(19) RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL
DE LA PROPRIÉTÉ INDUSTRIELLE

PARIS

(11) N° de publication : **2 619 941**
(à n'utiliser que pour les commandes de reproduction)

(21) N° d'enregistrement national : **87 12084**

(51) Int Cl⁴ : G 06 F 13/00, 11/32; G 06 K 19/00.

(12) DEMANDE DE BREVET D'INVENTION A1

(22) Date de dépôt : 31 août 1987.

(30) Priorité :

(43) Date de la mise à disposition du public de la demande : BOPI « Brevets » n° 9 du 3 mars 1989.

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

(71) Demandeur(s) : *COMPAGNIE DE SIGNAUX ET D'EQUIPEMENTS ELECTRONIQUES, société anonyme.* — FR.

(72) Inventeur(s) : Claude Gautier ; Patrice Duchemin.

(73) Titulaire(s) :

(74) Mandataire(s) : Cabinet Malemont.

(54) Système de contrôle de la liaison entre deux terminaux d'une installation de traitement de données.

(57) Système de contrôle de la liaison entre deux terminaux 1, 4 d'une installation de traitement de données, par l'intermédiaire du réseau téléphonique commuté RTC, caractérisé en ce qu'il comprend en combinaison :

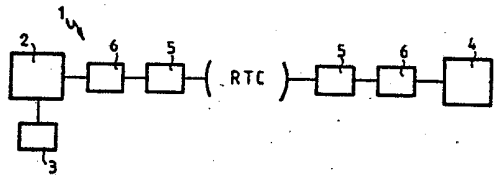
— une carte à microcircuit intelligente;

— un lecteur apte à recevoir ladite carte;

— un moyen 3 pour introduire dans le système un code confidentiel et une référence du terminal appelé 4 présentés par le porteur de la carte;

— ladite carte comportant, d'une part, des moyens pour reconnaître ce code confidentiel et autoriser, uniquement lorsque ledit code a effectivement été reconnu, l'établissement de la liaison téléphonique avec le système de contrôle 6 du terminal appelé 4, et d'autre part, un algorithme et une clé secrète permettant au système de contrôle 6 du terminal appelant 1 d'authentifier le système de contrôle 6 du terminal appelé 4, et réciproquement; et,

— des moyens pour autoriser, à l'issue de cette phase d'authentification, l'établissement de la liaison téléphonique entre les deux terminaux pour l'échange de données.



FR 2 619 941 - A1

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

Système de contrôle de la liaison entre deux terminaux d'une installation de traitement de données

La présente invention concerne un système pour contrôler la liaison entre deux terminaux d'une installation de traitement de données, par l'intermédiaire du réseau téléphonique commuté.

Il existe à l'heure actuelle de nombreux systèmes de contrôle destinés à empêcher qu'une personne non autorisée puisse avoir accès, par l'intermédiaire du réseau téléphonique commuté, à un système informatique contenant des informations considérées comme confidentielles.

Toutefois, les systèmes de contrôle connus jusqu'à maintenant n'offrent généralement pas une sécurité suffisante et malgré toutes les précautions prises, on a de multiples exemples de piratage informatique.

La présente invention a donc pour but principal de remédier à cet inconvénient et, pour ce faire, elle a pour objet un système de contrôle qui se caractérise essentiellement en ce qu'il comprend, en combinaison :

- une carte à microcircuit intelligente ;
- un lecteur apte à recevoir ladite carte ;
- un moyen pour introduire dans le système un code confidentiel et une référence du terminal appelé présentés par le porteur de la carte ;
- ladite carte comportant, d'une part des moyens pour reconnaître ce code confidentiel et autoriser, uniquement lorsque ledit code a effectivement été reconnu, l'établissement de la liaison téléphonique avec le système de contrôle du terminal appelé, et d'autre part un algorithme et une clé secrète permettant au système de contrôle du terminal appelant d'authentifier le système de contrôle du terminal appelé, et réciproquement ; et,
- des moyens pour autoriser, à l'issue de cette phase d'authentification, l'établissement de la liaison téléphonique entre les deux terminaux pour l'échange des données.

Grâce à cet ensemble de dispositions, la sécurité est assurée dans d'excellentes conditions et il est pratiquement impossible pour une personne non autorisée d'avoir accès aux terminaux ainsi équipés.

Dans un mode de réalisation particulier de l'invention, la carte à microcircuit intelligente comporte une liste de références des terminaux appelés autorisés, des moyens étant prévus pour n'autoriser la liaison téléphonique avec le système de contrôle du terminal appelé que lorsque la référence de ce terminal figure dans ladite liste.

Ainsi, chaque carte peut ne donner accès qu'à un nombre limité de terminaux équipés, selon le degré d'habilitation du porteur de la carte.

De préférence, le système de contrôle est intégré au terminal. De plus, il comprend un moyen de mémorisation secouru pour stocker des éléments secrets tels que des clés de chiffrement, ce moyen de mémorisation s'effaçant automatiquement en cas de tentative d'intrusion par ouverture du coffret renfermant le système de contrôle.

Dans une configuration de sécurité supérieure, le circuit électronique du système est protégé par une enveloppe externe formée de deux demi-capots rigides comportant sur leur paroi intérieure un circuit imprimé souple double face dont la surface est parcourue par une piste conductrice continue, formant un fin treillis, dans laquelle circule un courant, toute tentative d'intrusion par perçage ou découpage du capot se traduisant par une rupture de la piste et provoquant alors automatiquement l'effacement du moyen de mémorisation secouru.

Avantageusement, des moyens sont prévus pour réaliser le chiffrement des données échangées entre les deux terminaux, à l'aide d'un algorithme résidant en mémoire programme et d'une clé secrète contenue dans une zone protégée de la carte à microcircuit intelligente présente sur chaque terminal.

De plus, des moyens sont prévus pour réaliser une signature des informations transportées, cette signature permettant, d'une part d'en garantir l'intégrité durant la transmission contre toute tentative de modification ou d'insertion, et d'autre part d'en valider l'origine.

Une forme d'exécution de l'invention est décrite ci-après à titre d'exemple, en référence aux dessins annexés dans lesquels :

la figure 1 illustre de manière schématique la fonction du système de contrôle selon l'invention ;

- la figure 2 est un schéma synoptique simplifié du module de sécurité constituant l'élément essentiel du système de contrôle ;

- la figure 3 est un schéma synoptique plus détaillé de ce module de sécurité ; et

- les figures 4 et 5 représentent un mode de réalisation du coffret anti-intrusion du module de sécurité.

Le système de contrôle conforme à l'invention a pour but de contrôler avec un certain niveau de sécurité la liaison entre deux terminaux d'une installation de traitement de données, par l'intermédiaire du réseau téléphonique commuté. En se référant tout d'abord à la figure 1, on peut voir à une extrémité

un terminal 1, constitué par exemple d'un écran 2 associé à un clavier 3, et à l'autre extrémité un ordinateur hôte ou serveur 4 qui pourrait éventuellement être constitué aussi par un simple terminal. Le terminal 1 et l'ordinateur 4 sont, de façon connue en soi, reliés chacun au réseau téléphonique commuté RTC par l'intermédiaire d'un dispositif d'accès ligne 5.

Conformément à la présente invention, un module de sécurité 6 est intercalé à chaque extrémité entre le dispositif d'accès ligne 5 et l'équipement de saisie et/ou traitement de l'information correspondant 1 et 4. Ce module a pour but de garantir la sécurité de la liaison entre les deux équipements, en association avec une carte à microcircuit intelligente dont doit être détenteur l'utilisateur du terminal. La fonction sécurité est mise en oeuvre à l'établissement de la liaison et également durant la phase de transfert des données en liaison établie.

Ainsi qu'on peut le voir sur la figure 2, le module de sécurité 6 se compose essentiellement d'une carte électronique 7, contenue dans un coffret 8 et comportant un processeur de sécurité et de communication 9 qui gère, par l'intermédiaire d'un bus 10, des ressources privées propres à la sécurité, à savoir :

- un système d'identification/authentification 11 ;
- un moyen de mémorisation secouru effaçable 12 ; et
- un dispositif de protection contre l'intrusion 13.

On va maintenant décrire plus en détail ce module de sécurité, en se référant à la figure 3.

Le processeur de sécurité 9 constitue le coeur du module, puisqu'il gère l'ensemble des ressources de la carte électronique 7. Il se compose d'un microprocesseur 14, d'une mémoire morte 15 contenant le logiciel résident, d'une mémoire vive de travail 16, d'une horloge en temps réel secourue 17 assurant notamment la fonction horodateur, de circuits programmables d'entrée/sortie série et parallèle 18, 19, et de circuits de contrôle et décodage à usage général 20.

Le système d'identification/authentification 11 constitue la clé de voûte du dispositif de protection. Il permet l'exploitation d'une carte à microcircuit intelligente figurée en 21 et contenant des informations, des clés et des algorithmes secrets pour effectuer l'identification du porteur de la carte, la validation du point d'accès appelé et la reconnaisance mutuelle des deux modules

de sécurité 6 situés à chaque extrémité de la ligne, lors d'une phase d'authentification. Ce système se compose essentiellement des éléments suivants:

- une alimentation à découpage programmable 22 ;
- une logique de contrôle 23 ; et
- un dispositif d'insertion 24 de la carte à microcircuit 21.

Le dispositif d'insertion 24 permet le maintien de la carte à microcircuit 21 et l'établissement des contacts mécaniques et électriques avec le microcircuit de la carte permettant d'établir la liaison avec la logique de contrôle 23 par l'intermédiaire du câble 25 prévu à cet effet.

L'alimentation programmable 22 est utilisée pour générer la tension nécessaire pour inscrire des informations dans le microcircuit de la carte 21. La logique de contrôle 23 permet de générer un signal d'activation de la carte 21 et de transmettre des données sérielles sur la liaison 25. Le logiciel d'application et le logiciel de base nécessaires à la mise en oeuvre des fonctions de dialogue avec le microcircuit situé sur la carte 21 résident dans la mémoire morte 15.

Le moyen de mémorisation secouru effaçable 12 est essentiellement constitué d'une mémoire vive 26 alimentée par une alimentation de secours 27 au travers d'un dispositif de commutation 28. Quant au dispositif de protection contre l'intrusion 13, il est essentiellement constitué d'un dispositif de détection d'intrusion 29 relié au dispositif de commutation 28. Ce dispositif de détection peut, dans les cas les plus simples, se réduire à un microinterrupteur permettant de détecter l'ouverture du coffret 8 renfermant la carte électronique 7. Si une ouverture inopinée du coffret est détectée, le dispositif de commutation 28 coupe l'alimentation de la mémoire vive 26, provoquant ainsi l'effacement des éléments secrets qui s'y trouvent, tels que clés, algorithmes, listes, etc...

Bien entendu, il est possible d'intégrer directement la carte électronique 7 du module de sécurité 6 dans le terminal 1. Dans ce cas, la protection contre l'intrusion pourra faire intervenir un dispositif de protection au niveau de l'équipement d'accueil.

Pour un niveau de sécurité supérieur, le coffret peut être réalisé de la manière représentée sur les figures 4 et 5. Dans cette réalisation, l'enveloppe servant de coffret comprend tout d'abord deux demi-capots 30 moulés en une matière plastique rigide, enserrant la carte électronique 7. A l'intérieur de chacun de ces demi-capots 30 est disposé un circuit imprimé souple double face

31 dont la surface est parcourue par une piste conductrice continue de cuivre 32 formant un fin treillis. Un courant circule en permanence dans cette piste continue 32. Ainsi, toute tentative d'intrusion par perçage ou découpage du capot 30 se traduit immédiatement par une rupture de la piste 32 qui peut être facilement détectée au moyen d'un dispositif électronique approprié. L'effacement de la mémoire 26 est alors déclenché automatiquement, afin que les informations qui y étaient contenues ne soient pas compromises. Il va de soi par ailleurs qu'une telle enveloppe de protection peut également être incorporée à l'équipement d'accueil, dans le cas où le module de sécurité y est intégré.

On va maintenant décrire de manière succincte le fonctionnement global du système de contrôle selon l'invention dans une liaison terminal/serveur à travers le réseau téléphonique commuté.

Au départ, l'utilisateur introduit sa carte à microcircuit personnalisée 21 dans le dispositif d'insertion 24 et introduit ses paramètres d'identification (nom, prénom, code confidentiel) sur le clavier 3 de la console 2 du terminal 1. Ces informations sont transmises directement au module de sécurité 6 correspondant qui les compare à celles se trouvant sur la carte à microcircuit 21. En cas de divergence, le module de sécurité refuse de poursuivre la procédure d'accès et signale sur l'écran de la console 2 que l'identification doit être réitérée. Trois tentatives sont autorisées, à l'issue desquelles la carte à microcircuit de l'utilisateur se verrouille, ce qui la rend inutilisable.

Si la phase d'identification de l'utilisateur s'est achevée avec succès, celui-ci est invité à fournir la référence de l'équipement serveur appelé. Un contrôle de validité de la référence présentée est alors effectué et si celle-ci ne figure pas dans la liste de références autorisées se trouvant sur la carte à microcircuit 21, la demande est rejetée.

En cas de contrôle positif, l'établissement de la connexion et de la liaison entre les deux modules de sécurité 6 s'effectue de façon automatique sans intervention de l'utilisateur par l'intermédiaire des dispositifs d'accès à ligne 5, dans la mesure où ces derniers peuvent être commandés directement par les modules de sécurité.

Une phase de dialogue entre les deux modules de sécurité se déroule alors de la façon suivante :

Le module de sécurité appelant génère un pseudoaléa al constitué d'une séquence binaire pseudo aléatoire de longueur l, et l'envoie au travers de la liaison.

Le module de sécurité appelé, équipé lui aussi d'une carte à microcircuit, remet ce pseudoaléa à cette carte qui exécute un calcul algorithmique à l'aide d'un algorithme secret A et d'une clé secrète S.

La carte à microcircuit insérée dans le module de sécurité appelé retourne à celui-ci le résultat du calcul : $R = A(S,al)$.

Le module de sécurité appelé envoie ce résultat au module de sécurité appelant.

Le module de sécurité appelant remet à la carte à microcircuit qui y est insérée le même pseudoaléa al.

La carte à microcircuit effectue alors le même calcul algorithmique que précédemment à l'aide de son algorithme secret A' et de sa clé secrète et retourne au module de sécurité le résultat $R' = A'(S',al)$.

Le module de sécurité appelant compare R et R' ; si R égale R', il en déduit que les couples (A, S) et (A', S') sont identiques, ce qui signifie que les cartes à microcircuit présentes sur chacun des modules de sécurité partagent le même secret et appartiennent donc au même domaine de sécurité. Cette authentification est ensuite exécutée de la même façon par le module de sécurité appelé.

A l'issue de cette authentification mutuelle, les modules de sécurité basculent en "mode transparent" de sorte que les équipements de traitement et saisie d'informations d'extrémité puissent échanger des données sans voir la présence des modules de sécurité, dans la phase transfert de données.

Moyennant la mise en place en mémoire morte 15 d'un logiciel adapté, deux fonctions complémentaires existent.

La première est le chiffrement logiciel par bloc de données. Cette fonction est mise en oeuvre lors de la phase de transfert des données et permet de garantir la confidentialité des données échangées. L'algorithme de chiffrement réside en mémoire programme, tandis que la clé secrète est contenue dans une zone protégée de la carte à microcircuit présente à chaque extrémité, ou dans le moyen de mémorisation secouru effaçable (12).

La seconde fonction est la certification des messages. Cette fonction est également mise en oeuvre lors de la phase de transfert des données. Elle consiste à constituer des blocs de données et à y adjoindre un certificat

calculé après compression, à l'aide d'un algorithme et d'une clé secrète contenus dans le module de sécurité. La certification ou signature des messages permet d'assurer qu'il n'y a ni perte, ni ajout, ni duplication ou falsification du message, et permet également d'en garantir l'origine.

REVENDICATIONS

1. Système de contrôle de la liaison entre deux terminaux (1, 4) d'une installation de traitement de données, par l'intermédiaire du réseau téléphonique commuté (RTC), caractérisé en ce qu'il comprend en combinaison :

- une carte à microcircuit intelligente (21) ;
- un lecteur (24) apte à recevoir ladite carte ;
- un moyen (3) pour introduire dans le système un code confidentiel et une référence du terminal appelé (4) présentés par le porteur de la carte (21);
- ladite carte comportant, d'une part des moyens pour reconnaître ce code confidentiel et autoriser, uniquement lorsque ledit code a effectivement été reconnu, l'établissement de la liaison téléphonique avec le système de contrôle (6) du terminal appelé (4), et d'autre part un algorithme et une clé secrète permettant au système de contrôle (6) du terminal appelant (1) d'authentifier le système de contrôle (6) du terminal appelé(4), et réciproquement ; et,
- des moyens (18) pour autoriser, à l'issue de cette phase d'authentification, l'établissement de la liaison téléphonique entre les deux terminaux pour l'échange des données.

2. Système de contrôle selon la revendication 1, caractérisé en ce que la carte à microcircuit intelligente (21) comporte une liste de références des terminaux appelés autorisés, des moyens (18, 19) étant prévus pour n'autoriser la liaison téléphonique avec le système de contrôle du terminal appelé que lorsque la référence de ce terminal figure dans ladite liste.

3. Système de contrôle selon la revendication 1 ou 2, caractérisé en ce qu'il est intégré au terminal.

4. Système de contrôle selon l'une quelconque des revendications 1 à 3, caractérisé en ce qu'il comprend un moyen de mémorisation secouru (12) pour stocker des éléments secrets tels que des clés de chiffrement, ce moyen de mémorisation s'effaçant automatiquement en cas de tentative d'intrusion par ouverture du coffret (8) renfermant le système de contrôle.

5. Système de contrôle selon la revendication 4, caractérisé en ce que le circuit électronique (7) du système est protégé par une enveloppe externe formée de deux demi-capots rigides (30) comportant sur leur paroi intérieure un circuit imprimé souple double face (31) dont la surface est parcourue par une piste conductrice continue (32), formant un fin treillis, dans laquelle circule un courant, toute tentative d'intrusion par perçage ou découpage du capot se

traduisant par une rupture de la piste et provoquant alors automatiquement l'effacement du moyen de mémorisation secouru (12).

6. Système de contrôle selon la revendication 4 ou 5, caractérisé en ce qu'il comprend des moyens pour réaliser le chiffrement des données échangées entre les deux terminaux, à l'aide d'un algorithme résidant en mémoire programme et d'une clé secrète contenue dans une zone protégée de la carte à microcircuit intelligente (21) présente sur chaque terminal (1, 4), ou dans le moyen de mémorisation secouru effaçable (12).

7. Système de contrôle selon l'une quelconque des revendications 4 à 6, caractérisé en ce qu'il comprend des moyens pour réaliser une signature des informations transportées, cette signature permettant, d'une part d'en garantir l'intégrité durant la transmission contre toute tentative de modification ou d'insertion, et d'autre part d'en valider l'origine.

FIG.1

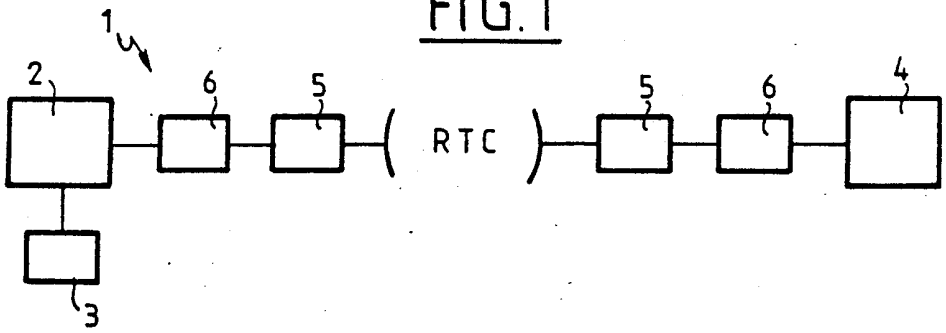


FIG.2

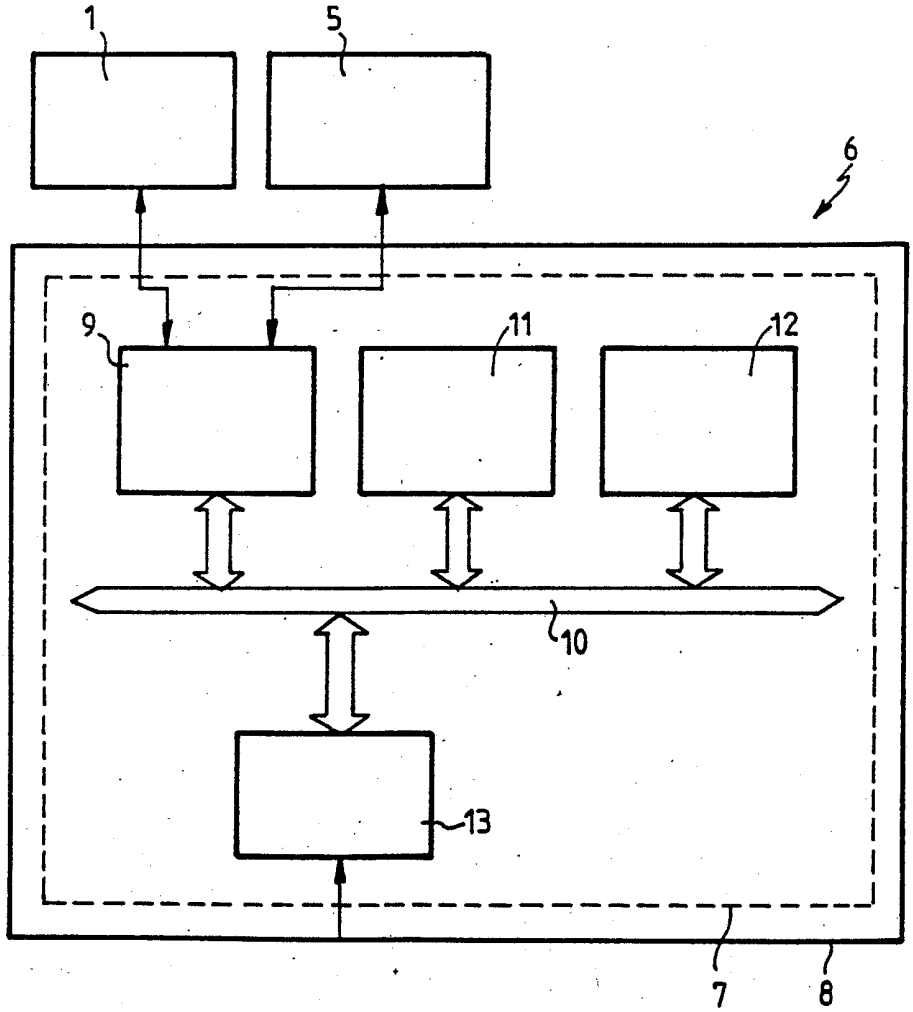


FIG. 3

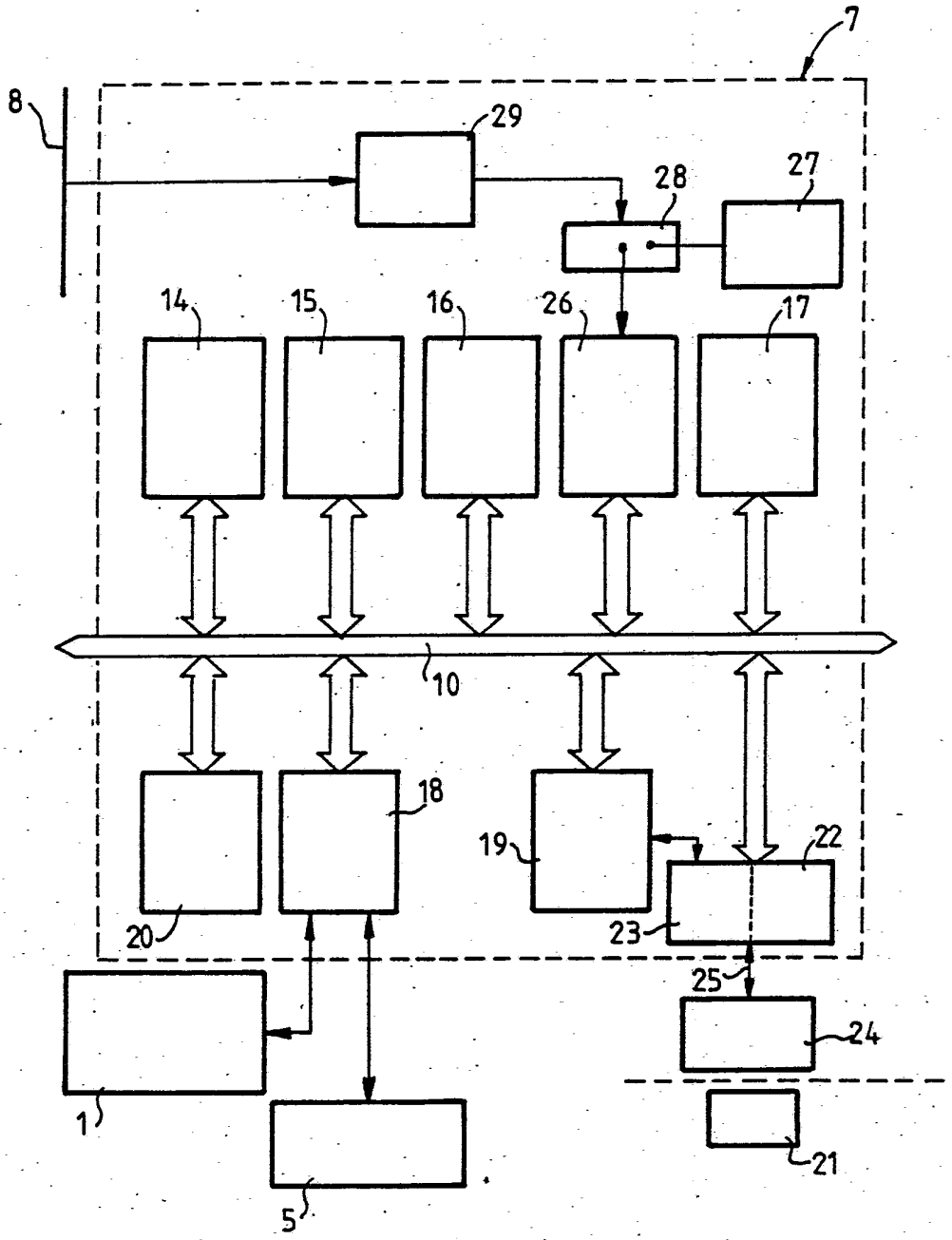


FIG. 4

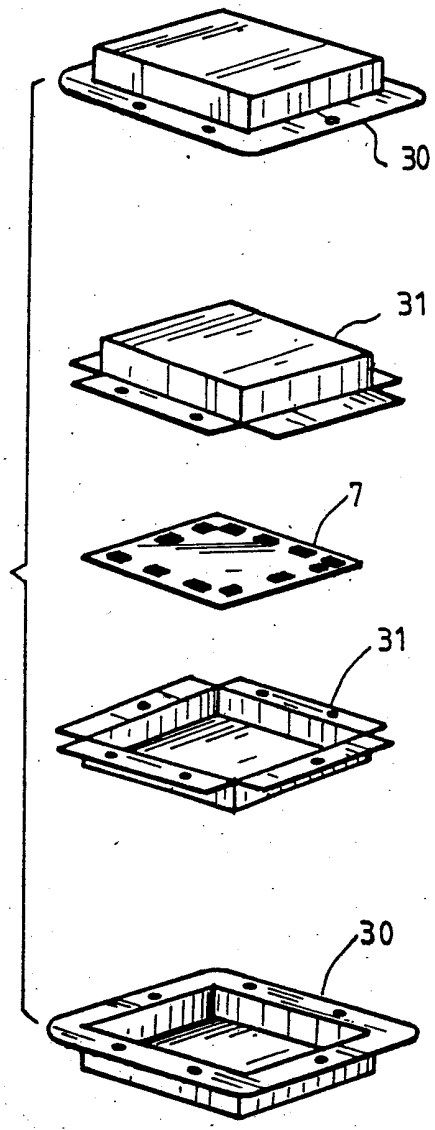


FIG.5

