurité</td></tr>
<tr><td>Type de station (si télésurveillance)</td><td>P2 ou P3</td><td>P2 ou P3</td><td>P3</td></tr>
<tr><td>Niveau de transmission [2] (si télésurveillance)</td><td>Niveau IV</td><td>Niveau IV</td><td>Niveau III</td></tr>
<tr><td>Téléalarme</td><td colspan="3">Complémentaire</td></tr>
</table>

[2] : Selon les exigences des niveaux de transmission du référentiel APSAD R31.

3.1.5 PRECONISATIONS SUR LES MATERIELS

3.1.5.1 CAS GENERAL

Afin de satisfaire aux principes généraux de sûreté de fonctionnement des matériels, une installation de détection intrusion est constituée de matériels certifiés NF&A2P :

Désignations	Liaison filaire	Liaison radio	Couvert par la certification	Non couvert par la certification
Centrale d'alarme	✓	✓	✓	
Coffret de commande	✓	✓	✓	
Coffret d'alimentation	✓		✓	
Contrôleur enregistreur intégré	✓	✓	✓	
Transmetteur d'alarme support PSTN (RTC)	✓	✓	✓	
Transmetteur d'alarme support GSM/GPRS	✓	✓	✓	
Transmetteur d'alarme support RNIS	✓	✓	✓	
Transmetteur d'alarme support TCP/IP	✓	✓	✓	
Détecteur d'ouverture à contact magnétique	✓	✓	✓	
Détecteur de chocs à masselotte	✓		✓	
Détecteur de chocs à bille (inertie)	✓	✓	✓	
Détecteur de chocs piézoélectrique	✓	✓	✓	
Détecteur bris de vitre piézoélectrique	✓	✓		✓
Détecteur bris de vitre acoustique	✓	✓		✓
Détecteur sismique	✓		✓	
Détecteur de mouvement à infrarouge passif	✓	✓	✓	
Détecteur de mouvement combiné ou multi-modes ou bivolumétrique	✓	✓	✓	
Détecteur de mouvement à hyperfréquence	✓		✓	
Détecteur de mouvement à ultrasons	✓		✓	
Barrière infrarouge	✓			✓
Barrière hyperfréquence	✓			✓
Câble détecteur à tension mécanique	✓			✓
Câble détecteur à champ capacitif	✓			✓
Câble détecteur à champ électrostatique	✓			✓
Câble détecteur microphonique	✓			✓
Câble détecteur sismique	✓			✓
Câble détecteur enterré rayonnant	✓			✓
Câble détecteur enterré à pression	✓			✓
Sirène intérieure	✓	✓	✓	
Sirène intérieure avec flash	✓	✓	✓	
Sirène extérieure	✓	✓	✓	
Sirène extérieure avec flash	✓	✓	✓	
Générateur de fumée	✓		✓	
Boîte de dérivation	✓		✓	

De plus, une installation de détection intrusion est constituée de matériels dont le nombre de boucliers respecte le tableau ci-après :

		Catégories		
		A	B	C
Matériel	Matériel NF&A2P	**1 bouclier**	**2 boucliers**	**2 boucliers**

Le recours à des matériels ne répondant pas aux exigences ci-dessus à l'initiative du prescripteur/donneur d'ordre est possible. Dans ce cas, les matériels doivent répondre aux exigences minimales suivantes :

Exigences minimales	Preuves documentaires associées
Les produits doivent être conformes à la norme correspondante : - NF C 48- XXX ou - EN 50131-X	- Certificat en vigueur.
Les documents suivants sont exigés pour les produits. Ces documents doivent être rédigés en français.	- Une notice d'utilisation. - Une notice d'installation. - Une notice de mise en service. - Une notice d'entretien, d'exploitation et de maintenance préventive.
Les produits doivent être certifiés par un organisme certificateur tierce partie accrédité selon la norme ISO/CEI 17065 par un organisme d'accréditation signataire du Multilateral agreement (MLA) – Certification dans le cadre de l'European cooperation for Accreditation (EA).	- Preuve de l'accréditation de l'organisme certificateur.
Le laboratoire doit être accrédité selon la norme ISO/CEI 17025 pour la réalisation des essais sur les produits.	- Preuve de l'accréditation du laboratoire pour le champ considéré.
Le processus de certification doit respecter le système 5 décrit dans la norme ISO 17067 : 2013, à savoir : - les produits doivent faire l'objet d'une évaluation initiale : - essais ; - audit du procédé de fabrication et d'une surveillance : - prélèvements ; - audits de suivi.	- Preuve du processus de certification utilisé (référentiel, attestation de l'organisme certificateur, etc.) - Rapports de contrôle. - Rapports d'essais.

L'installateur doit préciser dans l'offre la technologie des liaisons, le type, la référence, l'utilisation de matériels certifiés NF&A2P ou répondant aux exigences minimales, la quantité et la position sur le site de chaque matériel de détection et d'alarme.

Les matériels utilisant les liaisons hertziennes pour communiquer entre eux ne sont utilisables que pour les applications correspondant à la catégorie de zone A.

3.1.5.2 CAS PARTICULIER

Des matériels non certifiés (non certifiés NF&A2P et ne répondant pas aux exigences minimales) peuvent être utilisés dans les cas suivants :

- matériels appartenant à une famille de produits non couverte par une certification répondant aux exigences du présent document,
- fonction recherchée non présente dans du matériel certifié (dans ce cas, l'installateur titulaire de la certification NF Service & APSAD devra s'assurer des performances et de la compatibilité des matériels retenus),
- lors d'une prescription formalisée (dans ce cas, il appartient au prescripteur/donneur d'ordre de définir la méthode choisie pour garantir le niveau de sûreté de fonctionnement attendu. En l'absence de méthode préconisée, l'installateur justifiera le choix du matériel selon ses propres critères).

L'utilisation de matériels non certifiés doit être précisée dans l'offre.

3.2 REGLES D'INSTALLATION

3.2.1 REGLES GENERALES

Les matériels doivent être installés en respectant les notices des constructeurs. Ils doivent être solidement fixés sur leurs supports par les moyens prévus dans les notices constructeurs.

Le raccordement de tous les matériels constitutifs de l'installation de détection d'intrusion doit être réalisé de façon à autosurveiller les boîtiers, à l'ouverture et à l'arrachement si le matériel le permet (si cette fonction est optionnelle, elle doit être implantée dans le matériel).

Tous les coffrets sont concernés, y compris les boîtes de raccordement et de dérivation, à l'exception des télécommandes portables et des dispositifs d'alarme lumineuse.

Les liaisons filaires qui les relient (à l'exception des liaisons externes au site) doivent être autosurveillées à la coupure et au court - circuit total.

Le raccordement doit être effectué selon les règles de l'art et selon les dispositions de la norme NF C 15-100 Installations électriques à basse tension. Les textes réglementaires en vigueur ainsi que la publication UTE C 18 - 510 (notamment en matière d'habilitation électrique du personnel) doivent être respectés.

La ligne d'alimentation doit être dédiée exclusivement à l'installation de détection d'intrusion, le raccordement sur une prise 230 V n'est pas admis. Cette exigence ne s'applique pas pour l'alarme lumineuse dans le cas de reprise de l'éclairage des locaux.

Tous les éléments d'une installation de détection d'intrusion qui comportent une alimentation doivent respecter les conditions d'utilisation et de contrôle définies par le constructeur.

Les interventions sur l'installation autres que celles normalement pratiquées par l'utilisateur et pouvant entraîner une modification de celle-ci doivent :

- soit provoquer le passage à l'état « alarme »,
- soit utiliser les procédures d'appel sortant ou de contre - appel décrites dans les notices des constructeurs et respectant l'annexe C de la norme EN 50-131-3.

Les matériels doivent comporter des indications suffisantes pour être identifiés sans risque d'erreur (nom du fabricant, modèle, nombre de boucliers, etc.).

Il est rappelé qu'un matériel certifié ne peut pas être modifié et doit être utilisé en respectant les paramétrages de sa certification. Dans le cas contraire, le matériel ne peut plus être considéré comme certifié.

3.2.2 LIAISONS FILAIRES

Le câblage de l'installation de détection d'intrusion doit être suffisamment discret et installé de manière à ne pas faciliter une tentative de neutralisation.

En particulier, il est souhaitable de protéger mécaniquement les câbles des réseaux téléphoniques extérieurs aux locaux surveillés.

Les raccordements des liaisons entre les éléments doivent être réalisés sur leurs borniers et, éventuellement, dans des boîtes de raccordements complémentaires.

Les câbles doivent être d'un seul tenant.

Les barrettes de raccordement intermédiaires (en dehors des éléments et boîtes décrits ci-dessus) et les épissures sont interdites.

3.2.3 LIAISONS RADIO

Les liaisons non filaires étant dépendantes de leur environnement, il est souhaitable, avant de proposer ou d'installer un système à liaison non filaire, d'identifier les sources potentielles de perturbations (par exemple, présence au voisinage d'émetteur de forte puissance, transformateur HT, antennes, etc.).

La vérification de la marge de portée radioélectrique doit être effectuée en suivant la notice du constructeur.

Les dispositifs de surveillance des liaisons hertziennes contre les perturbations radioélectriques (brouillage, saturation, éblouissement) ou de contrôle des alimentations doivent être mis en œuvre selon les procédures définies dans les notices du constructeur.

3.2.4 CENTRALE D'ALARME

La centrale d'alarme doit être implantée à l'intérieur des locaux surveillés. Elle doit être accessible, pour permettre les contrôles et les manipulations d'exploitation.

La centrale d'alarme peut être constituée de plusieurs composants : coffret de traitement, coffret d'alimentation, organes de mise en service, dispositif de lancement de temporisation, dispositif de contrôle de mise en service et télécommande portable, etc.

Les coffrets de traitement et les coffrets d'alimentation certifiés NF&A2P avec 3 boucliers doivent être surveillés à l'arrachement.

Pour les coffrets de traitement et les coffrets d'alimentation certifiés NF&A2P avec 2 boucliers, la surveillance à l'arrachement doit être effective si les coffrets en sont équipés.

Les coffrets de traitement (à l'exception des concentrateurs, convertisseurs et boîtiers d'extension) et d'alimentation doivent faire l'objet d'une surveillance de mouvement ou être sous surveillance humaine en permanence.

Le coffret de traitement de la centrale d'alarme et, s'il existe, le coffret d'alimentation, doivent être scellés lors de la réception de l'installation et après chaque intervention.

3.2.5 ORGANES DE COMMANDE ET DE CONTRÔLE

Il est important que l'utilisateur puisse être informé de la mise en service effective de l'installation de détection d'intrusion. À cet effet, celle-ci doit comporter un dispositif de contrôle sonore ou visuel associé avec la centrale (par exemple : voyant, buzzer) dont le fonctionnement temporaire signale la mise en service effective de l'ensemble de l'installation. Ce dispositif doit être audible ou visible à proximité de l'issue de sortie.

Le dispositif qui permet de signaler à l'utilisateur le niveau faible des tensions d'alimentation au plus tard à la mise en service du système doit être en fonctionnement.

Le chemin de dernière issue doit être tel qu'il puisse être parcouru en un temps inférieur à 45 s. Les temporisations d'entrée et de sortie doivent être adaptées en conséquence. Dans le cas où la distance entre l'organe de commande et la sortie de l'établissement ou du bâtiment ne permet pas le respect de cette exigence, il est nécessaire de mettre en place un dispositif déporté de mise en/hors service, placé à l'intérieur des locaux surveillés et sous détection.

En présence d'un rideau métallique, sa durée de remontée mécanique dépassant fréquemment la minute, il est admis que la temporisation d'entrée soit d'une durée adaptée. Pour des questions d'exploitation, un boîtier shunt peut lancer une temporisation de la première détection pour une durée nécessaire. Celui-ci sera placé à l'extérieur et disposera d'une autosurveillance à l'arrachement. Cette disposition ne dispense pas de la seconde détection à l'ouverture et ne permettra pas l'accès aux zones de localisation des valeurs.

Les organes fixes de mise en service doivent faire l'objet d'une surveillance de mouvement ou être sous surveillance humaine en permanence.

L'organe fixe de mise en service certifié NF&A2P avec 3 boucliers doit être surveillé à l'arrachement.

Pour l'organe fixe de mise en service certifié NF&A2P avec 2 boucliers, la surveillance à l'arrachement doit être effective s'il en est équipé.

Les coffrets de lancement de temporisation d'entrée doivent également être surveillés à l'arrachement.

Les dispositifs de commande fixés à l'extérieur doivent être autosurveillés à l'arrachement. Les indices (IP/IK) de protection sont indiqués dans la notice des constructeurs.

3.2.6 DISPOSITIFS DE DETECTION

Le positionnement des détecteurs doit être tel que leur fonctionnement soit assuré avant qu'ils puissent être neutralisés. Le positionnement des détecteurs doit être choisi en tenant compte de leur mode de détection et de leur résistance à la fraude vis-à-vis des risques encourus.

Lorsque le mode de fonctionnement de l'installation de détection d'intrusion est à lancement de temporisation, le chemin de dernière issue temporisée ne doit pas comporter d'autres détecteurs que ceux faisant partie de ce chemin.

La détection d'ouverture doit être assurée avant que l'ouverture de l'ouvrant ne permette la neutralisation du détecteur de l'extérieur. Dans le cas d'issues et ouvrants à plusieurs battants, les détecteurs assurant la détection d'ouverture doivent détecter l'ouverture de chaque battant.

Les détecteurs de détérioration doivent être choisis en fonction des types et moyens d'attaques envisagés et du support surveillé, sachant que la détection doit être obtenue avant que le passage d'une personne ne soit possible.

Lorsque l'installation de détection d'intrusion est réalisée avec des détecteurs NF&A2P 3 boucliers, la fonction « antimasque » ne doit pas être désactivée. Cette fonction est obligatoire sur les détecteurs NF&A2P 3 boucliers.

Les détecteurs de mouvement doivent être implantés à une hauteur supérieure à 2,50 m ou à la hauteur maximale préconisée par le fabricant dans ses notices.

3.2.7 DISPOSITIFS LOCAUX D'ALARME

Les dispositifs d'alarme sonores ou lumineux doivent être difficilement accessibles. Le positionnement des dispositifs de signalisation d'alarme doit être choisi en tenant compte de leur résistance à la fraude vis-à-vis des risques encourus. Dans la mesure du possible, les dispositifs de signalisation d'alarme doivent être implantés à une hauteur supérieure à 2,50 m.

Le dispositif d'alarme sonore intérieur doit être judicieusement placé dans le site surveillé. Dans la mesure du possible, il ne doit pas être placé à proximité de la centrale d'alarme, afin de rendre plus difficile sa localisation en cas de déclenchement.

Dans le cas où le dispositif d'alarme sonore intérieur est incorporé par construction dans la centrale, l'ensemble doit être placé si possible à une hauteur difficile d'accès pour l'intrus, sans provoquer pour autant de gêne à l'exploitation.

Le dispositif d'alarme sonore doit être capable d'assurer sa fonction dissuasive pour chaque secteur sensible. Il peut être nécessaire de placer plusieurs dispositifs d'alarme pour atteindre cet objectif.

Les dispositifs d'alarme sonore placés à l'extérieur des locaux doivent être autosurveillés à l'arrachement.

La commande du dispositif d'alarme sonore intérieur doit être distincte de celle du dispositif d'alarme sonore extérieur.

Les dispositifs lumineux extérieurs doivent être placés judicieusement pour permettre un repérage à distance du bâtiment ou de sa périmétrie.

Les générateurs de fumée doivent être adaptés aux volumes à protéger. Leur détecteur de confirmation ne doit pas pouvoir être neutralisé avant que les détecteurs d'intrusion aient pu déclencher une alarme.

3.2.8 TRANSMETTEUR D'ALARME

Le transmetteur d'alarme est raccordé à une station de télésurveillance via une liaison de transmission utilisant un ou plusieurs supports de communication, afin de transmettre les informations d'alarmes provenant de la centrale.

Il peut, simultanément ou postérieurement, transmettre des informations telles que des images vidéo ou des données sonores pour permettre la levée de doute.

Il peut, en complément, envoyer des messages à un correspondant (téléalarme).

Dans le cas d'un raccordement à une station de télésurveillance, le transmetteur d'alarme doit satisfaire aux exigences du tableau du chapitre 3.1.4 en fonction de la catégorie de zone.

Dans le cas où le transmetteur d'alarme n'est pas incorporé à la centrale d'alarme, il doit faire l'objet d'une surveillance de mouvement.

Un document d'interface installateur/entreprise de télésurveillance doit être renseigné et mis dans le dossier technique.

Il est souhaitable que l'arrivée des câbles des réseaux de communication à l'intérieur des locaux soit protégée mécaniquement et, si possible, que les câbles soient encastrés dans les parois pour résister aux tentatives de neutralisation.

Le transmetteur d'alarme doit être scellé lors de la réception de l'installation et après chaque intervention.

Si un transmetteur d'alarme permet l'utilisation d'une fonction d'écoute suite à un déclenchement d'alarme, il est admis que cette fonction puisse suspendre l'émission sonore des sirènes pendant cette durée d'écoute. Cette durée ne doit pas excéder 120s.

4. PRECONISATIONS CONCERNANT LA VIDEOSURVEILLANCE

Une installation de vidéosurveillance a pour objectif la surveillance visuelle par l'exploitant, en direct ou en différé :

- de lieux (issues, locaux sensibles, etc.),
- d'objets de valeur (biens, mobiliers, fonds et valeurs, mais aussi produits ou documents).

Elle permettra à l'exploitant de déceler des situations anormales ou non autorisées (approche, déplacement ou comportement d'un individu) dans les secteurs visualisés (issues, locaux contenant des produits attractifs et/ou dangereux, etc.).

La vidéosurveillance est un des moyens de surveillance. Elle peut être associée à d'autres moyens tels que la surveillance humaine, la détection d'intrusion, le contrôle d'accès, etc.

Un système de vidéosurveillance doit remplir un ou plusieurs des rôles suivants :

- aider à la surveillance,
- déterminer l'origine d'un acte de malveillance,
- lever le doute,
- assister le contrôle des flux (véhicules ou personnes),
- détecter le déplacement d'objets ou d'individus.

4.1 REGLES DE CONCEPTION

4.1.1 PRECONISATIONS GENERALES

Une installation de vidéosurveillance doit posséder la qualité essentielle de sûreté de fonctionnement. Une telle installation est sûre lorsqu'elle remplit son rôle de façon durable, stable, dans les conditions définies par les constructeurs des matériels constitutifs de l'installation, tout en respectant les normes en vigueur.

Un défaut affectant un organe de l'installation ne doit pas avoir pour conséquence d'entraîner en cascade d'autres défauts (destruction ou défaillance) dans l'ensemble de l'installation.

Afin de réduire le risque d'erreurs de manipulation, il importe que l'utilisation soit simple. Le paramétrage et l'administration du système de vidéosurveillance doivent être réalisés par une personne formée et désignée par l'exploitant.

Le projet d'installation doit tenir compte d'une éventuelle extension du système.

4.1.2 PRECONISATIONS DE PRISE DE VUE

4.1.2.1 IMPLANTATION DES CAMERAS

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 rôle du système de vidéosurveillance dans ces secteurs.

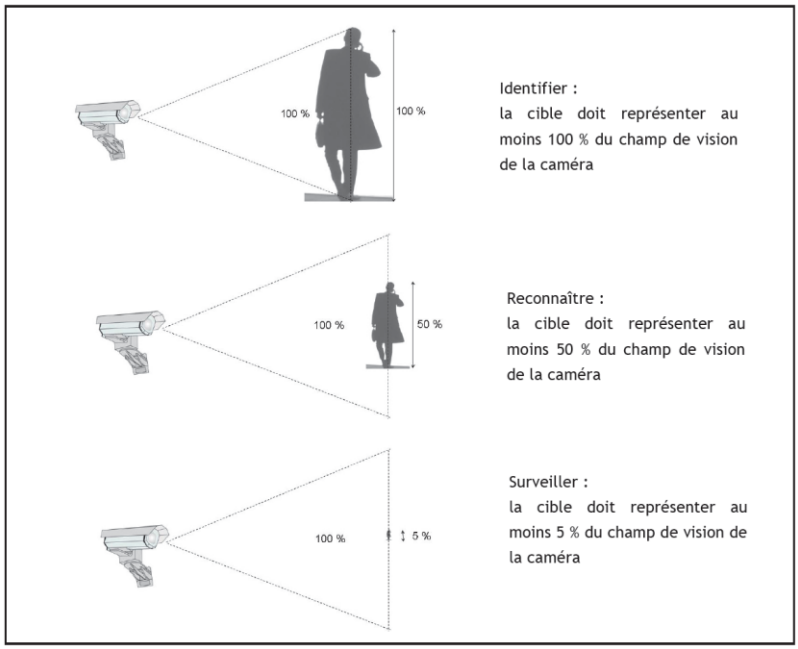
Le détail des images doit être compatible et adapté au niveau d'utilisation nécessaire. (aide à la surveillance, détermination de l'origine d'un acte de malveillance, levée de doute, assistance au contrôle des flux, détection du déplacement d'objets ou d'individus).

À ce titre, la mesure des performances des caméras, présentées dans le chapitre 4.1.2.3, permet d'anticiper la capacité d'une caméra à remplir son rôle et son objectif de prise de vue.

4.1.2.2 DIMENSIONNEMENT D'UN OBJET OU D'UNE CIBLE

Les dimensions d'un objet ou d'une personne (cible) sur l'écran de contrôle (en %) ou après enregistrement d'une image numérisée (en mm par pixel) correspondent à l'objectif recherché dans l'application du rôle de la caméra (par exemple : identification, reconnaissance ou surveillance), selon les recommandations suivantes :

- pour **identifier la cible** en direct, celle-ci doit représenter au moins **100 %** du champ de vision de la caméra (sans fonction zoom), à la distance maximale d'observation souhaitée ; sur les flux enregistrés, le visage d'un individu doit représenter au minimum une vignette de 90 x 60 pixels (arrêté du 3 août 2007),
- pour **reconnaître la cible**, celle-ci doit représenter au moins **50 %** du champ de vision de la caméra, à la distance maximale d'observation souhaitée,
- pour **surveiller la cible**, celle-ci doit représenter au moins **5 %** du champ de vision de la caméra, à la distance maximale d'observation souhaitée.



Cet objectif de prise de vue sera considéré en % de la hauteur de l'écran (comme ci-dessus) pour évaluer la qualité d'une restitution en direct mais sera pris en compte en pixel/m pour une restitution en différé, en particulier si les caméras utilisées sont des caméras mégapixels permettant l'obtention de détails lors de l'agrandissement d'une partie de l'image.

Le tableau ci-dessous permet, en fonction de l'objectif recherché, de déterminer la dimension de la cible sur l'écran de visualisation et sa correspondance en termes de pixels ou de dimension réelle (en m ou en mm) :

Objectif	Dimension de la cible (% du champ de vision de la caméra)	Valeur maximale au plan visé (mm/pixel)	Valeur minimale au plan visé (pixels/m)
Identifier	**100**	**4**	**250**
Reconnaître	**50**	**8**	**125**
Surveiller	**5**	**80**	**12,5**

Dans le cas de l'application de l'arrêté du 3 août 2007, l'identification d'une personne par la vignette visage de 90 x 60 pixels impose un maximum de 3mm/pixel au plan visé (équivalent à 360 pixels/m minimum), considérant une hauteur de visage de 25 cm.

4.1.2.3 CARACTERISTIQUES DES CAMERAS

La qualité des images fournies par le système de vidéosurveillance est très dépendante des caméras utilisées.

La grande majorité des caméras disponibles sur le marché est apte à produire une image correcte, permettant par exemple l'identification sans ambiguïté d'une personne entrant dans son champ de vision, dans des conditions d'éclairage standard (scène statique visée uniformément et modérément éclairée).

Mais cet état de fait peut ne pas être garanti dans des conditions dégradées de cet éclairage ou par un mouvement de la cible.

L'installateur doit donc choisir la « bonne » caméra en fonction de la situation de terrain rencontrée.

Les trois critères de performance « performance en faible éclairage », « performance en contre - jour » et « performance en visualisation de cibles mobiles » sont définis comme les critères fondamentaux pour l'évaluation de la performance opérationnelle d'une caméra de vidéosurveillance :

- La performance en faible éclairage permet de déterminer la capacité de la caméra à visualiser des détails sur des scènes faiblement éclairées. Plus l'éclairage est faible, plus les contrastes sont difficiles à reproduire pour la caméra.
- La performance en contre-jour permet de déterminer la capacité de la caméra à visualiser des détails dans les zones surexposées et/ou sous-exposées à la lumière, lors de prise de la vue sur des scènes proposant de gros écarts d'éclairage.

  Le réglage du temps d'exposition des capteurs de la caméra permet en général d'obtenir des détails, soit dans la zone sous-exposée, soit dans la zone surexposée.
- La performance en capture d'image sur cible mobile permet de déterminer la capacité de la caméra de vidéosurveillance à identifier une cible qui se déplace.

  Une caméra non adaptée à la visualisation de cible en déplacement rapide peut donner l'impression, comme en photographie, d'un phénomène de « trainée » sur l'image.

La spécification technique CNPP DEC 14 007 spécifie les exigences, les critères de performance et les méthodes d'essai pour l'évaluation des caméras de vidéosurveillance.

Le matériel utilisé doit, selon les rôles définis par l'analyse des besoins et des risques, se conformer aux exigences minimales définies dans le tableau ci-après :

<table>
<tr><td rowspan="2">Caractéristiques minimales</td><td colspan="5">Rôle du système de vidéosurveillance</td></tr>
<tr><td>Aide à la surveillance</td><td>Déterminer l'origine d'un acte de malveillance</td><td>Lever le doute</td><td>Assister le contrôle des flux</td><td>Détecter le déplacement d'objets ou d'individus</td></tr>
<tr><td>Résolution caméra numérique</td><td colspan="5">4 CIF</td></tr>
<tr><td>Résolution caméra analogique</td><td colspan="5">480 TVL</td></tr>
<tr><td>Caméra mobile : vitesse de rotation horizontale</td><td rowspan="4">Pas d'exigence minimale</td><td rowspan="4">-</td><td>180°
en un temps inférieur à 1 s</td><td rowspan="4">Pas d'exigence minimale</td><td rowspan="4">-</td></tr>
<tr><td>Caméra mobile : nombre de positions mémorisées</td><td>16 maximum</td></tr>
<tr><td>Zoom motorisé : temps de passage entre deux positions successives</td><td>Temps inférieur à 2 s</td></tr>
<tr><td>Limitation de la focale : temps de passage entre min. et max.</td><td>Temps inférieur à 2 s</td></tr>
<tr><td>Éclairage de la scène / réponse spectrale</td><td colspan="5">Obligation de l'exploitant d'éclairer la scène selon les données du prestataire</td></tr>
</table>

Les caméras mobiles ne peuvent être utilisées pour les rôles « déterminer l'origine d'un acte de malveillance » et « détecter le déplacement d'objets ou d'individus ».

Si ces rôles sont applicables, alors on utilisera des caméras fixes (éventuellement des caméras dômes avec position figée).

4.1.2.4 ECLAIREMENT DE LA SCENE

La source d'éclairage ou la source additionnelle de chaque secteur visualisé doit donner des images acceptables pour toutes les conditions vraisemblables de fonctionnement.

L'éclairement de la zone en surveillance doit être suffisant au regard des objectifs fixés. Le rapport entre l'éclairement maximal et minimal est idéalement de 4 : 1 ou mieux et ceci, dans la zone couverte et pour une scène quelconque.

Quand cela est possible, les éclairages doivent être installés de façon à ne pas dégrader la qualité de l'image fournie par la caméra. La caméra ne doit pas observer la scène au travers de faisceaux lumineux intenses.

Une attention particulière doit être apportée à la direction de l'éclairement ou aux changements rapides des conditions d'éclairement. Le but est de produire un contraste maximal. Un objet peut seulement être détecté si sa brillance est différente de celle de son arrière-plan.

Pour l'objectif d'identification et de reconnaissance, l'éclairement doit permettre de détailler les formes de l'objet et de voir les couleurs, quelles que soient les influences de l'environnement sur la visibilité.

Selon l'éclairement proposé, le choix du type de caméra doit être réalisé en fonction des avantages et des inconvénients rappelés dans le tableau ci-après :

Eclairage	Type de caméra	Avantages	Inconvénients
Éclairage visible	**Caméra en noir et blanc**	**Meilleure résolution des caméras** **Sensibilité plus importante que les caméras couleur**	**Peu d'informations lors de l'exploitation des images** **Nécessite un éclairage pour un fonctionnement nocturne**
	Caméra en couleur	**Plus d'informations qu'en noir et blanc lors de l'exploitation des images**	**Eclairage plus important, en particulier pour un fonctionnement nocturne**
Pas d'éclairage	**Caméra d'imagerie thermique**	**Ne nécessite pas d'éclairage supplémentaire**	**Insuffisant pour l'identification**
Éclairage dans l'infrarouge proche	**Caméra utilisée dans le proche infrarouge**	**Possibilité de vision nocturne avec un éclairage spécifique mais invisible**	**Peu de détails lors de l'exploitation des images**

4.1.3 PRECONISATIONS DE TRANSPORT DE DONNEES

Le signal vidéo en sortie de la caméra doit être transmis sans altération significative, de façon à être visualisé correctement après traitement.

De façon générale, la principale exigence de transport des données est de transporter le signal vidéo délivré par la caméra de façon à respecter les exigences de restitution.

Les principaux moyens de transport des données, analogiques et/ou numériques, sont les suivants :

- câble coaxial,
- réseau informatique dédié ou non,
- fibre optique,
- onde micrométrique ou fréquence radio,
- infrarouge ou laser,
- paires torsadées,
- réseau téléphonique commuté (RTC),
- réseau RNIS.

Les éléments suivants permettent de choisir un moyen de transport des données ou une combinaison de plusieurs moyens de transport des données :

- la méthode et le taux de compression,
- la bande passante de la voie de transport des données,
- le rapport signal sur bruit,
- la distorsion du signal,
- la distance à couvrir,
- l'immunité vis-à-vis des interférences,
- la sécurité et la confidentialité des communications,
- les contraintes relatives à l'installation,
- les contraintes relatives à la maintenance.

De nombreux systèmes sont disponibles, avec des caractéristiques (vitesses de transport des données et des résolutions) très variées. Le système choisi doit être évalué avec soin et de façon cohérente.

Dans tous les cas, le moyen de transport des données doit être choisi en fonction des conditions d'environnement et d'éloignement du poste d'exploitation.

Les distances maximales d'utilisation en fonction des technologies employées sont définies par une exigence sur l'atténuation maximale acceptable. L'atténuation maximale acceptable pour le signal est de **6 dB**.

A titre informatif, les tableaux ci-après donnent les limites couramment admises pour respecter cette atténuation maximale de 6 dB pour différents supports :

Câbles coaxiaux			
Type de câble	Distance maximale	Bande passante	Nombre d'amplificateurs max.*
KX-6 ou RG59U	**250 m**	**5 MHz**	**1**
KX-8	**400 m**	**5 MHz**	**1**
Câbles haute qualité (ex : VCB100)	**600 m**	**5 MHz**	**1**
** Le rapport signal/bruit des éventuels amplificateurs utilisés devra être indiqué et fera l'objet d'une vérification au niveau de la réception de l'installation.*			

Fibres optiques		
Type de fibre	Distance maximale	Nombre d'amplificateurs max.*
Monomode	**100 km**	**-**
Multimode	**10 km**	**-**
** Le rapport signal/bruit des éventuels amplificateurs utilisés devra être indiqué et fera l'objet d'une vérification au niveau de la réception de l'installation.*		

Paires de cuivre torsadées		
Type de paire	Distance maximale	Nombre d'amplificateurs max.*
Non blindée (UTP)	**55 m**	**-**
Blindée (STP)	**100 m**	**-**
** Le rapport signal/bruit des éventuels amplificateurs utilisés devra être indiqué et fera l'objet d'une vérification au niveau de la réception de l'installation.*		

4.1.4 PRECONISATIONS DE RESTITUTION DE L'IMAGE

4.1.4.1 PRECONISATION SUR LE MATERIEL

Le matériel utilisé pour la restitution de l'image doit au minimum permettre le respect des exigences fonctionnelles du tableau ci-dessous :

Caractéristiques minimales	Rôle du système de vidéosurveillance				
	Aide à la surveillance	Déterminer l'origine d'un acte de malveillance	Lever le doute	Assister le contrôle des flux	Détecter le déplacement d'objets ou d'individus
Restitution en direct					
Résolution par image sur le moniteur	**1 CIF**	**Sans objet**	**4 CIF**		
Nombre le client d'images affichées par seconde	**12**		**6**		
Restitution en différé					
Résolution de l'image enregistrée	**1 CIF / 4 CIF (1)**				
Nombre d'images enregistrées par seconde et par caméra	**6 / 12 images par seconde (1)**				
(1) Si l'objectif recherché de la prise de vue est d'identifier la cible (par exemple avec la nécessité de placer au minimum 90 x 60 pixels sur un visage), alors on doit enregistrer au format 4 CIF minimum et utiliser une vitesse d'enregistrement de 12 images par seconde minimum.					

Ce matériel doit permettre de réaliser la visualisation et/ou l'enregistrement permanent des caméras assurant la vidéosurveillance des secteurs visualisés désignés.

De plus, il peut permettre, de façon optionnelle :

- le multiplexage automatique ou l'affichage en mosaïque des caméras selon un scénario paramétrable, si l'exploitation le nécessite,
- la commande de la rotation des caméras (si celles-ci sont équipées),
- un zoom sur la zone surveillée sur demande (pour les caméras équipées).

Lorsqu'un enregistrement est demandé, manuellement ou automatiquement, toutes les images des caméras retenues doivent être enregistrées, indépendamment de leur visualisation sur un moniteur.

Le dispositif d'enregistrement des images doit :

- permettre une sélection des caméras, sur demande de l'opérateur ou par programmation (sur évènement ou selon des plages horaires),
- pouvoir mémoriser les images précédant un événement sur une durée réglable, à convenir avec l'exploitant en fonction des résultats de l'analyse des besoins et des risques,
- pouvoir mémoriser (si nécessaire) une quantité d'images supérieure ou égale à 12 images par seconde et par caméra,
- avoir une capacité de stockage suffisante pour mémoriser des évènements pendant une durée convenue avec l'exploitant.

En outre, pour faciliter l'exploitation des images enregistrées, il peut être nécessaire de disposer d'une solution technique permettant d'associer les images enregistrées à des évènements identifiés.

Les niveaux de résolution des images enregistrées demandés dans le tableau précédent s'entendent « à niveau de compression raisonnable ».

Un taux de compression d'image trop important peut dégrader de façon importante le flux vidéo.

Les taux de compression d'image sont le plus souvent réglables par l'utilisateur mais peuvent être automatiquement relevés (image dégradée) par l'enregistreur dans le cas où la capacité de celui-ci est dépassée en bande passante.

L'installateur et l'exploitant doivent s'assurer que les flux enregistrés permettent d'obtenir après exportation un niveau de détail équivalent à celui des flux visionnés « en direct ».

Les enregistreurs vidéo numériques doivent répondre aux exigences de l'arrêté du 3 août 2007.

4.1.4.2 CONFIGURATION DU POSTE D'EXPLOITATION

Le pupitre de commande doit être conçu de manière ergonomique, en faisant particulièrement attention à l'emplacement des écrans de visualisation pour éviter les réflexions provenant de sources lumineuses extérieures, tout en respectant les exigences éventuelles de confidentialité des images vis-à-vis des tiers (public, visiteurs, etc.).

Le matériel de traitement et d'enregistrement ainsi que le matériel de duplication (imprimantes vidéo, graveurs, etc.) doivent être installés dans des zones accessibles uniquement aux personnes autorisées.

Le nombre d'écrans de visualisation doit être déterminé en fonction de considérations fonctionnelles telles que la distance d'observation et le nombre d'opérateurs en activité simultanément.

Il est recommandé que les opérateurs soient placés à une distance correspondant à **4,7 fois** la taille de l'écran (mesuré par sa diagonale) pour les moniteurs à tube.

Pour les moniteurs LCD, qui rayonnent avec une énergie moindre, la distance peut être ramenée à **3,5 fois** la diagonale de l'écran.

L'usage de moniteurs à cristaux liquides (LCD) doit être privilégié. Ils dégagent moins de chaleur que les écrans à tubes, ce qui se traduit notamment par un allongement de la durée de vie des matériels et un meilleur confort des opérateurs.

De plus, les écrans LCD étant « plats », l'espace du poste de sécurité est optimisé.

Idéalement, les points suivants doivent être respectés :

- le nombre maximal d'écrans par opérateur est fixé à **2**,
- la taille minimale des écrans est de **20 pouces**,
- le nombre maximal d'images par écran est de **9** (si l'opérateur visualise deux moniteurs).

L'implantation de l'éclairage des postes de travail et l'inclinaison des moniteurs doivent être déterminés afin d'éviter les réflexions.

4.1.5 PRECONISATIONS DE SECURITE

4.1.5.1 INTEGRITE DU SYSTEME

Concernant la prise de vue, il peut être nécessaire de protéger les caméras avec un caisson dédié. La spécification CNPP DEC 15 004 décrit les critères permettant le choix d'un caisson adapté.

Concernant la transmission, le réseau utilisé pour la communication entre les différents organes du système devra être choisi et déployé pour respecter les exigences formulées dans l'analyse des besoins et des risques.

Concernant la restitution, le réglage des paramètres d'enregistrement ne doit pouvoir être modifié que par l'administrateur ou une personne désignée par l'exploitant (cette personne peut être l'installateur).

Au global, l'intégrité d'un système de vidéosurveillance peut être :

- de niveau 1 pour les exigences de base,
- de niveau 2 si les défaillances techniques sont signalées,
- de niveau 3 si les défaillances techniques ainsi que le masquage et le pivotement accidentels de la caméra sont signalés,
- de niveau 4 si les défaillances techniques et les tentatives d'attaque contre le système (sabotage, substitution, etc.) sont signalées.

Les niveaux 2 à 4 correspondent à une augmentation de la disponibilité du système de vidéosurveillance.

En fonction du rôle du système de vidéosurveillance, les exigences minimales d'intégrité sont définies dans le tableau ci-après :

Caractéristiques minimales	Rôle du système de vidéosurveillance				
	Aide à la surveillance	Déterminer l'origine d'un acte de malveillance	Lever le doute	Assister le contrôle des flux	Détecter le déplacement d'objets ou d'individus
Niveau d'intégrité associé	**1**	**1**	**2 ou 3 (1)**	**1**	**2 ou 3 (1)**
(1) Dans le cas où l'analyse des besoins et des risques montre que le risque d'attaque est à prendre en compte, le critère d'intégrité 4 est à retenir pour le(s) rôle(s) concerné(s).					

Les différentes attaques ou défaillances associées à un niveau d'intégrité sont définies dans le tableau ci-après :

Fonction	Défaillances ou attaques à signaler	Niveau d'intégrité associé			
		1	2	3	4
Prise de vue	**Défaillance de la caméra (y compris absence de l'alimentation)**	**-**	**x**	**x**	**x**
	Masquage de la caméra	**-**	**-**	**x (2)**	**x (1)**
	Pivotement de la caméra	**-**	**-**	**x (2)**	**x (1)**
	Substitution d'image	**-**	**-**	**-**	**x (1)**
Transport des données	**Défaillance des équipements de transport des données vidéo (y compris absence de l'alimentation ou défaillance du fournisseur d'accès)**	**-**	**x**	**x**	**x**
	Défaillance des liaisons de transport des données d'évènements à distance	**-**	**-**	**x**	**x**
Restitution	**Défaillance de l'enregistrement, y compris de l'alimentation du système**	**x**	**x**	**x**	**x**
	Défaillance disque dur	**-**	**x**	**x**	**x**

(1) Ces attaques doivent être signalées dans un délai inférieur à 60 s, préalablement défini lors de l'analyse des besoins et des risques.

(2) Les défaillances telles que le masquage et le pivotement accidentels de la caméra doivent être signalées dans le délai défini lors de l'analyse des besoins et des risques, à contractualiser.

La signalisation de ces défaillances ou attaques doit être réalisée de sorte qu'une information (générée par le système de vidéosurveillance) puisse être signalée à l'exploitant après la survenance de l'évènement.

Cette information peut être transmise, selon l'analyse des besoins et des risques, à une station de télésurveillance.

Un niveau d'intégrité de 2, 3 ou 4 implique l'existence d'une autre voie de communication pour le message d'alarme en cas de défaillance des équipements de transport des données. On recommande par exemple l'utilisation d'un réseau téléphonique commuté (PSTN public switched telephone network) permettant le relais vers la centrale d'alarme : on n'utilise alors pas le réseau IP principal sur lequel transite le flux vidéo pour transmettre la condition d'alarme.

4.1.5.2 ALIMENTATION

L'alimentation de l'installation doit être assurée en permanence. Les éléments doivent être alimentés par une alimentation principale fournie par un réseau basse tension ou très basse tension et sauvegardée si nécessaire par une alimentation secondaire (batteries d'accumulateurs, onduleur, etc.).

La ou les lignes d'alimentation principale doivent être dédiées exclusivement à l'installation.

L'alimentation secondaire doit assurer immédiatement, en cas d'absence de l'alimentation principale, le fonctionnement du système sans perte d'informations et doit, dans ce cas, assurer le fonctionnement de la partie secourue pendant une durée minimale de 15 min.

Un défaut d'alimentation (principale et/ou secondaire) doit être signalé à l'exploitant.

4.1.5.3 SECURITE DES POSTES

Poste d'exploitation :

Le choix du ou des sites où se trouvent implantés les locaux abritant les écrans de visualisation, et éventuellement les enregistreurs, doit tenir compte de l'environnement et des risques qui peuvent en découler.

Les exigences relatives aux postes d'exploitation vidéo à distance (PEVD) client sont développées ci-dessous :

- l'exploitation des images est entièrement sous la responsabilité de l'exploitant qui doit élaborer des consignes claires pour les opérateurs,
- le poste d'exploitation vidéo à distance ne peut pas être un dispositif portatif de type smartphone,
- le poste d'exploitation vidéo à distance doit être implanté dans un local identifié (où est situé l'opérateur) et doit répondre aux exigences minimales suivantes :
    - Enveloppe :

      le local doit être isolé des autres locaux de l'Université par des parois opaques de l'extérieur et le local doit être dédié à cette mission.
    - Climatisation :

      la température du local doit être maintenue en permanence dans les limites compatibles avec le bon fonctionnement des équipements.
    - Moyens de surveillance et d'accès :

      l'accès au local doit être fait par un système de contrôle d'accès.

Il est préférable que l'opérateur dispose d'outils lui permettant de replacer dans leur contexte les images reçues (plans de site, images de référence, etc.).

Les procédures d'exploitation des flux vidéo et les actions à mener doivent faire l'objet d'un document d'exploitation remis à l'opérateur.

De plus, l'opérateur s'engagera à travers une charte de déontologie.

Il appartient à l'exploitant de procéder aux vérifications prévues dans le tableau ci-après :

Eléments à vérifier par l'exploitant	Procédure
Horodatage exact et présent	**Contrôle visuel**
Libellé de la caméra exact et présent	**Contrôle visuel**
Durée d'archivage par caméra	**Contrôle des enregistrements**

Poste de télésurveillance :

L'exploitation à distance des évènements (alarmes ou dérangements) relatifs au système de vidéosurveillance doit être réalisée par une station de télésurveillance répondant aux exigences du référentiel APSAD R311 (ou titulaire de la certification APSAD de service de télésurveillance, de type P2 ou P3).

Dans le cas où le rôle affecté à l'exploitation du système de vidéosurveillance n'est pas limité à une levée de doute sur alarme, il y a lieu de spécifier le nombre d'écrans affectés par personne.

Local technique :

Dans le cas où les matériels de traitement et d'enregistrement ne sont pas installés dans le poste local d'exploitation, le ou les locaux techniques doivent être surveillés ou mécaniquement protégés et accessibles uniquement aux personnes autorisées.

L'environnement du local technique doit être adapté aux conditions de fonctionnement des matériels installés.

4.1.5.4 SECURITE NUMERIQUE

Dès lors que le système de vidéosurveillance est implanté et/ou exploité via un réseau IP, des précautions d'usage doivent être respectées au regard de la sécurité numérique.

En particulier, les mises à jour des pare-feu, du système d'exploitation, des logiciels antivirus et des logiciels spécifiques à la vidéosurveillance utilisés doivent être réalisés régulièrement.

La responsabilité de la sécurité numérique de l'installation doit être clairement établie (service sécurité informatique du site ou contrat de maintenance) et une politique de sécurité du système d'information doit être définie et appliquée.

Celle-ci va définir les méthodes et les acteurs de la garantie de confidentialité, de l'intégrité et de la disponibilité du système et des données qu'il contient.

Les exigences suivantes restent néanmoins indispensables pour une installation sécurisée :

- le site doit être protégé par un pare-feu configuré selon le principe du moindre privilège. Il appartient à l'installateur d'indiquer avec précision les protocoles et ports à libérer pour un fonctionnement correct du système. Le choix et la responsabilité de libérer ces protocoles et ports vers l'extérieur de l'organisation appartient au RSSI et doit être fait avec précaution,
- l'installateur a la responsabilité d'indiquer à l'exploitant l'ensemble des services protégés par mot de passe et il revient à l'exploitant, après que l'installateur lui en a indiqué la procédure, de modifier chacun de ces mots de passe. L'exploitant doit être le seul à en avoir connaissance,
- l'installateur doit également mettre le système à jour dans sa version la plus récente et, si les mises à jour ne sont pas automatiques, indiquer à l'exploitant comment les effectuer. L'exploitant doit alors les effectuer régulièrement. La politique de sécurité doit indiquer la fréquence de mise à jour. Une mise à jour tous les trois mois minimum est recommandée,
- afin d'assurer la bonne utilisation des protocoles de sécurisation de communication (https, messagerie électronique sur TLS, signature numérique de documents), le RSSI doit fournir un certificat délivré par une autorité de certification (qui peut être interne à l'Université) à l'installateur qui a la responsabilité de l'importer au système,
- enfin, si le système comprend des services à risque (par exemple, comprenant une authentification non chiffrée [telnet, ftp, etc.]), il appartient à l'installateur de déconseiller leur utilisation à l'exploitant et, si cela est permis par le système, de les désactiver. L'exploitant ne doit pas les réactiver et s'en servir.

4.2 REGLES D'INSTALLATION

4.2.1 REGLES GENERALES

Les matériels doivent être installés et solidement fixés sur leurs supports par les moyens prévus dans les notices constructeurs. Ils doivent comporter des indications suffisantes pour être identifiés sans risque d'erreur (nom du fabricant, modèle, type, etc.).

Le raccordement doit être effectué selon les règles de l'art et les dispositions de la norme NF C 15-100. Les textes réglementaires en vigueur ainsi que les préconisations des guides UTE C 15-520 et UTE C 15-900 (notamment en matière d'habilitation électrique du personnel) doivent être respectés.

Les caméras doivent être fixées aux endroits les plus pertinents pour réaliser les rôles choisis, sur chaque secteur visualisé. Un enregistrement et une impression des vues de référence (ce que voit la caméra) doit être réalisé.

En fonction des exigences de qualité des images requises par l'analyse des besoins et des risques, les modes et les taux de compression utilisés pour la visualisation en temps réel et/ou les enregistrements conduisent à choisir un support de transport des données et une capacité de stockage adaptés.

Le rapport signal sur bruit et la distorsion du signal ont des effets cumulatifs, peuvent provoquer la dégradation des images et donc dégrader l'efficacité du système.

4.2.2 LES LIAISONS

Il faut optimiser le cheminement des câbles en respectant la distance entre les matériels. Il faut cependant prendre en compte les possibilités d'extensions futures du système et toutes les modifications vraisemblables du site.

Les câbles sont choisis pour minimiser les chutes de tension et les pertes de signal. Les spécifications relatives à l'environnement et à la sécurité doivent être prises en compte et les câbles doivent être marqués conformément à leur type.

Pour les câbles de grande longueur, des matériels d'amplification (éventuellement intégrés aux équipements) peuvent être nécessaires pour satisfaire aux performances du système.

Si des fibres optiques sont utilisées, les pertes tolérables doivent correspondre au plus à trois réparations sur les câbles pendant la durée de vie du système.

Le rayon de courbure doit respecter les spécifications des fabricants.

Les connections doivent être adaptées à la fibre optique.

L'utilisation des chemins de câbles aériens est à éviter. Si cela n'est pas possible, il convient de conserver une hauteur de dégagement permettant la mise en place des câbles supports. Les fixations doivent satisfaire aux normes en vigueur.

Si des câbles sont installés dans des conduits enterrés, il convient de laisser dans le conduit un fil de tirage à la disposition de la maintenance.

Les câbles extérieurs aux bâtiments susceptibles d'être soumis à des détériorations mécaniques doivent être protégés.

Les câbles reliant les caméras mobiles doivent rester suffisamment flexibles sur toute la plage des températures correspondant à l'environnement.

Pendant l'installation des câbles, des précautions doivent être prises pour éviter l'humidité. Ceci est particulièrement important si l'on utilise des câbles coaxiaux creux.

Le câblage de l'installation doit être prévu et installé de façon discrète afin de ne pas faciliter une tentative de neutralisation.

Les raccordements des liaisons entre les éléments doivent être réalisés sur leurs connecteurs. Les câbles doivent être d'un seul tenant. Les barrettes de raccordement intermédiaires, les boîtes de raccordement et les épissures sont interdites.

4.2.3 MASQUAGE

Afin de satisfaire aux exigences réglementaires (Loi n° 78 - 17 du 6 janvier 1978 modifiée relative à l'informatique et aux libertés), un dispositif de masquage permettra d'occulter les zones privées interdites à la visualisation.

Les caractéristiques attendues du masquage dynamique sont, au minimum, les suivantes :

- masques variables en taille selon le zoom utilisé par l'opérateur,
- masques mobiles dans l'image afin de suivre la rotation de la caméra sur ses deux axes.

Le masquage peut être géré de façon autonome par la caméra.

4.2.4 PROTECTION CONTRE LES CHOCS ET LES INFLUENCES EXTERNES

Pour une utilisation à l'extérieur des bâtiments, les caméras et leur liaison (si elles sont accessibles) devront disposer d'un degré de protection IK08 contre les chocs ou dégradations et d'un degré de protection IP65 contre les pénétrations (solides et liquides).

4.2.5 DISTRIBUTION DES IMAGES

Dans un système de vidéosurveillance, la distribution des images sur le ou les moniteurs ou écrans, c'est-à-dire le choix du nombre d'images affichées simultanément, est réalisé par un des matériels suivants :

- matrice (technologie numérique ou analogique),
- multiplexeur (technologie analogique ou numérique via un logiciel de visualisation),
- quadravision (technologie analogique ou numérique via un logiciel de visualisation),
- enregistreur (enregistreur numérique en technologie numérique, magnétoscope en technologie analogique),
- décodeur (technologie numérique, matérielle ou logicielle),
- logiciel (numérique).

4.2.6 COMPRESSION

Les moyens de compression de données mis en œuvre doivent satisfaire aux objectifs de qualité des images et de garantie de l'intégrité des images.

5. PRINCIPES DE SÛRETE APPLICABLES A L'UNIVERSITE DE NANTES

L'Université de Nantes a défini un zoning de ces locaux et espaces en fonction du niveau de risque, du niveau de sensibilité et de la valeur marchande :

- **Les zones et axes sensibles extérieures**
  - routes publiques,
  - axes importants,
  - bâtiments très sensibles,
  - parking sensibles,
- **Les zones rouges** ne sont accessibles qu'à un nombre très limité de personnel :
  - Salles informatiques (salle serveurs et baie de brassage),
  - Stockage de matériels Informatique ou Vidéo à haute valeur marchande,
  - Archives,
  - Agence comptable et coffre-fort,
  - Stockage de produit chimique, de matières dangereuses,
  - Bureau de la Présidence,
  - Bureaux sensibles,
  - Autres zones sensibles,
- **Les zones oranges** ne sont accessibles qu'au personnel lié à la gestion de l'activité de la zone :
  - Laboratoires de recherche scientifique et informatique,
  - Locaux administratifs,
  - Stockage de produits intermédiaires à valeur marchande moyenne,
  - Locaux techniques (électriques, traitement de l'air, etc.),
  - Bâtiment à usage non étudiant,
- **Les zones vertes** sont accessibles aux étudiants, visiteurs et personnels pendant les heures ouvrées :
  - Tous les autres locaux non listés ci-dessus.

Ces zones déterminent le niveau sécuritaire des équipements à mettre en œuvre afin de les sécuriser.

La mise en sécurité des sites de l'Université de Nantes concernera conjointement :

- Le contrôle des accès aux zones sensibles internes à accès restreint (zone orange) et à accès limités (zones rouges),
- La surveillance contre les intrusions à la périmétrie des bâtiments, dans les bâtiments et dans certaines zones névralgiques,

- La vidéosurveillance de la périphérie des bâtiments accessibles directement depuis l'extérieur, des mouvements aux entrées des bâtiments et sites (parking) ainsi qu'à celles de certaines zones sensibles,
- L'asservissement des portes de circulation et des issues de secours aux systèmes de sécurité incendie existants.

Les systèmes de sûreté projetés pour la surveillance de l'Université de Nantes devront satisfaire aux critères suivants :

- Convivialité d'exploitation,
- Compatibilité et ouverture vers des applications connexes,
- Flexibilité,
- Modularité,
- Fiabilité.

Le système de sécurité intégré permettra de superviser le contrôle d'accès, la détection intrusion et la vidéosurveillance à partir d'un poste unique disposant d'une interface graphique conviviale.

L'architecture de supervision et d'exploitation de l'installation qui sera retenue devra permettre d'assurer une réaction efficace des services de sécurité.

Le système sera compatible les cartes professionnelles (cartes CMS) mises à disposition de chaque personnel et étudiant de L'Université de Nantes.

De plus, il permettra, pour des besoins temporaires, d'associer des badges (technologie similaire que les cartes CMS, également fournis par l'Université) à des prestataires ou personnes externes à l'Université ne figurant pas dans l'annuaire LDAP.

Le système permettra une gestion intégrée de cylindres ou béquilles type Serrure Autonome ou bandeau de ventouse côté extérieur et gâche électrique côté intérieur.

Le système devra pouvoir être hébergé sur l'infrastructure informatique de l'Université.

Le système, de type client-serveur, pourra assurer une gestion multi-site et multi-client/multi-entité.

Les fonctions de gestion des droits d'accès, de gestion d'exceptions, de gestion de filtres sur les historiques par des requêtes simples et préenregistrées, d'édition automatiques de rapports, de gestion d'intrusion, d'animation des synoptiques, de gestion des visiteurs, de gestion des rondes, de personnalisation des badges, d'exploitation vidéo et de communication inter-systèmes seront assurées par des modules logiciels parfaitement intégrés.

La vidéo surveillance sera conçue comme un outil de dissuasion, de levée de doute et d'enregistrement en vue d'une enquête et/ou une recherche ultérieure.

Les caméras couleurs seront de type IP PoE.

Afin de conserver l'autonomie de l'utilisateur, les modélisations se feront au travers de paramétrages et non de programmation.

Le système central devra pouvoir accueillir de nouveaux postes opérateurs, hiérarchisables et paramétrables.

En termes d'infrastructure, les solutions filaires devront être réalisées sur réseau IP.

5.1 ZONES VERTES

5.1.1 CONTRÔLE D'ACCES

Aucun système de contrôle d'accès ne sera mise en œuvre dans les zones vertes.

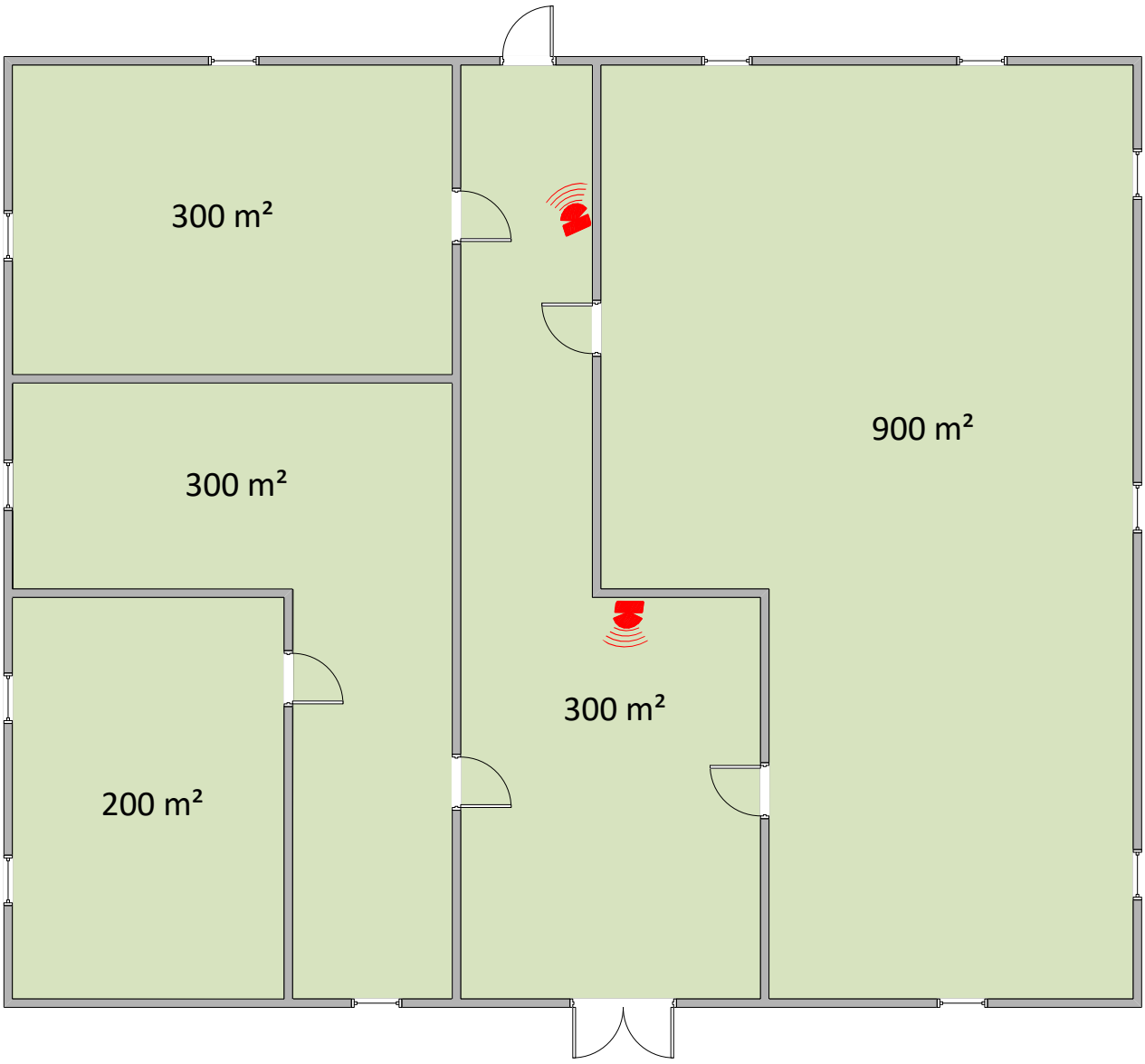
5.1.2 DETECTION D'INTRUSION

Une surveillance des pénétrations au niveau des issues principales ainsi qu'une surveillance des mouvement au niveau des passages obligés sera assurée par des détecteurs de mouvement volumétriques double technologie infrarouge et hyperfréquence (uniquement au niveau rez-de-chaussée).

5.1.3 VIDEOSURVEILLANCE

Aucun système de vidéosurveillance ne sera mise en œuvre dans les zones vertes.

5.1.4 SCHEMA DE PRINCIPE



LEGENDE	
LB Lecteur de badges	Détecteur volumétrique
Caméra	Détecteur d'ouverture

5.2 ZONES ORANGES

5.2.1 CONTRÔLE D'ACCES

Les zones oranges seront contrôlées, conformément aux préconications du chapitre 2 du présent document, par lecteurs de badges en entrée et libre en sortie par bouton poussoir pendant les heures ouvrées et non ouvrées (nuit, week-end et vacances scolaires).

Seul le personnel lié à la gestion de l'activité de la zone aura accès à ces zones.

Les portes de circulation et les issues de secours devront être asservies aux systèmes de sécurité incendie existants.

5.2.2 DETECTION D'INTRUSION

Pour les zones oranges inférieures à 800 m² (catégorie A), une surveillance des pénétrations au niveau des issues principales ainsi qu'une surveillance des mouvement au niveau des passages obligés sera assurée par des détecteurs de mouvement volumétriques double technologie infrarouge et hyperfréquence.

Pour les zones oranges supérieures à 800 m² (catégories B et C), une surveillance des pénétrations au niveau des issues principales, secondaires et des ouvrants sera assurée par des détecteurs d'ouverture magnétiques.

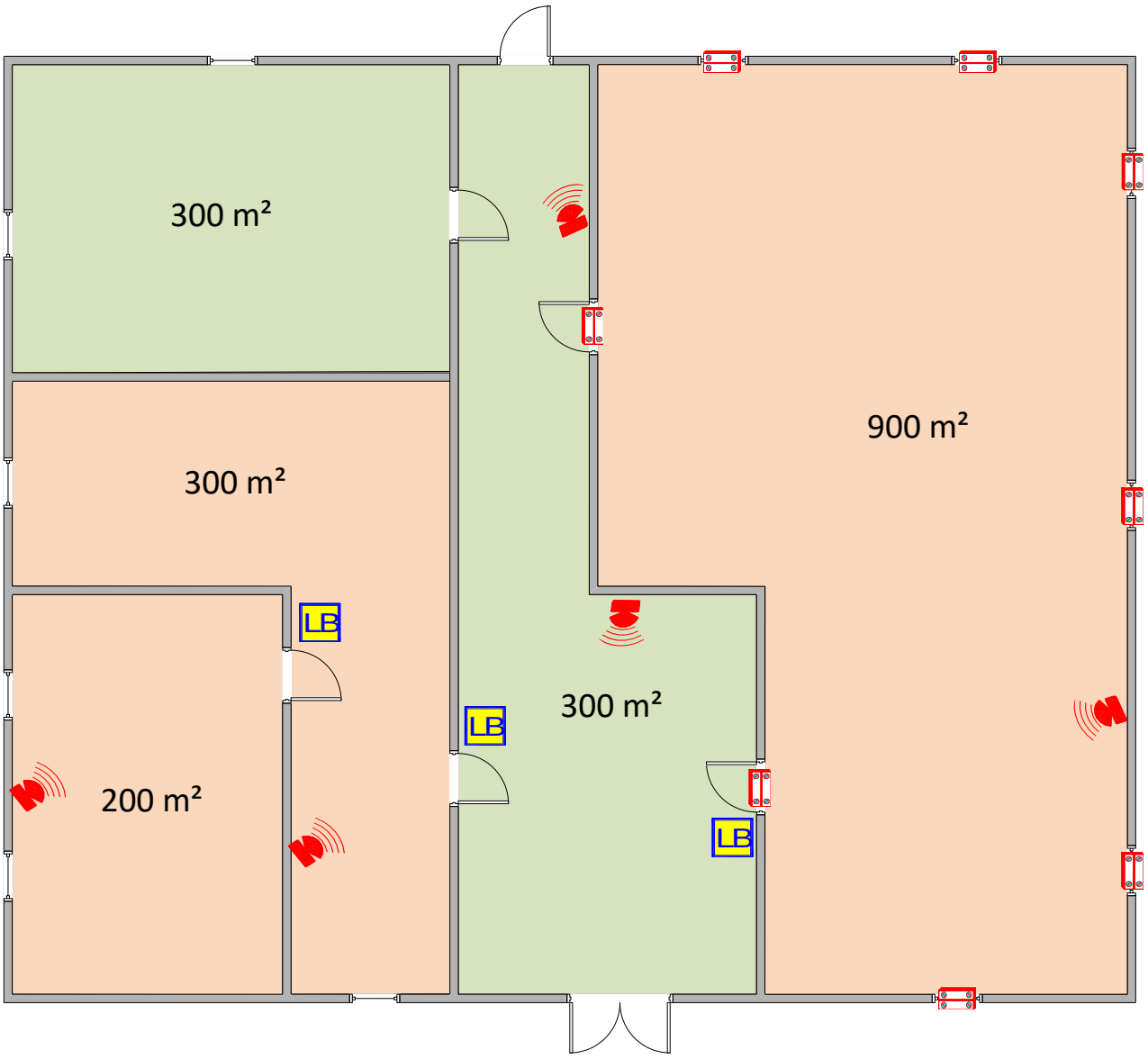
De plus, une surveillance des mouvement au niveau des passages obligés sera assurée par des détecteurs de mouvement volumétriques double technologie infrarouge et hyperfréquence.

La mise en œuvre de ces équipements de détection d'intrusion devra être réalisée conformément aux préconisation du chapitre 3 du présent document.

5.2.3 VIDEOSURVEILLANCE

Aucun système de vidéosurveillance ne sera mise en œuvre dans les zones oranges.

5.2.4 SCHEMA DE PRINCIPE



LEGENDE	
LB Lecteur de badges	Détecteur volumétrique
Caméra	Détecteur d'ouverture

5.3 ZONES ROUGES

5.3.1 CONTRÔLE D'ACCES

Les zones rouges seront contrôlées, conformément aux préconications du chapitre 2 du présent document, par lecteurs de badges en entrée et libre en sortie par bouton poussoir pendant les heures ouvrées et non ouvrées (nuit, week-end et vacances scolaires).

Seul un nombre très limité de personnel aura accès à ces zones.

Les portes de circulation et les issues de secours devront être asservies aux systèmes de sécurité incendie existants.

5.3.2 DETECTION D'INTRUSION

Pour les zones rouges (catégories B et C), une surveillance des pénétrations au niveau des issues principales, secondaires et des ouvrants sera assurée par des détecteurs d'ouverture magnétiques.

De plus, une surveillance des mouvement au niveau des passages obligés sera assurée par des détecteurs de mouvement volumétriques double technologie infrarouge et hyperfréquence.

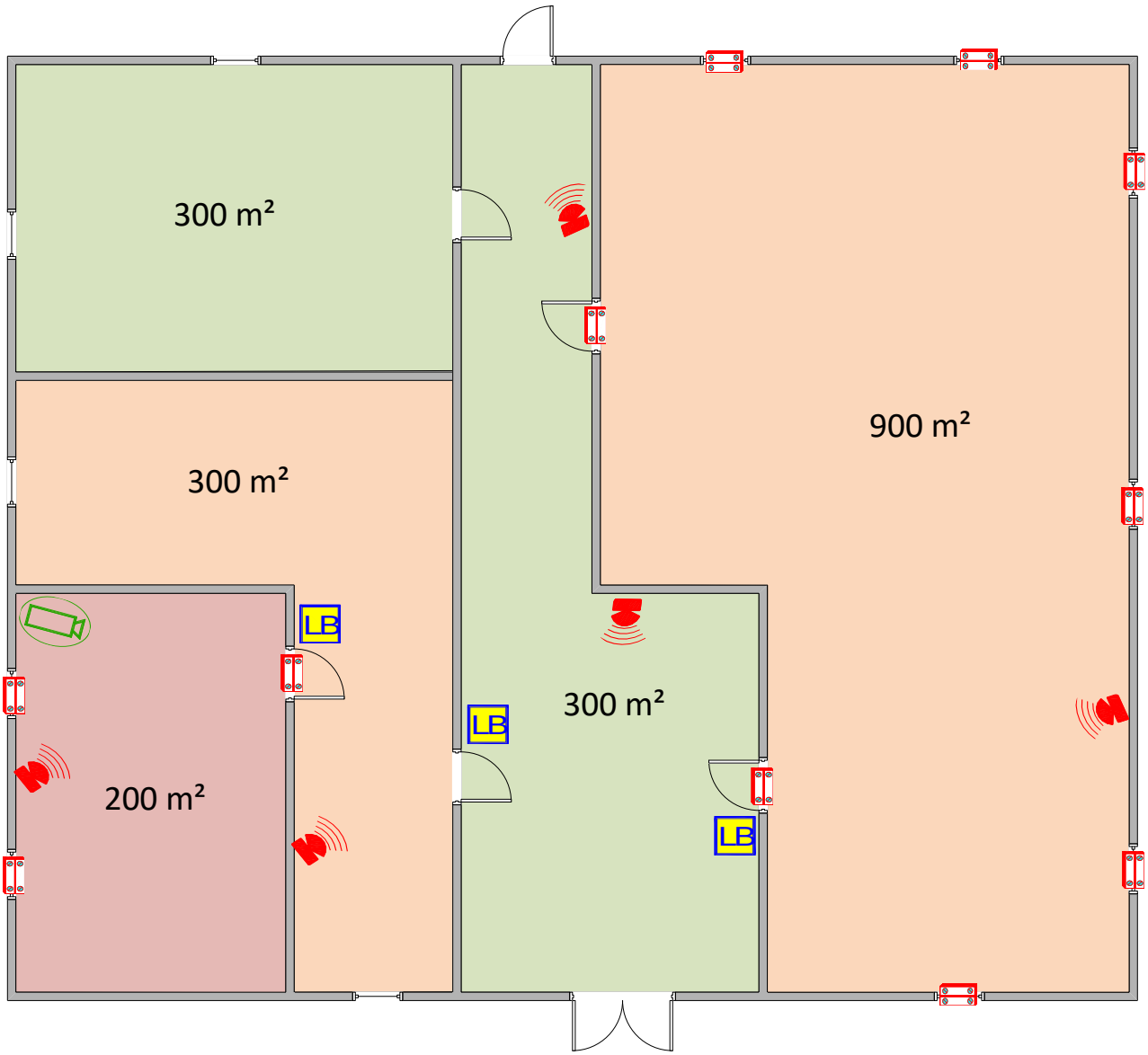
La mise en œuvre de ces équipements de détection d'intrusion devra être réalisée conformément aux préconisation du chapitre 3 du présent document.

5.3.3 VIDEOSURVEILLANCE

En fonction du niveau de risque de chaque local/espace (à étudier au cas par cas), une surveillance vidéo pourra être assurée, conformément aux préconisation du chapitre 4 du présent document *(par exemple, pour les salle serveurs et les locaux de stockage de produit chimique ou de matières dangereuses)*.

Les caméras seront enregistrées qu'en cas d'évènements ou incident anormaux (effraction d'une porte sous contrôle d'accès, porte ouverte trop longtemps, présentation d'un badge déclaré volé, alarme intrusion, etc.)

5.3.4 SCHEMA DE PRINCIPE



LEGENDE	
LB Lecteur de badges	Détecteur volumétrique
Caméra	Détecteur d'ouverture

5.4 ZONES ET AXES SENSIBLES EXTERIEURS

5.4.1 CONTRÔLE D'ACCES

En fonction du niveau de risque de chaque zone (à étudier au cas par cas), un contrôle d'accès par lecteurs de badges en entrée et libre en sortie par boucle magnétique au sol (ou lecteurs de badges en sortie) pourra être mis en œuvre pendant les heures ouvréers et non ouvrées (nuit, week-end et vacances scolaires).

Seul le personnel autorisé aura accès durant ces périodes.

La mise en œuvre de ces équipements de contrôle d'accès devra être réalisée conformément aux préconisation du chapitre 2 du présent document.

5.4.2 DETECTION D'INTRUSION

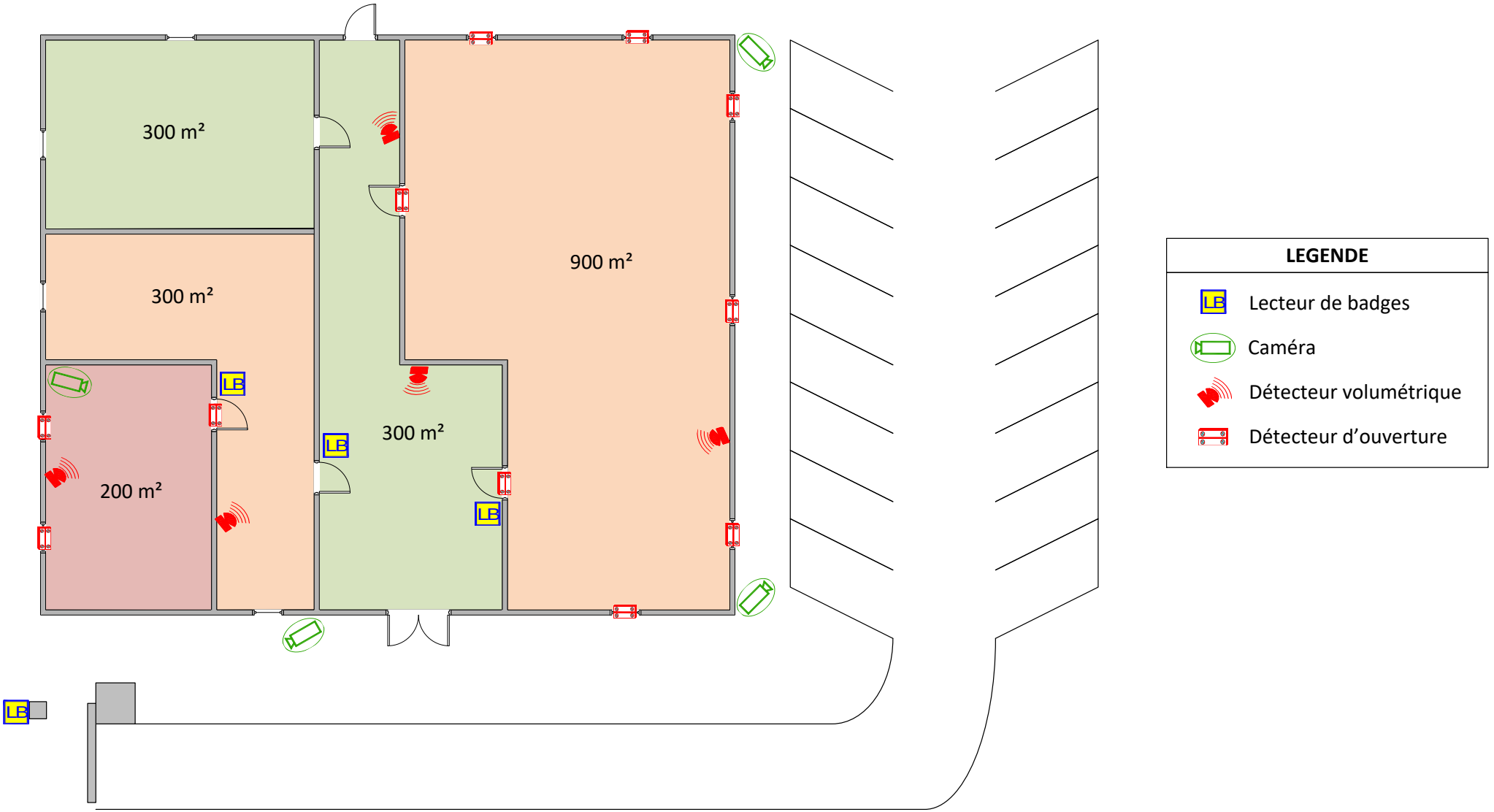
Aucun système de détection d'intrusion ne sera mise en œuvre dans les zones et axes sensibles extérieures.

5.4.3 VIDEOSURVEILLANCE

En fonction du niveau de risque de chaque zone (à étudier au cas par cas), une surveillance vidéo pourra être assurée, conformément aux préconisation du chapitre 4 du présent document.

Les caméras seront enregistrées en permanence, 24h/24, 7j/7.

5.4.4 SCHEMA DE PRINCIPE



5.5 ZONES A REGIME RESTRICTIF (ZRR)

Les zones à régime restrictif (ZRR) représentent un ensemble contigu de pièces/salles d'expérimentations clos, c'est-à-dire que toute personne souhaitant pénétrer à l'intérieur d'une ZRR doit franchir une barrière physique (porte) sur laquelle est apposée une signalétique spécifique (50 x 40 cm) :

ZONE A REGIME RESTRICTIF

INTERDICTION DE PENETRER SANS AUTORISATION

TOUT CONTREVENANT S'EXPOSE AUX PEINES PREVUES PAR L'ARTICLE 413-7 DU CODE PENAL

Toutefois, il n'y a aucune contrainte technique (porte sécurisée, badge d'accès, etc.) imposée pour les ZRR.

5.6 DIVERS

5.6.1 FILM DE SECURITE ANTI-EFFRACTION

Les façades vitrées (portes, fenêtres, cloisons) situées au rez-de-chaussée ou rez-de-jardin des bâtiments de l'Université de Nantes et facilement accessibles peuvent être protégées par des films de sécurité retardateurs d'intrusion.

Le film de sécurité anti-effraction, en polyester transparent, maintient en place les vitrages en cas de vandalisme ou de tentative d'effraction. Les fragments de verre restants solidaires du film.

Il est toutefois souhaitable d'associer à ces films de protection une caméra de vidéosurveillance.

Sans elle, l'intrus peut avoir suffisamment de temps pour neutraliser le film protecteur alors qu'avec une caméra visualisée en temps réel, la tentative d'effraction est d'une part retardée (film de protection) mais détectée.

5.6.2 BARREAUDAGE

La pose de barreaux sur les façades des locaux sensibles assure une protection mécanique efficace.

Si le barreaudage est suffisamment bien dimensionné, le temps nécessaire à l'effraction devient suffisamment long pour être dissuasif.

Le barreaudage sera constitué de barreaux en tube rond de diamètre 25 mm.

Chaque barreau sera soigneusement soudé en continu. L'espacement entre barreaux n'excèdera pas 110 mm selon la norme française NF P 01.012.

Le barreaudage sera traite anticorrosion de haute qualité.

5.6.3 TELESURVEILLANCE

Si un bâtiment ou site ne peut pas être surveillé et supervisé par un poste de sécurité (via l'intermédiaire d'un logiciel), il sera alors nécessaire de mettre en œuvre une télésurveillance.

Le référentiel APSAD R31 encadre les activités de télésurveillance : certification des stations de télésurveillance (type P2 ou P3).

Le référentiel ne traite pas de l'intervention, mais celle-ci doit être prise en considération lors de la souscription d'un contrat de télésurveillance.

On pourra se référer à la norme NFX 50777 relative aux services de surveillance par agents en poste, par agents itinérants, et d'intervention sur alarme.

En complément des règles de prescriptions de télésurveillance (référentiel APSAD R31) à suivre, les informations transmises à la station de télésurveillance seront les suivantes :

- Contrôle d'accès,
- Détection d'intrusion,
- Vidéosurveillance,
- Absence de tension 220v,
- Tests cycliques,
- Vandalisme, sabotage,
- Défaut transmission Protecline,
- Alarmes techniques de synthèse,
- Alarmes détection incendie de synthèse.

Enfin, le système de télésurveillance permettra la transmission d'images vidéos transmises sous IP en sortie des matrices de commutation du système de vidéosurveillance.

Ces images sont restituées sur les moniteurs vidéos de la station vidéosurveillance (interrogation à distance).

5.6.4 VIDEOPORTIER

Certains accès, de par leur implantation, leur éloignement, leur importance ou leur sensibilité, doivent être en liaison permanente avec l'accueil ou avec le personnel de sécurité.

Les vidéos portiers seront posés sur les mêmes potelets que les lecteurs de badges, en entrée et en sortie des parkings.

Ils pourront être également installés au niveau des entrées principales des bâtiments.

En cas de problème (oubli de badge, badge défectueux, entrée ou sortie d'un visiteur), l'agent de sûreté ou l'hôtesse aura à sa disposition le vidéoportier qui lui permettra de communiquer et de voir son interlocuteur.

Les vidéoportiers seront anti-vandalismes. Ils comprendront un bouton d'appel et un haut-parleur intégré ainsi qu'une caméra forma 1/3 avec dispositif autorisant le déplacement de l'objectif.

La caméra incorporera un contrôle électronique de la luminosité ainsi qu'une capacité infra rouge.

5.6.5 ARMOIRE A CLES

Pour un meilleur contrôle des clés, des armoires de gestion de clés seront installées dans un local sécurisé.

L'accès à ces armoires sera restreint.

La personne demandant une clé sera clairement identifiée et une alarme pourra être programmée pour repérer le dépassement de l'heure à laquelle la clé devait être rendue.

5.6.6 ARMOIRE ET COFFRE FORT

Toute amoire et coffre fort devra être positionné dans une pièce contrôlée par lecteur de badges et devra être scellé.

5.6.7 CÂBLE ANTIVOL POUR EQUIPEMENT INFORMATIQUE

Dans les salles informatiques en libre accès, l'ensemble des équipements informatiques (ordinateur, écran, imprimante, etc.) devront être équipé d'un câble antivol.

5.6.8 PEDALE ANTI-AGRESSION

Afin d'assurer une protection du personnel, en particulier la nuit, des pédales anti-agression peuvent être posées aux accueils et dans les locaux présentant des risques d'agression.

Ces pédales devront alerter les collègues se trouvant à proximité ou d'autres personnes habilitées à intervenir.

5.6.9 CONTRÔLE MECANIQUE ET PHYSIQUE D'ACCES AU SITE

Des obstacles physiques seront associés au contrôle d'accès des véhicules qui sera mis en place (lecteur de badges en entrée pour tout type de parking, boucle au sol en sortie des parkings extérieurs et bouton poussoir en sortie des parkings intérieurs).

Les matériels et équipements, adaptés à l'Université de Nantes, qui pourront assurer ces fonctions sont les suivants :

5.6.9.1 BARRIERE LEVANTE

Les barrières levantes doivent être robustes, rapides et légères (2.5 secondes maximum pour une lisse de 3 m).

Le moteur électrique doit supporter un fonctionnement intensif.

Un dispositif de sécurité y sera intégré.

Les barrières levantes seront télécommandées depuis la banque d'accueil et / ou depuis le poste de sécurité.

Les barrières situées aux entrées véhicules comprendront un lecteur de badges de proximité et un vidéoportier relié à l'accueil et / ou au poste de sécurité (si nécessaire).

5.6.9.2 BORNE RETRACTABLE

Si certains accès véhicules, en particulier les barrières levantes, sont la cible de détériorations et de vandalisme, des bornes rétractables pourront être posées en lieu et place de ces barrières.

Les bornes rétractables offrent l'avantage d'être beaucoup plus résistantes que des barrières levantes et sont moins facilement détruites.

L'inconvénient est le temps d'ouverture et de fermeture plus important que les barrières (un temps d'ouverture de 5 à 10 secondes pour les bornes contre 2 à 5 secondes pour les barrières).

D'autre part, lorsque la borne est baissée, il est difficile de savoir à quel moment celle-ci remonte (risque de détérioration du véhicule en cas de passage en force) si un feu de signalisation n'est pas associé.

5.6.9.3 PORTAIL PIETON

En cas de nécessité (manifestation, plan vigipirate, etc.), et comme les accès véhicules, les accès piétons devront pouvoir être fermés rapidement et de façon sûre.

Les portails piétons doivent donc être motorisés et commandés à distance depuis l'accueil et / ou le poste de sécurité.

Ces accès seront placés sous la surveillance de caméras (si nécessaire).

5.6.10 ALARME "ATTENTAT – INTRUSION"

L'alarme a pour objectif de prévenir, lors d'un attentat ou d'une attaque armée, tous les personnels et les étudiants présents dans l'établissement ou le campus.

L'alarme sera déclenchée en présence d'un danger afin que les personnes s'en protègent ; elle doit susciter, de la part de tous les étudiants et les personnels présents dans l'établissement ou sur le campus, une réaction adaptée à la situation (attentat ou attaque armée mais aussi incendie, risques majeurs).

L'alerte permet d'avertir de l'existence d'un danger de telle sorte que les personnes concernées puissent prendre des dispositions particulières :

- Constat de l'irruption d'un individu armé dans l'établissement ou dans le campus ➔ déclenchement de l'alarme pour que les personnels et les étudiants se mettent en sécurité en s'échappant ou en s'enfermant, puis alerte des forces de sécurité (17 ou 112) et la Présidence de l'Université (numéro d'urgence),
- Alerte de la part du rectorat, de la DSDEN, de la police ou de la gendarmerie, d'un danger qui menace l'établissement ou le campus ➔ déclenchement de l'alarme pour que les étudiants et les personnels adoptent la posture qui a été demandée (confinement ou évacuation de l'établissement ou du campus).

Le système d'alarme conditionne la réaction des personnels et des étudiants au sein de l'établissement ou du campus.

Ainsi, s'agissant d'un attentat ou d'une attaque armée, il faut qu'il soit différent de l'alarme incendie car la réaction attendue n'est pas la même (s'échapper, s'enfermer, alerter, faciliter l'intervention des forces de sécurité et de secours).

Il n'y a pas de dispositif technique particulier et obligatoire défini au plan national pour l'alarme « attentat-intrusion ».

Il convient donc l'Université de Nantes de choisir le dispositif d'alarme « attentat-intrusion » le plus adapté à la configuration de l'établissement ou du campus (site étendu ou pas, un ou plusieurs bâtiments, équipement déjà existant, etc.) et au public d'étudiants concerné :

- Dispositif permettant de moduler la sonnerie de début et de fin des cours,
- Corne de brume,
- Sirène,
- Sifflet disponible dans chaque classe de cours, notamment au sein des petites ou moyennes structures,
- Dispositifs de boîtiers (alarme sonore, messages pré-enregistrés, déclencheur manuel) déployés dans les locaux via le câble du réseau informatique,
- Dispositif informatique spécifique déployé sur les ordinateurs de chaque classe,

- Idéalement, Dispositif de haut-parleurs pouvant diffuser des messages préprogrammés (une solution Campus et non bâtimentaire sera préconisée afin d'alerter en même temps l'ensemble des bâtiments d'une zone determinée),
- Utilisation de mégaphones,
- « Bipeurs » qui font office d'alarme et avertissent la police municipale par SMS.

L'alarme doit être audible sur l'ensemble du site.

Le dispositif d'alarme doit être prioritairement sonore (sonneries, sirènes, haut-parleurs, mégaphones, sifflets, etc.), ce qui n'exclut pas la mise en place de systèmes complémentaires d'alerte tels que l'ENT de l'établissement, les dispositifs lumineux, les panneaux à affichage variable, l'utilisation de SMS ou encore l'ouverture d'une fenêtre sur l'écran de l'ordinateur.

L'alarme peut être déclenchée à partir de plusieurs endroits, ce qui permet à chacun d'intervenir une fois l'acte constaté.

À défaut, tous les personnels connaissent la procédure définie pour faire remonter l'alerte et permettre de déclencher l'alarme centralisée.

6. SPECIFICATIONS TECHNIQUES

6.1 CONTRÔLE D'ACCES

Le système de contrôle d'accès permettra d'assurer le filtrage et la traçabilité des mouvements, des usagers détenteurs d'un badge, en fonction des droits géographiques et temporels qui leur seront attribués et autorisés par l'administrateur du système.

6.1.1 PRINCIPE DE FOCNTIONNEMENT

Le système de contrôle d'accès à mettre en œuvre sera de type système de sécurité intégré à intelligence distribuée.

L'installation sera constituée :

- De lecteurs de badges de type carte à puce sans contact Mifare® DESFire EV1,
- D'équipements de portes (serrures, boutons poussoir de sortie, déclencheurs manuel vert, détecteurs d'ouverture, etc.),
- D'unités de traitement locales sur réseau IP (UTL),
- De cartes interfaces lecteurs sur bus RS485,
- D'un poste serveur,
- D'un poste d'administration,
- D'un poste d'exploitation et de supervision du système intégré.

Le futur système à mettre en place devra :

- Protéger l'accès aux données du badge Mifare® (lecture sectorielle) par l'utilisation des clefs de sécurité et du cryptage des communications,
- Permettre de faire évoluer, sans modification technique ultérieure, le système de contrôle d'accès, objet de la présente consultation, pour bénéficier des autres apports de la technologie Mifare® et IP (multi applications, multi sites, etc.),
- Garantir une réserve de 25% en terme d'extension future possible ; cette réserve s'exprimera en terme :
    - De nombre d'unités de traitement locales par système intégré de contrôle d'accès,
    - De nombre de lecteurs par unité de traitement locale,
    - De nombre d'interface lecteurs par bus de terrain.

6.1.2 MATERIELS

6.1.2.1 BADGE (CARTE CMS)

L'université de Nantes met à disposition de chaque personnel une carte professionnelle (cartes CMS) nominative et individuelle.

Les cartes CMS mises à disposition par l'Université se présentent sous la forme de badges au format carte de crédit pourvus de la technologie de puce sans contact Mifare® DESFire EV1.

Les cartes CMS ne peuvent être créées et éditées que via l'application UniCampus de l'UN.

Chaque carte CMS est pourvu d'un N° de carte unique "UID Number" associé à la puce sans contact.

Aucune application tierce n'est autorisée à écrire dans la mémoire embarquée des puces et aucune information complémentaire ne peut être imprimée/collée sur les cartes.

Les informations liées à la délivrance de chaque carte (N° de carte, validité, ...) et son association à un utilisateur sont relayées automatiquement et stockées dans l'annuaire LDAP de l'Université.

Les informations sont alors disponibles pour la mise en œuvre d'applications tierces (exemple : contrôle d'accès, services d'impression, etc.) via la mise en place d'un connecteur spécifique avec l'annuaire LDAP.

Les informations (ex UID User, Prenom, Nom, N° de carte, etc.) peuvent aussi être exportées de façon automatisée depuis l'annuaire LDAP vers les applications tierces via la mise en œuvre de scripts.

Pour des besoins temporaires, l'Université de Nantes fournit des badges (technologie similaire Mifare® DESFire EV1) à des prestataires ou personnes externes à l'Université ne figurant pas dans l'annuaire LDAP.

La solution de contrôle d'accès proposée devra réutiliser les cartes professionnelles de l'Université de Nantes et respecter les pré-requis du contexte ci-dessus exposé.

6.1.2.2 LECTEUR DE BADGES (CARTE CMS)

Les lecteurs de badges à mettre en place seront compatibles avec les badges de type Mifare® DESFire EV1.

Les lecteurs de badges devront assurer le décodage des badges jusqu'à 5 cm.

Une signalisation visuelle et sonore par LED multicolore et buzzer devra indiquer les états suivants :

- Attente,

- Accès autorisé,
- Accès refusé.

Les têtes de lectures intérieures seront fixées sur les cloisons (cloisons légères ou maçonnerie) ; les câbles seront passés en encastré sous fourreaux ou en apparent sous moulures et goulottes.

Les lecteurs seront conçus pour un usage intérieur et extérieur. Ils pourront être montés directement sur une surface métallique, sans altération des performances de lecture au moyen d'entretoise.

6.1.2.3 CYLINDRE ELECTRONIQUE

Afin de sécuriser l'accès des bureaux et locaux sensibles, il pourra être proposé la mise en œuvre de cylindres électroniques pouvant lire les badges de proximité.

6.1.2.4 EQUIPEMENTS DE PORTE

Les portes contrôlées à simple action, à deux vantaux seront toujours équipées que d'un seul dispositif de verrouillage installé sur l'ouvrant de service.

Le vantail semi-fixe sera bloqué par une crémone pompier existante ou dont l'adjonction sera à la charge de l'entreprise en cas de nécessité.

Trois types d'équipements de porte sont préconisés :

- Verrous électriques (de préférence pour les portes issues de secours),
- Ventouse / bandeau ventouse (de préférence pour les portes intérieures à fort passage),
- Serrure électrique à mortaiser (de préférence pour les portes intérieures à faible passage, pour les portes donnant sur l'extérieur ou pour les portes issues de secours).

Verrou électrique :

Les portes assujetties à un contrôle d'accès pourront être équipées de verrous électromécaniques 1 point pour montage en applique en imposte.

Le verrou devra pouvoir fonctionner de façon intensive en contrôle d'accès (au-delà de 1500 passages/jour).

L'utilisation de ces verrous ne devra diminuer en aucun cas la hauteur de passage libre.

Ce dispositif pourra être posé en applique horizontalement en imposte pour les portes à 1 ou 2 vantaux, sans entrave sur le passage donc préservant sa hauteur réglementaire de 2,04 m (Norme NFP 01-005).

L'entreprise assurera le raccordement des verrous de manière à gérer l'état de verrouillage des portes (sortie relais pêne sorti) au même titre que l'état de fermeture du vantail (contact magnétique déporté NF).

Ces informations seront dissociées sur deux entrées différentes et devront être toutes deux valides pour que la porte soit considérée en sécurité.

Le choix du modèle se fera en fonction du type de porte considéré et du mode de pose.

Ventouse / bandeau ventouse :

Certaines portes assujetties à un contrôle d'accès pourront être équipées de bandeaux ventouses et/ou ventouses.

Le bandeau ventouse et/ou ventouse devra pouvoir fonctionner de façon intensive en contrôle d'accès (au-delà de 1500 passages/jour).

L'utilisation de ces bandeaux ventouses et/ou ventouses ne devra diminuer en aucun cas la hauteur de passage libre.

Ces dispositifs pourront être posés en applique horizontalement en imposte pour les portes à 1 ou 2 vantaux, sans entrave sur le passage donc préservant sa hauteur réglementaire de 2,04 m (Norme NFP 01-005).

L'entreprise assurera le raccordement des bandeaux ventouses et/ou ventouses de manière à gérer l'état de verrouillage des portes.

Les bandeaux ventouses et/ou ventouses seront en aluminium.

Le choix du modèle se fera en fonction du type de porte considéré et du mode de pose.

Serrure électrique à mortaiser :

Ces serrures électriques pourront être utilisées chaque fois qu'il sera possible d'encastrer une serrure.

Elles permettront de conserver les canons (type européen) existants.

Le choix se portera de préférence sur des modèles à béquilles contrôlées.

Ces serrures devront garantir le bon verrouillage de la porte (1 déclencheur, 2 points de fermeture), et dans le cas d'une configuration entrée contrôlée / sortie libre permettront l'évacuation des personnes en toutes circonstances.

Toutes les sujétions de pose et fournitures diverses (passage des câbles dans les huisseries et au travers des portes, passages de câbles à mortaiser, flexibles apparents, moulures métalliques etc..) sont réputés inclus dans la prestation de pose des systèmes de fermeture.

A cet effet le soumissionnaire indiquera dans son mémoire technique les types de serrure par porte qu'il se propose d'installer.

6.1.2.5 DETECTEUR D'OUVERTURE

Les contacts d'ouverture permettant de gérer l'état de positionnement du vantail de la porte (ouverture trop longue ou porte bloquée par exemple) devront être fournis et installés.

Ils seront de type contact magnétique pour pose en saillie avec câble moulé 4 fils d'une longueur de 2m.

L'aimant de type ferrite permettra une utilisation sur les huisseries métalliques et support ferreux.

En fonction de contrainte esthétique potentielle, certaines portes pourront être dotées le cas échéant de détecteur encastré.

6.1.2.6 BOUTON POUSSOIR DE SORTIE

Les boutons poussoir de demande de sortie libre seront de couleur blanche.

Ils seront posés en applique ou en encastré selon configuration et constitués d'un cadre, d'un support, d'une plaque et d'un poussoir inverseur avec porte étiquette.

6.1.2.7 DECLENCHEUR MANUEL DE DEVERROUILLAGE D'URGENCE

Implanté à une hauteur de 1,30 m, au droit de chaque sortie de porte verrouillée, il sera de type déclencheur manuel, de couleur verte avec membrane déformable, indicateur mécanique d'état et capot de protection plastique transparent plombé.

Il sera muni d'un double contact :

- Le premier assurera la coupure de l'alimentation du système de verrouillage, le deuxième reportera l'information d'action sur le BBG, au poste de gestion de contrôle d'accès,
- Le deuxième contact sera raccordé sur l'électronique déportée de détection intrusion.

6.1.2.8 INTERFACE LECTEURS

Les cartes interfaces lecteurs assureront l'interface entre les équipements de portes et les unités de traitement locales décrites plus loin.

Elles devront permettre la gestion des configurations suivantes :

- Une ou plusieurs portes contrôlées en entrée avec sortie libre,
- Une ou plusieurs portes contrôlées en entrée et sortie,
- Une ou plusieurs portes contrôlées en entrée avec sortie libre.

Ces cartes seront installées en coffret autoprotégé à l'ouverture par micro rupteur à lame NO/NF.

Les coffrets seront installés en zone surveillée à proximité des portes à contrôlées et devront restés facilement accessibles pour la maintenance.

L'entreprise en charge des travaux aura à sa charge l'alimentation 12/24VDC des équipements de porte (serrures, verrous, bandeaux ventouse, ventouses) au départ des interfaces deux lecteurs depuis les racks d'alimentation secourue par batteries.

Elle prévoira également des dispositifs de protection par fusibles sur borniers sectionnables pour l'alimentation des organes de verrouillage.

Enfin, elle dimensionnera les câbles en conséquence pour s'affranchir des phénomènes de pertes en lignes et garantir le seuil de tension d'alimentation minimal de fonctionnement des dispositifs de verrouillage en bout de ligne même en mode de marche sur batteries seules.

6.1.2.9 UNITE DE TRAITEMENT LOCALE

Les unités de traitement locales seront raccordées directement sur le réseau informatique Ethernet.

L'unité de traitement locale devra assurer l'interface entre le poste informatique serveur et les périphériques de terrain.

Les unités de traitement locales disposeront d'une base de données complète des badges avec les droits associés.

Elles pourront fonctionner et prendre des décisions de façon totalement indépendante.

Elles assureront une mémorisation locale de la liste des badges autorisés, des plages horaires et des historiques et une gestion autonome des accès, même en cas de déconnexion du réseau Ethernet.

Elles permettront le fonctionnement des portes en mode dégradé en cas de rupture de communication avec le serveur de contrôle d'accès.

Lors de la reconnexion du réseau, les informations seront restituées automatiquement au serveur.

Les unités de traitement locales devront communiquer avec le serveur mais aussi entre elles pour assurer les interactions, asservissements ou fonctions répartis sur plusieurs unités de traitement locales, leurs dialogues, et les données échangées seront sécurisés par un cryptage de données.

Véritable automate, chaque unité de traitement locale sera entièrement programmable permettant souplesse et adaptation du système aux besoins présents et futurs du client.

Les unités de traitement locales seront constituées d'une interface qui gèrera un bus auquel seront raccordées les cartes interfaces deux lecteurs déportées.

6.1.2.10 COFFRET D'ALIMENTATION

Les dispositifs de verrouillage des accès contrôlés seront alimentés à partir d'alimentation secourues par batteries dédiées implantées dans des locaux techniques.

Le système de sécurité intégré devra traiter les informations reportées par les alimentations (présence secteur, défaut tension basse, et défaut batteries).

Les différents équipements (serrures, verrous, bandeaux ventouse, ventouse) des portes assujetties à du contrôle d'accès seront alimentées à partir de d'alimentation 12/24 VDC 8A.

Trois voyants de signalisation d'états seront présents en face avant.

Ils permettront le report d'alarme sur contacts secs des informations de défaut secteur, défaut chargeur et défaut batteries.

6.1.2.11 POSTE D'EXPLOITATION ET D'ADMINISTRATION

L'Université de Nantes devra fournir un poste informatique pour héberger les applications nécessaires au paramétrage, à l'administration et à l'exploitation du système de contrôle d'accès (commun avec les systèmes de détection d'intrusion et de vidéosurveillance).

Il sera installé, de préférence, dans le service technique et/ou sécurité du bâtiment et/ou site.

6.1.2.12 POSTE DE SUPERVISION

L'Université de Nantes devra fournir un poste informatique pour surveiller et superviser le système de contrôle d'accès (commun avec la surveillance et la supervision du système de détection d'intrusion et de vidéosurveillance).

Il sera installé, de préférence, dans le poste de sécurité du site.

6.1.2.13 SERVEUR

L'Université de Nantes devra fournir un serveur pour héberger et stocker la/les licence(s) logiciel(s) du système de contrôle d'accès (commun avec les systèmes de détection d'intrusion et de vidéosurveillance).

Il sera installé, de préférence, dans une salle informatique de l'Université de Nantes.

6.2 DETECTION D'INTRUSION

Le système de détection intrusion électronique sera destiné à détecter et signaler de manière précoce la pénétration et/ou le déplacement d'un intrus dans le bâtiment et les secteurs sensibles.

6.2.1 PRINCIPE DE FOCNTIONNEMENT

L'installation de détection d'intrusion sera composée :

- De capteurs intrusion : détecteurs d'ouverture, détecteurs volumétriques double technologie infrarouge hyperfréquence, contact de fond de pêne,
- De modules d'entrées et sorties déportés pour l'adressage des capteurs et la commande des actionneurs,
- D'un système de centralisation d'alarme,
- D'un clavier de mise en et hors service.

La centralisation des alarmes sera reliée au système de supervision contrôle d'accès – intrusion – vidéosurveillance pour gestion globale de la sûreté.

6.2.2 MATERIELS

6.2.2.1 DETECTEUR D'OUVERTURE

Les détecteurs d'ouverture seront certifiés et estampillées NF & A2P type 3.

Les contacts d'ouverture permettant de gérer l'état de positionnement des ouvrants devront être fournis et installés.

Ils seront de type contact magnétique pour pose en saillie avec câble moulé 4 fils d'une longueur de 2m minimum.

L'entreprise fera usage de boîte de raccordement en ABS blanc 5 ou 8 bornes à vis auto protégées NFA2P pour le raccordement côté porte.

L'aimant de type ferrite permettra une utilisation sur les huisseries métalliques et support ferreux.

En fonction de contrainte esthétique potentielle, certaines portes pourront être dotées le cas échéant de détecteur encastré.

Sur les portes métalliques pleines, il sera installé des contacts de type grand écartement avec boîtier en aluminium, assurant un écartement jusqu'à 35 mm.

6.2.2.2 DETECTEUR VOLUMETRIQUE

Les détecteurs volumétriques seront certifiés et estampillées NF & A2P type 3.

Les détecteurs seront de type double technologie infrarouge passif et hyperfréquence.

Ils intègreront la fonction signalant automatiquement toute tentative de masquage du capteur.

6.2.2.3 DECLENCHEUR MANUEL DE CONTROLE D'ACCES

Le 2ème contact des déclencheurs manuels verts de déverrouillage d'urgence sera raccordé sur les interfaces d'entrées d'alarme du système de détection d'intrusion et sera géré comme une information d'alarme intrusion.

6.2.2.4 INTERFACE D'ENTREES

Les détecteurs intrusion seront raccordés sur des cartes interface d'entrées de sécurité supervisées, elles-mêmes reliées au système de contrôle d'accès.

Ces interfaces disposeront au minimum de 8 entrées surveillées, avec vérification individuelle de l'état, pour la connexion de détecteurs d'alarme intrusion ou autre (alarmes techniques).

La distance maximale entre un détecteur et une interface d'entrée sera de 200 mètres maximum selon la section de câble.

Ces cartes déportées seront installées en coffret ABS auto protégé à l'ouverture par micro rupteur à lame NO/NF.

Les coffrets seront installés en zone surveillée et devront restés facilement accessibles pour la maintenance

Ils seront raccordés à la centrale intrusion sur IP.

La centrale sera conforme à l'EN 50.131-1 et à la norme NF A2P.

L'entreprise prévoira des dispositifs de protection par fusibles sur borniers sectionnables pour l'alimentation des détecteurs et dimensionnera les câbles en conséquence pour s'affranchir des phénomènes de pertes en lignes et garantir le seuil de tension d'alimentation minimal de fonctionnement des détecteurs en bout de ligne même en mode de marche sur batteries.

6.2.2.5 INTERFACE DE SORTIES

Les dispositifs de signalisation sonores et autres actionneurs seront raccordés sur des cartes interface à sorties relais, elles-mêmes reliées par bus à la centrale de détection d'intrusion.

La distance maximale entre un dispositif à commander et une interface de sorties sera fonction des phénomènes de perte en ligne, et notamment en mode de fonctionnement sur batteries seules.

Ces cartes seront installées en coffret ABS auto protégé à l'ouverture par micro rupteur à lame NO/NF.

Les coffrets seront installés en zone surveillée et devront restés facilement accessibles pour la maintenance.

L'entreprise prévoira des dispositifs de protection par fusibles sur borniers sectionnables pour l'alimentation des actionneurs et dimensionnera les câbles en conséquence pour s'affranchir des phénomènes de pertes en lignes et garantir le seuil de tension d'alimentation minimal de fonctionnement des dispositifs à commander en bout de ligne même en mode de marche sur batteries.

6.2.2.6 CLAVIER DE MISE EN/HORS SERVICE

Ce clavier permettra une exploitation de la détection d'intrusion en mode dégradé en cas de perte de communication entre les postes informatiques et la centralisation intrusion.

Il permettra également de mettre en/hors service la détection d'intrusion partiellement ou totalement dans le bâtiment.

Il sera raccordé à la centrale de détection intrusion.

6.3 VIDEOSURVEILLANCE

Le système de vidéosurveillance sera conçu comme un outil de dissuasion, de levée de doute et d'enregistrement en vue d'une enquête et/ou une recherche ultérieure.

L'enregistrement pourra être effectué, en fonction de plages horaires, en permanence, sur évènements (détection d'activité par analyse numérique de l'image) ou sur alarmes (asservissement au système de contrôle d'accès et de détection intrusion).

Il pourra également être réalisé de manière manuelle simple sur demande opérateur.

6.3.1 PRINCIPE DE FOCNTIONNEMENT

La solution logicielle de sécurité vidéo permettra la gestion des données vidéo numériques sur réseaux IP.

Cette solution sera entièrement extensible. Elle donnera également la possibilité de gérer plus d'une centaine de caméras, ce qui assurera flexibilité et évolutivité.

L'architecture ouverte et distribuée du système permettra le visionnage simultané à partir de plusieurs postes, de même que l'archivage sur des équipements standards.

Le logiciel reposera sur une architecture client-serveur répartie permettant la visualisation, le stockage et la saisie simultanés de services vidéo, audio et de données de qualité supérieure, à haute résolution.

L'installation sera composée de caméras IP, d'un poste serveur pour le stockage des images (fournit par l'Université de Nantes) et de postes de visualisation assurant l'affichage des images au poste de sécurité.

Les modules logiciels nécessaires au paramétrage et à l'exploitation à postériori des enregistrements seront implantés sur un poste d'administration du système intégré de sécurité.

Le système de vidéosurveillance sur IP, commun au système global de sécurité intégré gérant le contrôle d'accès et la détection intrusion, sera capable d'effectuer l'enregistrement et devra permettre la vérification vidéo sur alarmes dans les cas suivants :

- Détection intrusion par détecteurs de mouvements,
- Détection intrusion par détecteurs d'ouverture et fond de pêne,
- Détection de porte ouverte trop longtemps,
- Détection de porte forcée,
- Détection d'action sur déclencheur manuel vert activé,
- Non autorisation d'accès (badge refusé) pour les motifs suivants :
    - Badge bloqué (perdu, volé),
    - Porte non autorisée,
    - Badgeage hors période horaire autorisée,
    - Etc.

L'entreprise, devra rédiger un dossier d'analyse fonctionnelle complet, soumis pour approbation préalable au maître d'ouvrage et au maître d'œuvre, mettant en évidence les scénarios d'asservissement des différentes caméras vidéo avec les équipements terminaux de contrôle d'accès et de détection d'intrusion des zones visualisées.

6.3.2 LOCALISATION DES EQUIPEMENTS

Il appartiendra à l'entreprise de vérifier la cohérence et la pertinence des implantations théoriques par rapports aux objectifs à atteindre, voir de proposer une modification de l'implantation en regards de certaines contraintes techniques ou fonctionnelles.

Afin d'obtenir des performances optimales, l'entreprise prévoira des essais, de jour et de nuit, avec un ensemble caméra / moniteur portable ayant les mêmes caractéristiques réelles que celles définies dans le présent descriptif.

Elle effectuera sur site les tests de validation de positionnement des caméras conjointement avec la maîtrise d'œuvre de manière à répondre au besoin de visualisation du maître d'ouvrage.

En tout état de cause, quelles que soient les conditions d'exploitation, l'image devra être claire, nette et exploitable.

Le cas échéant, l'entreprise devra effectuer à sa charge les travaux de modification ou de renforcement de l'éclairage intérieure ou extérieure si le niveau d'éclairement actuel des zones à observer ne lui paraît pas suffisant.

6.3.3 MASQUAGE DES ZONES DE VIE PRIVEE

Afin de respecter la loi du 21 janvier 1995 et son décret d'application du 17 octobre 1996 modifié par les décrets 2006-929 du 28 juillet 2006 et 2009-86 du 22 janvier 2009 en matière de protection de la vie privée, les caméras intégreront un dispositif de masquage de la partie d'image concernée, sans occulter systématiquement la totalité de l'image visualisée.

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

Les opérateurs ne pourront en aucun cas modifier ou supprimer ce masquage.

Le nombre de fenêtre du masquage sera au minimum de 8 par caméra.

6.3.4 DOSSIER A REALISER

Rédaction par l'entreprise du dossier relatif à la demande d'autorisation préalable d'installation devant être adressé à la préfecture , conformément à la loi 95-73 du 21

janvier 1995 et au décret 96-926 du 17 octobre 1996 modifié par les décrets 2006-929 du 26 juillet 2006 et 2009-86 du 22 janvier 2009.

Ce dossier sera validé par l'Université de Nantes.

6.3.5 MATERIELS

6.3.5.1 CAMERA IP EXTERIEURE

Les caméras extérieures seront de type caméra réseau IP PoE commutable couleur / noir et blanc.

Les caméras extérieures auront la fonction jour /nuit.

Elles disposeront d'un objectif asservi à focale variable permettant d'ajuster la largeur de champs de vision à la zone à visualiser.

Elles seront intégrées dans des caissons équipés d'un pare-soleil réglable, l'ouverture du caisson pour accès à la caméra se fera de manière latérale, afin d'éviter de modifier le positionnement à chaque intervention.

Les caissons seront de type thermostatés ventilés et munis de filtres afin de se prémunir de toute infiltration de poussières et de sable.

Le support du caisson sera de type pied creux intégrant le passage des câbles. Il sera réglable par rotule en site et azimut.

Des spots Infra Rouge et projecteur seront installés en tant que de besoin avec les caméras.

Pour certains cas, des caméras IP extérieures de type motorisé pourront être utilisées.

6.3.5.2 CAMERA IP INTERIEURE

Les caméras intérieures seront de type caméra réseau IP PoE commutable couleur / noir et blanc.

Elles seront de type caméra réseau mini dôme fixe couleur installées au plafond ou au mur.

Les caméras seront dotées d'un boîtier en alliage d'aluminium de conception anti-vandalisme et coque durcie en polycarbonate étanche.

La caméra sera équipée d'un objectif asservi à focale variable permettant d'ajuster la largeur de champs de vision à la zone à visualiser.

Des spots Infra Rouge seront installés en tant que de besoin avec les caméras.

6.3.5.3 POSTE D'EXPLOITATION ET D'ADMINISTRATION

L'Université de Nantes devra fournir un poste informatique pour héberger les applications nécessaires au paramétrage, à l'administration et à l'exploitation du système de vidéosurveillance (commun avec les systèmes de contrôle d'accès et de détection d'intrusion).

Il sera installé, de préférence, dans le service technique et/ou sécurité du bâtiment et/ou site.

6.3.5.4 POSTE DE VISUALISATION

L'Université de Nantes devra fournir un poste informatique pour visualiser le système de vidéosurveillance (commun avec les systèmes de contrôle d'accès et de détection d'intrusion).

Il sera installé, de préférence, dans le poste de sécurité du site pour l'affichage sur deux ou quatre moniteurs informatique TFT 21".

L'entreprise devra intégrer la tablette de supportage et/ou les rotules de fixation murale des écrans de visualisation.

Il sera possible de visualiser jusqu'à 16 caméras par écrans avec un maximum de 32 flux vidéo de manière simultané sur l'ensemble des deux ou quatre moniteurs configurés en bureau étendu (1 écran maitre et 1 ou 3 écrans esclaves).

6.3.5.5 SERVEUR

L'Université de Nantes devra fournir un serveur pour héberger et stocker la/les licence(s) logiciel(s) du système de vidéosurveillance ainsi que les enregistrements vidéo (commun avec les systèmes de contrôle d'accès et de détection d'intrusion).

Il sera installé, de préférence, dans une salle informatique de l'Université de Nantes.

6.4 LOGICIEL DE SUPERVISION

L'Université de Nantes a retenu une solution de logiciel de supervision unique afin de pouvoir assurer une communication et un interfaçage entre les différents sous-systèmes de sûreté (contrôle d'accès, détection d'intrusion et vidéosurveillance).

De plus, cette solution technique permet de mutualiser les équipements informatiques de supervision (postes informatiques et écrans de visualisation) et de stockage (serveurs).

Le logiciel de supervision du système intégré de contrôle d'accès, détection d'intrusion et vidéosurveillance offrira les fonctionnalités minimums suivantes :

6.4.1 FONCTIONNALITES GENERALES D'EXPLOITATION

Exploitation en mode graphique :

Toutes les informations envoyées par les équipements terminaux des systèmes de contrôle d'accès, de détection d'intrusion et vidéosurveillance au poste d'exploitation et de supervision pourront être visualisées à l'aide de plans graphiques à icônes dynamiques :

- Exploitation en mode graphique rafraîchie en temps réel (synoptiques) des événements et de l'état de l'installation et des organes (accès ouvert, en alarme, en défaut, en ou hors service, perte de signal, etc.),
- Assistance graphique par affichage des plans à raison d'un plan par étage avec possibilités de zoom sur toutes les zones du plan, avec les équipements et leur état :
  - Animation graphique et commande des lecteurs, précisant l'état de l'équipement : portes contrôlée, porte en mode verrouillé, porte en mode libre accès,
  - Animation graphique et commande des capteurs intrusion et des zones d'intrusion : capteur en service, en alarme, à l'arrêt, en défaut, éjecté, zone en ou hors service,
  - Affichage automatique du plan sur lequel un capteur passe en alarme.
- Identification des ensembles fonctionnels par infos- bulle ou par menu contextuel et pointage sur les symboles des vues graphiques.

Les modules logiciels de gestion d'alarmes et de plans graphiques pourront fonctionner simultanément dans des fenêtres séparées réparties sur le bureau étendu grâce aux deux écrans informatiques, de sorte que l'utilisateur disposera aussi bien de textes d'alarme que de plans graphiques sur son poste de travail.

Le logiciel offrira un outil spécifique pour la création de plans graphiques. Cet outil sera en mesure d'importer des plans existants au format DXF.

Tous les icônes ou symboles devront être entièrement définissables par l'utilisateur.

A partir d'un plan graphique, il sera possible d'envoyer manuellement des commandes à des équipements déportés. Celles-ci seront utilisées, par exemple, pour masquer ou démasquer des détecteurs, activer la détection d'intrusion ou l'éclairage, ouvrir les portes, etc.

Pour exécuter une commande, il suffira de cliquer sur le symbole et la liste de commandes correspondantes apparaîtra dans une fenêtre séparée. S'il n'y a qu'une

seule commande qui corresponde au symbole, elle sera exécutée immédiatement lorsque l'utilisateur aura cliqué sur le symbole.

Paramétrage du système :

- Accès par code personnalisé,
- Paramétrage du micro-ordinateur et de ses périphériques,
- Paramétrages des équipements de contrôle d'accès,
- Paramétrages des badges,
- Paramétrages des capteurs intrusion,
- Paramétrage d'automatismes pour réaliser des asservissements entre des évènements et des commandes (ex : porte ouverte trop longtemps => enregistrement vidéo).

Gestion des systèmes :

- Commandes des équipements (mise en/hors service, télécommandes, inhibition, prise en compte) protégées par mot de passe,
- Activation/désactivation des modes de fonctionnement préalablement définis sur les sous-systèmes,
- Consultation de la base de données du système contrôle accès et intrusion,
- Supervision temps réel de l'état opérationnel des organes de la supervision et des sous/systèmes supervisés,
- Gestion d'import ou export de fichiers dans les formats usuels et suivant des protocoles de communication standard (WORD et EXCEL minimum).

Gestion des évènements :

Toute information sur le changement d'état des entrées sera signalée en temps réel à une ou plusieurs stations de travail. Chaque état sera signalé individuellement pour chaque entrée, de sorte qu'il sera possible de prévoir des actions spécifiques pour chaque état de chaque entrée.

Tous les messages apparaitront automatiquement dans le logiciel de gestion d'alarmes. Ce logiciel affichera l'adresse du module, le numéro du message et la date et l'heure de la détection.

En plus, l'utilisateur pourra définir des textes d'alarme dans l'éditeur de texte intégré.

Ces textes d'alarme apparaitront également automatiquement à la réception d'un message.

Lorsque plusieurs messages d'alarme arriveront simultanément, ils seront mis en attente jusqu'à ce qu'un opérateur les acquitte. Avant d'acquitter un message d'alarme, l'opérateur pourra introduire ses propres commentaires dans un journal de type main

courante. Ceux-ci seront enregistrés dans l'historique d'événements lors de l'acquittement et pourront consultés ultérieurement dans le journal.

Il sera possible de consulter l'historique d'alarmes complet dans le logiciel d'historique d'événements, qui contient plusieurs fonctionnalités comme des filtres pour faciliter la recherche d'événements.

Des commandes automatiques seront exécutées lors de la réception et de l'acquittement des messages d'alarme.

Ces commandes sont entièrement programmables par l'utilisateur pour chaque message d'alarme :

- Filtrage des événements et des vues graphiques paramétrables par profil utilisateur,
- Monitoring temps réel des événements et états de l'installation,
- Journal d'alarme textuel avec chronologie et code couleur différencié par niveau de priorité, horodatage, état et identification de l'alarme,
- Signalisation des alarmes par un bip sonore ou par message vocal asservi à l'acquittement,
- Fonctions d'impression multiples :
    - Evènements au fil de l'eau : le fil de l'eau précise les alarmes survenues associées à l'heure de l'alarme, la zone et le contact,
    - Edition de journaux (recherches sur historiques),
    - Copie d'écran,
    - Edition d'étiquettes format badges.

<u>Gestion des opérateurs</u> :

L'accès à n'importe quel module du logiciel intégré de sécurité ne s'obtiendra qu'avec le nom d'utilisateur et le mot de passe valable.

Pour chaque opérateur individuel, il sera possible de définir les droits d'accès dans le logiciel.

Pour chaque module du logiciel, il est également possible de définir si un opérateur peut utiliser ce module, s'il peut le fermer, quelles données il peut consulter, quelles données il peut modifier, etc.

Au moment de l'ouverture d'une session, l'utilisateur sera identifié par son nom et son mot de passe. A partir de ce moment, l'utilisateur obtiendra l'accès aux applications autorisées, tenant compte des programmations préférentielles personnelles (langue etc.) de cet utilisateur.

L'interaction avec le système sera conviviale et dans la langue de l'utilisateur.

L'attribution d'un niveau de sécurité particulier à un utilisateur lui permettra l'utilisation des commandes qui appartiennent à ce niveau, ou à un niveau inférieur.

Il sera possible de réattribuer des niveaux de sécurité à des utilisateurs pendant que le système est en ligne.

Un rapport d'historique avec l'heure et la date de toutes les commandes introduites et de chaque ouverture et fermeture de session des utilisateurs pourra être imprimé et archivé sur le disque.

Il sera possible de restreindre l'accès de l'utilisateur en fonction de certains groupes de points, liés à des types ou emplacements spécifiques.

6.4.2 FONCTIONNALITES LIEES AU CONTRÔLE D'ACCES

Le système permettra au minimum :

- L'attribution des critères d'accès par :
  - Zones (lieux physiques) : autant que de lecteurs,
  - Plages horaires définies zone par zone,
- De d'appuyer obligatoirement sur les badges multi-applications (cartes professionnelles CMS) de l'Université de Nantes,
- De reposer sur la relation avec l'annuaire LDAP de l'Université de Nantes pour l'administration des données et des droits d'accès des badges,
- La gestion anti pass-back en cas de besoin, gestion de sas,
- Gestion anti intrusion : définition de l'alarme par son libellé, son niveau de criticité et affectation de consignes associées,
- Gestion des badges par numéro et attribution de multiples champs associés à chaque badge,
- L'invalidation immédiate de badge,
- La gestion des badges permanents, temporaires, visiteurs,
- La gestions des absences et présence sur site,
- La gestion des badges perdus ou invalidés,
- La possibilité d'activer un affichage permanent pour un badge recherché,
- La possibilité de lire et d'accéder aux informations liées à un badge,
- La possibilité de mettre sous surveillance un badge,
- La gestion des passages :
  - Comptage sur une zone, sur un accès,
  - Porte ouverte trop longtemps,

- Porte forcée,
- Contrôle du temps entre deux passages du même badge,
- Edition de tous les passages,
- Impression sur fil de l'eau d'alarme ou anomalie programmable en niveau d'alarme ou sur plage horaire,
- Inhibition manuelle ou sur plage horaire d'évènements sur un passage,

✦ La commande d'ouverture ou de verrouillage permanent.

6.4.3 FONCTIONNALITES LIEES A LA DETECTION D'INTRUSION

Le système permettra au minimum :

✦ La supervision et gestion de fonctionnement de tous les capteurs intrusion et en, général de tout équipement délivrant une information binaire,

✦ La commande de mise en et hors service des capteurs de zones d'alarmes individuellement, immédiatement ou retardée,

✦ Mise en / hors service automatiquement sur plages horaires programmables et manuellement par commande direct : un tableau de mise en service permet la mise en et hors service, zone par zone, par simple clic de la souris sur le bouton mise en ou le bouton mise hors service,

✦ L'éjection par commande directe (clic sur la souris) d'un capteur intrusion en alarme par commande directe avec conservation de l'autoprotection,

✦ L'acquittement d'une alarme par clic de la souris sur un bouton présent en permanence. Après acquittement, une fenêtre présente la consigne associée à l'alarme et autorise l'édition d'un rapport,

✦ La remontée et le traitement des alarmes (élémentaires et synthèse) et routage selon profil,

✦ La supervision/visualisation des tentatives de sabotage (autoprotection, court-circuit, coupure, défaut de résistance…) sur les équipements, les boîtiers ou les liaisons (quelque soit leur mode opérationnel),

✦ Le niveau de priorité des alarmes.

6.4.4 FONCTIONNALITES LIEES A LA VIDEOSURVEILLANCE

La solution logicielle de vidéosurveillance permettra la gestion des données vidéo numériques sur réseaux IP.

Les équipements de vidéosurveillance seront de type entièrement distribué, autonome dans leur fonctionnement, d'acquisition d'image, de visualisation, d'enregistrement, et d'archivage.

Ils bénéficieront de l'infrastructure du réseau dédié à la sûreté pour l'ensemble de ces tâches et utiliseront les capacités de celui-ci pour assurer les fonctions de redondance de sauvegarde dans le cas d'une panne d'un équipement local d'enregistrement.

Les applications fonctionneront sous une logique Clients/Serveur afin de permettre une très grande souplesse d'exploitation.

Le réseau de transmission assurera le transport des images, et des données issues des équipements de vidéosurveillance (caméras, archives vidéo, etc.).

6.4.4.1 CARACTERISTIQUES PRINCIPALES

Les fonctions du système de vidéosurveillance seront :

- Architecture IP véritablement répartie de bout en bout pour réduire les coûts de câblage et de maintenance,
- Architecture client-serveur évolutive permettant la visualisation simultanée de source directe ou archivée par plusieurs utilisateurs autorisés,
- Gestion et supervision multi sites à l'échelle de l'Université sur réseau local ou étendu ou par Internet, pour un maximum de souplesse,
- Capacité de décentralisation du monitoring entre un nombre illimité de sites d'archivage et de caméras, sans contrainte géographique,
- Capacité de stockage adaptée sur disques locaux, systèmes de stockage en réseau (NAS) ou les deux,
- Cryptage des données et authentification pour un haut niveau de sécurité sur l'ensemble du réseau.

6.4.4.2 VISUALISATION DES IMAGES

L'application assurera une gestion selon un mode assurant la visualisation de l'ensemble des caméras des sites.

La page écran affichera les images en multi fenêtrage (bureau étendu).

Elle affichera également la liste des alarmes au fil de l'eau :

- Configuration de vues partagées et programmation de temps d'attente,
- Déclenchement manuel d'enregistrements audio et vidéo,
- Reprise instantanée : possibilité de revisionner un événement qui vient de se produire sans interrompre le monitoring sur les sources en direct,
- Visualisation et commande des séquences de caméra,
- Définition possible de préréglages et déplacements de caméras motorisées et de caméras dômes,
- Activation du mode zoom numérique,
- Visualisation des alarmes en temps réel et de l'historique des alarmes (depuis l'ouverture de session).

6.4.4.3 GESTION DES ALARMES

Le système de vidéosurveillance sur IP sera interconnecté au système intégré de contrôle d'accès et de détection d'intrusion pour effectuer l'enregistrement et la vérification vidéo dans le cadre de la levée de doute sur alarmes :

- Porte ouverte trop longtemps,
- Porte forcée,
- Déclencheur manuel vert activé,
- Non autorisation d'accès pour les motifs suivants :
  - Badge bloqué (perdu, volé),
  - Porte non autorisée,
  - Badgeage hors période horaire autorisée,
  - Etc.

La caméra concernée sera affichée automatiquement dans une fenêtre lors de la réception d'un message d'alarme.

Il sera également possible d'installer des symboles des caméras dans les plans graphiques pour la sélection manuelle de caméras.

Lorsque l'utilisateur cliquera sur une caméra d'un plan, la caméra assignée sera immédiatement sélectionnée et son image apparaîtra à l'écran du poste de supervision.

En sus de ces alarmes, l'application devra éditer les alarmes dites d'exploitation telles que :

- Remplissage du disque dur (seuil paramétrable),
- Erreur de login,
- Défauts techniques,
- Pertes de signal vidéo,
- Perte de liaison avec le poste serveur.

Il sera possible, d'éditer, d'archiver, d'imprimer ces listes d'alarmes ainsi que de trier ces alarmes par critères.

L'effacement sera soumis à autorisation.

6.4.4.4 GESTION DES ACTIVITES

Un journal d'état devra permettre la visualisation de toutes les opérations effectuées sur le microordinateur (login, sortie d'application, modification de paramétrage, etc.).

6.4.4.5 GESTION DES ENREGISTREMENTS

Le démarrage des enregistrements sera :

- Manuel sur commande de l'opérateur,
- Automatiquement sur alarme contrôle d'accès – détection d'intrusion.

Dans tous les cas, le démarrage de l'enregistrement sera programmable caméra par caméra, il sera issu d'un flux vidéo différent de celui de la visualisation temps réel et programmable caméra par caméra.

Un journal d'état devra permettre la visualisation de tous les enregistrements effectués. Ce journal affichera l'heure de début et l'heure de fin, la durée de l'enregistrement, la voie enregistrée.

6.4.4.6 GESTION DE RELECTURE

Pour l'exploitation à postériori des enregistrements, l'application vidéo devra disposer des possibilités suivantes :

- Restitution des données vidéo pour toute caméra en fonction de l'heure et du jour,
- Recherche de séquences vidéo à partir d'événements, d'alertes, de notes et de mouvements,
- Recherche de mouvements dans les séquences vidéo sur certaines zones de l'image,
- Lecture en mode image par image ou en mode rapide vers l'avant ou vers l'arrière,
- Agrandissement de l'image avec le zoom numérique,
- Enregistrement d'images sélectionnées au format JPEG ou BMP,
- Possibilité de convertir les fichiers vidéo au format AVI.

La gestion des enregistrements sera, pour l'utilisateur, indépendante de l'architecture du système et de l'endroit où se trouve physiquement l'enregistrement.

7. SECURISATION HUMAINE

L'Université de Nantes doit mettre en place une politique de sûreté pour l'ensemble de ses sites.

Cette politique est basée sur une organisation pyramidale articulée autour des acteurs suivants :

- Un service ou un responsable sûreté central et unique pour l'Université de Nantes,
- Un responsable sûreté par site ou pour un groupe de sites si ceux-ci sont trop petits,
- Des agents de sûreté (membre du personnel ou d'une société sous-traitante) par Poste Central de Sécurité (PCS).

Les fonctions, rôles et attribution de chacun de ces acteurs sont donnés ci-après.

7.1 LE RESPONSABLE SURETE CENTRAL

Le responsable sûreté central et unique de l'Université de Nantes aura pour rôle de :

- Elaborer la politique de sûreté commune à l'ensemble des sites de l'Université de Nantes,
- Elaborer les politiques de sûreté particulières aux différents sites, en fonction de leurs tailles, de leurs sensibilités et des risques identifiés et potentiels,
- Elaborer avec les responsables sûreté des différents sites les procédures à mettre en place,
- Elaborer avec les responsables sûreté des différents sites les livrets ou manuels sûreté / sécurité destinés aux personnels, aux enseignants et aux étudiants et qui recensent l'ensemble des risques, des procédures, des réglementations et des obligations applicables sur les différents sites,
- Vérifier que les recommandations et les obligations de la politique de sûreté sont mises en œuvre et appliquées,
- Elaborer un « reporting » régulier qui assure une remontée constante et fiable de l'ensemble des événements qui surviennent sur les différents sites (vols, agressions, incivilités, dégradations, intrusions, tags, etc.),
- Mettre en place une procédure (main courante au PCS et/ou dans les différents départements, rapport informatique sur intranet mis à disposition de la population la plus large, etc.), sur chacun des sites, qui permet d'avoir une image précise et immédiate de ces événements,
- Analyser ces données et mettre en place, avec les responsables sûreté des sites, les actions correctives adaptées,
- Vérifier, à différents intervalles, les résultats des actions correctives et l'évolution des événements suite à ces actions,

- Alerter les responsables de sûreté des sites des situations critiques (plan vigipirate ou manifestations annoncées) et s'assurer que les procédures correspondantes sont mises en œuvre,
- Mettre à jour régulièrement le Schéma Directeur Sûreté en fonction des évolutions normatives et/ou technologiques,
- Vérifier l'application du Schéma Directeur Sûreté sur l'ensemble des sites lors des travaux de rénovation ou de création,
- Piloter dans sa globalité le contrat de maintenance des installations de sûreté existantes sur l'ensemble des sites.

7.2 LE REFERENT SURETE DE SITE

Le référent sûreté de site aura un double rôle qui est de :

- Mettre en place et assurer le suivi de la politique de sûreté.

  Ce rôle consiste à :

  - Elaborer avec le responsable sûreté central les procédures à mettre en place,
  - Faire appliquer les recommandations et les obligations de la politique de sûreté,
  - S'assurer que le « reporting » de l'ensemble des événements qui surviennent sur le site (vols, agressions, incivilités, dégradations, intrusions, tags, etc.) est bien effectué,
  - Mettre en place la procédure (main courante au PCS et/ou dans les différents départements, rapport informatique sur intranet mis à disposition de la population la plus large, etc.), qui permet d'avoir une image précise et immédiate de ces événements,
  - Analyser ces données et mettre en place, avec le responsable sûreté central, les actions correctives adaptées,
  - Vérifier, à différents intervalles, les résultats des actions correctives et l'évolution des événements suite à ces actions,
- Assurer la gestion des équipes de sûreté et des systèmes installés.

  Ce rôle consiste à :

  - Encadrer les équipes de sûreté (hôtesses, gardiens, vigiles, qu'ils soient personnels de l'Université ou sous-traitant),
  - Gérer les systèmes de contrôle d'accès, de vidéosurveillance, de détection d'intrusion en étant le responsable et en ayant la main sur ces systèmes,
  - Gérer l'attribution des badges et des droits d'accès,
  - Exploiter les images enregistrées des différentes caméras,

    Le visionnage de ces images ne pouvant être réalisé que par un responsable nommément désigné,
  - Piloter et suivre les travaux de rénovation ou de création du système de sûreté,

- Gérer le contrat de maintenance des installations de sûreté existantes.

7.3 L'AGENT DE SÛRETE

L'agent de sûreté aura pour rôle de :

- Répondre aux appels émis par les visiteurs à travers les vidéoportiers sur les accès véhicules et piétons et commander l'ouverture des portails et obstacles physiques motorisés,
- Contrôler les images des caméras par l'intermédiaire du logiciel de supervision,
- Contrôler les évènements contrôle d'accès (porte ouverte trop longtemps, porte forcée, badge refusé, etc.) par l'intermédiaire du logiciel de supervision,
- Contrôler les évènements de détection d'intrusion (détection d'ouverture, détection volumétrique, etc.) par l'intermédiaire du logiciel de supervision,
- Intervenir en cas de problème,
- Assurer des rondes sur le site,
- Assurer les rondes de fermeture et vérifier que personne ne se laisse enfermer dans un bâtiment,
- Ouvrir le matin les bâtiments,
- Vérifier les identités des femmes de ménages et de toutes personnes appartenant à une entreprise extérieure, mais aussi par extension vérifier (ponctuellement ou de façon systématique en fonction des besoins) l'identité de toutes les personnes qui pénètrent sur le site,
- Appliquer de façon stricte les procédures adaptées à chaque situation à laquelle se trouve confronté l'agent de sûreté.

Les agents de sûreté travailleront dans les différents PCS (Poste Central de Sécurité) créés par l'Université de Nantes.

La création d'un PCS implique la disponibilité de 4 agents de sûreté minimum afin de prendre en compte les horaires (24h/24, 7j/7), les congés, les RTT et les maladies éventuelles.

En cas de plan Vigipirate, le nombre d'agents présents devra être augmenté, ce qui implique des équipes de cinq à six personnes.

Il est préconiser de fournir aux agents un équipement de radiocommunication doté d'un système de gestion de ronde et d'un dispositif de protection du travailleur isolé (DATI).

Le contrôle de ronde incorporant la technologie "homme mort", l'alarme sera instantanément donnée en cas de malaise ou d'agression de l'agent.

7.4 POSTE CENTRAL DE SECURITE

Le Poste Central de Sécurité (PCS) sera positionné sur le Campus du Tertre. Il sera armé en permanence de 2 agents de sécurité (H24, 7 jours sur 7, 365 jours /an).

La mise en place ultérieure d'un second PCS (sur le Campus Centre Loire) serait souhaitable afin de couvrir l'ensemble des secteurs de l'université de Nantes.

Le PCS du Campus Tertre sera supervisé par le chargé de sûreté (recrutement en cours). Il aura notemment pour mission de veiller à la bonne prise en compte des consignes et leur bonne application par les agents de sécurité du PCS.

Ce PCS devra être à même de recevoir l'ensemble des flux vidéos de l'Univeristé de Nantes, y compris les sites distants.

Il recevra également les rapports d'alarmes anti intrusion et incendie de l'ensemble des bâtiments de l'Univeristé de Nantes et aura un visuel sur le contrôle d'accès.

Il disposera des droits d'administration de l'ensemble des sites du périmètre du Campus Tertre afin de pouvoir gérer le contrôle d'accès. Pour les autres campus, il n'aura qu'un visuel sur les systèmes de contrôle d'accès afin de pouvoir intervenir pour les sites Nantais ou prévenir le ou les prestataires exterieurs pour les sites distants.

Il disposera d'un logiciel d'hypervision permettant la communication entre les différents systèmes (de marque différente) mis en place sur l'Univeristé de Nantes. Ce logiciel sera installé dans ce PCS et ainsi que sur l'ordinateur du responsable sûreté de l'Univeristé de Nantes qui disposera des droit d'administration du logiciel.

Le prestataire de sécurité du PCS devra relater sur une main courante electronique l'ensemble des élements survenus sur le perimètre de l'Université de Nantes. Un poste maitre sera disponible dans ce PCS afin de visualiser les evènemenbts survenus au fil de l'eau.

Ce PCS sera à même de prévenir l'astreinte sûreté de l'Université de Nantes ainsi que l'agent logé Université en charge du périmètre ou de juger necessaire une intervention.

ARCHITECTURE RÉSEAUX ET COMMUNICATION

SIEGE SOCIAL
Imm. Le Cid 10 rue Giboin
83110 Sanary Sur Mer
T +33 (0)4 94 74 54 80
F +33 (0)4 94 74 35 37
contact@arcbe.com

AGENCE GRAND SUD-OUEST
51 chemin du Port de l'Homme
33360 Latresne
T +33 (0)5 35 31 52 38
F +33 (0)4 94 74 35 37
www.arcbe.com

AGENCE ILE DE FRANCE
6 Rue de Madrid
75008 Paris
T +33 (0)1 40 15 39 20
F +33 (0)1 42 86 82 74
logiciel@arcbe.com

SAS au capital de 130 000 euros – RCS TOULON B 399 558 923 99 – SIRET 399 558 923 00039 – TVA FR 57399558923 – APE 7112B