CONTRÔLE D'ACCÈS

Sécurité des sites à usages professionnels

Guide pour la conception d'une installation automatique de contrôle d'accès

Référentiel CNPP n° 5083

Avertissement Version numérique - Reproduction exacte de la version papier à l'exception des pages blanches qui ont été supprimées (pages 4, 6, 12, 14, 32, 36, 40, 48)

ISBN : 2-900503-72-8

Editeur :
CNPP ENTREPRISE SARL – Service Editions
Route de la Chapelle Réanville – CD 64 - BP 2265 – F 27950 SAINT-MARCEL
Tél. : 33 (0)2 32 53 64 34 – Fax : 33 (0)2 32 53 64 80
www.cnpp.com

SOMMAIRE

Ces recommandations ont été élaborées dans le cadre d'un contrat d'études réalisé par le CNPP pour la FFSA (Fédération française des sociétés d'assurance).

1. INTRODUCTION

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

Il est d'usage de distinguer deux types de pénétrations dans le site d'une entreprise, auxquelles correspondent deux types de mesures de protection :
- mesures de protection contre les pénétrations physiques pour l'accès au site ou aux locaux,
- mesures de protection contre les pénétrations logiques aux informations via les réseaux de communication.

Ce document s'intéresse aux mesures de protection contre les pénétrations physiques.

Il convient de souligner que la mise en œuvre de la sécurité sur un site ne peut être efficace que si elle intervient en complément d'une protection mécanique de base sur les enceintes, constituée de dispositifs retardant la pénétration, tels que : clôtures, murs, portes, verrous, serrures, volets, grilles, rideaux, barreaux, produits verriers…

Ces dispositifs peuvent être complétés par un ou plusieurs systèmes de surveillance, en fonction des périodes d'activités du site, tels que : contrôle d'accès, vidéosurveillance, détection d'intrusion.

Un système de contrôle d'accès est l'un de ces outils mis à disposition d'un chargé de sécurité d'un site, qui permet d'éviter les pénétrations à l'intérieur de l'entreprise de personnes pouvant constituer une menace.

Le filtrage peut être réalisé par : des moyens humains assistés ou non (exemple gardiennage avec vidéo), ou par des moyens automatisés, voire une combinaison des deux.

Ce référentiel est restreint aux systèmes automatiques de contrôle d'accès pour des besoins de sécurité. Ceci exclut le gardiennage physique ou l'interphonie, qui peuvent être associés aux systèmes automatiques de contrôle d'accès.

Ces systèmes peuvent nécessiter, selon l'importance, la présence d'opérateurs et de gestionnaires.

Le référentiel préconise des règles :
- pour la mise en œuvre des moyens,
- pour la formation des utilisateurs,
- pour la maintenance.

2. DOMAINE D'APPLICATION

Le présent document s'applique aux systèmes automatiques de contrôle d'accès pour des applications de sécurité réalisées dans tous types de sites, bâtiments ou locaux à usages professionnels.

Il s'agit d'un référentiel à l'usage des utilisateurs, prescripteurs, concepteurs et installateurs de ces systèmes.

Remarque : un élément essentiel du contrôle d'accès est l'adhésion de l'ensemble du personnel dans la préparation, la mise en place et le suivi de celui-ci. Cette étude se limite aux seuls aspects techniques.

3. TERMINOLOGIE

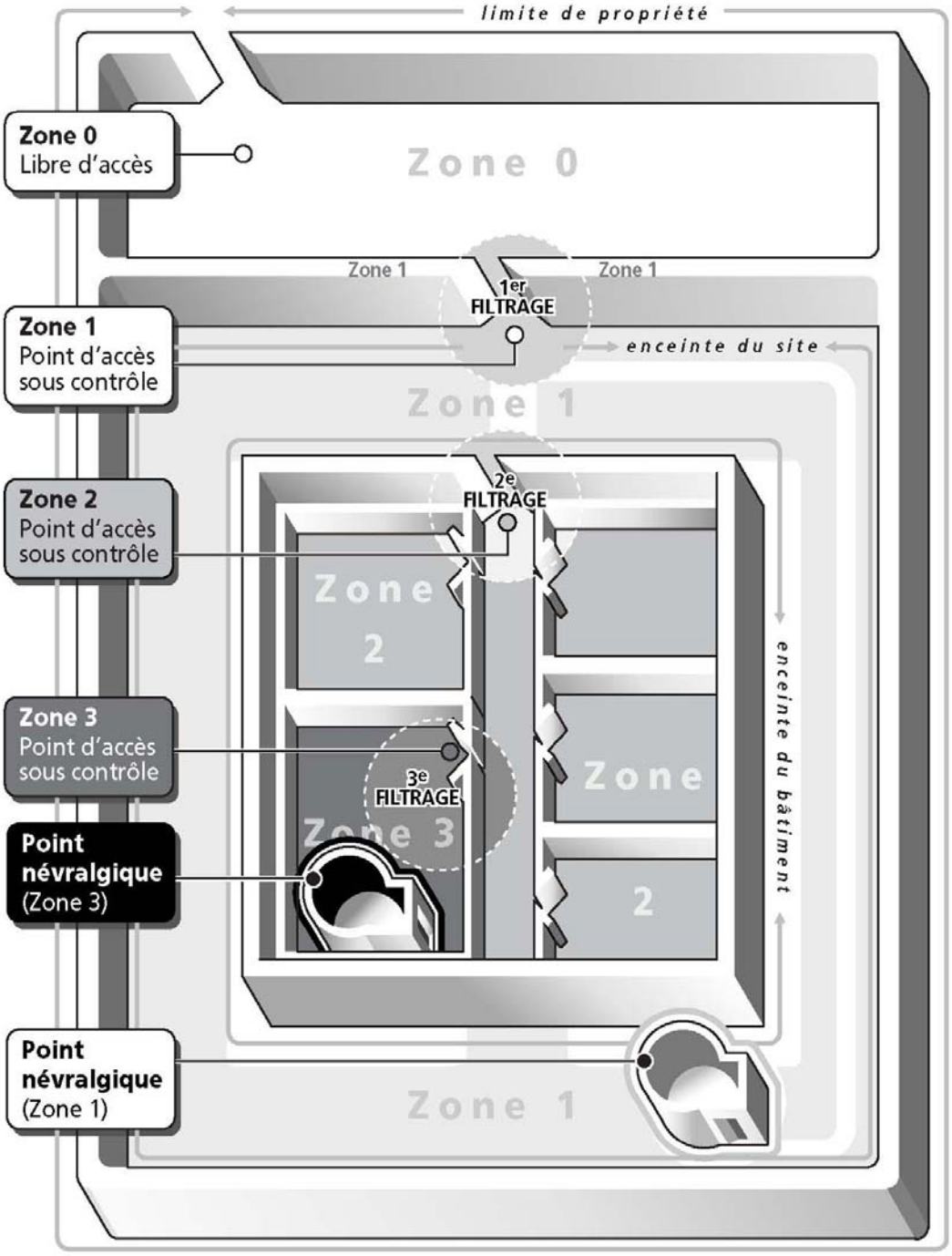
Les définitions du vocabulaire utilisé dans ce document sont les suivantes (la source est indiquée dans la dernière colonne) :

Accès	Action d'entrer ou de sortir d'une zone sous contrôle	EN 50133-1
Alarme sous contrainte	Information fournissant les mêmes résultats qu'une information mémorisée qui initialise une alerte.	EN 50133-7
Alerte / alarme	Demande d'une intervention humaine suite à l'activation d'une visualisation.	EN 50133-1
Alimentation	Partie d'un système de contrôle d'accès qui fournit l'énergie pour assurer le fonctionnement du système ou partie de celui-ci.	EN 50133-1
Anti-retour de zone sous contrôle (anti pass-back)	Mode de fonctionnement nécessitant que l'utilisateur soit présent dans une certaine zone sous contrôle, pour lui permettre d'accéder à une autre zone sous contrôle.	EN 50133-7
Anti-retour logique	Mode de fonctionnement nécessitant que l'utilisateur valide son départ d'une zone sous contrôle pour permettre son retour et vice versa.	EN 50133-7
Anti-retour temporisé	Mode de fonctionnement interdisant pendant un certain temps le processus d'autorisation à un accès en un certain point ou à une zone sous contrôle, à un utilisateur particulier après que celui-ci ait obtenu cette autorisation d'accès.	EN 50133-7
Anti-suiveur (anti tailgate)	Type de méthode d'unicité	EN 50133-7
Anti-trainard (anti loiter)	Méthode de surveillance du déplacement des utilisateurs au sein d'une zone sous contrôle	EN 50133-7
Apas	Actionneurs et capteurs d'un point d'accès. Exemples d'actionneurs : ouvreurs électriques de porte, serrures électriques, tourniquets, barrières levantes. Exemples de capteurs : contacts, interrupteurs, organes de signalisation à pression, contacteurs de porte.	EN 50133-1
Appel d'urgence	Synonyme d'alarme sous contrainte	EN 50133-7
Archivage	Enregistrement des événements	EN 50133-7
Autosurveillance	Détection d'ingérences délibérées dans le système	EN50131-1
Badge	Type d'identifiant	EN 50133-7
Base de données	Ensemble des données utilisées par le système automatique de contrôle d'accès	Référentiel
Biométrique (caractéristique)	Information qui se réfère à des attributs physiologiques uniques de l'utilisateur.	EN 50133-1
Carte	Type d'identifiant	EN 50133-7
Carte d'identification	Type d'identifiant personnalisé	EN 50133-7
Code (Numéro) personnel d'identification	Appelé " PIN " (abréviation anglaise : personnal identification number) : Synonyme de code personnel	EN 50133-7

Code personnel	Information mémorisée relative à un individu	EN 50133-7
Condition normale	Etat dans lequel le système de contrôle d'accès est entièrement fonctionnel et en mesure de traiter tous les événements dans le respect des règles établies.	EN 50133-1
Convivialité (commodité)	Caractérise la facilité d'utilisation	Référentiel
Demande d'accès	Action faite par l'utilisateur pour accéder au site	EN 50133-7
Dérangement (condition de défaut)	Toute condition qui génère l'interruption ou la dégradation de la fonctionnalité du système de contrôle d'accès.	EN 50133-1
Dérogation	Acceptation d'un accès en bipassant le processus de décision.	EN 50133-7
Dispositif de Fermeture automatique	Mécanisme assurant le fermeture automatique du point d'accès après le passage de l'utilisateur	Référentiel
Dispositif de verrouillage	Actionneur d'un point d'accès	Référentiel
Droit d'accès	Droit de l'utilisateur, en termes d'accès à une grille d'accès spécifique et à une grille horaire associée	Référentiel
Evénement	Changement apparaissant dans un système de contrôle d'accès.	EN 50133-1
Fausse acceptation	Autorisation d'un point d'accès à un utilisateur non autorisé.	EN 50133-1
Faux refus	Refus d'autorisation d'un point d'accès à un utilisateur autorisé.	EN 50133-1
Fermeture sur défaillance	Mode dans lequel l'apas ne permet pas le libre passage (apas fermé) si l'alimentation est supprimée.	EN 50133-7
Filtrage	Utilisation d'un dispositif limitant le nombre d'utilisateurs franchissant un point d'accès au même moment	EN 50133-7
Flux	Quantité d'utilisateur devant franchir le point d'accès en un temps donné	Référentiel
Grille d'accès	Une ou plusieurs zones sous contrôle allouées à un droit d'accès.	EN 50133-1
Grille horaire ou grille de temps	Une ou plusieurs zones horaires allouées à un droit d'accès.	EN 50133-1
Groupe d'accès (d'utilisateur)	Ensemble d'utilisateurs partageant le même droit d'accès	EN 50133-1
Historique	Enregistrement des événements	EN 50133-7
Identifiant	Données d'identification délivrées par des cartes d'accès, des clés, des étiquettes	EN 50133-1
Identité de l'utilisateur	Information qui est transférée directement, ou via un identifiant, par l'usager, à l'équipement d'identification.	EN 50133-1
Information d'identification	Synonyme d'identité d'un utilisateur	EN 50133-7
Information mémorisée	Information connue de l'utilisateur	EN 50133-1
Interface du point d'accès	Organe qui contrôle l'ouverture et la fermeture d'un point d'accès	EN 50133-1

Lecteur du point d'accès	Organe utilisé pour extraire les données d'identification d'un badge ou d'une caractéristique biométrique. Cet organe peut disposer d'un clavier associé lorsque l'utilisation d'une information mémorisée est prévue.	EN 50133-1
Libération	Signal donné à l'apas lorsque l'accès a été autorisé.	EN 50133-1
Libre sur défaillance	Synonyme d'ouverture sur défaillance	EN 50133-7
Mode dégradé	Mode pour lequel un accès est accepté sans réaliser la totalité du processus	EN 50133-7
Mot de passe	Chaîne de caractères qui une fois reconnue par le système de contrôle d'accès, permet d'accéder aux données du système.	EN 50133-7
Niveau de sécurité	Résistance au franchissement des points d'accès d'une zone sous contrôle sans autorisation, avec ou sans historique	Référentiel
Ouverture sur défaillance	Mode dans lequel l'apas propose le libre passage (apas ouvert) si l'alimentation est supprimée.	EN 50133-7
Paramétrage	Capacité à recevoir et à stocker des règles préétablies.	EN 50133-1
Par défaut	Paramètres de mise en service préréglés dans le système, sauf modification.	EN 50133-7
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.	EN 50133-1
Point d'accès	L'endroit où l'accès peut être contrôlé par une porte, un tourniquet ou autres barrières de sécurité.	EN 50133-1
Point névralgique	Partie du site pour laquelle l'accès par une personne non autorisée pourraient avoir des conséquences importantes.	Référentiel
Porte forcée	Synonyme de violation de l'apas	EN 50133-7
Portes interverrouillées (Sas)	Type de filtrage	EN 50133-7
Protection contre la fraude	Méthode utilisée pour protéger un système de contrôle d'accès, ou partie de celui-ci contre des ingérences délibérées.	EN 50133-1
Proximité (main libre)	Mode de fonctionnement permettant de proposer l'identité de l'utilisateur au matériel de reconnaissance sans imposer un contact physique.	EN 50133-7
Sas de sécurité (porte interverrouillées)	Apas assurant le filtrage d'unicité en permettant l'isolement de l'utilisateur afin de procéder à son identification et de lui autoriser l'accès	Référentiel
Système automatique de contrôle d'accès	Système qui comprend toutes les mesures conceptuelles et organisationnelles, ainsi que celles concernant les appareils, qui sont exigés pour contrôler automatiquement un accès.	EN 50133-1
Temps d'ouverture de porte	Temps alloué à l'apas pour rester ouvert après une ouverte autorisée.	Référentiel
Temps de libération	Temps alloué à l'utilisateur pour ouvrir l'accès	Référentiel

Traitement	Comparaison des informations avec les règles préétablies afin de prendre les décisions concernant l'autorisation ou le refus d'accès aux utilisateurs et/ou de comparer les événements avec les règles préétablies afin de déclencher les actions appropriées.	EN 50133-1
Transaction	Evénement qui correspond à la libération d'un point d'accès suite à la reconnaissance de l'identité de l'utilisateur.	EN 50133-1
Tripodes	Apas assurant le filtrage d'unicité	Référentiel
Unicité de passage	Limitation à un seul utilisateur franchissant un point d'accès au même moment.	EN 50133-7
Unité de contrôle d'accès	Organe qui prend la décision de libérer un ou plusieurs points d'accès et gère la séquence de commande associée.	EN 50133-1
Utilisateur	Personne qui demande à franchir un point d'accès.	EN 50133-1
Vérification de présence	Contrôle du nombre de personnes (max., min.) Dans la zone sous contrôle.	EN 50133-7
Verrouillé sur défaillance	Synonyme de fermeture sur défaillance	EN 50133-7
Violation d'apas	Utilisation non autorisée d'un point d'accès	EN 50133-1
Visualisation	Présentation d'une information aux responsables	Référentiel
Zone horaire	Une ou plusieurs plages horaires combinées avec des informations calendaires.	EN 50133-1
Zone sécurisée	Synonyme de zone sous contrôle	Référentiel
Zone sous contrôle	Zone entourée d'une barrière physique comprenant un ou plusieurs points d'accès.	EN 50133-1



Quelques définitions illustrées

4. ROLE D'UN SYSTEME AUTOMATIQUE DE CONTROLE D'ACCES

Les moyens de protection mécanique ou la détection électronique utilisés en période d'inactivité ne peuvent remplir pleinement leur rôle de protection d'accès aux locaux.

Pour son activité, un site à usage professionnel doit laisser pénétrer nécessairement des personnes et/ou des véhicules.

Un système automatique de contrôle d'accès permet de conserver une sécurité adaptée aux menaces potentielles durant cette période d'activité.

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

Par contrôler, il faut entendre filtrer, et donc accepter ou refuser les passages aux différentes entrées, après contrôle de l'identité et du droit d'accès des demandeurs.

Le système automatique de contrôle d'accès doit signaler, et dans certains cas assurer la traçabilité des événements, et éventuellement communiquer (échange d'informations) avec d'autres installations de sécurité.

5. MISE EN ŒUVRE

5.1 ETUDE CONCEPTUELLE

Dans le cadre du traitement du risque, une étude préalable doit mettre en évidence la nécessité de mise en œuvre d'un système automatique de contrôle d'accès à l'intérieur du périmètre de propriété d'un site.

L'étude préalable doit :

- identifier les points névralgiques d'un site et des zones à contrôler,

- analyser les flux d'individus et/ou de véhicules aux points d'accès à contrôler,

- adapter les niveaux de résistances mécaniques des enceintes,

- aboutir à un choix des niveaux de sécurité de filtrage à mettre en œuvre dans les zones sous contrôle.

En principe, l'accès à un point névralgique à l'intérieur d'une zone sous contrôle d'un site doit faire l'objet d'un filtrage. En fonction de l'étude, plusieurs filtrages consécutifs peuvent être préconisés sur le chemin de progression vers un point névralgique.

> ***Attention*** : pour tout projet, il est indispensable d'étudier le site en se rendant sur les lieux ou à partir de plans lorsqu'il s'agit d'une construction.

5.1.1 Localisation des points névralgiques et des zones sous contrôle

L'étude préalable a conduit à l'identification des points névralgiques (PN) du site, et des menaces potentielles envisagées.

La localisation de ces points névralgiques sur le site, dans des espaces physiques, permet de délimiter des zones à contrôler. Les zones sous contrôle (ZC) peuvent être : un site dans son ensemble, et/ou un bâtiment du site, et/ou un local d'un bâtiment, voire un équipement dans un local.

Le filtrage s'effectue aux différents points d'accès sur l'enceinte de la zone sous contrôle. Le filtrage peut être progressif selon la localisation des points névralgiques.

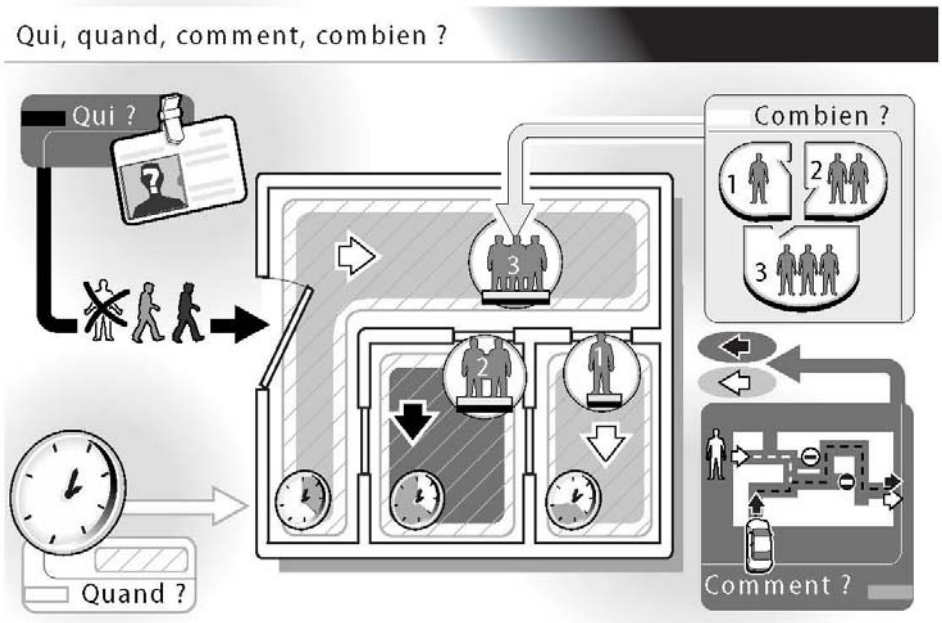
5.1.2 Analyse des flux

Une analyse des flux de circulations des individus et des véhicules doit être menée pour chaque point d'accès à contrôler. Elle doit permettre d'apporter les réponses aux questions de base :

QUI ? – QUAND ? – COMMENT ? – COMBIEN ?

L'analyse des flux doit prendre en compte :

- la nécessité de contrôler l'accès d'individus avec ou sans colis, de véhicules,
- les dimensions physiques des points d'accès à contrôler, et les natures des obstacles mécaniques,
- les différentes catégories : les individus (personnels en CDI ou CDD, intérimaires, agents de surveillance, sous-traitance à des sociétés externes, clients, visiteurs…), les véhicules (2 roues, auto, PL), les personnes handicapées,
- les différentes plages horaires,
- le nombre de passages prévisionnels, en entrée et en sortie, par catégories d'individus et par plages horaires,
- les exigences de circulation des moyens de secours et d'évacuation des personnes,
- le besoin de contrôler l'unicité de passage par des barrières adaptées, pour ne laisser passer que les personnes ayant obtenu l'autorisation.



5.1.3 Analyse des contraintes

Certaines contraintes peuvent venir orienter les choix pour la conception du système automatique de contrôle d'accès.
Ces contraintes peuvent améliorer ou réduire le niveau de sécurité du contrôle, tout au long de l'utilisation ou selon des plages horaires.

Les contraintes suivantes peuvent améliorer le niveau de sécurité, et parfois au détriment du confort d'utilisation :

- la limitation des fausses acceptations et faux refus aux points d'accès, ainsi que des fausses informations d'alarmes ou de dérangements, pour conserver la confiance en le système,

- l'acceptation des contraintes sécuritaires par les utilisateurs pour éviter les risques de dégradations ou de neutralisations de confort,

- la cohabitation avec d'autres systèmes de sécurité sur le même site (détection intrusion, détection incendie, CCTV…), ou sur d'autres sites,

- La nécessité d'avoir ou non un historique des événements passés (CNIL) pour des besoins de recherches ou de réclamations ultérieures,

- les phénomènes physiques environnementaux susceptibles d'altérer le fonctionnement des matériels (température, humidité, vibrations, foudre, perturbations électromagnétiques, etc.). Des mesures minimales doivent être prises pour en limiter les effets : par exemple mise en place de dispositifs de para-surtensions ou parafoudres, etc.

Les contraintes suivantes peuvent réduire le niveau de sécurité pour favoriser le confort d'utilisation :

- la commodité et la rapidité de passage pour les utilisateurs des éléments du système. Le nombre de lecteurs sera fonction du nombre de passages prévisionnels aux plages horaires de pointe,

- la convivialité qui impose pendant certaines plages horaires un filtrage automatique plus souple, voire des privilèges pour certaines catégories (clients VIP, autorisation sans procédures longues). Dans ce cas, des systèmes à lecture sans contacts sont à favoriser,

- l'esthétisme et l'image de marque de l'entreprise, pour un aspect plus accueillant du site,

- le fonctionnement en mode dégradé en cas de défaillances, avec le verrouillage ou la libération des points d'accès pour les besoins d'évacuations,

- le classement en ERP-IGH du bâtiment, avec l'obligation d'une classification d'identification 0 en sortie (article GHW7).

5.2 NIVEAUX DE SECURITE

> ***Attention*** : le niveau de sécurité est défini pour chaque zone sous contrôle.

Un niveau de sécurité (voir tableau ci-après) est affecté à tous les points d'accès d'une zone sous contrôle. La zone sous contrôle est caractérisée par le niveau de sécurité du plus faible de ses points d'accès.

Un niveau de sécurité définit la résistance au franchissement d'une zone sous contrôle par un individu (avec ou sans véhicule ou colis), ainsi que la nécessité de connaître les événements du passé à des fins d'investigations.

Le niveau de sécurité fait appel à différentes classifications : d'identification pour le filtrage, d'accès pour la traçabilité, et résistance à la malveillance pour des actes agressifs.

5.2.1 Classification d'identification

La classification d'identification des utilisateurs est caractérisée par la précision de l'identification des utilisateurs autorisés à pénétrer dans la zone sous contrôle.

La norme NF EN 50133-1 définit quatre classes d'identification croissantes :

- **Classe 0 –** Pas d'identification effective ;

demande d'accès sans identification (bouton poussoir, contact, détecteur).

- **Classe 1 –** Information mémorisée ;

reconnaissance de l'identification personnalisée d'un individu par composition d'un code personnel ou d'un mot de passe mémorisé (clavier).

- **Classe 2 –** Identifiant personnalisé ou caractéristique biométrique ;

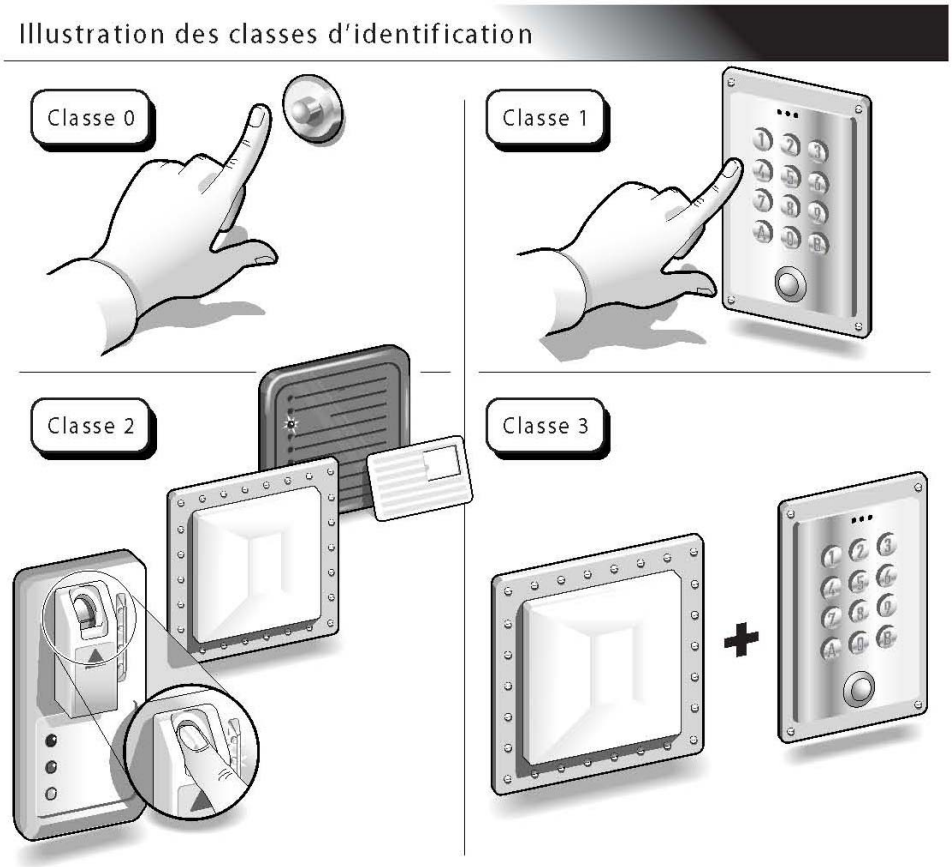
reconnaissance d'un individu par son identification personnalisée (carte magnétique, carte de proximité, carte à puce ou autre, implant, caractéristique biométrique).

Nota : La norme Européenne n'a pas fait de différence parmi les technologies selon leur difficulté à être dupliquées. Il faut cependant tenir compte de cette caractéristique dans le choix de l'identifiant.

- **Classe 3 –** Combinaison de l'identifiant personnalisé ou caractéristique biométrique + information mémorisée,
Reconnaissance d'un individu par son identification personnalisée et confirmation par un code personnel ou mot de passe mémorisé.

La classification d'identification est définie pour chaque point d'accès d'une zone sous contrôle, et peut être différente selon le sens de circulation, en entrée ou en sortie. *Par exemple, la sortie peut être sans identification au moyen d'un bouton poussoir.*

Attention : pour un niveau d'identification en entrée de classe 3, la sortie devrait se faire au minimum par un moyen d'identification de classe 1 ou 2.



5.2.2 Classification d'accès

Les systèmes automatiques de contrôle d'accès sont classés en fonction de la nécessité d'utiliser une grille horaire, constituée d'une ou plusieurs périodes horaires, pour définir les droits d'accès aux différentes catégories d'utilisateurs, et d'enregistrer les transactions d'accès.

La norme NF EN 50133-1 définit trois classes d'accès :

- **Classe A** – Pas de grille horaire, ni d'enregistrement des transactions.
- **Classe B** – Grille horaire et enregistrement des transactions.
- **Classe Ba** – Grille horaire mais sans enregistrement des transactions.

> ***Attention*** : la classification d'accès est définie pour chaque point d'accès d'une zone sous contrôle et peut être différente pour l'entrée et la sortie.

5.2.3 Classification de résistance à la malveillance

Les composants et les liaisons équipant les points d'accès d'un système automatique de contrôle d'accès sont classés selon des critères de résistance à la malveillance (fraude + effraction).

La résistance à la malveillance est définie pour chaque point d'accès de la zone sous contrôle. Elle comporte obligatoirement une résistance minimale à la poussée mécanique et à la fraude.

Elle peut être complétée par une résistance à l'effraction selon les paramètres établis pour les serrures de bâtiment (voir l'annexe 6 des Règles techniques T61 – Spécifications et méthodes d'essais – Serrures de bâtiment et le Règlement particulier de la marque A2P – H61 - CNPP).

- **Classe E0** – Résistance minimale à la poussée.
- **Classe E1** – Résistance à l'effraction correspondant à la catégorie ☆.
- **Classe E2** – Résistance à l'effraction correspondant à la catégorie ☆☆.
- **Classe E3** – Résistance à l'effraction correspondant à la catégorie ☆☆☆.

La classification de résistance à la malveillance d'un accès doit être en rapport avec la résistance mécanique des parois de la zone sous contrôle. Par exemple, il serait inutile d'imposer une classification de résistance à la malveillance E3, si de larges baies de simples vitrages délimitent la zone sous contrôle.

Les composants de traitement n'équipant pas directement les points d'accès ne sont pas classés car ils doivent être placés dans un lieu assurant leur sécurité vis-à-vis de la malveillance (ex : dans la zone sous contrôle concernée).

NIVEAUX DE SÉCURITÉ

Niveau	Filtrage des pénétrations Traçabilité des événements Actes de malveillances	Classification d'identification	Classification d'accès	Classification résistance	Descriptif du niveau de sécurité
I	Filtrage des pénétrations involontaires ou de curieux	1 ou 2	A	E0	Sans enregistrement Résistance minimale Information mémorisée ou identifiant personnalisé
II	Filtrage des pénétrations involontaires ou de curieux Traçabilité des évènements écoulés	1 ou 2	**B**	E0	**Enregistrement** Résistance minimale Information mémorisée ou identifiant personnalisé
III	Filtrage des pénétrations préméditées de personnes initiées Traçabilité des évènements écoulés Attaques mécaniques par outillage léger	1 ou 2	B	**E1**	Enregistrement **Résistance catégorie☆** Information mémorisée ou identifiant personnalisé
IV	Filtrage des pénétrations préméditées de personnes initiées et équipées - Contrôle de l'unicité de passage Traçabilité des évènements écoulés Attaques mécaniques par outillage lourd	**2**	B	**E2**	Enregistrement **Résistance catégorie☆☆** **Identifiant personnalisé**
V	Filtrage des pénétrations préméditées de personnes initiées, équipées, et en possession éventuelle d'identifiant- Contrôle de l'unicité de passage Traçabilité des évènements écoulés Attaques mécaniques par outillage lourd	**3**	B	E2	Enregistrement Résistance catégorie☆☆ **Information mémorisée + identifiant personnalisé**
VI	Filtrage des pénétrations préméditées de personnes initiées, fortement équipées, et en possession éventuelle d'identifiant- Contrôle de l'unicité de passage Traçabilité des évènements écoulés Attaques mécaniques par outillage lourd sur longue durée	3	B	**E3**	Enregistrement **Résistance catégorie☆☆☆** Information mémorisée + identifiant personnalisé

5.3 INSTALLATION

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

5.3.1 Généralités

Une installation de système automatique de contrôle d'accès doit posséder les qualités essentielles de fiabilité et de disponibilité. Une telle installation est sûre lorsqu'elle remplit son rôle de façon durable, non erratique, dans les conditions et circonstances définies par les constructeurs des matériels constitutifs de l'installation.

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

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

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

Le raccordement des équipements au réseau électrique doit être effectué, selon les différentes dispositions de la norme NF C 15-100 (cf. 5.4.2).

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

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

Les matériels doivent être solidement fixés sur leurs supports par les moyens normalement prévus dans les notices des constructeurs.

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

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

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

5.3.2 Fonctions fondamentales

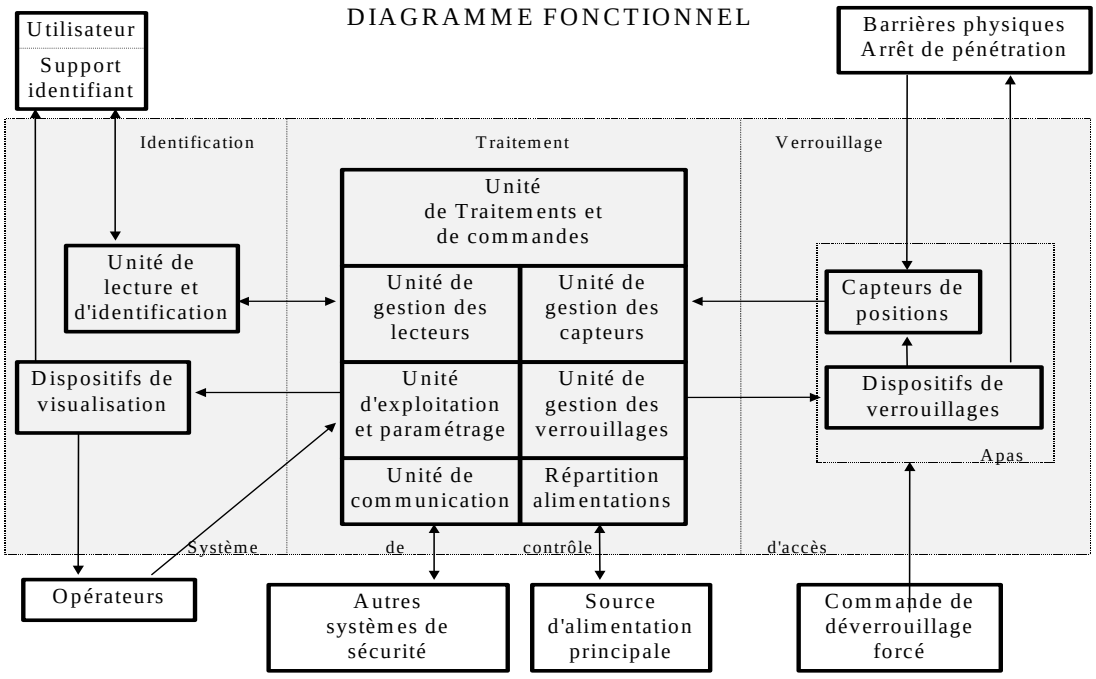
Une installation de contrôle d'accès peut être décomposée en fonctions fondamentales pour un ou plusieurs points d'accès, et qui assurent : l'identification des utilisateurs, le traitement des données et les commandes, et le verrouillage des points accès.

Ces fonctions peuvent être intégrées en un seul coffret ou être réparties dans plusieurs coffrets. Dans ce dernier cas, l'installation de contrôle d'accès est constituée de matériels compatibles, à liaisons filaires.

Le choix du type de matériel dépend des niveaux de sécurité du site.

Les matériels doivent comporter, de façon apparente ou non, des indications suffisantes pour être identifiés sans risque d'erreur (nom du fabricant, modèle, type, etc.).

Le diagramme suivant définit les relations entre les différentes fonctions dans une configuration de base d'une installation de contrôle d'accès. Certains systèmes peuvent ne regrouper que quelques fonctions fondamentales, et d'autres systèmes plus complexes les multiplier.



5.3.3 Lecteurs

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

Le dispositif est installé à proximité du point d'accès à contrôler. Pour les lecteurs sans contact, ils doivent être implantés derrière une paroi de protection ou à l'intérieur de la zone sous contrôle. Les préconisations des notices des constructeurs doivent être respectées.

Les vis de fixation des lecteurs ne doivent pas être directement accessibles hors de la zone sous contrôle avec le niveau de sécurité le plus important.

Le lecteur placé à l'extérieur de la zone sous contrôle doit être doté d'une autosurveillance à l'arrachement.

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

Une signalisation sur le lecteur ou à proximité doit informer l'utilisateur de l'accord et du refus de passage lors d'une demande d'accès.

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

5.3.4 Traitement et commandes

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

L'unité de traitement et de commandes centralisée doit être mise en place dans la zone sous contrôle du niveau de sécurité le plus élevé.

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

Les coffrets contenant des éléments vitaux du système (exemple : alimentations) doivent être implantés dans la zone sous contrôle du côté du niveau de sécurité le plus élevé.

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

5.3.4.1 Signalisations

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

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

Des capteurs doivent signaler à l'unité de traitement les positions des points d'accès (ouvert ou fermé) et des pênes des dispositifs de verrouillage (entrés ou sortis).

L'unité de traitement doit signaler à l'opérateur les événements suivants :

- Détection d'activation de l'autosurveillance.

- Point d'accès ouvert sans autorisation.

- Point d'accès ouvert par déverrouillage forcé provenant d'un système extérieur (système incendie, organe de commande mécanique).

- Point d'accès ouvert au-delà de la période autorisée (dans le cas de l'utilisation d'une grille horaire).

- Défaillance ou niveau bas d'une source d'alimentation.

5.3.4.2 Enregistrements

Un système de contrôle d'accès de classe d'accès B doit enregistrer de manière horodatée tous les événements suivants :

- Transactions avec identification de l'utilisateur et localisation de l'accès.

- Accès refusés aux utilisateurs, avec localisation de l'accès.

- Détection d'activation de l'autosurveillance, avec localisation de l'accès.

- Point d'accès ouvert sans autorisation.

- Point d'accès ouvert par déverrouillage forcé provenant d'un système extérieur (système incendie, organe de commande mécanique).

- Point d'accès ouvert au-delà de la période autorisée (dans le cas de l'utilisation d'une grille horaire).

- Entrée et sortie du mode de paramétrage.

- Défaillance ou niveau bas d'une source d'alimentation.

> ***Attention :*** le traitement d'informations nominatives doit être déclaré auprès de la CNIL. Il existe une délibération CNIL (n° 02-001 du 8 janvier 2002) concernant les traitements automatisés d'informations nominatives mis en œuvre sur les lieux de travail pour la gestion des contrôles d'accès aux locaux, des horaires et de la restauration – Voir les annexes.

5.3.5 Verrouillage

Le dispositif de verrouillage permet de réaliser le blocage mécanique du point d'accès, pour empêcher le passage de personnes non autorisées.

Ce dispositif doit offrir une résistance mécanique minimale aux tentatives de pénétrations. Il doit résister à une poussée perpendiculaire de la porte de 300 daN, et chaque pêne à un effort axial de 100 daN dans le sens de déverrouillage.

Selon les exigences particulières vis à vis d'ouverture anormale, le dispositif de verrouillage peut nécessiter une résistance à la malveillance plus élevée.

5.3.6 Liaisons

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

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

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

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

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

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

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

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

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

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

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

5.3.7 Cas du dispositif intégré autonome

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

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

Ces dispositifs ont un type d'alimentation limité en énergie et en puissance disponible. Leurs résistance mécaniques aux attaques sont relativement faibles et donc les utilisations sont restreintes à des niveaux de sécurité I ou II maximum.

Les vis de fixation du dispositif doivent être placées du coté de la zone sous contrôle de niveau de sécurité le plus élevé.

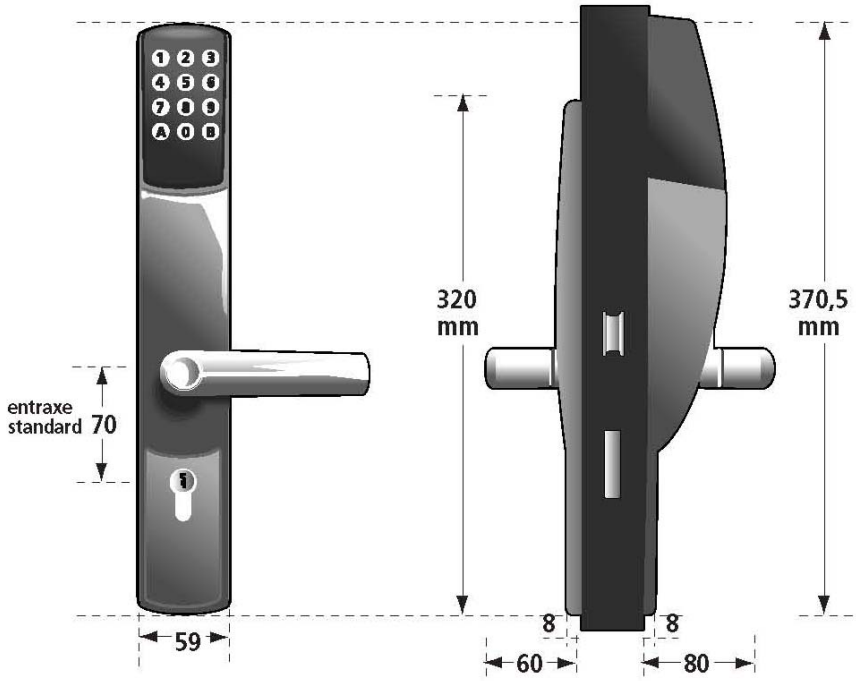
Le coffret du dispositif doit être doté d'une autosurveillance à l'ouverture et à l'arrachement. Une signalisation sonore interne doit intervenir en cas de manipulation non autorisée.

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

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

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

Face avant et profil du dispositif intégré autonome



5.4 ALIMENTATION ELECTRIQUE

5.4.1 Généralités

L'installation doit être alimentée :

- soit par une alimentation principale interne – dite autonome (piles).

- soit par une alimentation principale externe fournie par le réseau basse tension (230 V) et sauvegardée par une alimentation secondaire (batteries d'accumulateurs).

5.4.2 Sécurité électrique

Le raccordement des équipements au réseau électrique doit être effectué, entre autres, selon les règles de l'art, et dans le respect de la norme NF C 15-100 - Installations électriques à basse tension (diamètres des câbles, boîtiers de classe I et III, liaisons équipotentielles à la terre, degrés de protection IP et IK, etc.) et des décrets en vigueur (notamment en matière d'habilitation électrique du personnel).

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

5.4.3 Autonomie de l'installation

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

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

Pour un système à alimentation externe, l'alimentation secondaire doit assurer, en cas d'absence de l'alimentation principale, le fonctionnement de l'installation de contrôle d'accès pendant une durée minimale. Cette durée est fonction de la résistance à la fraude souhaitée de l'installation face aux coupures de l'alimentation principale. Elle ne doit pas être inférieure à **3 heures**.

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

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

Si les dispositifs de verrouillage nécessite une consommation importante, le site pourra disposer d'un groupe électrogène, l'installation peut y être raccordée, pour autant qu'une défaillance ou un défaut affectant les autres circuits alimentés par cette source ne perturbe pas le circuit d'alimentation de l'installation.

Le groupe électrogène doit assurer une reprise effective en énergie, de façon automatique, après la coupure de l'alimentation principale. Il ne se substitue pas à l'alimentation secondaire de l'installation.

A l'issue de cette durée d'autonomie, en absence totale d'alimentation, la conservation des données mémorisées doit être assurée par le système pendant au moins 120 heures. De plus, cela doit entraîner le verrouillage en entrée du ou des points d'accès concernés. En contre partie le système doit disposer d'un mécanisme manuel d'urgence pour le déverrouillage en sortie (évacuation) et en entrée pour la maintenance.

6. FORMATION DES UTILISATEURS

6.1 GENERALITES

Les systèmes de contrôle d'accès doivent permettre de gérer pratiquement en temps réel des demandes d'accès des utilisateurs. Chaque utilisateur peut se voir allouer des droits d'accès individuels plus ou moins restrictifs en fonction du temps et des points d'accès.

Les systèmes de contrôle d'accès utilisent des bases de données informatiques pour affectés les droits d'accès à chaque utilisateur. Les logiciels employés peuvent être très complexes et nécessitent donc une bonne formation des exploitants des systèmes.

La formation est spécifique selon la nature des interventions des exploitants. Il peut être distingué quelques familles principales :

- Les administrateurs – chargés de la configuration des matériels de l'installation et du paramétrage des droits d'accès et de la hiérarchisation.

- Les opérateurs – chargés de la saisie quotidienne des identifiants et de leurs affectations aux différents utilisateurs.

- Les utilisateurs internes à l'entreprise – Ils peuvent avoir des droits d'accès aux zones sous contrôle permanents ou temporaires.

- Les utilisateurs externes à l'entreprise – sociétés extérieures, stagiaires, visiteurs, etc. Ils peuvent avoir des droits d'accès aux zones sous contrôle permanents ou temporaires.

6.2 FORMATION INITIALE

La formation initiale est à faire avant la mise en place définitive de l'installation. Elle doit permettre aux administrateurs et opérateurs d'être prêts à l'exploitation du système dès le premier jour de mise en service afin de limiter un phénomène de rejet par les utilisateurs.

La formation des administrateurs est la plus longue et délicate. Elle est rendue indispensable par la nécessité de comprendre toute l'architecture du système et les logiques de paramétrage. Si le fournisseur de l'installation inclut un paramétrage initial du système, l'implication des administrateurs avant la réception est impérative.

Les formations peuvent avoir un caractère théorique, mais elles doivent se finaliser par des exercices pratiques et de préférence sur le système installé sur le site concerné.

6.3 FORMATION CONTINUE

Au fil des années, le renouvellement des personnels des utilisateurs peut entraîner une perte des connaissances sur les possibilités offertes par le système de contrôle d'accès. Il en résulte alors une utilisation restreinte aux habitudes avec l'incapacité de le faire évoluer, et parfois des dysfonctionnements pour des raisons de conflits de paramétrage.

Afin d'éviter que les performances du système décline, il est nécessaire de maintenir un niveau de formation pour les nouveaux administrateurs ou opérateurs. C'est un investissement en temps non négligeable, à planifier en dehors de période de crise, sans attendre le blocage du système.

Pour les opérateurs, la formation en interne peut être suffisante, en fonction de l'expérience du formateur : administrateur ou opérateur responsable.

Pour les administrateurs, la formation en interne est utile mais insuffisante. Le recours à une formation externe est nécessaire pour comprendre l'ensemble de l'architecture du système et des logiques de paramétrage.

6.4 SAUVEGARDES

Un dossier du paramétrage du système de contrôle d'accès doit être rédigé. Il doit mettre en évidence toutes les grilles temporelles créées, avec la raison de leurs création et les catégories d'utilisateurs associées.

Les bases de données informatiques évoluent sans cesse. Il est indispensable de prévoir une procédure de sauvegarde des données. Deux types de données peuvent être sauvegardées différemment :

- La base de configuration du système – par un administrateur.

- La base des utilisateurs et droits associés – par un administrateur ou un opérateur.

Au minimum, une sauvegarde devrait être réalisée une fois par trimestre. Cependant, plus les modifications de données sont fréquentes, plus les sauvegardes des bases de données doivent être rapprochées.

Les sauvegardes doivent être réalisées sur des supports de conservation différents que ceux des bases originales, et stockées dans des lieux différents sous contrôle d'accès. Si des supports magnétiques sont utilisés, ils doivent être remplacés régulièrement pour éviter les détériorations d'usure.

7. RECEPTION DE L'INSTALLATION

7.1 GENERALITES

La réception est une remise officielle de l'installation entre les mains de l'utilisateur, après que l'installateur ai effectué une vérification de conformité et remis un dossier technique.

La vérification de conformité a lieu à la mise à disposition ou après la modification d'une installation.

L'installateur doit faire le nécessaire pour que l'utilisateur et éventuellement le demandeur du système soit informé de la date de la vérification de conformité, afin qu'ils puissent être présents ou y déléguer un représentant.

La vérification de conformité a pour but de s'assurer que l'installation remplit effectivement les fonctions pour lesquelles elle est prévue.

7.2 CONSTITUTION DU DOSSIER TECHNIQUE

L'installateur établit un dossier technique en 2 exemplaires conservés dans des lieux sûrs. L'un est conservé par l'installateur, et le second est remis à l'utilisateur. Certains éléments ne sont portés qu'au dossier de l'utilisateur (éléments spécifiques à l'installation et à son fonctionnement).

Ce dossier comporte au minimum :

- l'étude conceptuelle, mettant en évidence les points névralgiques du site, les zones sous contrôle et les points d'accès,

- les niveaux de sécurité attribuées aux zones sous contrôle,

- le descriptif technique complet de l'installation,

- les modifications apportées au devis initial pour lesquelles l'utilisateur a donné son accord,

- la documentation des matériels utilisés (éléments destinés a l'utilisateur),

- les notices d'exploitation indiquant très clairement à l'utilisateur les opérations à effectuer pour assurer le fonctionnement de l'installation,

- les consignes en cas de panne et dysfonctionnement,

- les conditions de garantie et de maintenance.

7.3 VERIFICATION DE CONFORMITE

7.3.1 Vérifications générales

Elles consistent à procéder aux vérifications :

- de la conformité de l'installation avec le dossier technique,

- de l'existence des documents d'exploitation,

- du respect des règles de l'art et des normes en vigueur,

- de l'installation, aux emplacements prévus, des matériels solidement fixés,

- de l'accessibilité des lecteurs et des dispositifs de signalisations.

- de la conformité du câblage de l'installation aux spécifications du § 5.3.6.

7.3.2 Vérification fonctionnelle de l'installation

La vérification fonctionnelle de l'installation a pour but de s'assurer que toutes les fonctions sont effectivement opérantes.

7.3.2.1 Contrôle des alimentations

Vérifier la présence de l'alimentation principale autonome ou externe.

Dans le cas d'alimentation principale externe, vérifier que l'alimentation secondaire prenne le relais lors d'une coupure.

7.3.2.2 Essais de fonctionnement des lecteurs

Vérifier que, compte tenu des niveaux de sécurité retenus, les lecteurs répondent aux sollicitations de demande d'accès.

Vérifier que les signalisations d'autorisation ou de refus d'accès sont parfaitement visibles pour l'utilisateur.

7.3.2.3 Contrôle des dispositifs de verrouillage

Vérifier que les systèmes de fermeture automatique permettent de repositionner correctement les obstacles mécaniques des points d'accès.

Vérifier que les dispositifs de verrouillage condamnent parfaitement les points d'accès.

Vérifier que les contacts signalent les positions des dispositifs de verrouillage.

7.3.2.4 Vérification des temporisations

Lorsque le système dispose d'une base horaire, s'assurer que les temporisations de libération du point d'accès et des durées d'ouvertures sont conformes avec les paramétrages effectués.

7.3.2.5 Contrôle de l'autosurveillance

L'ouverture des boîtiers des différents éléments de l'installation (lecteurs, armoires de traitement, dispositifs de verrouillage, boîtiers de raccordement, etc.) doit déclencher les dispositifs de signalisation d'alarme.

7.3.3 Résultat de la vérification de conformité

A l'issue des opérations décrites précédemment, la réception de l'installation est prononcée si les toutes les conditions définies ci-dessus sont remplies.

L'installateur remet alors à l'utilisateur le dossier technique décrit au § 7.2.

Au terme de ces vérifications, l'installateur doit présenter l'installation à l'utilisateur, effectuer devant lui les manœuvres d'utilisation et s'assurer qu'elles ont bien été assimilées.

Les résultats de la vérification de conformité doivent être conservés par l'installateur.

8. MAINTENANCE

8.1 GENERALITES

Après la mise à disposition, une installation de contrôle d'accès est soumise à des vérifications régulières afin de conserver dans le même état de fonctionnement les matériels susceptibles de se dégrader ou défaillants.

Certaines de ces vérifications peuvent être réalisées par les services d'entretien interne à l'utilisateur, d'autres vérifications périodiques ou interventions correctives en cas de panne ou de dérangement seront réalisées par un installateur.

Pour ce faire, l'utilisateur doit souscrire auprès d'un installateur (de préférence celui qui a réalisé l'installation) un contrat de maintenance reconductible, pour effectuer un contrôle complet de l'installation.

Un contrat de maintenance doit préciser : la fréquence des visites de vérification périodique, la nature des opérations effectuées et un délai maximal d'intervention en cas de panne ou de dérangement.

8.2 ENTRETIEN PERMANENT

Certaines opérations de vérifications et d'entretien doivent être réalisées prises en charge directement par les services d'entretien de l'utilisateur.

Il s'agit de prévoir la possibilité de remplacer quotidiennement les éléments du système de contrôle d'accès qui ont un fort taux d'usure dans l'utilisation.

L'utilisateur doit disposer d'une réserve de pièces détachées pour assurer la continuité de fonctionnement du contrôle. Elles concernent essentiellement : les mécanismes de verrouillage, les ferme-portes automatiques, les badges, etc.

8.3 VERIFICATIONS PERIODIQUES

8.3.1 Rôle des vérifications périodiques

Ces visites de vérifications périodiques ont pour objectif, au titre de la maintenance préventive, de vérifier et d'informer sur le bon fonctionnement de l'installation.

Il est conseillé que les visites de vérifications périodiques soient effectuées régulièrement avec au minimum une visite annuelle. Selon l'importance de l'installation et la vulnérabilité du site, la fréquence des vérifications pourra être plus élevée en accord avec l'utilisateur.

A chaque visite de vérification périodique, l'installateur doit interroger l'utilisateur sur l'exploitation de l'installation de contrôle d'accès, et en particulier sur les problèmes éventuels liés à son fonctionnement.

Lors de la visite, l'installateur vérifiera l'application effective des sauvegardes régulière des données par l'utilisateur.

8.3.2 Nature des opérations de vérifications

Après un contrôle visuel de l'installation (permettant de déceler, par exemple, un lecteur mal fixé, l'endommagement des matériels, des portes se refermant mal, etc.), le technicien de maintenance vérifie l'efficacité de l'installation de contrôle d'accès.

Les contrôles qui doivent être effectués sont les suivants :

- Le contrôle des alimentations (voir § 7.3.5.1) :

- Vérification des tensions de batteries et de chargeurs, pour les systèmes avec alimentation principale externe et secondaire.

- Vérifications des consommations de l'installation.

Les opérations de maintenance sont effectuées sur la ou les sources d'alimentation secondaire.

- Vérification de l'état des piles, pour les systèmes avec alimentation autonome interne.

- Les essais de fonctionnement des lecteurs (voir § 7.3.5.2) :

- Nettoyage des lecteurs (touches, têtes de lecture, contact, etc.).

- Vérification les signalisations d'autorisation et de refus d'accès.

- Le contrôle des dispositifs de verrouillage (voir § 7.3.5.3) :

- Vérification de la fermeture automatique des points d'accès.

- Vérification du verrouillage des points d'accès.

- Vérification de la signalisation des positions des points d'accès.

• Vérification des temporisations (voir § 7.3.5.4) :

- Vérification des temporisations de libération des points d'accès.

- Vérification des durées d'ouverture.

• Le contrôle de l'autosurveillance (voir § 7.3.5.5) :

- Vérification de la détection à l'ouverture des boîtiers, y compris des boîtes de raccordement.

8.4 MAINTENANCE CORRECTIVE

Ces interventions ont pour objectif de remettre en état de fonctionnement l'installation suite à une panne ou une défaillance.

Les interventions sont à effectuer dans des conditions clairement définies dans le contrat : délais d'intervention, heures et jours d'intervention, coûts des prestations.

L'installateur doit être en mesure de procéder à une intervention en cas de panne ou de dérangement dans le délai imparti après l'appel de l'utilisateur, sous réserve que celui-ci lui donne l'accès aux locaux et sauf cas de force majeure. Ce délai imparti ne devrait pas être supérieur à 48 heures ouvrables.

Dans la mesure ou l'installation ne peut être remise en état dans un délai imparti, l'installateur doit en informer l'utilisateur en précisant le délai prévisionnel de remise en état, et le motif du report.

L'utilisateur doit, en cas de panne ou de dérangement de l'installation, avertir immédiatement l'installateur, pour faire effectuer les réparations et la remise en état de l'installation, et prendre pendant la période de panne ou de défaillance, toute mesure de sécurité ou de gardiennage qui s'impose.

8.5 REGISTRE DE MAINTENANCE

La mention des opérations effectuées, tant en internes que par un installateur, et les incidents constatés sont portés sur un registre de maintenance détenu par l'utilisateur.

Ce registre de maintenance doit faire clairement apparaître la traçabilité entre les vérifications anciennes et nouvelles.

L'installateur peut remettre à l'utilisateur une fiche de maintenance à l'issue de chaque visite de vérifications périodiques ou de maintenance corrective. Les fiches seront jointes au registre de maintenance.

Le détail des opérations effectuées par l'installateur et la durée de l'intervention devront être mentionnés dans le registre de maintenance ou sur les fiches de maintenance.

8.6 MODIFICATIONS APPORTEES A UNE INSTALLATION

Les modifications apportées à une installation de contrôle d'accès doivent être effectuées également selon les prescriptions du présent référentiel.

Toute modification de l'installation entraîne obligatoirement une mise à jour du dossier technique de l'installation.

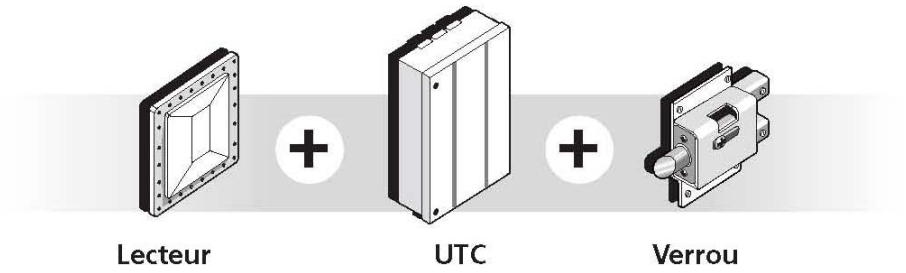
Une modification importante nécessite une nouvelle réception, partielle ou totale, de l'installation.

9. AIDE AU CHOIX DU NIVEAU DE SECURITE

Ce chapitre est une aide à un futur utilisateur ou prescripteur d'un système de contrôle d'accès pour définir son besoin en fonction du niveau de sécurité souhaité pour ses zones sous contrôle.

Niveau I – Filtrage des accès pour éviter des pénétrations involontaires ou de curieux.

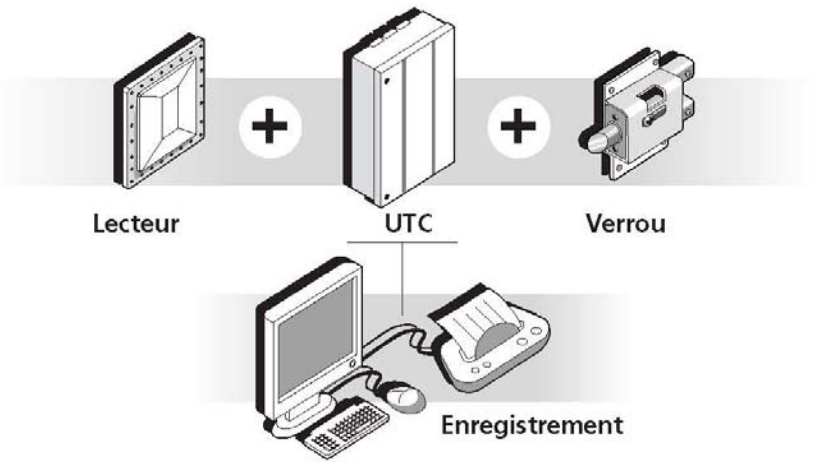
➔ Contrôle d'accès par identification simple (information mémorisée ou identifiant personnalisé) sans enregistrement.



A partir du niveau suivant, une traçabilité des demandes d'accès est requise pour permettre des investigations lorsque des évènements se sont produits.

Niveau II – Filtrage des accès pour éviter des pénétrations involontaires ou de curieux.

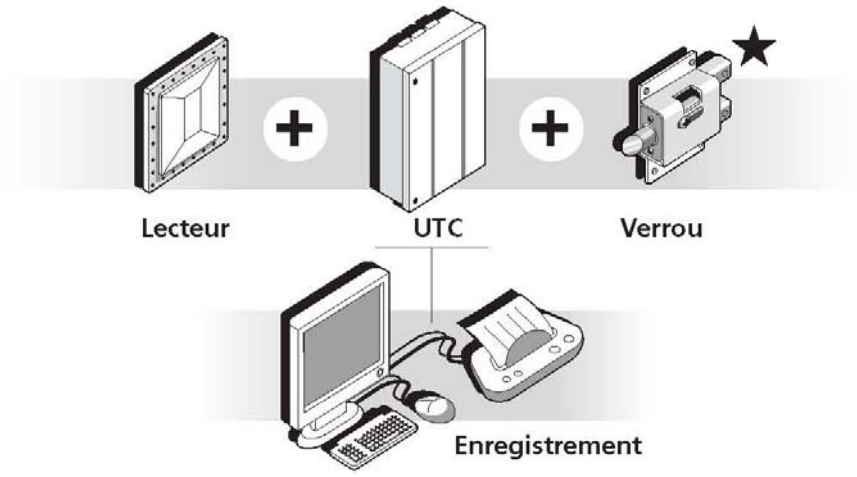
➔ Contrôle d'accès par identification simple (information mémorisée ou identifiant personnalisé) ***avec*** enregistrement.



Niveau III – Filtrage des accès pour éviter des pénétrations préméditées de personnes initiées.

➔ Contrôle d'accès par identification simple (information mémorisée ou identifiant personnalisé) ***avec*** enregistrement.

Résistance à l'effraction des accès par outillage léger (☆).

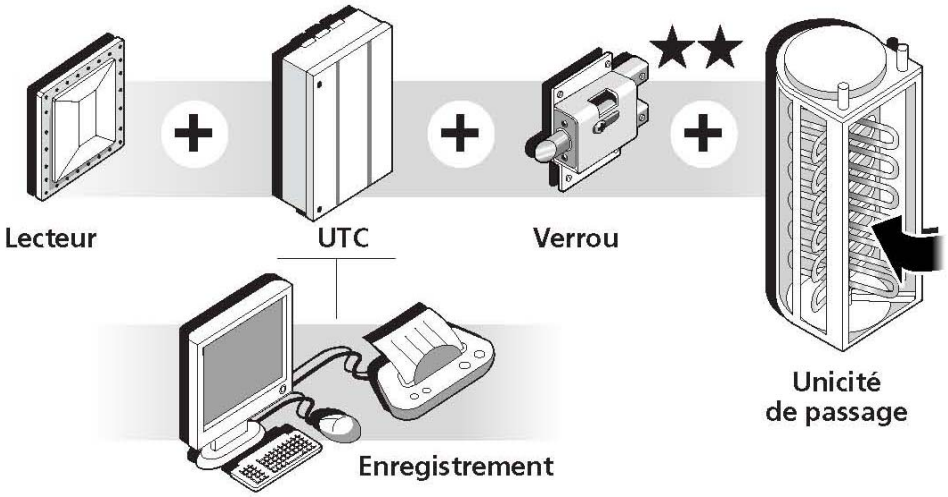


A partir du niveau suivant, la résistance des parois à l'effraction doit être équivalente à celle demandée pour les points d'accès pour homogénéiser la protection. Il est en outre opportun de contrôler l'unicité de passage aux accès.

Niveau IV – Filtrage des accès pour éviter des pénétrations préméditées de personnes initiées et équipées.

➔ Contrôle d'accès par identification simple (identifiant personnalisé) avec enregistrement, et contrôle de l'unicité de passage.

Résistance à l'effraction des accès ***par outillage lourd (☆☆).***

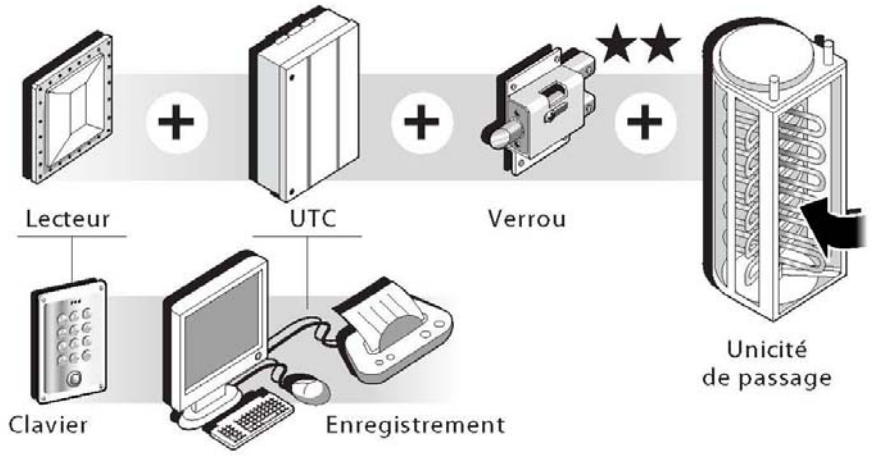


A partir du niveau suivant, il est nécessaire de vérifier que le possesseur du code ou du badge identifiant est bien le titulaire du droit d'accès.

Niveau V – Filtrage des accès pour éviter des pénétrations préméditées de personnes initiées et équipées.

➔ Contrôle d'accès par identification ***confirmée*** (***information mémorisée*** + identifiant personnalisé) avec enregistrement, et contrôle de l'unicité de passage.

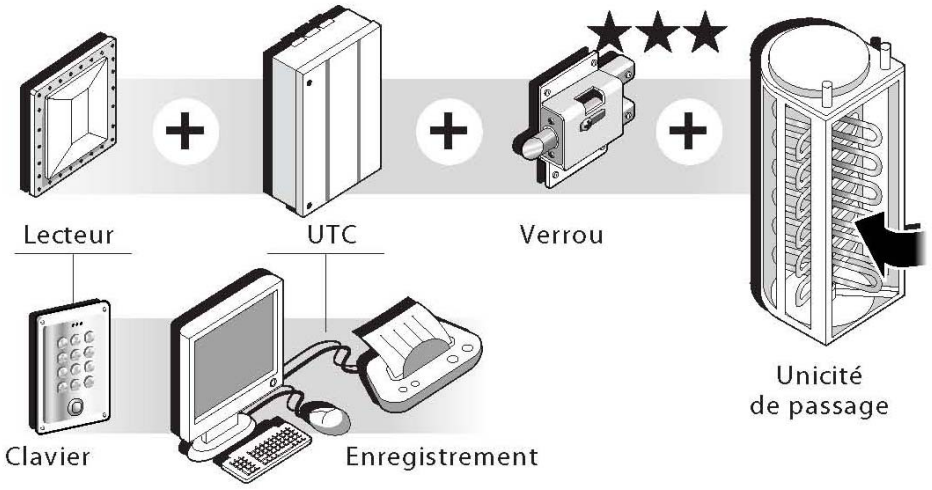
Résistance à l'effraction des accès par outillage lourd (☆☆).



Niveau VI – Filtrage des accès pour éviter des pénétrations préméditées de personnes initiées et fortement équipées.

➔ Contrôle d'accès par identification ***confirmée*** (***information mémorisée*** + identifiant personnalisé) avec enregistrement, et contrôle de l'unicité de passage.

Résistance à l'effraction des accès par outillage lourd ***et sur une longue durée (☆☆☆).***



ANNEXES

- CNIL – Norme simplifiée n° 42 concernant les traitements automatisés d'informations nominatives mis en œuvre sur les lieux de travail pour la gestion des contrôles d'accès aux locaux, des horaires et da la restauration

- CNIL – Modèle de déclaration simplifiée. Voir www.cnil.fr