

(19)



(11)

EP 1 561 192 B1

(12)

FASCICULE DE BREVET EUROPEEN

(45) Date de publication et mention
de la délivrance du brevet:
19.03.2014 Bulletin 2014/12

(51) Int Cl.:
G08C 19/28 (2006.01)

(21) Numéro de dépôt: **03769781.0**

(86) Numéro de dépôt international:
PCT/IB2003/005073

(22) Date de dépôt: **07.11.2003**

(87) Numéro de publication internationale:
WO 2004/044863 (27.05.2004 Gazette 2004/22)

(54) **PROCEDE DE SECURISATION DU MODE D ENREGISTREMENT D UN D ISPOSITIF
DOMOTIQUE**

VERFAHREN ZUR SICHERUNG DES REGISTRIERUNGSMODUS EINER
HAUSAUTOMATISIERUNGSVORRICHTUNG

METHOD FOR SECURING THE RECORDING MODE OF A HOME AUTOMATION DEVICE

(84) Etats contractants désignés:
**AT BE BG CH CY CZ DE DK EE ES FI FR GB GR
HU IE IT LI LU MC NL PT RO SE SI SK TR**

(30) Priorité: **12.11.2002 FR 0214093**

(43) Date de publication de la demande:
10.08.2005 Bulletin 2005/32

(73) Titulaire: **Somfy SAS
74300 Cluses (FR)**

(72) Inventeur: **BEJEAN, Alain
F-74450 Grussy (FR)**

(74) Mandataire: **Bugnion Genève
Bugnion S.A.
Conseils en Propriété Industrielle
Route de Florissant 10
Case Postale 375
1211 Genève 12 (CH)**

(56) Documents cités:
FR-A- 2 727 553

EP 1 561 192 B1

Il est rappelé que: Dans un délai de neuf mois à compter de la publication de la mention de la délivrance du brevet européen au Bulletin européen des brevets, toute personne peut faire opposition à ce brevet auprès de l'Office européen des brevets, conformément au règlement d'exécution. L'opposition n'est réputée formée qu'après le paiement de la taxe d'opposition. (Art. 99(1) Convention sur le brevet européen).

Description

[0001] L'invention concerne un procédé de sécurisation selon la revendication 1. L'invention se rapporte encore à un dispositif destiné à mettre en oeuvre le procédé selon l'invention.

[0002] Par émetteur d'ordres, on entend tout élément susceptible d'émettre un ordre par tout moyen et notamment en utilisant un signal électromagnétique, par exemple de type radiofréquence ou infrarouge, ou en utilisant un signal électrique.

[0003] Dans les dispositifs permettant le pilotage d'éléments de confort et/ou de sécurité, lorsque les émetteurs d'ordres et les récepteurs d'ordres communiquent à distance, il est nécessaire d'appairer ceux-ci. Cet appariement est réalisé par la mise en oeuvre d'une procédure d'identification et d'enregistrement des émetteurs, qui seront associés aux récepteurs pour permettre la commande à distance des actionneurs associés aux récepteurs.

[0004] Une telle procédure est décrite dans le brevet EP 0 867 848. Le dispositif permettant la mise en oeuvre de cette procédure comprend deux émetteurs possédant chacun un numéro d'identité et émettant un signal comprenant ce numéro et un ordre. Le dispositif comprend encore un récepteur muni d'une unité logique présentant un microprocesseur et une mémoire. Le microprocesseur est susceptible de fonctionner selon deux modes. Un premier dans lequel il permet l'exécution des ordres reçus et un deuxième dans lequel il permet l'enregistrement des numéros d'identité des émetteurs. On connaît également une autre procédure du document FR 2 727 553.

[0005] Un moyen de mise en mode d'enregistrement tel qu'un bouton-poussoir situé sur le récepteur peut agir directement sur le microprocesseur. Ce moyen de mise en mode d'enregistrement du microprocesseur peut également être associé à un émetteur, de telle sorte qu'au moyen de cet émetteur, il est possible de mettre le microprocesseur en mode d'enregistrement et d'enregistrer le numéro d'identité d'au moins un autre émetteur. Dans le cas d'un émetteur sans fil, le numéro d'identité de cet émetteur doit être connu du microprocesseur pour pouvoir activer la mise en mode d'enregistrement. La mise en mémoire du numéro d'identité de l'émetteur comprenant le moyen de mise en mode d'enregistrement peut être effectuée préalablement à l'installation, en usine par exemple. Cette mise en mémoire (ou appariement) peut également intervenir au moment de l'installation par l'activation d'une fonction de mise en mode d'enregistrement du microprocesseur au niveau du récepteur comme décrit précédemment. Cette fonction n'est plus nécessairement accessible une fois le dispositif complètement installé.

[0006] Dans le cas où le moyen de mise en mode d'enregistrement est uniquement accessible sur un émetteur, des problèmes se posent lors de la perte ou du vol de cet émetteur. D'une part, il n'est plus possible d'associer

ou de supprimer des émetteurs au dispositif et, d'autre part, dans le cas d'un vol, le dispositif n'est plus sécurisé.

[0007] Une solution simple permettant de résoudre ces problèmes est décrite dans le brevet EP 0 921 507. Elle consiste à commander la mise en mode d'enregistrement par une action spécifique sur l'alimentation secteur, par exemple une double coupure de courant dans un intervalle de temps réduit.

[0008] Il s'avère que cette solution permettant de faciliter l'appariement entre émetteurs et récepteurs présente un manque de sécurisation de l'accès à la mémoire des récepteurs.

[0009] En effet, si on prend l'exemple d'un portail ou d'un garage, éloigné du bâtiment principal et dont la porte est commandée par un système de commande à distance, il existe des accès non sécurisés à l'alimentation secteur, entre le portail ou le garage et le bâtiment principal. Ces accès peuvent être utilisés pour agir de manière frauduleuse sur l'alimentation secteur, de manière à mettre le récepteur du système de commande à distance en mode d'enregistrement et appairer un nouvel émetteur.

[0010] Un autre cas d'accès non sécurisé est le suivant : on trouve des interrupteurs situés au niveau du récepteur, notamment dans les systèmes d'actionneurs de portes de garage. Une action sur cet interrupteur active le mode d'enregistrement du récepteur. Dans le cas d'une porte de garage laissée ouverte temporairement, l'accès à l'interrupteur est libre et celui-ci peut être utilisé à des fins frauduleuses pour l'appariement d'un nouvel émetteur.

[0011] Les procédés et moyens permettant le passage du dispositif en mode d'enregistrement selon l'art antérieur sont représentés aux figures 1 et 2.

[0012] A la figure 1, le récepteur d'ordres est initialisé lors de l'installation du dispositif. La phase d'initialisation comprend également les procédures d'appariement d'un ou plusieurs émetteurs au cours desquelles le récepteur reçoit le numéro d'identité du ou des émetteurs et les stocke en mémoire.

[0013] Pour mettre le récepteur en mode d'enregistrement, un utilisateur effectue, sur un émetteur déjà connu par le récepteur d'ordres, une action A1 de mise en mode d'enregistrement, par exemple par appui sur un bouton spécifique prévu sur cet émetteur. L'émetteur prépare et envoie un message de programmation contenant son numéro d'identité ID et un code de programmation permettant le passage du récepteur en mode d'enregistrement.

[0014] Lors de la réception du message provenant de l'émetteur d'ordres, le récepteur vérifie si le numéro d'identité ID reçu est en mémoire. Si tel est le cas, le récepteur d'ordres est prêt à recevoir des messages de commande de l'actionneur de la part de l'émetteur. Dans le cas où un code de programmation est reçu, le récepteur passe en mode d'enregistrement. Il est alors possible d'appairer de nouveaux émetteurs ou d'en supprimer. La sortie du mode d'enregistrement est consécutive, soit au déroulement d'une temporisation, soit à une nouvelle

commande de l'utilisateur.

[0015] Une autre procédure de mise en mode d'enregistrement du récepteur, connue de l'art antérieur, est représentée à la figure 2. Cette procédure est initiée par une action A2 de l'utilisateur sur un moyen de mise en mode d'enregistrement, associé directement au récepteur ou par une action spécifique sur l'alimentation secteur.

[0016] Du brevet JP 2001032587, on connaît une solution proposant d'utiliser des unités indépendantes pour reprogrammer le système gérant l'ouverture des portes d'un véhicule. Cette solution a pour but une sécurisation du système par rapport au vol des émetteurs, mais ne résout pas le problème de l'accès aux moyens fixes de mise en mode d'enregistrement dans les procédures d'appariement entre émetteurs et récepteurs.

[0017] Le but de l'invention est de fournir un procédé permettant de résoudre les problèmes précités et d'améliorer les procédés de l'art antérieur. En particulier, l'invention se propose de mettre en oeuvre un procédé permettant de sécuriser l'accès aux fonctions d'enregistrement des récepteurs d'ordres dans le cadre de dispositifs assurant la sécurité et/ou le confort d'un bâtiment. L'invention se propose encore de réaliser un dispositif permettant de mettre en oeuvre ce procédé.

[0018] Le procédé selon l'invention est caractérisé par la partie caractérisante de la revendication 1.

[0019] Différents modes d'exécution de ce procédé sont définis par les revendications dépendantes 2 à 7.

[0020] La revendication indépendante 8 définit un dispositif permettant la mise en oeuvre de ce procédé.

[0021] La revendication 9 définit un mode de réalisation du dispositif selon l'invention.

[0022] On peut donc distinguer trois types d'émetteurs qui peuvent communiquer avec le récepteur d'ordres du dispositif :

- un émetteur simple de commande (montée/descente, ouverture/fermeture),
- un émetteur de programmation (commande et fonction d'activation du mode d'enregistrement du récepteur),
- un émetteur d'ordres sécurisé (commande optionnelle, fonctions d'activation du mode d'enregistrement et d'invalidation).

[0023] Les deux fonctions principales de l'émetteur d'ordres sécurisé sont donc la mise en mode d'enregistrement du récepteur et l'invalidation des fonctions d'activation du mode d'enregistrement. Ces fonctions principales sont activées soit par des actions différentes, soit par une action commune sur un ou plusieurs émetteurs présentant des moyens de mise en mode d'enregistrement et des moyens d'invalidation des fonctions d'activation.

[0024] De manière préférée, les émetteurs d'ordres sécurisés comportent des moyens sans fil de communication à distance avec le récepteur d'ordres.

[0025] Les émetteurs d'ordres sécurisés présentent de préférence deux dimensions sensiblement égales aux dimensions normalisées d'une feuille de papier afin de pouvoir être conservés facilement dans un endroit sûr tel qu'un coffre. Ils peuvent également être munis de moyens visuels tels que des étiquettes afin d'indiquer à l'utilisateur à quels dispositifs ils sont associés.

[0026] Le dispositif comporte un émetteur dont les fonctions sont la mise en mode d'enregistrement du dispositif et l'envoi d'un code de sécurisation et un récepteur tel que la réception du code de sécurisation provoque l'invalidation du ou des autres moyens de mise en mode d'enregistrement.

[0027] Le dispositif peut être utilisé de façon préventive. Une fois que les appariements souhaités entre émetteurs et récepteurs ont été effectués, on peut transmettre au récepteur, grâce à l'émetteur sécurisé, le code de sécurisation de manière à limiter ses possibilités de mise en mode d'enregistrement.

[0028] L'émetteur sécurisé ne comporte pas nécessairement de fonction de commande de l'actionneur. De cette manière, il peut consister en un émetteur simple, de moindre coût et plus facile à ranger dans un endroit sûr. Cependant, on peut prévoir un émetteur sécurisé associé à un émetteur plus évolué, qui pourrait être éventuellement fixé à l'intérieur de l'habitat.

[0029] L'émetteur sécurisé peut permettre une invalidation unique, c'est à dire une annulation irréversible du ou des moyens de mise en mode d'enregistrement. Il peut être prévu également sur l'émetteur sécurisé une fonction de réactivation des différents moyens de mise en mode d'enregistrement. Dans les deux cas, l'émetteur sécurisé peut être réutilisé pour la fonction d'activation du mode d'enregistrement du récepteur.

[0030] Il peut également être prévu une fonction d'effacement des numéros d'identité déjà enregistrés, par exemple par une manoeuvre spéciale sur l'émetteur sécurisé.

[0031] Le dessin annexé représente, à titre d'exemples, plusieurs modes d'exécution du procédé selon l'invention.

La figure 1 est un ordinogramme d'un procédé de mise en mode d'enregistrement selon l'art antérieur.

La figure 2 est un ordinogramme d'un autre procédé de mise en mode d'enregistrement selon l'art antérieur.

La figure 3 est un ordinogramme d'un premier mode d'exécution du procédé de sécurisation du mode d'enregistrement lors d'une première utilisation de l'émetteur d'ordres sécurisé.

Les figures 4a et 4b sont deux parties d'un ordinogramme d'un deuxième mode d'exécution du procédé de sécurisation du mode d'enregistrement lors d'une première utilisation de l'émetteur d'ordres sé-

curisé.

La figure 5 est un ordinogramme du premier mode d'exécution du procédé de sécurisation du mode d'enregistrement lors d'une utilisation ultérieure de l'émetteur d'ordres sécurisé.

La figure 6 est un schéma représentant un émetteur d'ordres et un récepteur d'ordres.

[0032] Le dispositif représenté à la figure 6 permet la mise en oeuvre du procédé selon l'invention. Il comprend un récepteur d'ordres 10 et un ensemble d'émetteurs d'ordres 20. Pour simplifier, un seul émetteur a été représenté à la figure 6.

[0033] Le récepteur d'ordres 10 comprend un module récepteur 12 raccordé, d'une part, à un dispositif de couplage 11 et, d'autre part, à une unité de traitement 13 de type microcontrôleur pilotant un équipement 14 tel qu'une porte, un volet roulant ou une installation d'alarme. Le récepteur d'ordre peut également comprendre une interface de commande 15 de type bouton-poussoir. Le récepteur d'ordres est relié à une alimentation secteur 17.

[0034] L'unité de traitement 13 comprend une zone de mémoire 16 destinée à contenir des programmes de fonctionnement du récepteur 10 et les numéros d'identité des émetteurs d'ordres 20 desquels le récepteur 10 est susceptible de recevoir des ordres.

[0035] Chaque émetteur d'ordres 20 comprend un module émetteur 22 raccordé, d'une part, à un dispositif de couplage 21 et, d'autre part, à une unité de traitement 23 de type microcontrôleur, et une interface de commande 24 de type clavier. Chaque émetteur d'ordres 20 contient son numéro d'identité dans une zone de mémoire 26 de l'unité de traitement 23.

[0036] Les émetteurs d'ordres sont susceptibles de transmettre des ordres par le biais d'ondes électromagnétiques, de type radio ou de type infrarouge ou encore par le biais de liaisons filaires.

[0037] Les communications entre émetteurs d'ordres et récepteurs d'ordres peuvent être bidirectionnelles. Dans ce cas, émetteurs et récepteurs sont munis de modules « émetteur-récepteur ».

[0038] Les émetteurs d'ordres, ou au moins certains d'entre eux, peuvent par une action ou une série d'actions de l'utilisateur faire passer le récepteur dans un mode d'enregistrement dans lequel il est possible de modifier la liste des émetteurs qui lui sont appariés par ajout ou par suppression de ceux-ci.

[0039] Parmi les émetteurs d'ordres, un émetteur particulier dit émetteur d'ordres sécurisé permet d'invalidiser certaines fonctions de mise en mode d'enregistrement du récepteur.

[0040] La figure 3 représente un premier mode d'exécution du procédé de fonctionnement du dispositif lors d'une première utilisation de l'émetteur d'ordres sécurisé.

[0041] La première action consiste à mettre le récepteur en mode d'enregistrement par une commande de type A1 (par un émetteur d'ordre) ou de type A2 (directement au niveau du récepteur ou sur l'alimentation secteur). L'utilisateur peut alors activer une commande de lancement de programme sécurisé A3 qui provoque l'envoi d'un message contenant le numéro d'identité ID de l'émetteur sécurisé BPS, pour l'apparier avec le récepteur, éventuellement un code de programmation et le code de programmation sécurisé.

[0042] Le récepteur reconnaît le numéro d'identité ID de l'émetteur.

[0043] La réception du code de programmation sécurisé provoque le lancement d'un programme de sécurisation associé et, par conséquent, l'invalidation des moyens de mise en mode d'enregistrement de type A1 et/ou de type A2.

[0044] Cette invalidation des moyens de mise en mode d'enregistrement peut consister en un changement d'état de mémoires binaires associées au récepteur et validant ou non les moyens de mise en mode d'enregistrement par les différents émetteurs.

[0045] Le récepteur peut alors activer un signal de fin de procédure signifiant à l'utilisateur que les moyens de mise en mode d'enregistrement ont été invalidés. Ce signal peut également être émis par l'émetteur d'ordres sécurisé après réception d'un message émis par le récepteur, dans le cas où la communication est bidirectionnelle.

[0046] Dans un tel mode d'exécution, les fonctions de mise en mode d'enregistrement et d'invalidation peuvent être soit communes à une même action sur l'émetteur d'ordres sécurisé, soit différenciées.

[0047] Dans le premier cas, la réception du code de programmation n'affecte pas le récepteur qui se trouve déjà en mode d'enregistrement. Eventuellement, dans le cas d'une fin de mode d'enregistrement consécutive au déroulement d'une temporisation, cette dernière peut être réinitialisée suite à la réception d'un code de programmation par le récepteur d'ordres.

[0048] Dans le deuxième cas, le code de programmation n'est pas envoyé par l'émetteur d'ordres sécurisé.

[0049] Les figures 4a et 4b représentent un deuxième mode d'exécution du procédé de fonctionnement du dispositif lors d'une première utilisation de l'émetteur d'ordres sécurisé, lorsque les fonctions d'identification de l'émetteur d'ordres sécurisé et la commande d'invalidation sont découplées. Dans ce cas, deux actions spécifiques doivent être effectuées sur l'émetteur d'ordres sécurisé par l'utilisateur. Ces deux actions peuvent être décalées dans le temps.

[0050] La figure 4a représente le procédé d'appariement de l'émetteur d'ordres sécurisé. Une première action A4, effectuée alors que le récepteur a été préalablement mis en mode d'enregistrement, permet d'apparier l'émetteur d'ordres sécurisé et le récepteur d'ordres. Elle provoque l'envoi uniquement du numéro d'identité ID de l'émetteur d'ordres sécurisé et sa réception et son stoc-

kage par le récepteur d'ordres.

[0051] La figure 4b représente le fonctionnement de l'émetteur d'ordres sécurisé une fois connu du récepteur. Une seconde action A5 provoque l'envoi d'un message contenant le numéro d'identité ID de l'émetteur d'ordres sécurisé, éventuellement un code de programmation et un code de programmation sécurisé. Le numéro d'identité de l'émetteur ayant été enregistré dans le récepteur lors de l'action précédente, celui-ci est reconnu par le récepteur et le code de programmation sécurisé est stocké en mémoire provoquant le lancement du programme de sécurisation associé à ce code. Les moyens de mise en mode d'enregistrement de type A1 et/ou de type A2 sont par conséquent invalidés.

[0052] Lorsque les fonctions de mise en mode d'enregistrement et d'invalidation sont communes à un type d'action sur l'émetteur d'ordres sécurisé, la réception des codes de programmation entraîne de façon sensible- ment simultanée la mise en mode d'enregistrement du récepteur et l'invalidation des fonctions d'activation du mode d'enregistrement.

[0053] De manière- générale, la fonction d'invalidation implique l'invalidation des fonctions d'activation du mode d'enregistrement, à l'exception de la fonction d'activation du mode d'enregistrement de l'émetteur d'ordres sécurisé.

[0054] Dans le cas où les deux fonctions de mise en mode d'enregistrement et d'invalidation doivent être activées par deux types d'actions différenciés, une action entraîne une mise en mode d'enregistrement du récepteur d'ordre, de la manière représentée sur la figure 1 et une action entraîne l'envoi du numéro d'identité ID de l'émetteur d'ordres sécurisé et du code de programmation sécurisé uniquement. Ainsi, seule la fonction d'invalidation est activée.

[0055] Comme dans le mode d'exécution précédent, le récepteur peut alors activer un signal de fin de procédure signifiant à l'utilisateur que les moyens de mise en mode d'enregistrement ont été invalidés. Ce signal peut également être émis par l'émetteur d'ordres sécurisé après réception d'un message émis par le récepteur, dans le cas où la communication est bidirectionnelle.

[0056] Il existe plusieurs cas pour lesquels l'émetteur d'ordres sécurisé est activé alors que son numéro d'identité ID est déjà connu du récepteur :

- Lors d'une première utilisation, dans le cas de la figure 4b, si l'émetteur d'ordres sécurisé a été apparié au récepteur d'ordres sans qu'il ne soit envoyé simultanément de code de programmation ou de code de programmation sécurisé,
- soit lors d'une utilisation ultérieure de l'émetteur d'ordres sécurisé, pour la mise en mode d'enregistrement du dispositif,
- soit s'il est prévu des moyens pour réactiver les moyens de mise en mode d'enregistrement origi- nels.

[0057] La figure 5 représente le procédé mis en oeuvre lorsque l'émetteur d'ordres est connu du récepteur, lors d'une utilisation ultérieure. Par une action A3 sur l'émetteur sécurisé, l'utilisateur provoque l'envoi d'un message contenant le numéro d'identité ID de l'émetteur d'ordres sécurisé, éventuellement le code de programmation, et le code de programmation sécurisé. Le récepteur reçoit ce message, reconnaît le numéro d'identité ID de l'émetteur d'ordres sécurisé et mémorise le code de programmation sécurisé.

[0058] Il est possible de prévoir un test de la validité des moyens de mise en mode d'enregistrement par exemple en testant l'état de mémoires binaires. Si les moyens de mise en mode d'enregistrement sont valides (test positif +), le récepteur les invalide avant d'enregistrer cette configuration. Il passe alors éventuellement en mode d'enregistrement. Si les moyens de mise en mode d'enregistrement sont déjà invalidés (test négatif -), le récepteur peut alors passer en mode d'enregistrement, de manière à pouvoir initier une procédure d'appariement.

[0059] Ce test est facultatif et évite uniquement de retransmettre un ordre d'invalidation vers des moyens de mise en mode d'enregistrement déjà invalidés, notamment dans le cas où une seule action sur l'émetteur d'ordre sécurisé entraîne à la fois la mise en mode d'enregistrement du récepteur et l'invalidation d'autres fonctions d'activation de ce mode d'enregistrement.

[0060] Bien entendu, dans tous les modes d'exécutions de l'invention, la transmission d'un numéro d'identité peut être remplacée par toute autre méthode d'identification, comme par exemple une méthode de Challenge.

[0061] De même, on peut aussi prévoir que le code de programmation sécurisé soit remplacé par une partie générique du numéro d'identité d'un émetteur d'ordres sécurisé, qui caractérise l'émetteur d'ordres sécurisé et la fonction d'invalidation associée.

Revendications

1. Procédé de sécurisation du mode d'enregistrement d'un dispositif comprenant un ensemble d'au moins un émetteur d'ordres (20), communiquant avec un récepteur d'ordres (10) capable de piloter un élément (14) assurant la sécurité et/ou le confort d'un bâtiment et susceptible d'être placé en mode d'enregistrement par une ou plusieurs fonctions d'activation, le mode d'enregistrement permettant d'enregistrer un émetteur d'ordres, **caractérisé en ce qu'une ou plusieurs actions dont l'une au moins est appliquée sur un émetteur d'ordres particulier de l'ensemble provoque l'invalidation d'au moins une fonction d'activation du mode d'enregistrement du récepteur d'ordres.**

2. Procédé de sécurisation selon la revendication 1,

caractérisé en ce que les actions sont menées de manière successive ou simultanée sur au moins un émetteur d'ordres particulier et sur au moins un autre émetteur d'ordres.

3. Procédé de sécurisation selon la revendication 1 ou 2, **caractérisé en ce que** la ou les actions sur l'émetteur d'ordres particulier activent le mode d'enregistrement du récepteur.
4. Procédé de sécurisation selon l'une des revendications 1 à 3, **caractérisé en ce que** la ou les actions sur l'émetteur d'ordres particulier invalident les fonctions d'activation du mode d'enregistrement à l'exception de celles des émetteurs d'ordres particuliers.
5. Procédé de sécurisation selon l'une des revendications précédentes, **caractérisé en ce que** l'invalidation de la fonction d'activation est irréversible.
6. Procédé de sécurisation selon l'une des revendications 1 à 4, **caractérisé en ce que** l'invalidation de la fonction d'activation est temporaire.
7. Procédé de sécurisation selon l'une des revendications précédentes, **caractérisé en ce qu'une** action sur un émetteur d'ordres particulier provoque, dans la mémoire du récepteur, l'effacement des numéros d'identité d'au moins certains émetteurs.
8. Dispositif destiné à mettre en oeuvre le procédé selon l'une des revendications 1 à 7, **caractérisé en ce qu'il** comprend au moins un émetteur d'ordres particulier, et éventuellement d'autres émetteurs d'ordres (20), communiquant avec un récepteur d'ordres (10) capable de piloter un élément (14) assurant la sécurité et/ou le confort d'un bâtiment.
9. Dispositif selon la revendication 8, **caractérisé en ce que** les émetteurs d'ordres particuliers comportent des moyens sans fil de communication à distance avec le récepteur d'ordres (10).

Patentansprüche

1. Sicherungsverfahren des Registrierungsmodus einer Vorrichtung, die eine Gruppe aus mindestens einem Befehlssenders (20) umfasst, der mit einem Befehlsempfänger (10) kommuniziert, der imstande ist, ein Element (14) zu steuern, das die Sicherheit und/oder den Komfort eines Gebäudes sicherstellt und anhand einer oder mehrerer Aktivierungsfunktionen in den Registrierungsmodus versetzbar ist, wobei der Registrierungsmodus erlaubt, einen Befehlssender zu registrieren, **dadurch gekennzeichnet, dass** eine oder mehrere Aktionen, von denen mindestens eine auf einen bestimmten Befehlssender

der der Gruppe angewendet wird, die Annullierung mindestens einer Aktivierungsfunktion des Registrierungsmodus des Befehlsempfängers bewirkt.

2. Sicherungsverfahren nach Anspruch 1, **dadurch gekennzeichnet, dass** die Aktionen aufeinanderfolgend oder gleichzeitig auf mindestens einen bestimmten Befehlssender und auf mindestens einen anderen Befehlssender durchgeführt werden.
3. Sicherungsverfahren nach Anspruch 1 oder 2, **dadurch gekennzeichnet, dass** die Aktion(en) auf den bestimmten Befehlssender den Registrierungsmodus des Empfängers aktivieren.
4. Sicherungsverfahren nach einem der Ansprüche 1 bis 3, **dadurch gekennzeichnet, dass** die Aktion(en) auf den bestimmten Befehlssender die Aktivierungsfunktionen des Registrierungsmodus annullieren, mit Ausnahme derjenigen der bestimmten Befehlssender.
5. Sicherungsverfahren nach einem der vorangehenden Ansprüche, **dadurch gekennzeichnet, dass** die Annullierung der Aktivierungsfunktion unumkehrbar ist.
6. Sicherungsverfahren nach einem der Ansprüche 1 bis 4, **dadurch gekennzeichnet, dass** die Annullierung der Aktivierungsfunktion zeitweilig ist.
7. Sicherungsverfahren nach einem der vorangehenden Ansprüche, **dadurch gekennzeichnet, dass** eine Aktion auf einen bestimmten Befehlssender im Speicher des Empfängers zur Löschung der Identitätsnummern mindestens bestimmter Sender führt.
8. Vorrichtung, die zur Umsetzung des Verfahrens nach einem der Ansprüche 1 bis 7 bestimmt ist, **dadurch gekennzeichnet, dass** sie mindestens einen bestimmten Befehlssenders und eventuell andere Befehlssender (20) umfasst, die mit einem Befehlsempfänger (10) kommunizieren, der imstande ist, ein Element (14) zu steuern, das die Sicherheit und/oder den Komfort eines Gebäudes sicherstellt.
9. Vorrichtung nach Anspruch 8, **dadurch gekennzeichnet, dass** die bestimmten Befehlssender drahtlose Fernkommunikationsmittel mit dem Befehlsempfänger (10) aufweisen.

Claims

1. A method of securing the learning mode of a device comprising an assembly of at least one command transmitter (20), communicating with a command receiver (10) capable of driving an element (14) pro-

viding for the security and/or the comfort of a building and capable of being switched to learning mode by one or more activation functions, the learning mode allowing to record a command transmitter, wherein one or more actions of which at least one is applied to a particular command transmitter of the assembly causes the disabling of at least one function of activation of the learning mode of the command receiver.

2. The method of securing as claimed in claim 1, wherein the actions are undertaken successively or simultaneously on at least one particular command transmitter and on at least one other command transmitter.
3. The method of securing as claimed in claim 1 or 2, wherein the action or actions on the particular command transmitter activate the learning mode of the receiver.
4. The method of securing as claimed in one of claims 1 to 3, wherein the action or actions on the particular command transmitter disable the functions of activation of the learning mode with the exception of those of the particular command transmitters.
5. The method of securing as claimed in one of the preceding claims, wherein the disabling of the activation function is irreversible.
6. The method of securing as claimed in one of claims 1 to 4, wherein the disabling of the activation function is temporary.
7. The method of securing as claimed in one of the preceding claims, wherein an action on a particular command transmitter causes, in the memory of the receiver, the erasure of the identity numbers of at least certain transmitters.
8. A device intended to implement the method as claimed in one of claims 1 to 7, which device comprises at least one particular command transmitter, and possibly other command transmitters (20), communicating with a command receiver (10) capable of driving an element (14) providing for the security and/or the comfort of a building.
9. A device as claimed in claim 8, wherein the particular command transmitters comprise wireless means of remote communication with the command receiver (10).

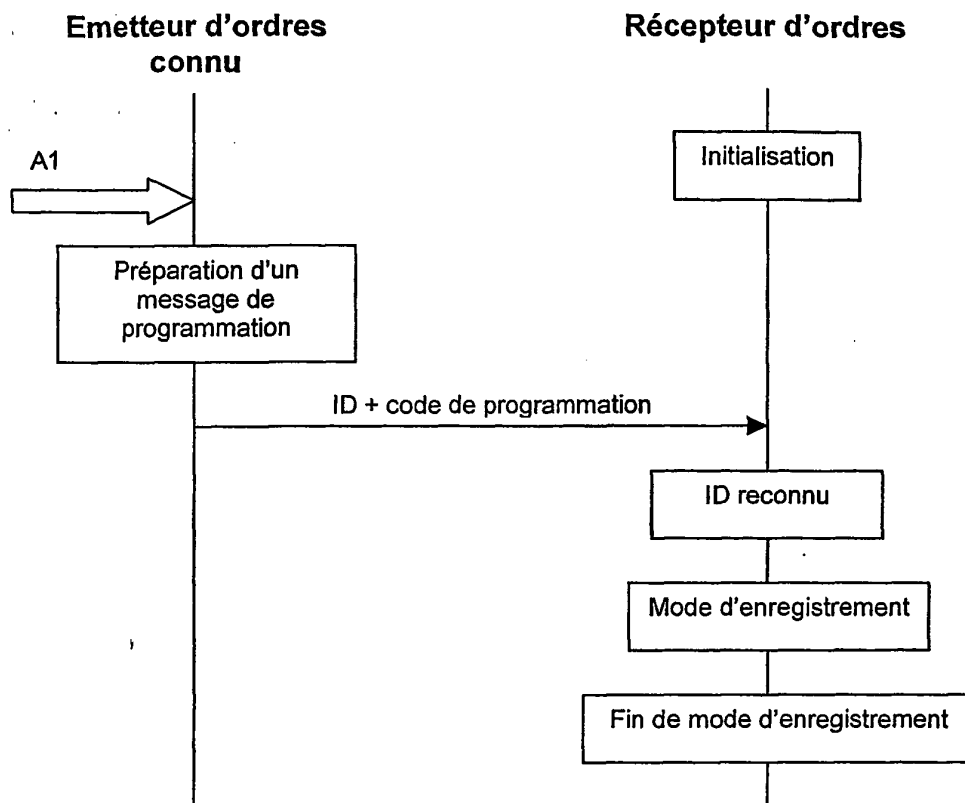


Fig. 1 (Art antérieur)

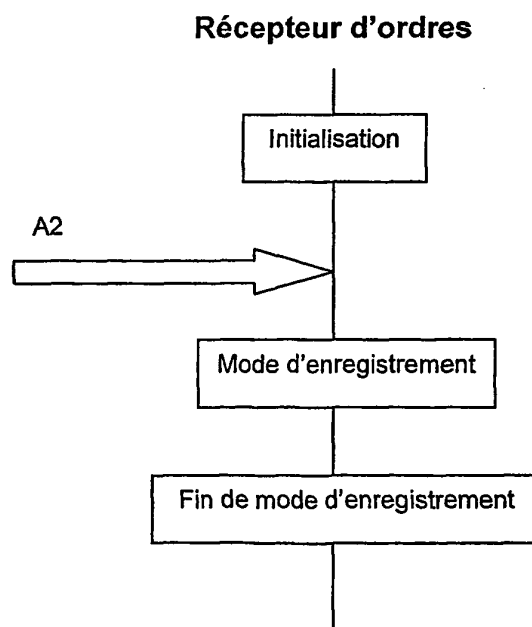


Fig. 2 (Art antérieur)

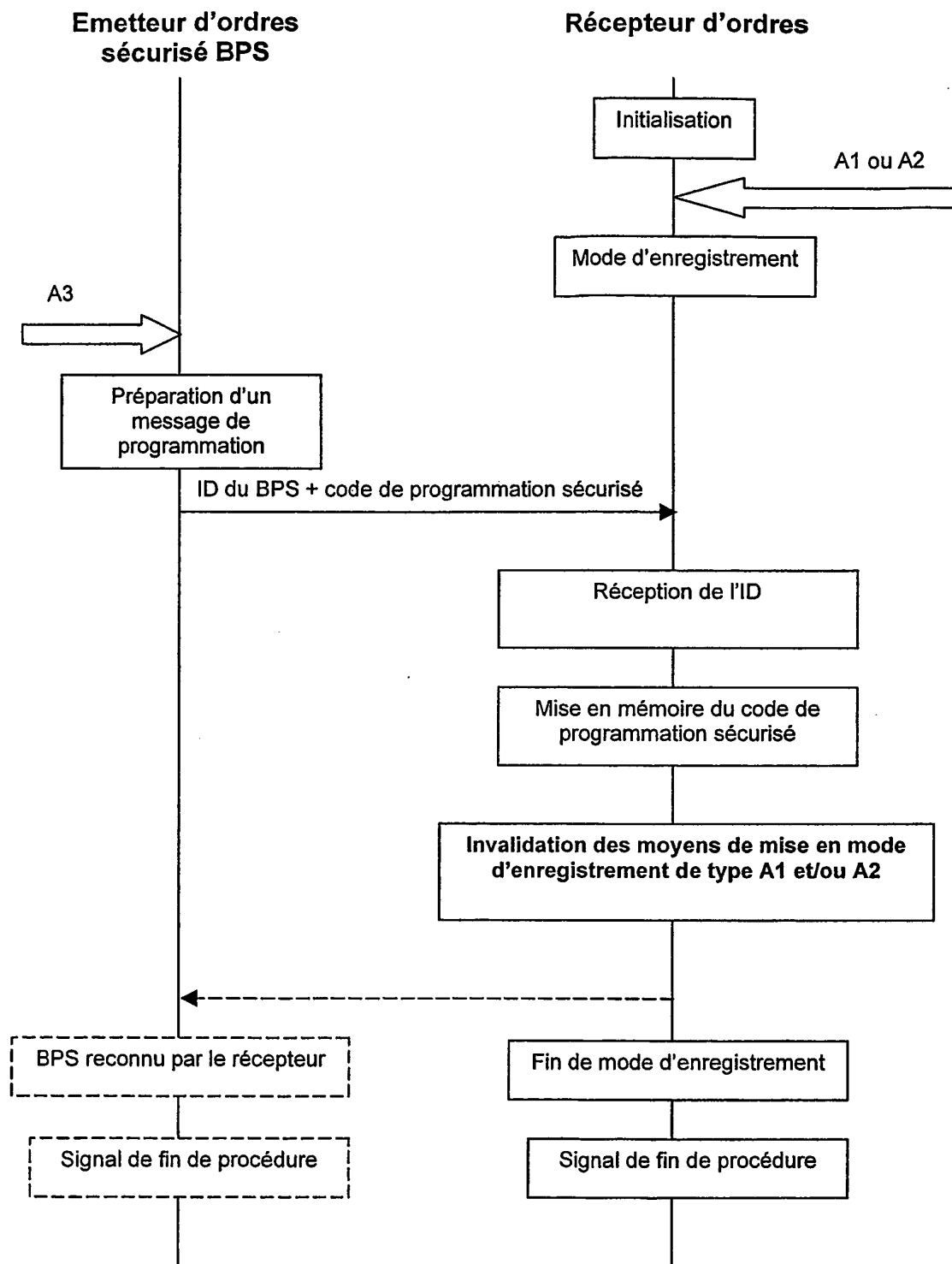


Fig. 3

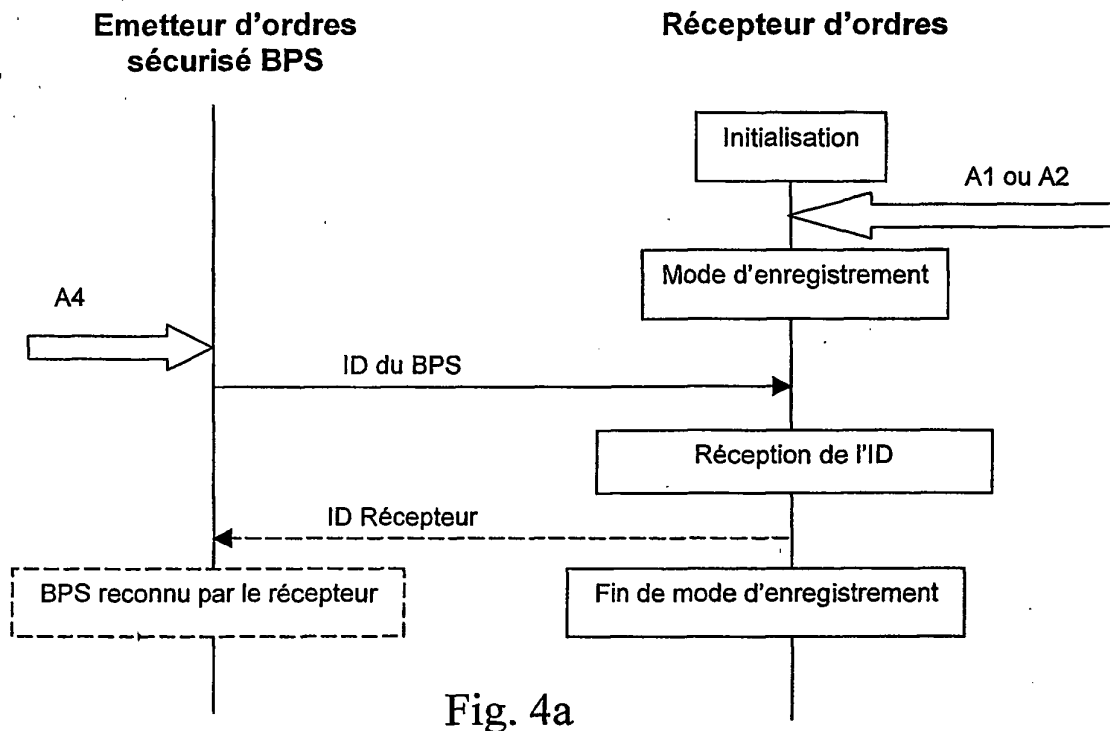


Fig. 4a

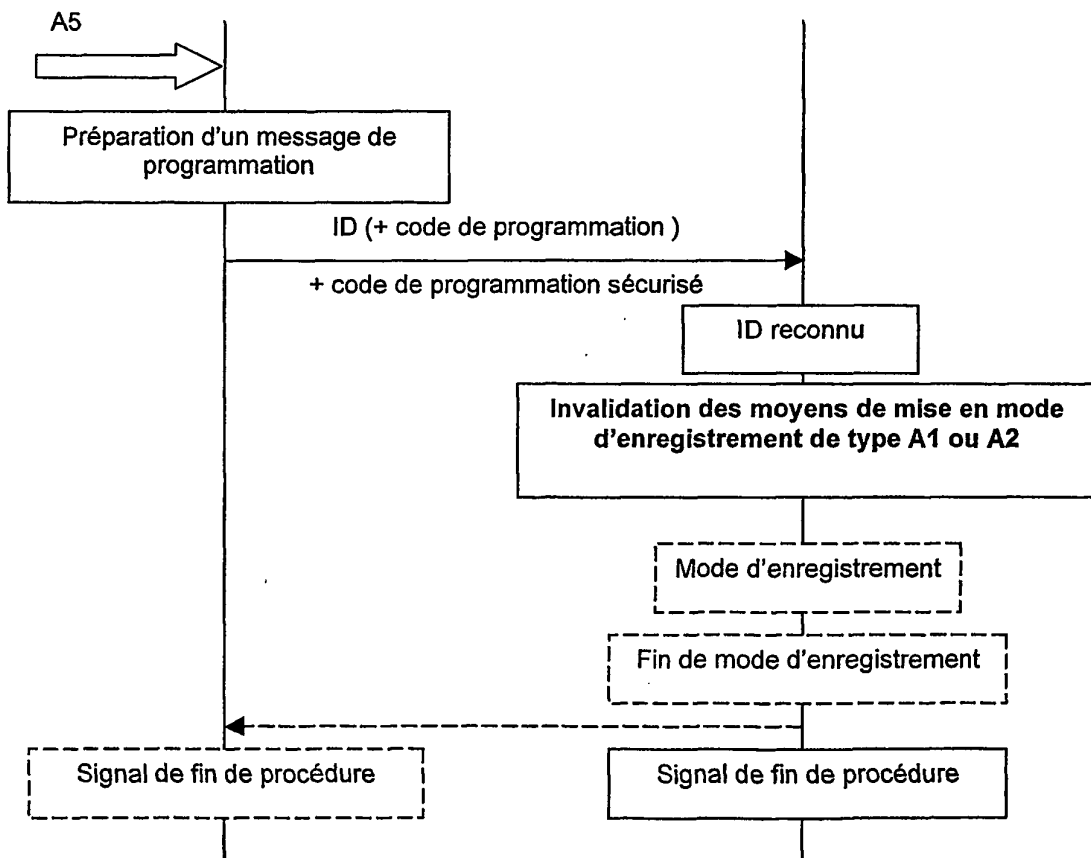


Fig. 4b

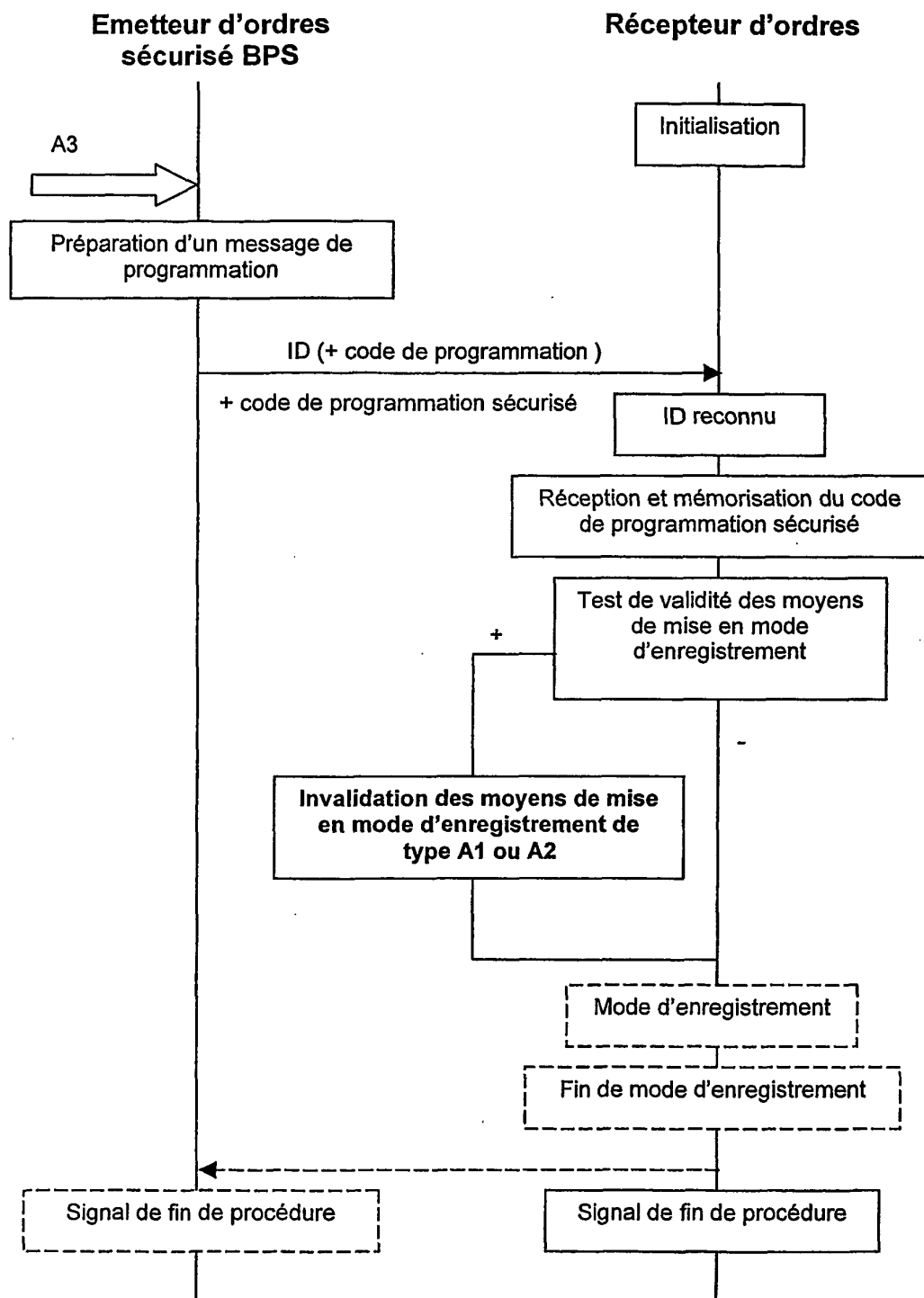


Fig. 5

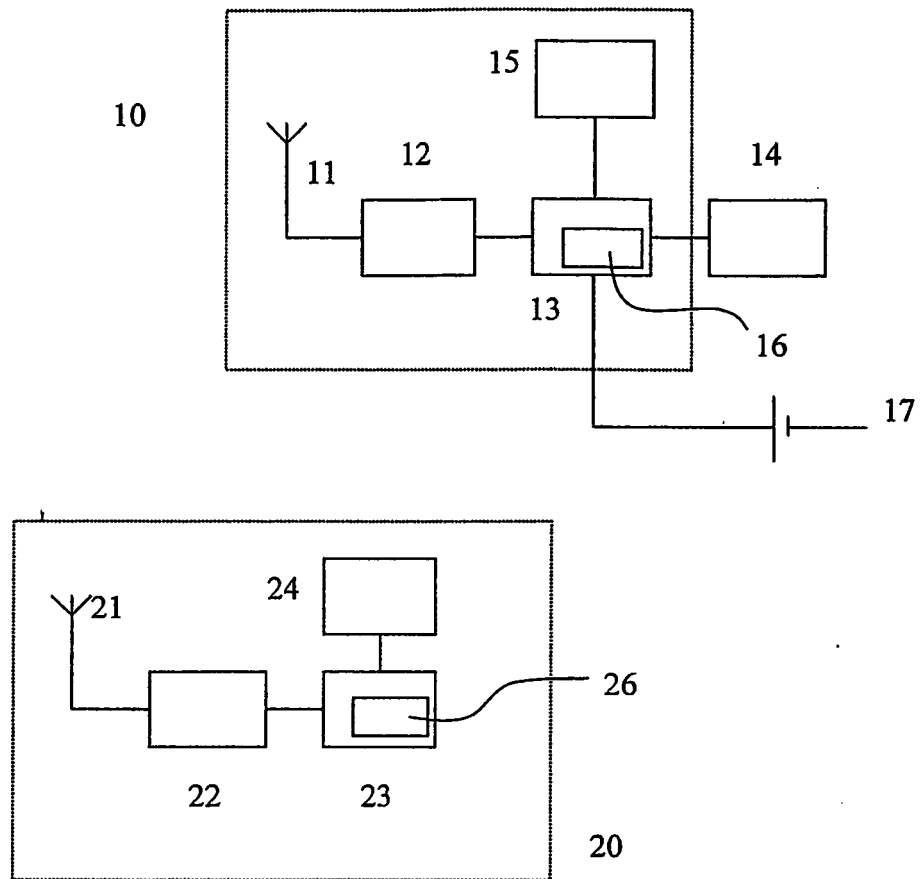


Fig.6

RÉFÉRENCES CITÉES DANS LA DESCRIPTION

Cette liste de références citées par le demandeur vise uniquement à aider le lecteur et ne fait pas partie du document de brevet européen. Même si le plus grand soin a été accordé à sa conception, des erreurs ou des omissions ne peuvent être exclues et l'OEB décline toute responsabilité à cet égard.

Documents brevets cités dans la description

- EP 0867848 A [0004]
- FR 2727553 [0004]
- EP 0921507 A [0007]
- JP 2001032587 B [0016]