

TRAVAUX DE SURETE



CAHIER DES CHARGES ET PRESCRIPTIONS TECHNIQUES DE LA SURETE

direction.d2s@u-bordeaux.fr

Sommaire

A. NORMES ET REGLEMENTS APPLICABLES	3
B. CONTROLE D'ACCES ET ANTI-INTRUSION	4
I. ARCHITECTURE MATERIELLE	5
II. ENTITÉS DE NIVEAU 0 - PERIPHERIQUES ENTREES ET SORTIES	6
1. ALIMENTATION ELECTRIQUE DE L'ENTITE 0	6
2. L'ENVIRONNEMENT DE PORTE.....	6
3. PORTE ET VERROUILLAGES	7
III. ENTITES DE NIVEAU 1 – UNITE DE TRAITEMENT LOCAL, MODULES, LECTEURS ...	12
1. ALIMENTATION ELECTRIQUE DE L'ENTITE 1	12
2. LES LECTEURS DE BADGE.....	12
3. LES MODULES.....	13
4. LES UNITES DE TRAITEMENT LOCALE	14
IV. ENTITE DE NIVEAU 2 SERVEUR ET POSTE CLIENT.....	15
1. SERVEUR	15
2. POSTE DE TRAVAIL CLIENT.....	15
V. ARCHITECTURE ANTI-INTRUSION	15
1. MATERIELS	15
VI. ARCHITECTURE CABLAGE DE COMMUNICATION ET RESEAU	16
1. CABLAGES BUS TERRAIN.....	16
2. EQUIPEMENTS ANNEXES AU CABLAGE	16
3. COMMUNICATION ET RESEAUX	16
VII. LOGICIEL DEDIE AU CONTROLE D'ACCES ET A L'ANTI-INTRUSION	17
1. INTRODUCTION.....	17
2. PLAGES HORAIRES / GROUPE DE LECTEURS / PROFILS / DES DROITS D'ACCES .	17
VIII. PROGRAMMATION ET MISE EN SERVICE	17
1. PROGRAMMATION.....	17
2. MISE EN SERVICE.....	18
3. PARAMETRAGE RESEAUX.....	18
IX. SYNOPTIQUE D'EXPLOITATION	19
C. DOSSIER D'EXECUTION ET DOE	20
I. DOSSIER D'EXECUTION	20
II. DOSSIER DOE	20

A. NORMES ET REGLEMENTS APPLICABLES

Les prestations des titulaires devront être conformes aux clauses de l'ensemble des lois, décrets, arrêtés, règlements, normes et tous les textes européens, nationaux ou locaux applicables aux prestations de la présente opération. Outre les prescriptions techniques particulières contenues dans le présent CCTP, les ouvrages et équipements obéiront aux règles de l'art et respecteront impérativement les normes et standards suivants :

Les documents, ci-après, sont applicables dans leur dernière édition, cette liste n'est pas exhaustive.

- **Norme NF C15.100** : installations électriques à basse tension,
- **Norme C18.510** : installations courants faibles et forts,
- **Norme NF C63.410** : ensembles d'appareillages basse tension montés en usine,
- **Norme NF C91.101** : perturbations radioélectriques et systèmes d'antiparasitage, textes officiels concernant le matériel alimenté en réseau de première catégorie et dont le rayonnement direct est faible,
- **Norme NF C91.104.** : perturbations radioélectriques et systèmes d'antiparasitage et textes officiels concernant les appareils servant aux réceptions individuelles ou collectives des émissions et radiodiffusion sonore ou visuelle,
- **Norme NF C92.130** : appareils électroniques et appareils associés à usage domestique ou à usage général analogue, reliés à un réseau de règles de sécurité.
- **Norme NF P25.362** : fermetures pour baies libres et portails, Spécifications techniques, Règles de sécurité,
- **Norme C32.321** : conformité des câbles de distribution basse tension,
- **Norme C32.201** : conformité du conducteur de protection,
- **Norme C32.310** : conformité des câbles basse tension résistant au feu.
- **Conforme** aux recommandations de **l'ANSSI** architecture 1
 - **Décret n° 96-926 du 17 octobre 1996 relatif à la vidéosurveillance pris pour l'application des articles 10 et 10-1 de la loi n° 95-73 du 21 janvier 1995**
 - **Circulaire n° 68234 du 22 octobre 1996 relative à la vidéosurveillance urbaine**
 - **Arrêté du 3 août 2007 portant définition des normes techniques des systèmes de vidéosurveillance**
 - **Décret n°2009-86 du 22 janvier 2009 modifiant le décret n°96-926 du 17 octobre 1996 relatif à la vidéosurveillance**
 - **Décret n° 2012-112 du 27 janvier 2012 modifiant le décret n° 96-926 du 17 octobre 1996 relatif à la vidéo protection**
 - **Textes codifiés applicables aux ouvrages réalisés et à la protection des personnels**
 - **Prescriptions du présent document suivant les règles de l'art**

L'installation de caméras sur les lieux publics ou privés est soumise à la loi informatique et liberté, ainsi qu'au règlement général sur la protection des données (RGPD).

B. CONTROLE D'ACCES ET ANTI-INTRUSION

L'Université de BORDEAUX a mis en œuvre un dispositif de sûreté constitué d'une organisation humaine et de systèmes de sûreté.

Ce document traite des systèmes de sûreté et de leur installation. Ils sont composés d'équipements de contrôle d'accès, de détection d'intrusion, de serveurs informatique et postes clients de supervision.

Les équipements associés, liés à la protection du patrimoine bâti et non bâti hormis ceux présents dans ce document seront abordés au cas par cas dans les programmes fonctionnels et techniques des opérations, ou, au moment de la formulation du besoin dans le cas d'établissement d'un devis.

Les objectifs principaux de la mise en place des systèmes de sûreté du dispositif de sûreté de l'Université de BORDEAUX et ses partenaires sont :

- De contrôler et filtrer le flux de personnes en gérant les accès (contrôle d'accès) **65.000 utilisateurs**
- D'empêcher et/ou détecter la pénétration des personnes indésirables sur le site (détection intrusion-anti-intrusion)

L'Université s'est pourvue d'un ensemble de systèmes d'un même constructeur avec un unique relais informatique de programmation et supervision. Les architectures matérielle et logicielle sont uniformes. L'Université développera son dispositif de sécurité dans cette logique d'uniformité matérielle, logicielle et architecturale.

Dans ce but, ce document définit les règles et prescriptions concernant les équipements et les travaux d'installation des systèmes de sûreté sur les sites de l'université de BORDEAUX et ses partenaires dont les caractéristiques doivent correspondre à une approche cohérente avec la mise en œuvre des équipements et des fonctions du dispositif de sûreté existant.

Les systèmes devront se connecter nativement au serveur MICRO-SESAME de TIL-TECHNOLOGIES présent à l'Université de Bordeaux.

Le fournisseur du système de contrôle d'accès et intrusion devra être le développeur et le concepteur, des parties logicielle et matérielle.

Pour la fiabilité d'approvisionnement des matériels, et dans une démarche environnementale, une préférence sera donnée aux systèmes conçus et fabriqués en France.

Les caractéristiques attendues sont :

- **Compatibilité et ouverture** : Les équipements et matériels proposés pour un système si différent de l'existant seront totalement compatible avec toutes les technologies d'identification (badges, biométrie, etc..) du système existant. Ils permettront également de gérer les alarmes techniques et de superviser des automates et autres équipements techniques en protocole MODBUS RTU ou OPC.
- **Flexibilité** : Les fonctions de sécurité avancée (antiretour, contrôle renforcé, code sous contrainte, etc...) seront préprogrammées, mais le système possédera une capacité de programmation pour permettre la mise en œuvre d'automatismes adaptés à chaque site et à chaque client. Ces automatismes pourront avoir un caractère permanent ou conditionnel (par exemple : gestion de mode crise, etc...).
- **Modularité** : Le système pourra assurer une gestion multi-site et multi-client / multi-entité. Les fonctions de gestion des accès, de gestion de la détection intrusion, d'animation des synoptiques, de gestion des visiteurs, de traçage de courbes, de gestion des rondes, de personnalisation des badges et de communication inter-systèmes, seront assurées par des modules logiciels provenant du même constructeur et donc parfaitement intégrés. Les logiciels de parties tierces ne seront pas admis.

- **Fiabilité** : Le système permettra une gestion intelligente de la maintenance. Notamment, Alarmes sur défaillance (envoi de messages SMS, télémaintenance, etc...). Il proposera des modes, secours, manuel etc... Toutes solutions assurant la continuité de service.
- **Intégration horizontale et verticale** : Des interfaces ou passerelles vers d'autres systèmes (incendie, G.T.B et vidéo protection (GENETEC)) permettront une meilleure intégration des fonctions de sûreté / sécurité. Des passerelles informatiques permettront d'aligner automatiquement la base de données des badges avec celle du service du personnel afin d'éviter les doubles saisies.

I. ARCHITECTURE MATERIELLE

- **Niveau 0** : Capteurs, relais : les détecteurs d'ouverture, volumétrique, bris de vitre, sirène, autres équipements terminaux de type entrée/sorties, serrure, barrière, ventouse, etc...
- **Niveau 1** : Automates de terrain sur réseau Ethernet : UTL, Modules d'extensions et lecteurs
- **Niveau 2** : Système de supervision serveur et postes clients.

Conformité ANSSI :

L'ensemble des matériels (UTL, modules d'extension, lecteurs, etc) et logiciels proposés devront être conformes aux recommandations du guide de l'ANSSI : « SÉCURITÉ DES TECHNOLOGIES SANS-CONTACT POUR LE CONTRÔLE DES ACCÈS PHYSIQUES » (Version du 19/11/2012), selon l'architecture 1 de façon native sans convertisseur.

La solution devra être sécurisée de bout en bout, du badge jusqu'au serveur.

Les principes et fonctionnalités suivants devront être disponibles et réalisés par les équipements et logiciels fournis :

- Cybersécurité certifié ANSSI:
 - Serveur web embarqué sécurisé HTTPS avec Firewall intégré contre les attaques DoS. - Firmware signé et téléchargeable qui inclut les derniers correctifs de vulnérabilités connues (CVE). –
 - Communications IP sécurisées (certificats TLSv1.2) et bus RS485 chiffrés (AES 128 bits). -
- Compatibilité 802.1X (Radius) et SNMPv3 pour une surveillance des états systèmes & alarmes métiers par la DSI
- La solution devra être compatible avec le réseau VLAN, VPN du site,
- La solution devra être compatible avec l'annuaire LDAP du site pour la gestion des opérateurs et de leurs droits,
- Communications réseau IP cryptées TLS AES 256 bits et signées (intégrité et authentification) entre le serveur et les UTL d'une part et les postes clients d'autre part,
- Communications bus RS485 cryptées AES 128 bits et signées,
- Toutes les clés de communication sur IP et RS485 devront être changées périodiquement de manière automatique par le système sans action humaine pour durcir le cryptage contre toute malveillance,
- Le client final aura obligatoirement la maîtrise de sa clé de communication initiale, qui créera automatiquement les clés suivantes périodiquement, par la saisie, sur un poste client lourd, de cette clé (cérémonie des clés),
- Protection des attaques par déni de service (DoS) par le Firewall des automates UTL,
- Paramétrage de la configuration IP des UTL à travers un Web serveur embarqué sécurisé HTTPS, SSH,
- UTL compatible avec serveur radius 802.1X
- Le module de porte communiquera en bus RS485 crypté AES128 bits avec les lecteurs
- Le module de porte devra obligatoirement avoir un composant SAM/HSM certifié ANSSI EAL5+ soudé sur cette carte comme imposé, pour leurs besoins propres, par les sites de haute sécurité (ministère des Armées...)
- Ce composant SAM/HSM sera le coffre-fort qui contiendra les clés de l'applicatif « contrôle d'accès » des badges. Ces clés devront être téléchargées depuis un poste client lourd, jusqu'aux modules SAM/HSM pour faciliter la diffusion des clés et pouvoir éventuellement changer les clés de tous les

modules depuis le système central, comme demandé dans le guide ANSSI,

- Le principe de diversification des clés devra pouvoir être disponible, activable, et devra permettre au client final de choisir sa formule par un padding personnalisable
- Lecture possible sur le même lecteur transparent jusqu'à 4 types de cartes DESFIRE (ex : carte très haute sécurité + carte sécurisée d'une filiale + carte sécurisée d'un site spécifique),
- Les lecteurs seront conformes ANSSI architecture 1, « lecteur transparent SSCPV2 (aucune clé de cryptage stockée dans le lecteur) et IP65, IK10, pour lire des badges DESFIRE,
- Les lecteurs devront aussi exister en version lecteur + clavier pour identifier une personne, pour un contrôle d'accès renforcé, conforme ANSSI architecture 1, pour lire des badges DESFIRE,
- toutes les entrées seront équilibrées pour l'intrusion et le contrôle d'accès pour détecter les éventuels sabotages
- Le firmware des automates sera téléchargeable depuis les postes clients lourds pour permettre la maintenance corrective et évolutive. Ce firmware sera signé pour valider son intégrité et son authentification.

II. ENTITÉS DE NIVEAU 0 - PERIPHERIQUES ENTREES ET SORTIES

1. ALIMENTATION ELECTRIQUE DE L'ENTITE 0

Les alimentations principales et leur secours utilisés pour les entités de niveau 0 leur seront exclusivement dédiée.

L'utilisation d'une source commune et de son secours pour des équipements d'autre niveau que le 0 est totalement proscrite.

Une note de calculs de l'autonomie des équipements sur sources de secours devra être fourni pour l'ensemble des éléments du niveau 0.

Avec pour objectif une autonomie sur secours de **24/48/72h** selon le domaine d'application des éléments (Porte intérieur, Accès extérieur, etc...)

La maitrise d'œuvre définira précisément l'autonomie souhaitée.

Une réserve de 30% d'autonomie est exigée afin d'anticiper d'éventuel extension de périphérique d'entrées/sorties.

2. L'ENVIRONNEMENT DE PORTE

Boutons-poussoirs de sortie extérieurs

Les Boutons-poussoirs de sorties extérieurs auront les caractéristiques suivantes :

- Bouton poussoir PHMR sur plaque carrée de marque IZYX-SYSTEM ou équivalent
- En inox (bouton + façade) - IP65/IK08
- Dimensions de la plaque : 80x80mm
- Montage en encastré dans boîte d'encastrement électriques normalisés
- Montage en applique possible
- Fixation par vis inox anti-vandales.
- Ils seront impérativement à double sécurité (un contact NO et un contact NF)
- Ils devront permettre, aux utilisateurs, de visualiser et d'entendre si la porte est fermée ou bien ouverte.
- Le BP devra être fixé entre 0.9 et 1.3 m par rapport au sol.

De ce fait, ils seront équipés d'un buzzer (volume réglable de 60 à 80 db à 1 m ou OFF) et d'un retro

éclairage au niveau du bouton. (Halo lumineux sphérique bleu/vert à LEDs)

Pour des raisons de sécurité, les contacts du bouton (NO/NF) permettront une double coupure de l'alimentation des ventouses ou des gâches commandés.

Bouton-poussoir de sortie intérieur

Les Boutons-poussoirs de sortie intérieurs auront les caractéristiques suivantes :

- Bouton poussoir PHMR
- En plastique
- Dimensions 87x87mm
- Montage encastré ou applique
- Un Contact inverseur NO/C/NC
- Voyant lumineux (12-24VDC)
- IP20

BBG vert (bris de glace)

Le boîtier de bris de glace vert sera visuel et sonore muni d'un capot de protection (Clés de réarmement et plomb seront fournis à la sûreté) conforme à la norme EN54-11 et la NFS61-936.

Déclencheurs manuels à membrane déformables avec indicateur d'alarme et d'ouverture du capot de protection (visuel et sonore) de marque IZYX-SYSTEM ou équivalent.

Le BBG devra être fixé entre 0.90 m et 1.30 m par rapport au sol fini pour être conforme PHMR.

Il comportera au minima deux contacts :

- Un contact pour la coupure de l'alimentation de la serrure libérant la porte et relié au SSI
- Un contact d'information pour un report vers la supervision du contrôle d'accès.

Détecteur d'ouverture

Chaque ouvrant devra avoir son DO intégré au système de verrouillage (serrure) ou en supplément sur l'accès si non existant pour être relié à une entrée du système de contrôle d'accès qui pourra contrôler, superviser l'état de l'accès et déclencher les alarmes type « effraction porte » et « porte ouverte trop longtemps »

Le câblage du DO devra être du type EQUI3 avec résistances, afin de remonter l'alarme et l'autoprotection sur une seule paire de fils.

Les contacts d'ouverture ajoutés seront de type applique avec gaine métallique pré-moulée certifié NFA2P Type 3. Dans le cas d'une double porte, il devra être installé un contact par ouvrant, l'ensemble étant relié à une boîte de dérivation autoprotégée NFA2P Type 3, il ne sera pas accepté de DO intégré aux menuiseries ni aux ventouses électromagnétiques. (ex : billes de contact, contact intégré sur bornier ventouse)

3. PORTE ET VERROUILLAGES

Sécurité Incendie

La plupart des établissements de l'Université de BORDEAUX étant des ERP (établissement recevant du public) l'asservissement et la libération des accès du dispositif d'évacuation doivent être obligatoire, toute création d'accès sécurisé fera l'objet d'un ajout d'une fonction d'asservissement avec le Système de Sécurité Incendie (SSI) du bâtiment en question.

Ce dernier se fera via l'ajout d'un relais de type Finder certifié NFSSI, en sécurité positive (en cas de

coupure d'alimentation du relais, libération de la tension de maintiens des verrous, câble d'alimentation R2V Classe 2) l'entreprise installatrice se rapprochera du gestionnaire du SSI afin de déterminer la position et la disponibilité sur les satellites du système SSI.

Un deuxième contact de ce relais sera obligatoirement raccordé directement sur une entrée de l'automate ou module afin de remonter l'information d'une libération d'accès sous asservissement incendie sur l'animation des synoptiques.

Verrou de type gâche électrique

Cette solution n'est pas recommandée par l'université, néanmoins elle pourrait être intégrée sur des accès à bas niveaux de sécurité tout en respectant à minima les conditions suivantes :

- Encastrée uniquement
- Fonctionnement à rupture de courant uniquement
- Tension fonctionnement 24VDC
- Conservation cylindre obligatoire
- Dimensions adaptées à la menuiserie

Verrou de type électromagnétique

Cette solution est recommandée par l'université sur des niveaux de sécurité standard tout en respectant à minima les conditions suivantes :

Ventouse électromagnétique sur équerre Z ou L – Sur porte intérieure uniquement

Les portes équipées de ce dispositif devront au minima répondre aux exigences suivantes :

- Conforme NFS 61937 DAS
- Alimentation en 24VDC
- Force de rétention 500kG
- Contact de position NO NC intégré (**ne remplace pas le détecteur d'ouverture Intrusion obligatoire**)
- **Conservation cylindre obligatoire**

Bandeau ventouse électromagnétique toute hauteur

Les portes équipées de ce dispositif devront au minima répondre aux exigences suivantes :

- Conforme NFS 61937 DAS
- Alimentation en 24VDC
- Force de rétention au minima 2x300kG
- **Conservation cylindre obligatoire**
- Hauteur personnalisée pour recouvrir toute hauteur de la porte
- RAL personnalisé à la couleur de la porte

De manière générale, ces systèmes de verrouillage devront être

- Conforme à la réglementation PMR et sortie de secours,
- L'élément de verrouillage devra respecter le PV coupe-feu de la porte, dans le cas d'un montage d'un système de verrouillage sur une porte coupe-feu, il faudra veiller à pouvoir justifier du PV coupe-feu sur cette dernière.

Il faudra prévoir la possibilité de verrouiller la porte avec un cylindre en cas de panne sur la ventouse ou son alimentation et prévoir un déverrouillage de la ventouse à clés (avec remontée d'information sur le système) si le contrôle d'accès est défaillant.

Verrou de type électromécanique

Cette solution est recommandée par l'université sur des « Haut niveau de sécurité » tout en respectant à minima les conditions suivantes :

La serrure devra être adaptée au nombre de passages (motorisés ou non motorisés) et au niveau de sûreté choisi (1 point ou 3 points).

Serrure électrique 1 point a contrôle de béquille extérieure.

Les portes contrôlées seront équipées de serrures électriques à contrôle de béquille à encastrer dans l'ouvrant, composées du coffre de serrure, de la gâche, d'un câble multipaire de 6 mètres avec connecteur rapide, et d'une paire de carrés séparés.

- La sortie pourra ou non s'effectuer par la béquille intérieure
- Entrée par béquille active ou inactive selon l'état électrique (paramétrable émission-rupture)
- Conformes à la norme EN14846, elles disposeront des performances suivantes :
- Résistance à l'effraction d'une valeur supérieure à 1 tonne par pêne
- Alimentation 24V DC
- La serrure devra impérativement être toutes mains (droite/gauche et poussant/tirant) pour que la maintenance ultérieure puisse être effectuée par un seul et unique modèle.
- Verrouillage automatique en 2 points sécurisé par le contre pêne de sécurité et le pêne demi-tour afin d'empêcher les sorties de pêne accidentelles.
- Axe et entraxe, respectivement à 50mm/70mm (menuiseries bois) et 35mm/92mm (menuiseries alu, PVC, métal), selon le standard français (autres refusés).

Les serrures seront raccordées avec le système de Contrôle d'accès (Ordre à temporiser), et **devront** recevoir les commandes et donner les informations suivantes :

- Activation de la béquille intérieure.
- Position de porte/pêne (contre pêne rentré + pêne sorti obligatoire).
- Utilisation du cylindre par clé.
- Boucle anti-sabotage.

La liaison entre huisserie et battant sera faite par flexible invisible.

Les dispositifs seront alimentés directement par les alimentations des lecteurs de contrôle d'accès.

La mise en œuvre des serrures sera adaptée en fonction du support de la porte (bois, métal ou verre).

Il appartient au présent lot de se rapprocher du lot menuiserie intérieure et/ou serrurerie afin de s'assurer que les blocs-portes assurent le degré coupe-feu ou pare-flamme demandé au lot menuiserie intérieure et/ou serrurerie, et pour que les équipements soient mis en place conformément au procès.

Serrure électrique multipoints a contrôle de béquille extérieure

Les portes contrôlées seront équipées de serrures électriques à contrôle de béquille à encastrer dans l'ouvrant, composées du coffre de serrure, de la gâche, d'un câble multipaires de 6 mètres avec connecteur rapide, et d'une paire de carrés séparés.

- La sortie pourra ou non s'effectuer par la béquille intérieure
- Entrée par béquille active ou inactive selon l'état électrique (paramétrable émission-rupture)
- Conformes à la norme EN14846, elles disposeront des performances suivantes :
- Résistance à l'effraction d'une valeur supérieure à 1 tonne par pêne
- Alimentation 24V DC
- La serrure devra impérativement être toutes mains (droite/gauche et poussant/tirant) pour que la maintenance ultérieure puisse être effectuée par un seul et unique modèle.
- Verrouillage automatique en 2 points sécurisé par le contre pêne de sécurité et le pêne demi-tour afin d'empêcher les sorties de pêne accidentelles.
- Axe et entraxe, respectivement à 50mm/70mm (menuiseries bois) et 35mm/92mm (menuiseries alu, PVC, métal), selon le standard français (autres refusés).

Les serrures seront raccordées avec le système de Contrôle d'accès (Ordre à temporiser), et seront aptes à recevoir les commandes ou donner les informations suivantes :

- Activation de la béquille intérieure.
- Position de porte/pêne (contre pêne rentré + pêne sorti).
- Utilisation du cylindre par clé.
- Boucle anti-sabotage.

Les dispositifs seront alimentés directement par les alimentations des lecteurs de contrôle d'accès.

La mise en œuvre des serrures sera adaptée en fonction du support de la porte (bois, métal ou verre).

Il appartient au présent lot de se rapprocher du lot menuiserie intérieure et/ou serrurerie, afin de s'assurer que les blocs-portes assurent le degré coupe-feu ou pare-flamme demandé au lot menuiserie

intérieure et/ou serrurerie, et pour que les équipements soient mis en place conformément au procès-verbal du fabricant de serrures.

Serrure motorisée multipoints très haute sécurité

Afin d'assurer la sécurité des lieux et le bon fonctionnement du système de contrôle d'accès, il sera prévu un système de verrouillage multipoints motorisé [encastré dans] des portes concernées, y compris sur les portes coupe-feu.

Elles disposeront des caractéristiques et performances suivantes :

- Serrure 4 points avec crochets en acier monobloc 9mm
- Résistance à l'effraction d'une valeur supérieure à 1,3 tonne par pêne
- Testées à 1 million de cycles pour un usage très intensif
- Alimentation 24V DC
- Consommation maximum de 1.4A en courant d'appel moteur
- La serrure devra impérativement être toutes mains (droite/gauche et poussant/tirant) pour que la maintenance ultérieure puisse être effectuée par un seul et unique modèle.
- Sortie par simple abaissement de la béquille et en une seule manœuvre conformément au Code du travail. Cette béquille sera donc toujours active.
- Déverrouillage rapide impérativement inférieur à 0,5 seconde.
- Verrouillage mécanique et automatique à chaque fermeture de porte
- La porte doit rester fermée et verrouillée même en cas de mode dégradé (absence de courant, foudre, panne...) pour empêcher tout accès de l'extérieur.
- 3 organes de manœuvre indépendants pour assurer une sécurité optimum des biens et des personnes : moteur – clé – béquille
- Connexion au système de contrôle d'accès par BUS RS485 pour assurer une sécurité maximum des données. Remontée des informations de la serrure sur le système de contrôle d'accès par un protocole propriétaire.

La mise en œuvre des serrures sera adaptée en fonction du support de la porte (bois, métal ou verre). Il appartient au présent lot de s'assurer que les équipements soient mis en place conformément au procès-verbal du fabricant de serrures.

Bloc-porte anti-effraction CR4 certifie A2P locaux techniques

Selon le besoin de sécurité sur les portes, il sera demandé sur les porte « **Haut niveau de sécurité** » des blocs porte spécifique répondant aux normes anti-effraction de type CR4 / CR3.

Bloc-porte antieffraction classe CR4 selon norme NF EN1627 (PV émis par un laboratoire indépendant à fournir) et certifié A2P CR4 bloc-porte locaux techniques.

Le bloc-porte est composé d'un bâti tubulaire permettant de nombreuses configurations de pose, d'un vantail affleurant à structure métallique avec profil anti-dégondage toute hauteur et de paumelles à roulement à billes. Il ne devra pas avoir de barre de seuil, afin de permettre un accès aisé.

Il sera équipé de :

- Serrure motorisée 4 points à pêne crochet et encastrée dans l'ouvrant
- Gestion électronique du cylindre permettant la détection des attaques et le blocage du cylindre à distance
- Fonctionnement à sécurité négative (à émission de courant). La porte doit rester verrouillée même en cas de coupure d'alimentation.
- Pêne demi-tour antirebond pour garantir la fermeture de la porte en toute situation
- Connexion par BUS RS485 et communication par protocole propriétaire
- Cylindre européen double entrée haute sûreté Protec² avec 3 clés brevetées
- Poignée de tirage extérieure avec bloc de protection cylindre
- Palette de sortie libre EXEA conforme à la norme EN179 avec bouton de sortie intégré
- Ferme-porte encastré conforme à la norme EN 1154 avec réglage de la force, de la vitesse initiale, de l'à-coup final, et frein à l'ouverture.
- Rejet d'eau si la porte donne sur l'extérieur
- Finition gris RAL7031, ou blanc RAL 9010 selon choix du Maître d'Ouvrage.

OPTION : Pare-balle FB4 selon la norme européenne EN 1522

OPTION : Résistance au feu EI260
OPTION : microviseur simple ou pare-balle
OPTION : Palette de sortie contrôlée EXEA Control

Bloc-porte anti-effraction CR3

Bloc-porte antieffraction classe CR3 selon norme NF EN1627 (PV émis par un laboratoire indépendant à fournir).

Le bloc-porte est composé d'un bâti tubulaire permettant de nombreuses configurations de pose, d'un vantail affleurant à structure métallique avec profil anti-dégondage toute hauteur et de paumelles à roulement à billes. Il ne devra pas avoir de barre de seuil, afin de permettre un accès aisé.

Il sera équipé de :

- Serrure motorisée 4 points à pêne crochet et encastrée dans l'ouvrant
- Gestion électronique du cylindre permettant la détection des attaques et le blocage du cylindre à distance
- Fonctionnement à sécurité négative (à émission de courant). La porte doit rester verrouillée même en cas de coupure d'alimentation.
- Pêne demi-tour anti-rebond pour garantir la fermeture de la porte en toute situation
- Connexion par BUS RS485 et communication par protocole propriétaire
- Cylindre européen double entrée haute sûreté Protec² avec 3 clés brevetées
- Poignée de tirage extérieure avec bloc de protection cylindre
- Palette de sortie libre EXEA conforme à la norme EN179 avec bouton de sortie intégré
- Ferme-porte encastré conforme à la norme EN 1154 avec réglage de la force, de la vitesse initiale, de l'à-coup final, et frein à l'ouverture.
- Rejet d'eau si la porte donne sur l'extérieur
- Finition gris RAL7031, ou blanc RAL 9010 selon choix du Maître d'Ouvrage.

La même gamme de bloc-porte devra équiper l'ensemble des accès de niveau antieffraction CR3 ou CR4 que les portes soient simples ou double-vantail, coupe-feu et/ou issues de secours afin de faciliter la maintenance et assurer une harmonisation esthétique et des équipements.

OPTION : double vantail
OPTION : Coupe-feu 30 minutes
OPTION : Microviseur simple ou coupe-feu
OPTION : Ferme-porte encastré
OPTION : Palette de sortie contrôlée EXEA Control

Lecteurs autonomes béquille ou cylindre sans-fil

Ce type de matériel sera proscrit sur l'ensemble des travaux de l'Université de Bordeaux.

Cas particulier de la gestion ascenseurs

La gestion des cabines d'ascenseurs se fera via l'adjonction d'une « TILLYS-CUBE » dédié avec Option LIFT (gestion de 2 ascenseurs maximum par UTL)

Cas particulier de la gestion des barrières/bornes/portails/roadblocker/portique

Au vu du nombre d'utilisateur de l'Université, les barrières/bornes/portails/roadblocker/portique auront des règles qui leurs sont propre à savoir :

- **des UTL dédiés** uniquement à la gestion des accès et commande de barrières/bornes/portail
- Maximum 6 lecteurs par UTL (100 000 identifiants par lecteurs – soit 600 000 par UTL)
- les cartes modules et UTL ne seront pas ajoutées dans les potelets de barrière et/ou coffrets portail, ces dernières seront installées dans les locaux techniques sous coffrets sécurisés.
- Contrôle des positions hautes et basses ou ouvert et fermé selon l'équipement.

Les automates dédiés aux barrières seront intégré sur Microsésame comme étant sur les sites « Barrière ». (site dédié uniquement à la gestion des barrières, portail, peu importe leur lieu

d'installation)

Les automates respecteront les règles d'installation et d'alimentation mentionnés au chapitre ENTITE DE NIVEAU 1 – UNITE DE TRAITEMENT LOGIQUE.

Pour le matériel installé, de son importance, il sera vérifié de façon spécifique.

L'entreprise installatrice privilégiera les marques de matériel déjà installé sur les universités.

III. ENTITES DE NIVEAU 1 – UNITE DE TRAITEMENT LOCAL, MODULES, LECTEURS

1. ALIMENTATION ELECTRIQUE DE L'ENTITE 1

Les alimentations principales et leur secours utilisés pour les entités de niveau 1 leur seront exclusivement dédiée.

L'utilisation d'une source commune et de son secours pour des équipements d'autre niveau que le 1 est totalement proscrite.

Une note de calculs de l'autonomie des équipements sur sources de secours devra être fourni pour l'ensemble des éléments du niveau 1.

Avec pour objectif une autonomie sur secours de **24/48/72h** selon le domaine d'application des éléments (Porte intérieur, Accès bâtiminaire, etc...)

Une réserve de 30% d'autonomie est exigée afin d'anticiper d'éventuel extension de l'UTL installée.

2. LES LECTEURS DE BADGE

Les lecteurs de badges seront de la gamme Transparent SSCPV2 **obligatoirement sérigraphié TIL Technologies.**

Ils permettront de lire plusieurs technologies : MIFARE Classic, MIFARE DESFire EV3, MONEO, selon les normes ISO14443 A/B niveau 1 à 4.

La gamme de lecteur devra être disponible en plusieurs déclinaison comme suivant :

- Version classique pour pose sur cloison ou mur
- Version étroite **pour montant de porte étroit exclusivement, la version classique (ST) est à privilégier.**
- Version avec écran tactile qui affiche un clavier tournant pour du contrôle d'accès renforcé. (Badge+code et/ou Badge ou code)

Lecture & communication transparente conforme aux prescriptions de l'ANSSI architecture 1 :

- Les lecteurs ne contiennent aucune clés, lecteur dit transparent.
- Lecture de l'identifiant des badges sécurisé et protégé par une clé.
- Cette clé est contenue dans un coffre-fort HSM/SAM certifié ANSSI EAL5+ dans le module de porte, qui gère le lecteur. (Voir chapitre ANSSI)
- Ce module de porte devra être installé dans une baie ou dans un coffret autoprotégé et placé dans un local sécurisé.
- Communication cryptée RS485 AES128 bits direct entre le lecteur, jusqu'à ce module de porte sans convertisseur ou interface. Ainsi les communications seront protégées à l'extérieur du local sécurisé contre toute tentative malveillante.
- Une analyse périodique de la communication (registre signal de vie) entre le lecteur et son module déporté lecteur devra permettre de déclencher une alarme si cette communication est

- inopérante et de la transmettre à l'UTL et à la supervision centralisée.
- Pour les lecteurs extérieurs, les lecteurs devront avoir un aspect soigné, ainsi qu'un haut niveau de résistance aux intempéries et aux dégradations extérieurs.
- Les lecteurs devront être au minimum anti-vandale IK10, IP 65 (hors connectique) un joint d'étanchéité acrylique devra être apposé sur ces derniers afin de se prémunir de tout ruissellement d'eau sur ses connectiques, et leurs températures de bon fonctionnement devra être comprise entre -10C à +60C.
- Les lecteurs de badges seront de type proximité passive avec une distance de lecture de l'ordre de 3 à 6cm.

Précaution d'installation :

Les lecteurs ne devront pas être fixés sur une surface métallique et/ou béton armé. (forte diminution de la distance de lecture)

Dans les situations qui l'imposerait (mur en béton armé, montant de menuiserie métallique), une entretoise sera installée entre le support et le lecteur, il faudra en informer le client et faire des tests de validation avant réception des travaux.

En cas de problème de lecture avéré à la mise en service, l'entreprise installatrice aura l'obligation de la reprise du lecteur pour l'ajout d'entretoise.

Une distance de 30 cm entre 2 lecteurs sur un même plan ou dos à dos.

Précaution de câblage :

Ils pourront être installés, jusqu'à une distance d'environ 300m de leur module de gestion avec l'utilisation d'un câble spécifique type bus belden.

De manière générale, tous les fils non utilisés sur chaque aboutissant du câble seront reliés ensemble et raccordés au 0V de l'alimentation dédié

3. LES MODULES

Les modules TIL TECHNOLOGIES installés seront de gamme CUBE minimum, compatible avec les UTL TILLYS CUBE via un bus RS485 sécurisé AES.

Si les travaux demandent une intégration sur une UTL existante, et si cette dernière n'est pas de gamme CUBE, une mise à jour vers la version CUBE est obligatoirement à prévoir, et le module ajouté sera de gamme CUBE également.

De manière générale le raccordement sur UTL existante est à proscrire dans le cadre de nouveau travaux.

Précaution d'installation :

L'ensemble des modules seront obligatoirement installés dans des coffrets en montage rail DIN, centralisé, autoprotégé et installé dans des locaux sécurisés.

L'installation en faux plafond technique ou apparent sera proscrite.

Précaution de câblage :

Ils pourront être installés, jusqu'à une distance d'environ 300m (cumulé pour le bus entier) de leur UTL avec l'utilisation d'un câble spécifique type bus belden.

L'entreprise installatrice devra vérifier les longueurs de câble et adapter la section pour éviter les chutes de tensions.

Si les tensions des modules déportés de l'installation sont inférieures à 12V, l'entreprise installatrice aura, **à sa charge**, le rajout d'alimentation de module dédié.

De manière générale, tous les fils non utilisés sur chaque aboutissant du câble seront reliés ensemble et raccordés au 0V de l'alimentation dédié

4. LES UNITES DE TRAITEMENT LOCALE

Caractéristiques :

Les UTL proposées seront de type TILLYS CUBE ou équivalent. Elles devront permettre la **gestion combinée du contrôle d'accès et de la détection intrusion**, permettant ainsi des automatismes et des asservissements optimisés entre les deux fonctions, des économies d'achat et d'installation.

Elles assureront également des asservissements particuliers tels que la gestion de sas ou d'ouvrants et la gestion des alarmes techniques.

Véritable automate, chaque UTL sera :

- Programmable permettant souplesse et adaptation du système aux besoins présents et futurs
- Autonome dans la gestion des accès, et intrusion en mode nominal et dégradé
- De conception industrielle obligatoire : T : -10°C à + 55°C, alimentation de 10 à 28 Vdc, bornier débrochable, entrée universelle paramétrable (TOR, comptage, équilibrée jusqu'à 6 états) signalisation d'état par LED sur chaque bus, réseau, alim, entrée
- Configurable au niveau réseau par un Web serveur embarqué sécurisé HTTPS
- D'une capacité minimum de :
 - 600 000 identifiants
 - 24 lecteurs de badge
 - 1 Prise RJ45 10/100 Mb natif pour être raccordé directement sur un réseau Ethernet avec la possibilité d'un VLAN (réseau local virtuel) - Carte réseau Ethernet 10/100 Mb base T (IP fixe ou DHCP), 802.1x, IPV6 ready, SNMP v3 (état système)
 - 32 jours fériés, 128 programmes horaires, 32 groupes de points intrusion,
 - 3 bus RS485 3 bus RS485, 57600 bauds, sécurisation AES 128 bits certifié ANSSI, Avec une topologie de câblage ouverte (bus, étoile, toile d'araignée) et une longueur jusqu'à 600 mètres, protégés contre les court-circuits, surtensions et inversions de polarités
 - Gérer des modules déportés selon les capacités à gérer sur ses bus RS485 permettant une architecture distribuée ou centralisée
 - **Grande adaptabilité** Compatibilité ascendante avec les anciennes générations de modules : NG (bus ML/V3) et V2 (bus MD/V2).
 - Devra pouvoir se fixer sur rail DIN à intégrer dans une armoire spécifique ou coffret TIL TECHNOLOGIES

Une réserve de disponibilité de 30% des lecteurs sur l'UTL est à prévoir pour tout chantier neuf. (soit 8 lecteurs de réserve pour UTL24)

Le fonctionnement en mode dégradé :

Les UTL posséderont et pourront traiter toutes les informations nécessaires à un fonctionnement autonome.

Les autorisations de passage, antiretour (sans transfert vers d'autre UTL), gestion de plages horaires, stockage des informations et événements, broadcast et partage d'informations seront assurés même en cas de déconnexion du réseau Ethernet. Lors de la reconnexion du réseau, les informations seront restituées automatiquement au PC serveur.

Communication directe inter TILLYS sur IP (anti-passback). Fonctionnement en mode autonome : en cas de perte de communication avec MICROSESAME, TILLYS CUBE conserve un historique des 10 000 derniers événements.

Sécurité

Fonctionnalité très importante : lors d'un téléchargement, les UTL devront continuer à fonctionner normalement, c'est-à-dire lire les badges, exécuter les automatismes embarqués dans l'UTL (commande de la gâche par exemple), et remonter les événements sur le superviseur en temps réel. Tout système ne permettant pas d'assurer cette fonctionnalité ne sera pas retenu.

Précaution d'installation :

L'ensemble des UTL seront obligatoirement installés dans des coffrets en montage rail DIN, centralisé, autoprotégé et installé dans des locaux sécurisés.
L'installation en faux plafond technique ou apparent sera proscrite.

Précaution de câblage :

Le câblage de la partie réseau devra respecter le processus décrit dans le chapitre VI. 3. Du présent dossier

Si les tensions des modules déportés de l'installation sont inférieures à 12V, l'entreprise installatrice aura, **à sa charge**, le rajout d'alimentation de module dédié.

De manière générale, tous les fils non utilisés sur chaque aboutissant du câble dans l'intégralité du coffret seront reliés ensemble et raccordés au 0V de l'alimentation dédié.

Les câblages non conformes aux préconisations seront à reprendre par l'entreprise installatrice et seront à reprendre à ses frais.

IV. ENTITE DE NIVEAU 2 SERVEUR ET POSTE CLIENT

1. SERVEUR

A la charge du service de la DSI, aucune modification ou création n'est prévue au présent marché.

2. POSTE DE TRAVAIL CLIENT

A la charge du service de la DSI, aucune modification ou création n'est prévue au présent marché.

V. ARCHITECTURE ANTI-INTRUSION

1. MATERIELS

Les systèmes intrusion seront de marque TIL TECHNOLOGIES et connectés au serveur MICRO SESAME existant, aucun système autonome ne sera accepté

Chaque boîte de raccordement et équipement anti-intrusion, sera auto-protégé et câblé en mode équilibré avec résistances 1kOhms obligatoire. L'ensemble des équipements de détection intrusion installés seront au minima NFA2P Grade 2.

L'utilisation d'un système point à point est recommandé, cependant le système TIL TECHNOLOGIES, propose une solution annexe en cas de complexité de passage de câble, la possibilité de raccordement d'un « BUS » Intrusion avec l'utilisation d'un module MLCK et de transpondeur EQUILOCK® (maximum 2x32 zones d'intrusion par MLCK).

Le choix de l'utilisation du système EQUILOCK® devra être justifié et validé par l'Université de Bordeaux selon chaque typologie de projet.

VI. ARCHITECTURE CABLAGE DE COMMUNICATION ET RESEAU

1. CABLAGES BUS TERRAIN

Le câble utilisé sera conforme aux prescriptions du fabricant de l'équipement concerné tout en étant conforme en tout point au câblage normé pour une liaison standard RS 485 dans sa performance la plus haute.

Dans le cas d'une impossibilité de répondre aux deux conditions ci-dessus, il sera mis en place deux câbles pour répondre aux attendus.

Les liaisons entre équipements se feront sans épissures ni dérivation en « ligne droite », les raccordements en étoiles et toiles d'araignée sont proscrits.

Les lecteurs de badges, détecteurs intrusion, etc... seront raccordés sur des modules déportés, eux-mêmes raccordés aux UTL par un bus de terrain RS485.

Pour limiter les problèmes de ce bus RS485 les installations raccordées en étoiles, ou en toiles d'araignées sont proscrites, les épissures et autres raccordements entre équipements sont proscrits.

Les modules déportés seront installés dans des locaux adaptés des bâtiments, l'installation de modules à l'extérieur des bâtiments dans des équipements techniques comme les fûts de barrières de parking, les chambres de tirages, les boîtes de dérivation etc. Sont proscrites.

Si toutefois aucune solution techniquement viable n'est possible il sera possible uniquement dans des Armoires extérieures étanches et feront l'objet d'une approbation de l'Université et devront présenter toutes les garanties concernant les risques climatiques, de malveillance, et auto-protégées.)

2. EQUIPEMENTS ANNEXES AU CABLAGE

Les répéteurs de signaux et convertisseur de signaux seront installés dans les locaux technique des bâtiments.

Leur installation à l'extérieur des bâtiments dans des équipements techniques comme les fûts de barrières de parking, les chambres de tirages, les boîtes de dérivation sont proscrites.

Si obligation, des Armoires extérieures étanches pourront être utilisées en dernier recours, elles feront l'objet d'une approbation de l'Université et devront présenter toutes les garanties concernant les risques climatiques, de malveillance, et seront auto-protégées.).

L'alimentation de ces équipements fera l'objet des mêmes exigences de secours que les équipements concernés.

3. COMMUNICATION ET RESEAUX

Les UTL, seront raccordées directement sur un réseau Ethernet et communiquerons directement avec le serveur sans passerelles ou adaptateurs.

L'installation d'UTL à l'extérieur des bâtiments dans des équipements techniques comme les fûts de barrières de parking, les chambres de tirages, les boîtes de dérivation etc. Sont proscrites. Si obligation, les armoires extérieures étanches feront l'objet d'une approbation de l'Université et devront présenter toutes les garanties concernant les risques climatiques, de malveillance, et auto-protégées.

Dans le cas du réseau Ethernet banalisé de l'Université, la communication s'effectue par le biais d'un V-LAN dédié.

Il appartient à l'entreprise de réaliser les travaux de câblage nécessaires selon les prescriptions de l'Université et d'effectuer les démarches auprès des services concernés pour le raccordement des UTL.

Une charte informatique définit les attentes de l'Université, elle doit être respectée à la lettre.

Les branchements des câblages verticaux sur les installations de l'Université et l'adressage IP se font sur demande auprès du référent sureté de l'Université.

Des documents d'exécution ainsi qu'un test de recettage du point RJ crée seront rendu et soumis à l'approbation de l'université.

Les liaisons radio sont proscrites

VII. LOGICIEL DEDIE AU CONTROLE D'ACCES ET A L'ANTI-INTRUSION

1. INTRODUCTION

Avec le raccordement sur serveur existant, les extensions de licences du logiciel MICRO-SESAME de TIL TECHNOLOGIES devront être prévues. (Version MS2023.3 PRIME)

Le logiciel permet le paramétrage et la supervision du contrôle d'accès, de la détection intrusion, de la GTB, des enregistreurs vidéo, et des différents systèmes tiers présents sur le site via des protocoles ouverts comme MODBUS RTU ou OPC.

Toute passerelle avec d'autres application, les nouveaux matériels seront soumis à validation des services DSI de l'UNIVERSITE DE BORDEAUX.

2. PLAGES HORAIRES / GROUPE DE LECTEURS / PROFILS / DES DROITS D'ACCES

A la charge du service de la DSI, aucune modification ou création n'est prévue au présent marché

VIII. PROGRAMMATION ET MISE EN SERVICE

1. PROGRAMMATION

Introduction

La programmation du système étant une opération complexe, sujette à des risques de fausse manipulation sur des automates déjà en service et en exploitation, seuls des professionnels compétents et formés par le fabricant seront habilités à intervenir.

De ce fait la programmation des automates sera réalisée dans chaque cas de figure par les services de l'université de Bordeaux (D2S - Direction de la Sécurité/Sûreté)

Prestation de l'entreprise installatrice

- L'entreprise installatrice doit finaliser intégralement ses travaux **sans réserve** et remettre un **Dossier des Ouvrages Exécutés (DOE)** complet. Ce DOE inclura :
 - Tous les documents techniques requis. (la composition minimale du DOE est disponible en C II.)
 - Un **cahier de recette global** détaillant l'ensemble des essais et validations effectués, attestant de la conformité de l'installation aux spécifications contractuelles.

Validation par la D2S

- Une **visite des installations** sera effectuée par le service de la D2S pour vérifier la conformité des équipements et leur mise en œuvre.
- En cas de **non-conformité**, l'entreprise installatrice devra reprendre à ses frais toutes les anomalies constatées, ou tout manquement au présent dossier y compris les reprises éventuelles nécessaires dans le DOE.
- La **programmation des équipements** sera effectuée exclusivement par la D2S une fois l'installation validée.

2. MISE EN SERVICE

La mise en service sera réalisée par la D2S, si un dysfonctionnement sur les matériels et/ou câblages livrés est détecté, l'entreprise installatrice devra assurer la remise en conformité de l'ensemble de son installation.

Étapes de mise en service :

- L'entreprise installatrice doit finaliser intégralement ses travaux **sans réserve** et remettre un **Dossier des Ouvrages Exécutés (DOE)** complet.
- La mise en service sera pilotée par les équipes D2S de l'Université, incluant des tests fonctionnels et des essais en conditions réelles d'utilisation.
- **Responsabilités de l'entreprise** : Toute non-conformité liée à l'installation, au câblage ou au matériel sera corrigée à la charge de l'entreprise installatrice.
- **Validation et levée de réserves.**
- Ajustements finaux du DOE si nécessaire.

3. PARAMETRAGE RESEAUX

Coordination avec la DSI :

L'entreprise installatrice devra coordonner avec les services de la DSI pour :

- Valider les **emplacements disponibles** dans les baies informatiques pour le raccordement des équipements au réseau.
- S'assurer que les **noyaux utilisés** pour le raccordement respectent les spécifications et normes de la baie concernée.

Recette des câblages réseau :

L'entreprise devra produire une **recette complète des câbles réseau**, attestant de leur conformité (test

de continuité, de performance, et de respect des standards).

Restrictions sur le jarretierage :

- Aucun **jarretierage** ne sera autorisé dans les baies informatiques sans une validation explicite des services de la DSI.
- Les jarretières, fournies par l'entreprise, devront être de **taille minimale requise** et installées uniquement après approbation.

Les paramètres réseaux des nouveaux automates seront fournis par le service de la DSI, le raccordement aux équipements actifs de l'université ne se fera que sous validation de cette dernière, en aucun cas l'entreprise installatrice ne pourra se raccorder sans accord préalable sur les équipements actifs de l'Université.

IX. SYNOPTIQUE D'EXPLOITATION

Dans le cadre des travaux, une attention particulière doit être accordée aux synoptiques, qui représentent les vues graphiques d'exploitation de nos systèmes de Contrôle d'Accès et d'Intrusion.

L'Université a mis en place un référentiel graphique spécifique afin d'uniformiser et de simplifier l'exploitation des synoptiques par l'ensemble de nos équipes de sécurité et techniques.

Cette charte graphique, conçue pour garantir une compréhension et une utilisation cohérentes des interfaces, doit être obligatoirement respectée par l'installateur.

Comme la programmation du site, la création des vues graphiques est à la charge des services de la D2S.

C. DOSSIER D'EXECUTION ET DOE

I. DOSSIER D'EXECUTION

L'ensemble des travaux devra inclure une phase de préparation, permettant à l'entreprise installatrice de produire un **dossier d'études techniques** exhaustif prenant en compte tous les éléments impactés par le projet.

Contenu du dossier d'exécution :

Le dossier d'exécution devra inclure, au minimum :

- La nomenclature détaillée du matériel prévu pour le projet.
- Plan d'implantation et de distribution avec les types de câbles indiqués sur chaque liaison
- Plan d'implantation des coffrets et périphérique et/ou supervision.
- Le synoptique global du projet (UTL, modules, périphériques terminaux).
- Une note de calculs d'autonomie des batteries, conformément aux exigences par niveau d'entité.
- Fiches techniques **et** manuels d'utilisation de chaque équipement.
- Un schéma logique du réseau IP
- Un plan de câblage détaillé (électrique et communication).

Validation préalable obligatoire :

S'agissant de la sûreté des bâtiments, ce dossier devra être **soumis à validation par les services spécialisés de la D2S** présents lors de la réception des travaux.

Aucune phase l'installation, de programmation ou de mise en service ne pourra être initiée tant que les éléments requis n'auront pas été validés.

Interdiction des travaux supplémentaires en cas de non-respect :

Tout manquement aux recommandations et prescriptions techniques de ce document entraînera :

- **Un rejet des propositions de travaux supplémentaires** ou de demandes de plus-values associées.
- Une obligation pour l'entreprise de se conformer aux spécifications sans compensation financière supplémentaire.

II. DOSSIER DOE

L'ensemble des travaux de création, d'extension ou d'évolution donneront lieu à la remise d'un Dossier des Ouvrages Exécutés (DOE) complet.

Tous les documents fournis seront conformes à l'installation réalisée au moment de la réception des ouvrages, en accordant une attention particulière au repérage des fils, câbles, bornes de connexion, borniers et repères d'appareillage.

Contenu du dossier DOE :

Le dossier des ouvrages effectué devra inclure, au minimum :

- La nomenclature détaillée du matériel prévu pour le projet (UTL, modules, lecteurs, coffrets, etc.) avec leur localisation et numéro de série / adresses mac / adresse ip, adapté selon les retours du chantier.

- Plan d'implantation et de distribution avec les types de câbles indiqués sur chaque liaison
- Plan d'implantation des coffrets et périphérique et/ou supervision.
- Le synoptique global du projet (UTL, modules, périphériques terminaux).
- Fiches techniques **et** manuels d'utilisation de chaque équipement.
- Schéma de raccordement **multifilaire** des périphériques, UTL, modules, coffrets incluant :
 - Type de câble utilisé.
 - Identification des bornes, connecteurs et points de raccordement.
 - Spécifications des sections de câble en cas de distance étendue.
- Schéma logique du réseau IP, incluant les configurations VLAN et les adressages validés par la DSI.
- Note de calcul des alimentations et batteries pour chaque entité, selon les exigences de durée de fonctionnement.
- Photos haute résolution des installations, incluant :
 - Coffrets ouverts (modules visibles).
 - Points d'accès sécurisés (portes, serrures).
 - Passages de câbles critiques.
- Documentation technique et manuels de maintenance.
- Cahier de recette détaillé comprenant :
 - Résultats des tests fonctionnels pour chaque composant (contrôle d'accès, intrusion, alimentation, remontées d'alarmes).
 - Essais de fonctionnement des équipements critiques (UTL, lecteurs, modules).
 - Validation des tensions et continuité des câblages.
 - PV des tests réseau (performance des câblages, conformité des jarretières, tests des points RJ).
 - Résultats des essais en conditions réelles.
- Le PV de réception du chantier sans réserve visé par les acteurs du projet (entreprise installatrice, DSI, D2S).

Conformité et mise à jour :

- Le DOE devra refléter l'installation finale après levée complète des réserves.
- Toute modification sur site (ajout, déplacement, reprise) devra entraîner une mise à jour systématique du DOE.

Coordination avec le Dossier d'Exécution :

- Le DOE devra être cohérent avec le dossier d'exécution validé.
- Toute incohérence entraînera un rejet jusqu'à correction.

Validation par la D2S et la DSI :

- Le DOE sera soumis à la validation des services spécialisés.
- La validation finale ne sera accordée qu'après vérification complète des documents et conformité totale des installations.

Refus des plus-values :

- Aucun manquement aux recommandations de ce document ou aux spécifications techniques ne pourra faire l'objet de travaux supplémentaires ou de demandes de compensation financière.

FIN DU DOCUMENT