

Direction des travaux et de l'architecture

Département **Patrimoine immobilier et équipements techniques**

2 avenue Foch – 29200 BREST

Référentiel technique

Sureté

Date : 15/06/2020

Rédaction : Stéphane TRAVERS



Coordination et rédaction

TRAVERS Stéphane Responsable sécurité incendie

Comité de lecture et validation

MAHEO Emmanuel, Ingénieur responsable du service exploitation

ROUSSEAU David Ingénieur responsable du département électricité

Indice	Date	Désignation
A	15/06/2020	Edition initiale

Annexe 1 : Plan de sécurisation des établissements de soins.Déploiement des contrôles d'accès sur le CHRU de Brest

1.	GENERALITES.....	4
1.1.	OBJET	4
1.2.	RÈGLEMENTATION EN VIGUEUR	4
1.3.	ABRÉVIATIONS :	8
1.4.	SUJÉTIONS EN MILIEU OCCUPÉ.....	11
1.5.	OBLIGATIONS EN MATIÈRE ENVIRONNEMENTALE	12
1.6.	AMIANTE ET PLOMB :.....	12
1.7.	DOCUMENTS À REMETTRE PAR LE PRESTATAIRE	12
1.8.	SYNTHESE SCHEMA DIRECTEUR SSI CHRU BREST	13
1.9.	GMAO/BIM	13
1.10.	FORMATION DU PERSONNEL	13
1.11.	CABLAGE.....	13
2.	LE DISPOSITIF DE CONTROLES D'ACCES ET ANTI INTRUSION :	15
2.1.	PROJETS NEUFS ET PÉRENNES :	15
2.2.	PHILOSOPHIE GÉNÉRALE DU PROCESS DE GESTION ET SUPERVISION DES CONTRÔLES D'ACCÈS.....	25
2.3.	QUALITÉ DU SYSTÈME	26
2.4.	ENVIRONNEMENT MATÉRIEL	27
2.5.	ARCHITECTURE MATÉRIELLE	28
2.6.	MATÉRIEL	29
2.7.	LES MODULES DÉPORTÉS (RS485)	31
2.8.	L'ENVIRONNEMENT DE LA PORTE	34
2.9.	LES LECTEURS DE BADGES	40
3.2.	LES POSTES CLIENTS	43
3.3.	CONFIGURATION RÉSEAU	43
4.	DESCRIPTIF DU LOGICIEL	45
4.1.	GÉNÉRALITÉS	45
4.2.	CONTRÔLE D'ACCÈS	46
4.3.	MICROCODES :	49
4.4.	MULTI-SITE / MULTI-CLIENT / MULTI-ENTITÉ.....	49
4.5.	INTRUSION	50
5.	SYNOPTIQUES.....	53
5.1.	VARIABLES	53
5.2.	INTERFACE HOMME - MACHINE (IHM).....	53
5.3.	CAS PARTICULIERS DE CONTRÔLES D'ACCÈS :	58
5.4.	ALARME ANTI INTRUSION – PROJET DE RÉHABILITAION À COURTS ET MOYEN TERME :	61
6.	LA VIDÉO PROTECTION.....	62
6.1.	GÉNÉRALITÉS :	62
6.2.	CONTEXTE :	62
6.3.	EXPLOITATION.....	63

6.4.	EVOLUTION DU SYSTÈME.....	63
6.5.	TRAITEMENT DES IMAGES :	64
6.6.	LES CAMÉRAS	64
6.7.	ENRÉGISTREMENT :	65
6.8.	CABLAGE.....	66
6.9.	SYNOPTIQUE DU SYSTÈME :	66
6.10.	RÉDUCTION DU STOCKAGE :	67
7.	INTERPHONIE ET VISIO PHONIE :	67
7.1.	PROJETS NEUFS ET PÉRENNES :	67
7.2.	STENTOFON :	71
7.3.	RÉABILITATION DE SERVICE :	72
7.4.	EQUIPEMENTS AIPHONE :	72
8.	SYSTÈMES ANTI-FUGUE.....	74
8.1.	GÉNÉRALITÉS :	74
8.2.	PROJETS NEUFS ET PÉRENNES :	75
8.3.	RÉABILITATION DE SERVICE :	76

AVANT-PROPOS

Ce document est une aide à la rédaction du Cahier des Clauses Technique Particulières dans le domaine de la sureté au CHRU de Brest. Les thématiques suivantes sont abordées : contrôle d'accès, vidéo protection et anti intrusion.

Le rédacteur ainsi que l'émetteur ne peuvent être tenu pour responsable :

- de l'utilisation ou l'interprétation qui pourrait en être faite,
- des effets de toute nouvelle règle technique ou normative intervenue après la rédaction de ce document.

1. GENERALITES

1.1. Objet

Ce document est destiné aux installateurs et aux fournisseurs d'équipements, il ne peut être substitué.

Sans un accord écrit du CHRU, aucune dérogation ne sera acceptée.

1.2. Réglementation en vigueur

Vidéo protection :

L'installation devra satisfaire à l'ensemble des normes et règlements en vigueur au moment de leur réalisation et en particulier à ceux désignés ci-après en les complétant :

- La loi n°95-73 du 21 janvier 1995 relative à la sécurité,
- Le décret n°96-926 du 17 octobre 1996 relatif à la vidéosurveillance,
- La circulaire du 22 octobre 1996 relative à l'application de l'article 10 de la loi n°95-73 du 21 janvier 1995,
- La loi n°2006-64 du 23 janvier 2006 relative à la lutte contre le terrorisme,
- Le décret n°2006-929 du 28 juillet 2006 relatif à la vidéosurveillance et modifiant le décret n°96-926 du 17 octobre 1996,
- L'arrêté du 03 août 2007 portant définition des normes techniques des systèmes de vidéosurveillance,
- La circulaire NORINTD0600096C exposant les modifications apportées à la réglementation sur la vidéosurveillance.
- La Loi n° 95-73 du 21 janvier 1995 d'orientation et de programmation relative à la sécurité,
- Au 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,
- La circulaire n° 68234 du 22 octobre 1996 relative à la vidéosurveillance urbaine,
- A l'arrêté du 3 août 2007 portant définition des normes techniques des systèmes de vidéosurveillance,
- Au décret n°2009-86 du 22 janvier 2009 modifiant le décret n°96-926 du 17 octobre 1996 relatif à la vidéosurveillance,
- Au décret n° 2012-112 du 27 janvier 2012 modifiant le décret n° 96-926 du 17 octobre 1996 relatif à la vidéo protection,
- Les textes codifiés applicables aux ouvrages réalisés et à la protection des personnels,
- Les prescriptions du présent document suivant les règles de l'art.
- l'arrêté du 26 février 2003 : Circuits et installations de sécurité des locaux de travail
- décret du 31 août 2006 : Règles relatives aux bruits de voisinage,
- les textes réglementaires sur la législation du travail et la protection des travailleurs
- le Code du Travail et le décret du 31 mars 1992
- le Règlement Sanitaire Départemental

Autres textes :

- APSADF R82 : règle d'installation des installations de vidéosurveillance
- NF C 15-100 relative aux travaux électriques B.T.A.,
- NF C 32 024 – méthodes d'essais communes pour les matériaux d'isolation et de gainage des câbles électriques,
- Compatibilité électromagnétique : marquage CE, FCC part 15 Class A (EN 55022 Class A), EN 50082-1, VCCI Class A,
- les avis techniques relatifs à la mise en œuvre des produits dans le cadre de leur PV d'essais,
- l'ensemble des normes AFNOR chaque fois qu'il existe une norme de fabrication relative aux appareils utilisés, en particulier :
 - Normes ISO/IEC 11801 v2 (et amendements 1 et EN50173 v2) définissant l'architecture, la structure et les performances des composants de câblage cuivre et optique
 - Normes ISO/IEC 14763-1 et 2 définissant la planification et l'installation des câblages (densité des répartiteurs et espaces de travail).
 - Normes ISO/IEC 18010 définissant les supports des câbles et prises.
 - Normes TIA-606 définissant les principes de repérage des composants du câblage

Contrôles d'accès :

Il est nécessaire que toutes les dispositions soient prises afin d'assurer prioritairement la sécurité des personnes en cas de catastrophes nécessitant des évacuations. Certaines procédures sont également à effectuer auprès de la Commission nationale de l'informatique et des libertés (CNIL), dans le cadre de la protection de la vie privée, en fonction des dispositifs mis en place. Pour finir, des contraintes plus spécifiques peuvent s'appliquer en fonction des zones protégées. Cette annexe n'a pas pour vocation d'être exhaustive, mais de fournir un aperçu des contraintes à prendre en compte dans un projet de mise en place de systèmes de contrôle d'accès.

Protection des personnes :

En cas de catastrophes nécessitant une évacuation (des incendies la plupart du temps, mais également d'autres risques potentiels en fonction de l'environnement de travail), des procédures doivent être précisément définies. En particulier, le système doit pouvoir déverrouiller tous les accès concernés par l'alarme (bâtiment ou zone), afin que l'évacuation ne soit pas bloquée ou ralentie, et éditer la liste des personnes se trouvant à l'intérieur (cf. normes NFS 61-937 et NFS 61-931 sur les issues de secours). Il appartient au responsable du site de définir les modalités de retour dans les locaux à l'issue d'une alerte :

- ouverture complète des points d'accès (nécessite alors un contrôle humain pour s'assurer que ceux qui rentrent en ont bien le droit)
- fonctionnement normal du système (il faut alors pouvoir réinitialiser le système).

En cas de panne d'un ou plusieurs composants du système, il appartient aussi au responsable du ou des sites de choisir quel doit être le fonctionnement dégradé du système en fonction des objectifs de sécurité, de la configuration du site et des capacités de l'organisme. Le comportement dégradé ne doit bien entendu pas perturber l'évacuation des personnes en cas de catastrophe. Le système pourra par exemple basculer en position « tout ouvert ». Mais ceci peut ne pas être du tout satisfaisant. Une autre solution pourrait être d'adjoindre une commande manuelle de déverrouillage depuis l'intérieur (selon le dispositif mécanique du point d'accès) permettant ainsi la sortie du personnel. Il faut alors traiter le cas de l'entrée d'individus avec le concours de personnels de sécurité.

Cela montre bien l'importance d'un système particulièrement redondant pour garantir la plus grande résilience possible.

Norme simplifiée n°42 de la CNIL :

La norme simplifiée n°42 de la CNIL concerne le traitement automatisé d'informations nominatives mis en œuvre sur les lieux de travail pour la gestion d'accès au locaux, des horaires et de la restauration.

Cette norme simplifiée ne traite pas le cas des dispositifs utilisant des données biométriques (cf. 3.4.2 Utilisation de la biométrie par empreintes). En général, les systèmes de contrôle d'accès utilisant des technologies sans contact relèvent, lorsqu'ils n'utilisent pas de techniques biométriques par empreintes, de cette norme simplifiée.

Ils sont donc soumis à un régime de déclaration de conformité à cette norme. Concernant la journalisation des événements, et conformément aux exigences de cette norme simplifiée, il est important de prendre en compte le fait que les éléments relatifs au déplacement des personnes ne peuvent être conservés au-delà de trois mois.

Pour finir, la CNIL fixe les règles quant au traitement des informations personnelles : communication et durée de conservation des éléments d'identification, information des usagers, etc.

Ces règles sont consultables sur le site de la CNIL.

Utilisation de la biométrie :

Tous les traitements de données à caractère personnel, dès lors qu'ils mettent en jeu des données biométriques (empreinte, contour de la main, etc. et à l'exception de la biométrie par veines par exemple), doivent faire l'objet d'une demande d'autorisation préalable auprès de la CNIL. Dans les cas suivants, les formalités sont allégées et se réduisent à une déclaration de conformité à des « autorisations uniques »:

- Cas des dispositifs reposant sur la reconnaissance du contour de la main et ayant pour finalité le contrôle d'accès ainsi que la restauration sur les lieux de travail (autorisation unique n°AU007)29.
- Cas des dispositifs reposant sur la reconnaissance de l'empreinte digitale exclusivement enregistrée sur un support individuel détenu par la personne concernée (c'est-à-dire le badge et non l'UTL) et ayant pour finalité le contrôle d'accès aux locaux sur les lieux de travail (autorisation unique n°AU-008). A5.4

Implication des instances représentatives du personnel :

La mise en place d'un système de contrôle d'accès doit se faire en accord avec le Code du Travail, puisqu'elle implique un changement des conditions de travail. La direction doit informer de son intention de mettre en place un contrôle des accès physiques, demander l'avis des instances représentatives du personnel (Comité hygiène et sécurité, Comité d'entreprise).

Personnes à mobilité réduite :

Lorsque les zones protégées sont susceptibles d'accueillir des personnes handicapées à mobilité réduite, il est important de prendre en compte la norme NF P 99-611 relative à l'accessibilité des personnes à mobilité réduite. Les têtes de lecture par exemple doivent être installées à une hauteur par rapport au sol de 1,10m à 1,30m par rapport au sol, ainsi que tout dispositif additionnel d'authentification (boîtier de saisie de code PIN, d'empreinte biométrique, etc.).

Autres :

Attention, certaines zones protégées sont concernées par des réglementations particulières qui impacteront les caractéristiques du système de contrôle des accès. C'est le cas par exemple des sites comportant des installations abritant des matières nucléaires, dont les systèmes d'information

participant à la protection des zones névralgiques ne peuvent en aucun cas être interconnectés au réseau public, ni aux autres réseaux, sauf dispositions particulières. On retrouve également d'autres contraintes réglementaires spécifiques pour les sites classés SEVESO30, les zones ATEX31, etc. Toutes ces contraintes doivent être clairement identifiées dès l'expression du besoin. 29 Par délibération n°2012-322 du 20 septembre 2012 publiée au JORF n°0238 du 12 octobre 2012, la CNIL a mis fin à la possibilité de recourir à l'autorisation unique n°AU-007 pour les dispositifs reposant sur la reconnaissance du contour de la main et ayant pour finalité la gestion des horaires de travail. Les systèmes préalablement autorisés disposent d'un délai de 5 ans à partir de la publication pour se mettre en conformité. 30 La directive 96/82/CE ou directive SEVESO est une directive européenne qui impose aux Etats membres d'identifier les sites industriels présentant des risques d'accidents majeurs. 31 La réglementation ATEX (Atmosphères Explosives) est issue de deux directives européennes (94/9/CE et 1999/92/CE). Cette réglementation a été transposée en France dans le code du travail à

L'ANSSI :

L'Agence nationale de la sécurité des systèmes d'information (ANSSI) a été créée le 7 juillet 2009 sous la forme d'un service à compétence nationale. En vertu du décret n°2009-834 du 7 juillet 2009 modifié par le décret n°2011-170 du 11 février 2011, l'agence assure la mission d'autorité nationale en matière de défense et de sécurité des systèmes d'information. Elle est rattachée au Secrétaire général de la défense et de la sécurité nationale, sous l'autorité du Premier ministre. Pour en savoir plus sur l'ANSSI et ses missions, rendez-vous sur <http://www.ssi.gouv.fr>

1.3. Abréviations :

Vidéo protection :

Vidéoprotection : C'est l'installation d'un système de caméras et d'un stockeur (enregistreur et traitement des images)

Vidéosurveillance : C'est le fait de confier à une société spécialisée et agréée, la surveillance des sites protégés par un système de vidéoprotection 24h/24, 7 jours/7, afin de prévenir en vue d'agir selon les consignes que vous aurez établies.

Analogique : Quand on parle de système analogique, on parle d'une vidéo représentant l'information comme un flux continu de données analogiques. Ce flux, basé sur le principe du balayage, est destiné à être affiché sur un écran de télévision. Il existe plusieurs normes pour la vidéo analogique. Les trois principales sont : PAL, NTSC, SECAM.

Coaxial : Un câble coaxial est utilisé en surveillance vidéo pour les branchements entre les différents éléments si le réseau n'est pas connecté en Wi-Fi. Il est constitué d'une âme en cuivre séparée d'une tresse par une épaisse couche d'isolant. En englobant l'âme, la tresse joue un rôle d'atténuation pour les interférences extérieures. En comparaison d'une paire torsadée, ce câble présente un meilleur rapport signal/bruit. C'est pourquoi il est utilisé pour des connexions réseaux à plus fort débit ou à des portées plus importantes.

FTP ou File Transfer Protocol : C'est un protocole de communication destiné à l'échange informatique de fichiers sur un réseau TCP/IP. Il peut héberger des fichiers tels que des images de surveillance vidéo qui sont de ce fait accessibles à distance. Il autorise également la copie de fichier

d'un ordinateur à un autre du même réseau, il permet d'alimenter un site web, ou encore de supprimer ou de modifier des fichiers sur un ordinateur distant.

Identification (ID) : En matière de surveillance vidéo, l'identification est un nombre ou un nom présent dans le signal vidéo et permettant d'identifier ce film. Elle peut être visible ou invisible.

Réseau TCP/IP ou Transmission Control Protocol/Internet Protocol : C'est un protocole utilisé sur Internet pour transmettre des données entre deux appareils. Le protocole de transport (TCP) prend à sa charge l'ouverture et le contrôle de la liaison entre deux ordinateurs, un appareil et un ordinateur.... Puis le protocole d'adressage (IP) assure le routage des paquets de données. Il faut voir cela comme un langage universel permettant à deux machines de communiquer entre elles quel que soit leur système d'exploitation. Le réseau TCP/IP est utilisé en **surveillance vidéo** pour les échanges de données entre les caméras et un ordinateur, un routeur...

Surveillance vidéo en temps réel : Elle correspond à une prise d'images rapide par une caméra (25 images par secondes). Ces images sont au format Jpeg. Elles sont ensuite assemblées par un logiciel et transformées en vidéo au format AVI et disponibles instantanément sur un serveur FTP. Par le biais d'une connexion internet, il est possible de regarder cette vidéo en temps réel.

PTZ : Pan/Tilt/Zoom qui veut dire incliner, pivoter, zoomer. (Dôme motorisé)

POE : Power Over Ethernet : fonction des caméras réseau, qui permet une alimentation électrique à partir du câble réseau

IP66 : Indice de Protection: Décrit l'indice de protection d'appareils en ce qui concerne la pénétration de corps étrangers et d'humidité.

FPS : Frames Per Second : Unité pour la fréquence d'images des enregistrements vidéo de caméras ou d'enregistreurs.

Dyn DNS ou DDNS : Entrée de nom de domaine dynamique sur serveur: Service réseau, qui tient à disposition des adresses IP de ses clients dans une base de données et les actualise.

AUTOFOCUS : Fonctionnalité permettant à la caméra de se concentrer sur une partie précise de la zone filmée.

BANDE PASSANTE : C'est la largeur de fréquence d'un signal électrique (ou distance entre deux impulsions électrique), que l'on mesure en Hertz, et que votre caméra pourra supporter. Ces impulsions sont les images et les voix, que transmet votre caméra à votre enregistreur. Les caméras de surveillance assurent en moyenne un débit de 50 Hertz par seconde, ce débit, programmé par le fabricant, permet la stabilité et la fiabilité du système de votre caméra.

DETECTEUR DE MOUVEMENT : C'est une fonction intelligente qui, grâce à la détection infrarouge (voir I INFRAROUGE) ainsi que la détection de chaleur, analyse l'environnement et se met à filmer dès que la caméra remarque un déplacement.

DVR/ PVR / DIGITAL VIDEO RECORDER / ENREGISTREUR : Enregistreur audio et vidéo, numérique, qui sera relié à votre décodeur (voir B BOX). Il est important de prêter attention à la capacité de votre DVR (Go), car il doit avoir une capacité de stockage adaptée à la quantité d'image que vous voulez stocker. C'est cet enregistreur qui vous permet de visionner à distance vos vidéos

POUCE / " / PO : Le Pouce est une unité de mesure correspondante à 2,54 centimètres.

ZONE DE MASQUE : Prenant la forme d'un carré de couleur sombre, cette zone est paramétrable au niveau des caméras lorsqu'on souhaite cacher une partie de la vidéo. Généralement pour des questions d'intimité.

Contrôle d'accès :

- Actionneurs et capteurs d'un point d'accès Ex. d'actionneurs : automatisme de porte, serrures et gâches électriques, tourniquets, barrières levantes, verrouillage électromagnétique (ventouse). Ex. de capteurs : contacts, contacteurs de porte, détecteurs de présence.
- Alimentation Partie d'un équipement de gestion de contrôle d'accès qui fournit l'énergie pour assurer le fonctionnement du système ou une partie de celui-ci.
- Anti-passback (ou anti-retour), anti-timeback Fonction effectuant une identification de l'utilisateur en entrée puis sortie d'une zone contrôlée afin de lui autoriser de nouveau l'entrée dans cette zone (ex : éviter l'entrée de deux véhicules dans un parking avec un seul véhicule entré). Empêche que l'identifiant ne soit lu deux fois de suite dans le même sens : un identifiant d'entrée ne peut que sortir. Une fonction équivalente est l'anti-timeback : démarrage d'une temporisation après un premier passage de badge pour en éviter un second tout de suite après.
- Authentification Vérification de l'association support et porteur du support (biométrie, code personnel associé à un badge, ...).
- Auto-surveillance à l'ouverture ou à l'arrachement Dispositif d'avertissement en cas d'ouverture frauduleuse (ou arrachement) d'un équipement de gestion de contrôle d'accès.
- Caractéristique biométrique Information qui se réfère à des caractéristiques physiologiques uniques de l'utilisateur. Condition de défaut Toute condition qui génère l'interruption ou la dégradation des fonctions d'un équipement de contrôle d'accès.
- Condition normale Etat dans lequel le système de contrôle d'accès est entièrement fonctionnel et est en mesure de traiter tous les événements dans le respect des règles établies.
- Évènement Information d'un changement d'état apparaissant dans le système de contrôle d'accès.
 - Grille d'accès Une ou plusieurs zones de sécurité contrôlées, allouées à un niveau d'accès.
- Grille de temps Une ou plusieurs zones de temps allouées à un niveau d'accès. • Groupe d'accès Ensemble d'utilisateurs partageant les mêmes droits d'accès.
- Identifiant Données d'identification délivrées par des badges, des cartes d'accès, des clés électroniques, par saisie, ... • Identification Prise en compte d'un identifiant.
- Interface du point d'accès Dispositif qui contrôle l'ouverture et la fermeture d'un point d'accès. 14 • Interphone Dispositif de communication permettant de mettre en relation vocale une personne extérieure et l'occupant d'un bâtiment ou d'une zone. Ce dispositif peut permettre l'ouverture d'une porte.
- Lecteur du point d'accès Dispositif utilisé pour collecter les données d'identification. Ces données sont transmises à l'UTL à distance ou localement. Dans ce dernier cas, lorsque le lecteur est intégré avec l'UTL dans un même boîtier, il est dit autonome.
- Mode dégradé Etat dans lequel l'équipement de gestion de contrôle d'accès est partiellement fonctionnel et est en mesure de traiter tout ou partie des événements dans le respect des règles établies. Ex : réseau de communication hors service, PC hors service, coupure d'alimentation électrique.
- Niveau d'accès Droit d'accès de l'utilisateur donné par une grille d'accès spécifique et, si applicable, par une grille de temps associé.
- Paramétrage Capacité à modifier et à mémoriser la configuration du système.

- Plage horaire Intervalle de temps entre deux moments donnés indiquant le commencement et la fin d'une période valide incluse dans une zone de temps.
- Point d'accès Endroit où l'accès peut être contrôlé : présence d'obstacle physique (porte, tripode, ..). • Portier Nom générique désignant un interphone ou un visiophone.
- RFID Radio frequency identification : technologie de lecture et/ou écriture d'une base de données sans contact (de quelques centimètres à quelques mètres). Cette technologie est principalement utilisée dans la conception de badges de contrôle d'accès.
- Système de contrôle d'accès Ensemble des éléments exigés qui permettent de contrôler un accès : gestion, mesures conceptuelles et organisationnelles, dispositifs divers.
- Traitement Analyse des informations par rapport aux règles préétablies afin de prendre les décisions appropriées (autorisation ou refus d'accès).
- Utilisateur Personne qui demande à passer un point d'accès.
- UTC Unité de Traitement Centralisé de contrôle d'accès. Cette unité de traitement prend la décision de libérer un ou plusieurs points d'accès et gère la séquence de commande associée. Une UTC peut être connectée à une ou plusieurs UTL. Les fonctions des UTC peuvent être réparties entre plusieurs éléments, ou peuvent être intégrées dans un seul boîtier.
- UTL Unité de Traitement Local : Système électronique qui permet d'appliquer la décision provenant de l'UTC. Cette UTL commande un ou deux points d'accès. Une UTL est nécessairement reliée à une UTC. Note : aussi appelé contrôleur d'accès ou gestionnaire de porte.
15 16
- UTS Unité de Traitement de Supervision de contrôle d'accès : Matériel qui assure les fonctions de superviseur pour des UTC et/ou des UTL. Ce matériel assure les fonctions d'interface du point d'accès, de traitement, d'annonce, d'alerte et assure leur alimentation. Note : aussi appelé GAC (Gestion des Accès Contrôlés).
- VIGIK® Marque d'un système d'ouverture des accès aux parties communes des immeubles pour les prestataires de service exclusivement ; il est souvent associé à un système de contrôle d'accès résidents.
- Vidéophone Dispositif de communication permettant de visualiser un visiteur et de dialoguer avec lui. Ce dispositif peut permettre l'ouverture d'une porte.
- Visiophone Dispositif de communication permettant d'établir une relation vocale et visuelle bidirectionnelle entre un visiteur et l'occupant d'un bâtiment. Ce dispositif peut permettre l'ouverture d'une porte.
- Zone de sécurité contrôlée Zone entourée d'une barrière physique comprenant un ou plusieurs points d'accès.
- Zone de temps Une ou plusieurs plages horaires combinées avec des informations calendaires

1.4. Sujétions en milieu occupé

Il est rappelé que les prestations peuvent se dérouler en milieu exploité. Le titulaire doit tenir compte et prévoir toutes les dispositions et aménagements nécessaires pour limiter au maximum les nuisances occasionnées lors des interventions (poussières, bruits...) qui viendraient troubler les activités de soins ou autres tant vis à vis des patients, usagers, résidents que du personnel de l'établissement.

Les indisponibilités de matériel de contrôle d'accès, vidéo protection et/ou anti intrusion des zones impactées par les travaux devront se faire avec l'autorisation du responsable sécurité incendie du site concerné.

1.5. Obligations en matière environnementale

Le titulaire respectera la réglementation en vigueur concernant la récupération, le recyclage ou l'élimination des déchets liés aux prestations de maintenance. Le transport, le stockage, le recyclage ou l'élimination des déchets sont à la charge du titulaire. Ce dernier fournira à l'établissement tous les documents nécessaires justifiant des procédures suivies. Le CHRU se réserve le droit de récupérer tout matériel déposé par le prestataire.

1.6. Amiante et plomb :

Aucun percement ne pourra avoir lieu sans l'accord préalable du conducteur d'opération en charge des travaux.

Les plans d'EXE seront transmis 2 semaines avant les percements à effectuer afin que les DAT puissent être effectués.

1.7. Documents à remettre par le prestataire

Il sera remis au CHRU, à chaque étape du projet (APS, APD, PRO, EXE, DOE, DEM) et à chaque évolution, les plans et documents aux formats papier et informatique. Tous les documents seront en langue Française.

Tout appareil sera présenté et validé par le CHRU avant son installation. La présentation, au choix du CHRU, pourra être écrite (Fiche de présentation fournisseur) et/ou physique (Echantillon complet fonctionnel).

Les plans d'implantation seront réalisés et remis sous formats autocad 2016 et PDF. Ils respecteront la charte DAO du CHU.

Les plans d'armoires seront réalisés et remis sous formats autocad 2016 et PDF. Ils respecteront la charte DAO du CHU. Ils seront réalisés en multifilaires. Tous les fils, câbles, appareils, bornes et borniers seront repérés. Ils respecteront la charte DAO du CHRU.

Il sera remis au CHRU, en phase finale du projet, le DOE (Dossier d'ouvrage exécuté) et le DEM (Dossier d'exploitation et de maintenance) de l'installation (se référer aux documents *Notice DOE* et *Notice DEM* pour plus d'informations). Ils respecteront les chartes CHU.

Les DOE et DEM seront remis en quatre exemplaires, en formats papier et informatique natif (Word, Excel, autocad 2016, etc.).

De manière générale et simplifiée, le DOE regroupe l'ensemble des plans et documents qui ont servi à la réalisation de l'ouvrage, mis à jour et conforme à la réalisation. Le DEM, lui, regroupe un ensemble de documents et de notices permettant l'exploitation et la réalisation de la maintenance des installations.

Les DOE et DEM respecteront les chartes CHU et seront remis en format papier seront mis sous classeurs, lesquels respecteront le code couleur du CHRU, à savoir :

- Bohars : bleu
- Carhaix : marron
- Cavale Blanche : vert
- Delcourt-Ponchelet : orange
- Guilers : noir
- Morvan : rouge
- Annexes : jaune

1.8. Synthèse schéma directeur ssi chru brest

1.9. GMAO/BIM

Tous les appareils installés par les prestataires pourront être ajoutés à la GMAO du CHRU à la demande du CHRU et respecteront la charte BIM.

1.10. Formation du personnel

Si un appareil nécessite une formation particulière pour l'utilisation de l'équipement, celle-ci sera assurée par le titulaire (ou par le constructeur) lors de la mise en service et consignée par écrit auprès du responsable d'exploitation du site concerné. Les formations seront toujours prévues sur deux sessions.

1.11. Cablage

Généralités :

La mise en œuvre du câblage à l'intérieur du bâtiment s'effectuera :

- En colonne montante entre le RDC, les étages et les combles sous Cablofil dédié.
- Sous chemin de câbles Cablofil dédié en sous-sol, combles et faux-plafonds des étages, pour les parcours groupés comportant plus de 5 câbles.

Mise à la terre et équipotentialité :

Mise à la terre des chemins de câbles et liaisons équipotentielle au réseau de terre tous les 15/20 m.

Respect des sections des conducteurs de protections et bornes adaptées.

Mode de pose des chemins de câbles :

Respect des préconisations des constructeurs sur l'emplacement des supports et des éclisses

Courbes et angles droits :

Emplacement des supports de chemin de câbles avant chaque inflexion de chemin de câble

Mettre un support à l'entrée et à la sortie des courbes à angle droits

Pour les coudes de grands rayons, placer un support d'appoint au milieu de la courbe

Compatibilité électromagnétique CEM :

Respect des règles de séparation des câbles énergie et d'information cf. EN 50 174-2

Croiser les différentes familles de chemins de câbles à 90°

Effet joule :

Respect des conditions de pose pour éviter les échauffements de câbles.

Privilégier les chemins de câbles ouverts

Assurer régulièrement un repérage des réseaux de chemins de câbles et câbles SSI

Câblage et parcours des liaisons électriques :

Mise en œuvre:

Il convient de prendre en considération la proximité d'émetteur/récepteur radio, relais téléphonique, transformateur HT, etc., qui peuvent générer des interférences électromagnétiques et perturber le fonctionnement de l'installation.

Les câbles courants faibles doivent être séparés des câbles courants forts. cf. EN 50 174-2

Des supports de canalisation électrique doivent être utilisés sous réserve de proportionner la section des conduits et canalisations pour faciliter la pose et la dépose des câbles. Les chemins de câbles, goulottes et conduits doivent être facilement accessibles.

Lorsqu'exceptionnellement aucun support de canalisation électrique (chemin de câbles, goulottes ou conduits) n'est mis en œuvre (cas des faux-plafonds, par exemple) les câbles doivent être fixés à un élément stable de la construction (en aucun cas, un câblage dit « volant » n'est acceptable).

Chaque fois que possible, ils doivent être placés en torons, ces torons ne doivent être constitués que de câbles courants faibles appartenant au système de sécurité incendie (SSI).

La nature des câbles sera choisie de manière à ce que ni les opérations de leur mise en place, ni les conditions d'environnement des lieux où ils cheminent n'altèrent leurs propriétés mécaniques et électriques selon les dispositions de la partie 5.2 de la norme homologuée NF C 15-100.

Le repérage des câbles doit faciliter les interventions dans un cadre de maintenance (préventive et/ou corrective) et/ou de modification d'installation lors d'une adaptation de celle-ci. Ainsi les câbles du SDI doivent être repérés au niveau des bornes : • de l'E.C.S ;

- des équipements d'alimentation électrique (EAE) ;
- des boîtes de jonctions et/ou de dérivation (voir 6.1).

Le repérage doit résister dans le temps. Sa mise en place doit être telle qu'il soit lisible après connexion aux équipements.

- ✓ Ajustement des seuils de sensibilité des détecteurs en fonction d'un cycle horaire
Offrir une capacité maximale de 128 points de détection.

Une réserve de 20% sera prévue sur chaque SDI.

2. LE DISPOSITIF DE CONTROLES D'ACCES ET ANTI INTRUSION :

2.1. Projets neufs et pérennes :

Classement des locaux :

Les locaux et accès sont classés suivant leur caractère sensible vis-à-vis de la sûreté. Ce classement conditionne les équipements mis en œuvre afin de répondre aux contraintes de résistance mécanique vis-à-vis de l'effraction notamment. Les tableaux de classement des locaux sont génériques mais doivent par la suite être adaptés aux différents projets.

Contrôles d'accès CHRU de Brest
--

1-Environnement matériel Till (automates-modules de portes – lecteurs de badges)

Dans un but de modularité, de flexibilité et d'évolutivité, l'UTL de type TILLYS-NG proposée devra impérativement disposer d'extensions sur des bus déportés type RS485.

Grâce à ces extensions, l'UTL pourra ainsi gérer par bus (jusqu'à 3 bus par UTL) 8 lecteurs, 16 modules, 8 claviers, 8 sirènes, 256 entrées analogiques, 128 sorties relais.

Les modules déportés pour gérer 1 lecteur de badge (MLD1) et pour gérer 2 lecteurs de badges (MLD2) se connectent sur le bus secondaire d'un automate TILLYS-NG.

Les lecteurs de badges seront de la gamme EVOLUTION avec lecture UID non sécurisée.

Les formats des lecteurs proposés doivent correspondre au besoin et à l'environnement du projet : intérieur de type encastrable, extérieur en saillie.

- Evolution IN encastré pour l'intérieur
- Evolution ST pour les extérieurs ou environnement dégradé

Les dispositions de la charte « contrôles d'accès/intrusion au CHRU de Brest » doivent être strictement respectées.

2-Serrures , gâches et ventouses :

2.1 Locaux sensibles et standards :

a) Les locaux dits **sensibles** seront équipés de serrures électriques à fonction sûreté (*) à émission de courant.

Elles ne seront pas asservies au SSI et seront équipées de contact de fond de penne.

Les portes seront équipées de cylindres européens selon l'organigramme en vigueur de l'établissement et de béquilles.

*Les portes des locaux sensibles ou la porte d'accès à un groupe de locaux sensibles seront équipées individuellement

Annexe n° 1 : typologie des locaux sensibles

Annexe n° 2 Cf. Serrures électriques Type 2 : EL 564 ou EL 460 de chez ABLOY

Couleur du point sur plan : rond rose



b) Les locaux dits **standards** :

Les locaux à l'intérieur du bâtiment seront équipés de gâches électriques à émission de courant.

Elles ne seront pas asservies au SSI et seront équipées d'un contact de position de porte type SHD 2.

Les portes seront équipées cylindres européen selon l'organigramme en vigueur de l'établissement et de béquilles.

Annexe n°3 : typologie des locaux standards

Annexe n°4 Cf. gâches électriques CDVI T 290 s avec contacts de position de porte de type SHD 2

Couleur du point sur plan : rond vert



2.2 Divers accès, cheminements et issues de secours

Annexe n° 5 CF. Typologie des accès, issues de secours, cheminements et recoupements

a) Portes battantes en périmètre de bâtiment utilisées en **issues de secours pour le public** :

Ces portes seront équipées de ventouses DAS 500 Kg à fonction sûreté

à rupture de courant associée à un BDM vert double contact ou de bandeau ventouses vertical DAS suivant le modèle de porte.


Elles seront asservies au SSI ;

b) Dans le cas où une porte joue le rôle d'une issue de secours et d'un accès fonctionnel, elle sera équipée d'un contact de position de porte de type SHD 2 et d'un contacteur à clé de dé condamnation associé à l'organigramme des clés du service.

Annexe n° 6 Cf. Ventouse DAS à rupture 500 kg type V5SRB 500 kg 12/24 V DC + relais/signal + buzzer


Annexe n° 7 Cf. Bandeau ventouse vertical DAS à rupture type BO 600 RP 2 x 300 kg ou

Bandeau ventouse vertical DAS à rupture type BO 600 RP 2 x 400 kg

Couleur du point sur plan : rond bleu 

c) Portes de recoupement de circulation : Les portes seront équipées de verrous motorisés DAS de type Alligator DSMCIP 2002-X .Ils seront systématiquement équipées d'une option gâche pour un rattrapage de porte de + ou – 20 mm.

Annexe n°8 Cf. Verrou motorisé IP Alligator DSMCIP 2002-X

Couleur du point sur plan : rond orange 

d) Portes coulissantes en périmétrie de bâtiment : ces portes devront être équipées de verrous électromécaniques à fonction sureté asservis au SSI.

Locaux dits « standards » :

Thématique	Intitulé du local	Fiche produit annexe n°
PCR - ASN		
	stockage propre froid	4
	Accès radio pharmacie	4
	Accès ira thérapie	4
Soins		
	Sanitaires Personnel	4
	Secrétariat	4
	Consultations	4
	Bureau IDE	4
	Préparation des Soins	4
	Salles de soins	4
	Local Vidoir	4
	Salle de pause - Espace Détente	4

Thématique	Intitulé du local	Fiche produit annexe n°
	Personnel	
	Office	4
	Poste infirmier	4
	Réserve matériel	4
	Rangement linge	4
	Rangement divers	4
	stockage	4
	consommables	4
	Reprographie	4
	Brancard - fauteuils	4
	Archives	4
	Local chambres froides - Congélateurs	4
	Retour soins sale	4
Logistique		
	Retour Logistique	4
	Nettoyage	4
	DASRI	4
	Déchets	4
	Décartonage	4

*Suivant la configuration des lieux et portes, les équipements peuvent être adaptés en fonction du projet

Equipements de contrôles d'accès pour les locaux standards :

Fiche produit gâche sans fonction sureté.

- Gâches à émission de courant.
- Elles devront être équipées de béquilles intérieures
- Les portes devront être équipées de contact de position.

T290S Têtière T290 + Gâches S



- **Bornier de raccordement.**
- **Têtière montée.**
- **Symétrique.**
- **Réversible.**
- **Encastrée.**
- **Rouleau réglable.**
- **1 temps ou 2 temps.**
- **Emission ou rupture.**
- **Varistance incorporée (Protection électronique contre l'effet de self).**

- **Dimensions :**
 - Gâche (L x l x P) : 75 x 20,5 x 28 mm.
 - Têtière (L x l x P) : 250 x 25 x 3 mm.
 - Rouleau réglable (tolérance de 4 mm).
- **Alimentation : 12 ou 24 V (selon modèle).**
- **Consommation « Emission » AC/DC :**
 - 12 V AC = 540 mA.
 - 12 V DC = 630 mA.
 - 24 V AC = 315 mA.
 - 24 V DC = 375 mA.
- **Consommation « Rupture » :**
 - 12 V DC = 200 mA.
 - 24 V DC = 100 mA.



F0513000021	T290S7R12	GÂCHE SYMÉTRIQUE + TÊTIÈRE ÉMISSION 1 TEMPS 12 V AC/DC
F0513000017	T290S7R12	GÂCHE SYMÉTRIQUE + TÊTIÈRE RUPTURE 12 V DC
F0513000026	T290S7R24	GÂCHE SYMÉTRIQUE + TÊTIÈRE RUPTURE 24 V DC
F0513000025	T290S7R12	GÂCHE SYMÉTRIQUE + TÊTIÈRE ÉMISSION 2 TEMPS 12 V AC/DC
F0513000027	T290S7R24	GÂCHE SYMÉTRIQUE + TÊTIÈRE ÉMISSION 2 TEMPS 24 V AC/DC
F0513000011	T290S7R12	GÂCHE SYMÉTRIQUE + TÊTIÈRE ÉMISSION 2 TEMPS 12 V AC/DC ¹
F0513000024	T290S7R12	GÂCHE SYMÉTRIQUE + TÊTIÈRE ÉMISSION 1 TEMPS 12 V AC/DC ¹
F0513000023	T290S7R12	GÂCHE SYMÉTRIQUE + TÊTIÈRE ÉMISSION 2 TEMPS 12 V AC/DC ^{1,3}
F0513000016	T290S7R12	GÂCHE SYMÉTRIQUE + TÊTIÈRE ÉMISSION 2 TEMPS 12 V AC/DC ^{1,3}

¹ Voir conditions de garantie à vie brulée.
² Établissement Sacrément du Public.

1 - Contact électronique
2 - Contact électronique invisible
3 - Levier de déblocage manuel
4 - Contact position pleine

Fiche produit de contact de porte pour les gâches électriques sans fonction « sureté ».



Locaux dits « sensibles » :

Thématique	Intitulé du local	Fiche produit annexe
Technique		
	Poste haute tension	2
	Local Enedis	2
	TGBT	2
	Local onduleur/ASI	2
	TGS TGO	2
	Transformateur	2
	LT CTA	2
	Fluides médicaux et compresseurs FM	2
	chaufferie	2
	sous station	2
	groupe froid	2
	SSI	2
	SRI	2
	VDI	2
	Autocommutateur	2
	local valise	2
	local pneumatique	2
	surpresseurs eau	2
	gare automates	2
	Local technique turbine pneumatique	2
Biomédical et Fluides médicaux		

	stockage FM	2
	local surpresseur ou compresseur FM	2
	local armoire de distribution secours FM	2
	Stockage Biomédical	2
PCR-ASN		
	stockage source PCR haute activité curiethérapie	2
	SAS de curiethérapie source haute activité	2
	Stockage sources scellées	2
	local réception colis Médecine nucléaire	2
	Local cuves radioactives	2
	Réception chaud	2
	salle dosimétrie	2
	déchet chambre décroissance	2
	Accès pharmacie cytostatiques	2
Organisationnel		
	Salle cellule de crise plan d'urgence	2
	Direction	2
	secrétariat direction	2
	PC sécurité	2
Soins		
	Pharmacie	2
	vestiaires	2
	stockage endoscope	2
	déconta endoscope	2
	Accès blocs opératoires	2
	Accès secteur stérile	2

Divers		
	Parking vélo personnel	

Equipements de contrôles d'accès pour les locaux sensibles :



TYPE 2

Serrure électrique à contrôle de béquille
Entrée contrôlée - sortie libre
Série EL564 (porte pleine) et EL460 (porte vitrée)

PRINCIPE DE FONCTIONNEMENT :

- Reverrouillage automatique
- Sortie libre par béquille intérieure.
- Entrée contrôlée par le système de contrôle d'accès
- Porte fermée, la béquille extérieure est inactive (débrayée)

AVANTAGES :

- Sortie toujours libre
- Verrouillage automatique : porte claquée = porte verrouillée
- Compatible avec tous les systèmes de contrôle d'accès.
- En cas de panne électrique, le niveau de sûreté est conservé. La porte reste fermée, avec possibilité d'entrée à la clé et de sortie d'urgence par béquille intérieure.
- Serrure complètement paramétrable, facilitant la maintenance : 12 ou 24V, droite/gauche, poussant/tirant, émission/rupture.
- Puissant verrouillage avec résistance des pènes jusqu'à 1 tonne.
- Conçue pour des portes à passage fréquent (100 ouvertures/jour)
- Disponible en version applique ou à encastrer
- Disponible en version mono ou multipoints
- Apte à équiper les portes coupe-feu
- Apte à équiper les voies d'évacuation EN179 et en conformité avec le Code du Travail et la réglementation Incendie



APPLICATIONS :

- Etablissement Recevant du Public ou des Travailleurs (ERP/ERT)
- Portes à passage fréquent
- Locaux à sécuriser : entrées de plateaux, portes de bureaux, locaux techniques,...

EQUIPEMENT A PREVOIR :

- Un demi-cylindre profil européen
- Une paire de béquille sur rosace ou plaque (ensemble monobloc à vis traversante)
- Un passe-câble
- Un ferme-porte
- Pour mise en applique, kit SLIM'ATIC



ADIA ABLOY Côté France

Régie Inter-Blue Alaparcoury Richet - 30460 Cusset-Montpel • Tél : 03 83 82 61 00 • Fax : 03 83 82 61 07 • Web : abloy.fr
 Adresse postale : CS 80381 - 30038 Nîmes Cedex 3 • 06 89 00 00 00 • 06 89 00 00 00 • 06 89 00 00 00 • 06 89 00 00 00 • 06 89 00 00 00 • 06 89 00 00 00

Accès, issues de secours, cheminements et recoupements :

Thématique	Intitulé	Fiche produit annexe n°
Divers accès		
	Porte de recoupement de circulation	8
	escalier de secours	6 ou 7
	portes coulissantes d'entrée en périmétrie de bâtiment	verrou électromécanique de sureté
	entrée personnel battante	6 ou 7
	issue de secours battante	6 ou 7

Equipements de contrôle d'accès pour issues de secours, portes de recoupements :

Ventouse DAS à rupture 500 kg type V5SRB 500 kg 12/24 V DC + relais/signal + buzzer



Fiche produit de contact de porte pour les gâches électriques sans fonction « sureté »

Contacteur à clé encastré



Fiche produit de contact de porte pour les gâches électriques sans fonction « sureté »



ANNEXE N° 8 – Portes de recouplement en va et vient

**GESTION DES ISSUES DE SECOURS**





Verrou motorisé IP
DSMCIP 2002-X

Verrou motorisé pour issues de secours conforme à la norme NF S 61-937

Matériel préconisé pour :

- tous types de porte à 2 vantaux,
- une utilisation intensive, même sur **porte va et vient montée sur pivot** ou sur double charnière à ressort (rénovation),
- les portes lourdes nécessitant un rattrapage de positionnement,
- les établissements nécessitant un mode sûreté hors présence des personnes.



Caractéristiques fonctionnelles

- Verrou à pènes rétractables, motorisé **3 états** à sécurité positive de haut de porte (sécurité, attente, sûreté).
- Visualisation externe par leds des différents états du verrou
- Montage sans empiètement dans le dégagement de la porte
- Rattrapage de porte : $\pm 10\text{mm}$ - Option W de gâche pour un rattrapage de $\pm 20\text{mm}$
- Entrée de commande pour le contrôle d'accès
- Sortie d'état via relais programmables (sécurité, attente, sûreté, défaut, position des vantaux)
- Verrou entièrement programmable par liaison série via protocole JBUS
- Liaison série vers déclencheur manuel Alligator
- Compatible fonction UGCIS
- Voie de communication Ethernet TCP/IP (prise RJ45) : nous consulter
- Conforme à la norme NF S 61-937
- N° PV : DA 93 01 03

Caractéristiques électriques

	24V	48V
• Sécurité :	150 mA	90 mA
• Attente :	200 mA	125 mA
• En limitation :	620 mA	350 mA

• Tension d'alimentation à sélection automatique (fonctionnement et télécommande) : 24 et 48 Vcc + 20 % / - 15 %

Caractéristiques mécaniques

- Indice de protection : IP 42
- Châssis : acier traité et inox
- Capot : tôle alu couleur RAL 9010
- Dimensions L x H x P :
 - verrou : 426 x 65 x 85 mm
 - gâche : 178 x 40 x 85 mm (x2)
- Poids : 7 kg

Document non contractuel, susceptible de modifications

www.alligator-sas.fr**Contact : 01 60 13 54 70**

2.2. Philosophie générale du process de gestion et supervision des contrôles d'accès

Ce document a pour but de définir le système de sûreté recherché dont les caractéristiques correspondent à une approche cohérente et intégrée de la sûreté avec la mise en œuvre des fonctions de Contrôle d'Accès, de Détection Intrusion et de supervision graphique globale. Il indique également la philosophie et les différentes règles de programmation à mettre en œuvre sur les différents sites du CHRU de Brest.

Les objectifs principaux de la mise en place du dispositif de sûreté du site sont :

- De contrôler et filtrer le flux de personnes (permanents, temporaires et visiteurs) en gérant les accès (contrôle d'accès),
- De détecter la pénétration des personnes indésirables sur le site (détection intrusion),
- D'apporter les informations souhaitées aux différentes personnes en charge de la sûreté (responsable sécurité, agents de sécurité, DSI) grâce à un système de supervision globale unique et cohérent
- D'acquérir et d'exploiter dans cette supervision globale un ensemble d'informations ou d'alarmes provenant d'autres dispositifs de sécurité ou techniques (vidéosurveillance, système CVC, G.T.B., système incendie, etc...).

Le système installé permet une exploitation simple et conviviale, alliant pérennité et évolution.

Pour cela, le fournisseur du système TIL TECHNOLOGIES est également le développeur et le concepteur tant sur la partie logicielle que matériel.

Le logiciel retenu et installé est Micro-Sésame

2.3. Qualité du système

- **Compatibilité ascendante** : Le constructeur du système respecte une politique de compatibilité ascendante de ses produits sur au moins 10 ans pour garantir la pérennité de l'investissement.
- **Indépendance** : La solution proposée permet d'être installée par des installateurs différents du concepteur de la solution afin de proposer au client un véritable choix sur les prestations (installation, maintenance, support)
- **Convivialité** : Le système permet de superviser le contrôle d'accès, l'intrusion et la vidéosurveillance à partir d'un poste unique disposant d'une interface graphique conviviale.
- **Ouverture** : Le système est compatible avec toutes les technologies d'identification (badges, biométrie, lecture de plaques minéralogiques, etc...). Il permet également de gérer les alarmes techniques et de superviser des automates et autres équipements techniques en protocole MODBUS RTU ou OPC/DA. Le système dispose également d'outils d'importation des usagers par toutes les interfaces suivantes :

Fichiers type csv
API type web service

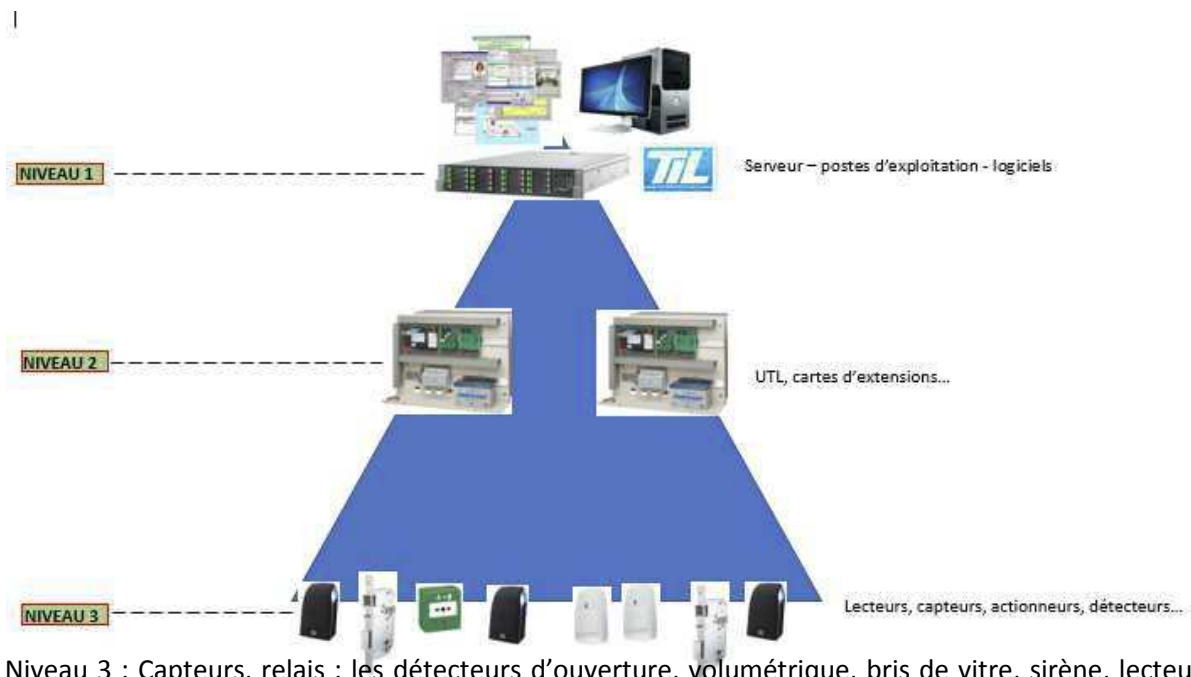
- **Flexibilité** : Le système dispose des fonctions de sécurité avancée (anti-retour, contrôle renforcé, code sous contrainte, etc...). Il possède également une capacité de programmation pour permettre la mise en œuvre d'automatismes adaptés à chaque site. Ces automatismes peuvent avoir un caractère permanent ou conditionnel (par exemple : gestion de mode crise, etc...).

- **Modularité** : Le système fonctionne avec une gestion multisites (Morvan, La Cavale Blanche...). Les fonctions de gestion des accès, de gestion de la détection intrusion, d'animation des synoptiques, sont propres à chaque site et sont accessibles en fonction des utilisateurs et de leurs droits
- **Maintenabilité** : Le système permet une gestion intelligente de la maintenance (envoi d'emails, télé-maintenance, filtres dans les historiques etc...).
- **Intégration horizontale et verticale** : Des interfaces ou passerelles vers d'autres systèmes (incendie, G.T.B.) peuvent être mise en place pour une meilleure intégration des fonctions de sûreté / sécurité.

2.4. Environnement matériel

Architecture réseau :

Le système installé à une architecture logicielle Client / Serveur. Le poste serveur est raccordé sur le réseau de type Ethernet TCP/IP du CHRU (Vlan spécifique). Il supervise le dialogue avec les centrales et les postes clients raccordés sur le réseau et dispose d'une capacité de stockage mémoire permettant le bon fonctionnement des applications. Les postes clients et automates (UTL) sont raccordés directement sur le réseau Ethernet du CHRU permettant un dialogue direct entre tous les organes du système.



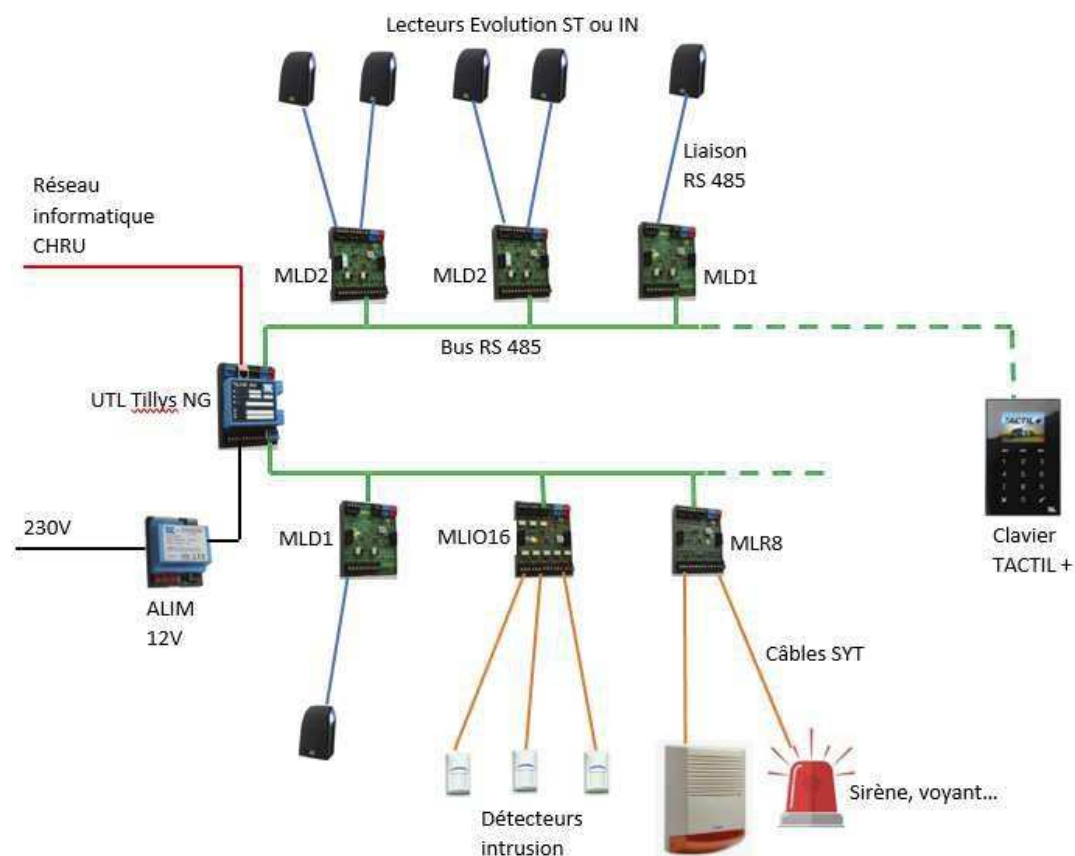
Niveau 3 : Capteurs, relais : les détecteurs d'ouverture, volumétrique, bris de vitre, sirène, lecteurs de badges, autres,

Niveau 2 : Automates de terrain sur réseau Ethernet : ici les Unités de Traitement Locales des informations et / ou les centrales d'alarmes,

Niveau 1 : Système de supervision Serveur et les postes clients éventuels.

Dans une logique de sécurité sans faille, protéger l'accès au bâtiment ne suffit pas. Il est également important de mettre en place des mécanismes pour sécuriser le système lui-même.

Sur toute l'architecture MICRO-SESAME, du badge jusqu'au serveur, des protections électroniques et informatiques sont mises en œuvre pour prévenir les malveillances ou le piratage.



2.5. Architecture matérielle

Les lecteurs de badges et autres accessoires (détecteurs intrusion, etc...) seront raccordés sur des modules déportés, eux-mêmes raccordés aux UTL par des bus de terrain RS485 pour une plus grande liberté de câblage.

Pour limiter les contraintes et réduire le câblage, chacun des bus RS485 aura obligatoirement une topologie ouverte (étoile, en bus ou en toile d'araignée) et une longueur jusqu'à 600 m.

Le principe d'architecture à respecter est le suivant :



Toutefois, afin de faciliter la maintenance du système et la simplicité des câblages, il est fortement conseillé de concentrer le matériel (UTL et cartes) dans un coffret centralisateur situé au centre de la zone à couvrir dans un local technique (SRI...).

2.6. Matériel

Les Unités de Traitement Local (UTL) en Contrôle d'Accès et Intrusion

Les UTL proposées seront de type TILLYS NG. 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.



Les capacités de base :

De base, les capacités minimums des UTL sont :

- 1 Prise RJ45 10/100 Mb auto-adaptatif native pour réseau Ethernet.
- 3 entrées équilibrées libres de paramétrage (défauts alimentation, auto-protection, accès, intrusion, GTB, divers).
- 10 000 événements mémorisés (historique) et horodatés par l'horloge de l'UTL mise à jour régulièrement par le serveur du système.
- 32 groupes de points intrusion.
- Paramétrage de la configuration IP à travers un Web serveur embarqué sécurisé HTTPS, SSH.
- 1 à 3 bus RS485 pour modules déportés selon les capacités à gérer ayant obligatoirement une topologie de câblage ouverte (bus, étoile, toile d'araignée) et une longueur jusqu'à 600 mètres.
- T : -10°C à + 55°C, alimentation de 10 à 28 Vdc, bornier débrochable.
- Entrées universelle paramétrables : TOR, comptage, équilibrée 4 états ou 5 états, signalisation d'état par LED sur chaque bus, réseau, alim, entrée

Elles assurent :

- La gestion combinée du Contrôle d'Accès et de l'Intrusion.
- L'acquisition d'entrées logiques Tout ou Rien ou équilibrées avec surveillance de lignes, et analogiques permettant la gestion des points de détection de l'installation : volumétriques, contacts d'ouvertures, bris de vitres, etc...
- L'acquisition et la gestion locale des données et commandes nécessaires au contrôle d'accès permettant la gestion de lecteurs de badges.
- La commande sous forme de sorties logiques à relais ou transistors permettant de commander des serrures électriques.
- La mémorisation et l'horodatage des événements, avec restitution « au fil de l'eau »
- La remontée des informations de panne ou de malveillance : arrachement, ouverture de coffret, défaut de communication et d'alimentation (secteur, batterie basse, chargeur)

Le fonctionnement en mode dégradé, haute disponibilité :

Les UTL et claviers doivent fonctionner de manière autonome en mode normal comme en mode dégradé sans réseau Ethernet et/ou serveur.

Les autorisations de passage, anti-retour, gestion de plages horaires, les détections & asservissements intrusions (ex : sirène sur alarme), les fonctionnalités aux claviers déportés, le stockage des informations et événements, le partage d'informations seront assurés même en cas de déconnexion du réseau Ethernet.

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

Les UTL peuvent également dialoguer directement entre elles, sur le ou la partie du réseau Ethernet restant fonctionnelle, pour assurer les interactions, asservissements, gestion anti-retour, ou fonctions réparties sur plusieurs UTL. Il est primordial d'avoir la meilleure continuité opérationnelle possible en l'absence de serveur et/ou d'une partie du réseau Ethernet (ex WAN inter-sites si le serveur se trouve sur un autre site).

Communication :

Toutes les communications IP et RS485 seront avec signe de vie pour informer d'un éventuel défaut de communication

Les UTL seront natives IP c'est-à-dire raccordées directement sur le réseau informatique Ethernet (sans convertisseur intermédiaire).

Les échanges de données entre UTL et le serveur se feront par des trames UDP afin d'optimiser les échanges et l'encombrement du réseau informatique.

Les UTL devront pouvoir s'adapter dans un maximum de configurations réseau grâce aux fonctionnalités suivantes qu'elles doivent permettre :

- Auto-négociables (configuration automatique en fonction de la vitesse du réseau, de 10 à 100 Mb/s),
- Auto-MDI (configuration automatique en fonction du type de câble réseau : droit ou croisé),
- IPv4, IPv6
- Adresse IP fixe ou DHCP
- Compatible serveur radius 802.1x

2.7. Les modules déportés (RS485)

Les capacités avec extension :

Dans un but de modularité, de flexibilité et d'évolutivité, l'UTL TILLYS NG dispose d'extensions sur des bus déportés type RS485. Ces extensions ont la forme de modules montables sur rail DIN pour intégration dans un coffret alimenté (solution préférée), ou disponibles sous la forme de boîtiers muraux téléalimentés.

Grâce à ces extensions, l'UTL pourra ainsi gérer jusqu'à :

- 24 claviers déportés d'exploitation de la détection intrusion
- 24 lecteurs ou lecteurs/clavier de contrôle d'accès
- 768 entrées équilibrées
- 368 sorties relais
- 32 entrées analogiques,

Gamme standard : Liste des modules disponibles :

MODULE MLD1 : Module Déporté pour gérer un lecteur de badge pour 1 porte en entrée :

- 1 entrée lecteur RS485 ou dataclock/wiegand.
- 2 entrées TOR (libre de paramétrage).
- 3 entrées équilibrées (libre de paramétrage).
- 1 sortie relais avec choix entre NO/NF et supportant une charge de 2A sous 24vdc minimum.
- 1 sortie transistor, 1 buzzer.

MODULE MLD2 : Module Déporté pour gérer 2 lecteurs de badge pour 2 Portes en entrée ou 1 porte en entrée/sortie :

- 2 entrées lecteur RS485 ou dataclock/wiegand,

- 2 entrées TOR (libre de paramétrage),
- 3 entrées équilibrées (libre de paramétrage),
- 2 sorties relais avec choix entre NO/NF et supportant une charge de 2A sous 24vdc minimum.
- 1 sortie transistor, 1 buzzer,



MODULE E/S MLIO16 : Module déporté pour gérer 16 entrées et/ou sorties :

- 8 entrées équilibrées (libre de paramétrage),
- 8 points à configurer individuellement en entrées ou sorties transistor de puissance 150 mA



MODULE 8 RELAIS MLR8 :

- 8 sorties relais NO et NF, 2A maxi, 48V maxi, 60 W maximum



MODULE ML-EQUILOCK permettant la communication de 2 bus (étoile, toile d'araignée et d'une longueur jusqu'à 300 mètres) avec des transpondeurs intégrés dans les radars intrusion :

- 2 bus de 32 détecteurs (300m) soit 64 adresses au total
- 2 sorties relais bi-stable avec switch NO et NF, 2A maxi, 48V maxi, 60W maxi



Les claviers déportés :

Des claviers déportés avec afficheur seront mis en place afin de permettre la gestion des fonctions intrusion (directement sur le clavier) :

- Utilisation autorisée par un code personnalisé par utilisateur
- Mises En / Hors surveillance du système de détection intrusion
- Gestion des zones (groupes de points) autorisées par utilisateur
- Consultation des alarmes en temps réel
- Consultation des défauts secteurs et batteries basses
- Arrêt sirènes
- Éjection manuelle des points autorisés et en alarme
- Consultation de l'historique (derniers événements)

Ces claviers seront raccordés directement sur l'un des bus RS485 de l'UTL.



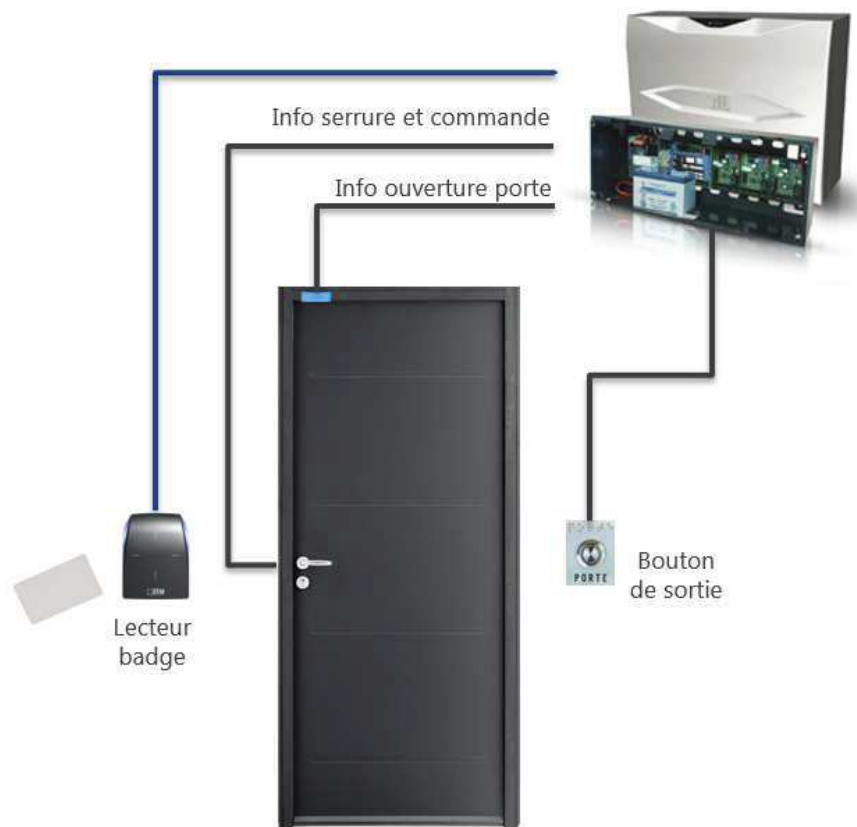
Le clavier TACTIL+ peut intégrer un lecteur de badge embarqué permettant de gérer les systèmes intrusion par badge ou code.

Nota : En aucun cas un lecteur EVOLUTION KB avec clavier intégré (lecteur/clavier) ne peut servir d'organe de mise en service pour l'intrusion. Ce matériel n'est utilisé que pour une notion de contrôle d'accès renforcé. La fonction clavier de ce matériel ne peut être gérée indépendamment du badgeage.

2.8. L'environnement de la porte

Sur une porte contrôlée en accès, on doit retrouver les éléments suivants :

- 1 lecteur de badge Evolution pour l'ouverture
- La béquille (poignée, barre anti-panique) permettant d'ouvrir la porte librement en sortie (gâche) ou 1 bouton de sortie (ventouse). Le bouton doit impérativement être raccordé sur une entrée du système afin de remonter l'information au système pour inhiber le contact de porte en sortie.
- 1 contact donnant l'état de la porte (magnétique ou information disponible dans la serrure) pour remonter l'état de la porte à la supervision et gérer l'intrusion
- 1 commande de gâche ou serrure
- Si la porte est équipée d'une ventouse il est obligatoire d'installer un déclencheur manuel vert pour permettre une sortie d'urgence. Ce dernier doit obligatoirement être à double contact afin de remonter l'information au système.



Le système étant supervisé, il est impératif de remonter l'état de toutes les portes contrôlées afin de connaître à tout moment leur position (ouverte ou fermée, POTL). La mise en place de contacts d'ouverture sur les portes équipées en accès est donc obligatoire.

Câblages :

- Le type de câble à utiliser pour le lecteur de badge (liaison RS485) et obligatoirement du câble à paire torsadé de catégorie 5 minimum
- Le type de câble à utiliser pour l'équipement de la porte (contact, serrure, Bp...) est obligatoirement de type SYT1 ou TRANXALARM en 2, 3, ou 5 paires (6 ou 9/10èmes)

Boutons poussoirs de sortie :

Il existe 2 configurations :

- Porte équipée d'une serrure permettant la sortie libre par béquille ou barre anti-panique (serrure Eff-Eff, Abloy ou gâche...) dans ce cas on récupérera l'information de sortie dans la serrure.
- Porte ne permettant pas la sortie libre (ventouse, gâche avec poignées palières...) dans ce cas, la pose d'un bouton de sortie est obligatoire (associée à un BBG vert pour une issue de

secours). Les types de boutons à prévoir sont de type poussoir NO ou NF, en plastique ou métallique anti- vandale selon la configuration.



BBG Vert (bris de glace) :

Afin de respecter la conformité à la norme EN 54-11 et la NFS61-936 concernant les issues de secours, si la serrure ne dispose pas d'organe de sortie libre, cette dernière doit impérativement être équipée d'un déclencheur manuel de couleur verte permettant la sortie d'urgence. Le BBG devra être fixé à 1.3m par rapport au sol.

Il comportera impérativement deux contacts :

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



Nota : Seul un boîtier bris de glace vert est conforme pour une issue de secours ou un déverrouillage car il coupe directement son alimentation.

Un boîtier bris de glace rouge ne coupe pas l'alimentation de la porte directement et ne sert qu'à déclencher l'alarme incendie. Après son déclenchement, c'est le système incendie qui renvoie une information au système de contrôle d'accès pour éventuellement déverrouiller certaines portes.

Les boîtiers BDM et ci-dessous sont recommandés pour les zones publiques où l'activation du BDM peut être particulièrement contraignante pour le personnel.

Déclencheur manuel vert 2 contacts avec capot + buzzer et led / déverrouillage d'issue de secours :



Détecteur d'Ouverture porte (DO)

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. Ceci afin de contrôler, superviser l'état de la porte et déclencher les alarmes type « effraction porte » et « porte ouverte trop longtemps »

S'ils ne sont pas intégrés à la serrure, ils seront de type magnétique (PVC ou métallique) et NFA2P.



Montage et raccordement des automates et modules déportés :

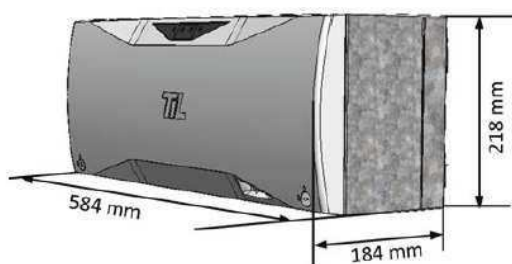
Les UTL et les modules d'extension se fixent sur rail DIN dans une armoire ou coffret spécifique à alimenter en 220 V. Ces coffrets seront répartis dans les locaux techniques courants dans le bâtiment, à proximité des chemins de câbles.

Les coffrets seront obligatoirement protégés par un contact d'autoprotection.

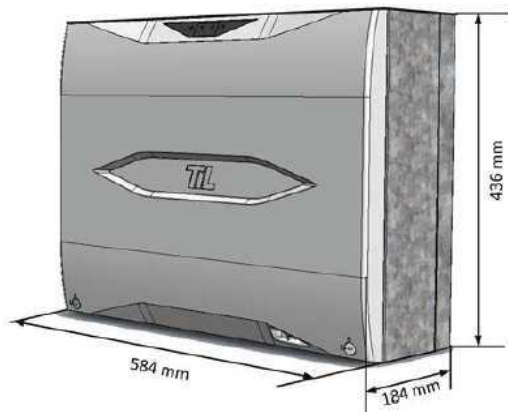
Le coffret intégrant l'UTL disposera de :

- Rails DIN permettant la fixation de l'UTL, l'alimentation et des modules d'extension,
- Goulottes pour l'organisation des câblages
- 1 contact d'autoprotection pour avoir une alarme à l'ouverture
- 1 bornier sectionnable pour le raccordement du secteur 220 V monophasé Une dimension suffisante pour y loger une batterie entre 7 et 24 AH
- Un lien RJ45 pour la mise en réseau de l'automate

Coffret 1 rangée équipé d'un rail DIN :



Coffret 2 rangées équipé de 2 rails DIN :



Vue intérieur d'un coffret 2 rangées



Si le coffret se révélait trop petit par rapport à l'équipement de la zone concernée, il sera mis en place dans un local technique un coffret 1000x1000 double porte pouvant accueillir un automate, plusieurs alimentations et les modules d'extension de 3 bus (soit 32 modules, automate et alimentations comprise).



Le coffret sera de type 1000x1000x300 de chez E.T.A avec les caractéristiques suivantes :



CARACTERISTIQUES

Coffret et porte en tôle d'acier épaisseur 1,5 mm.
Plaque de montage en tôle d'acier épaisseur 2,5 mm avec bords pliés.

PEINTURE

Epoxy polyester cycle standard ETA.
Couleur: RAL 7035 texturée.

COMPOSITION

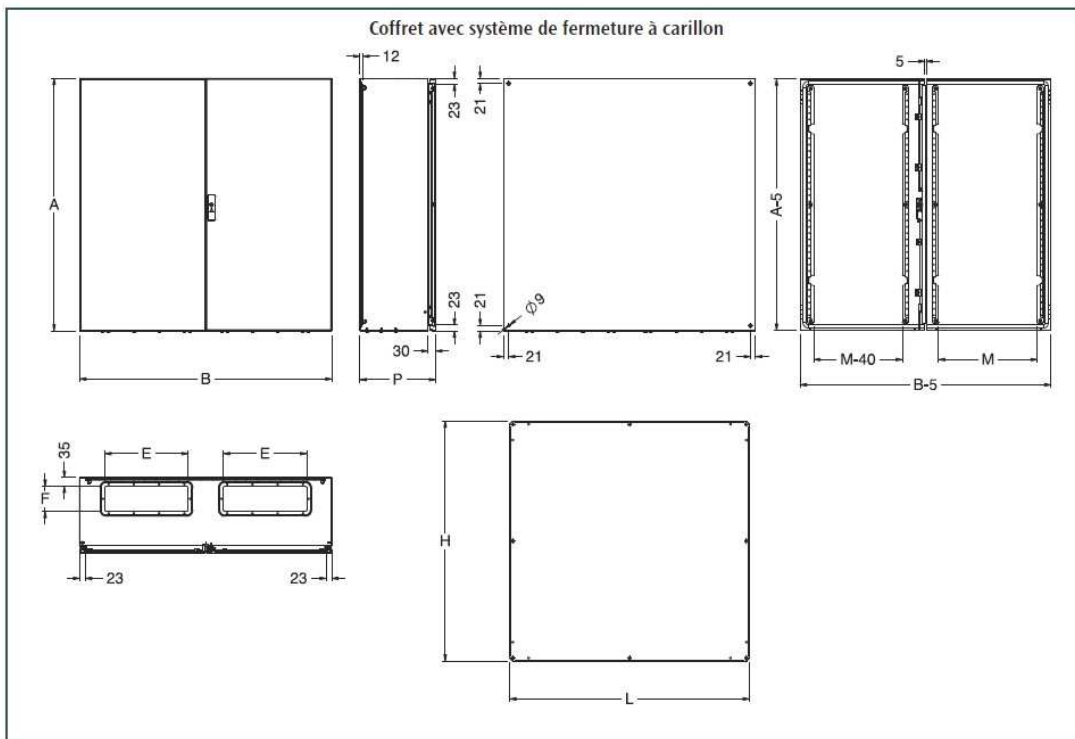
Le coffret comprend:

- logement
- 4 rails électrozingués à fixer sur la porte
- plaque de montage
- 2 plaques pour presse-étoupe avec joint d'étanchéité
- vis pour mise à la terre et accessoires de montage
- porte avec de fermeture à double ailette, ø 3 mm.

INDICE DE PROTECTION

- IP 66 conformément à la norme IEC EN62208; EN60529
- NEMA 12 conformément à la norme UL508A; UL50
- degré de protection garanti par le joint en résine polyurethane bi-composante
- degré de résistance au choc IK10 conformément à la norme IEC EN62208; EN62202.

Note: Principaux accessoires à commander séparément: pattes pour montage mural, voir page 170



2.9. Les lecteurs de badges

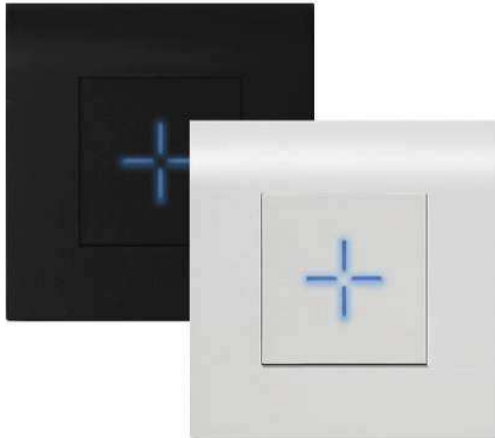
Les lecteurs de badges préconisés pour le CHRU seront impérativement de la gamme « Evolution ». Deux modèles ont été retenus.

Le lecteur EVOLUTION ST (saillie intérieur ou extérieur) est un lecteur sans contact multi-protocole et entièrement programmable. Il sait lire l'ensemble des identifiants de la famille Mifare® : Ultralight, Ultralight C, Mifare Classic, Mifare Plus, DESFire et DESFire EV1.



Le lecteur EVOLUTION IN (encastrable) possède les mêmes caractéristiques que l'Evolution ST mais il est spécialement conçu pour s'intégrer dans les boîtes d'encastrement électriques, son

capot standard peut être remplacé par n'importe quel cache ARNOULD ESPACE ou LEGRAND MOSAIC.



Caractéristiques techniques :

- Alimentation : 7 à 28 VDC
- Consommation moyenne : 100 mA
- Fréquence / Identifiants : 13.56 MHz - ISO14443 A & B, ISO18092 (NFC).
Puces MIFARE® Ultralight & Ultralight C, MIFARE Classic, MIFARE Plus, MIFARE DESFire EV1 & EV2, NFC, SMART MX, CPS3, Moneo, iCLASS, PicoPass
- Distance max. entre le module et le lecteur : 100 m (Wiegand/Dataclock) à 600 m (RS485) Interface de communication : Data/clock ISO2, Wiegand ou RS485 crypté AES128
- Connectique : Bornier débrochable 10 points
- Protection : Détection de l'arrachement par accéléromètre + possibilité d'effacement des clefs Distance de lecture : Jusqu'à 8 cm avec un badge Mifare Classic et 6 cm avec un badge Desfire EV1, sur tout type de support y compris métal, sans entretoise
- Signalisation paramétrable :
 - 2 LEDs RVB pilotables - 360 coul. Programmables par badge
 - Buzzer intégré (pilotable avec automates NG / V3 uniquement)
- Résistance / étanchéité : IK10 (hors capteur biométrique), IP65 (hors connectique)
- Température de fonctionnement : -20°C à +70°C ou -10°C à +50°C si capteur biométrique

Précaution d'installation :

Les lecteurs ne devront pas être fixés directement sur une surface en inox ou métallique (forte diminution de la distance de lecture). Dans les situations qui l'imposaient (surtout inox), il faudra informer le client, et procéder à des tests au préalable. Le cas échéant, des entretoises (cales PVC) seront à prévoir entre le lecteur et le mur.

Respecter une distance de 20 à 30 cm entre 2 lecteurs sur un même plan ou dos à dos sur une même cloison.

3. ENVIRONNEMENT INFORMATIQUE & LOGICIEL

3.1. Le poste serveur

Le poste serveur est raccordé sur le réseau de type Ethernet TCP/IP du CHRU Brest. Il supervise le dialogue avec les centrales et les postes clients raccordés sur le même réseau.

Le logiciel de contrôle d'accès, intrusion et supervision est installé sur ce poste, permettant à la fois de paramétrer, d'exploiter les badges et de visualiser des alarmes, défauts et états de fonctionnement du système sur des vues IHM représentant les plans du bâtiment par niveaux et par zones.

Le Serveur MICRO-SESAME fonctionne sous Windows 2016 Server (64 bits). Il met en œuvre plusieurs programmes spécifiques fonctionnant 24H/24 :

- La scrutation : C'est le noyau de l'application. Elle assure les échanges entre les équipements de terrain et la base de données.
- Le Master Agent, les services et applications surveillées par le Master Agent.
- Les pilotes chargés de la communication avec chaque type de matériels.

Le serveur héberge la base de données et son moteur relationnel (SQL Server 2016). Les services de la base de données ne doivent pas être arrêtés tant que l'application MICRO-SESAME est en fonctionnement.

Configuration du serveur :

- Serveur Rack 1U type DELL POWEREDGER330
- Windows server 2016 R2 Standard Edition
- Base de données SQL Serveur 2016 standard
- Processeurs 2 x Intel Xeon E3-1220V6/3 GHz
- Disques durs enfichables à chaud
- Blocs d'alimentation redondants enfichables à chaud
- RAM 32 Go DDR4
- Disques : 1 DD système, 1 DD temp, 3 DD de 1 To SATA en RAID 5
- 2 Cartes réseau Ethernet PCI Gigabits
- Clavier, souris
- 2 à 4 ports USB
- Garantie 3 ans sur site J+1.

Une sauvegarde automatique et périodique de la base de données est effectuée sur le serveur et sur un serveur annexe (au service informatique du CHRU). Le logiciel Micro-Sésame permet de définir et de paramétrer la date, l'heure, le chemin et la fréquence des sauvegardes.

Cette sauvegarde est un Backup complet de l'installation, permettant en cas de défaillance de recharger l'application en cours avec sa programmation et la base de données complète.

3.2. Les postes clients

Le ou les postes clients seront raccordés sur le même réseau sûreté que le poste serveur. Ils ont les mêmes capacités de gestion que le poste serveur.

Configuration typique pour le poste client d'une installation moyenne :

- Micro-ordinateur compatible PC type i3 (3 GHz),
- Carte Ethernet 1000/100 Mb/s,
- 4 Go de RAM,
- Disque dur 100 Go minimum,
- 1 lecteur DVD (pour l'installation du logiciel),
- Ecran plat TFT 24", résolution 1280 x 1024 au minimum,
- Clavier, souris, Windows 7, 8 et 10 Professional 64 bits
- 1 port série au minimum,
- 2 ports USB,
- Licence client Microsoft SQL.

L'applicatif Micro-Sésame peut également être hébergé sur un poste du CHRU après installation du logiciel comme poste client lourd (nécessité d'avoir 1 licence poste client disponible).

3.3. Configuration réseau

Tous les éléments constituant le réseau de sûreté du CHRU (Serveur, poste client, automate...) sont à raccorder sur les Switchs des baies informatiques du client. Il est nécessaire pour cela de définir les besoins et les points de branchements avec le SI (Service Informatique) du CHRU. L'installateur devra prévoir les liaisons RJ45 de chaque UTL vers les éléments actifs du CHRU en réalisant un cheminement des câbles tenant compte des contraintes liées au réseau Ethernet (distance, etc...).

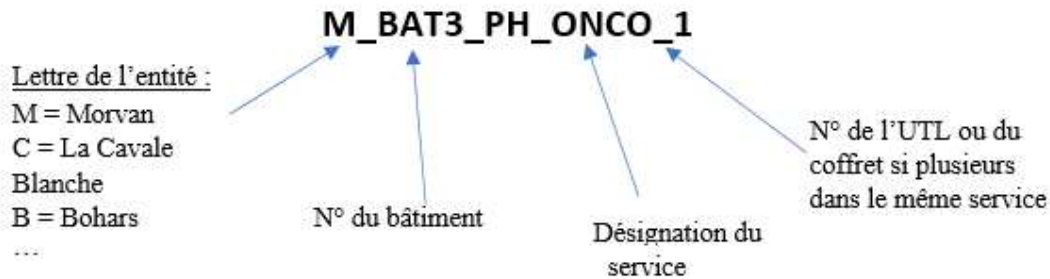
Tous ces éléments actifs seront obligatoirement configurés en DHCP sur le réseau informatique et non en IP fixe. Par défaut, chaque UTL à un nom déjà créé par le fabricant qu'il faut relever afin que le service informatique du CHRU puisse le retrouver aisément et le paramétrer sur le réseau.

En retour, le service informatique transmettra l'adresse IP exact du module sur le réseau (pour le paramétrage dans Micro-Sésame).

Il est à préciser au service informatique qu'il s'agit de matériel de contrôle d'accès et par conséquent, les IP ne doivent pas changer dans le temps (au risque d'une perte de communication) ; elles doivent être figées.

Demande de raccordement avec le service informatique :

- Relever le nom de réseau de l'automate par défaut et son adresse MAC puis configurer l'automate en DHCP
- Relever le n° du Switch et le port sur lequel est branché l'automate (si le Switch n'a pas de repère, compter à partir du haut vers le bas dans la baie)
- Faire une demande par mail à : centre-appels@chu-brest.fr en précisant les relevés ci-dessus
- et en demandant l'adresse IP correspondante en retour
- Le service informatique configure l'automate sur le VLAN contrôle d'accès (77) et vous communique son IP (à saisir dans le logiciel)



TILLYS NG Maintenance Configuration System Information

Network

System configuration

Hostname: UTILV3-0102eA

IP address:

Subnet mask:

Gateway:

☒ DHCP

Subnet:

Laisser le nom de l'automate par défaut dans l'interface Web et le paramétrer en DHCP

Interface de configuration NIS Créer Télécharger Assistant de programmation Affichage Paramètres

M-BAT3-PH-ONCO-1

M-BAT3-PH-ONCO-1

Commentaire

Le nom de l'automate est à renseigner dans la page de paramétrage.

Il faut également le renseigner dans son nom de supervision

Récupérer l'adresse IP définie par le SI du CHRU afin de la renseigner ici également

Configuration

Matériel

Contrôle d'accès

Microcode

Echanges avec le serveur

Echanges avec les autres UTL

4. DESCRIPTIF DU LOGICIEL

4.1. Généralités

Le logiciel d'exploitation est « MICRO-SESAME » de chez TIL Technologies, il permet le paramétrage et la supervision du contrôle d'accès, de la détection intrusion, de la GTB, et des différents systèmes tiers présents sur le site via des protocoles ouverts comme MODBUS RTU, OPC/DA, ASCII, web services.

Il fonctionne sous un environnement Windows 64 bits et communique avec les UTL par liaison IP.

En tant que superviseur, le logiciel peut également permettre de réaliser des passerelles suivantes :

- Synchronisation automatique entre de la base de données des usagers avec le logiciel RH (ou autre référentiel)
- Gestion des opérateurs de MICRO-SESAME et de leurs droits à travers l'annuaire LDAP, et active directory. Il sera possible d'attribuer plusieurs profils par opérateur par ce mécanisme.

L'accès des opérateurs sur le logiciel est contrôlé par des droits opérateurs qui sont personnalisables. Ces droits opérateurs permettent de filtrer les accès aux fonctions suivantes par opérateur :

- Contrôle d'accès :
 - Création,
 - Visualisation,
 - Modification des usagers et des droits d'accès
 - Attribution des droits d'accès.
- Plages horaires
- Historiques,
- Paramétrage système,
- Synoptique :
 - Visualisation
 - Télécommandes

Il est donc possible et conseillé de créer des profils opérateurs prédéfinis, et d'affecter à chaque opérateur un ou plusieurs profils prédéfinis facilitant la gestion des opérateurs. Une modification dans le profil opérateur aura pour conséquence de changer les droits pour tous les opérateurs ayant ce profil.

Pour une traçabilité, chaque intervention dans le système est archivée dans l'historique avec le nom de l'opérateur et l'heure.

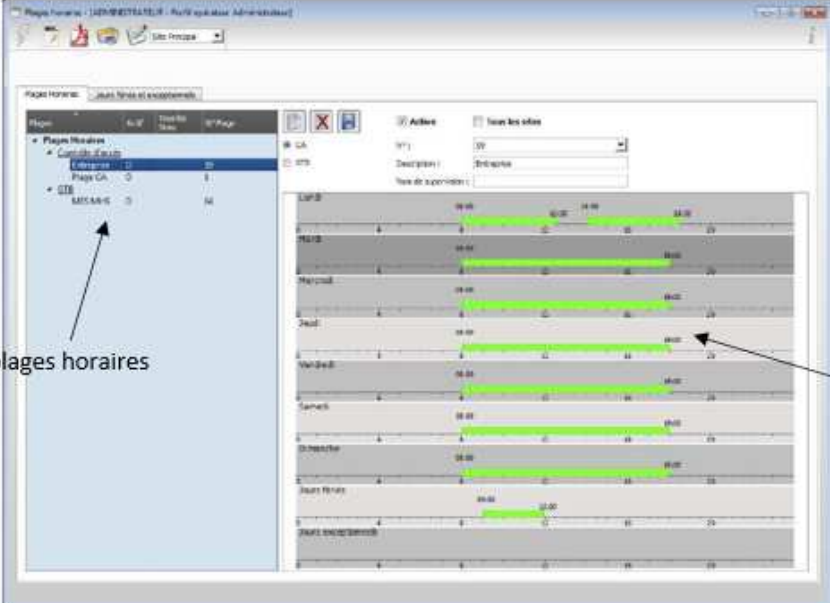
La durée d'accès au système est également paramétrable.

4.2. Contrôle d'accès

Plages horaires :

Le système peut gérer au minimum 128 plages horaires différentes par site. Elles ont les particularités suivantes :

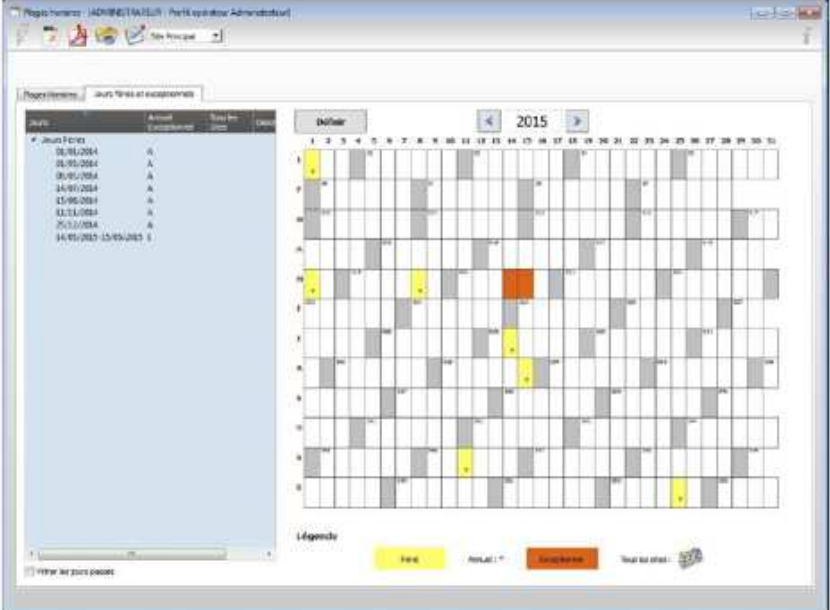
- Jusqu'à 2 ou 4 créneaux par jour
- Prise en compte des jours fériés de type annuel ou exceptionnel
- Définition du type de plage (quotidienne, hebdomadaire)
- Plage horaire et jours fériés valable pour 1 site donné ou pour tous les sites (gestion multi-site)
- Plage active ou inactive



Paramétrage des plages horaires

Nom des plages horaires

Créneaux horaires



Paramétrage des jours fériés

Groupes de lecteurs :

Le système permet de créer jusqu'à 1024 groupes de lecteurs. Un groupe de lecteurs est un ensemble regroupant de 1 à 1024 lecteurs (portes). Il permet de simplifier la gestion des droits d'accès des usagers et de créer des zones géographiques particulières.

Attribution des droits d'accès aux usagers :

Le profil d'accès permet de prédéfinir les accès autorisés pour une catégorie d'usagers sur un ou plusieurs sites. La définition des profils est gérée par le CHRU, une réunion préalable avec les responsables est par conséquent à prévoir afin de définir les plages horaires, groupes et profils.

L'attribution des droits d'accès aux usagers pourra se faire de deux façons différentes qui peuvent se cumuler :

- Gestion individuelle

Les droits d'accès peuvent se faire usager par usager (cette gestion n'est pas conseillée) :

- L'attribution de lecteurs, ou de groupes de lecteurs
- L'affectation d'une plage horaire pour chaque lecteur,
- Une date de début et de fin de validité pour chaque attribution de droits.

- Gestion multi-profils

- A chaque usager, il sera possible d'associer un (ou plusieurs) profil(s) d'accès. On pourra ainsi associer un profil général (droit d'accès incluant plusieurs groupes, lecteurs, niveaux d'ascenseur) à plusieurs personnes, facilitant ainsi la création des profils d'un groupe de personnes ayant les mêmes droits d'accès.
- Chaque lecteur, niveau ascenseur, groupe et profil d'accès, attribué à un usager, pourra également être associé à une date de début et de fin de validité qui se rajoute à celle définie pour l'usager et décrite ci-dessous. Cela permettra de gérer notamment des missions temporaires. Un usager pourra ainsi avoir plusieurs profils actifs en même temps.
- Un niveau de priorité permettra de définir les accès autorisés. Le système permet d'associer 4 profils et/ou groupes d'accès par usager pour s'adapter à la diversité des types d'usagers et réduire le nombre de profil à créer et à exploiter.

Pour les personnes ayant un droit d'accès total, afin d'éviter d'ajouter dans leurs profils, à chaque fois, pour chaque nouveau lecteur qui serait installé, le système dispose nativement d'un profil d'accès « tout accès site »

Attribution des droits intrusions aux usagers :

Le système permet d'attribuer des droits intrusion (groupe ou zone de points) de manière centralisée pour chaque usager depuis les postes clients pour l'ensemble des centrales intrusions type TILLYS ou équivalent.

Un code secret pour les fonctions intrusion peut être choisi par usager et utilisable pour toutes les centrales intrusions.

La fiche identifiés (utilisateurs) :

Elle permet d'identifier chaque usager (porteur de badge, etc...) et de gérer ses droits d'accès. Elle contient les fonctions et champs dont certains pourront être paramétrés comme obligatoire à la saisie. Les champs minimums à renseigner lors de la création de nouveau utilisateur sont à voir avec le CHRU.

Le système permet la gestion d'au moins 4 types d'identifiants (ici il n'en est utilisé que 2, voir chapitre II.4 sur les lecteurs de badge)

Un code secret pour les fonctions intrusion ou contrôle d'accès renforcé (badge + code) peut également être attribué par utilisateur, pour faciliter l'exploitation, le système possède une fonction de recherche avancée des usagers qui permet de rechercher les usagers (Nom, Prénom, Société, Service, champ libre...).

Tout changement intervenant sur la fiche usager est tracé (ajout, modification, ou suppression) sur un ou plusieurs champs de la fiche. Il sera également notifié le nom de l'opérateur ayant réalisé la manipulation.

Utilisation de plusieurs technologies d'identification :

Le système permet la gestion au moins de 4 identifiants distincts par utilisateur sur une même fiche usager mais au CHRU, il n'en a été retenu que 2.

Chaque identifiant peut appartenir à une des 2 technologies définies au CHU, permettant ainsi de mixer plusieurs technologies sur le site. Par exemple, il sera possible d'attribuer un badge de technologie A, un badge de technologie B à une personne sur la même fiche usager.

Ceci permettra d'utiliser simultanément plusieurs technologies de contrôle d'accès sur un même site, sans créer de doublons et de réduire le nombre d'UTL.

Identifiants au CHRU :

Comme évoqué aux paragraphes précédents, une seule technologie de badges est acceptée au CHRU et un seul pilote a été créé pour le site et est autorisé. Il est impératif de respecter la technologie installée.

Les badges à fournir doivent être de technologie MIFARE/DESFIRE EV1

Pilote lecteur : 2 MS ISO2 - Magstripe

Longueur code : 14 caractères

Lecture : Hexadécimal

Remplissage : Gauche

4.3. Microcodes :

Les microcodes ne doivent pas être conçus sans organisation, titre et commentaires. Pour la maintenance il est impératif d'appliquer la règle :

« Une ligne de commande = un commentaire »

Exemple pour 1 porte :

```
;***** PORTE N°001 **** PORTE ACCES EXT| NORD COULOIR 009 *****
;----- Section Init -----
#PROGRAM#
;---- Section Combinatoire ----
XA011=V1||R1          ;Equation d'ouverture porte (R1=Tc depuis syno)
XA013=V128            ;Equation voyant vert
XA014=V127            ;Equation voyant rouge
M70=DEFAULT_LECTEUR_1 ;Defaut lecteur
;--- Section événementielle ---
EV(LA01==AUTORISE)    ;Quand je passe un badge autorisé
  V1=PULSE(50)        ;je passe V1 à 1 pendant 5s pour libérer la porte
  V128=PULSE(50)      ;J'allume le voyant vert 5s
EV(LA01==INTERDIT)    ;Quand je passe un badge interdit
  V1=0                ;je n'ouvre pas la porte (je la force à rester fermée)
  V127=PULSE(50)      ;J'allume le voyant rouge 5s
EV(R1==1)             ;Quand j'ai une TC depuis le syno
  V1=PULSE(50)        ;je passe V1 à 1 pendant 5s pour libérer la porte
  V128=PULSE(50)      ;J'allume le voyant vert 5s
  XA015=PULSE(5)       ;J'enclenche le buzzer pendant 1s
EV(DA011==0)          ;quand la porte s'ouvre
  TN1=VN1             ;Lancement timer sur porte ouverte
EV(TN1)               ;quand le timer se termine
  M128=1              ;Apparition du défaut POTL
  XA015=PULSE(100)    ;J'enclenche le buzzer pendant 15s
EV(DA011==1)          ;Quand la porte se referme
  SI(DA012==0)        ;Si le bâti est resté ouverte
    M1=1              ;j'active la variable d'effraction
    TN1=0             ;Reset timer sur porte fermée
    M128=0            ;Reset défaut POTL
    XA015=0           ;reset du buzzer POTL
  SINON               ;Sinon
    TN1=0             ;Reset timer sur porte fermée
    M128=0            ;Reset défaut POTL
    XA015=0           ;reset du buzzer POTL
    M1=0              ;Reset variable d'effraction
  FINSI               ;fin de la condition
;*****
```

4.4. Multi-site / Multi-client / Multi-entité

Principe

Pour bénéficier d'une gestion autonome du contrôle d'accès par site sur un système serveur centralisé multi-site, le système de contrôle d'accès permet de cloisonner, filtrer :

- Les lecteurs par site : Les sites sont dans l'ordre géographique (Morvan, La Cavale Blanche, Bohars...). Le système peut gérer 128 sites différents et permet à chacun d'avoir une maîtrise différenciée de ses accès.

Chaque site est un système indépendant et dispose de 128 plages horaires indépendantes utilisées soit dans le cadre du contrôle d'accès, soit dans le cadre de la gestion technique de bâtiment, il permet également à chacun d'avoir une maîtrise différenciée de ses usagers

Gestionnaire principal et opérateur gestionnaire

Le système comporte un gestionnaire principal.

Ce dernier sera le seul qui aura accès à la totalité de la base de données commune aux différents sites.

Le gestionnaire principal voit tous les sites et toutes les entités, peut les créer, les supprimer, ou les modifier. Il a aussi la fonction d'administrateur général et doit dans ce cadre attribuer les droits opérateurs de chaque opérateur gestionnaire.

Les gestionnaires de site peuvent gérer uniquement :

- Les lecteurs de son ou ses sites dans l'attribution des droits d'accès,
- Les usagers de son ou ses entités dans leur gestion dont l'attribution des droits d'accès,

Zones communes

Cette configuration prend en compte la possibilité de gestion de zones communes à plusieurs clients. Ce cas de figure implique nécessairement la gestion d'une base de données unique et commune (détenu intégralement par le seul gestionnaire principal).

Certains lecteurs peuvent en effet être gérés en communs par plusieurs opérateurs gestionnaires.

De même, un usager peut appartenir à plusieurs entités et peut de ce fait avoir accès à plusieurs sites. Un usager « multi-site » pouvant accéder à plusieurs sites peut recevoir ces droits d'accès de chaque opérateur gestionnaire pour chaque site ou par le gestionnaire principal ayant capacité à gérer tous les sites concernés.

4.5. Intrusion

Introduction

Chaque UTL peut également gérer l'intrusion de la partie qu'il gère. Les détecteurs intrusion peuvent être raccordés directement sur des entrées (carte MLIO16, MLD1, MLD2...) ou raccordés via un bus Equilock déployé dans le bâtiment (voir module Equilock).

Le pilotage de l'intrusion peut se faire classiquement depuis un clavier dédié (Tactile +) ou via un lecteur de badge.

La partie intrusion se paramètre dans l'UTL à la rubrique intrusion.

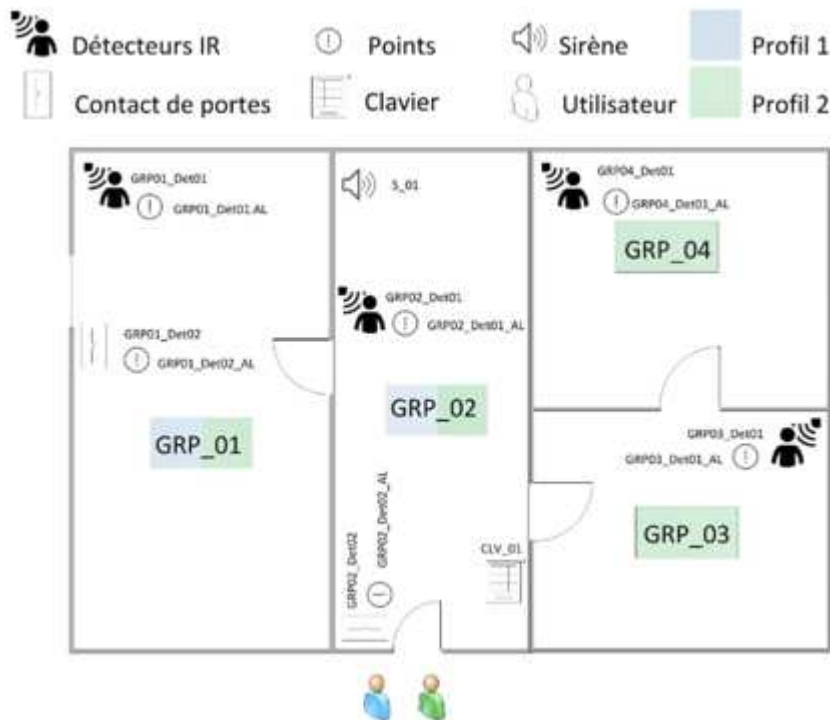
Principe de base

Les différents détecteurs (points) seront regroupés dans un ou plusieurs « groupe de détecteurs » suivant le fonctionnement défini.

Avec un seul groupe de détecteurs, toutes les alarmes seront mises en ou Hors service en une fois ; avec plusieurs groupes, il sera possible de ne lever que partiellement certains groupes.

Il sera ensuite créé des profils utilisateurs permettant d'attribuer des droits aux utilisateurs. Ainsi, un utilisateur pourra disposer de droits pour lever certains groupes et pas d'autre tandis qu'un utilisateur maître pourra gérer tous les groupes.

Exemple :

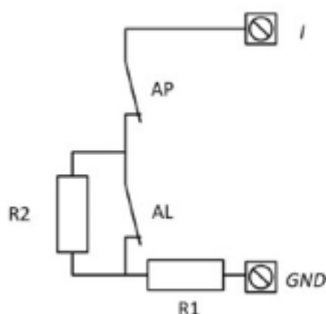


Dans l'exemple ci-dessus, il y a 2 utilisateurs qui ont 2 profils différents. L'utilisateur 1 peut gérer tous les groupes tandis que le deuxième n'a accès qu'aux groupes 2 et 1.

Détecteurs :

Chaque détecteur d'alarme doit être déclaré comme un point dans le système et doit posséder une zone d'alarme et une autoprotection (24/24h).

Le câblage à mettre en place sur une entrée est le principe des contacts équilibrés :



2 contacts équilibrés pour montage dans détecteurs d'alarme
Résistances standard (Ω)
- R1=1K
- R2=1K

État	Reg Ei	Reg Fi	Standard TIL (Ω)
Coupure ou AP ouvert	0	1	∞
AL ouvert, AP fermé	0	0	2k
AL fermé, AP fermé (repos du detecteur)	1	0	1k
RAZ fermé	1	1	0

Gestion des alarmes :

Pour tout événement (changement d'état d'une entrée ou d'une sortie, alarme, passage de badge, action d'un opérateur...), un message horodaté apparaît au fil de l'eau et est archivé dans l'historique.

Les alarmes - et d'une manière générale les variables surveillées par le système – sont classées par catégories suivant leur type (contrôle d'accès, incendie, intrusion ou techniques) et /ou suivant leur localisation géographique. Le fil de l'eau permet de tracer les événements horodatés suivants :

- Pour un changement d'état ou une alarme
 - La désignation de la voie (le libellé en clair)
 - Son état (normal, défaut, etc.)
- Pour un passage de badge
 - Le nom de la personne
 - L'heure
 - L'état d'autorisation du badge (autorisé, inconnu, hors plage horaire...)
- Pour les actions d'un opérateur
 - L'opération effectuée
 - Le nom de l'opérateur
 - Le poste concerné
- Pour les autres événements
 - Le type d'événement,
 - Le nom de l'organe du système concerné,
 - Le poste concerné.

Le fil de l'eau affiche les événements par couleur, selon leur nature (alarmes en rouge).

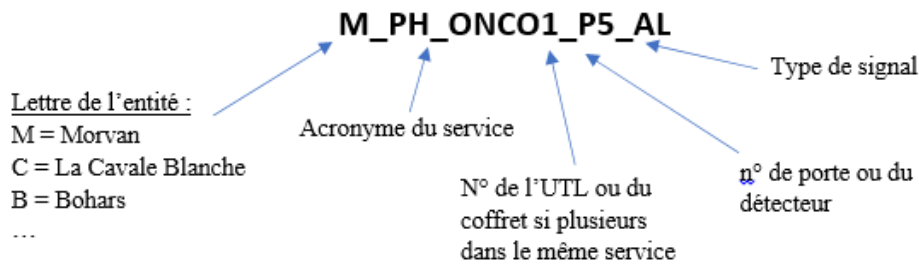
Les apparitions, acquittements et effacements d'alarmes sont tous horodatés et archivés en base de données.

5. SYNOPTIQUES

5.1. Variables

Que ce soit pour l'intrusion où pour le contrôle d'accès, les variables correspondantes sont à créer pour une remontée vers la supervision.

Les variables d'un UTL seront créées de la même manière que le nom de ce dernier :



Le nom de la variable ne doit pas dépasser 20 caractères

Liste des actionneurs :

- Pn° = porte suivie de son numéro
- COFF = coffret
- Vn° = Volumétrique, suivit de son numéro
- CHOC = détecteur choc

Liste des Types de signaux :

- DEF_SECT = Défaut 220V coffret
- DEF_BAT = Défaut batterie de l'alimentation
- DEF_ALIM = défaut technique alimentation
- AP = Autoprotection
- AL = Alarme
- POTL = Porte Ouverte Trop Longtemps
- CO = contact porte
- BATI = contact bâti
- BBG = contacte bris de glace vert

5.2. Interface Homme - Machine (IHM)

Généralités :

Le système permet la supervision des équipements sur des synoptiques représentant des vues et des niveaux des bâtiments.

Pour cela, le système propose un éditeur de synoptiques qui permet de personnaliser des plans existants sous forme de fichiers. L'éditeur possède des fonctions de dessin ce qui permet la personnalisation de chaque plan.

Chaque vue représentera un tableau ou plan dynamique permettant une exploitation conviviale avec icônes, animations, télécommandes, changement de couleurs, etc...

Sur apparition d'une alarme, le système peut afficher le synoptique correspondant à cette alarme (localisation physique ou tableau de synthèse) avec une gestion de consigne et de priorité.

La mise en place des synoptiques rend l'exploitation des alarmes plus conviviale pour l'exploitant grâce à des vues détaillées et personnalisées de l'installation. A partir de la page d'accueil, l'exploitant doit pouvoir appeler des menus lui permettant de superviser et de piloter l'ensemble de son installation.

Afin d'optimiser l'exploitation du système, il est prévu une vue par niveau et par bâtiment. Toutefois, le système n'est pas limité dans le nombre de synoptiques ou de vues. Chaque synoptique peut commander n'importe quel autre synoptique, afin que l'opérateur puisse obtenir le détail de l'alarme s'il le souhaite par des « sous plans » permettant un effet de zoom, en cliquant simplement sur le plan (le nombre de sous plan n'est pas limité).

L'exploitant peut également piloter les différentes sorties du système et matériels interfacés par de simples clics sur le synoptique : pilotage d'un éclairage, affichage d'une caméra vidéo, réponse à un appel interphone, etc...

Arborescence des synoptiques :

Les boutons du menu de droite doivent être organisés comme sur les illustrations suivantes. Ils donnent l'accès à la page d'accueil de chaque site et cette vue permet ainsi l'accès aux différents services du bâtiment.

L'arborescence retenue pour le menu de gauche est : Site, bâtiment, service

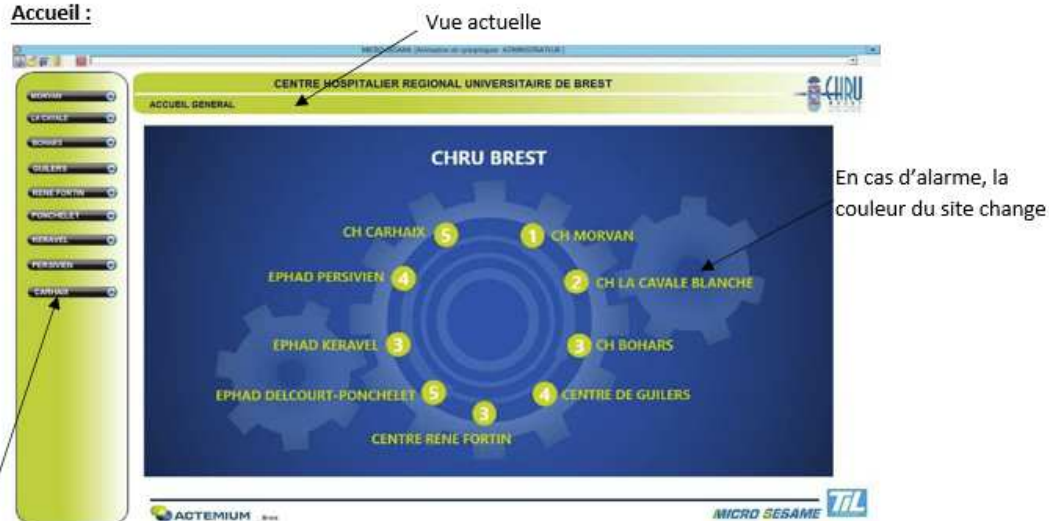
Les profils utilisateurs seront paramétrés pour démarrer à la page d'accueil du site concerné. Seul un utilisateur ayant un profil administrateur pourra avoir accès à tous les sites (1^{er} menu).

Un utilisateur travaillant à Morvan devra démarrer sur la page d'accueil de Morvan lorsqu'il lance l'application synoptiques.

La trame de fond à utiliser pour le synoptiques est disponibles sur le serveur dans le dossier :

C://Msesame/config/symboles/Trames de fond

Accueil :



Menu principal des
« Sites »

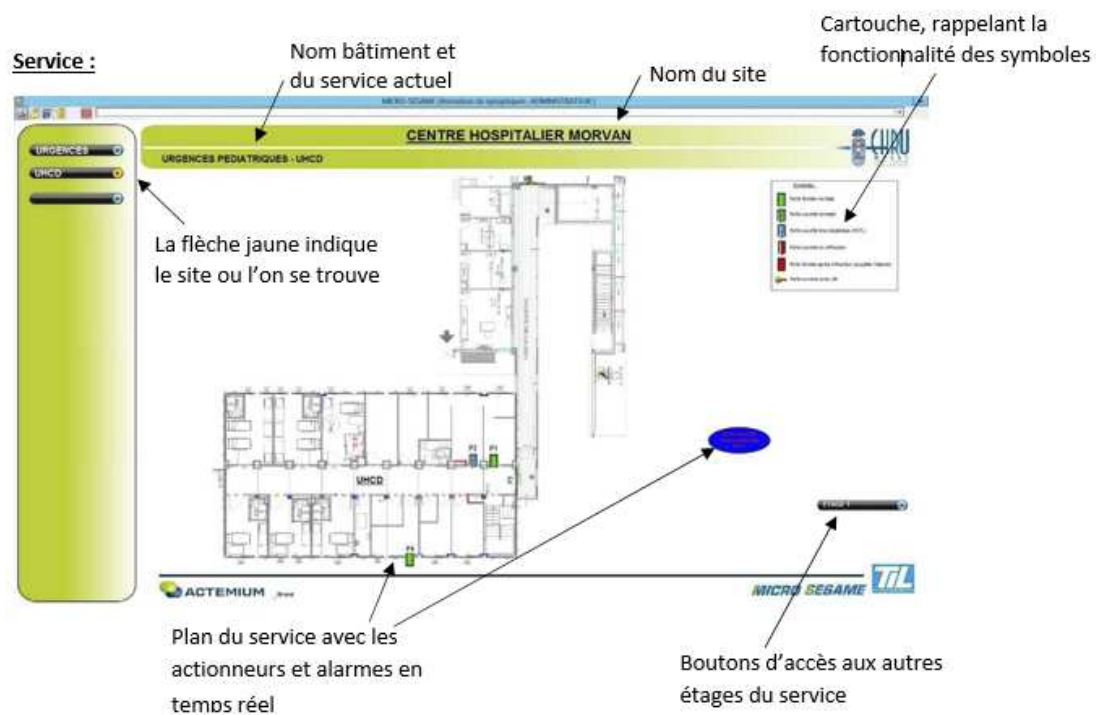
Un clic sur un bâtiment doit renvoyer l'utilisateur vers le détail de ce dernier

Bâtiment :



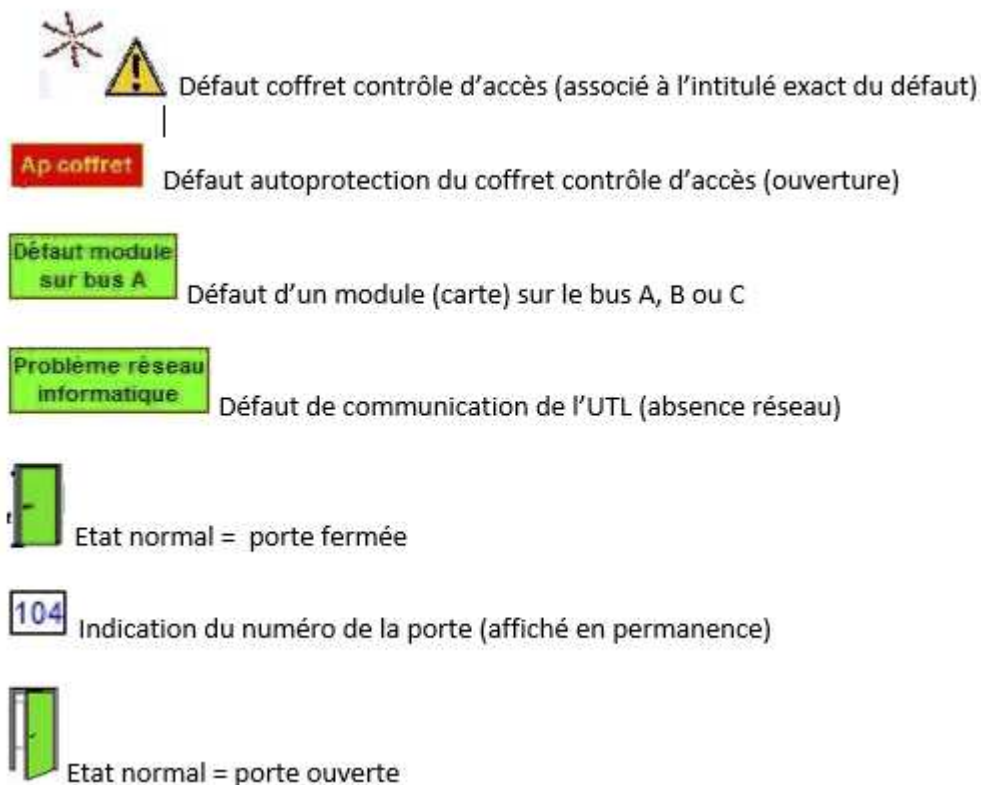
Arborescence du bâtiment,
cliquer sur un service pour y
accéder

Un clic sur un service doit renvoyer l'utilisateur au plan détaillé du service.



Symboles des synoptiques

Une bibliothèque des symboles utilisés pour la supervision est disponible sur le serveur dans le dossier C ://Msesame/config/symboles/symboles IHM





Porte ouverte trop longtemps (POTL), tempo d'ouverture dépassée (pas d'alarme)

POTL = 60s symbole est présent en permanence à chaque porte. Il indique la valeur de réglage de la durée du POTL. Un simple clic dessus permet (en fonction des droits de l'utilisateur) de modifier la valeur en secondes.



Effraction porte (porte ouverte non conformément) Nécessite un acquittement de l'alarme (prise en compte) pour un retour à l'état normal



Porte refermée après effraction mais alarme non acquittée (attente acquittement)



Ce symbole apparait en plus à chaque alarme sur une vue IHM



Ce symbole apparait en plus sur la vue à chaque défaut POTL



Ouverture porte avec clé, ce symbole passe la porte en rouge (effraction)



Ce symbole apparait lorsqu'une porte n'est pas verrouillée (pêne serrure non sorti)



Bouton poussoir de commande porte depuis synoptique (ouverture à distance)



Apparition de ce symbole lors du déclenchement d'un BBG vert



Signalisation de l'effraction



Signalisation d'une alarme intrusion générale (apparait à chaque défaut)



Bouton d'acquiescement des alarmes (présent uniquement lors d'un déclenchement) Lorsqu'il n'y a pas d'alarme, aucun symbole n'apparaît sur la vue générale.

En cas d'alarme, les symboles suivants apparaissent en fonction du défaut et à l'endroit du défaut :



Alarme volumétrique (entourage rouge du symbole clignotant)



Autoprotection capteur 1

Autoprotection volumétrique entrée tunnel (sabotage)



Dérangement

Défaut du détecteur (anti-masque, encrassement, rotation, erreur)



5.3. Cas particuliers de contrôles d'accès :

Des dispositifs de contrôles d'accès sont déployés sur la SSR de Guilers dans l'unité de soins « Ker Anna ».

Dans cette unité de soins où les personnes accueillies ne peuvent de manière volontaire présenter un badge à une distance suffisante du lecteur pour provoquer l'ouverture de porte, il a été choisi de mettre en place un dispositif de gestion des accès par bracelets.

Ce système est de marque « Dormakaba ».

Il permet une ouverture de porte par impédance du corps lorsque le résident met la main sur la poignée de porte de la chambre à ouvrir.

Les avantages du système :

Serrure particulièrement silencieuse.

Il n'y a pas la nécessité de présenter le lecteur à une distance suffisante du lecteur pour obtenir l'ouverture de la porte.

Inconvénient :

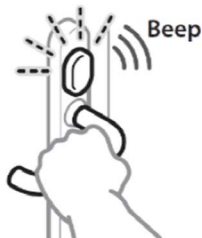
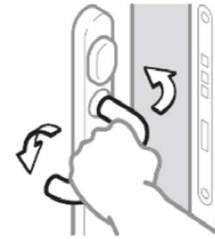
Mise en place d'un nouveau serveur et poste d'exploitation.

Kaba TouchGo E310

Principe de fonctionnement

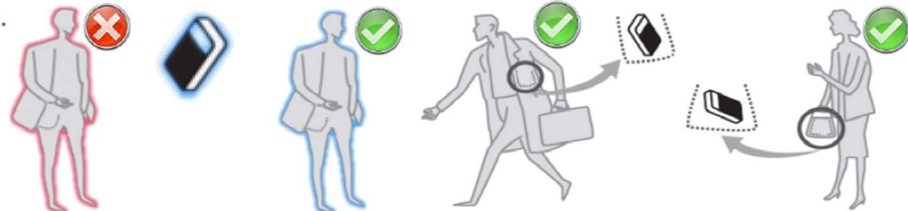


- > Le système Kaba TouchGo permet l'ouverture des portes sans manipulation des clés ou badges.



- > Par effleurement de la poignée, la serrure électronique reconnaît, si la personne porte un média utilisateur autorisé.

- > Il suffit de porter l'identifiant TouchGo sur soi à une distance de 5-10 cm au corps.

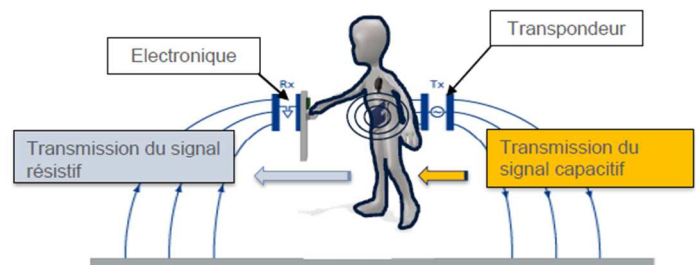


Kaba TouchGo E310

Resistive Capacitive Identification

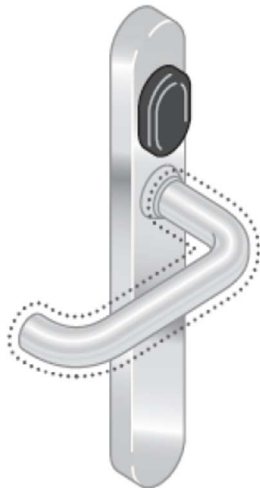


Comment ça fonctionne?



1. Le transpondeur TouchGo envoie un signal par voie aérienne (couplage capacitif) sur le corps de l'utilisateur = Le signal est couplé au champs électrostatique de l'utilisateur et utilise le corps humain comme un « fil mouillé ». Si le transpondeur se trouve à proximité de la poignée, la liaison s'effectue également directement avec la poignée.
2. Lorsque vous touchez la poignée de c-lever, l'électronique TouchGo se réveille (capteur capacitif) et est à la recherche d'un signal proche. Le canal est ouvert pour recevoir des données.
3. L'électronique reçoit le signal provenant du transpondeur.
4. La c-lever TouchGo compare les données avec la base de données stockée.
5. Si l'ID (paquet de données) en provenance du transpondeur est le même que celui de la base de données la porte s'ouvre. Sinon, elle reste verrouillée.

Principe de fonctionnement TouchGo™



- > L'électronique est à l'intérieur de la garniture
- > En raison de l'utilisation de champs électrostatiques, le transfert d'informations se fait via des électrodes (pas des antennes).
- > La poignée est l'électrode réceptrice
- > Le signal est transporté sur le corps de l'utilisateur.
- > L'électronique est réveillée par contact avec la poignée

Kaba TouchGo E310 Solution Intégrée



TouchGo c-lever E310
Combinaison de la
technologie RFID et RCID
dans la même garniture de
porte

- > Combinaison parfaite:
 - > Technologies combinés: RFID et RCID
 - > compatible avec les applications CardLink
 - > plus de confort à moindre coût
- > Basé sur les fonctionnalités de la c-lever Kaba evol
- > Jusqu'à 1000 utilisateurs TouchGo

Gestion des données avec le programmeur
Kaba evol 1460, CardLink et gestion
logicielle



Porte carte Kaba TouchGo RCID



Transpondeur Kaba TouchGo
avec combinaison des
technologies RFID et RCID



Kaba TouchGo E310

Aperçu

KABA

MIFARE

c-lever:

2621MID/**E310**/...

media:

KMID-MA00**4**

KMID-MB00**4**



LEGIC

c-lever:

2621LEA/**E310**/...

media:

KLEA-MB00**3**

KLEA-MA00**3**



HTGO-BE00**1**

AX02-BE**204**
DESFire (4K)



HTGO-BE00**1**

AX04-BE**202**
Prime (1K)

AX05-BE**204**
Advent (4K)



5.4. Alarme anti intrusion – Projet de réhabilitaion à courts et moyen terme :

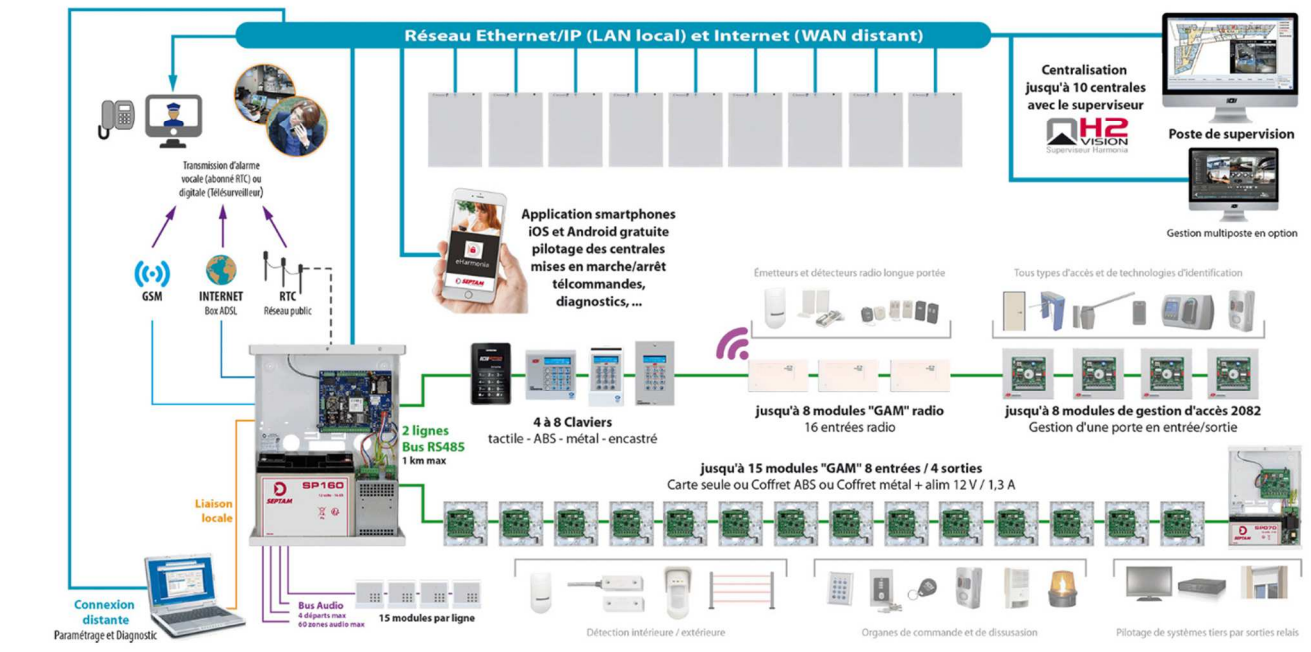
Les éléments liés au contrôle d'accès et anti -intrusion de marque Till sont honéreux. Une solution est proposée pour les projet à court et moyen terme.

Il s'agit d'équipements de la gamme « harmonio » de la marque Setpam.

Ces éléments ne nécessitent pas d'être sur le réseau IP mais peuvent renvoyer des alarmes sur les DECT ou les serveurs d'alarme en place sur le CHU.

Harmonia 3

2653/2663/2683



6. LA VIDÉO PROTECTION

6.1. Généralités :

- Installation passive -> exploitation à posteriori des images -> **reconnaissance et identification** des personnes
- Passer de 7 jours à 10 jours d'enregistrement (préconisation forces de l'ordre)
- Tenir compte de l'éclairage, distance et de la stabilité du support dans le choix des caméras
- Le format de compression choisit pour le transport des images peut dégrader la lecture des enregistrements
- Plusieurs choix de réseaux possibles (VLAN dédié déjà initié pour la CB), stockeur centralisé ou plusieurs stockeurs, plusieurs enregistreurs ou stockeurs et enregistreurs intégrés (solution VRM)

6.2. Contexte :

- Résolution caméras : **rapport qualité image/taux de compression non linéaire** :
 - plan large 1 CIF (352x288 pixels)
 - plan étroit 4 CIF (704x576 pixels) format MPEG 2/MJPEG -> environ 5 Mbits/s
 - format MPEG 4 -> 2 à 3 Mbits/s

- Format H 264 < 1 Mbit /s. Le taux de compression impacte directement la qualité des images
- Caméras HD méga pixels (1280x1024 pixels)
- **Données distances:**
 - Réseau Ethernet sur Cu (4 paires FPT) max 90 m – 1 km avec commutateurs LRE (long reach ethernet)
 - Réseau Ethernet sur fibre optique : 550 m en multi mode et 5 Km monomode
 - Sans fil – faisceau hertzien -> suivant environnement 50 m à 1 km (problème de sécurité)

6.3. Exploitation

- **Fonctionnalités du logiciel d'exploitation:**
 - Il devra être uniforme sur l'ensemble des sites et multimarque (ouvert)
- **Incrustation**
 - le logiciel permettra la gestion des textes incrustés sur la vidéo.(le nom de la caméra et le texte correspondant à la zone visualisée, Date et heure sont également incrustées à la relecture des scènes enregistrées)
- **Visualisation**
 - Choix du mode d'affichage : multivision ou plein écran
 - Choix des caméras à afficher dans une liste
- **Recherche de séquences vidéo**
 - La visualisation des images numériques enregistrées devra être obtenue après :
 - Recherche des images d'une caméra à une date et heure données
 - Recherche d'un événement d'alarme dans le fichier des historiques
 - Recherche des images enregistrées sur une zone géographique donnée
- **Remontée de défauts** : ex -> Défauts racks vidéos – stockage – perte communication caméra – vandalisme – alarmes techniques

6.4. Evolution du système

- **Evolutivité et ouverture**
 - Le dispositif et les matériels proposés doivent être dotés de capacités d'évolution en fonction des nouvelles technologies numériques et de transmission du signal vidéo.

- La **supervision vidéo** devra être **multimarque et ONVIF**, c'est-à-dire capable de traiter des flux issus de caméras de **différentes marques**.
- L'enregistrement suivra également ce principe. En plus d'être compatible à tout type et fournisseur de matériel, le système de vidéosurveillance devra pouvoir s'adapter :
 - Aux extensions futures
 - Aux ajouts d'équipements et de systèmes en relation avec les évolutions prévisibles de la réglementation ;
 - Aux ajouts des différents postes de visualisation ;
 - Aux évolutions prévisibles des standards actuels (H264/265 et autres)

6.5. Traitement des images :

- **Traitement des flux vidéo**
 - Le logiciel devra traiter **le format natif des flux vidéo IP**, compressés, délivrés par les équipements des constructeurs (caméras IP, encodeurs vidéo, enregistreurs vidéo).
 - Les flux vidéo correspondront à la résolution maximale de la caméra (si HD/ lecture HD) en visualisation et enregistrement.
 - Les flux de compression demandés sont à minima du H264 voir H 265
 - L'enregistrement prendra en compte la détection de mouvement pour l'ensemble des caméras (existantes et du projet) afin de limiter la capacité de stockage nécessaire.(réduction de bruit)
 - Les flux des caméras à installer seront obligatoirement en H 264 / 265 ou autre format de qualité de compression au moins équivalente.

6.6. Les caméras

- Des caméras couleur fixes équipées d'objectifs de type varifocale. Ces caméras intégrant un dispositif jour/nuit permettant la visualisation de zones sensibles où la lumière d'ambiance peut ne pas être adaptée à la vidéosurveillance. Ces équipements devront à minima avoir les caractéristiques techniques suivantes :
- Les produits de vidéo IP doivent être basés sur des normes ouvertes (**ONVIF**) et pouvant s'intégrer facilement au système d'information du CHRU
- Compression H264 / H 265
- Norme IEEE802.1X pour le contrôle d'accès réseau
- Protocole IPv6 natif
- Balayage progressif

- Compensation de contre-jour
- Fonctionnement jour et nuit
- Réduction de bande passante (distinction entre les bruits et les informations pertinentes)
- Caméra couleur
- Alarme de détérioration des connexions des entrées/sorties
- Fonction de gestion des alarmes
- Déclenchement sur gestion d'évènements paramétrables
- Technologie d'alimentation par Ethernet (Pas de POE car les Switch CHU sont équipés d'alimentation intégrées)
- Objectif à diaphragme automatique pour l'exposition lumineuse du capteur d'image
- Caisson de protection adapté (IP66 et thermostaté)
- Stabilisateur électronique d'image
- Masquage de confidentialité coordonné aux mouvements (conformité avec la loi du 21 janvier 1995)
- Analyse vidéo intelligente -> scénarios d'alarmes avancés - classification d'objet – investigations accélérées – solution ouverte
- Production d'images couleurs même dans des conditions d'obscurité extrême
- Réglage automatique de l'exposition de la caméra
- **Garantie cinq (5) ans.**

6.7. Enregistrement :

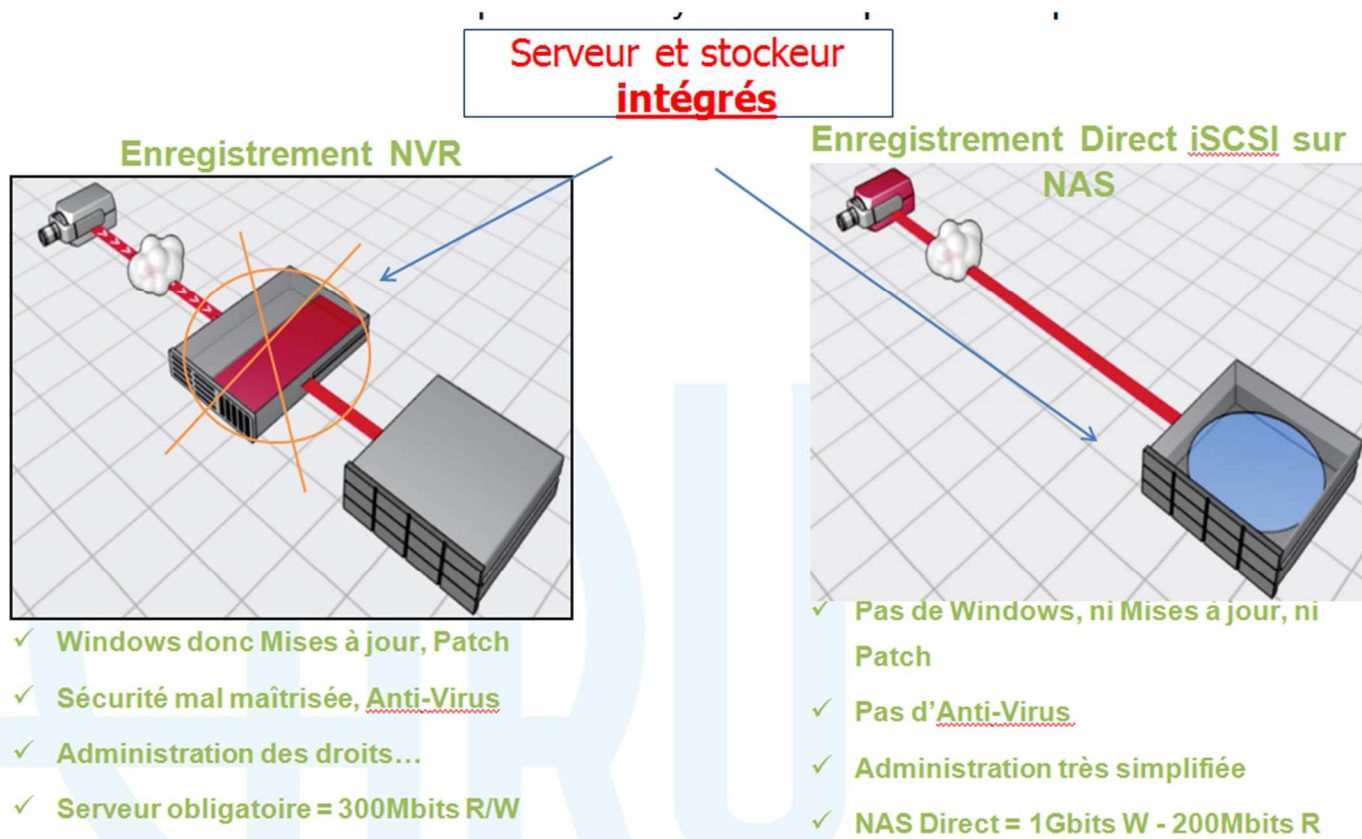
- Capacité d'enregistrement
 - Le système de stockage devra être évolutif et permettre, par adjonction de mémoire de masse, d'augmenter la capacité de stockage (évolution jusqu'à **3 fois la capacité initiale**) avec une réserve de stockage initiale de **40 %**.
 - Le stockage des flux vidéos se fera dans la résolution maximale du capteur de la caméra et sera conservé 10 jours.
- La qualité des images correspondra aux exigences de visualisation des flux en direct.
- Afin d'optimiser le volume de stockage, mettre en place :
 - un enregistrement sur alarme (événement intéressant la sûreté : intrusion, ouverture de portail, passage de ligne parking, capteur de mouvement...)

- enregistrement ininterrompu – résilience maximale

6.8. Cablage

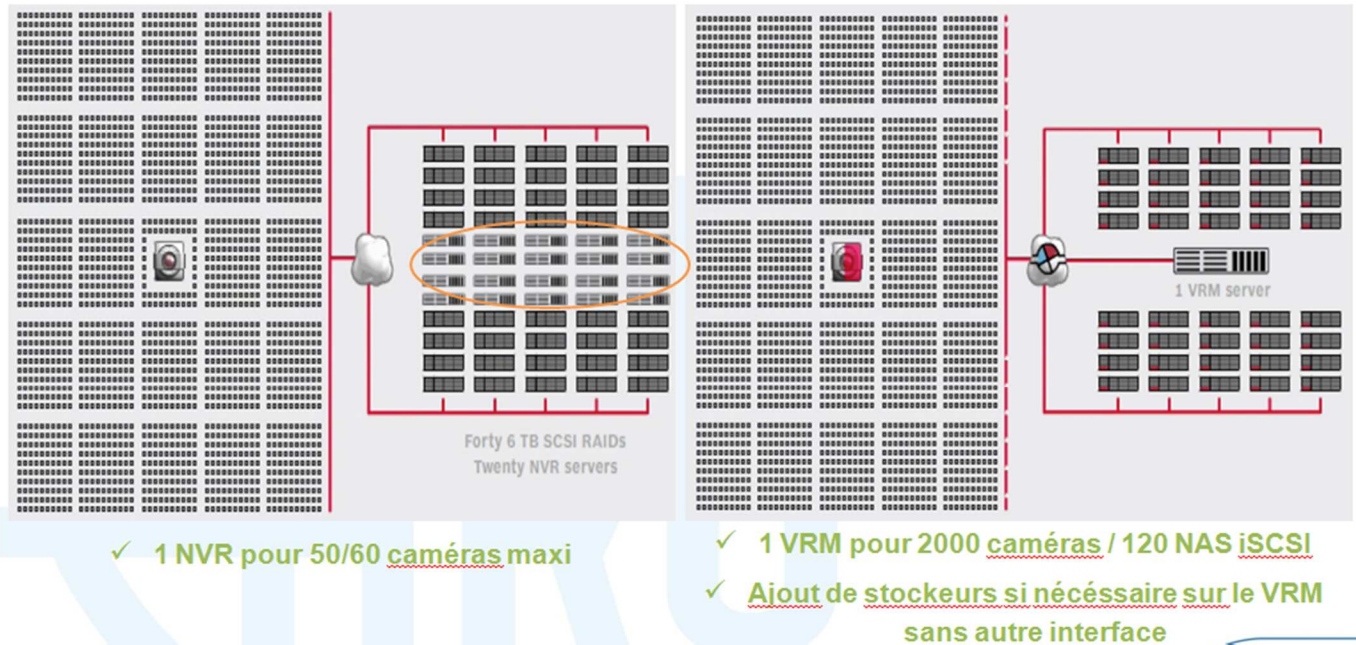
- Exigences connecteurs RJ 45
- (extrémités, fixation, étiquetage, connecteurs, raccordement câble, blindage, équipotentialité)
- Points d'accès utilisateurs dans les baies SRI
- câbles de distribution cuivre 4 paires, multi paires téléphoniques, fibres optiques
- Brassage informatique / téléphonique / optique
- Cordons de brassage

6.9. Synoptique du système :



6.10. Réduction du stockage :

► Architecture NVR vs VRM -> analyse du retour d'expérience à effectuer



7. INTERPHONIE ET VISIO PHONIE :

7.1. Projets neufs et pérennes :

Généralités :

Dans le cadre de projets neufs et prérennes, les systèmes déployés sont des systèmes relativement honéreux, qui présentent des fonctionnalités évolutives intéressantes pour les services à savoir:

- Renvoi sur les DECT
- Ouverture de gâches
- Les dispositifs présentent un haut niveau de sécurité informatique.

Pré-requis :

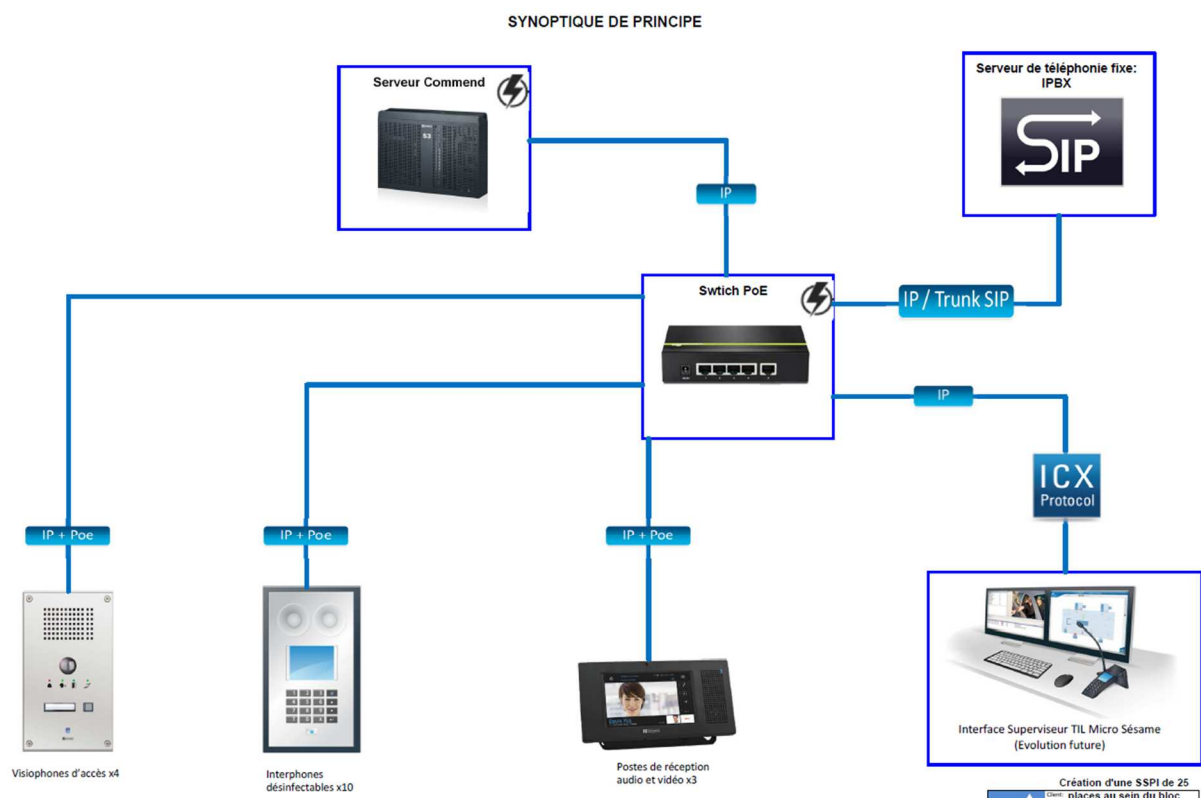
Les dispositifs doivent être compatibles avec les équipements et serveurs de contrôles d'accès déployés sur le CHRU de Brest. 2 marques sont référencées:

- Commend
- Stentofon.

Commend :

Solution performante et évolutive. Elle nécessite un serveur et des terminaux sur réseau IP.

- **Synoptique de principe :**





Passion pour l'Audio

par Commend

L'intelligibilité de la parole en toutes circonstances

L'OpenDuplex® avec HD Voice + par Commend autorise des conversations naturelles en mode mains libres – aussi claires et compréhensibles que des conversations en face à face.



Communication Naturelle



eHD Voice



Volume élevé



Suppression des bruits de fond



Surveillance du Haut-Parleur et du Microphone

Audio // Basics

eHD Voice	Le HD Voice + par Commend diffuse le signal audio avec une bande passante de 16,000 Hz, restituant ainsi l'ensemble du spectre des fréquences de la voix humaine.
STI	Indice de transmission vocal 0.96 – mesurée en laboratoire acoustique. STI est une mesure standard de l'intelligibilité de la parole. La valeur maximum est de 1.00, laquelle correspond à une intelligibilité parfaite.
Amplificateur	Amplificateur classe "D" de 2.5 W
Microphone	Microphone électret omnidirectionnel pour une distance de conversation jusqu'à 7 m
Haut-Parleur	Haut-Parleur 2 x 8 Ω avec membrane spéciale anti-humidité pour une qualité sonore optimale.

En savoir plus
audio.commend.com

Audio // Fonctions

- Suppression dynamique de **bruit de fond**, élimine quasiment tous les bruits ambiants
- **Ajustement automatique du volume** aux bruits ambiants
- **Surveillance haut-parleur/micro** – assure la disponibilité de l'interphone tout en réduisant la nécessité d'une vérification manuelle de ses fonctions
- **Surveillance Audio (Audio Monitoring)** – Déclenchement automatique d'un appel d'urgence sur cri ou sons pré-définis - pour la sécurité des utilisateurs
- **Peer2Peer Audio** permet de réduire la charge du réseau et d'assurer une utilisation efficace des ressources
- **Fonction de sonorisation**
- **Enregistrement audio** et enregistrement synchronisé de l'audio/vidéo des conversations pour l'archivage et la constitution de témoignages
- **Fonction de conférence téléphonique** pour dialoguer avec plusieurs interlocuteurs simultanément
- **Détection de modulation** permet de détecter que les appels sont terminés (plus de signal du microphone) et de mettre automatiquement fin à la communication
- **Mode Simplex** pour les applications qui requièrent un contrôle des communications - par ex des solutions de sécurité basées sur la méthode "appuyer pour parler/relâcher pour écouter"
- **Egaliseur** pour une adaptation aux conditions de bruit ambiant

• Les switches :

Les switches POE sont fournis par la DSIS

- Les terminaux :

Les principaux avantages

Les deux haut-parleurs intégrés permettent une utilisation du poste à des volumes élevés et délivrent une haute intelligibilité; ils permettent également la diffusion automatique de messages pré-enregistrés pour orienter les utilisateurs.

Caméra couleur intégrée spécialement conçue pour les environnements où les exigences en matière de sécurité sont élevées.

Les **LEDs avec pictogrammes** fournissent aux utilisateurs des informations claires sur l'état de fonctionnement du poste.



Le système de boucle à induction garantit durablement un haut niveau de fonctionnalités pour fournir une aide aux personnes malentendantes. Le poste YAP201VICEDA comporte un dispositif simple et compact à la différence de certains autres systèmes nécessitant des haut-parleurs et des boucles à induction déportés.

Sa construction **robuste en acier inoxydable** et l'indice de protection IP 65 garantissent un fonctionnement ininterrompu et infailible dans les lieux publics extérieurs.

Le **microphone électret** omnidirectionnel permet une distance de conversation jusqu'à 7m. En conséquence, les conditions de communication optimale sont maintenues, même lorsque la distance de conversation entre l'utilisateur et le microphone est relativement importante (pour les utilisateurs en fauteuil roulant par exemple).

Principe de "bi-sensorialité"

Ce principe définit qu'une information doit être présentée de sorte qu'elle puisse être perçue par deux sens complémentaires : une information sonore doit également être émise visuellement, et une information visuelle doit être également représentée de manière sonore ou tactile.

7.2. Stentofon :

Ce système est équivalent au dispositif « Commend » avec une sécurité informatique très performante.

- Postes d'interphonie IP STENTOFON
- Haut-parleurs IP STENTOFON
- Téléphones IP 3^{es} partie
- Passerelles téléphoniques IP
- IP DECT STENTOFON 300

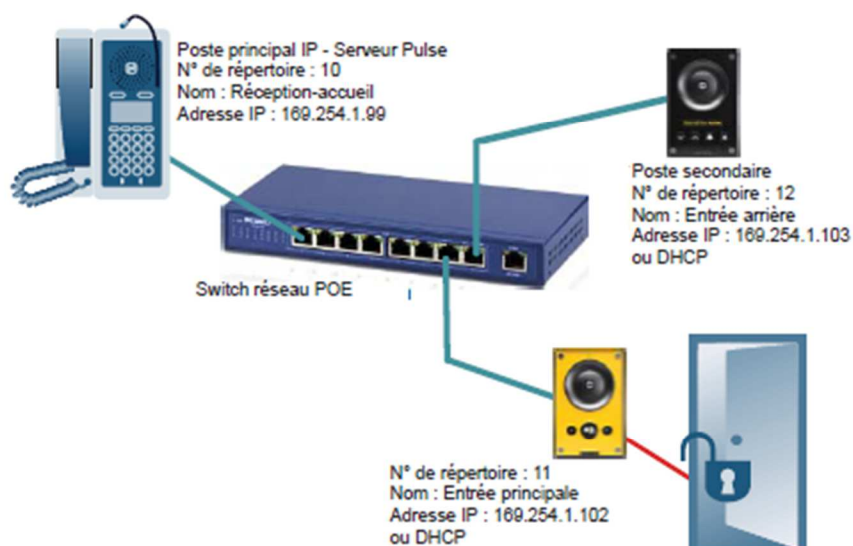


1.1 Aperçu du système Pulse

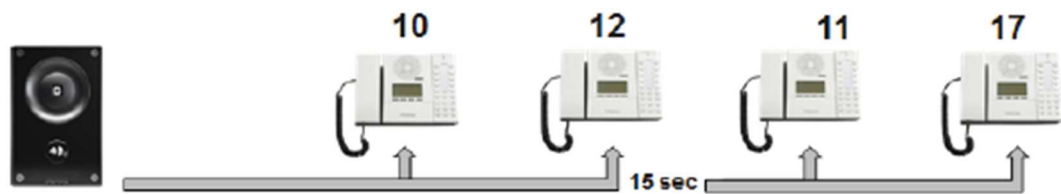
Pulse STENTOFON est un système d'interphonie IP pour une utilisation allant jusqu'à 16 postes. Le système fonctionne avec tous les postes d'interphonie IP STENTOFON. Par ailleurs, il est possible d'étendre le système avec des terminaux SIP et des passerelles 3^{es} partie.

Dans une installation Pulse, un des postes d'interphonie STENTOFON IP est désigné comme le Serveur Pulse. Ce Serveur Pulse agit tel un serveur SIP, gérant la configuration des postes et leur routage. De plus, le Serveur Pulse fournit un point unique pour la configuration de tous les postes d'interphonie dans le système..

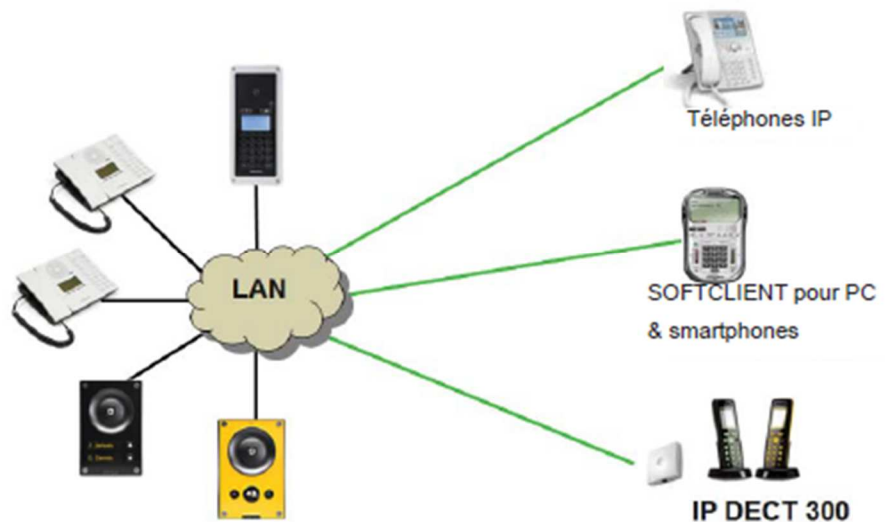
① *Tous les postes d'interphonie IP au sein d'une installation Pulse doivent être situés sur le même LAN (IP subnet).*



Raccordement au réseau IP :



3.7 Ajouter des comptes SIP pour téléphone IP 3^{ce} Partie et IP DECT



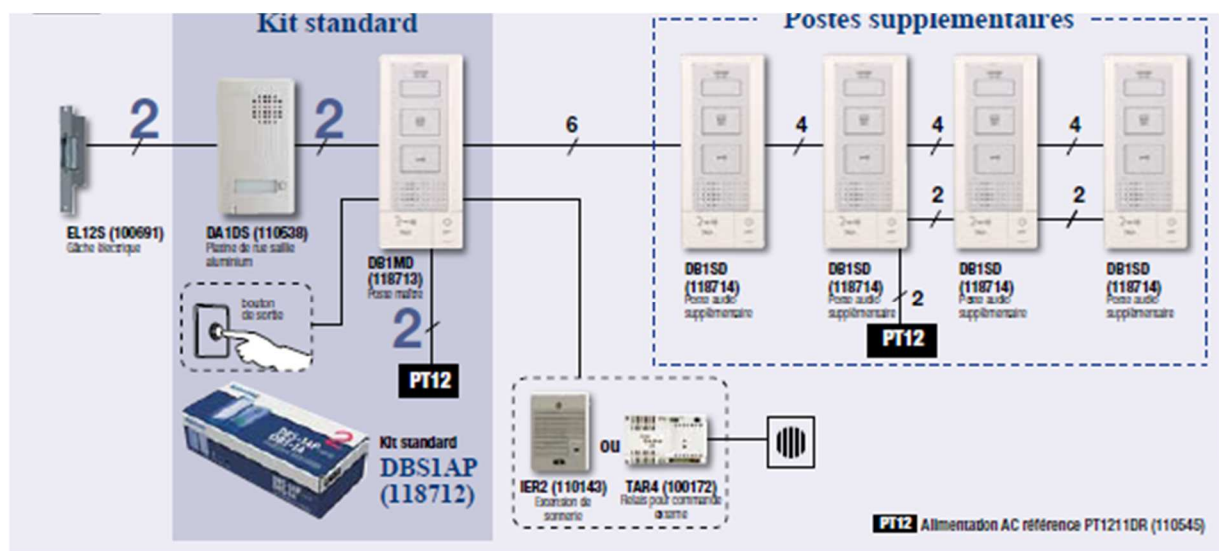
7.3. Réhabilitation de service :

Les équipements « Commend » et « Stentofon » sont très honéreux.

Dans le cadre de réhabilitation de service existants ou développés à court et moyen terme, une solution alternative est proposée. Cette solution est développée sur plusieurs opérations ponctuelle.

7.4. Equipements Aiphone :

Ces équipements ne nécessitent pas de connexion sur le réseau IP et peuvent fonctionner en autonomie pour la gestion des communications et l'ouverture à distance d'une ou plusieurs portes.



Seulement 27 mm



Bouton optionnel

Pour commander un dispositif externe, par exemple l'éclairage de l'entrée.

Intercommunication

Pour faire un appel général sur tous les postes et entrer en communication avec un poste.

Ajustement des volumes

Pour ajuster (ou couper) le volume de la sonnerie et / ou du haut parleur

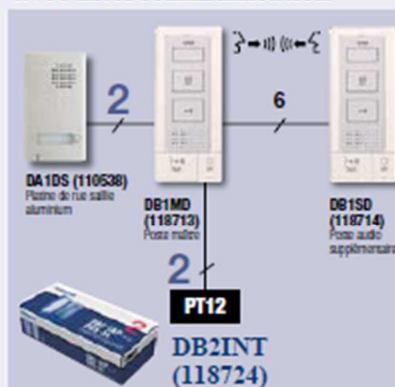
Bouton OFF

Pour arrêter la communication

Bouton TALK

Pour prendre la communication mains libres

Kit 2 postes intérieurs DB2INT (118724) avec intercommunication



Options



KDA2 (110580)

Adaptation façade inox encastrée, 1 appel, résistante au vandalisme avec clavier rétro éclairé 100 codes, 2 relais



KDA4 (110581)

Adaptation façade inox encastrée, 2/4 appels, résistante au vandalisme avec clavier rétro éclairé 100 codes, 2 relais



SKDA (110582)

Cadre saillie avec visière pour KDA2 & KDA4



FSDB1 (118719)

Adaptation façade inox saillie, 1 appel, résistante au vandalisme



FDB1 (118718)

Adaptation façade inox encastrée, 1 appel, résistante au vandalisme



FDB2 (118720)

Adaptation façade inox encastrée, 2 appels, résistante au vandalisme

Synthèse interphonie – visio phonie :

Projet neuf et perenne	Marque	Déployé dans les services	Fonctionnalités
	Commend	SSPI CB	Interphonie Visiophonie ouverture des portes par DECT Ouverture des portes par visiophones
		CMA CB	
		CCA CB	
		UHCD pédiatrie	
		Bloc RDC Morvan	
		Bloc Niveau 1 Morvan	
	Stentofon	Portes coulissante des urgences Bt 5 Morvan	Interphonie Visiophonie ouverture des portes par DECT Ouverture des portes par visiophones
Projets d'éréhabilitation et court/moyen terme	Marque	Déployé dans les services	Fonctionnalités
	Aiphone	Caisson hyperbarre	

8. SYSTÈMES ANTI-FUGUE.

8.1. Généralités :

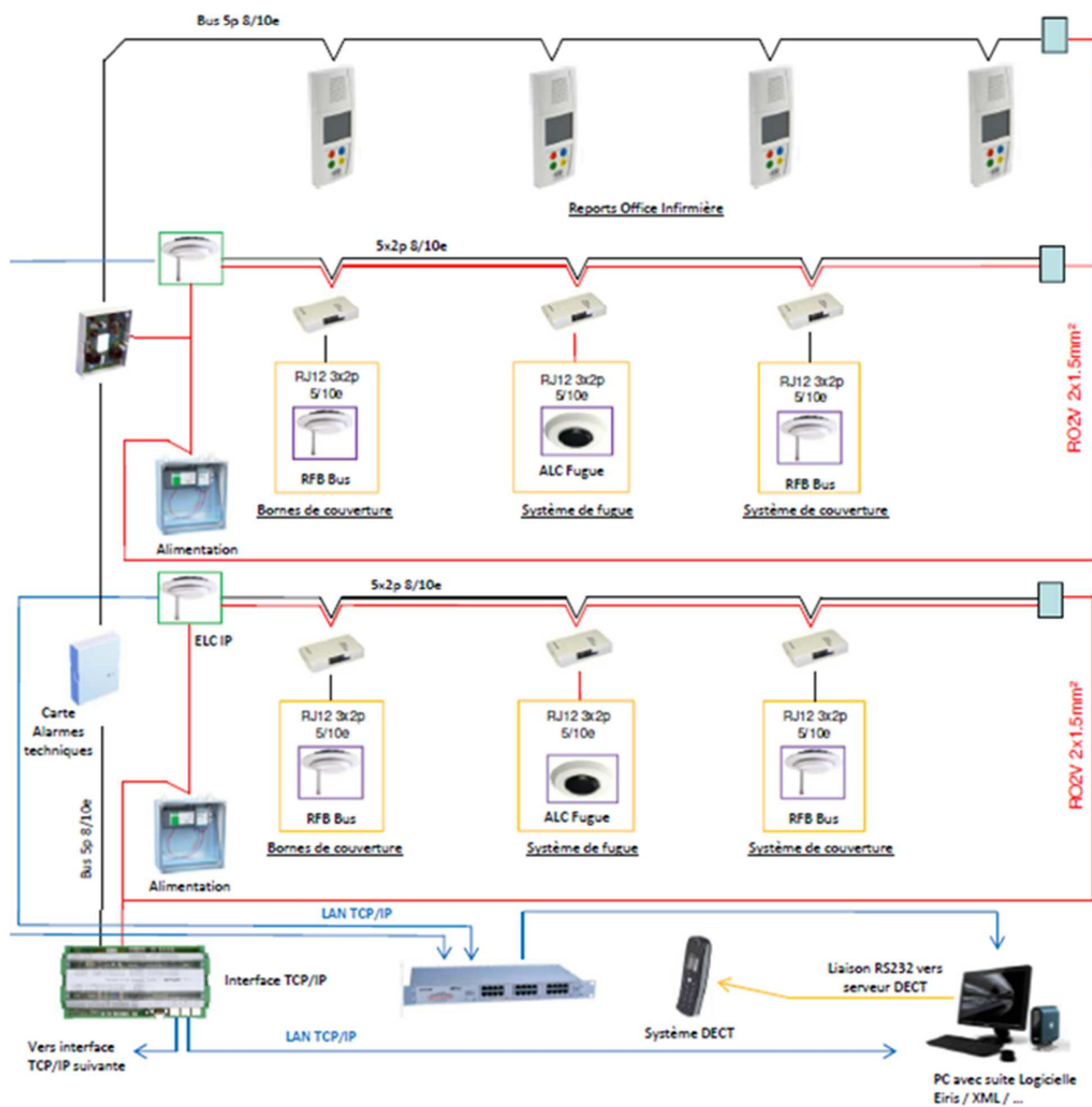
Certains services de soins nécessitent de surveiller les entrées/sorties patients/résidents et d'être alertés au cas où une personne sortirait sans autorisation.

8.2. Projets neufs et pérennes :

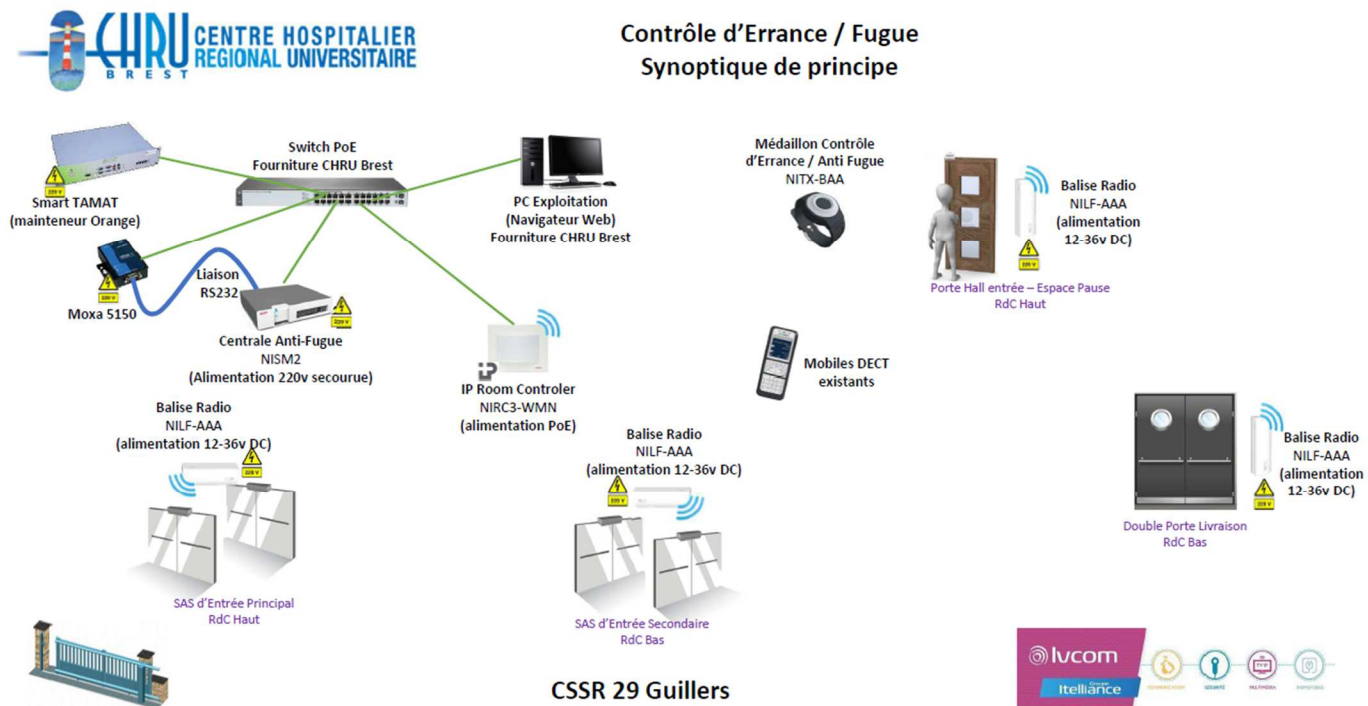
Pour les projets pérennes la solutions en lien avec le système d'appel Zettler est envisagée.

Synoptique Zettler

ELPAS – Medical 800



Les équipements suivants sont développés sur les sites et notamment à la SSR de Guilers (2020)



Synthèse anti fugues:

Projet neuf et perenne	Marque	Déployé dans les services	Fonctionnalités
Projets d'éréhabilitation et court/moyen terme	Marque	Déployé dans les services	Fonctionnalités
	LVCOM	SSR Guilers	