SIEMENS

Contrôle d’accès

www.siemens.ch/controle-acces

Sommaire

1. Contrôle d'accès

1.1. Introduction

Le contrôle d'accès régit l'accès aux bâtiments ou aux zones nécessitant une protection selon les principes «Qui, quand, où?» et, éventuellement, «avec qui?». Un système de contrôle d'accès est un outil électronique responsable de contrôler les accès et vérifiant automatiquement si une personne a les autorisations pour accéder à un bâtiment, une zone ou une pièce déterminée. La durée de ces autorisations est également définie. Celles-ci peuvent être uniques, limitées dans le temps ou illimitées. Un système de contrôle d'accès augmente sensiblement la sécurité et soutient les processus de l'entreprise.

1.1.1. Mission d'un contrôle d'accès

Un système de contrôle d'accès organise l'accès via un ensemble de règles définies par l'exploitant. Les autorisations sont accordées selon des critères basés sur les personnes, les locaux et le temps. Il est ainsi possible de n'octroyer l'accès qu'aux personnes qui se sont identifiées par un dispositif déterminé (p. ex. une carte, un badge, un code PIN ou des caractéristiques biométriques).

Objectifs du contrôle d'accès

- Un système de contrôle d'accès n'accorde l'accès régulier qu'aux personnes autorisées
- Il régit qui a accès, quand, où et éventuellement, avec qui

Basés sur des mesures électroniques, organisationnelles et architecturales, les systèmes modernes de contrôle d'accès protègent les bâtiments, les équipements, et surtout les personnes, des attaques et des menaces de personnes non-autorisées et empêchent le vol de propriété intellectuelle. Le défi particulier du contrôle d'accès tient au fait qu'il faut limiter aussi peu que possible la liberté de mouvement des personnes autorisées, tout en interdisant totalement l'accès aux personnes non-autorisées. Le contrôle d'accès possède également un rôle préventif important par l'effet de dissuasion. Il n'empêche certes pas les attaques par les personnes autorisées mais permet néanmoins leur identification en cas d'incident.

1.2. Structure d'un système de contrôle d'accès

Un système se compose au moins des trois éléments suivants:

- **Lecteur:** le lecteur identifie ou vérifie l'identité de l'utilisateur et transmet ces informations à la centrale.
- **Composant:** si la vérification est positive dans la centrale, l'accès est autorisé.
- **Centrale de contrôle d'accès:** la centrale vérifie elle-même des paramètres spécifiques de la demande d'accès (système hors ligne) ou demande leur confirmation à une instance de contrôle centralisée (système en ligne).

Les différents composants d'un système de contrôle d'accès sont décrits en détail dans les chapitres qui suivent. Les concepts systèmes diffèrent selon le fabricant. Parmi les systèmes électroniques de contrôle d'accès, on distingue les solutions en ligne et les solutions hors ligne.

1.2.1. Contrôle d'accès hors ligne

Dans les solutions hors ligne, les droits d'accès sont enregistrés sur les équipements numériques de la porte ou sur les supports d'identification (badge, porte-clés, clé).

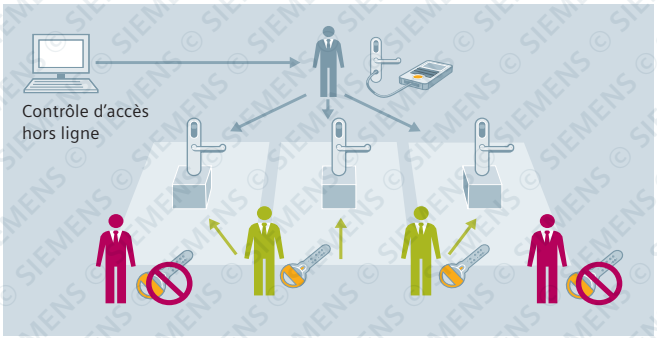


Fig. 1.1: Contrôle d'accès hors ligne avec composants de porte numériques: le système ou l'opérateur charge les autorisations sur les éléments de la porte. «Vert» = droit d'accès sur son support; «rouge» = pas de droit d'accès

Droits d'accès dans les équipements numériques de la porte

Les systèmes hors ligne se composent de cylindres numériques, de gâches et de lecteurs d'accès. Certains fournisseurs proposent même des cylindres numériques à ouvrir avec une clé ou une puce. Les droits d'accès et plages horaires sont gérés par un logiciel centralisé et chargés sur les éléments numériques de la porte par un programmateur. Cette programmation locale est nécessaire après chaque modification ou suppression.

Avantages
- Pas de câblage nécessaire
- Possibilité d'équiper les portes ultérieurement sans difficulté
- Montage et installation rapides

Inconvénients
- Les droits d'accès doivent être chargés localement sur les composants de la porte
- Les droits d'accès ne sont pas disponibles immédiatement
- Le blocage des cartes n'est pas immédiat

Droits d'accès sur un support d'identification
Un logiciel centralisé gère les droits d'accès et les plages horaires et les enregistre à l'aide d'un lecteur de mise à jour sur les supports d'identification tels que des badges, porte-clés, etc. Les droits d'accès peuvent ainsi être modifiés et enregistrés sur les différents supports. Si un support est égaré, il est bloqué dans le système. Le blocage est transmis aux composants hors ligne de la porte via un programmateur ou un support d'identification.

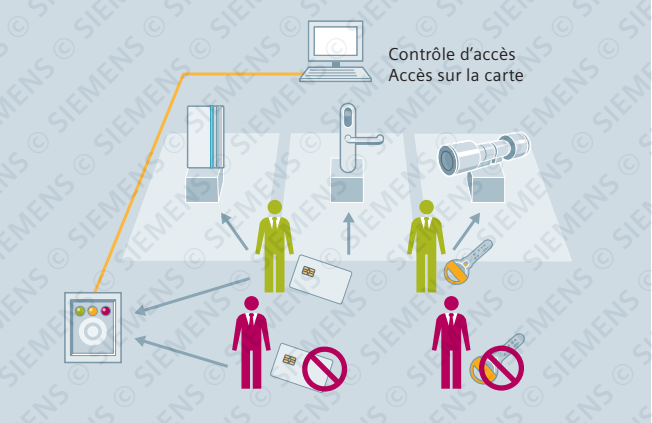


Fig. 1.2: Contrôle d'accès hors ligne avec droits d'accès sur le support: «vert» les droits sont chargés et actualisés sur son support avec le lecteur de mise à jour. «Rouge» ce n'est pas le cas.

Avantages
- Pas de câblage nécessaire
- Montage et installation rapides
- Possibilité d'équiper les portes ultérieurement sans difficulté
- Les droits d'accès sont enregistrés sur le support d'identification

Inconvénients
- Les droits d'accès ne sont pas disponibles immédiatement
- Le blocage des cartes doit être chargé localement sur les composants de la porte et n'est actif qu'ensuite

Contrôle d'accès autonome
Un logiciel centralisé gère les droits d'accès et plages horaires et charge ces informations dans une centrale ou un contrôleur de portes à l'aide d'un programmateur ou d'un ordinateur portable. Dès que les droits d'accès sont modifiés ou supprimés, ils doivent être rechargés dans la centrale. Un contrôle d'accès autonome s'utilise généralement avec des portes coulissantes ou équipées d'une serrure motorisée. Ces types de portes ne peuvent pas être munis d'une poignée hors ligne activée manuellement. Ces portes (lourdes) nécessitent un moteur pour l'ouverture. C'est pourquoi il faut un système qui fonctionne hors ligne.

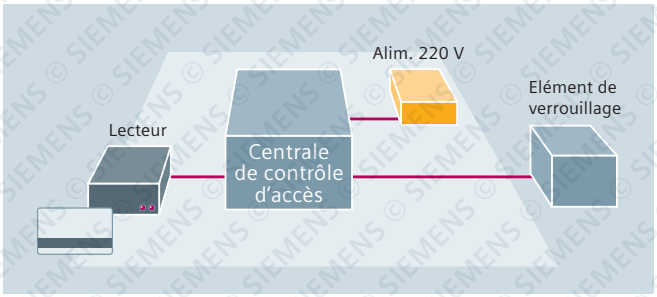


Fig. 1.3: Contrôle d'accès autonome

Avantages
- Pas de câblage réseau nécessaire

Inconvénients
- Les droits d'accès doivent être enregistrés dans la centrale de contrôle d'accès locale
- Les droits d'accès ne sont pas disponibles immédiatement
- Le blocage des cartes n'est pas immédiat

1.2.2. Contrôle d'accès en ligne
Dans les solutions en ligne, la décision d'accorder l'accès ou non à une personne est prise dans la centrale. Les droits d'accès sont généralement redondants dans la centrale et sur le serveur d'accès. Les systèmes de contrôle d'accès se retrouvent généralement dans une topologie centralisée ou décentralisée, ou sous une forme mixte.

Droits d'accès en ligne avec les composants de porte
Un logiciel centralisé gère les droits d'accès et les plages horaires et les charge dans la centrale via le réseau informatique, ce qui permet de modifier les droits d'accès en ligne ou, par exemple, de bloquer immédiatement les badges perdus. Toutes les unités de commande des portes et les lecteurs d'accès sont reliés à la centrale par un système de bus où les unités de commande de porte doivent être câblées de façon centralisée ou décentralisée.

Avantages
- Les droits d'accès sont disponibles immédiatement
- Blocage immédiat des cartes
- Possibilité de surveillance centralisée des portes
- Messages d'incidents disponibles immédiatement

Inconvénients
- Frais de câblage

Installation centralisée
Dans une structure centralisée, tous les capteurs (lecteurs) et composants (gâches, sas, etc.) sont connectés à la centrale centralisée. Celle-ci est généralement installée dans une zone sécurisée comme une salle technique. La centrale qui peut être reliée à plusieurs portes prend les décisions d'accès pour toutes les portes. Les verrouillages de porte et contacts magnétiques sont également reliés à la centrale ou à une unité de commande de porte. Ici, seule la centrale est reliée au serveur d'accès via le réseau informatique (voir fig. 1.4).

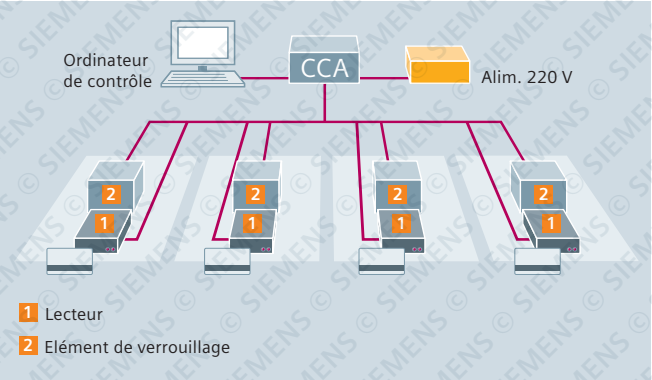


Fig. 1.4: Installation centralisée avec lecteurs et éléments de verrouillage

Installation décentralisée

Une structure décentralisée se compose de nombreuses petites centrales, généralement reliées entre-elles, à proximité directe du lecteur et des composants. Les centrales prennent toutes les décisions d'accès de façon autonome et sont reliées via Ethernet, EIB ou port série RS485 ou sont connectées à un ordinateur principal centralisé. Les lecteurs de contrôle d'accès, les verrouillages de porte et les contacts magnétiques sont connectés à cette centrale (voir fig. 1.5). Ce type d'installation convient particulièrement aux plus petites installations. Si un réseau est souhaité, l'infrastructure correspondante doit être disponible. En l'absence de réseau informatique, un système de bus plus avantageux est recommandé pour relier les différents éléments.

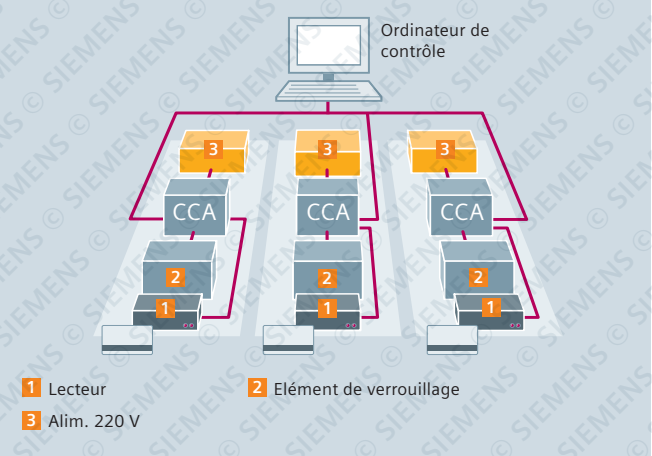


Fig. 1.5: Installation décentralisée avec lecteurs et unités de verrouillage

Avantages

- Faibles coûts d'installation sur un réseau existant
- Administration centralisée

Inconvénients

- Alimentation électrique de secours pour la centrale
- Connexions à des systèmes tiers (SAI, IDI, etc.)

1.2.3. Différences entre les systèmes hors ligne et en ligne

Dans les systèmes de contrôle d'accès en ligne, le serveur est toujours relié directement avec les lecteurs et unités de verrouillage via un réseau. Ces éléments échangent les données d'autorisation et de mouvement via la centrale. Mais il y a aussi des systèmes où les autorisations sont vérifiées en mode en ligne par le serveur et pas par la centrale. De cette façon, dans les solutions en ligne, la décision d'accès dépend toujours des données actuelles dans la centrale. Dans les systèmes en ligne, il peut y avoir une ouverture unique des portes, une ouverture permanente ou un blocage. Il est aussi possible de bloquer ou d'autoriser immédiatement un badge ce qui confère, d'une part, une sécurité très élevée et, d'autre part, une grande souplesse. Il est en outre possible d'obtenir une analyse actuelle avec les informations sur l'identité, le moment et l'endroit où l'accès a eu lieu ou a été refusé.

Les portes périphériques (p. ex. entrées principales) et celles aux exigences de sécurité élevées (p. ex. portes vers les salles de serveurs, portes de liaison, etc.) doivent toujours être surveillées par des lecteurs en ligne. Si une surveillance en temps réel et, éventuellement, une alarme sont importantes pour la protection de l'enveloppe extérieure du bâtiment, les solutions à l'intérieur du bâtiment (p. ex. portes de bureaux et locaux de nettoyage) ne doivent pas toutes satisfaire aux mêmes critères de sécurité. C'est pourquoi les solutions hors ligne se sont établies comme complément idéal, supprimant ainsi les coûts élevés d'intégration en ligne sans pour autant diminuer le niveau de sécurité.

Les systèmes peuvent être installés et étendus sans problème même ultérieurement. En cas de déménagement ou de transformations, tous les composants peuvent ainsi être réutilisés. Tous les avantages du système en ligne pour la gestion des autorisations s'appliquent aussi aux solutions hors ligne. Il suffit de bloquer les cartes perdues dans le système et de nouvelles cartes peuvent être éditées à tout moment avec les droits actualisés.

Actuellement, les systèmes modernes de contrôle d'accès peuvent gérer des droits d'accès à la fois hors ligne et en ligne. Les exploitants d'une installation ne doivent donc pas opter pour une solution plutôt qu'une autre mais bénéficient des avantages des différentes variantes. Certains fournisseurs proposent des systèmes en ligne et des systèmes hors ligne et peuvent ainsi gérer également les installations de fermeture mécaniques. Il est en outre possible d'intégrer des solutions hors ligne directement dans le système. On distingue ici l'intégration partielle et l'intégration complète. Une solution entièrement intégrée repose sur une seule banque de données tandis qu'il faut accéder à deux banques de données (en ligne et hors ligne) pour une intégration partielle. La gestion de deux banques de données augmente toutefois aussi les frais d'entretien.

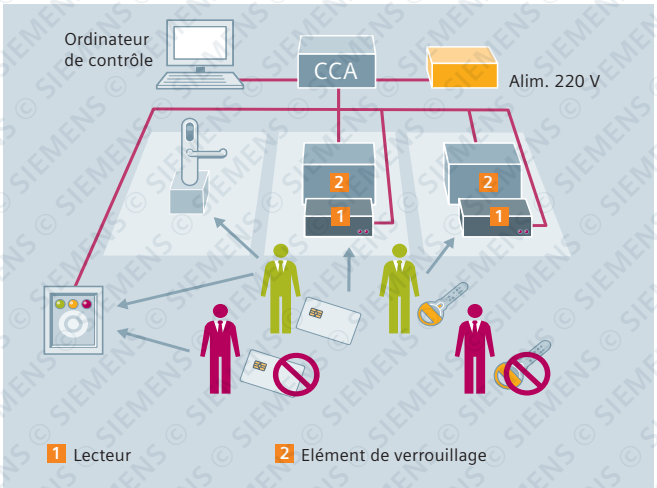


Fig. 1.6: Systèmes modernes de contrôle d'accès avec solution en ligne et hors ligne

1.3. Support

Le lecteur transmet à la centrale les caractéristiques d'identification relatives à un utilisateur. L'identification d'un utilisateur nécessite la possession d'une carte ou d'un tag, la connaissance d'un PIN ou d'un code, des caractéristiques personnelles (biométrie), ou une combinaison de plusieurs de ces éléments. Les différentes méthodes vont de pair avec un degré de sécurité plus ou moins élevé.

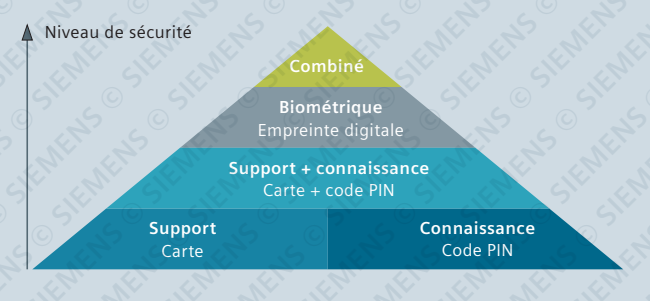


Fig. 1.7: Degrés de sécurité des différentes méthodes

La sécurité d'un système de contrôle d'accès peut être adaptée aux exigences de l'utilisateur. Si seule la possession d'un support ou la connaissance d'un code est vérifiée, la sécurité est faible. Le support (p. ex. une carte) peut être facilement transmis ou volé. Il en va de même pour la connaissance d'un code PIN car il est facile d'espionner un utilisateur ou de transmettre un code. Mais si les deux méthodes sont combinées, le niveau de sécurité est nettement renforcé. Toutefois, ici aussi, la connaissance et la possession ne sont pas liées à une personne. La sécurité dépend donc de son attitude. La biométrie, enfin, offre le degré de sécurité le plus élevé parce que les caractéristiques liées à une personne ne peuvent être ni transmises, ni espionnées, ni falsifiées. Ce chapitre aborde les supports les plus fréquemment utilisés.

1.3.1. Formes

Carte

La carte à puce au format de carte de crédit est la forme la plus courante et la mieux adaptée comme badge visuel. La carte à puce, souvent aussi appelée Smartcard ou Integrated Circuit Card (ICC), est une carte en plastique spéciale équipée d'un circuit intégré (puce) contenant une logique matérielle, une mémoire ou un microprocesseur. Les cartes à puce sont contrôlées par des lecteurs de cartes spéciaux.

Fig. 1.8: Carte à puce au format de carte de crédit

Le design des cartes en plastique est pratiquement illimité. Ces cartes peuvent être pourvues du logo de la société, de la photo du collaborateur ou d'éléments de sécurité tels que des hologrammes. Il existe plusieurs procédés pour imprimer sur des cartes en plastique. Les cartes peuvent ainsi être éditées indépendamment du fournisseur avec des imprimantes spéciales offset ou thermiques.

Clé

Dans les solutions mécatroniques où il y a utilisation parallèle de lecteurs sans contact et de cylindres mécaniques traditionnels, il est particulièrement avantageux d'intégrer un composant RFID dans la clé. Toutefois, la distance de lecture est limitée avec cette méthode.

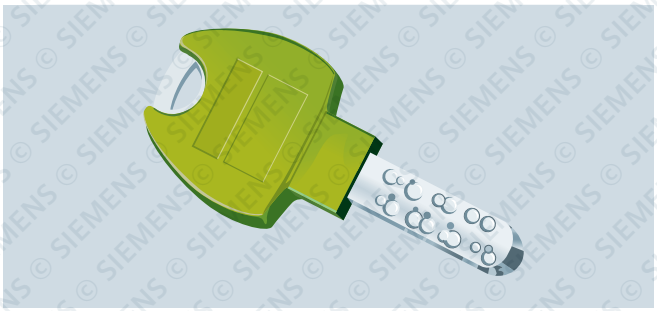


Fig. 1.9: Clé avec composant RFID

Porte-clés / bracelet

Dans cette variante, un composant RFID est intégré dans un porte-clés ou un bracelet. Il s'agit ici d'une variante très robuste où la distance de lecture est nettement inférieure à celle de la carte à puce.

Abb. 1.10: Porte-clés et bracelet avec puce RFID

Les questions suivantes peuvent aider dans l'évaluation de la meilleure solution:

- Le badge doit-il être personnalisé (p. ex. logo de la société)?
- Faut-il ajouter d'autres caractéristiques de sécurité (p. ex. hologramme)?
- Le support doit-il pouvoir être lu sans contact et à une distance relativement grande?
- Le support doit-il aussi servir de clé?
- Le support doit-il être très robuste (sollicitation mécanique, humidité, température)?

1.3.2. Choix de la bonne technologie

Pour pouvoir déterminer la bonne technologie pour chaque projet, ces questions doivent être prises en compte:

- Quelles sont les exigences de sécurité?
- Quel est le secteur d'utilisation?
- Y a-t-il déjà des technologies utilisées? Faut-il pouvoir utiliser toutes les applications avec une seule et même carte?
- Y a-t-il d'autres applications prévues?
- Quelles sont les vitesses de lecture attendues?
- Faut-il enregistrer des données sur le support et quelle doit être la taille de la mémoire?
- Quelles doivent être les distances de lecture?
- Le support est-il vérifié par une personne ou un appareil?

1.4. Lecteurs

Les lecteurs se déclinent en une foule de modèles et de variantes de conception avec les critères de distinction suivants:

- Avec/sans clavier
- Technologie de lecteur (LEGIC, mifare, EM, Hitag, etc.)
- Distance de lecture
- Protection contre le vandalisme
- Classe de protection IP (utilisation intérieure/extérieure)
- Avec/sans écran (terminal p. ex. aussi pour la saisie du temps)
- Possibilité de fonctionnement en mode autonome
- Intégration dans la serrure, dans la gâche

1.4.1. Avec ou sans clavier

Il est possible d'équiper les unités de lecture RFID d'un clavier pour saisir le code PIN. Cette combinaison permet de vérifier la possession et la connaissance. Il est également possible d'augmenter la sécurité en les combinant avec des systèmes biométriques. Le gros inconvénient des lecteurs RFID avec clavier est la possibilité d'apparition de signes d'usure en cas d'utilisation fréquente des touches, selon la qualité du clavier. Les codes PIN sont alors très faciles à espionner.

C'est pourquoi il existe des unités de lecture spéciales pour les applications de haute sécurité, appelées lecteurs de Scramble Code. Ces appareils changent aléatoirement la position des chiffres après chaque saisie. Les différentes applications ont leur forme correspondante. En Suisse, Feller-Edizio s'est imposé comme un quasi-standard. Dans les applications industrielles, on trouve généralement des modèles apparents, parfois avec protection contre les chocs et les éclaboussures. La combinaison avec des dispositifs vocaux et des caméras est aussi possible.

1.4.2. Lecteurs hors ligne

Dans certains cas, des lecteurs ne sont pas intégrés dans un réseau et ne communiquent donc pas avec une centrale. Ces solutions, appelées poignées avec lecteur, conviennent pour des portes individuelles sans exigence de sécurité ou si aucune clé mécanique ne doit être utilisée.

Si ces lecteurs doivent être utilisés sur des portes coupe-feu ou des issues de secours, ils doivent impérativement être autorisés par les autorités compétentes.

1.5. Modes de communication

Les systèmes de contrôle d'accès actuels n'utilisent pratiquement plus que des cartes à puce et des technologies sans contact. Les autres technologies de cartes (bande magnétique, code-barres, infrarouge, etc.) se rencontrent encore parfois sur des systèmes plus anciens où les supports sont à usage unique et où le prix est un critère important, p. ex. dans les bibliothèques, les foires ou les parkings.

1.5.1. Communication avec des cartes à puce

Les cartes équipées d'une puce à contact sont généralement utilisées pour l'accès au PC car elles permettent différentes possibilités de codage et de sécurité. La capacité de la mémoire est souvent élevée mais dépend aussi de la puce intégrée. Les possibilités de modification, de falsification et de copie sont pratiquement exclues grâce aux mesures organisationnelles (p. ex. hologramme). Les puces sont équipées de contacts dont l'emplacement a été défini dans une norme ISO. C'est pourquoi il faut des lecteurs de cartes onéreux capables de mettre en rapport les capteurs de contact dans le lecteur avec les surfaces de contact de la carte.

1.5.2. RFID

Le RFID (angl. radio frequency identification) est l'identification à l'aide d'ondes électromagnétiques et désigne une technologie de systèmes d'émetteurs-récepteurs pour l'identification automatique et sans contact et la localisation d'objets par des ondes radio. Cette technologie facilite considérablement la saisie de données. Un système RFID se compose toujours d'un transpondeur intégré dans un objet (p. ex. badge) et contenant un code déterminé ainsi que d'un lecteur pour la lecture de ce code. On parle alors de lecture de proximité avec une distance maximale de 10 cm. Il existe toutefois aussi des systèmes destinés à des distances supérieures (p. ex. pour les camions, chariots-élévateurs, etc.) fonctionnant avec des fréquences supérieures et des supports ID propres. En Suisse, Legic et mifare sont les technologies les plus utilisées dans le domaine du contrôle d'accès. Les autres applications sont entre-autres:

- Accès informatique
- Automatisation bureautique (libération d'imprimantes et de copieurs)
- Saisie du temps et des prestations
- eTicketing (concerts, manifestations sportives, etc.)
- ePayment (cash, vente, solutions de catering, etc. pour le paiement aux automates et aux caisses)
- Solutions de parking, etc.

1.5.3. Near Field Communication

La Near Field Communication (NFC) est une norme de transmission internationale pour l'échange sans contact de données par technologie radio sur des distances de quelques centimètres. L'octroi de droits d'accès se fait «over the air» (OTA), c'est-à-dire que les données peuvent être copiées par accès distant sur un téléphone mobile via GSM et Internet. Ceci est particulièrement intéressant lorsque les droits doivent être attribués pour une courte période et pour des lieux éloignés les uns des autres. Un technicien peut ainsi effectuer un dépannage tôt le matin sans grandes démarches administratives en obtenant les autorisations via OTA peu avant son intervention.

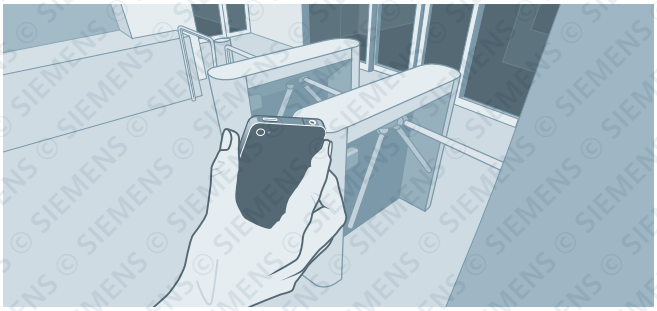


Fig. 1.11: Avec la NFC, les données et droits peuvent être transmis via GSM et Internet.

1.5.4. Resistive Capacitative Identification (RCID)

La RCID est une technologie de transmission d'informations à l'aide de champs électriques (quasi-) statiques totalement inoffensifs pour le corps. Contrairement à la technologie RFID, la RCID n'utilise pas de champs électromagnétiques. Dans les champs électrostatiques, la transmission d'informations se fait par des électrodes (non par des antennes). Le corps de l'utilisateur devient porteur du signal émetteur. Dès que celui-ci touche l'électrode réceptrice, la moitié du circuit électrique est fermée. L'autre moitié se ferme via l'environnement. Si l'on porte un émetteur sur soi (p. ex. dans la poche du pantalon) et que l'on touche un récepteur (p. ex. poignée de porte ou tapis de sol), le circuit se ferme et l'identification a lieu.

1.6. Systèmes biométriques

Ces dernières années, les méthodes d'identification biométriques ont connu un immense essor. Les progrès technologiques permettent de mesurer de plus en plus rapidement les caractéristiques biologiques (p. ex. doigts, yeux) et de les analyser, pour un coût abordable et une qualité élevée. L'utilisation de la biométrie est donc une approche prometteuse pour résoudre les problèmes persistants de nombreux concepts de sécurité: comment relier les identités et les droits correspondants avec les personnes physiques présentant la bonne identité? L'utilisation de badges volés par exemple est alors fortement compliquée, voire impossible.

Dans l'identification de personnes, les procédés biométriques font partie des principales méthodes d'authentification automatisables. Ici, l'authentification signifie l'«attestation ou la vérification de l'authenticité». Tandis que les techniques d'authentification traditionnelles comme le code PIN, le mot de passe ou la Smartcard (carte à puce) reposent sur la vérification par la connaissance ou la possession (voir chapitre 1.4. Lecteurs), la biométrie se base sur les caractéristiques physiologiques de la personne elle-même – et non se rapportant simplement aux personnes.

La vérification et l'identification font partie des principaux types de reconnaissance pour l'analyse. La vérification signifie «confirmation de l'identité» où une comparaison 1:1 vérifie si l'identité supposée peut être prouvée. Une personne s'identifie, par exemple, par une carte ou un code PIN. Le système décide sur la base de la comparaison de ses données de biométrie (modèle) avec la mesure du capteur si la personne peut avoir accès ou pas. Si le modèle de référence est également enregistré sur une carte, il ne faut pas gérer de banque de données centralisée, ce qui représente un gros avantage en termes de protection des données.

L'identification signifie «constatation de l'identité» et consiste en la comparaison par le système des caractéristiques biométriques d'une personne avec toutes les données de références stockées dans la banque de données. Il y a donc une comparaison 1:n avec une foule de jeux de données. Plus le système contient de jeux de données de référence, plus l'identification est longue.

Souvent, un lecteur biométrique est plus cher qu'un appareil RFID. Comme l'achat et la gestion des cartes RFID ne sont plus nécessaires, ce surcoût est toutefois quelque peu compensé.

1.6.1. Exigences relatives aux caractéristiques biométriques

Une caractéristique biométrique doit remplir au moins les propriétés suivantes:

- **Caractère distinctif/unicité (Distinctiveness):** traits différents entre les personnes
- **Durabilité/constance (Permanence):** traits permanents de la personne. Les procédures adaptatives permettent de compenser les légères modifications (p. ex. petite blessure au doigt)
- **Accessibilité/saisissabilité (Collectability):** quelque chose dont on peut obtenir une image facilement
- **Universalité/diffusion (Universality):** quelque chose que tout le monde possède

Les propriétés suivantes sont en outre souhaitables:

- **Acceptation (Acceptance):** pas de résistance à la collecte de données
- **Performance (Performance):** robuste, précis, efficace et rapidement analysable
- **Fiabilité (Reliability):** pour compliquer les falsifications et le contournement des prescriptions

1.6.2. Techniques et méthodes

Il y a en principe deux groupes d'identification biométrique:

- **Caractéristiques physiologiques** (aussi appelées «caractéristiques passives»): empreintes digitales, réseau veineux, géométrie de la main, yeux (rétine, iris), visage
- **Caractéristiques spécifiques au comportement** (aussi appelées «caractéristiques dynamiques»): signature, timbre de la voix, allure, type de frappe au clavier

Les caractéristiques spécifiques au comportement s'utilisent généralement plutôt dans le domaine du confort, p. ex. pour la commande vocale d'appareils, etc. Les systèmes qui analysent les caractéristiques statiques servent au contrôle d'accès. Il est bien sûr également possible de combiner les méthodes, p. ex. la reconnaissance faciale et vocale. Les différentes caractéristiques sont décrites plus en détail ci-après.

Empreintes digitales

Comme on n'a pas trouvé à ce jour deux personnes partageant les mêmes empreintes digitales, on mise sur leur unicité. Une empreinte digitale dispose au total d'env. 35 marques (minuties) différentes telles que des intersections, des terminaisons, des bifurcations ou des points. Pour une identification claire, il suffit généralement de vérifier 8 à 22 caractéristiques ainsi que leur distance et leur emplacement.

Fig. 1.12: Lecteur et minuties d'une empreinte digitale

Avantages

- Besoin de mémoire minime pour le modèle
- Economique

Inconvénients

- Les utilisateurs peuvent émettre des réserves pour des questions d'hygiène
- Limitation en cas de modèle d'empreinte manquant ou faible
- Dépend de la température

Structure des vaisseaux sanguins au dos de la main

Un système biométrique identifie le tracé individuel des veines et travaille avec un algorithme d'identification spécifique. Celui-ci repère la structure des vaisseaux sanguins de la main extraite par une technologie infrarouge et la compare avec les jeux de données de référence enregistrés dans le système. Même chez les jumeaux monozygotes, ce tracé est différent car il n'est pas déterminé exclusivement par l'ADN.

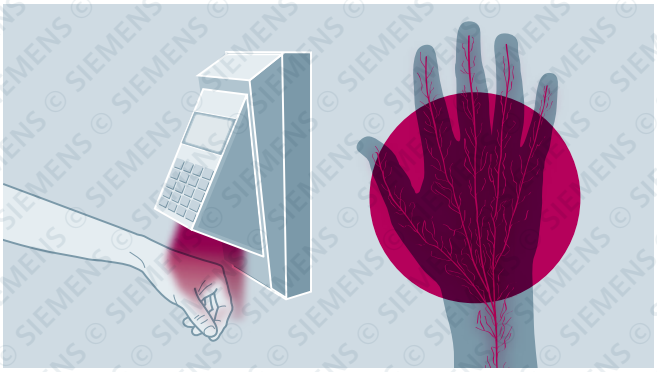


Fig. 1.13: Lecteur de structures de vaisseaux et de structures veineuses de la main

Avantages

- Pas de fausse identification car chacun possède un tracé veineux
- La position des veines reste identique tout au long de la vie et est différente chez chaque personne
- L'état de la surface de la peau n'a aucune influence sur le modèle, la mesure se fait sous la peau
- Les petites blessures et la saleté ne génèrent pas d'erreur d'identification

Inconvénients

- Dépend de la température

Iris

L'iris de l'œil est sa membrane pigmentée. Il s'agit de la caractéristique la plus complexe du corps humain convenant pour l'analyse biométrique. L'iris n'est pas influencé par les gènes et est donc le fruit du hasard. Avec ses points, ses collerettes, ses taches pigmentaires et sa couronne ciliaire, l'iris recèle au total 266 caractéristiques biologiques potentiellement exploitables par des systèmes biométriques.

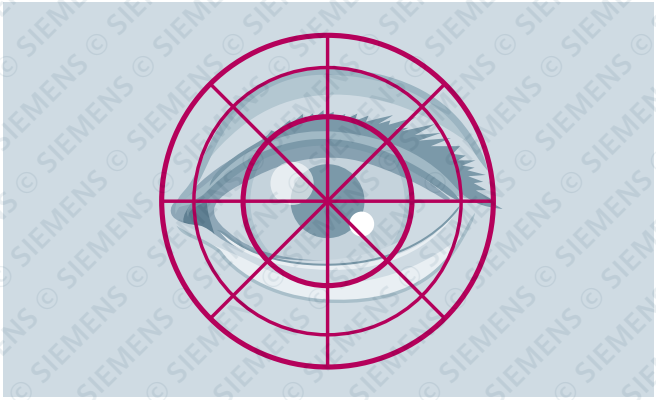


Fig. 1.14: Une caméra vidéo analyse l'iris

Avantages

- L'iris ne change pas durant la vie et est unique à chaque personne

Inconvénients

- Acceptation, réticences à se laisser scanner les yeux
- Difficultés de lecture chez les personnes porteuses de lunettes ou de lentilles
- Refus de personnes autorisées après de petites blessures pouvant être causées par des corps étrangers dans l'œil

Reconnaissance faciale 2D/3D

Le menton, la bouche, le nez, les yeux et leur situation les uns par rapport aux autres constituent des caractéristiques uniques du visage. Les obstacles à la reconnaissance faciale sont les caractéristiques qui peuvent évoluer comme une nouvelle barbe, le port de lunettes ou une luminosité différente. C'est pourquoi le système doit extraire ces informations évolutives de l'image enregistrée par la caméra et limiter son analyse aux seuls paramètres clairs du visage. Une mimique différente peut aussi perturber la reconnaissance faciale.

Des caractéristiques particulières du visage sont saisies à l'aide de graphes. Pour cela, un quadrillage est superposé au visage. La technologie place alors les nœuds du quadrillage sur les éléments marquants du visage tels que les yeux, la commissure des lèvres ou la pointe du nez. Les points sélectionnés sur le visage constituent une grille élastique «courbée» aux relations fixes. Cette relation fixe est conservée même en cas de distorsions causées par une mimique différente ou par une autre position de la caméra.

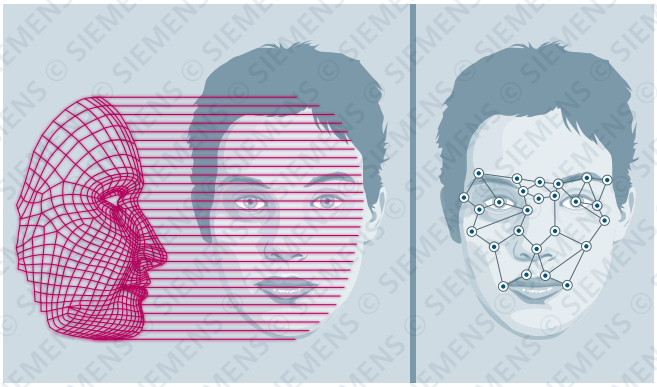


Fig. 1.15: Des caractéristiques déterminées du visage sont mesurées, ce qui produit un modèle

Dans la reconnaissance faciale 2D, les caractéristiques sont saisies par une caméra. Le système de reconnaissance faciale se compose d'un émetteur infrarouge et d'un scanner fonctionnant comme récepteur. L'émetteur projette une grille infrarouge invisible à l'œil humain sur le visage d'une personne. Le modèle infrarouge reflété par la surface du visage est saisie par un scanner spécial et converti en informations visuelles.

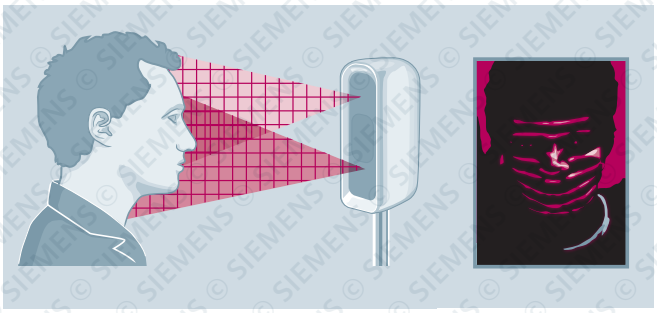


Fig. 1.16: Fonctionnement de la reconnaissance faciale

Avantages

- Pratiquement insensible à la saleté et à l'usure
- Forte acceptation car il s'agit d'une méthode sans contact

Inconvénients

- Méthode coûteuse

Questions à se poser lors de l'évaluation de systèmes biométriques:

- Quels sont les objectifs à atteindre avec un système de reconnaissance biométrique?
- S'agit-il d'une identification ou d'une vérification biométrique?
- Quelles sont les mesures à appliquer?
- Quels sont les justificatifs pour le traitement des données?
- Combien de personnes sont enregistrées?
- Les données biométriques doivent-elles être enregistrées dans un système centralisé ou décentralisé?
- En cas de stockage décentralisé: selon quel procédé?

1.7. Gestion des portes

Les systèmes de contrôle d'accès doivent être associés à la commande de portes et sas ainsi qu'à des systèmes d'alarme. Il faut toutefois des contrôleurs et composants de porte spéciaux. Les portes et lecteurs sont commandés et surveillés par un contrôleur de porte.

La performance d'un contrôleur de porte dépend toutefois du niveau de qualité de la porte elle-même et de ses composants de sécurité. Selon la fréquentation et la situation de la porte, il peut y avoir plusieurs centaines de passages par jour, ce qui représente une sollicitation énorme pour des pièces mécaniques et électromécaniques. Il est donc essentiel de s'occuper de la planification suffisamment tôt et en détail en impliquant tous les spécialistes. On évite ainsi que des composants tombent en panne précocement ou que la sécurité ne puisse plus être garantie. Il est tout aussi important de bien réfléchir aux fonctions de protection des portes, p. ex. contre l'effraction, l'incendie et les chocs, mais aussi aux issues de secours.

Dans les installations complexes, les composants de porte ne sont plus gérés par un contrôleur de porte mais transmis à un système de contrôleur de porte subordonné (TMS), comme un contrôleur programmable (SPS). Ce système déclenche un asservissement programmé par la connexion «filaire». Les capteurs (contacts de porte, barrières lumineuses, etc.) et les acteurs (contacteur de porte à ouverture, gâche électrique, etc.) sont branchés directement sur le SPS. Qu'il agisse comme groupes centralisés ou solution modulaire aux modules décentralisés, le SPS garantit une flexibilité élevée et une évolutivité. Les interfaces du contrôle d'accès peuvent aussi être numériques.

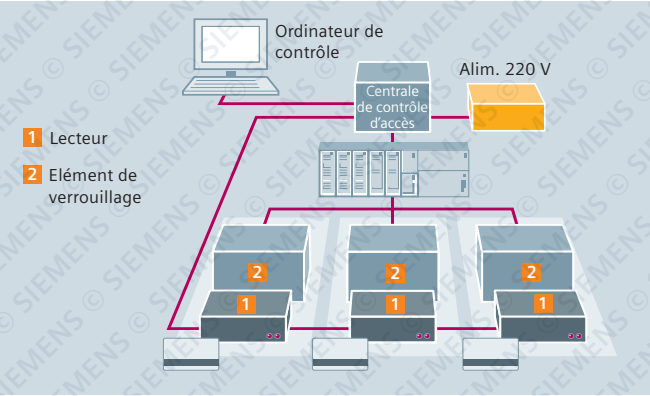


Fig. 1.17: Le système de contrôleur de porte commande et surveille les composants de porte

Avec une interface série intégrée, il est possible de se passer d'un câblage coûteux. Si plusieurs modules SPS sont utilisés, ils sont reliés via le réseau (Ethernet), ce qui augmente nettement la flexibilité et la vitesse.

1.7.1. Types de portes

Il existe différentes sortes de portes et d'accès:

- **Portes tambour:** deux ou quatre battants de porte tournants dans un espace circulaire pour permettre les entrées et sorties simultanées
- **Portes à deux battants:** séparation des espaces intérieurs et extérieurs, verrouillage par une serrure
- **Tourniquets:** deux, trois ou quatre battants verticaux pour isoler les grands groupes de personnes
- **Portes coulissantes:** un vantail/plusieurs vantaux, guidés en haut ou en bas, s'ouvrant latéralement
- **Tourniquets tripodes:** équipement fixe muni de trois barres pour un accès individuel
- **Sas:** cabines avec deux portes en vis-à-vis comme mesure d'individualisation
- **Sas avec capteurs:** accès surveillé par des capteurs et équipé de portes coulissantes ou battantes

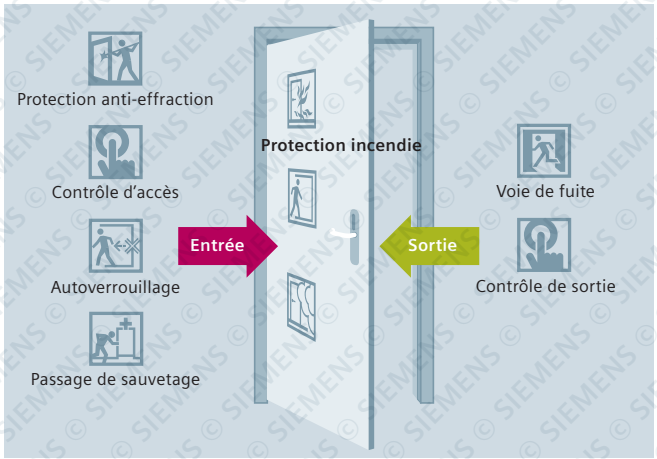


Fig. 1.18: Fonctions d'une porte

1.7.2. Elemente einer Türe

Une porte comprend les éléments suivants:

- **Gâche électrique:** dispositif intégré dans l'encadrement de porte avec déverrouillage électromagnétique du pêne
- **Serrure de sûreté:** serrure particulièrement sécurisée avec un cylindre fixé par plusieurs broches
- **Serrure autoverrouillante:** le verrou se referme automatiquement après chaque ouverture de la porte
- **Verrouillage multipoints:** serrure de sûreté avec verrouillage multipoints (généralement trois) pour compliquer l'ouverture par forçage mécanique
- **Contacts de surveillance:** pour la surveillance de l'état des portes (fermées, verrouillées, ouvertes), essentiellement des contacts magnétiques ou des contacts de pêne

1.8. Fonctions centrales d'un contrôle d'accès

1.8.1. Structures des autorisations

Les différents fournisseurs ont différentes approches pour la constitution des autorisations dans le système. Tous ont néanmoins une chose en commun: ils indiquent qui peut aller où et quand.

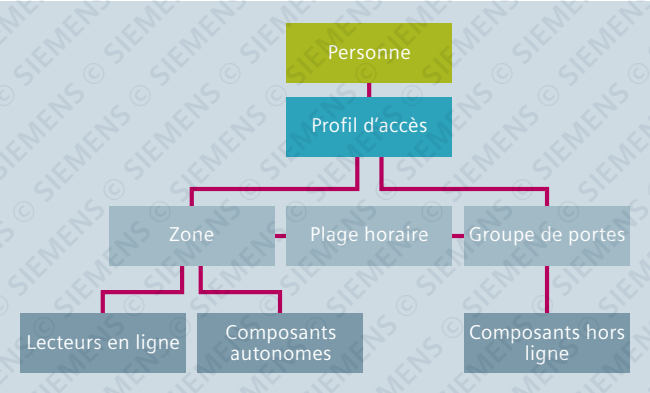


Fig. 1.19: Structures d'autorisations d'un contrôle d'accès

Les lecteurs et portes avec composants en ligne et hors ligne constituent le tout premier niveau d'un contrôle d'accès. Le deuxième niveau se compose des différentes zones spatiales et temporelles ainsi que des groupes de portes. Le troisième et dernier niveau gère les profils d'accès des différentes personnes.

Pour simplifier et clarifier la gestion, les portes sont rassemblées en groupes, ce qui peut se faire à différents niveaux. Ces niveaux contiennent à la fois des groupes logiques de lecteurs et de profils d'accès. De cette façon, les personnes peuvent être regroupées selon leur fonction, leur département, leur appartenance géographique ou leur centre de coûts. Une telle répartition permet d'attribuer le plus rapidement possible le bon droit d'accès à un collaborateur.

Comme l'application de l'attribution de droits est aussi personnelle que le système, l'utilisateur doit communiquer clairement ses besoins au fournisseur. Il est en outre utile de concevoir le concept ensemble. En effet, après l'introduction, le gérant doit être en mesure d'étendre intelligemment le modèle et de procéder seul à l'attribution des droits.

1.8.2. Commandes de sas

Seules les personnes autorisées peuvent se trouver dans un sas (p. ex. une pièce ou une cabine). Il faut absolument que le sas soit protégé par au moins deux terminaux d'accès. Si une pièce est convertie en sas vers d'autres zones sécurisées, il ne doit être possible d'y accéder ou d'en sortir par plus d'une porte en même temps. C'est pourquoi une opération n'est possible que si toutes les portes du sas sont fermées ou si une opération d'accès est terminée.

Il est également possible d'utiliser un sas pour l'individualisation de personnes. Dans ce cas, aucune porte de cette pièce ne peut être ouverte avant que la personne autorisée ait quitté la pièce (le sas). Dans la plupart des cas, l'individualisation de personnes est soumise à une limite temporelle après le dépassement de laquelle la personne doit revenir dans la zone d'où elle vient. En cas d'utilisation de sas, les points suivants doivent être respectés:

- Le fonctionnement d'un sas nécessite beaucoup de courant. Même en cas de coupure d'alimentation, tous les composants nécessaires doivent fonctionner efficacement.
- Les compétences des différents systèmes de surveillance (effraction, incendie, vidéo, accès) doivent être clairement définies
- Ne pas oublier l'issue de secours
- Les sas limitent fortement le flux de personnes. Lors de la planification, les flux de personnes escomptés doivent être pris en compte.
- Les individualisations de personnes coûtent cher et doivent être planifiées par des spécialistes.
- Les sas doivent être entretenus régulièrement. La complexité nécessite une interaction exacte de tous les composants.
- Prendre en compte la question du transport de marchandises ou d'objets personnels (bagages, PC, etc.)
- Logique multi-personnes et bloque l'accès

1.8.3. Contrôle de changement de zone et comptage

Un secteur de sécurité contient des secteurs partiels avec des zones composées d'une ou plusieurs pièces et une ou plusieurs entrées et sorties. Chaque zone ne peut contenir qu'une seule personne. En outre, le système empêche l'accès à une zone voisine si la personne est saisie comme «non présente» dans la zone où elle se trouve.

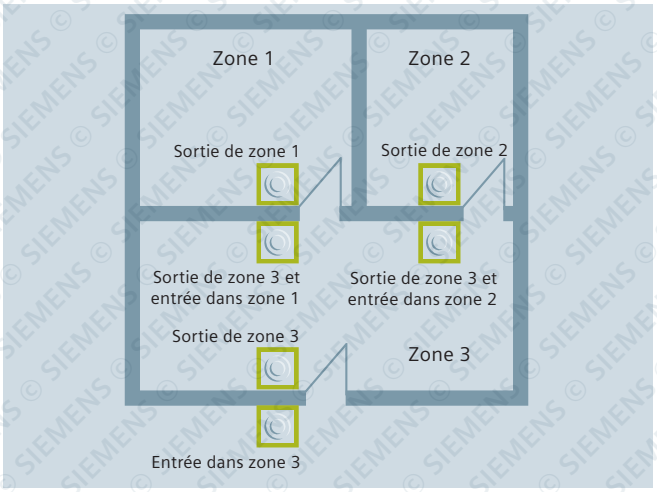


Fig. 1.20: Division en plusieurs zones

Tous les lecteurs d'une zone peuvent être réunis en un groupe. Il est en outre possible d'octroyer d'autres attributs à la zone:

- Violation de zone: l'entrée peut être possible malgré la violation de zones mais est consignée ou déclenche une alarme
- Violation de zone: l'entrée peut être possible malgré la violation de zones mais est consignée ou déclenche une alarme
- Nombre de personnes qui se trouvent en ce moment dans la zone
- Plage horaire pendant laquelle le droit d'accès s'applique à une zone
- Nombre de personnes minimal qui doivent se trouver dans une zone
- Durée maximale de présence dans la zone

- Zone vide/non vide, une alarme se déclenche en fonction des prescriptions
- Nombre de personnes maximal pouvant entrer dans une zone. Si le maximum est atteint, une personne doit quitter la zone pour qu'une autre puisse entrer.

1.8.4. Commandes d'ascenseurs

Il existe plusieurs variantes pour combiner contrôle d'accès et commandes d'ascenseurs:

- L'ascenseur ne peut être appelé que par des personnes autorisées. Les lecteurs d'accès ne se trouvent pas dans la cabine mais aux étages et servent à appeler l'ascenseur.
- Le lecteur d'accès se trouve dans la cabine:
  - Tous les étages sont librement accessibles après une identification valable.
  - Après une identification, l'étage attribué au support est appelé.
  - On ne peut choisir que les étages pour lesquels il existe une autorisation (activation des boutons).

Il convient de respecter les points suivants pour les commandes d'ascenseurs: c'est un grand avantage que de pouvoir coordonner au plus tôt les possibilités offertes par le fournisseur d'ascenseur et de contrôle d'accès. Mais attention: un ascenseur n'est pas un dispositif d'individualisation des personnes.

1.9. Fonctions étendues et modules

1.9.1. Possibilités d'intégration

D'autres systèmes et modules peuvent interagir avec le contrôle d'accès. Il est important de distinguer l'étendue de l'intégration:

- **Intégration partielle:** combinaison d'une application de tiers généralement préexistante avec une application d'accès personnelle
- **Intégration totale:** extension de l'application de contrôle d'accès, l'utilisateur se sert de l'extension comme application de base
- **Interfaces matérielles:** regroupement de plusieurs systèmes via des interfaces matérielles de sorte que les incidents importants et les asservissements agissent sur les deux systèmes
- **Interfaces logicielles:** en cas d'intégration minimale, p. ex. via un service web, les données communes ne doivent être gérées que dans une seule application

Intégrer le contrôle d'accès dans un système pilote de sécurité est largement répandu. Cette solution permet au personnel de sécurité de commander tous les sous-systèmes de sécurité de façon uniforme et commune et d'avoir une vue d'ensemble globale. Une interface graphique claire facilite la commande.

1.9.2. Gestion des visiteurs

La gestion des visiteurs se distingue de celle des collaborateurs par les droits généralement limités dans le temps, le blocage du laissez-passer après sa restitution et la réutilisation de celui-ci pour le visiteur suivant, etc. Toutefois, la traçabilité est assurée.

Fonctionnalités et avantages:

- Gestion des places de parking
- Enregistrement préalable des visiteurs et accueil automatique
- Accès réglementé dans les zones sensibles (accès interdit, accompagné, etc.)
- Archivage de toutes les visites, y compris de la personne visitée
- Accès possible même si la réception n'est pas occupée (auto-enregistrement)
- Vue d'ensemble des visiteurs se trouvant dans le bâtiment (urgences, évacuation)
- Identification des personnes et sociétés indésirables (blacklist)
- Les visiteurs peuvent se déplacer librement dans les zones prédéfinies
- Fonctions supplémentaires comme la réservation de pièces et de ressources (p. ex. catering)
- Activation d'ascenseurs pour certains étages
- Le compte-rendu des accès est garanti à tout moment

1.9.3. Transmission des alarmes

Les éventuelles alarmes sont transmises à la police ou à des services d'intervention privés par SMS ou e-mail. Cette transmission doit être sécurisée ou cryptée et un message interne, par exemple du responsable technique, peut créer un intérêt supplémentaire. Dans la plupart des cas, le contrôle d'accès est utilisé simultanément comme élément de commande du système anti-intrusion (SAI). Selon les possibilités offertes par le système de contrôle d'accès, des solutions intéressantes peuvent en résulter: les procédures peuvent être automatisées et les synergies utilisées. Il est important de noter que le contrôle d'accès ne remplace pas le SAI. De plus, des solutions de confort associées au contrôle d'accès ne peuvent pas être certifiées par SES.

1.9.4. Vidéosurveillance

Il peut être très utile d'intégrer le contrôle d'accès dans un système de vidéosurveillance. Cela facilite la constatation a posteriori d'un abus éventuel de laissez-passer à l'aide d'enregistrements d'accès autorisés et non-autorisés. Dès qu'une personne s'approche d'un accès ou d'une porte ou s'identifie sur un lecteur, les programmes correspondants permettent d'activer immédiatement la caméra vidéo via le détecteur de mouvement. Pour le personnel de sécurité, il est possible d'effectuer un contrôle supplémentaire soit en direct sur l'écran soit ultérieurement sur la base des images enregistrées.

1.9.5. Création et gestion des laissez-passer

Beaucoup de systèmes de contrôle d'accès disposent, en plus de la gestion des laissez-passer, de modules pour la personnalisation des supports, par exemple l'impression et la programmation. Dans le cadre de la gestion des supports, il est possible d'avoir également le contrôle effectif des applications telles que la gestion des places de parking, le dépôt de clés, le paiement sans argent liquide, l'utilisation des copieurs, la gestion des prêts, etc. Néanmoins, seuls des fournisseurs spécialisés dans les systèmes de contrôle d'accès proposent ce genre de modules.

Fig. 1.21: Applications possibles dans le cadre de la gestion des supports

1.9.6. Dépôt de clés

L'utilisation d'un dépôt de clés électronique a pour immense avantage que plus aucune clé ne quitte l'enceinte de la société. Autres avantages d'un dépôt de clés en combinaison avec un contrôle d'accès:

- Alarme en cas de non restitution après un horaire déterminé ou pas de possibilité de sortir du bâtiment tant qu'une clé n'est pas restituée
- Moins de clés en circulation
- Surveillance des clés empruntées (quelles sont les clés manquantes à cet instant précis?)
- Chaque prise et restitution de clé est automatiquement enregistrée: qui, quand, quelles clés ?
- Définition claire des droits (qui peut avoir quelle clé à quel moment?)

Un dépôt de clés peut toutefois être utilisé aussi à d'autres fins, p. ex. outils, instruments de travail (PC), etc.

1.9.7. Interfaces vers des systèmes tiers

Il est possible d'intégrer par exemple des systèmes de biométrie, des installations de vidéosurveillance ou des commandes d'ascenseurs via des interfaces série. L'échange de données se fait au niveau du management via le réseau. Cette application est couramment utilisée pour la reprise des données personnelles d'un système RH et évite les redondances dans la saisie de données. Comme les entrées et sorties ainsi que les changements de département sont enregistrés dans le système RH, cela augmente non seulement la simplification et la prévention des erreurs mais aussi la sécurité.

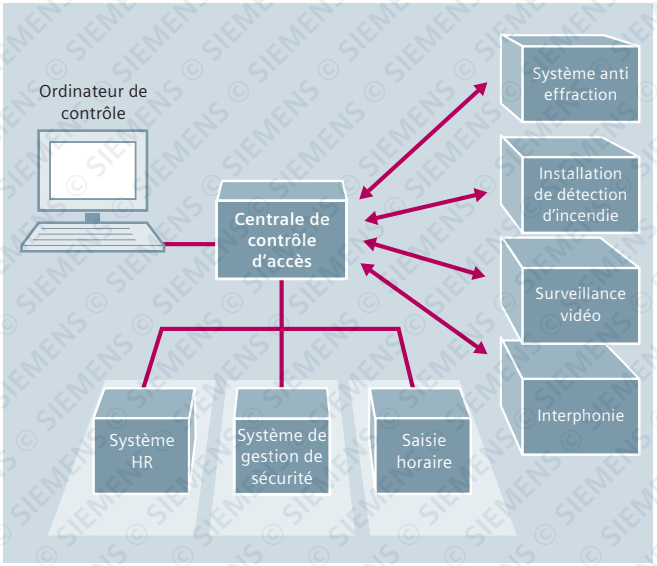


Fig. 1.22: Intégration de systèmes tiers via des interfaces série

Les interfaces peuvent être très coûteuses selon les exigences (technique d'accès, type de données, procédure en cas d'erreurs et de conflits, périodicité, enregistrement, etc.) et l'implémentation. Il faut beaucoup de connaissances et d'expérience avec les deux systèmes à combiner.

1.9.8. Rapports

Des rapports et évaluations doivent aussi pouvoir être établis à l'aide du système de contrôle d'accès. Outre les requêtes prédéfinies, il doit être possible d'obtenir les requêtes filtrées selon divers critères ainsi que leur exportation dans les programmes Office actuels. Plus les exigences sont spéciales, plus cela vaut la peine de préciser les spécifications de ces rapports et de vérifier le travail nécessaire.

1.9.9. Saisie des temps

Le contrôle d'accès et la saisie des temps ont deux éléments en commun: les données de base (données personnelles) et les laissez-passer (identification). C'est pourquoi la plupart des systèmes intègrent en plus du contrôle d'accès une saisie et un traitement des temps. Cette solution a pour avantage que l'accès au bâtiment n'est possible, par exemple, qu'au moment défini, c'est-à-dire pendant le temps de travail correspondant mais pas pendant les congés.

Selon les exigences de l'utilisateur, il convient de déterminer au cas par cas si la meilleure solution est un système intégré ou une simple combinaison via une interface. Pour le savoir, les points suivants doivent être éclaircis:

- Qu'attend l'utilisateur du contrôle d'accès?
- Quelle est la technologie de cartes à utiliser?
- Comment les responsabilités (utilisation, entretien, etc.) sont-elles définies?
- Y a-t-il des exigences de la part de systèmes de salaires ou RH?
- Quelle est la technologie de banque de données utilisée?
- Qu'attend l'utilisateur de la saisie et du traitement des temps?
- Y a-t-il d'autres liens avec la saisie des données de l'entreprise ou de la productivité?
- Le système d'informations personnelles peut-il mettre des données à disposition?

1.9.10. Comparaison «application locale» et «client web»

La plupart des systèmes de contrôle d'accès permettent l'obtention de données et la communication avec les périphériques à l'aide d'un serveur. Il y a deux méthodes pour la saisie et la gestion des données d'accès: soit via des clients «normaux» soit via des clients web. Les différentes possibilités ont leurs avantages et leurs inconvénients.

Si l'installation se fait avec des clients, un logiciel est installé sur chaque PC pertinent pour accéder aux données du serveur. Cette technologie permet à la fois une commande sécurisée et performante des systèmes et un fonctionnement rapide et précis du contrôle d'accès. Toutefois, il faut prévoir une mise à jour de l'application sur chaque PC, ce qui est coûteux.

Avec la solution du client web, une application web est installée sur le serveur de contrôle d'accès pour permettre l'accès via le navigateur web. Le fait qu'il ne soit plus nécessaire d'installer de logiciel séparé sur chaque PC est un immense avantage. De nos jours, la bande passante d'Internet ne joue généralement plus aucun rôle pour le bon fonctionnement de l'installation web, mais certains paramètres doivent être correctement définis. La mise à jour ne doit se faire que sur le serveur.

1.10. Sécurité et protection des données

Un système d'accès doit impérativement être protégé de sorte que le système ne soit plus disponible pour une attaque ou que la sécurité ne soit pas compromise par des mesures techniques ou organisationnelles simples. Il faut donc un concept de protection structuré, surtout lorsque l'on sait que près de 70 % de la criminalité informatique est commise par les collaborateurs de l'entreprise visée.

Outre le système, les données personnelles doivent aussi être protégées. La loi fédérale sur la protection des données (LPD) stipule que les données personnelles doivent être protégées contre un accès non-autorisé par des mesures techniques et organisationnelles appropriées. La sécurité peut aller à l'encontre du confort. Si un système limite trop fortement un collaborateur ou s'il ne comprend pas clairement les raisons des restrictions, il mettra tout en œuvre pour le contourner.

Un concept de sécurité comprend plusieurs aspects:

- **Sécurité des informations:** les systèmes traitant et stockant des informations doivent garantir la confidentialité, la disponibilité et l'intégrité des données. Cela peut se faire par cryptage.
- **Matériel:** les cartes, lecteurs, composants de porte, contrôleurs, clients, etc. doivent être protégés contre l'accès, le sabotage, les virus, la duplication et autres dangers.
- **Fiabilité:** toutes les données des événements (accès, ouverture de porte, etc.) doivent être enregistrées intégralement et chronologiquement et être soumises à une révision.
- **Disponibilité:** l'accès aux données doit être garanti dans une période convenue. La disponibilité est d'autant plus élevée que les défaillances et dysfonctionnements sont réduits, ce qui peut être assuré notamment par le bon choix des composants informatiques, de réseau et de portes ainsi que par un service technique et une formation appropriés.

Aperçu graphique

WAN/LAN

Serveur
SiPass Integrated

Contrôleur
AC5200

Imprimante pour badges
et cartes

Lecteur enrôleur

Ethernet

Administrateur système

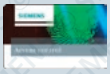
Terminal utilisateur
SiPass Integrated

Contrôleur
AC5102

Gestion des visiteurs

Gestion du personnel

Contrôleur sécurité



Badge

Contrôleur graphique

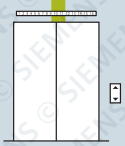
Porte offline

Réseau RS485

AFO5100
Module de sortie

ADD5160
Module de commande de porte

AFI5100
Module d'entrée



Commande ascenseur

Lecteur d'empreintes digitales 3D (lecteur biométrique)

L'AFI5100 constitue une interface locale entre l'AC5100 et des appareils utilisés pour la surveillance de l'installation (détecteur infrarouge, p. ex.).

Réseau RS485

ADD5160
Module de commande de porte

ADD5160
Module de commande de porte

ADD5160
Module de commande de porte

AFO5200
Module entrée/sortie

Lecteur d'empreintes digitales 2D (lecteur biométrique)

Lecteur d'empreintes digitales 3D (lecteur biométrique)

Lecteur de badges/codes PIN

Lecteur de badges

Badge

Sorties d'alarmes et de commandes

SiPass Integrated: Liberté de mouvements dans un environnement sécurisé

SiPass® integrated est un système de contrôle d'accès extrêmement performant et souple, offrant un très haut niveau de sécurité, sans avoir d'incidence négative sur la convivialité et la facilité d'accès pour les utilisateurs. Conçu pour s'intégrer dans un environnement IT, SiPass integrated, grâce à sa structure modulaire et extensible, peut être facilement adapté à l'évolution des besoins de n'importe quelle organisation.

En conséquence, des milliers d'entreprises, aéroports, ports, agences gouvernementales, hôpitaux et universités, ainsi que d'autres organisations, dans toutes les parties du monde, ont choisi de faire confiance à SiPass integrated pour leurs systèmes de contrôle d'accès.

Le contrôle d'accès sur mesure pour vos besoins spécifiques

Flexible et hautement sécurisé
SiPass integrated est conçu pour repondre aux exigences du contrôle d'accès dans les conditions les plus diverses: non critiques ou critiques, simples ou très complexes. Conçu pour des organisations de toutes tailles, opérant sur un ou plusieurs sites, il est absolument idéal: pour les implantations existantes comme pour les immeubles nouvellement construits. Le nombre total de titulaires de badges et de portes dans un système SiPass integrated est virtuellement sans limite. La gestion du système peut être confiée à différents opérateurs, disposant de droits divers.

Extrêmement flexible, SiPass integrated gère l'accès pour tous les types de locaux du petit bureau individuel ou immeuble résidentiel de quelques entrées aux grands complexes aux nombreux étages comportant des dizaines de milliers de portes, portails, barrières et ascenseurs, sur de nombreux sites répartis dans le monde.

Fonctionnalités personnalisables
SiPass integrated convient tout particulièrement aux environnements là où les informations sont très sensibles et où les risques potentiels d'espionnage sont élevés. Les interfaces normalisées permettent une intégration aisée aux processus de sécurité et systèmes commerciaux existants. Une large variété d'extensions logicielles peuvent servir à personnaliser le système afin de répondre à n'importe quels besoins spécifiques d'une organisation. Dans les cas où une organisation est devenue trop importante pour son système de contrôle d'accès, un nouveau système SiPass integrated peut prendre en charge les lecteurs, ainsi que les badges existants (Siemens ou fournisseur tiers). Les investissements effectués antérieurement en matière de sécurité ne sont pas perdus – on procède tout simplement à une migration vers le nouveau système.

Intégration avec d'autres systèmes
Capable de fournir des fonctionnalités de contrôle d'accès hautement évoluées, SiPass integrated supporte entièrement la prise en charge de systèmes de vidéosurveillance et de détection d'intrusion – de Siemens ou de fournisseur tiers – créant ainsi un système global de sécurité. Une intégration de base avec les systèmes de sécurité incendie est également disponible.

Les décennies d'expérience de Siemens en matière d'intégration de systèmes et de technologies normalisées nous permettent de proposer des systèmes de contrôle d'accès intégré, de détection d'intrusion, de vidéosurveillance et de sécurité incendie qui disposent de fonctionnalités et d'une qualité hors pair tout en apportant une grande pérennité aux investissements.

Points forts

- Architecture système modulaire pour l'adaptation sur mesure à tous les besoins
- Gestion étendue de l'identité avec intégration biométrique et cryptage DESFire
- Advanced Security Programming (ASP) pour les processus de sécurité automatisés
- Logiciel intuitif, convivial et d'une gestion aisée
- Reporting interactif perfectionné
- Support de composants Salto hors ligne
- Exploitable via WAN/LAN en environnement informatique TCP/IP existant

Hôpitaux

Universités

Aéroports

SiPass integrated: Composantes matérielles

SiPass integrated est entièrement personnalisé pour répondre aux besoins de l'organisation où il est installé. Il peut être paramétré pour surveiller les accès, ou les entrées et les sorties (anti-passback), et/ou il peut servir à commander le fonctionnement des ascenseurs. Les zones d'un immeuble où les exigences de sécurité sont plus élevées qu'ailleurs peuvent être sécurisées avec une technologie de vidéosurveillance.

Un système SiPass integrated est composé de toute une variété de composantes matérielles: contrôleurs centraux (ACC et ACC-Lites), modules de porte, modules de signalisation, lecteurs et badges. La sauvegarde et la restauration automatique de la base de données du système sont la garantie de l'intégrité du système. Transmission sécurisée des données sur tout le circuit – du badge d'identification au serveur – garantissant un haut niveau de sécurité global.

Contrôleurs

Les contrôleurs centraux AC5102 (ACC)
et l'AC5200 (ACC-Lite) jouent un rôle essentiel dans le système SiPass integrated; ce sont les interfaces entre le logiciel SiPass integrated et les équipements sur site (modules d'interface lecteurs, modules de point d'entrée et modules de point de sortie). Le contrôleur AC5200 assure pratiquement toutes les fonctions de l'AC5100 et les deux types de contrôleurs peuvent être associés sur un même site. Les communications entre les contrôleurs et le système sont de type point à point indépendamment du serveur SiPass; si la connexion avec le serveur est interrompue, le fonctionnement du système n'est pas affecté.

L'AC5102 est généralement utilisé dans des installations de grande taille tandis que l'AC5200 convient idéalement aux plus petites. Basé sur le matériel SR34i du système SiPass® Entro, l'AC5200 peut commander jusqu'à 8 portes; c'est une alternative très économique pour les succursales ou les sites distants.

Lecteurs et cartes d'identification

L'interface Wiegand spéciale de Siemens permet de connecter pratiquement n'importe quel lecteur Wiegand standard au système SiPass integrated. Diverses technologies de lecteurs peuvent se combiner à votre gré pour former un système répondant sur mesure aux exigences de sécurité propres à chaque installation (fonctions incluses: ouverture de session sécurisée sur PC, identification du véhicule et paiement en numéraire).

SiPass integrated: Composantes logicielles

Robuste et convivial, le logiciel SiPass integrated est le coeur du système. Le nombre total de contrôleurs pouvant être connectés est virtuellement illimité. Le logiciel, certifié Windows, dispose d'une architecture client/serveur performante; il est aisé à installer via son interface utilisateur de type graphique. Des fonctionnalités comme l'historique des événements, le traitement des alarmes, la fonctionnalité antipassback (y compris anti-passback pour groupe de travail), l'interverrouillage de porte, le mode escorte, la vidéosurveillance et les interfaces DVR – ainsi que la fonctionnalité Wiegand personnalisée exclusive du Siemens et le téléchargement intégré du firmware des équipements – sont toutes intégrées en standard dans SiPass integrated. Une large variété d'autres fonctions avancées sont également disponibles en complément.

SiPass integrated peut en outre offrir des interfaces sur mesure vers d'autres applications, afin d'assurer à tout moment une communication parfaite. Le logiciel supporte par ailleurs Citrix Services pour exploitation à distance, si nécessaire.

Fonctionnalités de base

SiPass integrated inclut toutes les fonctions que l'on est en droit d'attendre d'un système performant de contrôle d'accès, y compris le cryptage DESFire, le support de modems GSM, de lecteurs d'empreintes digitales, de périodes horaires, envois de commandes manuelles, l'affichage graphique d'états, actualisé de façon dynamique, des fenêtres d'acquittement d'alarme avec remarques et explications, une fonction complète d'archivage et de restauration du système et de nombreuses autres fonctions avancées.

Outil intégré de rapports interactifs

Le générateur de rapports interactifs garantit une identification et une évaluation rapides des événements du système. Le logiciel comprend un outil visuel de rapports en ligne, un système de rapports sur la base de données, un système de rapports sur l'historique, la possibilité de générer des rapports simultanés, des options de filtrage avancées, des critères de recherche avancés ainsi qu'une vue arborescente pour faciliter l'utilisation. Le système comporte une fonction de rapport pointer-cliquer, une structure d'informations hautement configurable et la possibilité d'effectuer un tri ciblé des informations.

Historique des événements

Traçabilité claire de toutes les modifications apportées dans le système, garantissant un enregistrement détaillé des changements dans la base de données. Les modifications sont simultanément enregistrées et affichées à l'écran, inclus le nom de l'utilisateur qui a effectué ces opérations. Cette fonctionnalité prouve que SiPass integrated est parfaitement adapté aux segments du marché pour répondre aux exigences strictes en matière de traçabilité et peut être validé comme système de contrôle d'accès conforme à la norme 21 CRF Part 11.

Gestion intégrée des alarmes

Le système de gestion des alarmes permet de configurer jusqu'à 1000 niveaux de priorité d'alarme. Afin de faciliter une gestion plus rapide, les alarmes sont affichées et mises en évidence graphiquement selon leur priorité. Le système propose aussi des instructions d'alarme personnalisables pour assister le personnel chargé de la sécurité.

Anti-passback et rapport de rassemblement

La fonction anti-passback est d'empêcher que le même badge serve pour deux accès. Les entrées dans une zone anti-passback et les sorties de cette zone doivent concorder, sinon les entrées ou sorties suivantes peuvent être refusées. L'anti-passback permet également de générer un rapport de rassemblement qui assure la précision du décompte des personnes, de leur identification, de leur localisation à une heure donnée, ce qui peut être crucial en cas d'urgence. SiPass integrated comprend aussi une fonction anti-passback par groupe de travail, ce qui signifie que lorsqu'une zone anti-passback a été définie, il est possible de contrôler combien de personnes d'un groupe particulier se trouve dans cette zone à un moment donné. Cela peut être effectué tout en gérant les limites de la zone globale.

Partitionnement des privilèges d'opérateur

Le partitionnement peut servir à subdiviser les privilèges d'opérateur de manière à ce que les opérateurs gèrent uniquement l'accès aux zones qui leurs sont attribuées. Le système peut contrôler les titulaires de badges, les unités, les équipements FLN et les périodes horaires pouvant être gérés par les opérateurs. Une structure arborescente permet d'identifier et de sélectionner aisément les privilèges correspondants pour les affecter à un opérateur. Lorsque le partitionnement est effectué par titulaire de badge, il est possible de limiter l'accès à la zone du groupe de travail et/ou de limiter l'accès aux masques du titulaire de badge et visiteur. Le résultat correspond à une meilleure maîtrise de la sécurité des informations et la capacité d'empêcher une affectation non autorisée de privilèges d'accès.

Gestion des titulaires de cartes d'identification

Ajouter dans SiPass integrated des informations sur un titulaire de carte, c'est tout simple. Si nécessaire, il est possible d'attribuer plusieurs cartes à une même personne. Le modèle de conception défini par l'utilisateur permet l'établissement d'un layout spécifique, grâce à la configuration drag and drop, y compris le réglage des paramètres pour différents champs et boutons. On peut également importer ou exporter dans les systèmes SiPass integrated des pages au format XML définies par l'utilisateur.

Contrôle avec escorte

SiPass integrated dispose d'une fonction de contrôle avec escorte qui prévoit que deux badges valides doivent être présentés pour l'ouverture de la porte. Cette fonctionnalité peut être très utile dans les zones de haute sécurité où les visiteurs et les employés sont escortés par un agent de la sécurité ou un superviseur. Le mode auto-autorisation et le mode superviseur/accompagnant sont tous les deux disponibles et il est aussi possible de configurer l'heure de début et de fin, ainsi qu'un délai.

Interverrouillage de porte

Cette fonctionnalité permet de définir un groupe de portes pour assurer que, lorsque l'une des portes de ce groupe est ouverte, aucune des autres ne pourra être déverrouillée. L'interverrouillage de portes permet de créer des sas pour répondre aux besoins dans les domaines médicaux, bio-tech, dans les aéroports ou dans d'autres applications de haute sécurité.

Téléchargement intégré du firmware des équipements

Fonction rapide et simple pour modifier le firmware des équipements matériels directement depuis l'interface utilisateur (GUI). Le firmware de tous les équipements connectés peut être aisément mis à niveau de manière simultanée afin de garantir que la dernière version est installée. Ceci peut être effectué en une seule opération, ce qui représente une grande économie de temps et d'argent.

Points forts

- Fonction interactive de reporting
- Affectation distincte des droits des utilisateurs
- Gestion des données des utilisateurs
- Fonction escorte
- Advanced Security Programming
- Disponibilité intégrale

Interface avec la gestion vidéo SiNVR

Cette interface permet de connecter SiPass Integrated au système de gestion vidéo SiNVR de Siemens et d'enregistrer les images caméra sur la base des événements d'accès.

Fonctionnalités supplémentaires

Les modules logiciels en option pour SiPass integrated permettent de personnaliser le système afin de répondre pratiquement à toutes les exigences en matière de contrôle d'accès.

Composants Salto hors ligne
Cette fonction permet d'ajouter des composants Salto hors ligne (portes) à un système SiPass integrated. Il est possible d'affecter des autorisations d'accès dans le logiciel SiPass integrated, aussi bien pour les composants en ligne que hors ligne.

Photo d'identification et vérification d'image
Cette option permet de capturer et d'enregistrer la photo et la signature du titulaire de badge et de l'imprimer sur un badge pour servir à une identification visuelle.

Exportation Temps et présence
Cette option permet d'extraire toutes les données d'activités consignées dans SiPass integrated et de les exporter vers une gestion du temps et de présence de votre choix, au format adapté.

Gestion d'ascenseur
L'interface de gestion d'ascenseur permet de gérer chaque étage comme point d'entrée avec les options de contrôle d'accès inclus les horaires où l'accès est possible, le code d'accès journalier l'affectation du PIN et même la vérification d'image pour une sécurité complète.

Envoi de message
L'option d'envoi de message permet d'envoyer automatiquement des messages texte personnalisés aux pagers, téléphones mobiles ou adresses e-mail des personnes importantes en cas de violation de la sécurité ou d'autre événement important.

Echange de données personnelles (API HR)
L'API HR standard permet de faire communiquer des applications professionnelles tierces avec SiPass Integrated et d'échanger des données générales. Cela évite d'avoir à entrer des données identiques dans plusieurs systèmes. Les données relatives au contrôle d'accès des titulaires de cartes et d'autres personnes peuvent être lues et modifiées p. ex. via un navigateur Web ou un système HR. Outre les fonctions de l'API HR standard, l'API HR étendue offre d'autres possibilités pour les applications tierces, comme l'attribution d'autorisations d'accès aux titulaires de cartes ou l'octroi d'un droit d'accès provisoire à un visiteur.

Poste de gestion (API)
Le poste de gestion API permet l'intégration aisée à pratiquement tout système de gestion.

Gestion des visiteurs
L'option de gestion des visiteurs permet d'utiliser une même interface utilisateur graphique pour la gestion des titulaires de cartes permanentes et l'enregistrement des utilisateurs. Cela permet d'enregistrer des photos des visiteurs et de les copier dans des fichiers images existants, de saisir des données personnelles, d'imprimer des cartes de visiteurs individuelles et de suivre l'emplacement du visiteur dans le système SiPass-Integrated.

Graphiques
L'option Graphiques permet de concevoir, importer et réaliser des graphiques personnalisés permettant aux agents de sécurité de gérer visuellement les conditions d'alarme et de surveiller en permanence l'état de tous les points du système.

Encodage de badge Mifare (DESFire)
La technologie des badges Mifare permet d'utiliser un badge pour toute une variété de fonctions, y compris l'accès aux portes et la monétique. Le codage complet des badges Mifare et la configuration des profils sont une fonctionnalité unique de SiPass integrated. Le système prend aussi en charge le codage des badges Mifare 4K.

Interface DVR tiers
A l'aide de cette interface logicielle, il est possible de lancer un enregistrement à partir de n'importe quelle caméra en cliquant avec la souris, en utilisant des raccourcis basés sur l'enregistrement, créés facilement et placés sur des graphiques. Tous les événements enregistrés et leur état apparaissent en temps réel sur le fil de l'eau et peuvent être rediffusés instantanément en cliquant sur l'événement enregistré.

Station de travail activée en vidéosurveillance
Cette performante fonction supplémentaire permet de visualiser directement sur le client SiPass integrated les images des caméras IP ou analogiques du système de vidéosurveillance. Une carte de capture vidéo intégrée permet de visualiser la sortie de n'importe quelle caméra et d'utiliser les commandes pour les fonctions de vidéosurveillance standard comme le zoom, le panoramique, l'inclinaison et les mouvements de caméra.

Interface de matrice de vidéosurveillance tiers
Cette extension logicielle permet d'établir une interface pour une large gamme de systèmes de vidéosurveillance afin de transformer votre client SiPass standard en un poste de vidéosurveillance interactif, et ainsi de contrôler le fonctionnement des composantes de vidéosurveillance à partir de l'interface utilisateur SiPass.

Module intrusion
Cette option garantit les fonctions de détection d'intrusion natives. Lorsqu'il est installé, il est possible de connecter des détecteurs de mouvement directement à SiPass integrated; le système peut être utilisé à la fois comme système de contrôle d'accès et de détection d'intrusion. Les mêmes lecteurs de badges sont alors utilisés pour le contrôle d'accès et pour activer et désactiver le système de détection d'intrusion. Ou alors, dans les cas où un système de détection d'intrusion certifié est exigé, cette option permet d'intégrer une centrale dédiée Intrunet SI dans un système SiPass integrated. Il est également possible aux clients Intrunet SI d'utiliser ce module pour d'ajouter une application de contrôle d'accès complète à leur suite d'outils de gestion d'immeuble.

Points forts

- Support de composants Salto hors ligne
- Cryptage Mifare et Mifare DESFire
- Commande d'ascenseur évoluée
- Intégration sans faille de modules de détection d'intrusion SPC et Sintony
- Poste de gestion API
- DVR API
- Interopérabilité OPC alarmes et événements

Interopérabilité OPC alarmes et événements
L'interface serveur OPC permet de transmettre événements et alarmes de SiPass integrated aux clients OPC, p. ex. aux systèmes de gestion des bâtiments, et de recevoir leurs réponses. Le client OPC permet quant à lui d'établir une liaison avec le serveur OPC: SiPass integrated peut ainsi recevoir des avis sur les alarmes et événements d'autres systèmes et créer une application commune pour la surveillance et l'information en temps réel. A réception d'un message, SiPass integrated l'affiche dans sa propre interface graphique. L'exploitant n'a donc rien à modifier à ses programmes pour le lire.

Applications SiPass integrated

La souplesse, la fiabilité et la capacité supérieure d'évolution de SiPass est la garantie de pouvoir le mettre en place dans pratiquement tous les environnements – grands immeubles de bureau, agences gouvernementales, sites commerciaux, sociétés pharmaceutiques ou encore institutions financières, pour ne citer que quelques exemples. Les fonctionnalités avancées de SiPass integrated peuvent aider différents types d'organisation à répondre aux défis de la vie réelle de différentes manières suivantes.

Universités et autres campus

Idéal pour les campus pour gérer facilement l'accès à des nombreux bâtiments avec différentes exigences de sécurité et enregistrer et traiter de grandes quantités de données de titulaires de badges. Durant les périodes particulièrement chargées comme celles des inscriptions, il n'est pas difficile d'attribuer les droits d'accès, en créant des numéros de badge et en imprimant une grande quantité, tout en communiquant simultanément avec le système de base de données des étudiants de l'université.

Aéroports

Conçu pour gérer le contrôle d'accès d'un trafic important, c'est un choix parfait pour les aéroports. Il assure une solution complète de contrôle d'accès et de sécurité avec intégration à des systèmes de vidéosurveillance et autres infrastructures de l'aéroport. L'interface d'une utilisation simple permet au personnel de sécurité de l'aéroport de surveiller aisément et efficacement leurs systèmes de sécurité à tout moment.

Complexes multi-mandants

Cette fonction permet à plusieurs entreprises d'exploiter pleinement, mais en toute indépendance, le même système de contrôle d'accès. C'est particulièrement utile dans les environnements où des unités résidentielles, des bureaux et des magasins de détail sont regroupés sous un même toit. Chaque niveau du système gère les groupes de personnes. Les installations existantes peuvent être intégrées sans difficulté et l'utilisation de différentes technologies de badge ne constitue pas un problème.

Hôpitaux

Trouver le bon équilibre en sécurité et accessibilité revêt une importance essentielle dans les environnements hospitaliers. Le trafic important, généralement caractéristique pour un hôpital et la combinaison de zones à faible sécurité avec des zones à haute sécurité, rend le choix d'un système souple et convivial comme SiPass integrated, comme le mieux adapté en matière de contrôle d'accès.

Sites de production

La sécurité est d'une importance capitale sur un site de production ou un site industriel. SiPass integrated contribue à faire respecter les exigences en matière d'hygiène et de sécurité en contrôlant les accès, en offrant des fonctions antipassback et en effectuant le décompte des personnes, ce qui permet d'établir rapidement et facilement un rapport de rassemblement et d'assurer le suivi des titulaires de badges dans les situations d'urgence.

Aperçu technique

SiPass Integrated MP2.6	
Système	
Nombre de portes	jusqu'à 96 par contrôleur (en fonction de la configuration du système)
Nombre de détenteurs de badges enregistrés (utilisateurs)	jusqu'à 500 000 par contrôleur (en fonction de la configuration du système)
Nombre de contrôleurs	jusqu'à 499 par système
Installation du matériel	Plug & Play (der ACC erfordert eine Erstkonfiguration)
Architecture Client/Serveur	Oui
Options de mise en réseau pour contrôleurs et serveurs	LAN/WAN/RTC (redondance possible)
Langues de base	allemand, français, italien, anglais, espagnol (autres langues également disponibles)
Interfaces	
Interface de vidéosurveillance Siemens intégrée	SiNVR
Intégration de la vidéosurveillance de tiers	option
Intégration DVR de tiers	option
HR API	option
Exploitation	
Interface utilisateur intuitive de type graphique	Oui
Générateur de rapports	Manuel ou automatique avec plus de 60 rapports standard
Gestion des alarmes	1000 niveaux de priorité d'alarme et notification d'alarme multimédia
Fonctions de contrôle d'accès étendues	Gestion des droits d'accès (par personne ou par groupe), profils d'accès temporaires, antipass-back global (contrôle des changements de secteurs), contrôle d'accès (quatre yeux), escorte et contrôle de suivi
Journal des événements	Actualisé en temps réel
Fenêtre d'état graphique	Oui
Journal opérateur	Oui
Base de données	
Administration étendue des données personnelles	Oui
Champs supplémentaires de base de données	définissables par l'utilisateur
Sauvegarde/restauration des données du système	manuelle ou automatique
Configuration requise	
Système d'exploitation	Windows 8, Windows 7, Windows XP, Windows Server 2012, Windows Server 2008, Windows 2003 Server
Systèmes de gestion de base de données	MS SQL Server 2005 Standard Edition, MS SQL Server 2005 Express Edition, MS SQL Server 2008, MS SQL Server 2008 Express Edition, MS SQL Server 2012 Standard Edition, MS SQL Server 2012 Express Edition

Plus de sécurité et plus de confort – le nouveau SIPORT

La garantie de la sécurité dans l'environnement commercial actuel requiert de la part des responsables une approche stratégique proactive permettant de garder en permanence de l'avance par rapport aux risques en constante évolution. Les experts en sécurité ont besoin de solutions robustes tournées vers l'avenir qui peuvent être utilisées de manière flexible lorsque les exigences de sécurité évoluent. Siemens relève ces défis avec le nouveau système SIPORT.

SIPORT est un système global, modulaire et fiable de contrôle d'accès et de gestion horaire. Il permet en toute simplicité aux personnes autorisées, comme vos collaborateurs ou vos visiteurs, de se déplacer librement dans votre bâtiment ou complexe de bâtiments tout en refusant l'accès aux personnes non autorisées. Et cela en temps réel. SIPORT dispose en outre d'une nouvelle interface intuitive que vous pouvez configurer selon vos besoins. L'utilisation de toutes les fonctions SIPORT est encore plus facile et vous gardez toujours une vue d'ensemble.

Sécurité et flexibilité grâce à la communication en temps réel

Sur le plan technique, la communication en temps réel implique p. ex. qu'une unité de commande de porte peut enregistrer 100 événements par seconde ou encore qu'un serveur en temps réel peut traiter jusqu'à 100 000 événements par seconde. Un système de contrôle d'accès en temps réel permet donc de localiser ou de suivre des personnes sur un site ou dans un bâtiment. Ces données de suivi peuvent être consultées en temps réel de façon permanente ou en fonction des événements.
Sur le plan de la sécurité, la communication en temps réel implique avant tout des données actuelles fiables et donc une possibilité d'intervention rapide en cas de besoin

Réseau global

SiPort vous offre une solution de contrôle d'accès au sein de votre entreprise en exploitant les infrastructures réseau existantes: que ce soit au niveau local pour une seule implantation ou au niveau mondial pour de nombreux sites aux fuseaux horaires différents.

Ouvert et évolutif

SiPort s'adapte efficacement aux processus de votre entreprise. Grâce à son architecture système ouverte, cette solution de contrôle d'accès s'intègre aisément aux environnements informatiques existants et peut évoluer en fonction des exigences croissantes.

Multiples possibilités d'intégration

L'utilisation de systèmes de gestion avancés permet de regrouper tous les messages d'alarme importants émis par SiPort sur une seule et même interface utilisateur – un gage de simplicité et de lisibilité accrues.

Fiabilité et sécurité

Toutes les données clients relatives aux l'accès sont enregistrées de manière redondante à différents endroits – dans l'unité de commande de porte ou dans le lecteur. En cas de panne d'ordinateur ou de réseau, les unités locales de commande de porte ou les lecteurs prennent le relais et assurent le contrôle d'accès. SiPort permet d'utiliser une carte d'entreprise valable dans le monde entier, par exemple pour l'ouverture d'une session sur ordinateur. Du lecteur au serveur, toutes les liaisons sont cryptées.

Modularité et extensibilité

Grâce à sa structure modulaire, SiPort permet d'adapter la taille et les fonctionnalités du système pour répondre en permanence à vos exigences croissantes. Vous pouvez également augmenter le nombre de cartes d'identification (1 000 000) et d'unités de commande de porte ou de lecteurs de proximité (jusqu'à 8192 par serveur) selon vos besoins et sans frais supplémentaires.

Points forts

- Vérification du système de contrôle d'accès en ligne par RTC (Real Time Communication) en «temps réel»
- Interfaces avec les systèmes IT, de surveillance vidéo, de détection d'intrusion* et d'alarme
- Possibilité d'adaptation aux besoins individuels, aux structures organisationnelles et aux processus de travail
- Système flexible de gestion horaire avec interfaces vers les programmes de gestion des salaires

* nécessaire dans la certification DE VdS

Confortable grâce à la nouvelle interface utilisateur: aperçu à travers la page de démarrage.

Le nouveau SIPORT est indépendant du navigateur et convient également aux tablettes.

Caractéristiques de performance: sécurité, confort et efficacité

Tous les modules logiciels de SIPORT 3.0 disposent d'une interface utilisateur commune, intuitive et conviviale.

Un nouveau confort d'utilisation exceptionnel

La nouvelle page de démarrage globale fournit un accès rapide et facile à chaque fonction du système. L'indépendance du nouveau navigateur de SIPORT offre un réel avantage: peu importe que vous utilisiez un ordinateur de bureau ou la fonction tactile de votre tablette. La flexibilité est inégalée et le confort d'utilisation optimal. De plus, le même poste de travail permet à plusieurs utilisateurs d'ouvrir une session dans la langue de leur choix et de travailler ainsi efficacement. Le login multilingue est disponible en allemand, en anglais et en français, et d'autres langues sont intégrées sur demande. Les messages peuvent être émis en version bilingue, p. ex. en anglais et en arabe. Un avantage qui sera particulièrement apprécié par les entreprises et les sociétés d'envergure internationale employant un personnel multinational.

Gestion sûre des utilisateurs

Un mot de passe protège l'accès aux fonctions du systèmes et aux banques de données. La gestion des utilisateurs du système de contrôle d'accès et de gestion horaire permet d'attribuer individuellement les autorisations d'accès aux fonctions et informations. Diverses options d'ouverture de session garantissent souplesse et sécurité d'accès: login direct dans SiPort, login depuis le compte Windows, depuis le PKI ou depuis le LDAP* (les données personnelles sont stockées dans une banque de données LDAP).

Gestion efficace des données personnelles

Quelques secondes suffisent pour modifier les droits d'accès: le caractère intuitif de l'interface renforce la sécurité. Affecter les données personnelles, les numéros de carte, les profils d'accès et les durées de validité est un jeu d'enfant. Les modifications sont aussitôt enregistrées dans tout le système et un seul ordre suffit pour modifier simultanément toutes les données sélectionnées.

Gestion d'identités

Un système de gestion d'identité s'appuie sur un service Active Directory permettant de gérer des profils d'utilisateurs et de participants, des certificats

* Importation à partir de répertoires accessibles via une connexion LDAP

Fonctionnalité mandant: différentes sociétés dans le même bâtiment peuvent utiliser le même système SIPORT.

numériques pour des infrastructures à clés publiques, des informations d'autorisation, des autorisations d'accès ainsi que d'autres attributs pertinents pour les utilisateurs et les participants pour fournir un accès protégé aux données, aux ressources réseau ou aux services distribués.

Gestion simple et claire des autorisations d'accès

La multiplication du nombre de profils d'accès peut brouiller la vision d'ensemble. La gestion des profils SIPORT vous aide à créer et attribuer les autorisations d'accès en toute simplicité. Vous pouvez rechercher, lister et modifier tous les profils existants selon divers critères. Ces filtres permettent de visualiser plus facilement à quel endroit et à quel moment les personnes ont des droits d'accès et quels lecteurs de carte sont affectés à quelles zones. Les serrures et cylindres électroniques intégrés de divers fabricants sont gérés comme des lecteurs de carte.

Traçabilité des événements et des alarmes

SiPort enregistre avec exactitude tous les événements et toutes les alarmes dans divers journaux (p. ex. accès autorisés ou refusés, heures de présence, alarmes de sabotage, etc.). Aux fins de traitement ultérieur, ces données peuvent être facilement affichées, triées, sélectionnées et imprimées sous forme de listes, voire exportées.

Fonctionnalité multi-mandant

Les grands bâtiments abritent souvent plusieurs entreprises. L'accès aux espaces dédiés à chacune d'entre elles doit être géré séparément, tandis que les zones destinées à un usage général doivent être accessibles à tous. Chaque client (une société ou une division, par exemple) gère ses propres données et reçoit uniquement les messages (alarmes, par exemple) qui le concernent. Les autres mandants ne peuvent donc pas consulter ces informations. Grâce à sa fonctionnalité multi-mandant, SiPort offre une gamme de configurations pratiquement illimitée. Il en va de même pour les entreprises à croissance rapide: un système conçu pour un étage peut rapidement être étendu à tout un bâtiment, voire à de multiples sites répartis aux quatre coins du monde.

Points forts

- Gestion efficace et sûre: les changements prennent effet immédiatement
- Attribution simple de profils et définition d'exceptions
- Flexible grâce à la fonctionnalité mandant et aux possibilités d'extension
- Capacité d'adaptation individuelle grâce aux routines programmables
- Confort d'utilisation élevé grâce au multilinguisme
- Options de recherche librement configurables
- En plus des jours fériés nationaux, possibilité de définir des jours fériés régionaux ou locaux

Cardholder Management

Par excellence: commande intuitive et conviviale

Le logiciel SIPORT de base peut être complété par de nombreux modules supplémentaires.

Personnalisation des cartes (SIPORT SCEM)

SIPORT peut être complété par le module de codage de carte à puce Mifare® de SIPORT qui assure la personnalisation des cartes à puce.

- Personnalisation de puces Mifare* dans les cartes d'identification via le module de lecture et d'écriture Mifare externe ou intégré aux imprimantes de cartes
- Gestion de clés Mifare pour plusieurs clés et jeux de clés définissables
- Gestion de la mémoire Mifare
- Attribution d'un ID aléatoire pour un changement permanent du numéro d'identification unique (UID)
- Key Diversification: changement constant de la clé de chiffrement dérivé de la clé principale

Création de cartes d'identification (SiPort VAS)

SiPort dispose d'un système intégré de création de cartes permettant de concevoir, de gérer et de personnaliser des cartes ISO. Un seul et même processus permet à des imprimantes spéciales de coder et d'imprimer des cartes des cartes de proximité ou à codes-barres.

Tableau de présence (SiPort Display)

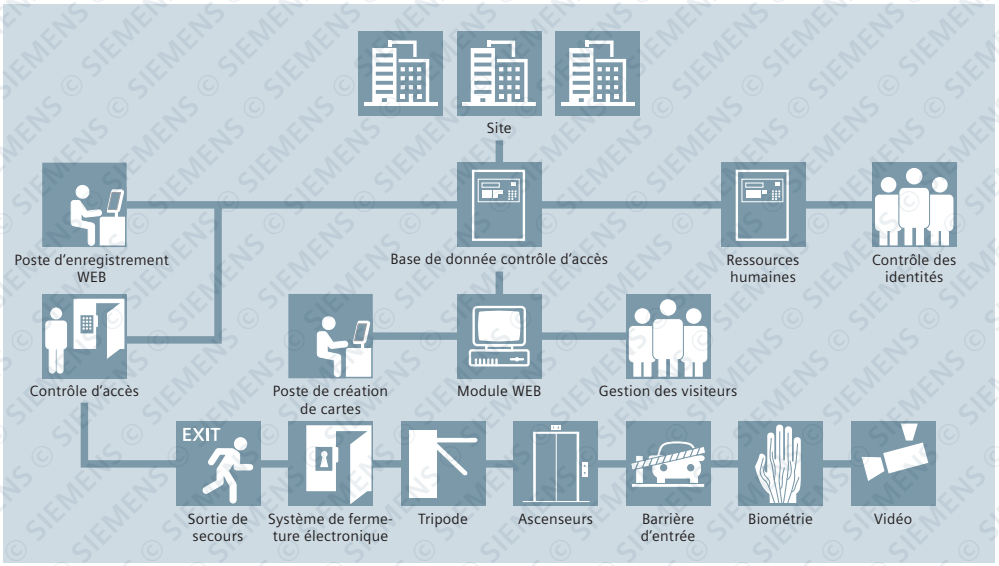
Il affiche en un clin d'œil les présences et les absences, ainsi que la localisation actuelle des personnes. SiPort Display est un instrument idéal pour le personnel de l'accueil, de la centrale téléphonique ou de la sécurité.

Représentation graphique du site (SiPort Graphic)

SiPort Graphic affiche en temps réel sous forme graphique les situations d'alarme, l'état des portes et des contacts, ainsi que les dysfonctionnements. En cas d'incident, le plan du site s'ouvre automatiquement et un changement de couleurs signale l'état actuel.

Le graphique permet le l'activation manuelle de certaines fonctions, comme l'ouverture, le verrouillage ou le blocage des portes, ainsi que le contrôle via des caméras de vidéosurveillance et l'affichage de leurs images.

* MIFARE Classic, MIFARE DESFireEv1



SIPORT permet d'attribuer différentes autorisations, comme p. ex. l'accès à des zones définies, l'accès au parking, l'attribution d'un poste de travail, etc. Les autorisations peuvent être limitées dans le temps.

Pré-enregistrement des visiteurs sur Internet (SIPORT Web Visit)

Basé sur Internet, le programme SIPORT Web Visit permet de préenregistrer les visiteurs depuis n'importe quel PC connecté à Internet ou Intranet.

Gestion des visiteurs (SiPort Visit)

SiPort Visit est l'outil idéal pour une loge ou une réception: il permet d'enregistrer les données des visiteurs et d'éditer des cartes d'accès. Cette extension logicielle supporte des fonctions supplémentaires, telles que l'impression d'étiquettes ou la prise de photos.

Gestion sur internet des données de détenteurs de carte (SiPort Web Cardholder)

Basé sur internet, SiPort Web Cardholder est un outil de gestion des données de détenteurs de carte.

Gestion des portes (SiPort WebDoor)

SiPort WebDoor permet de contrôler et de surveiller les portes via internet, ainsi que d'afficher des informations d'état, de planifier des libérations et fermetures ainsi que diverses fonctions de commande.

Connexion hôte

L'interface hôte SiPort sert à raccorder le système SiPort à un système supérieur (p. ex. SAP R/3) ou à importer des données d'une banque de données via une interface ODBC. Il est ainsi possible d'échanger des données personnelles avec d'autres systèmes de gestion.

Adéquation avec les applications pharmaceutiques

SiPort satisfait aux exigences de la réglementation 21 CFR partie 11, ainsi qu'à diverses autres directives internationales sur les «bonnes pratiques de fabrication». Il garantit la traçabilité constante des modifications, la définition et le contrôle des procédures lors de l'accès aux sections de bâtiment concernées.

Verrouillage de portes

La fonction de verrouillage permet de bloquer certains locaux pour une durée limitée. Le droit d'accès aux diverses zones, la durée et la cause du verrouillage sont enregistrés dans le profil d'accès des collaborateurs. Cette fonction peut s'avérer utile dans l'industrie pharmaceutique pour empêcher des contaminations croisées, par exemple.

Web Audit Trail

Cette application de gestion d'alarmes et de journaux permet à l'utilisateur d'accéder aux données de base SIPORT par Internet à partir d'un poste de commande.

Comparaison d'images

SIPORT permet de comparer des images enregistrées et des images en direct. De plus, il est possible de gérer simultanément plusieurs sas de sécurité sur un poste de travail.

Réservation de salles: directe, rapide et pratique

SIPORT peut faire encore plus

Pour optimiser l'efficacité des processus et des infrastructures, SIPORT s'intègre sans difficulté dans d'autres plateformes et sources d'informations.

Intégration à d'autres systèmes

SIPORT peut être intégré dans des systèmes de gestion de dangers et de bâtiments. L'échange d'informations d'états et de messages, ainsi que le déclenchement d'actions sont possibles de part et d'autre.

L'intégration de SIPORT dans Desigo Insight permet des interactions entre le système de contrôle d'accès et la technique de gestion du bâtiment. Cela permet en outre de réaliser des économies d'énergie. Il est ainsi possible de réduire ou d'éteindre l'éclairage, le chauffage ou la climatisation dans les zones où aucun collaborateur n'est présent.

Gestion de vidéos DVR

SIPORT et gestion de vidéos vont de pair. Des fonctions comme l'émission et l'enregistrement d'alarmes, l'affectation d'images ou de vidéos à une alarme et la lecture de l'enregistrement peuvent être directement réalisées à partir du système SIPORT ; le module SIPORT Graphic facilite l'affectation des caméras ou des moniteurs ainsi que la commande des fonctions de la caméra.

Caméras IP

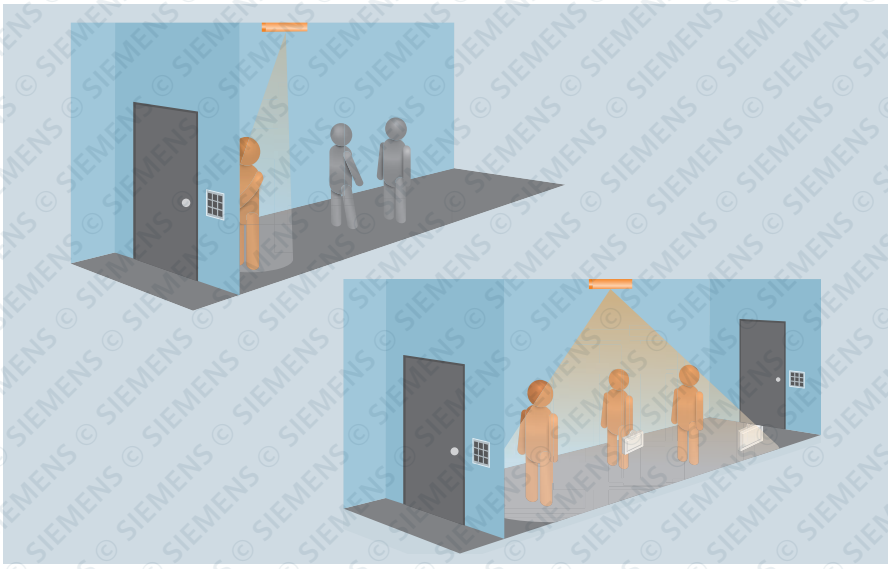
Les caméras IP pour l'enregistrement de séquences d'images en cas d'alertes ou de notifications peuvent être intégrées complètement dans SIPORT. Vous pouvez visualiser les enregistrements à tout moment en sélectionnant l'entrée adéquate dans le fichier journal. En toute simplicité et convivialité.

Réservation de salles

Les réservations complexes sont faciles à réaliser dans le système. Dans le Self-service Lobby, chaque utilisateur peut se connecter et réserver des salles, effectuer des réservations en série, choisir la disposition des chaises, commander des services de restauration, déclencher l'ouverture ou la fermeture des parois mobiles et même attribuer les autorisations d'accès correspondantes. La gestion en temps réel permet également d'effectuer des réservations ad hoc. Chacun peut réserver de manière directe et pratique et accéder rapidement aux salles disponibles, ce qui permet de réduire les coûts de l'organisation. Les surfaces disponibles sont occupées et utilisées de façon optimale.

* Importation à partir de répertoires accessibles via une connexion LDAP

SIPORT avec reconnaissance des plaques d'immatriculation



La solution de capteurs 3D identifie les individus et empêche l'entrée de personnes non autorisées.

Reconnaissance automatique des plaques d'immatriculation

Les plaques d'immatriculation peuvent servir à l'identification pour l'accès. Les plaques nationales et internationales sont toutes reconnues. Les opérations peuvent être enregistrées dans les journaux SIPORT et sont donc traçables rapidement et à tout moment. Cette fonction peut s'avérer utile, par exemple, pour l'accès au parking ou pour l'enregistrement des véhicules des visiteurs.

Capteurs 3D pour la détection des personnes

L'utilisation de solutions vidéo traditionnelles ne suffit pas toujours pour protéger les personnes et les objets. C'est pourquoi les solutions de capteurs 3D, qui comptent ou isolent les personnes mais le font de façon anonyme et sans atteinte à la vie privée, constituent désormais un composant essentiel d'une gestion de sécurité professionnelle.

Interface ODBC

Une interface de données de base peut être paramétrée simplement pour toutes les banques de données avec support ODBC. Son exécution peut être manuelle ou programmée. Une configuration par défaut de n'importe quel champ de données est possible.

Points forts

- Economie d'énergie et d'argent grâce à la connexion de SIPORT à la technique de gestion du bâtiment
- Contrôle d'accès pratique grâce une reconnaissance automatique des plaques d'immatriculation
- Connexion d'autres systèmes via ODBC et d'autres interfaces
- En plus des jours fériés nationaux, possibilité de définir des jours fériés régionaux ou locaux

Cylindre de verrouillage électronique intégré à SIPORT

Authentification biométrique, p. ex. par lecteurs d'empreintes digitales 3D et 2D

Des lecteurs ouverts à toutes les options

Polyvalents et performants, les lecteurs SIPORT se distinguent par leur design. La nouvelle gamme de lecteurs SIPORT se compose de divers types de lecteurs permettant une utilisation flexible dans les grandes et les petites entreprises.

Lecteurs de proximité

Ils fonctionnent avec des cartes de proximité, des porte-clés ou autres transpondeurs. Les données d'accès cryptées sont transférées sans contact de la carte au lecteur.

Lecteurs avec clavier

Pour plus de sécurité, la présentation de la carte de proximité s'accompagne de la saisie d'un code secret personnel.

Lecteurs d'accès pour interphones

Les lecteurs de carte peuvent également s'intégrer aux interphones: les collaborateurs et les visiteurs occasionnels disposent ainsi d'une seule interface.

Reconnaissance biométrique pour une sécurité accrue

SiPort offre un large éventail de possibilités d'utilisation des caractéristiques biométriques pour le contrôle d'accès: reconnaissance des empreintes digitales avec le lecteur biométrique Prestige, reconnaissance du visage, de l'iris ou des veines, etc.

Serrures et cylindres électroniques

Pour les lecteurs câblés ainsi que pour les serrures et cylindres électroniques non câblés, SIPORT permet une configuration et une commande constantes avec gestion partagée des autorisations. La transmission des données d'historique des serrures et des cylindres non câblés aux journaux SIPORT permet la traçabilité permanente de toutes les actions et modifications. La position de la porte est également transmise par hub radio.

Standard de sécurité élevé grâce à l'encodage

Légitimation: aussi simple que sûre

Tout confort

La carte RFID permet de commander des lecteurs sans contact. La carte combinée offre encore plus de confort avec deux technologies intégrées (p. ex. UHF et 13,56 MHz) pour différentes fonctions, p. ex. le contrôle d'accès avec une seule carte.

Sécurité accrue

Des cartes inscriptibles permettent également de répartir les diverses applications sur plusieurs segments ou secteurs. La responsabilité et la protection de l'accès aux différentes applications sont ainsi distinctes. La carte permet de stocker les données en toute sécurité. Toute transmission de données entre la carte, le lecteur et le serveur est cryptée. Si l'on complète une vérification par la saisie d'un code PIN ou la reconnaissance des caractéristiques biométriques (doigt, visage, iris, veines), la sécurité est encore plus élevée.

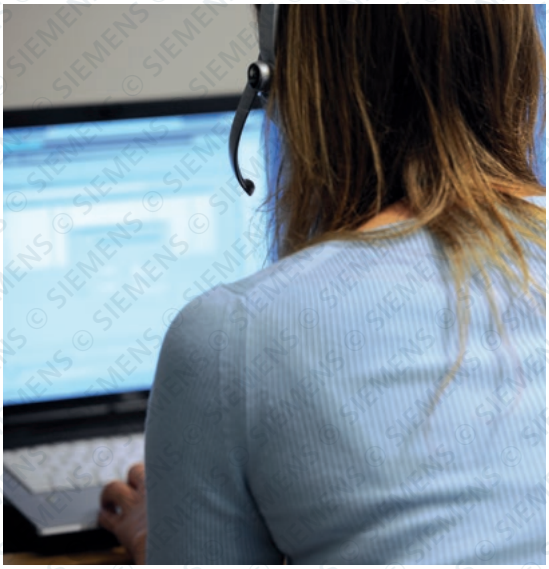
Multifonctionnalité

La multifonctionnalité de la carte à puce permet d'accéder au bâtiment et aux ordinateurs, d'ouvrir une application pour des sessions logicielles, de payer sans espèces à la cantine ou aux distributeurs de boissons, de saisir les horaires, etc.

L'enregistrement rapide et sécurisé des données dans la carte à puce mémoire inscriptible permettent de l'utiliser comme support de données (autorisations d'accès, modèles biométriques, etc.). L'utilisateur transporte ainsi les informations et les autorisations sur la carte.

Points forts

- Sécurité accrue grâce aux cartes inscriptibles, à la saisie du code PIN et aux photos imprimées sur les cartes
- Multifonctionnalité des cartes à puce: accès aux bâtiments et aux ordinateurs, paiement à la cantine, etc.
- Puces mémoires inscriptibles permettant le transport des informations et autorisations sur la carte



Pour gérer différents horaires de travail de façon confortable: p. ex. en production, IT ou logistique

Gestion et traitement des horaires: modernité et efficacité

Le système de gestion horaire de SiPort contrôle et gère les modèles flexibles du temps de travail, grâce à l'enregistrement automatique des timbrages au décompte du temps de travail et aux possibilités d'évaluation individuelle pour divers types d'horaires variables. Cette solution permet de collecter toutes les données nécessaires au calcul des salaires et au traitement des horaires.

Gestion et traitement des horaires

Particulièrement conviviale, cette solution système permet de saisir localement les horaires de travail pour les évaluer de façon centralisée, qu'il s'agisse d'horaires de travail mensuels, d'horaires variables, travail en équipes, de jours de congés ou de maladie. Toutes les informations peuvent être traitées, gérées ou évaluées en fonction des planifications et transférées à des systèmes supérieurs pour le calcul des salaires.

La saisie est grandement simplifiée par l'utilisation de lecteurs de proximité, de technologies de cartes multifonctionnelles ou de terminaux internet (solution mobile). Le système de gestion horaire de SiPort peut gérer jusqu'à 50 000 personnes en toute sécurité et en toute simplicité.

Intégration SAP R/3 et SiPort pour un échange mutuel de données

SiPort dispose d'une interface certifiée SAP pour l'échange de données entre SAP R/3 et le système de gestion horaire de SiPort. Les données du personnel peuvent être conservées dans le système SAP et transférées à SiPort. A l'inverse, l'interface permet le transfert de toutes les données horaires de SiPort vers SAP R/3, afin qu'elles soient disponibles pour le calcul des salaires.

Solutions pour des exigences spécifiques

SiPort permet de définir et programmer des routines pour résoudre les exigences particulières: horaires de pauses spécifiques, congés particuliers ou jours spéciaux.




Que ce soit à Johannesburg, Paris ou Singapour – SIPORT offre un accès dans le monde entier.

Efficacité des procédures automatisées grâce au module de flux de travail

Le module de flux de travail est une solution WEB efficace permettant aux collaborateurs autorisés de gérer leurs horaires de façon autonome: demandes de congés, absences ou corrections sont automatiquement transmises aux responsables par internet, selon des profils d'autorisation définis.

Accès universel grâce au terminal internet

SiPort Web client permet aux collaborateurs de saisir et de modifier leurs horaires de travail via un navigateur internet courant et de consulter leur décompte horaire. Accessible à tout moment et en tous lieux, cette fonction ne nécessite aucun logiciel supplémentaire.

Hosting

A présent, nous pouvons vous garantir la disponibilité des systèmes de gestion des temps ainsi que la transparence des coûts. Toutes les ressources IT requises sont dans les mains d'une équipe professionnelle.

Le déploiement et la maintenance du logiciel avec vos applications spécifiques sont réalisés dans notre centre informatique. Nous vous assurons ainsi une fiabilité élevée avec un équipement de sécurité et d'exploitation de première qualité.

Bien entendu, seuls les utilisateurs authentifiés ont accès à ces informations. Notre Siemens Security Network (SiSeNet) est un réseau de sécurité à large bande qui est disponible sur l'ensemble du territoire et répond aux exigences de sécurité les plus strictes.

Grâce à la transparence des coûts ainsi obtenue et la réduction de charge de travail de votre équipe IT, vous obtenez un retour sur investissement durable (ROI).

Points forts

- Interface certifiée entre SIPORT et SAP R/3
- Mise en œuvre d'exigences spécifiques aux clients (p. ex. réglementation des congés, temps de pause, etc.)
- Module de workflow pour des processus efficaces
- Hébergement pour la transparence et la réduction des coûts

1. Contrôle d'accès aux bâtiments
2. Etablissement des cartes
3. Gestion des visiteurs
4. Contrôle d'accès aux sites
5. Commande des ascenseurs
6. Autorisation d'accès à certaines zones
7. Systèmes de fermeture électroniques
8. Réservation de salle de réunion
9. Serveur de contrôle d'accès
10. Droits de stationnement
11. Utilisation de la station de chargement de voitures électriques

SIPORT se cache dans le détail

Plus qu'un simple contrôle d'accès

SIPORT est bien plus qu'un système de contrôle d'accès. Avec SIPORT et des extensions de matériel appropriées, vous êtes en mesure de gérer sûrement et efficacement une multitude de tâches.

Champion de la polyvalence

Les multiples fonctions de SIPORT sont utilisées à de nombreux endroits dans votre entreprise: il peut s'agir de l'accès à votre site, du parking souterrain, de la zone d'accueil, du centre de conférence ou même de la station de chargement pour les voitures électriques. Cela vaut aussi bien pour un bâtiment isolé que pour un campus, mais également pour les sites d'une entreprise à des endroits totalement différents dans le monde.

Savoir ce qui se passe

Grâce à la communication en temps réel, toutes les informations sont constamment à jour dans le système et peuvent être consultées n'importe où. Avec SIPORT, vous gardez toujours une vue d'ensemble.

Contacts centraux

Siemens Suisse SA
Building Technologies
Freilagerstrasse 40
8047 Zurich
Suisse
Tél. +41 585 578 700

Sécurité des bâtiments
Siemens Suisse SA
Building Technologies
Safety Technology
Industriestrasse 22
8604 Volketswil
Suisse
Tél. +41 585 578 700

Automatisation des bâtiments
Siemens Suisse SA
Building Technologies
Comfort Technology
Sennweidstrasse 47
6312 Steinhausen
Suisse
Tél. +41 585 579 200

CVC/KNX intégrateurs de systèmes, concepteurs, revendeurs et OEM
Siemens Suisse SA
Building Technologies
Control Products & Systems
Sennweidstrasse 47
6312 Steinhausen
Suisse
Tél. +41 585 579 220

Succursale de Bâle
Duggingerstrasse 23
4153 Reinach
Suisse
Vente
Tél. +41 585 567 111
Service Center
Tél. +41 842 842 013

Succursale de Berne
Obere Zollgasse 73
3072 Ostermundigen
Suisse
Vente
Tél. +41 585 576 111
Service Center
Tél. +41 842 842 013

Succursale de Lucerne
Platz 3
6039 Root D4
Suisse
Vente
Tél. +41 585 576 565
Service Center
Tél. +41 842 842 013

Succursale du Tessin
In Tirada 34
6528 Camorino
Suisse
Vente
Tél. +41 585 567 780
Service Center
Tél. +41 842 842 000

Succursale de Lausanne
Avenue des Baumettes 5
1020 Renens
Suisse
Vente
Tél. +41 585 575 677
Service Center
Tél. +41 842 842 033

Succursale de Genève
Chemin du Pont-du-Centenaire 109
1228 Plan-les-Ouates
Suisse
Vente
Tél. +41 585 575 100
Service Center
Tél. +41 842 842 033

Succursale de Zurich
Industriestrasse 22
8604 Volketswil
Suisse
Vente
Sécurité des bâtiments
Tél. +41 585 578 900
Automatisation des bâtiments
Tél. +41 585 578 278
Service Center
Tél. +41 842 842 023

Succursale de St.Gall
Industriestrasse 149
9201 Gossau
Suisse
Vente
Tél. +41 585 578 578
Service Center
Tél. +41 842 842 023

Succursale d'extinction
Dornierstrasse 18
9423 Altenrhein
Suisse
Vente
Tél. +41 585 575 575
Service Center
Tél. +41 842 842 023

Les informations fournies dans le présent document contiennent des descriptions générales des possibilités techniques qui peuvent ne pas s'appliquer pour tous les cas d'utilisation.
Les caractéristiques de performance souhaitées doivent toujours être spécifiées dans le contrat.
Le document contient un aperçu général des produits. La disponibilité peut varier en fonction du pays.
Pour obtenir des informations détaillées sur les produits, veuillez contacter la représentation locale de la société ou les partenaires agréés.

Notre monde connaît des mutations qui nous obligent à penser autrement: évolution démographique, urbanisation, réchauffement de la planète, restriction des ressources. Priorité est donnée à une efficacité maximale – et pas seulement en matière d'énergie. Il faut aussi offrir encore plus de confort pour assurer le bien-être des utilisateurs. Quant au besoin de protection et de sécurité, il ne cesse de croître. Pour nos clients, le succès se mesure à notre capacité de relever avec brio ces défis. Siemens possède les réponses.

«Nous sommes le partenaire technologique fiable pour des bâtiments et des infrastructures écoénergétiques, sûrs et protégés.»

www.siemens.ch/buildingtechnologies