ROYAUME DE BELGIQUE

SPF ECONOMIE, P.M.E.,

CLASSES MOYENNES & ENERGIE

BREVET D'INVENTION

NUMERO DE PUBLICATION : 1014777A3

NUMERO DE DEPOT : 2001/0837

Classif. Internat. : H04L

Date de délivrance le : 06 Avril 2004

Le Ministre de l'Economie,

Vu la loi du 28 Mars 1984 sur les brevets d'invention, notamment l'article 22;

Vu l' arrêté royal du 2 Décembre 1986 relatif à la demande, à la délivrance et au maintien en vigueur des brevets d'invention, notamment l'article 28;

Vu le procès verbal dressé le 21 Décembre 2001 à 24H00 à l 'Office de la Propriété Intellectuelle

ARRETE:

ARTICLE 1.- Il est délivré à : THALES COMMUNICATIONS BELGIUM S.A. rue des Frères Taymans 28, B-1480 TUBIZE(BELGIQUE)

un brevet d' invention d' une durée de 20 ans, sous réserve du paiement des taxes annuelles, pour : SYSTEME DE COMMUNICATIONS SÉCURISEES, COMPORTANT UN RESEAU LOCAL PAR EXEMPLE DU TYPE ETHERNET, NOTAMMENT EMBARQUE DANS UN AERONEF.

INVENTEUR(S) : Vervust Marc, Thales Communications Belgium S.A., rue des Frères Taymans 28, B-1480 Tubize (BE); Hugaerts Mark,Thales Communications Belgium S.A., rue des Frères Taymans 28, B-1480 Tubize (BE)

ARTICLE 2.- Ce brevet est délivré sans examen préalable de la brevetabilité de l'invention, sans garantie du mérite de l'invention ou de l'exactitude de la description de celle-ci et aux risques et périls du(des) demandeurs(s).

Pour expédition certifiée conforme

PETIT M.
Conseiller adjoint

Bruxelles, le 06 Avril 2004
PAR DELEGATION SPECIALE :

PETIT M.
Conseiller adjoint

Système de communications sécurisées, comportant un réseau local par exemple du type Ethernet, notamment embarqué dans un aéronef

La présente invention concerne un système de communications sécurisées comportant un réseau local, par exemple du type Ethernet. Elle s'applique notamment pour les systèmes de communication multifonctions où il est nécessaire d'assurer un haut niveau de sécurité dans la transmission de la voix ou de données, comme c'est le cas par exemple pour certains systèmes embarqués dans des aéronefs.

Des systèmes de communications entre plusieurs membres d'un même équipage, embarqués dans des avions par exemple, sont connus. Dans ce cas les communications peuvent d'ailleurs être étendues à l'extérieur de l'aéronef. Les différents membres d'équipage vont échanger entre eux des informations de niveaux de sécurité différents. Tous les destinataires ne peuvent pas recevoir toutes les informations transmises par un opérateur donné. Il est donc important que le système puisse de la façon la plus fiable possible séparer les données selon leur niveau de confidentialité afin notamment que chaque opérateur soit sûr que ce sera le destinataire autorisé qui recevra son message. La sécurisation du transfert de l'information est un aspect essentiel dans ce type de systèmes de communications, le destinataire recevant l'information de façon intentionnelle ou non.

Un but de l'invention est notamment de permettre une transmission fiable des données à l'intérieur d'un réseau de communication local. A cet effet, l'invention a pour objet un système de communication, comportant au moins un réseau local et des terminaux connectés à ce réseau et échangeant des paquets de donnée. Chaque terminal comporte une table mémorisant les adresses des groupes de terminaux avec lesquels il peut entrer en communication. Un terminal qui émet un paquet de données sur le réseau en mode multicast crée une adresse réseau multicast dont des bits, par exemple les octets de poids fort, ont une valeur donnée et qui comporte l'adresse du groupe destinataire du paquet de données, chaque

terminal comparant l'adresse du groupe destinataire avec le contenu de sa table une fois l'adresse réseau émise sur le réseau.

D'autres caractéristiques et avantages de l'invention apparaîtront à l'aide de la description qui suit faite en regard de dessins annexés qui représentent :

- la figure 1, un schéma fonctionnel d'un système selon l'invention ;
- la figure 2, un schéma synoptique d'un système selon l'invention ;
- la figure 3, une illustration des couches logiciel d'un terminal récepteur intervenant dans le filtrage des données transmises dans le système ;
- la figure 4, une illustration du mode d'adressage des paquets de données utilisé par un terminal émetteur ;
- la figure 5, une illustration de l'analyse des adresses de paquets transmis effectuée par un terminal récepteur ;
- la figure 6, un exemple de structure d'un paquet de données transmises par un terminal émetteur ;
- la figure 7, un exemple de classement d'adresses dans une table associée à chaque terminal du système.

La figure 1 présente un schéma fonctionnel d'un système 1 selon l'invention. Il permet à plusieurs opérateurs de communiquer, en particulier selon plusieurs niveaux de sécurité et échanger plusieurs types d'informations, vocales ou non. Ces opérateurs sont par exemple les membres d'équipage d'un avion.

Ce système 1 relie entre eux plusieurs éléments de radiocommunication R_i, R_j, 2. Ces éléments sont par exemple des postes tels que des récepteurs radio et des émetteurs radio, ou sont par exemple des ensembles 2 d'écouteurs / microphones intégrés notamment dans des casques. Le système 1 peut encore relier par exemple ces éléments à des moyens d'enregistrement 3, à des moyens de traitement de données 4, à des moyens de commande 5 notamment pour la maintenance. Il permet aussi de relier à tous ces éléments des moyens de cryptage KY de façon à protéger certaines données sensibles, ces données représentant une voix ou

toute autre information, numérisée ou non, lors des communications ou échanges d'informations.

Le système 1 comporte notamment un réseau local 21, par exemple du type LAN à haut débit, dont les nœuds comportent des unités d'émission / réception qui sont reliées à ces éléments R_i, KY, 2, 3, 4, 5 directement ou par l'intermédiaires d'interfaces. Ces unités comportent des moyens tels que par exemple des protocoles d'adressage et de communication qui permettent l'aiguillage des données d'un groupe d'éléments à un autre groupe d'éléments.

La figure 2 illustre par un synoptique le système 1 précédent, ce dernier étant par exemple un système de communication multifonctions entre plusieurs opérateurs.

Le système comporte au moins des terminaux multicanaux MCTU et des terminaux à simple canal SCTU situées aux nœuds du réseau 21. Il comporte par ailleurs des interfaces de commande et de contrôle 6. Ces interfaces 6 peuvent être plus ou moins élaborées. Les unités MCTU sont reliées à des postes radio R_1, ... R_N, à des moyens de cryptage KY, ainsi par exemple qu'à des moyens de maintenance non représentés. Un terminal multicanaux MCTU peut être relié à plusieurs éléments du type poste radio ou moyens de cryptage par exemple. Les unités SCTU sont reliées aux interfaces de commande et de contrôle 6. Une unité SCTU et une interface 6 peuvent par exemple être regroupées dans une même boîte. Les unités SCTU sont par ailleurs par exemple reliées à des casques audio et des microphones, ou tout autre moyen de communication audio, voire visuel. Une interface de commande et de contrôle 6 est une interface homme-machine élaborée, par exemple un panneau de contrôle comportant un écran tactile et diverses touches, qui permet à un opérateur de sélectionner ses canaux de communication. L'interface 6 relie donc les unités MCTU et SCTU à des moyens de communication audio du type microphone ou casque, mais aussi à des moyens de contrôle du type touche ou écran tactiles précités. Elle est donc par exemple couplée à une station de commande.

Le système 1 peut aussi communiquer avec des interfaces simplifiées CB. Une telle interface CB est par exemple une interface homme-machine de base destinée à un opérateur, cette interface est reliée

directement à une unité MCTU. Elle comporte une interface audio qui peut être soit un casque ou un microphone, ou tout autre moyen de communication. Une interface CB accède au système à travers un canal de communication propre relié à une unité MCTU. En particulier elle n'accède pas à une unité MCTU via le réseau local 21.

Une unité terminale multicanaux MCTU est donc interfacée avec un certains nombre de canaux analogiques et numériques reliés notamment aux postes radio R_i et aux moyens de cryptage KY. Un canal analogique, appelé par la suite canal audio, consiste en une ligne bidirectionnelle et un certains nombre d'entrées / sorties discrètes fournissant un contrôle des émissions et réceptions. Le canal est encore appelé « full duplex » dans la littérature anglo-saxonne dans la mesure où les communications peuvent se faire simultanément dans un sens et dans l'autre. Un canal numérique, appelé par la suite canal de données, consiste en une ligne bidirectionnelle, de type « full duplex » avec des entrées / sorties discrètes pour fournir un contrôle des émissions et réceptions. Chaque MCTU est ainsi interfacée avec le réseau local 21 par un circuit approprié. Ce circuit est commandé par une couche logicielle. De même, chaque unité SCTU est interfacée avec le réseau 21 par un tel circuit. De la sorte, le réseau local 21 interconnecte entre elles toutes les unités MCTU et SCTU. Il véhicule toutes les données audio, numériques ou de contrôle à travers tout le système.

Une unité MCTU réalise notamment des conversions analogique-numérique et numérique-analogique pour tous les canaux audio qui lui sont interfacés. Elle convertit et route les données d'entrées d'un canal de données vers le réseau 21. Vice et versa, elle convertit et route les données du réseau vers les canaux de données. Toutes les données entrantes dans une unité MCTU , audio ou numériques, mais aussi les adresses sont par exemple automatiquement affectées d'un tag selon leur niveau de sécurité. De la sorte une donnée peut être reconnue de façon sécurisée et utilisée par un récepteur approprié du réseau 21. En particulier, deux niveaux de sécurité sont à considérer, un niveau dit rouge et un niveau dit noir. Si le niveau de sécurité d'un signal, une voix digitalisée ou des données, est rouge ce signal sera affecté d'un premier type de tag, dit rouge. Si le niveau de sécurité d'un signal, une voix digitalisée ou des données, est noir ce signal sera affecté d'un deuxième type de tag, dit noir. Il est à noter que l'affectation de tags

n'est pas limité à des tags rouge ou noir, mais peut aussi être étendu à d'autres niveaux de sécurité.

Une unité terminale à simple canal SCTU constitue notamment un nœud d'entrée ou de sortie du réseau local 21 pour les signaux audio, représentant particulièrement les voix des différents opérateurs. Elle forme donc une entrée / sortie audio pour le système 1. Une unité SCTU comporte ainsi, via une interface de contrôle 6, une liaison avec une interface audio qui peut être par exemple un casque audio, un microphone ou un masque à oxygène. L'unité SCTU comporte par exemple un deuxième canal destinée à un observateur. Ce deuxième canal n'est pas un canal de données séparé, mais est issu d'un multiplexage analogique avant numérisation des signaux. Comme pour l'unité MCTU, un canal analogique, appelé par la suite canal audio, consiste en une ligne bidirectionnelle de type « full duplex » et un certains nombre d'entrées / sorties discrètes ou non fournissant un contrôle des émissions et réceptions. Les informations de contrôle sont notamment fournies par l'interface 6 associée. Ces informations dépendent par exemple du niveau de sécurité demandé et des destinataires ou des émetteurs des messages. Comme cela a été indiqué précédemment, une unité SCTU est interfacée directement avec le réseau local 21 par l'intermédiaire d'un circuit approprié. Elle réalise notamment les conversions analogique-numérique et numérique-analogique. Elle affecte ses données entrantes d'un tag correspondant à leur niveau de sécurité. Une unité SCTU est reliée à une interface de contrôle 6 par un bus série. Ce bus est seulement utilisé pour le transfert des informations de contrôle, c'est-à-dire pour le contrôle et l'analyse des commandes envoyées vers l'interface 6 ou provenant de cette dernière. Il ne contient pas des informations de voix. L'unité SCTU transfert notamment les données issues de l'interface 6 vers le réseau local 21.

Chaque nœud du système, c'est-à-dire soit une unité MCTU ou une unité SCTU, est physiquement connecté au réseau local 21 par un circuit intégré numérique connu par ailleurs, par exemple à microprocesseur. Ce circuit comporte les entrées et sorties nécessaires aux données véhiculées ainsi qu'aux diverses informations de contrôle, y compris l'adressage matériel du circuit. Ce dernier est par exemple relié au réseau au moyen d'un nombre de paires de conducteurs, soit quatre conducteurs par

connexion, deux de type RX et deux de type TX. D'autres modes de liaison au réseau sont bien sûr possibles.

Un des nœuds du système, une unité MCTU ou une unité SCTU, joue le rôle de serveur, en particulier pour la mise en marche du système. N'importe quelle unité MCTU ou SCTU peut jouer ce rôle. Ce serveur contient la base de données du système. Lorsque le serveur est mis en marche, il met à jour la base de données du système dans tous les nœuds du réseau, c'est-à-dire dans toutes les unités MCTU et SCTU. Chaque nœud a ainsi la même base de données et a ainsi accès à la configuration opérationnelle de tout le réseau. La base de données système permet d'identifier pour chaque poste les opérations autorisées, par exemple les canaux de communication qu'un opérateur peut sélectionner au travers de son interface de commande et de contrôle 6 . Quand l'opérateur effectue une sélection et presse par exemple sur un bouton de commande de transmission, le message audio est échantillonné, c'est-à-dire qu'il subit une conversion analogique-numérique par l'unité SCTU reliée à l'interface 6. Puis il est par exemple traité pour former un paquet de données d'une certaine longueur Δt. Il est alors transféré sur le réseau local 21. Le paquet audio ainsi défini est ensuite capté par les autres nœuds MCTU, SCTU du réseau qui le sont autorisés. Ainsi par exemple, si un utilisateur veut parler à deux radios R_i, R_k en même temps, chaque Δt son poste envoie deux paquets de signaux numériques audio successifs sur le réseau, un paquet pour le poste radio R_j et un pour le poste radio R_k. L'en-tête d'un paquet détermine qui est autorisé à le recevoir, c'est-à-dire qu'il comporte l'adresse du ou des destinataires. Le système utilise par exemple les protocoles TCP/IP et UDP/IP pour communiquer dans le réseau local 21. Le protocole utilisé a une structure en couches empilées où chaque couche fournit un service à la couche qui lui est immédiatement inférieure. Un paquet qui est reçu matériellement par une unité doit traverser ensuite chaque couche avant d'être présenté à l'applicatif qui réside sur la couche supérieure de la pile.

Chaque couche réalise un filtrage du paquet reçu de façon à ce que les paquets non autorisés soient rejetés le plus tôt possible. Cela est particulièrement nécessaire pour des raisons de sécurité. A cet effet, une table d'adressage est implémentée dans chaque terminal MCTU, SCTU. Le réseau local Ethernet par exemple, utilise six octets d'adresse au niveau

matériel. La couche IP (Internet Protocol) située au-dessus de la couche d'interface matérielle utilise quatre octets d'adresse. Finalement, les protocoles TCP et UDP utilisent par exemple des numéros de ports pour adresser un process donné.

Dans un réseau sécurisé, toutes les données transmises ne peuvent pas aller sur n'importe quel récepteur. A titre d'exemple, on se base ici sur des données de type rouge et des données de type noir, d'autres niveaux de sécurité pouvant bien sûr être gérés par un système selon l'invention. Dans l'exemple de configuration de la figure 2, certaines données doivent être cryptées avant transmission à des postes radio. A cet effet, des unités MCTU dédiées sont reliées à des moyens de cryptages KY, celles-ci sont destinées à router les données rouges qui doivent être cryptées avant transmission aux postes radio par exemple. D'autres unités MCTU sont reliées directement aux postes radios et sont destinées à router les données noires qui ne nécessitent pas de cryptage. Une unités MCTU est soit rouge, soit noire de façon figée dans le temps. Au contraire, une unité SCTU peut être rouge à un instant donné et noire à un autre instant. Les moyens de cryptage KY sont par ailleurs reliés à des éléments de communications vers l'extérieur via une unité MCTU, soit reliés directement à des éléments de communications non représentés.

La figure 3 illustre comment le filtrage des données est appliqué au niveau de chaque composant hôte 31, chaque fois qu'une trame ou paquet passe sur le réseau local 21. Ce composant 31 est par exemple une unité MCTU ou une unité SCTU. La première couche de filtrage est effectuée par le circuit matériel 32 associé à chaque unité, c'est-à-dire le circuit 32 directement connecté au réseau local 21. Ce circuit 32 de connexion pourra être appelé par la suite circuit Ethernet pour faciliter la description. Tout autre circuit 32 qui est une interface matérielle réseau peut bien sûr être utilisé. Ce circuit 32 comporte une première couche logicielle 33. Donc, dans une première étape, le circuit Ethernet 32 analyse l'adresse de chaque paquet qui passe sur le réseau. Il agit en particulier différemment selon que le paquet de données et du type unicast ou multicast.

La figure 4 illustre le mode d'adressage des paquets de données utilisé dans un système selon l'invention, pour une transmission du type multicast. Une transmission multicast permet la transmission d'un paquet de données depuis un nœud du réseau, dans le cas présent une unité MCTU ou SCTU, vers un groupe de nœuds du réseau, c'est-à-dire vers un ensemble d'unités MCTU ou SCTU. Chaque groupe multicast est identifié par une adresse spécifique. L'appartenance à un groupe multicast donné est dynamique, c'est-à-dire que des unités peuvent rejoindre ou quitter un groupe à n'importe quel instant. Une unité peut appartenir à plusieurs groupes à la fois. Une unité n'a pas besoin d'être membre d'un groupe pour envoyer des données vers les membres de ce groupe.

Les groupes multicast sont par exemple identifiés par une adresse 41 de classe D, correspondant au protocole TCP/IP, c'est-à-dire par une adresse dont les quatre bits de poids fort sont 1110, formant la valeur E en hexadécimal. Cette adresse est codée sur 32 bits. En notation Internet standard, les adresses des groupes multicast occupent donc l'espace compris entre 224.0.0.0. et 239.255.255.255. L'adresse 224.0.0.0. n'est par exemple pas utilisée et l'adresse 224.0.0.1. est par exemple réservée pour le groupe multicast correspondant à toutes les unités MCTU et SCTU. Les adresses des groupes multicast sont mémorisées dans une table 42, appelée par la suite table multicast. Cette table 42 est présente dans chaque unité MCTU, SCTU, plus particulièrement dans son circuit Ethernet 32 associé. Une unité MCTU, SCTU est reliée au réseau local 21 par l'intermédiaire de ce circuit. A un instant donné, la table multicast stockée dans une unité, ou plus particulièrement dans son circuit de connexion 32, représente l'ensemble des groupes multicast auxquels appartient cette unité. A chaque groupe multicast correspond donc une adresse, et à cette adresse correspond un canal.

Pour pouvoir parler à un poste radio ou à un réseau de conférence donné, il est nécessaire d'utiliser un canal. Un canal est en fait une connexion virtuelle qui existe entre un initiateur du canal, typiquement l'opérateur activant son interface de commande et de contrôle 6, et une ou plusieurs stations. Un canal est identifié par un numéro unique de telle façon qu'il puisse être utilisé à l'intérieur du réseau local 21 sans ambiguïté. Ainsi par exemple, lorsqu'un opérateur active son interface de contrôle et de

commande 6 pour entrer en communication avec un groupe d'interlocuteurs, cet interface 6 envoie un message à son unité SCTU associée lui indiquant le numéro de canal choisi, correspondant au groupe sélectionné. Le numéro de canal correspond par exemple à l'emplacement de l'adresse de groupe multicast dans la table 42.

L'unité SCTU va donc chercher dans sa table multicast 42 l'adresse de groupe multicast correspondante puis crée l'adresse réseau multicast du paquet de données qui va être transmis, cette adresse réseau 43 étant par exemple codée sur 48 bits, comme l'illustre la figure 4. A cet effet, les 23 bits de poids faible de l'adresse de groupe multicast 41 forment les 23 bits de poids faible de l'adresse réseau 43. Le bit suivant n'est par exemple pas utilisé, et fixé arbitrairement à 0 dans l'adresse réseau. Enfin, les trois octets de poids fort de l'adresse réseau 43 sont toujours fixés à une même valeur, par exemple une valeur d'adresse Ethernet codée en base hexadécimale 01 00 5E. Une adresse réseau commençant par cette valeur 01 00 5E sera comprise comme une adresse Ethernet multicast. Les cinq bits de l'adresse de groupe multicast 41 compris entre les 23 bits de poids faible et les quatre bits de poids fort formant la valeur hexadécimale E ne sont pas utilisés, et donc pas reportés dans l'adresse réseau. A titre d'exemple, si une adresse de groupe multicast a la valeur E1 55 55 55, ses données correspondantes seront transmises avec l'adresse réseau 01 00 5E 55 55 55. Dans l'exemple de création d'adresse réseau 43 par une unité émettrice, on a considéré à titre d'exemple que l'adresse transférée était du type IP (Internet Protocol), notamment TCP/IP. D'autres types de protocoles peuvent bien sûr être considérés. Par ailleurs, cette adresse a été transférée sur 23 bits. Elle peut évidemment être transférée sur un autre nombre N de bits, notamment en fonction de la structure du réseau et des circuits de réception.

Dès lors, l'analyse des adresses effectuées par le circuit de connexion 32 se fait conformément à la figure 5. On suppose qu'une unité SCTU envoie un paquet avec une adresse de destination. Les circuits Ethernet 32 des autres unités analysent cette adresse comme l'illustre la figure 5. Sur Ethernet par exemple, le bit de poids faible de l'octet de poids fort de l'adresse multicast est fixé à 1. Ainsi, en base hexadécimale, cette

adresse est du type X1 : XX : XX : XX : XX. Le circuit 32 ayant vérifié qu'il s'agit d'une adresse Ethernet, il vérifie dans un premier test 51 que l'adresse réseau 43 contient une adresse multicast 41 de classe D, c'est-à-dire conformément à la création des adresses précédemment décrite, que cette adresse réseau commence par la valeur 01 00 5E. Si ce n'est pas le cas, il vérifie dans un test suivant 52 que l'adresse reçue correspond à son adresse physique. Si c'est bien le cas, cela signifie qu'il est destinataire du message, le message est alors traité par une couche logicielle suivante 34. Dans le cas contraire, le message est rejeté 53, il n'est pas pris en compte. Si le premier test 51 confirme qu'il s'agit d'un message multicast, c'est-à-dire que l'adresse commence par 01 00 5E, alors le circuit 32 va vérifier pár un test suivant 54 s'il appartient bien au groupe multicast destinataire du message. Pour cela, il reconstitue l'adresse multicast par l'opération inverse de celle illustrée par la figure 4, en extrayant notamment les 23 bits de poids faible. Puis il vérifie que l'adresse multicast ainsi obtenue est contenue dans sa table multicast 42. Si c'est le cas, il appartient bien au groupe multicast destinataire et le message est ensuite traité par la couche logicielle suivante 34. Cette adresse sera ensuite traitée classiquement comme une adresse multicast dans le protocole de communication qui est par exemple du type TCP/IP ou UDP/IP. Si l'adresse multicast n'est pas contenue dans la table multicast du circuit 32, ce dernier rejette 53 le message.

On se reporte de nouveau à la figure 3. Donc, en règle générale, le circuit Ethernet 32 reçoit seulement les paquets dont l'adresse de destination correspond soit à son adresse matérielle, soit à une adresse de groupe multicast contenue dans sa table 42. Ce circuit est commandé par une couche logicielle 33 qui est le premier de l'empilement des couches logicielles successives qui vont filtrer les messages reçus. Cette première couche logicielle 33 transmet les paquets à la couche suivante 34 qui est par exemple une couche IP. Ce protocole Internet IP effectue un filtrage basé sur les adresses source et destination, et transmet le datagramme à la couche suivante 35, qui est une couche TCP/IP ou UDP/IP, si tout est conforme. Chaque fois que cette dernière couche 35 reçoit un datagramme de la couche IP 34, elle réalise un filtrage basé sur le numéro du port de destination, et éventuellement aussi sur le numéro de port source. Il y a donc

ici un niveau de filtrage supplémentaire qui prend en compte le numéro de port de la source d'émission. Un système selon l'invention est réalisé de telle sorte que chaque canal ait une adresse multicast unique, et aussi par exemple de telle sorte que chaque unité source, notamment les unités SCTU, ait un numéro de port unique. Cela permet à une unité réceptrice, au niveau de sa couche logicielle 35 de dernier niveau par exemple, de distinguer pour chaque canal les différentes sources. Pour un canal donné, c'est-à-dire pour une adresse multicast donnée, et un numéro de port source donné N1, N2, N3, ... la couche logicielle 35 d'une unité réceptrice peut ainsi activer un applicatif correspondant 36, 37, 38. A chaque couple canal – numéro de port peut donc correspondre un traitement spécifique.

Un autre niveau de sécurité peut être basé sur le type d'informations transmises. Comme indiqué précédemment, ce niveau de sécurité peut être basé sur le classement rouge ou noir des données. A cet effet, chaque paquet émis comporte un tag dont la valeur indique si les données transmises sont rouges ou noires. Ce tag ne donne pas obligatoirement une information binaire, en particulier il peut affecter les données émises d'une information autre que le type rouge ou noir. Ce tag est généré par l'unité émettrice. L'analyse du tag est notamment exécutée par les couches logicielles de l'unité réceptrice. Ainsi, si une unité MCTU reçoit un message rouge alors qu'elle est classée noire, elle rejettera le message.

La figure 6 illustre un exemple de structure de paquet de données 61 généré par une unité SCTU dans un système selon l'invention. Ce paquet comporte en en-tête l'adresse réseau 43, le numéro de port 62 de l'unité émettrice, du tag 63 et du message 64. L'adresse 43 est de type multicast en cas d'émission multicast, elle est donc par exemple égale à 01 00 5E XX XX XX. Le numéro de port 62 est codé sur un nombre de bits compatible avec le nombre d'unités source en jeu. Le tag est codé sur un nombre de bits donnés, par exemple 8 bits. Même s'il ne définit qu'un état binaire, par exemple la qualification rouge ou noire des messages, il est plus fiable qu'il soit codé sur un nombre de bits supérieur à un. Enfin le message proprement dit 64 représente par exemple le codage d'un message vocal en cas de système de communication entre opérateurs. Ce message peut bien sûr coder tout autre type d'informations.

La figure 7 illustre un exemple de classement d'adresses de groupe multicast dans la table multicast 42 à des fins de filtrage, permettant notamment un renforcement du filtrage des données transmises. La sécurité des transmissions étant importante, il est avantageux de recourir à plusieurs tests successifs comme cela vient d'être décrit. Un test supplémentaire peut être effectué sur la place des adresses multicast dans la table multicast 42 associée à chaque unité. Ce niveau de sécurité est ici basé sur la place des adresses multicast dans cette table 42 comme le décrit la figure 7. En d'autres termes, les canaux sont classés en catégories, la position de l'adresse multicast d'un canal dans la table 42 étant fonction de sa catégorie. Une zone de la table, disjointe ou non, est associée à chaque catégorie. La position de l'adresse multicast est définie par son adresse dans cette table 42. La catégorie peut bien sûr définir un niveau de sécurité, par exemple rouge ou noir. La figure 7 illustre un rangement des adresses multicast dans la table 42 en fonction de leur catégorie. Les adresses de la première catégories occupent par exemple les N premières cases de la table, les adresses de la deuxième catégorie occupent les M cases suivantes et ainsi de suite. Un espace de plusieurs cases inoccupées peut être laissé entre deux catégories d'adresses. Dans le cas d'un niveau de sécurité rouge et noir, les adresses multicast rouges occupent par exemple les N premières cases et les adresses multicast noires occupent par exemple les cases suivantes. Avantageusement, grâce au rangement des adresses multicast dans la table 42, un filtrage peut être fait en se basant sur ce rangement. Ainsi, une unité réceptrice noire qui reçoit une adresse multicast rangée dans la zone rouge de la table va rejeter l'information. En combinant par exemple ce filtrage avec les autres filtrages, on augmente encore la fiabilité sur la sécurité de transmission des informations, on augmente par exemple la fiabilité sur la séparation des informations rouges et noires.

En se référant de nouveau à la figure 3, une fois que la dernière couche logicielle 35 d'une unité réceptrice a confirmé que la donnée reçue est bien destinée à cette unité, par l'application d'un ou plusieurs filtrages précédemment décrits, elle active l'applicatif prévu pour cette donnée. A titre d'exemple, si l'unité réceptrice est une unité MCTU, cet applicatif correspond

en la transmission des données vers des moyens de cryptage si l'unité MCTU est rouge ou en une conversion numérique-analogique du signal et sa transmission vers un poste radio si le l'unité MCTU est noire. Dans la suite des différents filtrages effectués sur les données reçues, des alarmes peuvent être générées au cas où une donnée non conforme franchit un premier niveau de sécurité, typiquement une donnée rouge reçue par une unité noire.

Un système selon l'invention peut être embarqué dans un avion ou un navire par exemple. Il permet notamment dans ce cas à tous les membres d'équipage de communiquer entre eux et avec l'extérieur selon plusieurs niveaux de sécurité. Les informations échangées sont dans ce cas des messages vocaux mais ces informations peuvent en fait représenter bien d'autres types de données. Ces données pourraient être par exemple des données vidéo, des messages écrits, des figures, des traitements informatiques etc ...

Le système a été décrit avec des terminaux multicanaux MCTU et des terminaux à simple canal SCTU. L'invention s'applique bien évidemment à des systèmes ne comportant que des terminaux multicanaux ou que des terminaux unicanal. Ces terminaux communiquant avec des interfaces ou des postes radio comme décrit ici ou avec tout autre type de moyens de communication.

REVENDICATIONS

1. Système de communication, caractérisé en ce qu'il comporte au moins un réseau local (21) et des terminaux (MCTU, SCTU) connectés à ce réseau et échangeant des paquets de données (61), chaque terminal comportant une table (42) mémorisant les adresses des groupes de terminaux avec lesquels il peut entrer en communication, un terminal qui émet un paquet de données (61) sur le réseau en mode multicast créant une adresse réseau multicast (43) dont des bits ont une valeur donnée (01 00 5E) et qui comporte l'adresse (41) du groupe destinataire du paquet de données, chaque terminal comparant l'adresse (41) du groupe destinataire avec le contenu de sa table (42) une fois l'adresse réseau (43) émise sur le réseau.

2. Système selon la revendication 1, caractérisé en ce que des octets de poids fort de l'adresse réseau (43) ont la valeur donnée.

3. Système selon l'une quelconque des revendications précédentes, caractérisé en ce que les N bits de poids faible de l'adresse de groupe (41) forment les N bits de poids faible de l'adresse réseau multicast (43).

4. Système selon l'une quelconque des revendications précédentes, caractérisé en ce que l'adresse de groupe est une adresse TCP/IP de classe D.

5. Système selon l'une quelconque des revendications précédentes, caractérisé en ce qu'un terminal (MCTU, SCTU) analyse les adresses des paquets de réseau de sorte que s'il s'agit de l'adresse réseau multicast (43) comportant la valeur donnée (01 00 5E), il compare l'adresse de groupe (41) qu'elle contient avec sa table (42) et que s'il ne s'agit pas de l'adresse (43) comportant la valeur donnée (01 00 5E), il n'accepte le paquet seulement si cette adresse donnée (43) correspond à son adresse physique.

6. Système selon l'une quelconque des revendications précédentes, caractérisé en ce que l'analyse de l'adresse réseau (43) est faite au niveau d'une couche logicielle (33) implémentée dans le circuit de connexion (32) de chaque terminal.

7. Système selon l'une quelconque des revendications précédentes, caractérisé en ce que le paquet de données transmises (61) comporte outre l'adresse réseau (43) et l' information (64) à transmettre, le numéro de port (62) du terminal source.

8. Système selon la revendication 7, caractérisé en ce qu'une couche logicielle (35) active un applicatif (36, 37, 38) en fonction du numéro de port (62) du terminal source.

9. Système selon l'une quelconque des revendications précédentes, caractérisé en ce que le paquet de données transmises (61) comporte outre l'adresse réseau (43) et l' information (64) à transmettre, un tag (63) représentant une catégorie de données.

10. Système selon la revendication 9, caractérisé en ce que le système véhicule au moins deux catégories de données.

11. Système selon l'une quelconque des revendications 9 ou 10, caractérisé en ce qu'une couche logicielle (35) analyse les données reçues en fonction de la valeur du tag.

12. Système selon l'une quelconque des revendications précédentes, caractérisé en ce que les adresse de groupe (41) sont stockées dans des zones (C1, C2, ...CN) de la table (42) fonctions de leurs catégories.

13. Système selon la revendication la revendication 12, caractérisé en ce caractérisé en ce qu'une couche logicielle (35) analyse les données reçues en fonction de la place de leur adresse de groupe (41) dans la table.

14. Système selon la revendication 13, caractérisé en ce qu'une donnée dont l'adresse ne se situe pas dans la zone attendue est rejetée.

15. Système selon l'une quelconque des revendications précédentes, caractérisé en ce qu'il comporte des terminaux (MCTU) reliés à des éléments de communication (R_i) et des terminaux (SCTU) reliés chacun à une interface de commande et de contrôle (6) pour la transmission des données, un terminal (SCTU) créant l'adresse réseau (43) en fonction des instructions reçues de l'interface.

16. Système selon la revendication 15, caractérisé en ce qu'il comporte des moyens de cryptage des données (KY) reliés à des terminaux pour la transmission de données sécurisées, un terminal relié directement à des moyens de communication (R_i) n'étant jamais relié en même temps à des moyens de cryptage (KY).

17. Système selon l'une quelconque des revendications 12 à 14 et la revendication 16, caractérisé en ce qu'il véhicule au moins deux catégories de données, les données d'une première catégorie étant destinées aux terminaux reliés aux moyens de cryptage.

18. Système selon l'une quelconque des revendications précédentes, caractérisé en ce que la valeur donnée est 01 00 5E en base hexadécimale.

19. Système selon l'une quelconque des revendications précédentes, caractérisé en ce qu'il est embarqué dans un aéronef.

2001/0837.

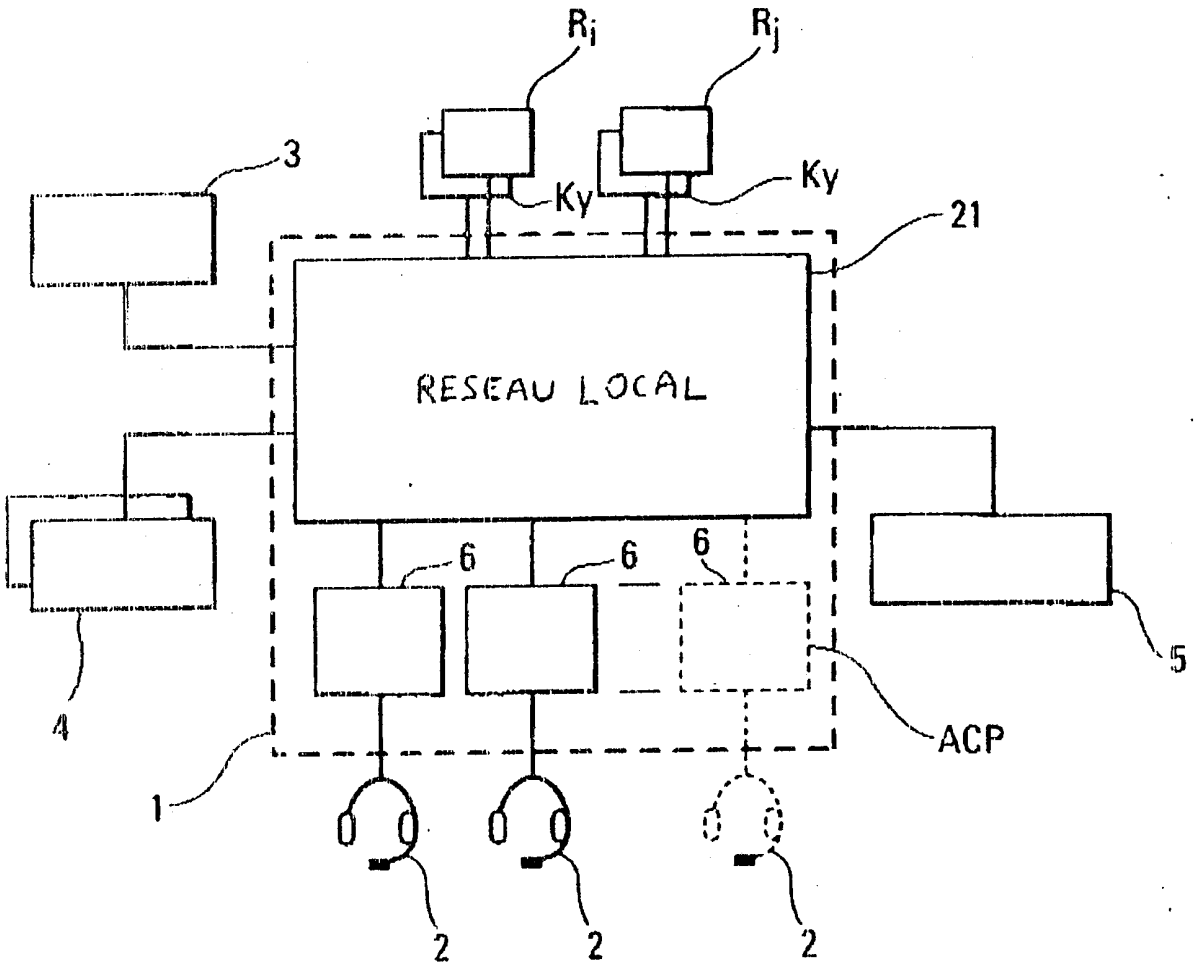

Fig. 1

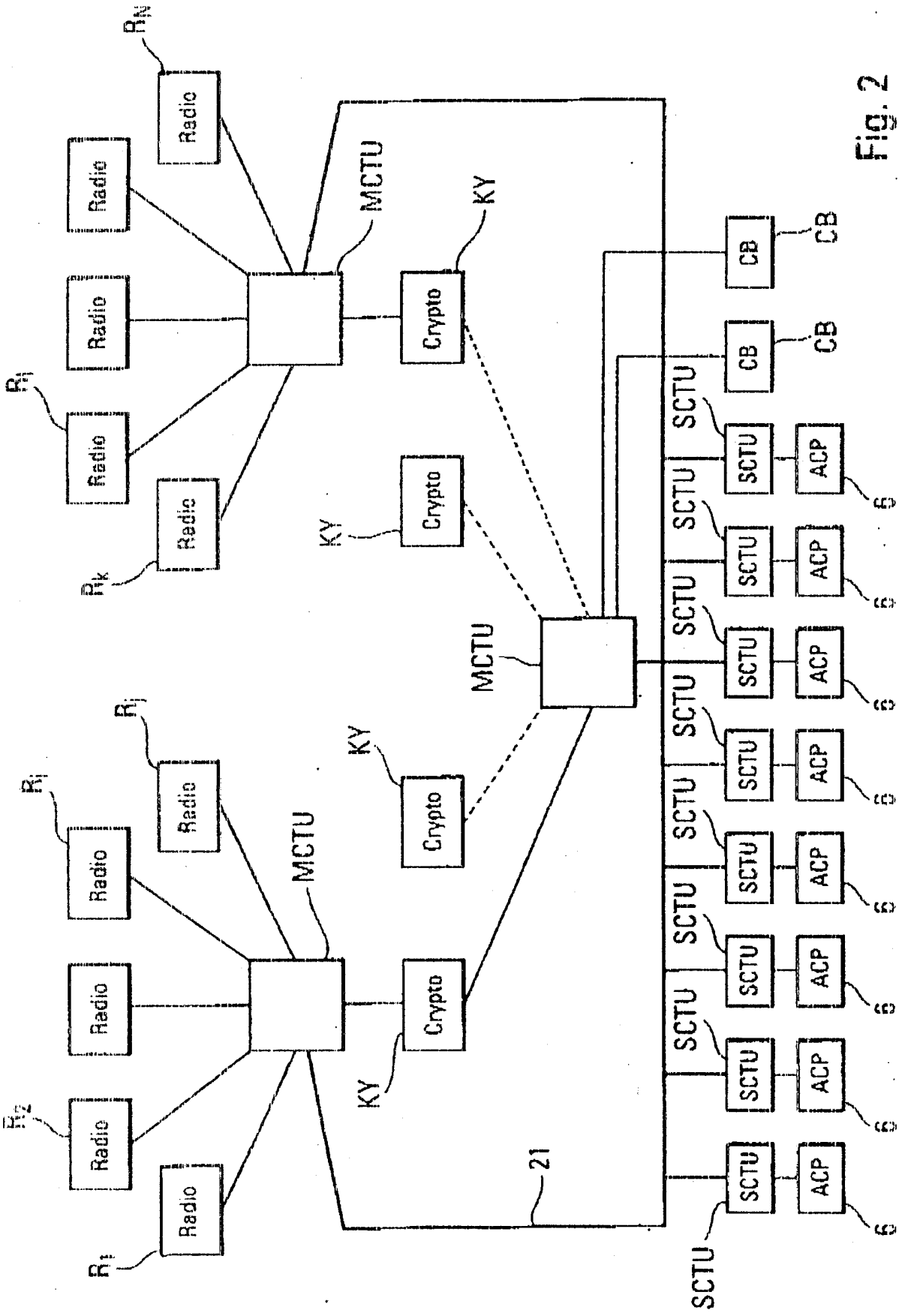

Fig. 2

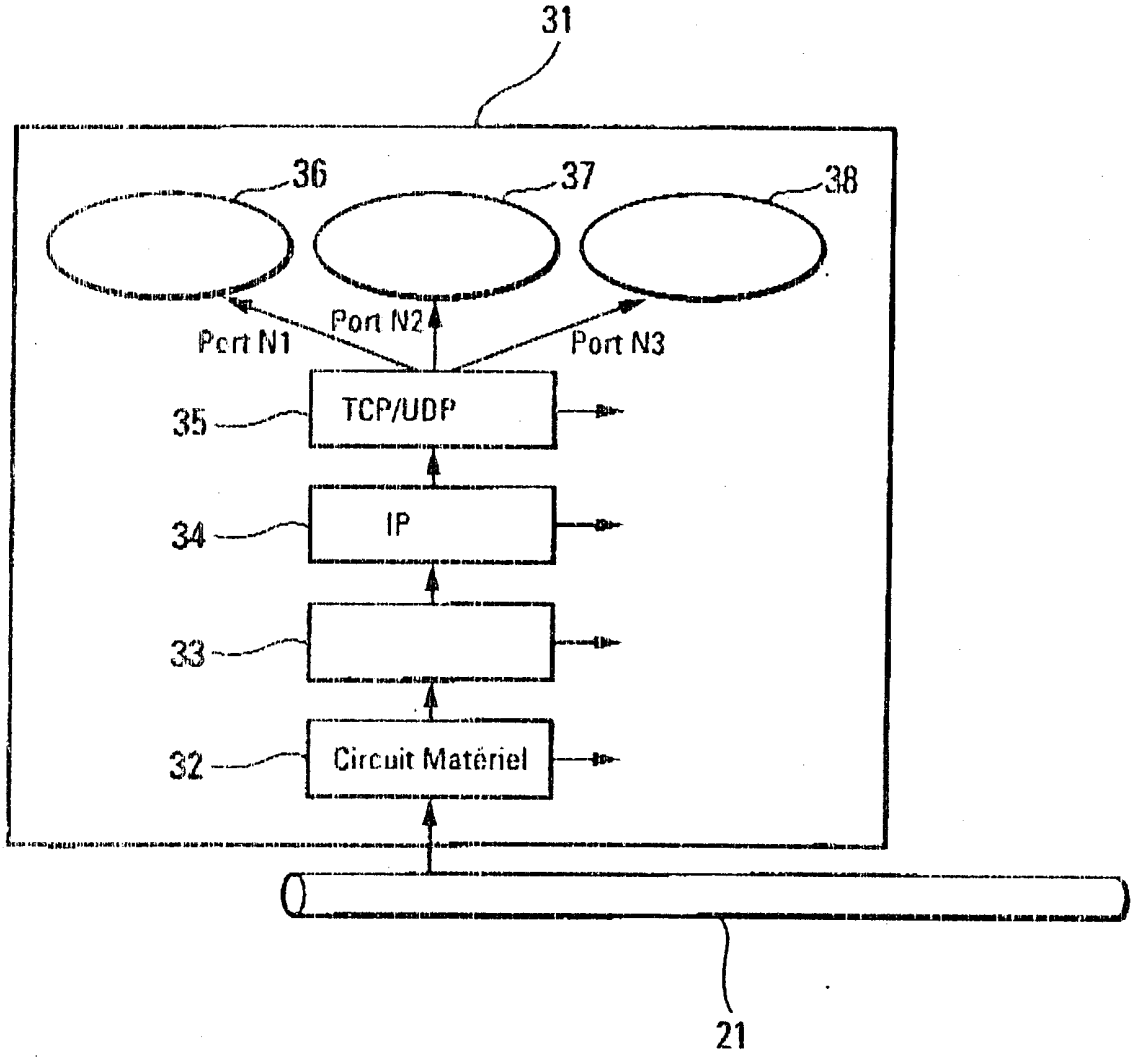
31
36
37
38
Port N1
Port N2
Port N3
35
TCP/UDP
34
IP
33
32
Circuit Matériel
21

Fig. 3

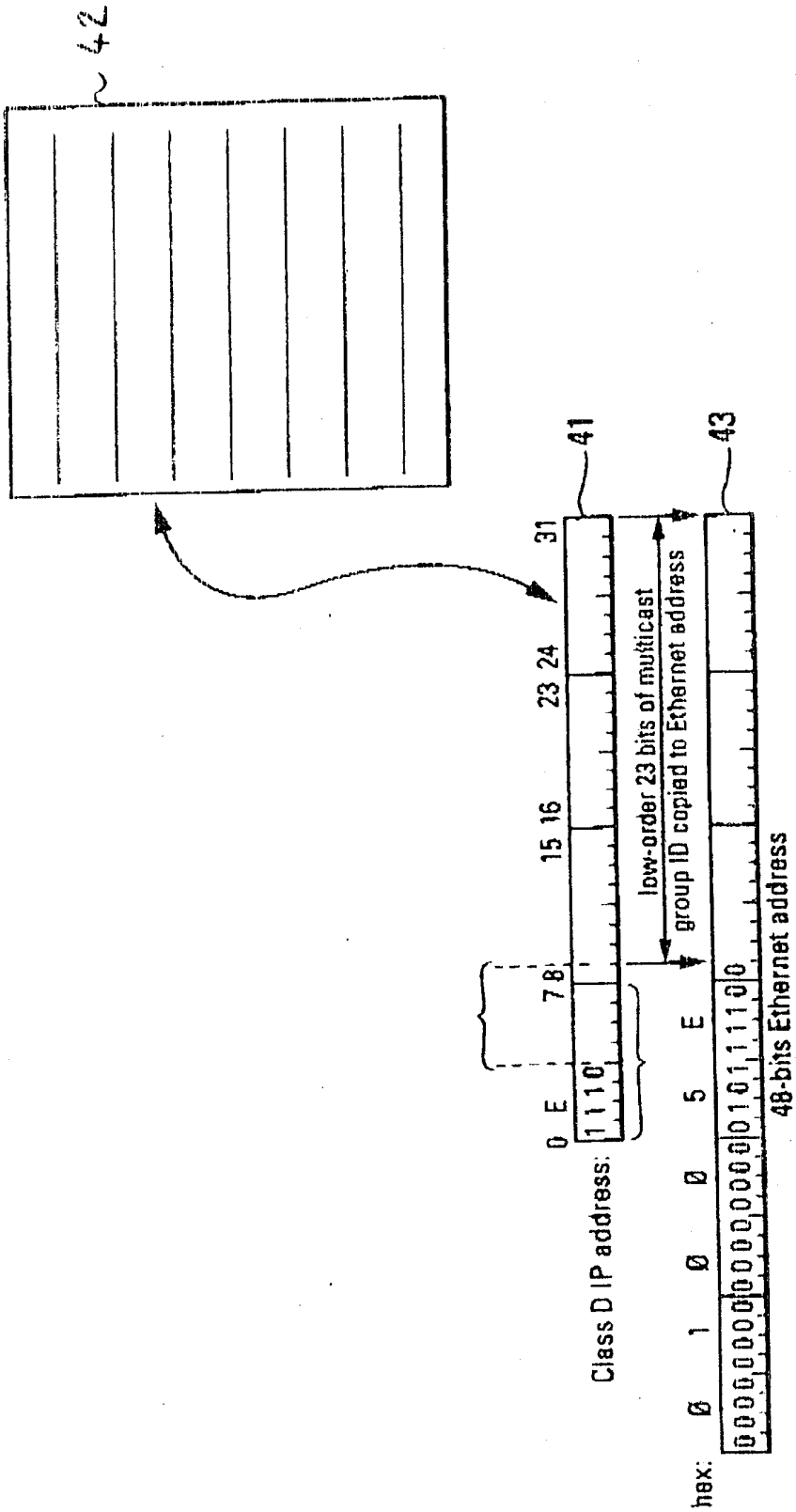
42
41
43
31
23 24
15 16
7 8
0 E
1 1 1 0
Class D IP address:
low-order 23 bits of multicast
group ID copied to Ethernet address
48-bits Ethernet address
hex:
0 1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 1 0 1 1 1 1 1 0

Fig 4

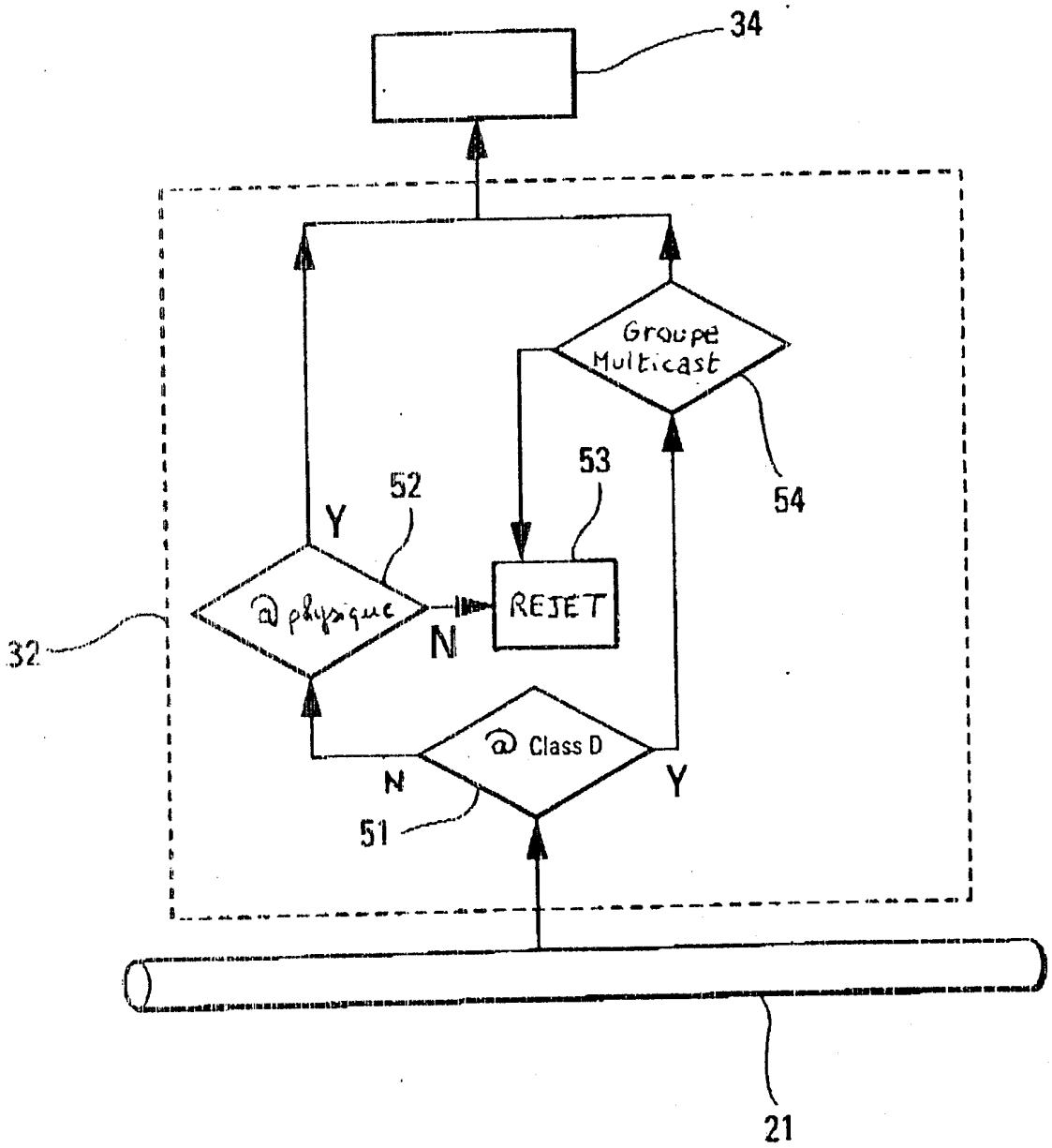
34
Groupe Multicast
54
53
52
Y
@ physique
N
REJET
32
@ Class D
N
Y
51
21

Fig. 5

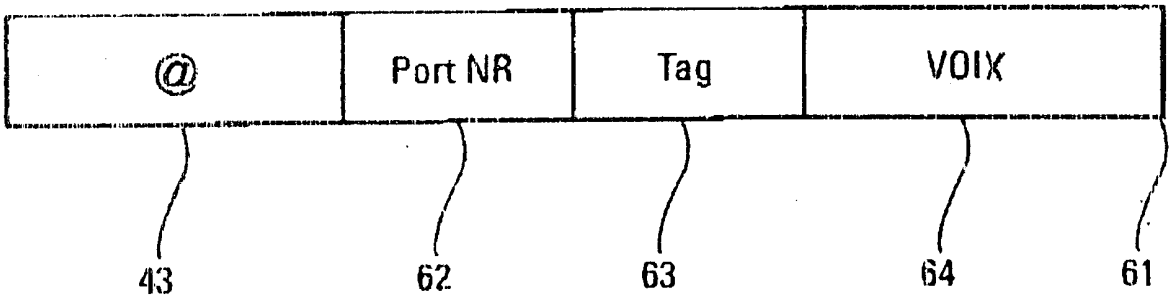

Fig. 6

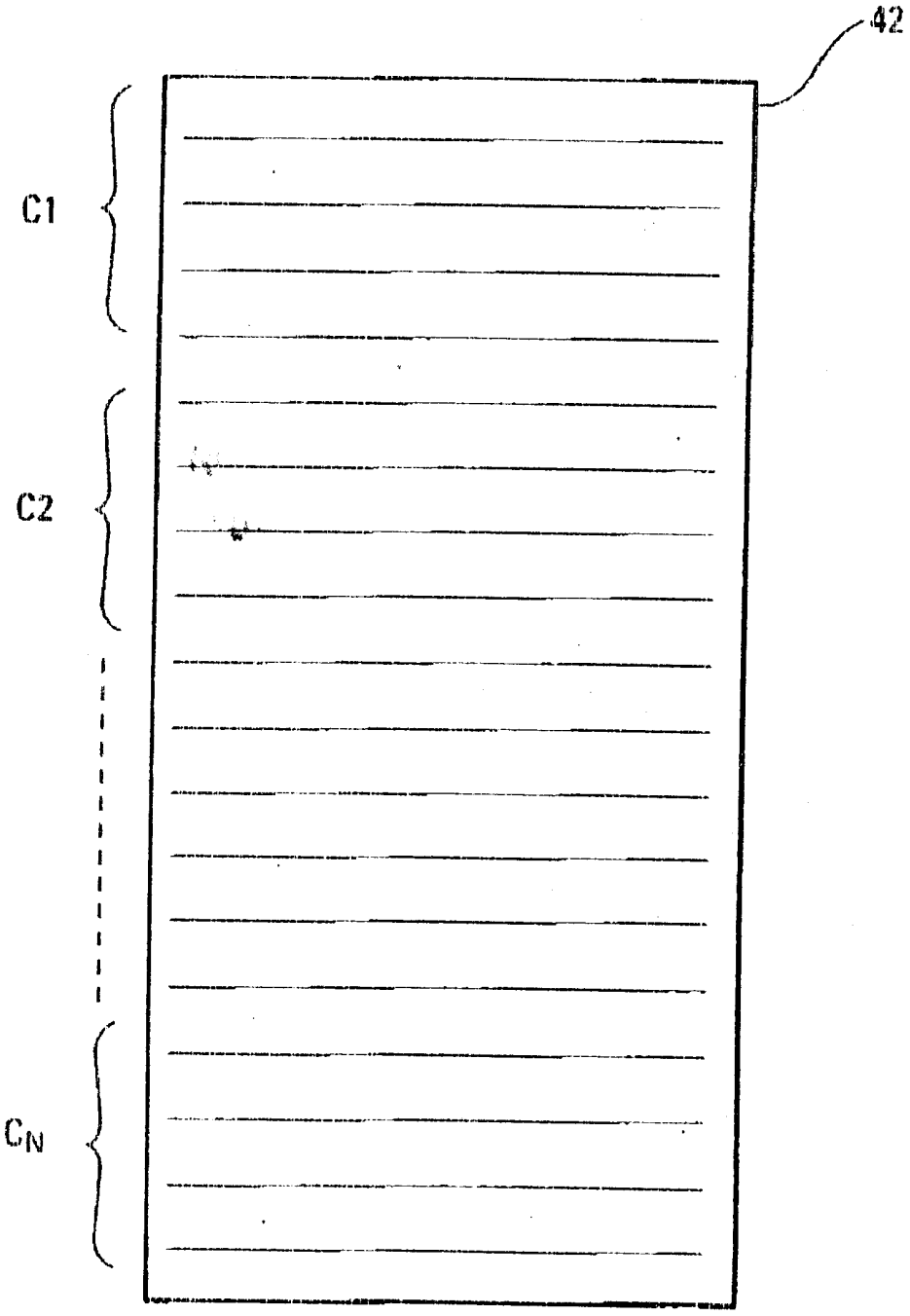

Fig. 7

ABREGE

Système de communications sécurisées,
comportant un réseau local par exemple du type Ethernet,
notamment embarqué dans un aéronef

La présente invention concerne un système de communications sécurisées comportant un réseau local, par exemple du type Ethernet.

Le système comporte au moins un réseau local et des terminaux connectés à ce réseau et échangeant des paquets de donnée. Chaque terminal comporte une table mémorisant les adresses des groupes de terminaux avec lesquels il peut entrer en communication. Un terminal qui émet un paquet de données sur le réseau en mode multicast crée une adresse réseau multicast (43) dont des bits, par exemple les octets de poids fort, ont une valeur donnée (01 00 5E) et qui comporte l'adresse (43) du groupe destinataire du paquet de données, chaque terminal comparant l'adresse du groupe destinataire avec le contenu de sa table une fois l'adresse réseau émise sur le réseau.

L'invention s'applique notamment pour les systèmes de communication multifonctions où il est nécessaire d'assurer un haut niveau de sécurité dans la transmission des données, comme c'est le cas par exemple pour certains systèmes embarqués dans des aéronefs.

Figure 4.

Numero de la demande nationale

Office européen des brevets

RAPPORT DE RECHERCHE

établi en vertu de l'article 21 § 1 et 2
de la loi belge sur les brevets d'invention
du 28 mars 1984

BO 8765
BE 200100837

DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie	Citation du document avec indication, en cas de besoin, des parties pertinentes	Revendication concernée	CLASSEMENT DE LA DEMANDE (Int.Cl.7)
	ABSENCE D'UNITE D'INVENTION voir feuille supplémentaire B		H04L12/18 H04L12/413
X	DEERING S: "HOST EXTENSIONS FOR IP MULTICASTING" INTERNET SPECIFICATION RFC, XX, XX, no. 1112, 1 août 1989 (1989-08-01), pages 1-17, XP002007299 * alinéas '07.2!-'07.4! *	1-8,15, 18,19	
X	US 6 061 350 A (MIN KYUNG PA) 9 mai 2000 (2000-05-09) * abrégé * * colonne 1, ligne 65 - colonne 3, ligne 47 *	1-8,15, 18,19	

DOMAINES TECHNIQUES RECHERCHES (Int.Cl.7)

H04L

Date d'achèvement de la recherche	Examinateur
22 août 2003	Goller, W

CATEGORIE DES DOCUMENTS CITES

X : particulièrement pertinent à lui seul
Y : particulièrement pertinent en combinaison avec un autre document de la même catégorie
A : arrière-plan technologique
O : divulgation non-écrite
P : document intercalaire

T : théorie ou principe à la base de l'invention
E : document de brevet antérieur, mais publié à la date de dépôt ou après cette date
D : cité dans la demande
L : cité pour d'autres raisons

& : membre de la même famille, document correspondant

EPO FORM 1503 03.82 (P04C48)

ABSENCE D'UNITÉ D'INVENTION
FEUILLE SUPPLÉMENTAIRE B

Numéro de la demande

BO 8765
BE 200100837

La division de la recherche estime que la présente demande de brevet ne satisfait pas à l'exigence relative à l'unité d'invention et concerne plusieurs inventions ou pluralités d'inventions, à savoir :

1. revendications: 1-8, 15 ,18, 19

   Configuration d'un terminal pour la réception des paquets multicast.

2. revendications: 9-11

   Séparation des données en plusieurs catégories par l'utilisation d'un tag.

3. revendications: 12-14, 17 (si dépendent des revendications 12-14)

   Stockage des adresses de groupe en fonction de leurs catégories.

4. revendications: 16, 17 (si dépendent de 16)

   Système multicast comportant des moyens de cryptage.

La recherche a été limitée au premier sujet.

ANNEXE AU RAPPORT DE RECHERCHE RELATIF A LA DEMANDE DE BREVET BELGE NO.

BO 8765
BE 200100837

La présente annexe indique les membres de la famille de brevets relatifs aux documents brevets cités dans le rapport de recherche visé ci-dessus.
Lesdits membres sont contenus au fichier informatique de l'Office européen des brevets à la date du
Les renseignements fournis sont donnés à titre indicatif et n'engagent pas la responsabilité de l'Office européen des brevets.

22-08-2003

Document brevet cité au rapport de recherche	Date de publication	Membre(s) de la famille de brevet(s)	Date de publication
US 6061350 A	09-05-2000	DE 19751270 A1	14-01-1999
		JF 2961531 B2	12-10-1999
		JP 11039238 A	12-02-1999