(19) RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL
DE LA PROPRIÉTÉ INDUSTRIELLE

PARIS

(11) N° de publication : **2 635 895**
(à n'utiliser que pour les commandes de reproduction)

(21) N° d'enregistrement national : **88 11252**

(51) Int Cl[5] : G 07 C 9/00.

(12) DEMANDE DE BREVET D'INVENTION A1

(22) Date de dépôt : 26 août 1988.

(30) Priorité :

(43) Date de la mise à disposition du public de la demande : BOPI « Brevets » n° 9 du 2 mars 1990.

(60) Références à d'autres documents nationaux apparentés :

(71) Demandeur(s) : *Société dite : UNIDEL SECURITE, Société anonyme.* — FR.

(72) Inventeur(s) : Gilbert Deroudilhe ; Hélène Gaury.

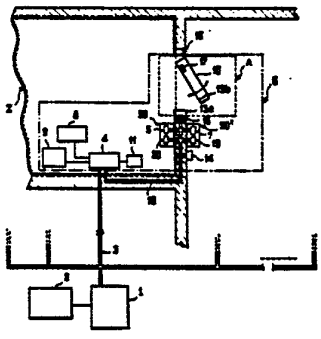
(73) Titulaire(s) :

(74) Mandataire(s) : Cabinet André Bouju.

(54) Système de gestion d'accès pour cartes à microcalculateur incorporé et procédé s'y rapportant.

(57) Le système de gestion d'accès à des zones d'accès contrôlé Z, mettant en œuvre des cartes à microcalculateur incorporé, comprend pour chaque zone d'accès contrôlé Z au moins un dispositif de contrôle d'accès 6 comportant des moyens de commande d'accès A, des moyens de lecture et d'écriture L pour cartes à microcalculateur incorporé, des moyens de saisie C de données externes et des moyens de gestion d'accès 4 reliés auxdits moyens de commande d'accès A, auxdits moyens de lecture et d'écriture L et auxdits moyens de saisie C pour mettre en œuvre lesdits moyens de commande d'accès A. Les paramètres de fonctionnement de chaque dispositif de contrôle d'accès peuvent être modifiés à partir desdits moyens de saisie C en combinaison avec la lecture par lesdits moyens de lecture et d'écriture L de données prédéterminées contenues dans une carte d'opérateur à microcalculateur incorporé.

Utilisation pour le contrôle d'accès à des zones et sites protégés.



FR 2 635 895 - A1

Vente des fascicules à l'IMPRIMERIE NATIONALE, 27, rue de la Convention — 75732 PARIS CEDEX 15

La présente invention concerne un système de gestion d'accès à des zones contrôlées, ces accès étant soumis à la présentation d'une carte à microcalculateur incorporé.

L'invention vise également le procédé mis en oeuvre dans le système conforme à l'invention.

Le contrôle des accès a un site ou une zone protégée présente une importance vitale pour la sécurité des installations et des personnes concernées. Pendant très longtemps, les contrôles d'accès ont été exclusivement assurés par du personnel de surveillance avec des contraintes de service assez sévères nécessitant des rotations et le risque de défaillances humaines. Par ailleurs, le développement de nouvelles méthodes de travail au sein des entreprises et la grande variété des aménagements horaires de travail, alliés bien souvent à une organisation complexe des services dans l'entreprise, ont rendu les contrôles d'accès très compliqués dans la mesure où le personnel affecté à un poste de contrôle d'accès doit pouvoir effectuer à la fois l'identification de la personne demandant l'accès et vérifier si celle-ci est effectivement autorisée à accéder dans la zone concernée à un instant donné. Il doit en outre consigner la demande et tous les paramètres liés à celle-ci. On comprend que, plus le site protégé est grand et les personnes habilitées à y accéder nombreuses, plus le risque de défaillance dans le contrôle d'accès augmente, affectant alors considérablement le niveau de sécurité du site.

On connaît déjà des systèmes de contrôle d'accès utilisant des cartes individuelles à support d'informations magnétique ou optique. Ces cartes, détenues par un utilisateur, sont insérées par celui-ci dans un lecteur approprié situé à proximité immédiate de l'accès contrôlé. Après lecture d'un code inscrit sur la carte d'utilisateur, ce code est ensuite comparé à un code prédéterminé propre à

l'accès concerné. Un résultat positif de cette comparaison commande la mise en oeuvre de moyens de déverrouillage de l'accès. Ce type de lecteur n'est en général relié à aucun autre dispositif central et est programmé localement.

On connaît aussi des systèmes de contôle d'accès tels que décrits ci-dessus mais comportant en outre un clavier. Après avoir inséré sa carte d'utilisateur dans le lecteur du système, le porteur de la carte frappe sur le clavier du système un code qui est propre à sa carte.

Le système compare alors le code frappé par le porteur au code lu par le lecteur sur le support magnétique de la carte. S'il y a identité, les moyens de commande d'accès sont mis en oeuvre. Le système de contrôle d'accès peut aussi en retour écrire des informations sur le support magnétique de la carte.

Ces systèmes, actuellement très répandus, présentent cependant plusieurs limitations et inconvénients. L'expérience a montré qu'il était relativement aisé à un spécialiste disposant de matériels appropriés de réaliser des cartes frauduleuses se substituant à des cartes authentiques et de neutraliser ainsi tout contrôle d'accès. Il existe des systèmes permettant de lire les bandes magnétiques qui sont le support des informations codées d'une carte. Ces systèmes présentent donc un niveau de sécurité assez faible. Par ailleurs, la gestion des droits d'accès détenus par un porteur de carte s'avère particulièrement délicate dès que sont envisagés des accès sélectifs dans le temps et dans l'espace pour un même détenteur de carte, qui doivent de plus pouvoir être modifiés en fonction des contraintes de service.

Le prestataire du service de contrôle d'accès doit pouvoir à la fois intervenir sur chacun des dispositifs de contrôle d'accès pour les paramétrer et sur les cartes d'utilisateur pour y implanter des codes

représentatifs des droits d'accès personnels du détenteur de la carte.

Ces opérations de paramétrage des dispositifs de contrôle d'accès et de personnalisation des cartes d'utilisateur doivent pouvoir être effectuées avec le maximum de sécurité et de souplesse de gestion. Les systèmes de contrôle d'accès actuels ne permettent pas de réaliser ces opérations dans ces conditions.

L'utilisation de cartes à microcalculateur incorporé, telles que décrites par exemple dans les brevets français 2 266 222, 2 311 365 et 2 311 360 est un atout majeur pour parvenir à un système de gestion d'accès présentant à la fois des garanties de sécurité et une grande souplesse d'emploi. En effet, ces cartes peuvent contenir un nombre élevé d'informations codées dont les accès en écriture et en lecture sont protégées de façon sélective. Ainsi, les cartes développées à partir du masque IV de la société BULL comportent un espace-mémoire structuré en zones de fonctions prédéterminées.

Une demande de brevet déposée le même jour que la présente par la demanderesse et intitulée "procédé de personnalisation pour cartes à microcalculateur et système pour sa mise en oeuvre" concerne précisément un procédé de personnalisation pour cartes à microcalculateur incorporé mettant à profit les spécificités du type précité.

Le but de la présente invention est de résoudre les difficultés liées à l'utilisation et à la gestion des systèmes de contrôle d'accès actuels en proposant un système de gestion d'accès à des zones d'accès contrôlé par la présentation d'une carte à microcalculateur incorporé.

Le système visé par l'invention comprend pour chaque zone d'accès contrôlé, au moins un dispositif de contrôle d'accès comportant des moyens de commande d'accès et des moyens de saisie de données extérieures.

Suivant l'invention, ce système est caractérisé

en ce que chacun desdits dispositifs de contrôle comprend en outre des moyens de lecture et d'écriture pour cartes à microcalculateur incorporé et des moyens de gestion d'accès reliés auxdits moyens de commande d'accès, auxdits moyens de lecture et d'écriture et auxdits moyens de saisie et coopérant avec lesdits moyens de lecture et d'écriture et lesdits moyens de saisie pour mettre en oeuvre lesdits moyens de commande d'accès en fonction, d'une part, de données indicatives de droits d'accès lues par lesdits moyens de lecture et d'écriture dans la mémoire du microcalculateur d'une carte d'utilisateur, et, d'autre part, de paramètres de fonctionnement prédéterminés contenus dans lesdits moyens de gestion d'accès et lesdits moyens de lecture et d'écriture, des moyens étant prévus pour modifier lesdits paramètres de fonctionnement à partir desdits moyens de saisie en combinaison avec la lecture par lesdits moyens de lecture et d'écriture de données prédéterminées contenues dans une carte d'opérateur à microcalculateur incorporé.

Ainsi, le système conforme à l'invention présente les caractéristiques requises pour, d'une part, assurer l'exploitation des demandes d'accès et d'autre part, permettre une gestion aisée des accès. En effet, l'existence, au sein du système conforme à l'invention, de moyens de gestion d'accès contenant des paramètres de fonctionnement prédéterminés, combinée à la présence dans la mémoire du microcalculateur incorporé dans la carte présentée par un demandeur d'accès, de données indicatives des droits d'accès conférés au porteur de la carte, autorise de grandes possibilités, d'une part, en matière de paramétrage des droits d'accès et d'autre part, en ce qui concerne la gestion des accès. Le fait que les paramètres de fonctionnement, qui sont par exemple les paramètres des plages horaires, de jours travaillés ou non travaillés, des listes d'opposition ou d'accès privilégiés,

puissent être modifiés en utilisant directement le lecteur de carte et le clavier du dispositif de contrôle d'accès facilite considérablement le paramétrage du contrôle d'accès puisqu'un opérateur habilité, titulaire d'une carte d'opérateur, peut intervenir directement sans manipulation complexe, sur les fonctions de paramétrage du dispositif.

Dans une version préférée de l'invention, le système de gestion d'accès comprend en outre des moyens de gestion à distance reliés à l'ensemble desdits moyens de gestion d'accès par des moyens de liaison et coopérant avec lesdits moyens de gestion d'accès pour paramétrer et exploiter lesdits dispositifs de contrôle d'accès. Ainsi, des moyens de gestion à distance peuvent assurer la gestion de plusieurs dispositifs de contrôle d'accès à des zones protégées distinctes, couvrant alors le contrôle des accès à un site complet. Par ailleurs, ces moyens de gestion assurent à distance le paramétrage de chaque dispositif de contrôle d'accès qui peut ainsi être effectué de deux façons : soit par intervention directe sur ce dispositif de contrôle d'accès en insérant une carte d'opérateur et en utilisant les moyens de saisie du dispositif, soit par transfert des paramètres de fonctionnement à partir des moyens de gestion à distance.

Selon un autre aspect de l'invention, le procédé de gestion d'accès à des zones d'accès contrôlé mis en oeuvre dans le système de gestion conforme à l'invention, comprend : une première étape de paramétrage du système au cours de laquelle, d'une part, des paramètres d'équipement sont définis et stockés de manière permanente respectivement dans les moyens de gestion d'accès et les moyens de lecture et d'écriture de chacun des dispositifs de contrôle d'accès, et d'autre part, des paramètres de fonctionnement, indicatifs des modes de fonctionnement spécifiques de chaque dispositif de contrôle d'accès, sont définis et stockés dans chacun des moyens de gestion

d'accès, et, pour chaque dispositif de contrôle d'accès, une étape d'exploitation de demandes d'accès, reçues à tout instant par lesdits moyens de lecture et d'écriture et lesdits moyens de saisie, et traitées par lesdits moyens de gestion d'accès.

La première étape du procédé conforme à l'invention peut être commune à l'ensemble des dispositifs de contrôle d'accès compris dans le système de gestion d'accès selon l'invention, tout en étant adaptée aux spécificités de chaque dispositif de contrôle d'accès (plages horaires, droits d'accès, notamment). Par contre, l'exploitation en temps réel, des demandes d'accès est effectuée à l'échelon du dispositif de contrôle d'accès préalablement paramétré.

Selon une version préférée de l'invention, le procédé de gestion d'accès comprend en outre, au cours de chacune desdites étapes d'exploitation, une ou plusieurs étapes de gestion dudit dispositif de contrôle d'accès, au cours desquelles un opérateur peut :

- obtenir des informations sur l'état et lesdits paramètres dudit dispositif de contrôle d'accès,
- modifier lesdits paramètres de fonctionnement,
- éditer des données indicatives de l'état dudit dispositif de contrôle d'accès et lesdits paramètres de fonctionnement.

Cette version du procédé illustre particulièrement la volonté d'obtenir une très grande souplesse dans la gestion des dispositifs de contrôle d'accès locaux, problème que vise à résoudre l'invention.

Ainsi, à tout moment pendant l'étape d'exploitation, un opérateur peut intervenir pour modifier les paramètres de fonctionnement, contrôler l'état du dispositif et obtenir l'édition des informations recueillies pendant cette opération de gestion.

D'autres particularités et avantages de

l'invention apparaîtront encore dans la description ci-après. Aux dessins annexés donnés à titre d'exemples non limitatifs :

- la figure 1 est le schéma synoptique du système de gestion selon l'invention,
- la figure 2 est le schéma synoptique d'un système de gestion structuré en réseau selon une version préférée de l'invention,
- la figure 3a montre un ensemble-lecteur de cartes à microcalculateur incorporé utilisé dans une version préférée de l'invention,
- la figure 3b montre un autre ensemble-lecteur de cartes de structure simplifiée, à microcalculateur incorporé utilisé dans d'autres versions de l'invention,
- la figure 4 représente la structure détaillée d'une partie du système selon l'invention, dans une application au contrôle d'accès par une porte,
- la figure 5 représente une version de réalisation du dispositif de contrôle d'accès dans laquelle un seul ensemble-lecteur conforme à la figure 3a est utilisé,
- la figure 6 représente une autre version de réalisation du dispositif de contrôle d'accès dans lequel un seul ensemble-lecteur simplifié est utilisé,
- la figure 7 montre en perspective la structure d'une unité de gestion à distance conforme à l'invention et ses liaisons avec les moyens de gestion d'accès,
- la figure 8 est l'organigramme général du procédé mis en oeuvre dans l'invention,
- la figure 9 est l'organigramme d'une séquence élémentaire d'exploitation d'une demande d'accès,
- la figure 10 montre les relations entre les différentes opérations de la séquence illustrée en figure 9 et les différents composants matériels d'un dispositif de contrôle d'accès,

- la figure 11 illustre les paramètres de fonctionnement affectés à un dispositif de contrôle d'accès conforme à l'invention ainsi que les codes principaux présents dans une carte d'utilisateur.

Le système de gestion d'accès conforme à l'invention et dont le schéma synoptique est présenté en figure 1, comporte plusieurs dispositifs de contrôle d'accès 6.1, 6.2, ..., 6.N, contrôlant l'accès à des zones Z1, ..., Z.M, des unités de gestion d'accès (UGA) 4.1, ... 4.N associées à chacun des dispositifs de contrôle d'accès, et un poste de gestion à distance 1 relié à l'ensemble des unités de gestion d'accès par un réseau de liaisons numériques 3. Ce poste de gestion à distance 1 peut comprendre des moyens de contrôle et de traitement 1a et une imprimante 2 pour la consignation des informations concernant le système. Chaque zone contrôlée Z1, Z2, ZM peut présenter un ou plusieurs accès contrôlés équipés d'un dispositif de contrôle d'accès. Celui-ci comporte des moyens d'accès, par exemple une porte, A1, A2, ..., AN, des moyens de saisie C1,C2, ..., CN situés de part et d'autre des moyens d'accès A1, A2,..., AN, qui peuvent être un clavier alphanumérique ou un bouton poussoir et des moyens de lecture et d'écriture L1, L2, ..., LN de cartes à microcalculateur incorporé. Dans une réalisation particulière de l'invention, le dispositif de contrôle d'accès comporte un premier dispositif lecteur de cartes L1, ..., LN à l'intérieur de la zone contrôlée Z1, Z2, ..., ZN et un second lecteur de cartes L'1, ..., L'N situé à l'extérieur de la zone contrôlée, ces deux dispositifs lecteurs étant tous deux placés à proximité de la porte d'accès A1, A2, ..., AN.

Dans une version avantageuse du système selon l'invention, illustrée par la figure 2, un poste de gestion centrale 31 relié par un réseau de communications 33 à plusieurs postes de gestion à distance 1.1, ..., 1.K,

assurant chacun la gestion du contrôle d'accès dans les différentes zones Z1.1, Z2.1, ..., ZM.1 d'un site SL1, ..., SLK, permet la gestion à partir d'un poste unique d'un nombre très élevé (jusqu'à 512) de dispositifs de contrôle d'accès à des zones géographiques dispersées, à travers un réseau de postes de gestion à distance 1.1, ..., 1.K, d'unités de gestion d'accès 4.1, 4.2, ... 4.N et de dispositifs de contrôle d'accès 6.1, ..., 6.N. Le poste de gestion centrale 31 peut avantageusement comprendre un microordinateur relié à une imprimante de consignation 32.

Un mode de réalisation préféré de l'invention consiste à regrouper les moyens de saisie externe C1, C2, .., CN et les moyens de lecture et d'écriture de cartes L1, L2, ..., LN au sein d'un ensemble unique 50, appelé boîtier-lecteur.

La figure 3a représente un exemple effectif d'un tel boîtier-lecteur, comprenant un clavier alphanumérique 51 de conception classique, un dispositif de lecture/écriture 54 pour cartes à microcalculateur incorporé, tel que celui développé par la société BULL, des afficheurs disposés en ligne 52, et optionnellement un interphone permettant d'engager une communication orale avec un gardien. Un tel boîtier-lecteur est en général scellé à une paroi et relié aux autres éléments du dispositif de contrôle d'accès de telle sorte qu'aucune liaison ni aucun organe de fixation ne soit accessible de l'extérieur du boîtier.

Une version simplifiée d'un tel boîtier-lecteur, représentée à la figure 3.b comporte uniquement un dispositif de lecture/écriture 64, semblable à celui installé dans les boîtiers-lecteurs 50 décrits ci-dessus, un bouton-poussoir 61, et optionnellement un interphone 63. Un boîtier-lecteur 50 de ce type est mis en oeuvre dans des versions simplifiées d'un système de contrôle d'accès conforme à l'invention qui seront décrites dans la suite.

Dans un mode de réalisation tel que celui illustré par la figure 4, un dispositif de contrôle d'accès 6 à une zone protégé Z comporte une porte 10 munie d'un équipement de verrouillage 13b qui, combiné avec un autre équipement de verrouillage 13a situé dans la paroi fixe de la zone Z, assure le verrouillage de la porte 10.

Le dispositif de contrôle d'accès 6 comporte en outre deux boîtiers-lecteurs 50, 50' disposés de part et d'autre de la paroi de la zone Z à proximité immédiate de la porte 10. Le boîtier-lecteur 50 contrôle la sortie de la zone Z tandis que le boîtier-lecteur 50' en contrôle l'entrée.

Chacun d'entre eux comporte un dispositif de lecture et d'écriture de cartes à microcalculateur incorporé 5, 7 et un clavier alphanumérique 20, 19 et est relié par une liaison numérique 18, par exemple de type liaison série, à une unité de gestion d'accès 4.

L'unité de gestion d'accès 4 a pour fonction de recevoir et de traiter des informations en provenance, d'une part du poste de gestion à distance 1 auquel elle est reliée par une liaison numérique 3, et d'autre part, de capteurs 15, 16, 17, des boîtiers-lecteurs 50, 50' et de boutons poussoirs 20, 14 situés respectivement à l'intérieur et à l'extérieur de la zone contrôlée Z, et de commander sélectivement l'accès à la zone contrôlée Z par activation du dispositif de commande de verrouillage 15. L'unité de gestion d'accès peut assurer aussi la consignation de l'ensemble des demandes d'accès et de leurs résulats par une imprimante de consignation 11 ainsi que la visualisation de ces informations sur un terminal vidéo 8.

Les capteurs 15, 16, 17 permettent d'assurer des fonctions de contrôle et de surveillance en fournissant à l'unité de gestion d'accès des signaux détectant respectivement :

capteur 15 : le verrouillage de la porte,

capteur 16 : la position de la porte (ouverte ou fermée (par un contact de feuillure),

capteur 17 : l'ouverture par effraction de la porte.

Elle assure aussi la mise en oeuvre de moyens d'alarme 9 en cas de transgression des moyens d'accès A.

Les boutons poussoirs 14, 20 sont utilisés pour demander respectivement l'accès à la zone contrôlée Z et la sortie de cette dernière, lorsque des conditions précises de paramétrage sont remplies, par exemple lorsqu'un accès libre est prévu dans une plage horaire prédéterminée.

D'autres versions du dispositif de contrôle d'accès 6 peuvent être envisagées. Ainsi, la sortie de la zone contrôlée Z peut n'être demandée que par la mise en action d'un bouton poussoir 20, en référence à la figure 5, suivant une disposition bien connue. De même, le boîtier-lecteur 60, situé à l'extérieur de la zone contrôlée Z, peut ne comporter qu'un bouton-poussoir 19b à la place du clavier 19a, en référence aux figures 6 et 5. Toutes ces combinaisons matérielles sont bien entendu soumises à des conditions de paramétrage et de gestion différentes.

L'intérêt du système de gestion d'accès réside principalement dans la possibilité d'assurer une gestion à distance de plusieurs dispositifs de contrôle d'accès.

En référence à la structure de réseau présentée à la figure 2, les postes de gestion à distance (1.1, 1.2, ... 1.K) jouent un rôle essentiel car ils assurent la liaison entre le poste de gestion centrale 31 et chacun des sites SL1, ..., SLK regroupant des zones contrôlées. Ces sites sont équipés d'autant d'unités de gestion d'accès 4.1, 4.2, ..., 4.N que d'accès à contrôler A1, A2, ..., AN. Chaque poste de gestion à distance 1 comporte, en référence à la figure 7, des moyens de contrôle et de traitement 100, un clavier alphanumérique classique 102, une imprimante de consignation 103 et un terminal vidéo 101. Dans une

réalisation effective de l'invention.

Chaque poste de gestion à distance 1, appelé en pratique unité de télégestion de système, peut gérer jusqu'à 32 unités de gestion d'accès à travers un réseau constitué de branches et de tronçons.

Une unité de télégestion de système 1 peut supporter 4 ou 8 branches, qui sont des lignes sortant de cette unité de télégestion 1 et sur lesquelles sont installées les unités de gestion d'accès 4 et des répéteurs R permettant chacun 4 extensions. En référence à la figure 7, chacune des branches 31, 32, 33, 34 est constituée de tronçons TR, définis comme des morceaux de branche ne traversant pas un répéteur R.

Un tronçon TR débute donc en sortie d'une unité de télégestion de système 1 ou d'un répéteur R et s'achève à une entrée d'un autre répéteur R ou à la dernière unité de gestion d'accès connectée sur la ligne.

Le poids des équipements connectés sur un tronçon TR est représenté par un nombre de charges. Ainsi, une unité de gestion 4 équivaut à 1 charge,

- une entrée de répéteur R, autonome ou intégré dans une unité de gestion d'accès équivaut à 4 charges,
- une sortie de répéteur, autonome ou intégré dans une unité de gestion d'accès équivaut à 1 charge,
- une entrée d'unité de gestion d'accès intégrant un répéteur équivaut à 5 charges,
- une sortie d'unité de télégestion de système équivaut à 1 charge.

Le réseau doit répondre simultanément aux trois conditions suivantes :

- une unité de télégestion gère au maximum 32 unités de gestion d'accès,
- un tronçon supporte au maximum 32 charges,
- la distance d'un tronçon doit être inférieure à 1,2 km.

Les techniques de transmission employées

s'appuient sur l'utilisation de liaisons-séries classiques (par exemple RS 485).

Les moyens de contrôle et de traitement 100 du poste de gestion à distance 1 incluent des mémoires vives, des mémoires reprogrammables (REPROM), une carte à microprocesseur et des moyens de transmission numérique de signaux. Ils sont reliés au poste de gestion central 31 par une liaison numérique série 33 pour les courtes distances (inférieures à 25 m) ou par une ligne téléphonique équipée de modems pour les distances plus élevées.

Dans une réalisation pratique du système conforme à l'invention, les unités de gestion d'accès 4, 4.1, ... 4. N, les moyens de contrôle et de traitement 100 du poste de gestion à distance 1 et les boîtiers-lecteurs comportent des mémoires non volatiles et reprogrammables, telles que des mémoires REPROM destinées à stocker les paramètres définissant les moyens de contrôle et de surveillance et les moyens de verrouillage.

On va maintenant décrire de façon détaillée le fonctionnement du système de gestion d'accès et plus particulièrement le procédé de gestion d'accès mis en oeuvre dans le système conforme à l'invention.

D'une manière générale, le procédé de gestion de droits d'accès comporte, en référence à la figure 8, une première étape de paramétrage EP du système de gestion, commune à l'ensemble des composants de ce système, suivie d'une étape d'exploitation EE1, ..., EEN des demandes d'accès spécifique à chaque accès contrôlé.

Chaque étape d'exploitation EE1, ..., EEN comporte une succession de séquences élémentaires D d'exploitation de demande d'accès et d'étapes de gestion EG du dispositif de contrôle d'accès 6.1, ..., 6.N qui peuvent être effectuées dans un ordre et une périodicité quelconques.

Une séquence élémentaire D d'exploitation d'une demande d'accès peut être divisée en plusieurs opérations illustrées sur la figure 9 :

- la vérification D ϕ de la carte d'utilisateur présentée par le demandeur d'accès et insérée dans un boîtier-lecteur et la recherche du bloc de contrôle d'accès parmi l'ensemble des blocs de service de l'espace mémoire EM de la carte,

- la lecture D1 de codes de droits d'accès CD et de codes prédéterminés, notamment un numéro d'identification NI, contenus dans la carte d'utilisateur,

- la saisie D2, par tabulation sur le clavier du boîtier-lecteur, de données externes d'identification, notamment un code d'utilisateur CP, fournies par le demandeur d'accès,

- le traitement D3 des codes prédéterminés lus dans la carte d'utilisateur en combinaison avec les codes de droit d'accès, les données externes d'identification et le paramètres de fonctionnement définis au cours de l'étape de paramètrage EP. Ce traitement, effectué par l'unité de gestion d'accès 4.1, ..., 4.N aboutit à une prise de décision concernant l'autorisation d'accès,

- si l'accès est autorisé, les moyens de commande d'accès A1, A2, ..., AN sont mis en oeuvre (opération D4). Dans la situation contraire, il y a rejet de la demande (opération D5), se traduisant en pratique par l'affichage d'un message de rejet sur les afficheurs du boîtier-lecteur sur lequel la demande d'accès a été enregistrée.

A chaque dispositif de contrôle d'accès 6,6.1, ... 6.N est associé un ensemble de paramètres de fonctionnement PF représenté à la figure 11.

Les paramètres de fonctionnement PF peuvent être groupés suivant des critères d'affinité fonctionnelle. On distingue ainsi des listes LB, LV, LR, LN contenant chacune un ensemble de numéros d'identification de cartes

d'utilisateur correspondant à des traitements particuliers des demandes d'accès.

Ainsi, une liste "noire" LN contient les numéros de cartes mises en opposition (cartes perdues ou volées, par exemple). Lorsqu'un dispositif de contrôle d'accès détecte une carte d'utilisateur dont le numéro appartient à cette liste noire LN, il provoque le blocage logique de cette carte, enlève le numéro considéré de sa liste noire LN et refuse l'accès au porteur de la carte.

Une liste "rouge" LR concerne les cartes dont les porteurs ne sont pas temporairement autorisés à franchir l'accès. A chaque numéro de carte contenue dans cette liste, est associée une date de fin d'appartenance à la liste. Une liste "verte" LV contient les numéros des cartes dont les porteurs sont temporairement autorisés à franchir l'accès sans contrôle des droits d'accès enregistrés. Enfin, une liste "blanche" LB contient les numéros des cartes dont les porteurs sont temporairement autorisés à franchir l'accès sans présentation de code quel que soit le mode de fonctionnement du système, hormis en fonction veille.

D'autres paramètres de fonctionnement sont l'indication des jours travaillés JT et des jours non travaillés JNT, les zones de temps ZT consistant en un ensemble de plages horaires autorisées en accès.

L'ensemble des paramètres de fonctionnement PF comporte en outre un sous ensemble de paramètres d'environnement PE permettant de définir l'environnement du dispositif de contrôle d'accès.

Les paramètres principaux de ce sous-ensemble sont :

- le numéro de zone d'accès ZA,
- un code de mode d'accès MA déterminant le type de mode d'accès utilisé,
- un code commun CC,
- un ensemble de temporisations T appliquées aux

signaux de commande et d'alerte du dispositif de contrôle d'accès,

- un code de mode de consignation MC des informations de gestion de droits d'accès.

Enfin, une horloge H constitue un paramètre essentiel de l'ensemble de paramètres de fonctionnement PF.

Le code de mode d'accès MA conditionne de façon prédominante le type de fonctionnement du dispositif de contrôle d'accès 6. Dans la réalisation pratique qui est décrite, il existe 5 modes d'accès correspondant à des niveaux de contrôle et de sécurité croissant et une fonction de veille.

On distingue ainsi :

- le mode commun simple : le franchissement de l'accès s'effectue en tabulant le code commun CC associé à cet accès,

- le mode commun normal : le franchissement de l'accès s'effectue en utilisant une carte d'utilisateur et en tabulant le code commun CC associé à cet accès,

- le mode normal : le franchissement de l'accès s'effectue en utilisant une carte d'utilisateur et en tabulant le code personnel CP associé à la carte,

- le mode accéléré : le franchissement de l'accès s'effectue en utilisant une carte d'utilisateur et sans tabulation de code,

- le mode d'alerte : le franchissement de l'accès s'effectue en utilisant une carte d'utilisateur et en tabulant un code alerte prédéterminé associé à la carte.

En fonction veille, le franchissement de l'accès est systématiquement refusé.

L'ensemble des paramètres de fonctionnement PF décrits ci-dessus est entré dans une mémoire vive de l'unité de gestion d'accès 4, en référence à la figure 11, lors de l'étape de paramétrage EP et peut être modifié lors d'une étape de gestion de droits d'accès EG pendant une

étape d'exploitation EE1, ..., EEN.

L'initialisation et la modification des paramètres de fonctionnement PF peuvent être effectuées par un opérateur soit à partir d'un boîtier-lecteur 50 en utiisant une carte d'opérateur, soit à partir du poste de gestion à distance 4 associé à l'accès concerné soit encore à partir du poste de gestion centralisé 1 contrôlant un ensemble de sites, si on considère une version complète du système de gestion d'accès conforme à l'invention,telle que représentée à la figure 2.

Par ailleurs, un ensemble de paramètres PL définit la structure matérielle du dispositif de contrôle d'accès 6, par exemple, la nature et les caractéristiques des dispositifs de contrôle et de surveillance 15, 16, 17 (contact de verrouillage, contact de feuillure, contact d'effraction) et des dispositifs de verrouillage. Ces paramètres, définis lors de l'installation matérielle du système de contrôle d'accès et spécifiques à chaque installation, sont transférés par des moyens bien connus de codage numérique et de transfert, dans des mémoires non volatiles ML et de préférence reprogrammables, telles que des mémoires REPROM.

Ces mémoires ML sont ensuite implantées dans les boîtiers-lecteurs 50 qui leur sont associés. De la même façon, à chaque unité de gestion d'accès 4 appartenant à un dispositif de contrôle d'accès donné 6, on associe lors de l'installation un ensemble de paramètres PM définissant l'environnement matériel de cette unité de gestion d'accès, par exemple, le nombre et la nature des boîtiers-lecteurs, la présence de moyens d'alarme, les capteurs existant.

Ces paramètres, ainsi qu'un microprogramme de gestion d'accès correspondant à l'exécution d'une séquence élémentaire de demande d'accès D (voir figure 10), sont écrits dans une mémoire MG non volatile reprogrammable de type REPROM. Cette mémoire est ensuite insérée dans l'unité

de gestion d'accès 4 correspondante.

Dans un système de gestion de droits d'accès conforme à l'invention et tel que celui représenté à la figure 1, le poste de gestion à distance 1, appelé dans une réalisation pratique de l'invention, unité de télégestion de système (UTS) comporte de préférence une "clé d'accès" informatique qui pourrait d'ailleurs être une carte opérateur, afin de n'autoriser l'accès aux fonctions de gestion à distance des dispositifs de contrôle d'accès qu'uniquement à des opérateurs habilités. Des paramètres PC définissant une clé d'accès peuvent être déterminés lors de l'installation du poste de gestion à distance 1, écrits dans une mémoire MC non volatile et reprogrammable, par exemple de type REPROM.

Cette mémoire MC est ensuite insérée au sein des moyens de contrôle et de traitement 100 du poste de gestion à distance 1.

Si on considère maintenant une carte d'utilisateur CM, celle-ci comporte un microcalculateur dont l'espace-mémoire EM est structuré en différents blocs, comme le représente la figure 11. La structuration de l'espace-mémoire EM est effectuée par mise en oeuvre du procédé de personnalisation objet d'une demande de brevet déposée le même jour que la présente demande et intitulé "procédé de personnalisation pour cartes à microcalculateur et système pour sa mise en oeuvre".

Les principaux blocs mémoire d'une carte à microcalculateur incorporé au format CLEMATIC CP8 ont déjà été divulgués et sont :

- une zone secrète ZS, comportant notamment le code personnel CP de la carte,
- une zone de mémoire d'accès ZA,
- une zone confidentielle ZC,
- une zone de travail ZT comportant notamment un bloc de service de contrôle d'accès BS,

- une zone d'information commune aux services ZI,
- une zone libre ZL,
- et une zone de fabrication ZF comportant notamment le numéro d'identification NI de la carte d'utilisateur CM.

Le bloc de service BS est constitué d'un ensemble de codes de droits d'accès DA1, DA2, ..., DAN, chacun de ces codes étant associé à une autorisation accordée au porteur de la carte d'utilisateur CM d'accéder à une zone contrôlée dans une plage temporelle donnée.

Chaque code de droit d'accès DA1, DA2,..., DAN est constitué de la juxtaposition d'un code de zone d'accès CA, indicatif de la zone accordée et d'un code de zone de temps CT, indicatif de la plage de temps accordée.

Ces codes de droits d'accès DA1, DA2, ..., DAN sont déterminés par le prestataire du service de contrôle d'accès physique, pour chacune des cartes d'utilisateur CM et entrés dans les microcalculateurs par mise en oeuvre du procédé de personnalisation évoqué plus haut. Ils peuvent être à tout moment modifiés par ce même procédé.

Lors du traitement d'une demande d'accès et plus particulièrement lors de l'exécution d'une séquence élémentaire D, représentée par les figures 9 et 10, l'utilisateur demandeur d'accès, introduit sa carte d'utilisateur CM, représentée à la figure 11, dans le boîtier-lecteur 50 (opération D1).

Le numéro d'identification NI de la carte est alors lu et comparé aux différentes listes LN, LR, LV, LB. Sa présence sur l'une de ces listes va entraîner un traitement particulier de la demande, comme cela a été décrit précédemment.

Si on considère le cas particulier où le numéro d'identification NI n'est présent sur aucune des listes, l'opérateur devra alors frapper sur le clavier C du boîtier-lecteur L, un code (opération D2). Ce code, soumis à un

algorithme de cryptage est alors comparé au code personnel CP écrit dans la zone secrète ZS de la carte. En général, un nombre limité prédéterminé de tentatives est autorisé. En cas d'échec, la carte peut être invalidée.

Sinon, à l'issue d'une séquence préalable de recherche du bloc de service de contrôle d'accès, les codes de droits d'accès DA1, ..., DAN contenus dans le bloc de service de contrôle d'accès BS de la carte sont lus et comparés aux paramètres d'identification de la zone d'accès ZA, des zones de temps autorisées T, de jours travaillés JT ou non travaillés JNT (opération D3). Si l'un au moins des droits d'accès contenus dans la carte est en conformité avec les paramètres de fonctionnement PF du dispositif de contrôle d'accès 6, l'accès est alors autorisé et les moyens d'accès A sont mis en oeuvre.

Toutes les étapes de la phase d'accès (déverrouillage, ouverture de la porte, fermeture, reverrouillage) sont contrôlées par les moyens de contrôle et de surveillance et éventuellement consignés, soit par une imprimante 11 reliée à l'unité de gestion d'accès 4, soit par une imprimante 2 reliée au poste de gestion à distance 1, en référence à la figure 4.

Bien entendu, l'invention n'est pas limitée aux exemples décrits et représentés et de nombreux aménagements peuvent être apportés à ces exemples sans sortir du cadre de l'invention.

Ainsi, le système de gestion d'accès selon l'invention peut aisément être adapté à d'autres services d'attribution sélective répartis en différents points d'un site, tels que des services de télécommunication ou de reproduction de documents.

REVENDICATIONS

1. Système de gestion d'accès à des zones d'accès contrôlé (Z, Z1, ..., ZM) dont l'accès est soumis à la présentation d'une carte (CM) à microcalculateur incorporé, comprenant, pour chaque zone d'accès contrôlé (Z, Z1, ..., ZM), au moins un dispositif de contrôle d'accès (6, 6.1, ... , 6.N) comportant des moyens de commande d'accès (A, A1, ... , AN) et des moyens de saisie (C, C1, ..., CN) de données externes, caractérisé en ce que chacun desdits dispositifs de contrôle d'accès (6,6.1, 6.2, ..., 6.N) comprend en outre des moyens de lecture et d'écriture (L, L1, ..., LN) pour cartes à microcalculateur incorporé, et des moyens de gestion d'accès (4, 4.1, ... 4.N) reliés auxdits moyens de commandes d'accès (A, A1, ..., AN), auxdits moyens de lecture et d'écriture (L, L1, ..., LN) et auxdits moyens de saisie (C, C1, ..., CN) et coopérant avec lesdits moyens de lecture et d'écriture (L, L1, ..., LN) et lesdits moyens de saisie (C, C1, ..., CN) pour mettre en oeuvre lesdits moyens de commande d'accès (A, A1,..., AN) en fonction, d'une part, de données lues par lesdits moyens de lecture et d'écriture (L, L1, ..., LN) dans la mémoire du microcalculateur de ladite carte (CM) présentée et, d'autre part, de paramètres de fonctionnement prédéterminés (PF) contenus dans lesdits moyens de gestion d'accès (4, 4.1, ... ,4.N) et lesdits moyens de lecture et d'écriture (L, L1, ... , LN), des moyens étant prévus pour modifier lesdits paramètres de fonctionnement (PF) à partir desdits moyens de saisie (C, C1, ..., CN) en combinaison avec la lecture par lesdits moyens de lecture et d'écriture (L, L1, ..., LN) de données prédéterminées contenues dans une carte d'opérateur à microcalculateur incorporé.

2. Système de gestion d'accès conforme à la revendication 1, caractérisé en ce qu'il comprend en outre des moyens de gestion à distance (1), reliés à l'ensemble desdits moyens de gestion d'accès (4, 4.1, ... 4.N) par des

moyens de liaison (3) et coopérant avec lesdits moyens de gestion d'accès (4, 4.1, ..., 4.N) pour paramétrer et exploiter lesdits dispositifs de contrôle d'accès (6, 6.1, ..., 6.N).

3. Système de gestion d'accès à des zones d'accès contrôlé (Z, Z1, ..., ZM) conforme à la revendication 1, lesdites zones d'accès contrôlé étant regroupées en plusieurs sites locaux (SL1, ..., SLK) géographiquement distincts, caractérisé en ce qu'il comprend :

- pour chaque zone d'accès contrôlé (Z, ...) , au moins un dispositif de contrôle d'accès (6, 6.1, ..., 6.N) comportant des moyens de commande d'accès (A, A1, ..., AM), des moyens de lecture et d'écriture (L, L1, ..., LN) pour cartes à microcalculateur incorporé, des moyens de saisie (C1, ..., CN) de données externes et des moyens de gestion d'accès (4, 4.1, ..., 4.N) reliés auxdits moyens de commande d'accès (A, A1, ..., AN), auxdits moyens de lecture et d'écriture (L, L1, ..., LN) et auxdits moyens de saisie (C, C1, ..., CN) et coopérant avec lesdits moyens de lecture et d'écriture (L, L1,..., LN) et lesdits moyens de saisie (C, C1,..., CN) pour mettre en oeuvre lesdits moyens de commande d'accès (A,A1, ..., AN) en fonction de données lues par lesdits moyens de lecture et d'écriture (L,L1, ..., LN) dans la mémoire du microcalculateur de ladite carte présentée (CM),

- pour chacun desdits sites locaux (SL1, ..., SLK) des moyens de gestion à distance (1.1, ..., 1.K) reliés à l'ensemble desdits moyens de gestion d'accès (4, 4.1, ..., 4.N) par des moyens de liaison (3.1, ..., 3.K) et coopérant avec lesdits moyens de gestion d'accès (4, 4.1, ..., 4.N) pour paramétrer et exploiter lesdits dispositifs de contrôle d'accès (6.1, 6.2, ... 6.N), et des moyens de gestion centralisée (31) reliés à l'ensemble desdits moyens de gestion à distance (1.1, ..., 1.K) par des moyens de liaison (33) et coopérant avec lesdits moyens de gestion

à distance (1.1, ..., 1.K) pour organiser, surveiller et gérer l'ensemble desdits dispositifs de contrôle d'accès (6. 1, ..., 6.N).

4. Système de gestion d'accès conforme à l'une des revendications 1 à 3, caractérisé en ce que dans l'un au moins desdits dispositifs de contrôle d'accès (6, 6.1, .. ., 6.N) à une zone déterminée (Z, Z1, ..., ZM) lesdits moyens de lecture et d'écriture (L, L1, ..., LN) comprennent, d'une part, des moyens de lecture et d'écriture d'entrée (7) situés à l'extérieur de ladite zone (Z, Z1, ..., ZM) et, d'autre part, des moyens de lecture et d'écriture de sortie (5), situés à l'intérieur de ladite zone (Z, Z1, ..., ZM), lesdits moyens de saisie (C, C1, ..., CN) comprenant, d'une part, des moyens de saisie d'entrée (19) situés à l'extérieur de ladite zone (Z, Z1, ..., ZM), et d'autre part, des moyens de saisie de sortie (20) situés à l'intérieur de ladite zone (Z, Z1,...,ZM) et en ce que lesdits moyens de gestion d'accès (4, 4.1, ...,4.N) sont situés à l'intérieur de ladite zone (Z, Z1, ...,ZM).

5. Système de gestion d'accès conforme à l'une des revendications 1 à 4, caractérisé en ce que dans l'un au moins desdits dispositifs de contrôle d'accès (6, 6.1, .. ., 6.N) à une zone déterminée (Z, Z1, ..., ZM) lesdits moyens de lecture et d'écriture (L, L1, ..., LN) sont regroupés à l'extérieur de ladite zone (Z, Z1, ..., ZM) et constituent ainsi des moyens de lecture et d'écriture d'entrée (7), lesdits moyens de saisie (C, C1, ..., CN) comprenant, d'une part, des moyens de saisie d'entrée (19) situés à l'extérieur de ladite zone (Z, Z1, ..., ZM), et d'autre part, des moyens de saisie de sortie (20) situés à l'intérieur de ladite zone (Z, Z1, ..., ZM) et en ce que lesdits moyens de gestion d'accès (4, 4.1,..., 4.N) sont situés à l'intérieur de ladite zone (Z, Z1, ..., ZM).

6. Système de gestion d'accès conforme à l'une des revendications 4 ou 5, caractérisé en ce que lesdits

moyens de lecture et d'écriture d'entrée (7) et lesdits moyens de saisie d'entrée (19) appartenant à un même dispositif de contrôle d'accès (6, 6.1, ..., 6.N) sont regroupés dans un boîtier-lecteur unique (50'),

- lesdits moyens de lecture et d'écriture de sortie (5) et lesdits moyens de saisie de sortie (20) appartenant à un même dispositif de contrôle d'accès (6, 6.1, ... 6,N) sont regroupés dans un boîtier lecteur unique (50).

7. Système de gestion d'accès conforme à la revendication 6, caractérisé en ce que l'ensemble desdits boîtiers-lecteurs (50, 60) comprend :

- un premier groupe de boîtiers-lecteurs (50) dans lesquels lesdits moyens de saisie (C, C1, ..., CN) comprennent un clavier,

- un second groupe de boîtiers-lecteurs (60) dans lesquels lesdits moyens de saisie (C, C1, ..., CN) comprennent un bouton poussoir.

8. Système de gestion d'accès conforme à la revendication 7, caractérisé en ce que lesdits boîtiers-lecteurs (50) dudit premier groupe comprennent en outre des moyens d'affichage (52).

9. Système de gestion d'accès conforme à l'une des revendications 6 à 8, caractérisé en ce que l'un au moins desdits boîtiers-lecteurs (50, 60) comprend en outre des moyens de communication orale (53, 63) reliés auxdits moyens de gestion d'accès (4, 4.1, ..., 4.N).

10. Système de gestion d'accès conforme à l'une des revendications 2 à 9, caractérisé en ce que lesdits moyens de gestion à distance (1, 1.1, ..., 1.K) comprennent:

- des moyens de contrôle et de traitement (100), pour traiter des informations saisies par des moyens de saisie (102) et des informations provenant desdits moyens de gestion d'accès (4.1, ..., 4.N) reliés par des moyens de

liaison (3) auxdits moyens de contrôle et de traitement (100),

- des moyens de visualisation (101) reliés auxdits moyens de contrôle et de traitement, pour visualiser les données traitées par lesdits moyens de contrôle et de traitement et afficher des messages d'information sur le fonctionnement dudit système de gestion.

11. Système de gestion d'accès conforme à la revendication 10, caractérisé en ce que lesdits moyens de gestion à distance (1, 1.1, ..., 1.K) comprennent en outre des moyens d'impression (103) pour consigner sur un support écrit lesdites données traitées et lesdits messages d'information.

12. Système de gestion d'accès conforme à l'une des revendications 10 à 11, caractérisé en ce que lesdits moyens de liaison (3) reliant lesdits moyens de contrôle et de traitement (100) à chacun desdits moyens de gestion d'accès (4.1, ..., 4.N) sont des liaisons série.

13. Système de gestion d'accès conforme à la revendication 3, caractérisé en ce que lesdits moyens de gestion centralisée (31) comprennent un microordinateur relié auxdits moyens de gestion à distance (1, 1.1, ... 1. K) par des liaisons série (33).

14. Système de gestion d'accès conforme à l'une des revendications 10 à 12, caractérisé en ce qu'il comprend en outre des moyens répéteurs (R) reliés à l'un au moins desdits moyens de gestion d'accès (4.1, ..., 4.N) et permettant auxdits moyens de gestion à distance (1, 1.1, ... 1.K) de gérer à distance des moyens de gestion d'accès supplémentaires (4.10, 4.20, 4.30, 4.40).

15. Système de gestion d'accès conforme à l'une des revendications précédentes, caractérisé en ce que chacun desdits dispositifs de contrôle d'accès (6, 6.1, ..., 6.N) comprend en outre des moyens de contrôle et de

surveillance (16, 17, 15) à proximité immédiate desdits moyens de commande d'accès (A, A1, ..., AN) et reliés auxdits moyens de gestion d'accès (4, 4.1, ..., 4.N) pour déterminer à tout instant l'état desdits moyens de commande d'accès et détecter toute action intempestive sur lesdits moyens de commande d'accès (A, A1, ..., AN).

16. Système de gestion d'accès conforme à l'une des revendications précédentes, caractérisé en ce que lesdits moyens de commande d'accès (A, A1, ..., AN) comprennent des moyens d'accès (10) tels qu'une porte, et des moyens de verrouillage (13a, 13b) comportant une première partie (13a) située sur lesdits moyens d'accès (10) et une seconde partie (13b) située en position fixe en un point de la frontière de ladite zone (Z, Z1, ..., ZN) contrôlée par ledit dispositif (6, 6.1, ..., 6.N), ladite seconde partie (13b) étant commandée par lesdits moyens de gestion d'accès (4, 4.1, ..., 4.N).

17. Système de gestion d'accès conforme à l'une des revendications 15 à 16, caractérisé en ce que l'un au moins desdits dispositifs de contrôle d'accès (6, 6.1, ..., 6.N) comprend en outre des moyens d'alarme (9), reliés auxdits moyens de gestion d'accès (4, 4.1, ..., 4.N) pour émettre des signaux d'alarme en réponse à la détection de situations anormales par lesdits moyens de contrôle et de surveillance (15, 16, 17).

18. Système de gestion d'accès conforme à l'une des revendications 15 ou 17 et 16, lesdits moyens d'accès (10) étant constitués d'une porte, caractérisé en ce que lesdits moyens de contrôle et de surveillance (15, 16, 17) comprennent :

- un contact d'effraction de porte (17) pour détecter l'ouverture par effraction de ladite porte,
- un contact de fermeture (16) pour détecter si ladite porte est ouverte ou fermée,
- un contact de fond de pêne (15) pour détecter

le verrouillage de ladite porte.

19. Système de gestion d'accès conforme à l'une des revendications précédentes, caractérisé en ce que chacun desdits moyens de gestion d'accès (4, 4.1, ..., 4.N) comprend en outre des moyens de mémorisation non volatiles et reprogrammables (MG) pour le stockage d'un microprogramme de gestion d'accès et de paramètres (PM) concernant l'ensemble des dispositifs reliés auxdits moyens de gestion d'accès (4, 4.1, ..., 4.N).

20. Système de gestion d'accès conforme à l'une des revendications 10, 11, 12, 14 et à l'une des revendications 15 à 19, caractérisé en ce que lesdits moyens de contrôle et de traitement (100) comprennent des moyens de mémorisation non volatiles et reprogrammables (MC) pour le stockage de paramètres (PC) définissant une clé d'accès, notamment une carte opérateur, autorisant l'accès auxdits moyens de gestion à distance (1).

21. Système de gestion d'accès conforme à l'une des revendications 6 à 20, caractérisé en ce que chacun desdits ensembles-lecteurs (50, 60) comprend en outre des moyens de mémorisation non volatiles et reprogrammables (ML) pour le stockage de paramètres (PL) d'équipement définissant lesdits moyens de contrôle et de surveillance (15, 16, 17) et lesdits moyens de verrouillage (13a, 13b).

22. Système de gestion d'accès conforme à l'une des revendications 19 à 21, caractérisé en ce que lesdits moyens de mémorisation (MG, MC, ML) sont des mémoires à semi-conducteur, de type REPROM.

23. Procédé de gestion d'accès à des zones contrôlées (Z, Z1, ..., ZM), mis en oeuvre dans le système de gestion de droits d'accès selon l'invention, ledit système de gestion comprenant pour chaque zone contrôlée (Z, Z1, ..., ZM) au moins un dispositif de contrôle d'accès (6, 6.1, ..., 6.N) comportant des moyens de commande d'accès (A, A1, ..., AN), des moyens de lecture et d'écriture pour

cartes à microcalculateur incorporé (L, L1, ..., LN), des moyens de saisie de données externes (C, C1, ..., CN) et des moyens de gestion d'accès (4, 4.1, ..., 4.N), caractérisé en ce qu'il comprend :

- une première étape de paramétrage (EP) dudit système de gestion (S) au cours de laquelle, d'une part, des paramètres d'équipement (PM, PL), sont définis et stockés de manière permanente respectivement dans lesdits moyens de gestion d'accès (4, 4.1, ..., 4.N), et lesdits moyens de lecture et d'écriture (L, L1, ..., LN) de chacun desdits dispositifs de contrôle d'accès (6, 6.1, ..., 6.N), et d'autre part, des paramètres de fonctionnement (PF), indicatifs des modes de fonctionnement spécifiques de chaque dispositif de contrôle d'accès (6, 6.1, ..., 6.N) sont définis et stockés dans chacun desdits moyens de gestion d'accès (4, 4.1, ..., 4.N),

- et pour chaque dispositif de contrôle d'accès (6, 6.1, ...,6.N), une étape d'exploitation (EE1, ..., EEN) de demandes d'accès reçues à tout instant dans lesdits dispositifs de contrôle d'accès (6, 6.1, ..., 6.N) par lesdits moyens de lecture et d'écriture (L, L1, ..., LN) et lesdits moyens de saisie (C, C1, ..., CN), et traitées par lesdits moyens de gestion d'accès (4, 4.1, ..., 4.N).

24. Procédé de gestion d'accès conforme à la revendication 23, caractérisé en ce qu'il comprend en outre, au cours de chacune desdites étapes d'exploitation (EE1, ..., EEN), une ou plusieurs étapes de gestion (EG) de l'un desdits dispositifs de contrôle d'accès (6, 6.1, ..., 6.N) au cours desquelles un opérateur peut obtenir des informations sur l'état et lesdits paramètres de fonctionnement dudit dispositif de contrôle d'accès, modifier lesdits paramètres de fonctionnement, éditer des données sur l'état dudit dispositif et lesdits paramètres de fonctionnement.

25. Procédé de gestion d'accès conforme à la

revendication 24, ledit système de gestion comprenant en outre des moyens de gestion à distance (1) reliés en réseau à l'ensemble desdits moyens de gestion d'accès (4, 4.1, ... 4.N), caractérisé en ce que lesdites étapes de gestion (EG) de chacun desdits dispositifs de contrôle d'accès (6, 6.1, ..., 6.N) peuvent être réalisées par lesdits moyens de gestion à distance (1) et en ce qu'elles permettent en outre de commander à distance la mise en action des moyens de commande d'accès (A) de chacun desdits dispositifs de contrôle d'accès.

26. Procédé de gestion d'accès conforme à la revendication 24, caractérisé en ce que la réalisation desdites étapes de gestion (EG) d'un dispositif de contrôle d'accès (6, 6.1, ..., 6.N) est soumise à la détention d'une carte d'opérateur à microcalculateur incorporé et à sa lecture par lesdits moyens de lecture et d'écriture (L, L1, ..., LN) dudit dispositif de contrôle d'accès (6, 6.1, ..., 6.N).

27. Procédé de gestion d'accès conforme à l'une des revendications 23 à 26, caractérisé en ce que pendant ladite seconde étape d'exploitation (EE1, ...EEN), une surveillance permanente des accès auxdites zones contrôlées, autorisées ou non autorisées, est effectuée, incluant la détection d'anomalies de franchissement ou d'effraction par des moyens de contrôle et surveillance (15,16, 17).

28. Procédé de gestion d'accès conforme à l'une des revendications 23 à 27, caractérisé en ce que ladite étape d'exploitation (EE1,..., EEN) comporte en outre une succession de séquences élémentaires d'exploitation (D) de demande d'accès à une zone contrôlée (Z, Z1, ..., ZM), effectuées à partir d'un dispositif de contrôle d'accès (6, 6.1,..., 6.N), comprenant chacune les opérations suivantes :

- la vérification (Dϕ) de la carte d'utilisateur à microcalculateur incorporé présentée par le demandeur d'accès et insérée dans lesdits moyens de lecture et

d'écriture (L, L1, ..., LN) et la recherche d'un bloc de service de contrôle d'accès (BS1) parmi les blocs de service (BS) contenus dans ladite carte d'utilisateur,

- la lecture (D1) de codes de droits d'accès (DA1, ..., DAN) et de codes prédéterminés, et notamment un numéro d'identification (NI), contenus dans la carte d'utilisateur à microcalculateur incorporé présentée par le demandeur d'accès, par lesdits moyens de lecture et d'écriture (L, L1, ...,LN),

- la saisie (D2) par lesdits moyens de saisie (C, C1, ...,CN) de données externes d'identification (CP), et notamment un code d'utilisateur, fournies par ledit demandeur d'accès,

- le traitement (D3) desdits codes prédéterminés lus dans ladite carte d'utilisateur, en combinaison avec lesdits codes de droits d'accès (DA1, ...,DAN), lesdites données externes d'identification et lesdits paramètres de fonctionnement définis au cours de la première étape de paramétrage (EP), aboutissant à une prise de décision concernant l'autorisation d'accès,

- la mise en oeuvre (D4) desdits moyens de commande d'accès (A, A1, ...,AN) lorsque l'autorisation d'accès est accordée, ou le rejet (D5) de la demande dans l'hypothèse contraire.

29. Procédé de gestion d'accès conforme à la revendication 28, caractérisé en ce que lesdits codes de droits d'accès (DA1, ..., DAN) contenus dans ladite carte d'utilisateur (CM) comportent chacun, d'une part, un code de zone d'accès (CA) indiquant l'accès que le porteur de ladite carte d'utilisateur (CM) peut franchir, et d'autre part, un code de zone de temps (CT), indiquant les périodes pendant lesquelles le porteur de ladite carte d'utilisateur (CM) peut franchir lesdits accès indiqués par ledit code de zone d'accès (CA).

30. Procédé de gestion de droits d'accès conforme

à l'une des revendications 28 ou 29, caractérisé en ce que lesdits paramètres de fonctionnement (PF) spécifiques à chaque dispositif de contrôle d'accès (6, 6.1, ..., 6.N) comportent des listes (LN, LR, LV, LB) comportant chacune un ensemble de numéros d'identification (NI) de cartes d'utilisateur, chacune desdites listes correspondant à un traitement particulier prédéterminé, par ledit dispositif de contrôle d'accès, des demandes d'accès effectuées avec une carte d'utilisateur dont le numéro d'identification appartient à ladite liste, et en ce que les contenus de chacune desdites listes (LN, LR, LV, LB) peuvent être modifiées pendant desdites étapes de gestion (EG).

31. Procédé de gestion d'accès conforme aux revendications 28 à 30, caractérisé en ce que lesdits paramètres de fonctionnement (PF) de chaque dispositif de contrôle d'accès (6, 6.1, ..., 6.N) comportent en outre un code de mode d'accès (MA) représentatif du choix par l'opérateur d'un mode d'accès prédéterminé pour ledit dispositif de contrôle d'accès (6, 6.1, ..., 6.N) indiquant d'une part, si une carte d'utilisateur (CM) est requise pour le franchissement d'accès, et, d'autre part, le type de données externes d'identification devant être saisies par lesdits moyens de saisie (C, C1,...CN).

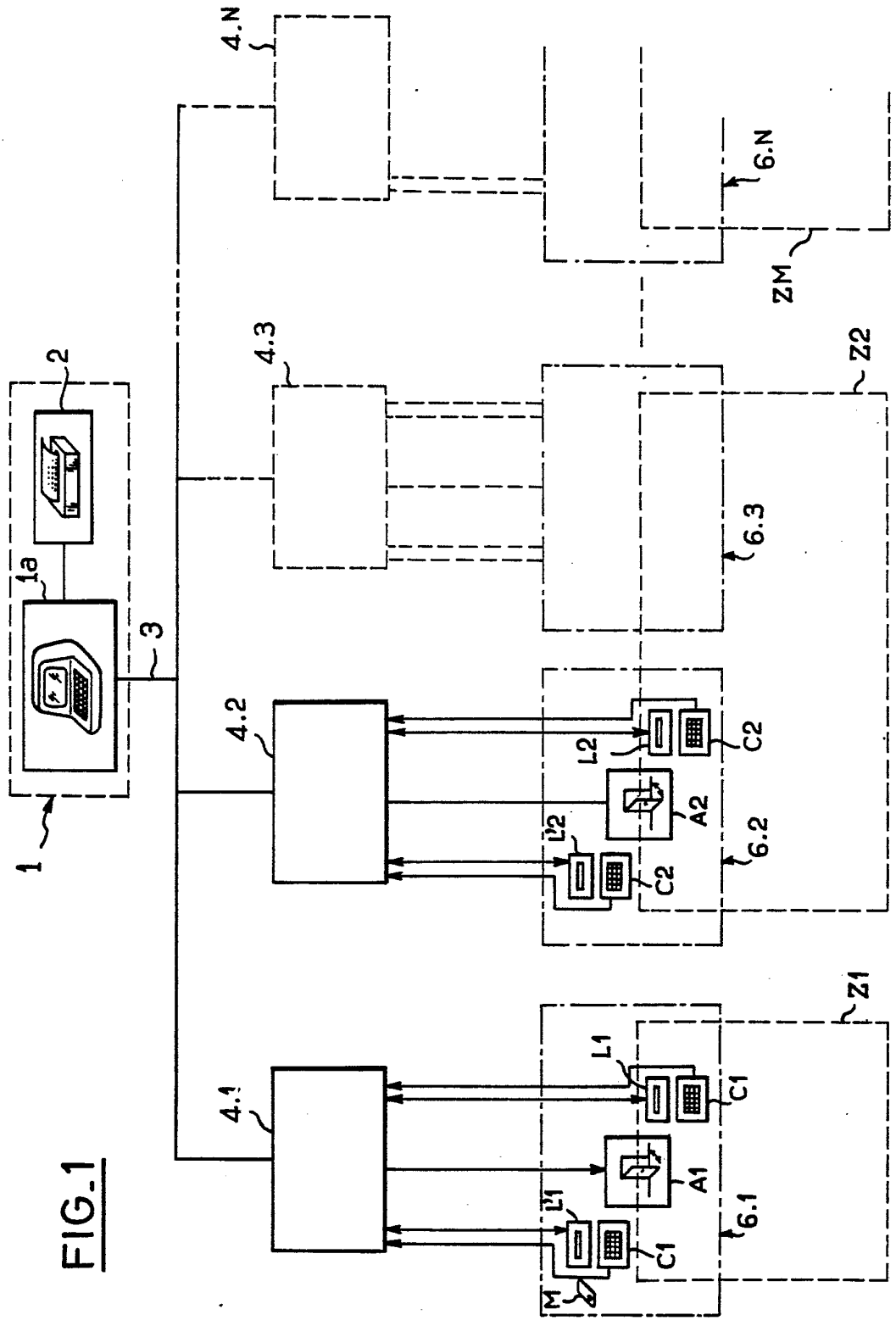


FIG.1

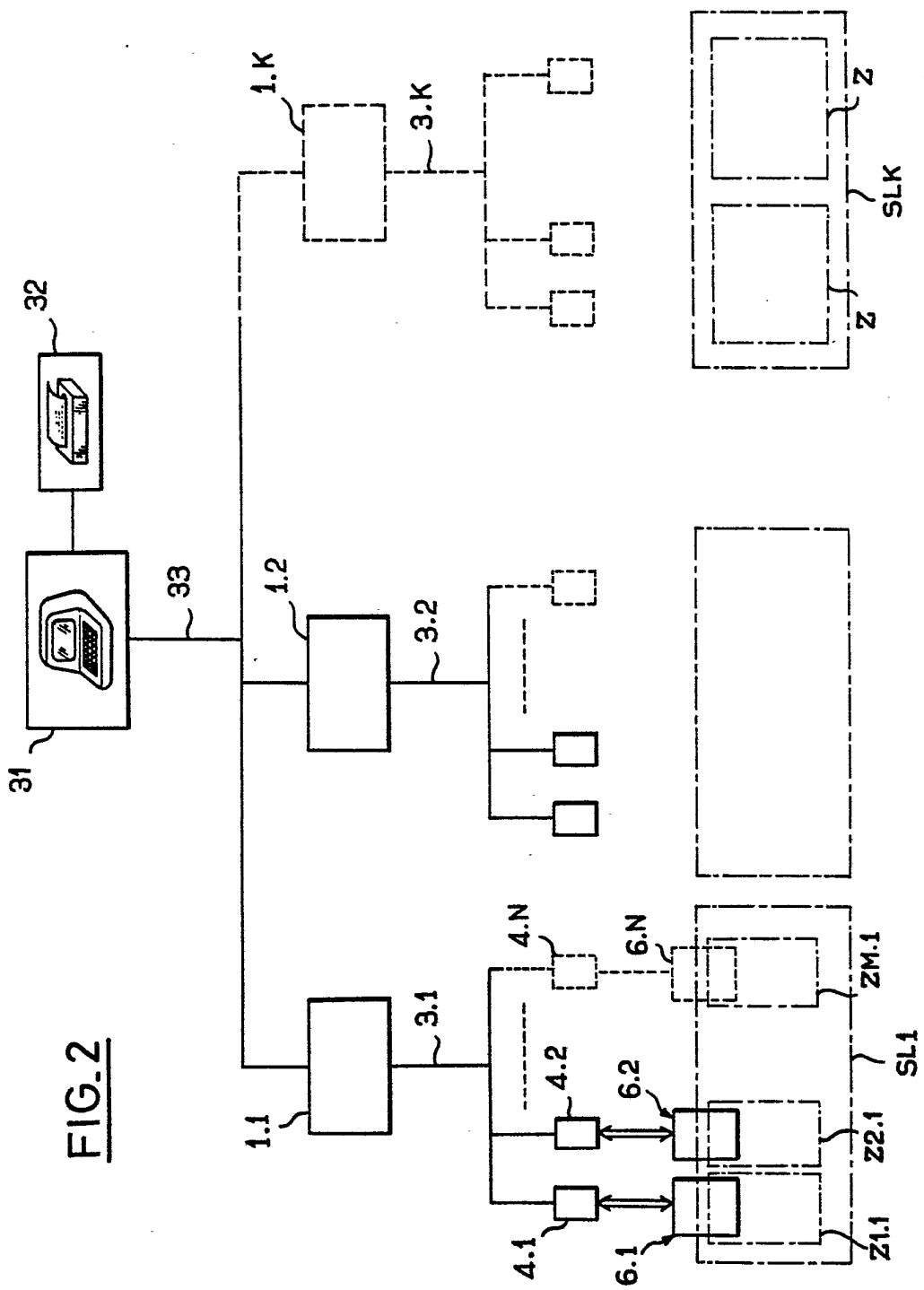


FIG.2

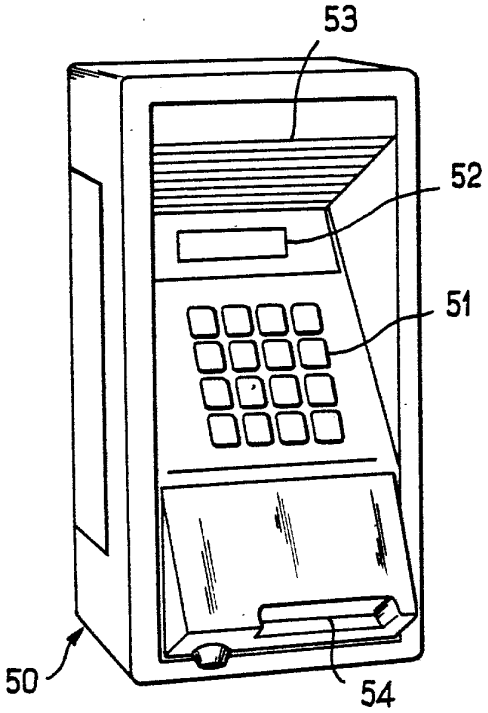


FIG.3a

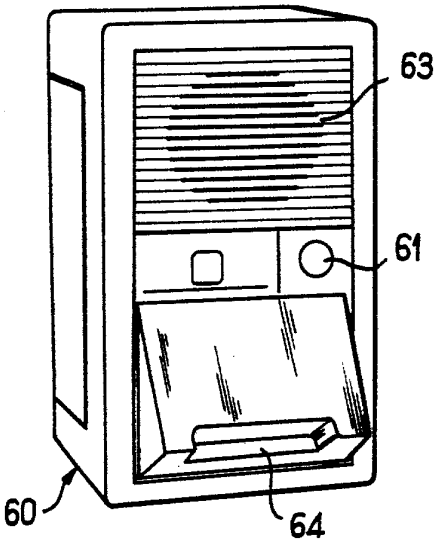


FIG.3b

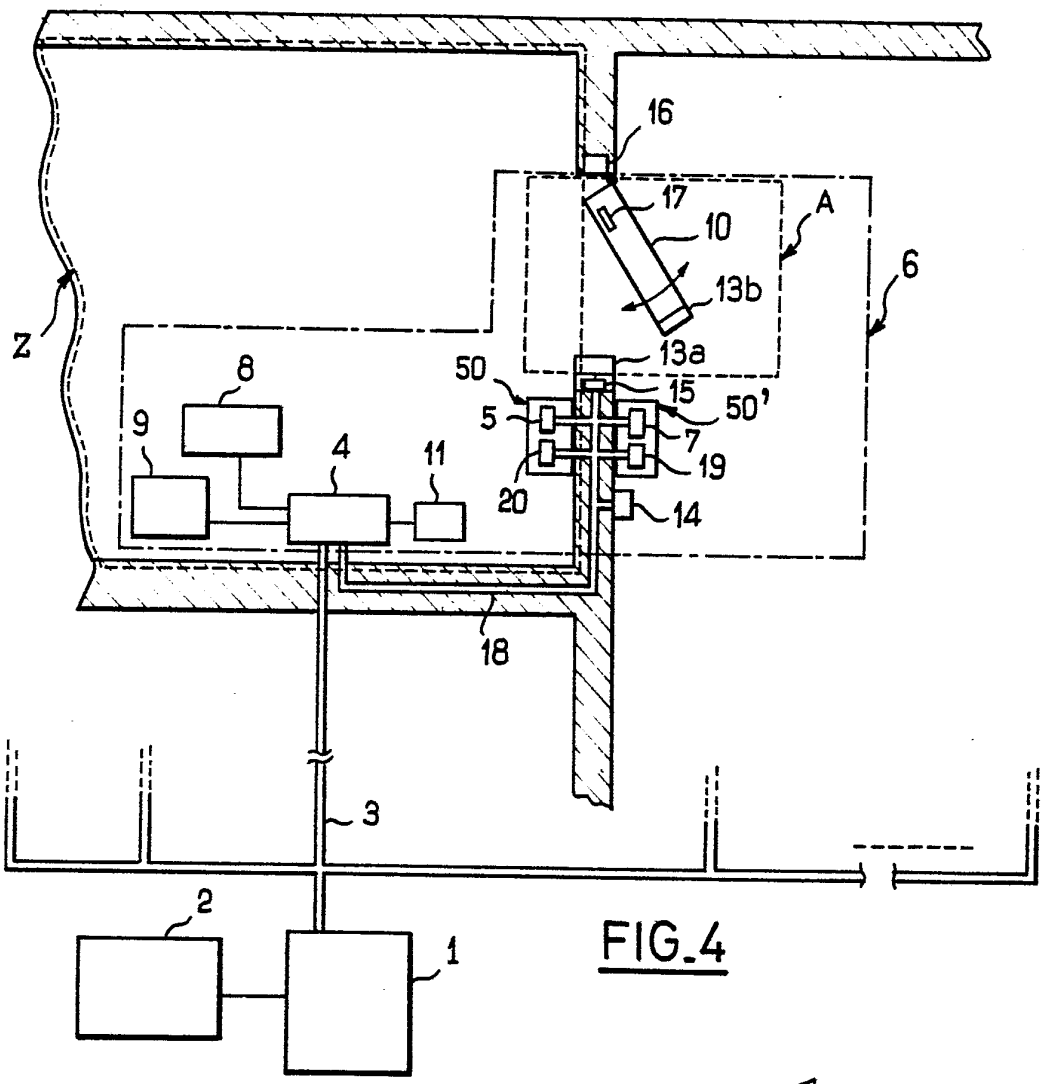


FIG.4

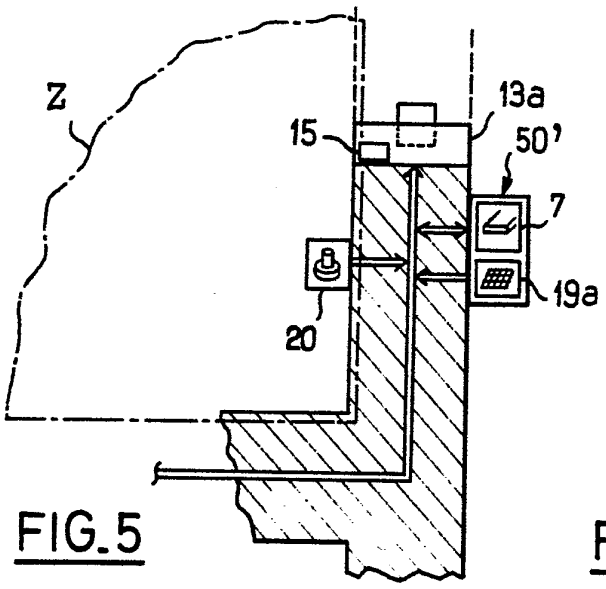


FIG.5

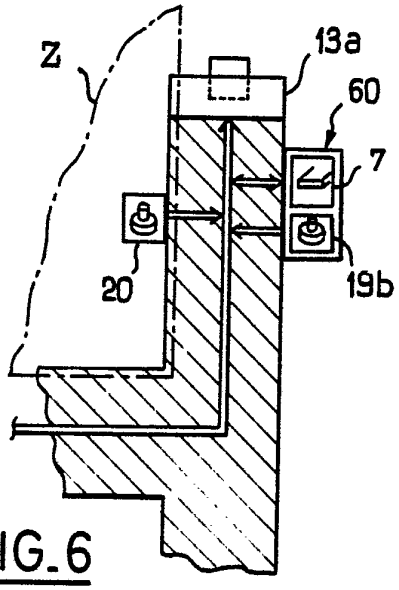
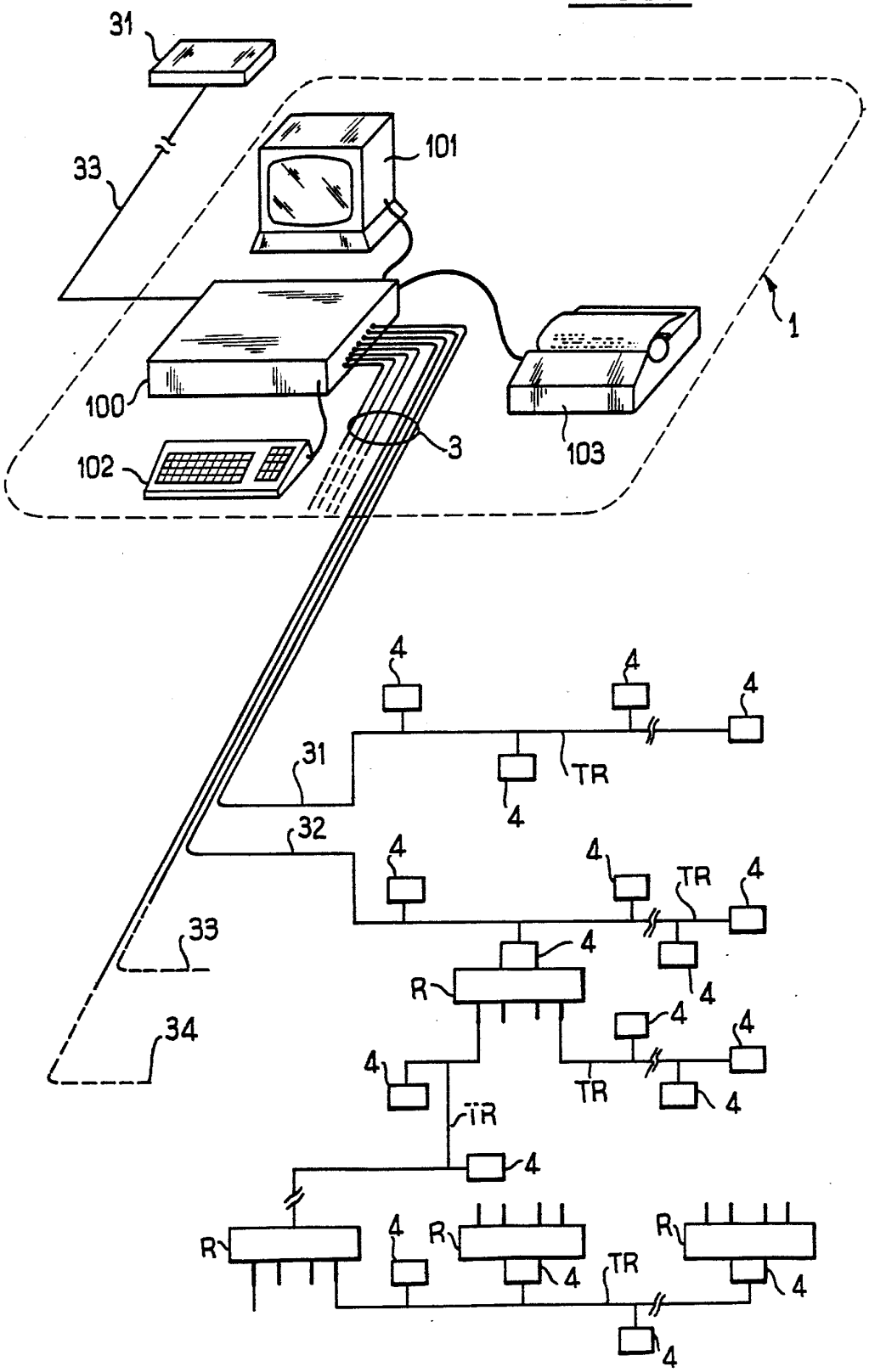


FIG.6

FIG_7



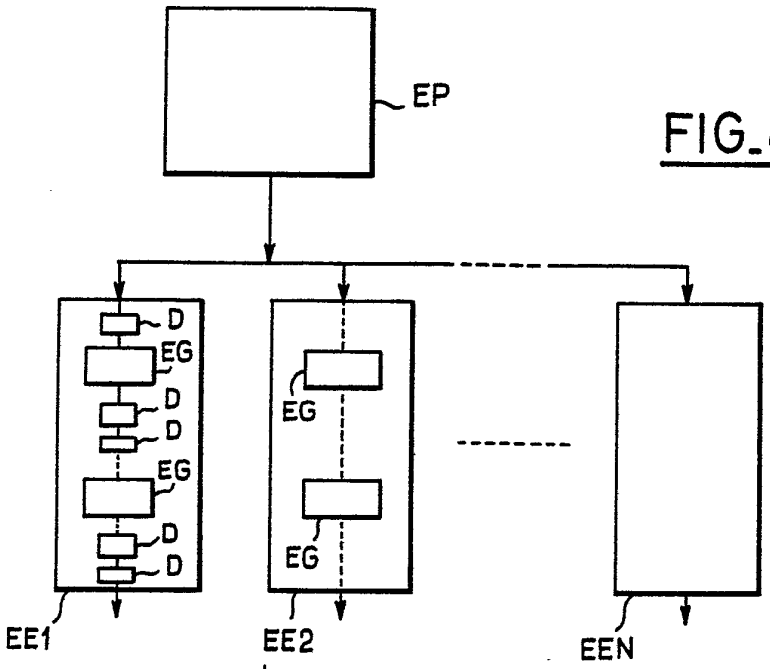


FIG_8

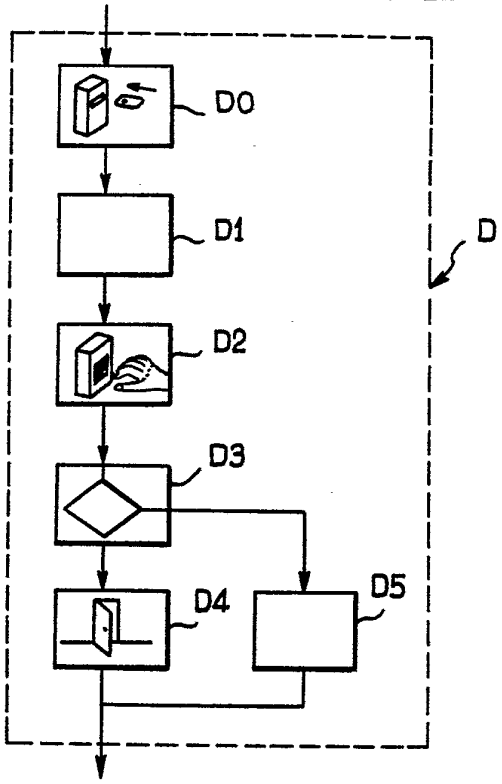


FIG_9

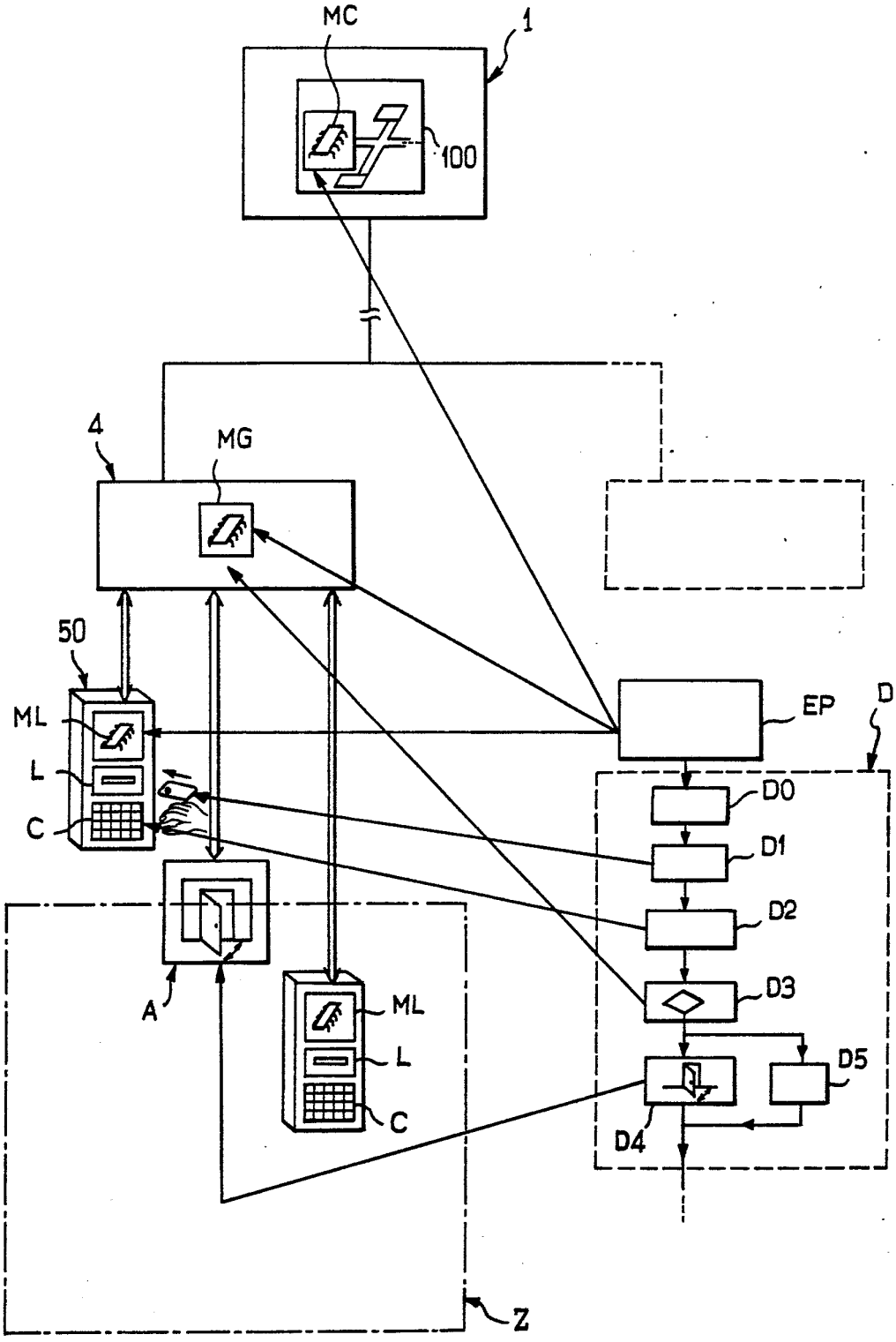


FIG.10

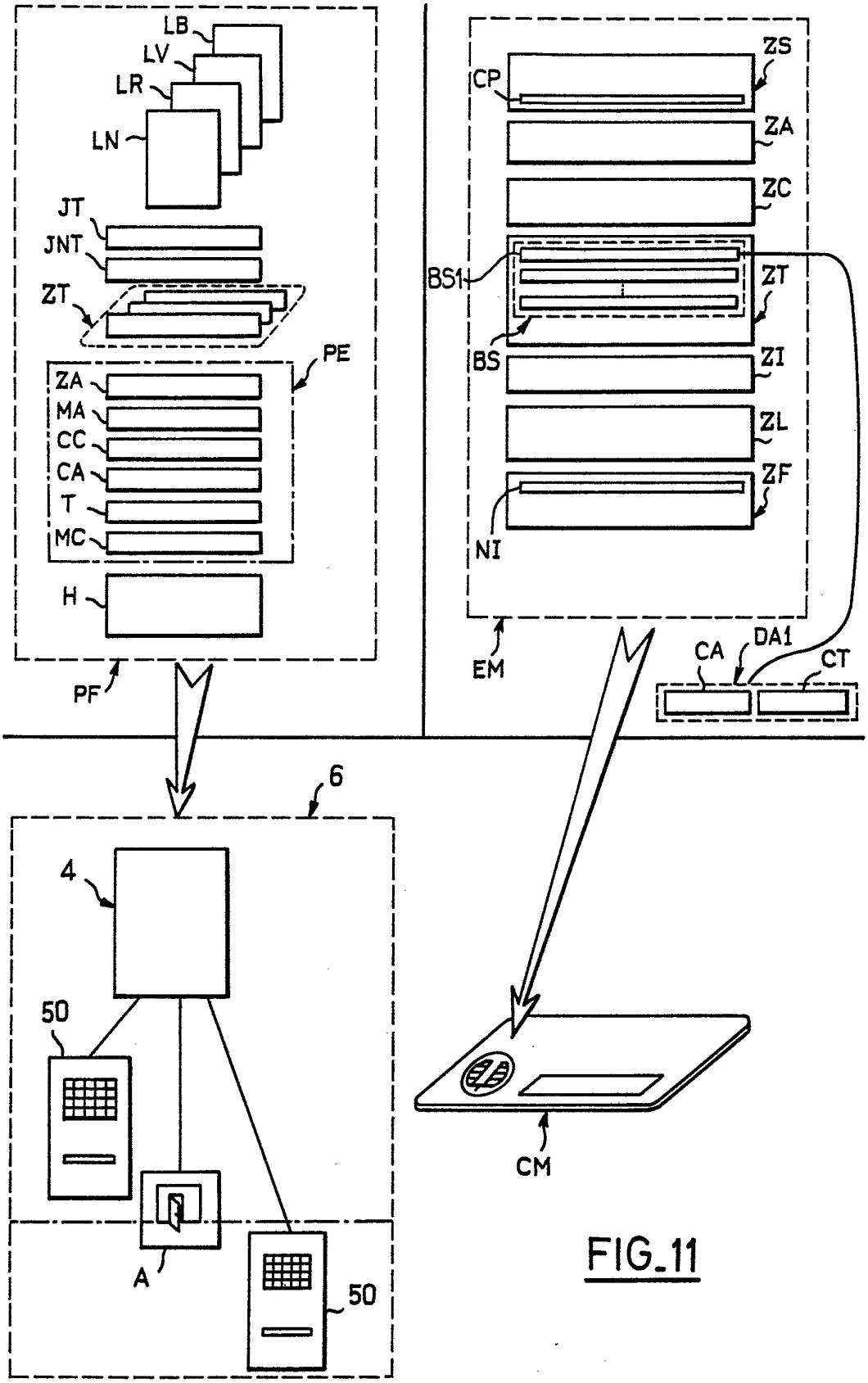

LB
LV
LR
LN
JT
JNT
ZT
PE
ZA
MA
CC
CA
T
MC
H
PF
ZS
CP
ZA
ZC
BS1
ZT
BS
ZI
ZL
ZF
NI
EM
CA
DA1
CT
6
4
50
A
50
CM

FIG_11