(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 1 337 985 B1

(12) **EUROPEAN PATENT SPECIFICATION**

(45) Date of publication and mention of the grant of the patent:
09.08.2006 Bulletin 2006/32

(21) Application number: **01998947.4**

(22) Date of filing: **29.11.2001**

(51) Int Cl.:
G08B 13/24 *(2006.01)* ***G08B 13/12*** *(2006.01)*

(86) International application number:
PCT/GB2001/005267

(87) International publication number:
WO 2002/045042 (06.06.2002 Gazette 2002/23)

(54) **Method of transferring the ownership of items using security tags**

Verfahren zum Eigentumstransfer durch Benutzung von Sicherheitsetitketten

Mèthode de transfer de la proprieté d'articles moyennant des etiquettes de securité

(84) Designated Contracting States:
AT BE CH CY DE DK ES FI FR GB GR IE IT LI LU MC NL PT SE TR
Designated Extension States:
AL LT LV MK RO SI

(30) Priority: **01.12.2000 GB 0029392**

(43) Date of publication of application:
27.08.2003 Bulletin 2003/35

(73) Proprietor: **De La Rue International Limited**
Basingstoke, Hampshire RG22 4BS (GB)

(72) Inventors:
- **IRELAND, Phillip Michael William**
  Rowlands Castle
  Hampshire PO9 6HE (GB)
- **BROOKS, David Alan**
  Waterloovville,
  Hants PO7 6SU (GB)
- **TRIBE, Raglan Horatio Andrew Harold**
  Rowlands Castle,
  Hants PO9 6DA (GB)
- **ARMANINI, Pietro**
  38060 Mattarello (TN) (IT)

(74) Representative: **Skone James, Robert Edmund**
Gill Jennings & Every LLP
Broadgate House
7 Eldon Street
London EC2M 7LH (GB)

(56) References cited:
WO-A-00/16284
US-A- 5 367 289
US-A- 5 650 770
US-A- 5 955 951
US-A- 6 002 343

EP 1 337 985 B1

Description

[0001] The present invention relates to a method of transferring the ownership of items using security tags.

[0002] Security tags are used commonly with articles of merchandise, particularly clothing and the like, to prevent unauthorised removal of such articles. These tags are usually securely connected to the items and an interrogation system is located at the exit to a retail store or the like which can detect the passage of a tag and initiate an alarm. Tags are also known for securing an article or item in place and providing an indication if the tag or the article becomes detached.

[0003] A variety of security tag systems are described in the prior art. WO-A-00/16284 describes a card to which a key can be securely attached via a tether which is electrically conductive so that its condition can be monitored when the card is fixed to a separate monitoring system. In another embodiment, the card is attached to a flexible bag having electrically conductive wires whose condition can be monitored so that an attempt to break into the bag can be detected. The drawback of this device is the need for permanent attachment to the monitoring system.

[0004] US-A-6002343 discloses an electronic tag which can be affixed to an object via a resistive element whose electrical resistivity is monitored by an on-board processor with information being transmitted to a separate detection system if the monitoring indicates that the resistive element has been compromised. This leads to a more flexible system than that described above but does not address attempts which may be made by sophisticated attackers to attack the tag itself.

[0005] US-A-5367289 discloses an electronic article surveillance tag which would typically be connected to clothing or the like and which includes a piezoelectric film which generates a voltage when subject to mechanical forces. The tag includes an alarm which is activated if the voltage exceeds a reference. This device has been developed to detect an attempt to detach the tag from the article but in fact achieves this by looking for the application of forces to the tag. The tag could be detached from the article without activating the alarm by carefully severing the connection to the article.

[0006] GB-A-2257278 describes an anti-pilferage tag including a microcircuit to enable data communication between the tag and a host computer. Although there is brief mention of some form of tamper detection, the prime purpose of the tag is to enable the location of stock to be monitored.

[0007] US-A-5099228 describes a security tag which can be attached to an article of merchandise by means of a tack and including a sensor for sensing the presence of the head of the tack. An attempt to tamper with the tack will therefore be detected.

[0008] US-A-5955951 discloses another type of tag/tack arrangement.

[0009] WO-A-98/15921 describes a security system for use at a transport terminal, the system including an electronic passenger tag including a memory and a wireless communication device, the memory storing a unique passenger identification code in a tamper proof manner; and an electronic luggage tag having a wire memory and a wireless communication device. In this way, the tags can be uniquely registered with one another.

[0010] US-A-6052068 describes a vehicle identification system including a set of vehicle identification tags which are attached to vehicles and which communicate with an interrogator to enable the vehicle identification to be determined.

[0011] WO00/16284 discloses an assembly in which a key is tethered to an associated key card. Means are provided to detect tampering with the tether.

[0012] US6002343 describes an electronic seal in which an electrically resistive element is electrically connected to a tag and bonded to an item. Tampering with the bonding is detected by a change in the electrical resistance.

[0013] There is a need to improve such security tags and we have developed a new security tag which in turn leads to novel methods of use for such a security tag.

[0014] In accordance with the invention we provide a method of transferring the ownership of item(s), the method comprising:

a. Securely identifying the item(s) by attaching a security tag to the item(s), the security tag comprising:

  a. A housing;
  b. A securing mechanism for securing the housing to the item(s);
  c. A monitoring system for monitoring a tag status, the tag status indicating at least whether the housing and the securing mechanism have been tampered with;
  d. A store for storing item data, the item data identifying the item(s); and,
  e. A communication system adapted to communicate the tag status and the item data to a remote host;

b. Detecting remotely the condition of the monitoring system; and

c. Causing the remote host to register a change in ownership of the item(s) when the monitoring system does not indicate a tamper condition.

[0015] We have realised that each security tag of the prior art suffers from one or more of a number of disadvantages and have devised a new security tag which overcomes all these disadvantages. In particular, the tag includes an on-board monitoring system so that tampering is detected immediately and not only when the tag is interrogated by a remote host; and in addition the monitoring system monitors not only the securing mechanism by which the tag is secured to an item but also the condition of the housing itself. Thus, all types of tampering

relating to the tag can be detected in contrast to the prior art.

[0016] In addition, where the item or a container enclosing the item is suitable, tampering of the item or container can also be monitored.

[0017] Although the tag could be remotely powered, for example from a main supply to a GSM/satellite module connected to the tag allowing long distance communication, in the preferred arrangement, the tag includes an on-board power supply. This provides another advantage of having an on-board monitoring system in that use of power from the power supply can be minimized. In addition, any external connection could provide an access point for any person trying to defeat the system. The tag when closed during manufacture would never be reopened unless for service or during attack. Being fully enclosed it makes the system much more resistant to any attack and removes any direct electrical connection to the internal components of the tag.

[0018] In use, if the monitoring system detects tampering, it can initiate a communication with a remote host via the communications system and typically this will include information about the tag status i.e. the fact that it is being tampered with as well as item data identifying the item concerned. The provision of an on-board monitoring system enables tampering to be detected at a very early stage and to be communicated with the remote host thus enabling remedial action to be taken as soon as possible. This makes the security tag particularly suitable for use with valuable item(s) such as articles of value including coins and banknotes.

[0019] Monitoring the condition of the housing provides an early indication of an attempt to tamper with the security tag which can be communicated to the remote host. This also prevents thieves from being able to damage the tag so as to stop the remote host from detecting that item(s) have been stolen. In one example, the housing can include a conductive portion with the monitoring system being adapted to monitor the electrical properties of the conductive portion to thereby determine the integrity of the housing. Thus, for example, if somebody pierces the housing in an attempt to destroy the internal workings of the security tag, then there will be a change in the electrical properties, such as the impedance, of the conductive portion which can be detected by the housing detector.

[0020] In an alternative example, the housing includes piezoelectric material and the monitoring system is adapted to monitor the electrical potential across the piezoelectric material to determine the integrity of the housing. Again, if somebody attempts to interfere with the housing this will generally cause vibrations which will in turn cause the piezoelectric material to generate a potential. This potential can be detected by the monitoring system so that again tampering with the housing is detected.

[0021] The monitoring system preferably includes an item detector to detect the integrity of the item(s). This may not be required however if the security tag is attached to a secure container, such as a safe, or the like.

[0022] Typically the item(s) are enclosed within a conductive enclosure in which case the item detector is adapted to monitor the electrical properties of the conductive enclosure to determine the integrity of the item (s). In this case, cash (coins and/or banknotes) could be placed for example in a bag in which wires are interwoven with the bag fabric. The conductivity of the bag would then be altered if an attempt was made to pierce the bag to extract the contents. Thus, this would allow the security tag to detect any attempt to remove item(s) from the bag.

[0023] Preferably the securing mechanism comprises a conductive member for securing the housing to the item (s). In this case, the monitoring system includes a mechanism detector adapted to monitor electrical properties of the conductive member to thereby determine the integrity of the securing mechanism.

[0024] The securing mechanism can include a piezoelectric material. In this case, the monitoring system may include a mechanism detector adapted to monitor the electrical potential across the piezoelectric material to determine the integrity of the securing mechanism.

[0025] As a further option, the securing mechanism could include a fine wire film, properties of which could be monitored by the monitoring system using a RF field applied to the film.

[0026] The securing mechanism usually includes an identification mark-up which can be associated with an indication of the item(s). This allows an additional amount of security to be provided.

[0027] The housing is usually formed from a tamper resistant material such as a lamination of rubber in a reinforced plastic as this is extremely difficult to tamper with. However, other high strength impact resistant materials can also be used.

[0028] In addition to this the housing usually includes a metal cage to protect at least the store, and also any other delicate electronic components. The metal cage will act as a Faraday cage to protect any delicate components included in the tag from EMP (electro magnetic pulse) attack.

[0029] The communication system may be any one of a number of communication systems, such as radio, infra-red, inductive or magnetic communication systems. Thus, for example, the communications system may comprises a Bluetooth type radio system. Alternatively inductive loop couplings may be provided so that when the security tag is brought in the vicinity of a reader, the tag status and some data can be read out from the store via an inductive loop.

[0030] Typically the communications system is adapted to encrypt the tag status and/or the item data prior to transfer to the remote host, for example using a PKI encryption system. This prevents third parties generating their own tag status and item data to mask the tag status of the genuine tag.

[0031] The communication system is preferably adapt-

ed to communicate with the remote host system on at least one of the following occasions:

i. At predetermined time intervals;
ii. Upon request from remote host systems; or,
iii. Upon a change in tag status indicating that the security tags and/or the item(s) have been tampered with.

[0032] It will be realised that a number of other options are available, such as allowing the communication system to communicate with the remote host every time it reaches a predetermined location, or only on one type of occasion (i-iii) mentioned above.

[0033] Conveniently, therefore, the security tag includes a location detector for detecting the location of the tag, the tag status including an indication of the tag location. This allows the location of the tag to be tracked as the item(s) are moved around.

[0034] Currently, if it is desired to transfer ownership of items from one party to another, it is necessary to actually physically move the items from the transferor to the transferee. This process can be subject to risk, particularly if the items have a high value, such as for example banknotes. Typically in these situations, the items are secured within a locked container which is then moved by a security company or the like under secure conditions.

[0035] In order to increase the security of such systems, the security companies typically use timed locks to ensure that the items cannot be removed from the container for a predetermined time interval. This may be achieved for example by locking the container in a security van in such a way that the container can only be removed at a predetermined point in time which corresponds to the time at which the driver will reach the desired destination.

[0036] In addition to this, it is now possible to track the location of the containers and the vans so that the current location of the container and hence the items can be monitored.

[0037] However, such systems suffer from the drawback that it is still possible for the items to be stolen whilst in transit. Thus, for example the container can be removed from the van forcibly, or alternatively the van can be stolen and the container removed at the correct time at a different location. Although the location of the container in the van can be tracked, it is still possible to remove the items from the container without this being detected, thereby allowing the items to be stolen.

[0038] The present invention recognises that once the item(s) have been secured, the ownership of the item(s) can be transferred even if the item(s) are not. In addition, the item(s) can be kept under less secure conditions.

[0039] Thus, for example, a shop owner may place money taken at the shop in a suitable container and then attach a security tag, as outlined above. At this point, the cash in the container is securely identified. Ownership of the contents of the container can then be transferred to the shop owner's bank, or the like, by registering a change in ownership at the remote host. From this point, the money is effectively owned by the bank which then has responsibility for the money. However, the container remains physically at the same location.

[0040] If at any stage the item(s) or the tag is tampered with then an indication of this can be transferred to the remote host, such as a central control centre, which can identify that there is a security problem. This provides the owners with full traceability of the current status of the item(s) so that the owners can be confident that the Item(s) are being transferred securely.

[0041] It will be realised that as soon as ownership of the money has been transferred, the money can be credited into the shop owner's bank account, allowing the shop owner to make transactions on the account in respect of the money which is still held on the premises. This is because the bank can account for the exact location and security of the money at all times.

[0042] Should the shop owner subsequently require cash from the bank, the shop owner can then simply arrange for ownership of the money to be transferred back, allowing the shop owner to retrieve the cash from the container in accordance with the bank's instructions. Accordingly, whilst the cash has been owned by the bank for a period of time, it has never left the shop premises. This therefore allows ownership of item(s) to be transferred without the item(s) themselves having to be moved which in turn helps reduce security risks.

[0043] The invention is particularly suitable for use with articles or documents of value such as banknotes and coins.

[0044] An example of the present invention will now be described with reference to the accompanying drawings, in which:-

Figure 1 is a plan view of a security tag for use with the present invention;
Figure 2 is a side view of the security tag of Figure 1;
Figure 3a is a cross-sectional view of the mounting of the security tag of Figure 1 along the line A-A';
Figure 3b is a cross-sectional view of the mounting of Figure 3a along the line B-B';
Figure 4 is a cross-sectional view of the security tag along the line C-C';
Figure 5 is a schematic diagram of the internal components of the security tag of Figure 1;
Figure 6 is a schematic diagram showing the security tag of Figure 1 attached to a solid container;
Figure 7 is a schematic diagram of the security tag of Figure 1 fitted to a fabric container; and,
Figure 8 illustrates a wrapped pack of banknotes attached to a security tag.

[0045] Figures 1 and 2 show a security tag for use with the present invention. As shown, the security tag includes a housing 1 with an attached mounting pad 2. The hous-

ing 1 may carry a security device such as a hologram or kinegram. Provided at respective locations around the perimeter of the housing 1 are four one shot fixings 3, such as rivets, or the like, which can be used on one occasion only to attach the housing 1 to a mounting plate 4. Also attached to the housing 1 is a mounting 5 which is adapted to receive an attaching member or clamp 6 as shown.

[0046] The mounting is shown in more detail in Figure 3a and 3b. Figure 3a shows a cross-section of the mounting along the line A-A' shown in Figure 2, whilst Figure 3b shows a cross-section of the mounting 5 along the line B-B' shown in Figure 1. The mounting includes two channels 7a, 7b each of which is designed to receive a respective arm 6a, 6b of the attaching member 6. Each channel 7a,7b includes a number of springs 8 which are designed to urge the arms 6a,6b of the attaching member 6 against the upper side of the respective channel. The shape of the springs is such that the arms 6a,6b are only able to move through the channels in the direction shown by the arrow 9.

[0047] Accordingly, in use the attaching member 6 may be inserted into the mounting 5 in the direction shown by the arrows 9. However, it is impossible to extract the attaching member 6 in the reverse direction. Accordingly, the attaching member 6 can only be removed from the mounting 5 by physically breaking the attaching member and then drawing each of the arms 6a,6b through the respective channels 7a,7b independently. As a result, the attaching member 6 can be used to attach the housing to fabric type objects, as will be explained in more detail below.

[0048] A cross-sectional view of the inside of the housing is shown in Figure 4. As shown, the housing is formed from a tough, anti-tamper laminated layer 10 formed from a lamination of rubber and high strength reinforced plastic which provides sufficient impact resistance to protect the internal components of the security tag even under extreme attack conditions.

[0049] Positioned inside the housing 1 is a printed circuit board (PCB) 11 on which are mounted the electronic components required to operate the tag. The PCB 11 is generally mounted in a layer of impact absorbing material 12 such as sponge, rubber or the like, to provide further impact resistance. In this example, a piezoelectric film 13 is positioned on the inside of the laminated layer 10, with a protective film 14 being positioned between the piezoelectric film 13 and the impact absorbing material 12.

[0050] A conductive external elastomeric coating may also be provided on the outside of the laminated layer 10, as shown by the dotted line 15.

[0051] Finally, a portion of the PCB 11 can also be contained within a metal can 16 which acts as a Faraday cage to protect the electronic components on the PCB from an EMP attack. It should be noted that in this case, sensors typically have to be located on the PCB 11 outside the metal can 16 in order to function correctly. Accordingly, surge arresting devices would be attached to these external sensors.

[0052] A schematic diagram showing the arrangement of the components mounted on the PCB 11 inside the housing 1 is shown in Figure 5. As shown, the security tag typically includes a microprocessor 20, a radio transceiver 21 and a store 22 coupled together via a bus 23. Also coupled to the bus 23 are a number of sensors 24. These components are all powered from an on-board power supply 27.

[0053] In this example, five sensors 24 are shown although, as will be appreciated from the description below, more sensors will be required in certain circumstances. Each of these sensors form part of a sensing system which is used to monitor the status of the security tag and the items to which the security tag is attached.

[0054] Signals detected by the sensors are transferred to the processor 20 which is adapted to monitor the signals and determine when these indicate that the security tag and/or the items are being tampered with. Sensitivity of the measurement is set to a level which prevents the processor 20 determining that normal handling constitutes tampering but low enough so that tampering can be detected before the security tag, items or the like, become damaged. This can be done in one of two ways:

i. By analysis of the signals; or,
ii. By comparing the signals to predetermined thresholds.

[0055] In the first example, the processor can be formed from a neural net. In this case, the neural net is trained under normal operating circumstances so that it learns what signals should be obtained from the sensors 24 when the security tags and items are being handled correctly. As a result, when signals outside the expected range are sensed then the processor determines that either the security tag or the items are being tampered with.

[0056] In the second example, an indication of the range of acceptable signals that should be obtained from each sensor 24 is stored in the memory 22. Accordingly the processor 20 can compare the obtained signals to the respective range of acceptable signals, and from this determine whether the items or security tag are being tampered with.

[0057] When any tampering is detected, the processor 20 is adapted to transfer a signal via the transceiver 21 to a remote monitoring system 26 indicating that the security tag or the items are under attack, as will be explained in more detail below.

[0058] In use, the security tag includes a large number of different security features which may be used separately or together in combination depending on the circumstances. The security features will now be explained below with reference to Figures 6 and 7.

[0059] Figure 6 shows how the security tag is connected to a sealed container 30. As shown, the security tag

is fitted to the body 32 of the container by placing the mounting pad 2 on a surface 31. The mounting pad 2 is formed from a tamper evident double sided adhesive pad which allows the housing 1 to be attached to the surface 31. The pad is designed so that if an attempt is made to remove the housing 1 from the surface 30, at least a portion of the pad will remain on the surface 30, whilst a corresponding portion will remain attached to the housing 1, thereby showing that a tag has been removed.

[0060] In addition to this (or optionally as an alternative), the one shot fixings 3 are inserted through the container body 30 and attached to the mounting plate 4 as shown, thereby securing the security tag in place.

[0061] An example of attaching the security tag to a fabric bag is shown in Figure 7. In this example, the fabric bag 40 is attached to the security tag using the attaching member 6. The attaching member 6 is wrapped around the neck of the bag 40 and then the arms 6a,6b are inserted into the mounting 5. The arms 6a and 6b are then pulled into the channels 7a,7b as far as possible thus preventing removal of the security tag from the fabric bag 40.

[0062] Operation of the security tag will now be described. The security tag includes 3 different types of sensing mechanism, namely:

i. A housing sensor system to check the integrity of the housing;
ii. An attachment sensor for checking the integrity of the attachment to the container; and,
iii. An item sensor for checking the integrity of the container containing the items.

[0063] Each of these will now be described below.

Housing Sensor

[0064] The housing sensor system is used to detect the integrity of the housing 1. This is carried out to prevent the security tag being tampered with to destroy the internal workings.

[0065] In a first example, the housing sensor system is formed from the piezoelectric film 13 and a corresponding one of the sensors 24. In this case, the sensor 24 is a current sensor, such as an ammeter or the like, which is adapted to detect electric currents generated in the piezoelectric film 13.

[0066] Accordingly, if the laminated layer 10 is deformed, for example by an attempt to crush or pierce the housing, this will cause corresponding deformation of the piezoelectric film 13. This will cause the generation of a current within the film which can be detected by the sensor 24.

[0067] As mentioned above, the sensor 24 is coupled to the processor 20 which monitors the signals obtained therefrom and determines whether these are representative of the housing being tampered with.

[0068] Thus, in general, a certain amount of current will be detected by the sensor 24 in normal operation, such as for example if the housing 1 is knocked during transit. However, if the current detected exceeds a threshold, and this is indicative of the fact that someone is attempting to open the housing 1, then this is detected by the processor 20 which causes a signal to be transferred via the transceiver 21.

[0069] In an alternative example, the sensor 24 can be adapted to measure the conductivity of the elastomeric coating 15. In general, the elastomeric coating will have a conductivity which can be measured by a sensor 24. This can be achieved for example by fabricating the sensor to apply a potential across the coating and to measure the current flow through the coating. The tag electrometric coating will contain a conductive compound such as graphite or compounds that consist of fine granules that can be added to the elastomer during compounding (manufacture). This coating can then be monitored in the same way as the strap. In this case, if the elastomeric coating 15 is interfered with, for example if it is pierced, this will change its conductivity, which will be detected by the processor 20 so that an appropriate response can be generated.

Attachment Sensor

[0070] The attachment sensor can be implemented in any one of a number of ways.

[0071] In a first example, a piezoelectric film (not shown) is sandwiched between the mounting pad 2 and the housing 1. Accordingly, if an attempt is made to remove the housing 1 from the surface 31 of a container, this will deform the piezo-electric film. The piezoelectric film will in turn generate a current which is detected by a current sensor 24.

[0072] Again, a certain amount of current generation is to be expected in normal use, for example due to movement during transit. However, if the generated current exceeds a threshold, this will be detected by the processor 20 which determines that an attempt has been made to remove the security tag from the container 30.

[0073] In a second example, the piezoelectric film is replaced by a capacitive film (not shown). The sensor 24 is then adapted to measure the capacitance of the film by applying an RF field to the film and measuring the response of current flow through the film. In this case, any variation in the capacitance indicates that the properties of the film are being effected, which in turn indicates that the coupling of the housing 1 to the container 30 is being tampered with.

[0074] Similar results could also be obtained by replacing the piezoelectric film in the mounting pad with either a conductive film, or a number of fine wires. In each case, the conductivity of the film or wires would be measured by an appropriate sensor 24.

[0075] In a third example, a sensor 24 is connected to the one shot fixings 3. In this case, the sensor 24 is used to monitor the electrical properties of the mounting plate

4. Thus, the system can operate to pass a current through the one shot fixings and hence through the mounting screws to allow the conductivity of the mounting plate 4 to be monitored.

[0076] This is preferably achieved by having the one shot fixings 3 form part of a transmission line with appropriate termination having the ability to change the capacitance and impedance as required. Once activated the tag will minimise the VSWR using a variable impedance and capacitive termination network allowing the tag to determine any alteration in the properties of the transmission line using an appropriate sensor 24.

[0077] In this example, if either the one shot fixings 3 or the mounting plate 4 are tampered with, a change in conductivity will be detected using the sensor 24 and again this will be signaled to the processor 20.

[0078] Finally, the attaching member 6 is generally formed from a conducting material. Accordingly, a sensor 24 is coupled to the channels 7a,7b to detect the conductivity of the attaching member. If the conductivity changes are more than a predetermined threshold amount, then this is detected by the microprocessor 20 which determines that the attaching member is being interfered with.

[0079] Again the attaching member 6 could be formed from a piezoelectric material which would then be coupled to an appropriate sensor 24.

Item Detection

[0080] Means for detecting whether the items have been disturbed can also be provided. In the case in which the security tag is attached to a metal container (for example as shown in Figure 6), the conductivity of the container can be measured using one of the sensors 24. Again, a change in conductivity can indicate that the container has been opened in which case this will be detected by the processor 20.

[0081] In the case of a fabric bag 40 (Figure 7) the fabric material can have conducting wires interwoven within the fabric. In this case, a sensor 24 can be attached to the fabric material via the conducting attaching member 6. The conductivity of the fabric can then be measured so that if the fabric is ripped in an attempt to extract items from the bag 40, this will be detected by the sensor 20.

[0082] Such a sensing technique could be improved by utilising two independent sets of wires which run in perpendicular directions. The conductivity of each set could be measured separately using two sensors 24, allowing variations that only effect the bag in a single direction to be detected.

[0083] Optionally, the items contained within either the container 30 or the bag 40 may have sensing means attached to them. This could take the form, for example, of part of a tuned inductive circuit. The first part of the inductive tuned circuit will consist of the sensor 24 whilst the second part will consist of suitable electronics attached to the item(s) within the container. Accordingly, the proximity of the two portions of the tuned circuit will affect the strength of a signal detected by the sensor 24 and relayed to the processor 20. This allows the processor to determine the proximity of the item(s) to the sensor 24 and hence determine if the item(s) are moved more than a predetermined distance from the security tag.

[0084] As a further option, piezoelectric films can be embedded in the packaging film of banded packs of banknotes 40 (Figure 8). The banding will be provided in two wide strips 41,42 extending about the middle of the long and short edges of the note respectively such that a single note cannot be removed without deforming the film, which can be detected by an appropriate sensor 24 of a tag 43 secured to the films, in a manner similar to those described above (Figure 6). Similar conductive techniques can be used and the security tag can be wired to the items as appropriate.

General Operation

[0085] In use, the security tag is attached either directly to an item of value or to a container 30 or bag 40 containing article(s) to be protected, in the manner described above.

[0086] Once this has been completed, details of the items to which the security tag is attached are supplied to the memory 22 of the security tag via the communications transceiver 21 from the host 26 or another input device (not shown). This can be achieved using, for example, a computing device such as a PDA, laptop, desktop computer, or the like, or a mobile communications device such as a WAP phone, depending on the nature of the communications transceiver.

[0087] In particular, if the transceiver is a Bluetooth piconet, a Bluetooth enabled PDA, WAP phone or the like, can be used to send a list of items to the memory 22 via the transceiver.

[0088] It is also possible to transfer an activation signal indicating to the processor 20 that it is to monitor the status of the sensors 24.

[0089] If at any time once the tag is activated the processor 20 determines that the signals from any one of the sensors 24 is outside the expected range, then the processor 20 determines that an attempt has been made to interfere with the item(s). Accordingly, the processor 20 generates an alarm signal which is transferred via the transceiver 21 to a remote control centre such as the host 26 or a security company, the police, a bank, or the like, which is responsible for the transfer of the money.

[0090] The alert signal is detected by the remote control centre which can determine that the items are being tampered with in some way.

[0091] In addition to this, the security tag may also send additional information, such as an indication of the sensor readings that are currently being obtained, thereby allowing the remote control centre to determine what is happening to the security tag.

[0092] Thus the security tag usually includes a location

sensor 24 which is capable of determining the location of the security tag. This would usually take the form of a GPS satellite navigation type sensor which is capable of pinpointing the location of the security tag and transferring an indication of this to the remote control centre with any alarm signal. This allows the remote control centre to determine the location of the security tag at the time the interference took place, as well as at other times.

[0093] As an additional level of security, the processor 20 can be adapted to periodically send a status signal to the remote host confirming the current status of each of the sensors. This can allow the remote control centre to make their own observations regarding the integrity of the system, including the security tag's current location. Alternatively, the remote host can poll the system and request that the information be transferred as required.

[0094] In addition to this, because details of the items associated with the security tag are stored in the memory 22 this can allow the remote host to determine the value of the associated items.

[0095] For additional security the transfer of information from the processor 20 to the remote host 26 via the transceiver 21 can involve the encryption of the data prior to transfer using a conventional PKI system. This prevents a third party intercepting the signals from the security tag and then transmitting their own signals which indicate that the tag has not been interfered with when the tag is in fact sending alarm signals.

[0096] It will be appreciated from this that the tag can be used to secure documents for both identification and transfer purposes. Accordingly, an additional feature of the present invention is that the security tag can be used to transfer ownership of documents such as, for example cash.

[0097] In this case, once the documents have been securely coupled to the tag, for example by placing in a suitable container and attaching the tag to the container, the user can enter details of the items into the memory 22 in the usual way. The owner can also enter a transfer code which causes ownership of the documents (e.g. banknotes) in the container to be transferred to a third party.

[0098] Upon entry of such a transfer code, the processor 20 transmits information to the remote control centre to allow the transfer to be registered centrally. From this point on the documents are effectively owned by the transferee.

[0099] Accordingly, the documents can be left in their current physical location in the knowledge that they cannot be tampered with or interfered with without the transferee's authorization to shut down the security tag. The items can then be transferred to a different physical location at a later date if necessary.

[0100] Thus for example a shopkeeper may wish to deposit cash in a bank. Accordingly, the shopkeeper would fill a suitable bag with cash, enter the value in the memory 22 and then transfer ownership of the cash to the bank, using the above described technique. The cash can actually be left on the shop premises as its location is known from the security tag. The cash can then be physically transferred to the bank at a later date.

[0101] Alternatively, if before the cash is transferred the shop then requires cash for some reason, for example to pay a supplier, it is possible for the bank to transfer ownership of the cash back to the shop owner. The shop owner can then validly deactivate the security tag and access the cash which has never left the shop premises. However despite this the cash has in fact been for a period of time deposited in the shop owner's bank account allowing the shop owner to make transactions using this cash which in fact remains on the premises.

Claims

1. A method of transferring the ownership of item(s), the method comprising:

   a. Securely identifying the item(s) by attaching a security tag to the item(s), the security tag comprising:

      a. A housing (1);
      b. A securing mechanism for securing the housing to the item(s);
      c. A monitoring system (13 , 24) for monitoring a tag status, the tag status indicating at least whether the housing and the securing mechanism have been tampered with;
      d. A score (22) for storing item data, the item data identifying the item(s); and,
      e. A communication system (21) adapted to communicate the tag status and the item data to a remote host;

   b. Detecting remotely the condition of the monitoring system; and
   c. Causing the remote host to register a change in ownership of the item(s) when the monitoring system does not indicate a tamper condition.

2. A method according to claim 1, wherein the security tag further comprises a power supply mounted on or in the housing.

3. A method according to claim 1 or claim 2, wherein the housing includes at least a conductive portion (13), and wherein the method further comprises using the monitoring system to monitor the electrical properties of the conductive portion to thereby determine the integrity of the housing.

4. A method according to any of claims 1 to 3, wherein the housing includes piezoelectric material and wherein the method further comprises using the monitoring system to monitor the electrical potential

across the piezoelectric material to determine the integrity of the housing.

5. A method according to any of the preceding claims, wherein the securing mechanism comprises a conductive member for securing the housing to the item (s), wherein the monitoring system includes a mechanism detector and wherein the method further comprises using the mechanism detector to monitor electrical properties of the conductive member to thereby determine the integrity of the securing mechanism.

6. A method according to any of the preceding claims, wherein the securing mechanism comprises a piezoelectric material, wherein the monitoring system includes a mechanism detector and wherein the method further comprises using the mechanism detector to monitor the electrical potential across the piezoelectric material to determine the integrity of the security mechanism.

7. A method according to any of the preceding claims, wherein the securing mechanism comprises a clamp member having a pair of arms (6a, 6b) which can be pushed into corresponding apertures in a mounting on the housing, and a lock system for preventing the clamp from being removed from the mounting, the method further comprising inserting the arms into the apertures and operating the lock system.

8. A method according to any of claims 1 to 6, wherein the securing mechanism comprises an electrically conductive member, to which the housing is connected with part of an item or a container for the item sandwiched therebetween, the conductive member forming part of a transmission line and wherein the impedance of the transmission line is monitored.

9. A method according to any of the preceding claims, wherein the housing is formed from a tamper resistant material such as a lamination of rubber and reinforced plastic.

10. A method according to any of the preceding claims, wherein the housing includes a Faraday cage to protect at least the store.

11. A method according to any of the preceding claims, wherein the communication system (21) operates by one of radio, infra-red, inductive, or magnetic communications.

12. A method according to any of the preceding claims, wherein the communications system (21) encrypts the tag status and/or the item data prior to transfer to the remote host.

13. A method according to any of the preceding claims, wherein the communication system (21) communicates with the remote host on at least one of the following occasions:

i. At predetermined time intervals
ii. upon request from the remote host; or,
iii. Upon a change in tag status indicating that the security tag and/or the item(s) have been tampered with.

14. A method according to any of the preceding claims, wherein the monitoring system includes a location detector, the method further comprising detecting the location of the tag with the location detector, the tag status including an indication of the tag location.

15. A method according to any of the preceding claims, wherein the monitoring system includes an item detector, the method further comprising detecting the integrity of the item(s) using the item detector.

16. A method according to claim 15 wherein the tag is attached to a conductive enclosure (40), and wherein the item detector monitors the electrical properties of the conductive enclosure to thereby determine the integrity of the enclosure.

17. A method according to claim 1, wherein the item(s) are not physically transferred between owners in step (c).

18. A method according to claims 17 or 18, wherein the item(s) comprises an article of value such as a banknote and/or coin.

19. A method according to claim 18, wherein the item(s) is securely located in a container to which the security tag is attached.

20. A method according to claim 18, wherein the security tag is attached to a wrapper located about a stack of banknotes.

Patentansprüche

1. Verfahren zum Übertragen des Eigentumsrechts von einem oder mehreren Gegenständen, wobei das Verfahren folgendes umfaßt:

a. sicheres Identifizieren des oder der Gegenstände durch Anbringen eines Sicherheitstags an dem oder den Gegenständen, wobei das Sicherheitstag folgendes umfaßt:

a. ein Gehäuse (1);
b. einen Befestigungsmechanismus zum Befestigen des Gehäuses an dem oder den

Gegenständen;
c. ein Überwachungssystem (13, 24) zum Überwachen eines Tagstatus, wobei der Tagstatus zumindest anzeigt, ob das Gehäuse und der Befestigungsmechanismus manipuliert worden sind;
d. einen Speicher (22) zum Speichern von Gegenstandsdaten, wobei die Gegenstandsdaten den oder die Gegenstände identifizieren; und
e. ein Kommunikationssystem (21), das dafür ausgelegt ist, den Tagstatus und die Gegenstandsdaten an einen abgesetzten Host zu übertragen;

b. abgesetztes Detektieren des Zustands des Überwachungssystems; und
c. Bewirken, daß der abgesetzte Host eine Änderung beim Eigentumsrecht des oder der Gegenstände registriert, wenn das Überwachungssystem keinen Manipulationszustand anzeigt.

2. Verfahren nach Anspruch 1, wobei der Sicherheitstag weiterhin eine an oder in dem Gehäuse montierte Stromversorgung umfaßt.

3. Verfahren nach Anspruch 1 oder 2, wobei das Gehäuse mindestens einen leitenden Abschnitt (13) enthält und wobei das Verfahren weiterhin die Verwendung des Überwachungssystems zum Überwachen der elektrischen Eigenschaften des leitenden Abschnitts umfaßt, um dadurch die Integrität des Gehäuses zu bestimmen.

4. Verfahren nach einem der Ansprüche 1 bis 3, wobei das Gehäuse ein piezoelektrisches Material enthält und wobei das Verfahren weiterhin die Verwendung des Überwachungssystems zum Überwachen des elektrischen Potentials am piezoelektrischen Material zum Bestimmen der Integrität des Gehäuses umfaßt.

5. Verfahren nach einem der vorhergehenden Ansprüche, wobei der Befestigungsmechanismus ein leitendes Glied umfaßt zum Befestigen des Gehäuses an dem oder den Gegenständen, wobei das Überwachungssystem einen Mechanismusdetektor enthält und wobei das Verfahren weiterhin die Verwendung des Mechanismusdetektors umfaßt zum Überwachen der elektrischen Eigenschaften des leitenden Glieds, um dadurch die Integrität des Befestigungsmechanismus zu bestimmen.

6. Verfahren nach einem der vorhergehenden Ansprüche, wobei der Befestigungsmechanismus ein piezoelektrisches Material umfaßt, wobei das Überwachungssystem einen Mechanismusdetektor enthält und wobei das Verfahren weiterhin die Verwendung des Mechanismusdetektors umfaßt zum Überwachen der elektrischen Eigenschaften am piezoelektrischen Material, um die Integrität des Befestigungsmechanismus zu bestimmen.

7. Verfahren nach einem der vorhergehenden Ansprüche, wobei der Befestigungsmechanismus ein Klemmglied mit einem Paar Arme (6a, 6b) umfaßt, die in entsprechende Öffnungen in einer Fassung an dem Gehäuse geschoben werden können, und ein Verriegelungssystem, um zu verhindern, daß die Klemme aus der Fassung entfernt wird, wobei das Verfahren weiterhin das Einführen der Arme in die Öffnungen und Betätigen des Verriegelungssystems umfaßt.

8. Verfahren nach einem der Ansprüche 1 bis 6, wobei der Befestigungsmechanismus ein elektrisch leitendes Glied umfaßt, mit dem das Gehäuse verbunden ist, wobei Teil eines Gegenstands oder eines Behälters für den Gegenstand dazwischen geschichtet ist, wobei das leitende Glied Teil einer Übertragungsleitung bildet und wobei die Impedanz der Übertragungsleitung überwacht wird.

9. Verfahren nach einem der vorhergehenden Ansprüche, wobei das Gehäuse aus einem manipulationsbeständigen Material wie etwa einer Laminierung aus Kautschuk und verstärktem Kunststoff ausgebildet ist.

10. Verfahren nach einem der vorhergehenden Ansprüche, wobei das Gehäuse einen Faraday-Käfig enthält, um zumindest den Speicher zu schützen.

11. Verfahren nach einem der vorhergehenden Ansprüche, wobei das Kommunikationssystem (21) über Funk-, Infrarot-, induktive oder magnetische Kommunikation arbeitet.

12. Verfahren nach einem der vorhergehenden Ansprüche, wobei das Kommunikationssystem (21) den Tagstatus und/oder die Gegenstandsdaten vor der Übertragung zu dem abgesetzten Host verschlüsselt.

13. Verfahren nach einem der vorhergehenden Ansprüche, wobei das Kommunikationssystem (21) mit dem abgesetzten Host bei zumindest einer der folgenden Gelegenheiten kommuniziert:

i. in vorbestimmten Zeitintervallen
ii. bei Anforderung von dem abgesetzten Host oder
iii. bei einer Änderung im Tagstatus, die anzeigt, daß das Sicherheitstag und/oder der oder die Gegenstände manipuliert worden sind.

14. Verfahren nach einem der vorhergehenden Ansprüche, wobei das Überwachungssystem einen Positionsdetektor enthält, wobei das Verfahren weiterhin das Detektieren der Position des Tags mit dem Positionsdetektor umfaßt, wobei der Tagstatus eine Anzeige der Tagposition enthält.

15. Verfahren nach einem der vorhergehenden Ansprüche, wobei das Überwachungssystem einen Gegenstandsdetektor enthält, wobei das Verfahren weiterhin das Detektieren der Integrität des oder der Gegenstände unter Verwendung des Gegenstandsdetektors umfaßt.

16. Verfahren nach Anspruch 15, wobei das Tag an einer leitenden Hülle (40) angebracht ist und wobei der Gegenstandsdetektor die elektrischen Eigenschaften der leitenden Hülle überwacht, um dadurch die Integrität der Hülle zu bestimmen.

17. Verfahren nach Anspruch 1, wobei der oder die Gegenstände im Schritt (c) nicht physisch zwischen Eigentümern übertragen werden.

18. Verfahren nach Anspruch 17 oder 18, wobei der oder die Gegenstände einen Wertartikel wie etwa eine Banknote und/oder Münze umfassen.

19. Verfahren nach Anspruch 18, wobei sich der oder die Gegenstände sicher in einem Behälter befinden, an den das Sicherheitstag angebracht ist.

20. Verfahren nach Anspruch 18, wobei das Sicherheitstag an einer Banderole angebracht ist, die sich um einen Stapel von Banknoten herum befindet.

Revendications

1. Procédé de transfert de la propriété d'article(s), le procédé comprenant les étapes consistant à :

a. Identifier en toute sécurité l'(les) article(s) en attachant une étiquette de sécurité à l'(aux) article(s), l'étiquette de sécurité comprenant :

a. Un logement (1) ;
b. Un mécanisme de fixation destiné à fixer le logement à l'(aux) article(s) ;
c. Un système de surveillance (13, 24) destiné à surveiller un état d'étiquette, l'état d'étiquette indiquant au moins si le logement et le mécanisme de fixation ont été altérés ;
d. Une réserve (22) destinée à stocker des données d'article, les données d'article identifiant l'(les) article(s) ; et
e. Un système de communication (21) adapté pour communiquer l'état d'étiquette et les données d'article à un hôte éloigné ;

b. Détecter à distance la condition du système de surveillance ; et
c. Amener l'hôte éloigné à enregistrer un changement de propriété de 1'(des) article(s) lorsque le système de surveillance n'indique pas une condition d'altération.

2. Procédé selon la revendication 1, dans lequel l'étiquette de sécurité comprend en outre une alimentation électrique montée sur ou dans le logement.

3. Procédé selon la revendication 1 ou la revendication 2, dans lequel le logement comprend au moins une portion conductrice (13), et dans lequel le procédé comprend en outre l'étape consistant à utiliser le système de surveillance pour surveiller les propriétés électriques de la portion conductrice pour déterminer ainsi l'intégrité du logement.

4. Procédé selon l'une quelconque des revendications 1 à 3, dans lequel le logement comprend un matériau piézoélectrique et dans lequel le procédé comprend en outre l'étape consistant à utiliser le système de surveillance pour surveiller le potentiel électrique aux bornes du matériau piézoélectrique pour déterminer l'intégrité du logement.

5. Procédé selon l'une quelconque des revendications précédentes, dans lequel le mécanisme de fixation comprend un organe conducteur destiné à fixer le logement à l' (aux) article(s), dans lequel le système de surveillance comprend un détecteur de mécanisme et dans lequel le procédé comprend en outre l'étape consistant à utiliser le détecteur de mécanisme pour surveiller les propriétés électriques de l'organe conducteur pour déterminer ainsi l'intégrité du mécanisme de fixation.

6. Procédé selon l'une quelconque des revendications précédentes, dans lequel le mécanisme de fixation comprend un matériau piézoélectrique, dans lequel le système de surveillance comprend un détecteur de mécanisme et dans lequel le procédé comprend en outre l'étape consistant à utiliser le détecteur de mécanisme pour surveiller le potentiel électrique aux bornes du matériau piézoélectrique pour déterminer l'intégrité du mécanisme de sécurité.

7. Procédé selon l'une quelconque des revendications précédentes, dans lequel le mécanisme de fixation comprend un organe de serrage ayant une paire de bras (6a, 6b) qui peuvent être poussés dans des ouvertures correspondantes dans un montage sur le logement, et un système de verrouillage destiné à empêcher l'attache (organe de serrage) d'être éli-

minée du montage, le procédé comprenant en outre les étapes consistant à insérer les bras dans les ouvertures et mettre en oeuvre le système de verrouillage.

8. Procédé selon l'une quelconque des revendications 1 à 6, dans lequel le mécanisme de fixation comprend un organe électriquement conducteur, auquel le logement est connecté avec une partie d'un article ou un conteneur pour l'article pris en sandwich entre eux, l'organe conducteur faisant partie d'une ligne de transmission et dans lequel l'impédance de la ligne de transmission est surveillée.

9. Procédé selon l'une quelconque des revendications précédentes, dans lequel le logement est formé à partir d'un matériau résistant à l'altération tel qu'un stratifié de caoutchouc et de matière plastique renforcée.

10. Procédé selon l'une quelconque des revendications précédentes, dans lequel le logement comprend une cage de Faraday pour protéger au moins la réserve.

11. Procédé selon l'une quelconque des revendications précédentes, dans lequel le système de communication (21) fonctionne par l'une des communications radio, infrarouge, inductrice ou magnétique.

12. Procédé selon l'une quelconque des revendications précédentes, dans lequel le système de communication (21) chiffre l'état d'étiquette et/ou les données d'article avant le transfert à l'hôte éloigné.

13. Procédé selon l'une quelconque des revendications précédentes, dans lequel le système de communication (21) communique avec l'hôte éloigné à au moins l'une des occasions suivantes :

i. A des intervalles de temps prédéterminés
ii. Lors d'une requête de l'hôte éloigné ; ou
iii. Lors d'un changement en état d'étiquette indiquant que l'étiquette de sécurité et/ou l'(les) article(s) a (ont) été altéré(s).

14. Procédé selon l'une quelconque des revendications précédentes, dans lequel le système de surveillance comprend un détecteur d'emplacement, le procédé comprenant en outre l'étape consistant en détecter l'emplacement de l'étiquette avec le détecteur d'emplacement, l'état d'étiquette comprenant une indication de l'emplacement d'étiquette.

15. Procédé selon l'une quelconque des revendications précédentes, dans lequel le système de surveillance comprend un détecteur d'article, le procédé comprenant en outre l'étape consistant en détecter l'intégrité du (des) article(s) utilisant le détecteur d'article.

16. Procédé selon la revendication 15, dans lequel l'étiquette est attachée à une gaine conductrice (40), et dans lequel le détecteur d'article surveille les propriétés électriques de la gaine conductrice pour déterminer ainsi l'intégrité de la gaine.

17. Procédé selon la revendication 1, dans lequel l'(les) article(s) ne sont pas physiquement transférés entre les propriétaires dans l'étape (c).

18. Procédé selon la revendication 17 ou 18, dans lequel l'(les) article(s) comprend (comprennent) un article de valeur tel qu'un billet de banque et/ou une pièce de monnaie.

19. Procédé selon la revendication 18, dans lequel l'(les) article(s) est (sont) situé(s) en toute sécurité dans un conteneur sur lequel est attachée l'étiquette de sécurité.

20. Procédé selon la revendication 18, dans lequel l'étiquette de sécurité est attachée à un emballage situé autour d'une pile de billets de banque.

Fig.1.

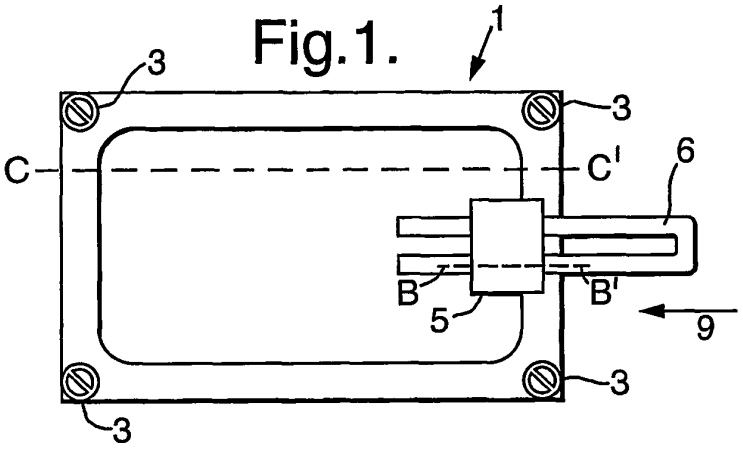

Fig.2.

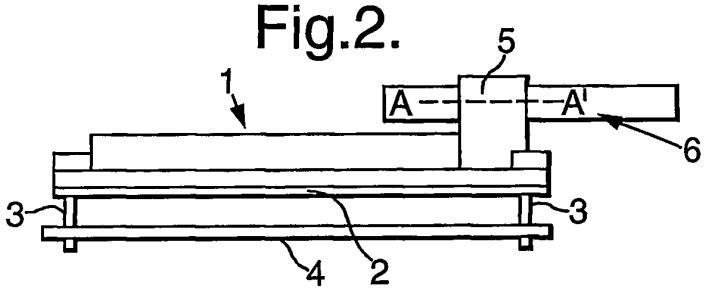

Fig.3a.

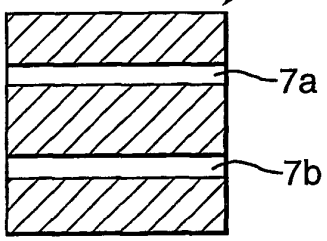

Fig.3b.

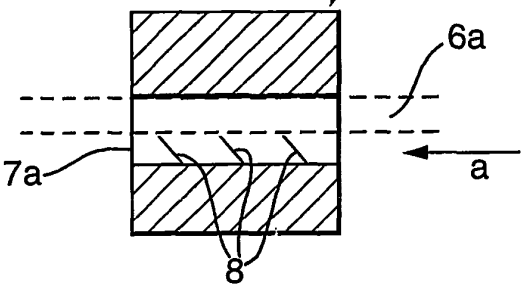

Fig.4.

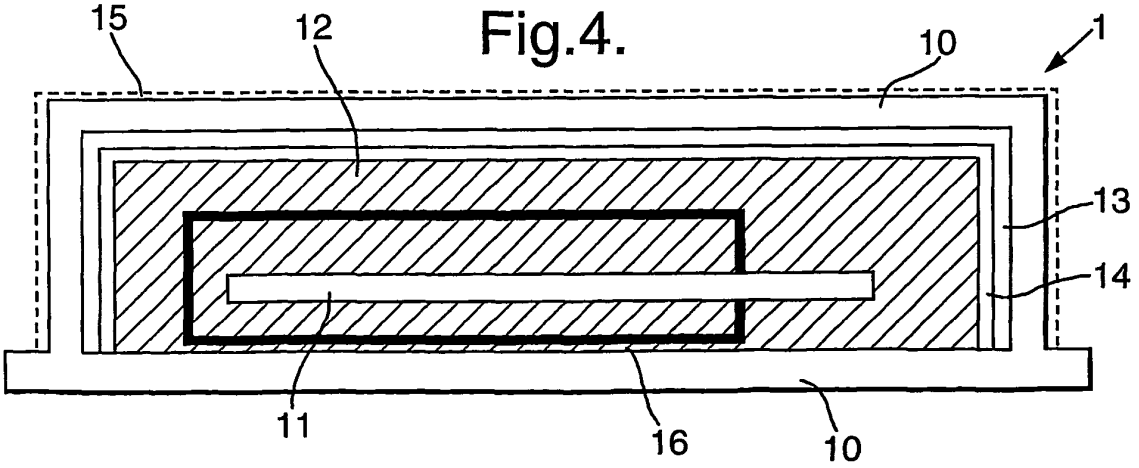

Fig.5.

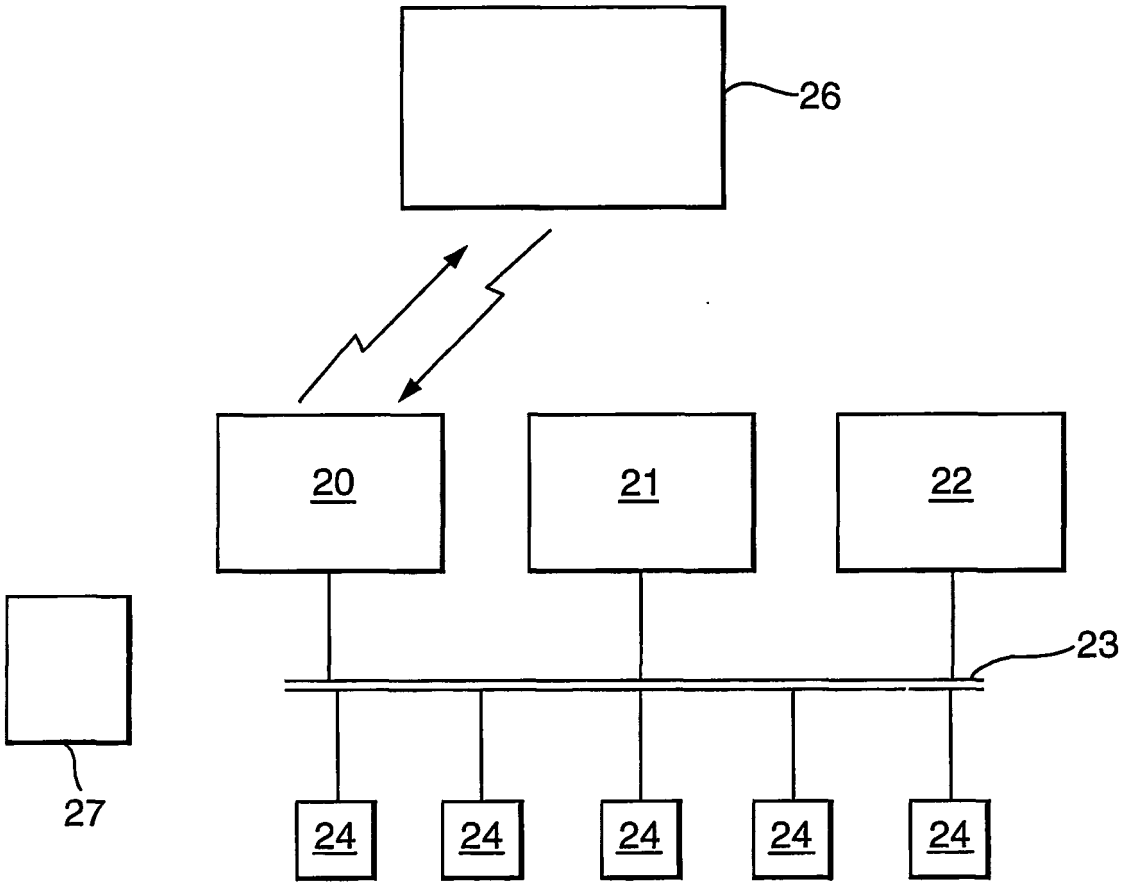

Fig.8.

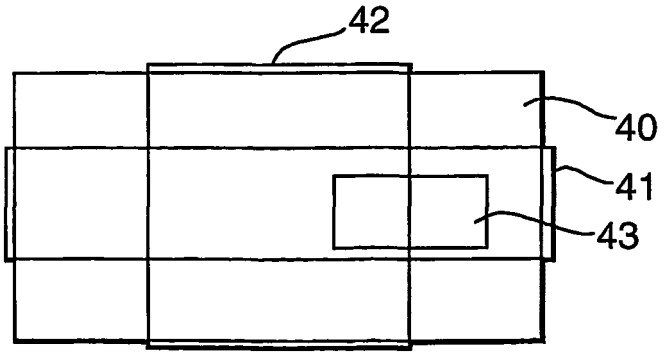

Fig.6.

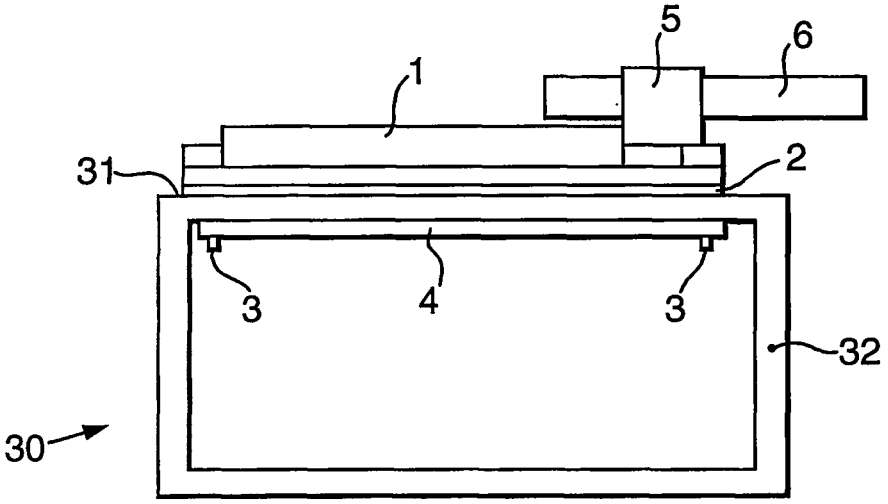

Fig.7.