GUIDE METHODOLOGIQUE POUR LES SYSTEMES DE CONTROLE D'ACCES ELECTRONIQUES

(résidentiel, tertiaire / industriel)




Guide réalisé par IGNES, GPMSE, SVDI

ignes
Industries du Génie Numérique, Energétique et Sécuritaire

GPMSE
Groupement Professionnel
des Métiers de la Sécurité Électronique

SVDI

Ce guide donne les bonnes pratiques, définit les règles de l'art, liste les questions à se poser et apporte les réponses adéquates pour le succès d'un projet de contrôle d'accès électronique dans les domaines tertiaire / industriel et résidentiel (individuel et collectif).

Ce guide est destiné à tous les intervenants de la filière : utilisateurs finaux, installateurs, constructeurs, Bureau d'Etudes, prescripteurs….

SOMMAIRE

Schéma de principe d'un système d'accès résidentiel individuel

De plus en plus de logements individuels sont équipés de contrôle d'accès. Celui-ci renforce le sentiment de sécurité afin de valider ou non l'entrée du requérant.

Il s'agit le plus souvent d'un clavier codé installé à la porte d'entrée et d'une interface audio ou vidéo placée à l'intérieur du logement. Le schéma suivant illustre ce concept.

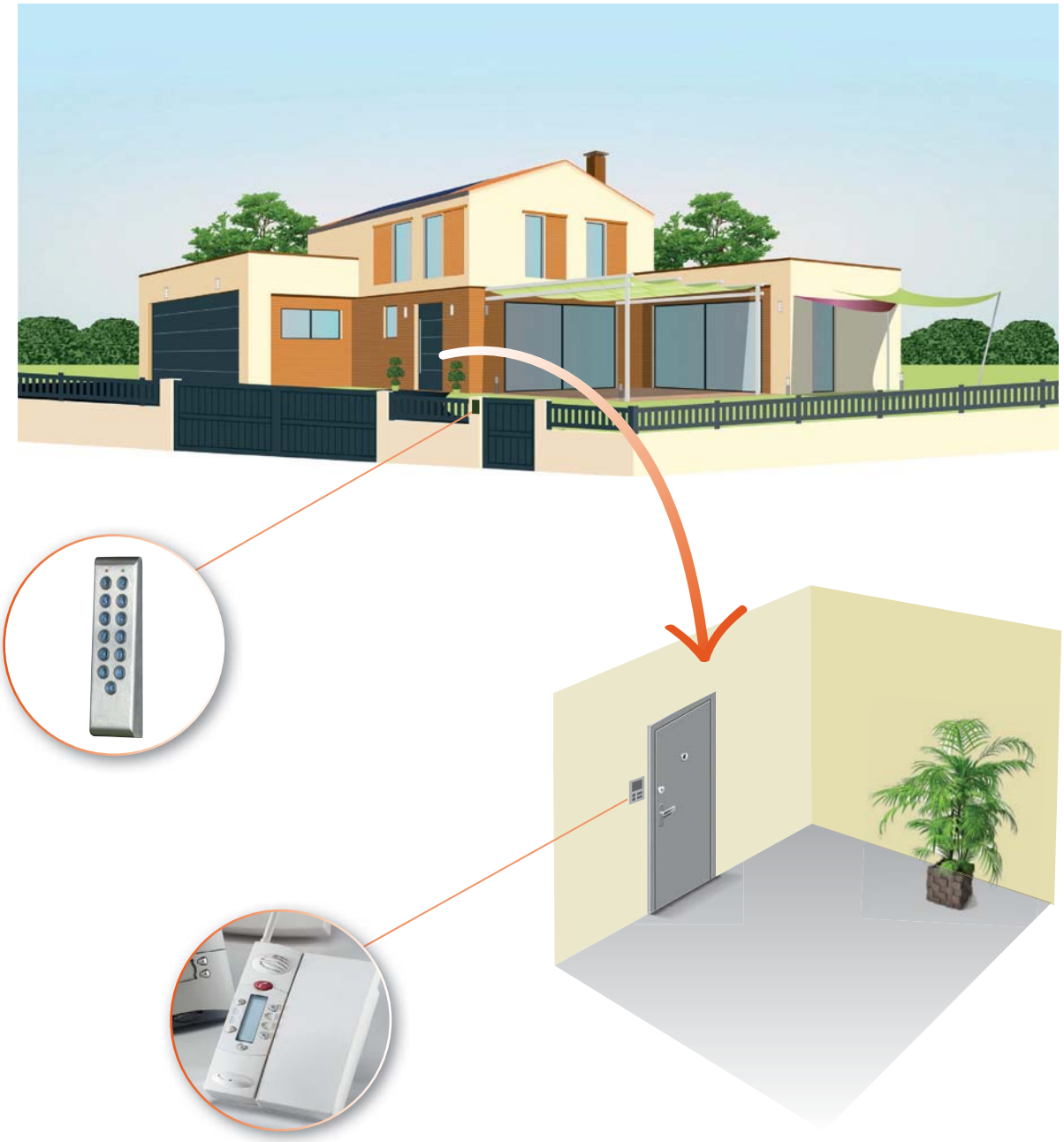

Schéma de principe d'un système d'accès résidentiel collectif

Un grand nombre de logements collectifs sont équipés de contrôle d'accès résidents. Dans la plupart des cas, ce contrôle d'accès résidents est associé à un contrôle d'accès prestataire extérieur. Le seul point commun entre les deux pouvant être la tête de lecture, les deux traitements étant bien distincts.

Le schéma suivant illustre ce type de système.

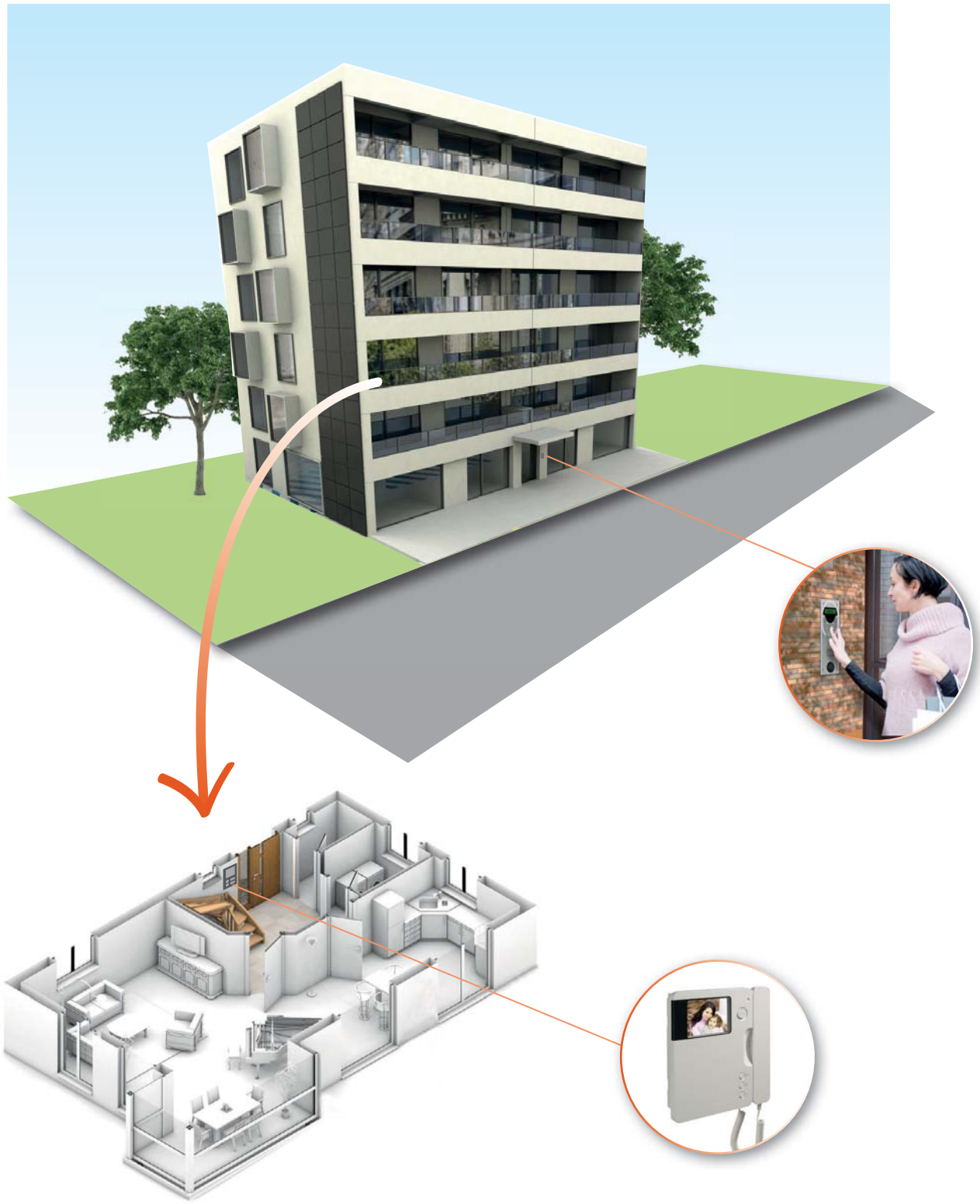

Schéma de principe d'un système d'accès tertiaire/industriel

Les sites tertiaires ou industriels sont le plus souvent équipés de système de contrôle d'accès. Ces systèmes se déclinent à la fois pour pénétrer sur le site et pour accéder à certains bâtiments sur le site lui-même. Le niveau de contrôle d'accès dépend de la sensibilité du site et de ces bâtiments.

Le schéma suivant illustre ces niveaux.

Point d'accès

UTC Unité de traitement centralisé de contrôle d'accès

UTL Unité de traitement local de contrôle d'accès

UTS Unité de traitement de supervision de contrôle d'accès

Généralités

Questions à se poser	► Conseils / Exigences
Contexte général Type de risque : quel est le niveau de sécurité pour chaque zone ?	Le niveau de sécurité impacte chaque rubrique. Voir les conseils / exigences correspondants.
Quel type de site : immeuble, bâtiment, site étendu, multi-sites ?	Soit plusieurs systèmes autonomes, soit un seul système avec cloisonnement de plusieurs zones gérées par des opérateurs différents.
Quel est le niveau de « continuité de service » souhaité ? (ex : coupure secteur, panne système)	Conditionne le fonctionnement en mode dégradé du système.
Quel est le flux de personnes (nombre de personnes) par zone ?	Détermine le nombre d'accès et le type d'accès.
Nombre d'accès contrôlés aujourd'hui et demain ?	Dimensionne les capacités du système et son évolutivité.
Nombre d'utilisateurs (personnel permanents / temporaires) ?	Impacte la capacité de l'UTL et du système.
Qui gère quoi ? - Création, modification, suppression usagers ? - Affectation des droits d'accès ? - Accès à l'historique des mouvements ? - Traitements des alarmes & défauts jour/nuit ? - Administration du système ?	Impacte l'organisation et la politique sécuritaire du client. Implication DRH, DSI, gestionnaire d'immeubles, ... S'assurer que le système permet de répondre aux attentes (profil opérateur, gestion des visiteurs,...).
Y a-t-il un système de détection intrusion ?	Créer des droits d'accès compatibles avec les zones sous surveillance afin d'éviter des alarmes intempestives.

Règles / Normes / Réglementations / Directives

Questions à se poser	► Conseils / Exigences
Quels sont les principaux textes réglementaires en vigueur en France ?	Obligation de prévenir le comité d'entreprise avant installation d'un contrôle d'accès. Pas de déclaration, déclaration simplifiée CNIL exigée en France, demande d'accord préalable de la CNIL (par exemple en biométrie). Consulter le site de la CNIL. Déclaration sélectionnée numéro 42 CNIL concernant la conservation d'évènements liées aux personnes. Conditionne le choix technologique. NFS 61-937 – NFS 61-931 : issue de secours. Loi de prévention de la délinquance (décret 1048 de 2007). Loi accessibilité : (arrêté 1658 de 2007). Les équipements doivent respecter entre autres les directives CEM/DBT/RTTE.
Votre activité est-elle concernée par l'un des cas suivants : - Site SEVESO ou ISPS Ports, - Zone ATEX : anti déflagrante, - FD21 pour l'industrie alimentaire avec les USA ou pharmacie/médicaments qui exigent de la traçabilité, - ……	Détermine certaines fonctions du système. Obligation de compter / lister les personnes en temps réel dans les zones à risque. Matériel ATEX ! Traçabilité des mouvements des usagers & actions opérateurs.
Devez-vous transmettre des rapports, recherches, tris réguliers ?	Détermine certaines fonctions du système.

Type d'identifiant et de lecteur

Questions à se poser	► Conseils / Exigences
Le type d'identifiant et/ou de lecteur est-il existant ou imposé ?	Définit ou impose la technologie des lecteurs avec ses limites d'utilisation dont l'utilisateur devra être informé.
Quel est le choix de l'identifiant et du lecteur ? code, badge, carte à puce, biométrie, autres (lecture plaque, ...).	- Niveau d'identification et/ou d'authentification. - Confort d'utilisation, fluidité. - Contraintes d'installation (design, robustesse, ...). - Contrainte réglementaire (loi accessibilité, ...).
Y a-t-il un seul type d'identifiant et de lecteur pour tous les accès ? (ex : badges proximité pour les portes, longue distance pour les véhicules).	S'assurer de la capacité du système à gérer plusieurs technologies.
Comment seront gérés les identifiants volés, perdus, oubliés, hors service, ... ?	Mettre en place des procédures internes. S'assurer des fonctions du système. Prévoir un stock de rechange pour les identifiants.
Comment gérer un défaut lecteur ?	Prévoir une solution de secours d'accès (batterie, exigences clients, ...). Vérifier que le système peut informer l'exploitant du défaut. Prévoir un stock de produits associé au contrat de maintenance.

Mode de gestion du système/ Fonctions d'exploitation

Questions à se poser	► Conseils / Exigences
Gestion des opérateurs - Quels sont les types d'opérateur : hôtesse, agent, responsable et fonctions par opérateur ?	S'assurer que le système dispose d'une gestion de droit d'administration par type d'opérateur.
- Combien de poste de gestion/opérateurs ?	S'assurer de la capacité du système.
Gestion des utilisateurs - Comment les identifiants seront personnalisés, attribués et distribués pour les salariés, intérimaires, locataires, visiteurs, sociétés de service, ... ?	S'assurer des fonctions du système. Prévoir l'organisation adéquate.
- Qui peut accéder où et quand ?	S'assurer des fonctions du système (droit d'accès, plages horaires, jours fériés, ...).
Comment gérer les alarmes et les événements ? - Consignes. - Acquittement. - Synoptiques. - Interface tiers. - Exploitation jour / nuit. - ……	S'assurer des fonctions et capacité du système.
Y aura-t-il des fonctions complémentaires ? - Gestion de parkings avec comptage. - Comptage / Anti-passback. - Gestion ascenseur. - ……	S'assurer des fonctions et capacité du système. Prévoir les obstacles physiques adéquats (sas, tripode, ...).
Infrastructure de communication - Nécessité d'un réseau dédié pour la sécurité et/ou bande passante ?	S'assurer du bon dimensionnement du réseau informatique (intranet, extranet, web) et téléphonique (privé, public).
- Si non, y a-t-il un réseau existant ? - Peut-on l'utiliser ?	La collaboration avec l'administrateur du réseau est recommandée avant le déploiement.
- Comment faire accéder les entreprises extérieures (visiteurs / sous-traitants) ?	Vérifier la compatibilité des logiciels avec les outils mis à disposition par votre société.
Gestion des sauvegardes Qui sauvegarde, archive régulièrement le système (paramétrages systèmes, personnes, identifiants) et où ?	Attention, sans sauvegarde, pertes totales des données si défaillance. S'assurer des fonctionnalités de sauvegarde locale et/ou déportée.

Type d'accès / Portes / Verrouillage / Serrure / Obstacle physique

Questions à se poser	► Conseils / Exigences
Comment définir un type d'accès ?	Adapter la porte et son dispositif de verrouillage (solidité …) au niveau de sécurité souhaité.
Que doit-il se passer sur perte de l'alimentation normale et secours (batterie vide) ?	Assurer une cohérence entre le niveau du dispositif de verrouillage et le niveau de résistance de l'accès. Rien ne sert de mettre une serrure 3 points sur une porte en «carton». Vérifier la nature des travaux sur l'accès (suppression de la poignée, plaque propreté, flexible,…). Choisir si l'accès doit rester ouvert ou fermé, donc le dispositif de verrouillage électrique associé.
Quel est le flux de passage (accès principaux / accès secondaires) par accès ?	Détermine le nombre et le type d'accès. Une porte est plus rapide qu'un SAS.
Y a-t-il des fonctions SAS, porte contrôlée en entrée seule, porte contrôlée en entrée et en sortie ? ...	Vérifier que le système gère ces fonctions
Est-ce que les portes sont déjà équipées ?	Vérifier que le système gère ces équipements .
Quel type de verrouillage choisir ?	A adapter selon les besoins : gâche / ventouse / serrure électrique / verrous / barrière levante / porte de parking / motorisations, ...
Quels sont les critères de choix ?	Les critères suivants déterminent le type de verrouillage : - degré de sécurité, - normes, marques tierce partie : NFA2P, et CERTALARM), et label (VIGIK®), - structure du point d'accès, - esthétique, - conditions climatiques, - rapidité de déverrouillage, verrouillage, - faisabilité d'adapter les portes existantes, - nombre de passages.
Y a-t-il un comptage du nombre d'identifiant (parking, ...) ?	Prévoir un dispositif mécanique permettant d'assurer l'unicité de passage.

Equipements de l'accès contrôlé

Questions à se poser	► Conseils / Exigences
S'agit-il une issue de secours ?	Respecter les réglementations.
S'agit-il d'un accès pour tous ?	Respecter les réglementations (indications visuelle et sonore + règles de mise en oeuvre).
Voulez-vous l'information : porte forcée, porte ouverte trop longtemps ?	Si oui, prévoir un contact pour le contrôle de la position du point d'accès déporté ou intégré au système de verrouillage.
Comment s'effectue la sortie en mode normal ? - par poignée, - par bouton poussoir, - par détecteur, - par boucle au sol, - par lecteur.	Si l'information d'alarme est requise (porte forcée et/ou porte ouverte trop longtemps), prévoir les adaptations mécanique et électrique, ainsi que la programmation. La refermeture automatique de la porte est fortement conseillée (ex. ferme porte).
Comment s'effectue la sortie en mode de secours ? - par bris de glace, - par dispositif mécanique (clé, barre anti-panique, ...).	Prévoir l'adaptation mécanique et la sélection des dispositifs électromécaniques (coupure alimentation par déclencheur manuel).
Où implantez-vous les équipements techniques et les contrôleurs (centrale, UTL, ...) ?	Prévoir l'implantation des fermes portes, UTL (centrale), cartes électroniques, ... à l'intérieur de la zone contrôlée et accessible pour la maintenance ! Ceci peut conditionner le type d'équipements (coffret, rail DIN,….) Faire attention aussi aux distances maximales possibles selon constructeur.
Les coffrets doivent-ils être auto-surveillés à l'ouverture ?	Vérifier les données constructeur.
De quelle autonomie doit-on disposer en cas de rupture secteur (alimentation lecteur, UTL, centrale, organe de verrouillage) ?	Prévoir une alimentation et une capacité de batterie appropriées.
Nécessité d'être averti (alarme) sur défaut secteur ?	Vérifier les données constructeur.
Faut-il prévoir un fonctionnement local de la gestion des accès en cas de défaillance du réseau et/ou serveur « mode dégradé » ?	L'UTL (centrale) doit disposer de cette fonctionnalité et doit avoir une capacité suffisante (en nombre de personnes et d'événements).

Interface avec d'autres systèmes

Questions à se poser	► Conseils / Exigences
Y a-t-il besoin de communiquer avec ? - un annuaire d'entreprise, - une gestion horaire, - une gestion de restaurant, - autres.	Vérifier la compatibilité des systèmes. Privilégier le badge unique et/ou une base usagers commune.
Y a-t-il besoin de communiquer avec ? - un système de détection d'intrusion, - un système de supervision, - un système de vidéosurveillance, - GTB, GTC, - autres.	Vérifier la compatibilité des systèmes. Avec un système de détection d'intrusion, définir les différents modes de fonctionnement notamment la mise en/hors service intrusion.
Faut-il alerter en cas de perte de communication (alarme) ?	Vérifier les données constructeur.
Faut-il gérer l'ascenseur ? - appel palier, - gestion des niveaux autorisés.	Consulter systématiquement l'ascensoriste.

Glossaire

- **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.

- **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 aux utilisateurs, déclenchement d'alarme, ...).

- **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.

- **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.

Notes

Guide diffusé par :

ignes
Industries du Génie Numérique, Energétique et Sécuritaire

17, rue de l'Amiral Hamelin - 75016 Paris
Tél : 01 45 05 70 83 / 01 45 05 70 95
contact@ignes.fr - www.ignes.fr

GPMSE
Groupement Professionnel
des Métiers de la Sécurité Électronique

17, rue de l'Amiral Hamelin - 75016 Paris
Tél : 01 45 05 71 71
secretariat@gpmse.com - www.gpmse.com

FEDELEC
PROFESSIONS ELECTRICIENS ELECTRONICIENS

1, Place Uranie - 94345 Joinville-le-Pont cedex
Tél : 01 43 97 31 30
secretariatfederation@fedelec.fr - www.fedelec.fr

SVDI

5, rue de l'Amiral Hamelin - 75116 Paris
Tél : 01 44 05 84 40
contact@svdi.fr - www.svdi.fr

BCC bcconsultants.fr - Mai 2014