US00RE43415E

(19) **United States**

(12) **Reissued Patent**

Tuttle

(10) **Patent Number: US RE43,415 E**

(45) **Date of Reissued Patent: *May 29, 2012**

(54) **ANTI-THEFT METHOD FOR DETECTING THE UNAUTHORIZED OPENING OF CONTAINERS AND BAGGAGE**

(75) Inventor: **John R. Tuttle**, Longmont, CO (US)

(73) Assignee: **Round Rock Research, LLC**, Mt. Kisco, NY (US)

(*) Notice: This patent is subject to a terminal disclaimer.

(21) Appl. No.: **12/038,473**

(22) Filed: **Feb. 27, 2008**

Related U.S. Patent Documents

Reissue of:

(64) Patent No.: **5,831,531**
Issued: **Nov. 3, 1998**
Appl. No.: **08/827,037**
Filed: **Mar. 25, 1997**

U.S. Applications:

(63) Continuation of application No. 08/421,571, filed on Apr. 11, 1995, now Pat. No. 5,646,592, which is a continuation of application No. 08/151,599, filed on Nov. 12, 1993, now Pat. No. 5,406,263, which is a continuation-in-part of application No. 07/921,037, filed on Jul. 27, 1992, now abandoned.

(51) **Int. Cl.**

G08B 13/14	(2006.01)
G08B 21/00	(2006.01)
A45C 13/18	(2006.01)
A45C 13/10	(2006.01)

(52) **U.S. Cl.** **340/572.1**; 340/572.7; 340/686.1; 340/540; 340/541; 340/652; 190/101; 190/120

(58) **Field of Classification Search** 340/568.1, 340/568.2, 568.6, 568.7, 571, 572.1, 572.8, 340/572.9, 686.1; 190/101, 102, 119, 120

See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

3,426,166	A	2/1969	Canceill
4,117,468	A	9/1978	Vasquez

(Continued)

OTHER PUBLICATIONS

Tuttle, John, U.S. Appl. No. 07/921,037; "Anti-Theft Method for Detecting the Unauthorized Opening of Containers and Baggage", filed Jul. 27, 1992, now abandoned.

(Continued)

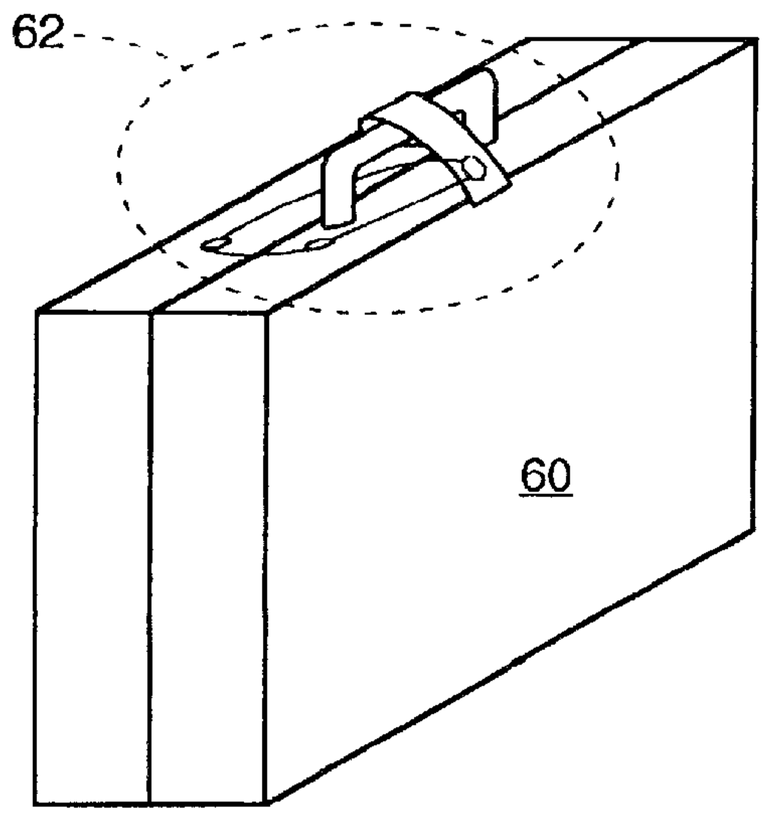
Primary Examiner — Jennifer Mehmood

(74) *Attorney, Agent, or Firm* — Lerner, David, Littenberg, Krumholz & Mentlik LLP

(57) **ABSTRACT**

A simple trip-wire or magnetic circuit associated with a shipping container provides continuity, which is detected electrically. Simply, if continuity is disabled by a forced entry of the container, electrical detection means, such as a radio-frequency-identification (RFID) tag, will alert the owner or monitoring station. The trip-wire concept would require the replacing of a broken trip wire (resulting from forced entry), while the magnetic circuit concept can be reused repetitively. In a second embodiment a magnetic circuit and the detection device (RFID tag) are embedded into the shipping article during manufacturing. The preferred detection device, an RFID tag, could also be a battery backed transceiver type on which a replaceable or rechargeable battery could be mounted on the inside of the shipping container during manufacturing. The RFID tag would communicate with an interrogator unit, which could be connected to a host computer. The interrogator and/or the host computer and/or other alarm devices would then monitor the shipping container's status (opened or closed).

68 Claims, 8 Drawing Sheets



U.S. PATENT DOCUMENTS

4,155,079	A	*	5/1979	Chiu et al.	340/571
4,262,284	A		4/1981	Stieff et al.	
4,591,835	A	*	5/1986	Sharp	340/574
4,684,929	A		8/1987	Edwards et al.	
4,908,606	A	*	3/1990	Kevonian	340/571
5,099,228	A	*	3/1992	Israel et al.	340/572.1
5,111,184	A		5/1992	Heaton et al.	
5,126,719	A		6/1992	De Sorbo	
5,169,188	A		12/1992	Kupperman et al.	
5,189,396	A		2/1993	Stobbe	
5,396,218	A		3/1995	Olah	
5,406,263	A		4/1995	Tuttle	
5,510,768	A	*	4/1996	Mann	340/571
5,646,592	A		7/1997	Tuttle	
5,831,531	A		11/1998	Tuttle	

OTHER PUBLICATIONS

Tuttle, John, U.S. Appl. No. 12/057,270; "Anti-Theft Method for Detecting the Unauthorized Opening of Containers and Baggage", filed Mar. 27, 2008.

USPTO Transaction History of U.S. Appl. No. 07/921,037, filed Jul. 27, 1992, entitled "Anti-Theft Method for Detecting the Unauthorized Opening of Containers and Baggage," now abandoned.

USPTO Transaction History of U.S. Appl. No. 08/151,599, filed Nov. 12, 1993, entitled "Anti-Theft Method for Detecting the Unauthorized Opening of Containers and Baggage," now U.S. Pat. No. 5,406,263.

USPTO Transaction History of U.S. Appl. No. 08/421,571, filed Apr. 11, 1995, entitled "Anti-Theft Method for Detecting the Unauthorized Opening of Containers and Baggage," now U.S. Pat. No. 5,646,592.

USPTO Transaction History of U.S. Appl. No. 08/827,037, filed Mar. 25, 1997, entitled "Anti-Theft Method for Detecting the Unauthorized Opening of Containers and Baggage," now U.S. Pat. No. 5,831,531.

USPTO Transaction History of U.S. Appl. No. 12/057,270, filed Mar. 27, 2008, entitled "Anti-Theft Method for Detecting the Unauthorized Opening of Containers and Baggage."

* cited by examiner

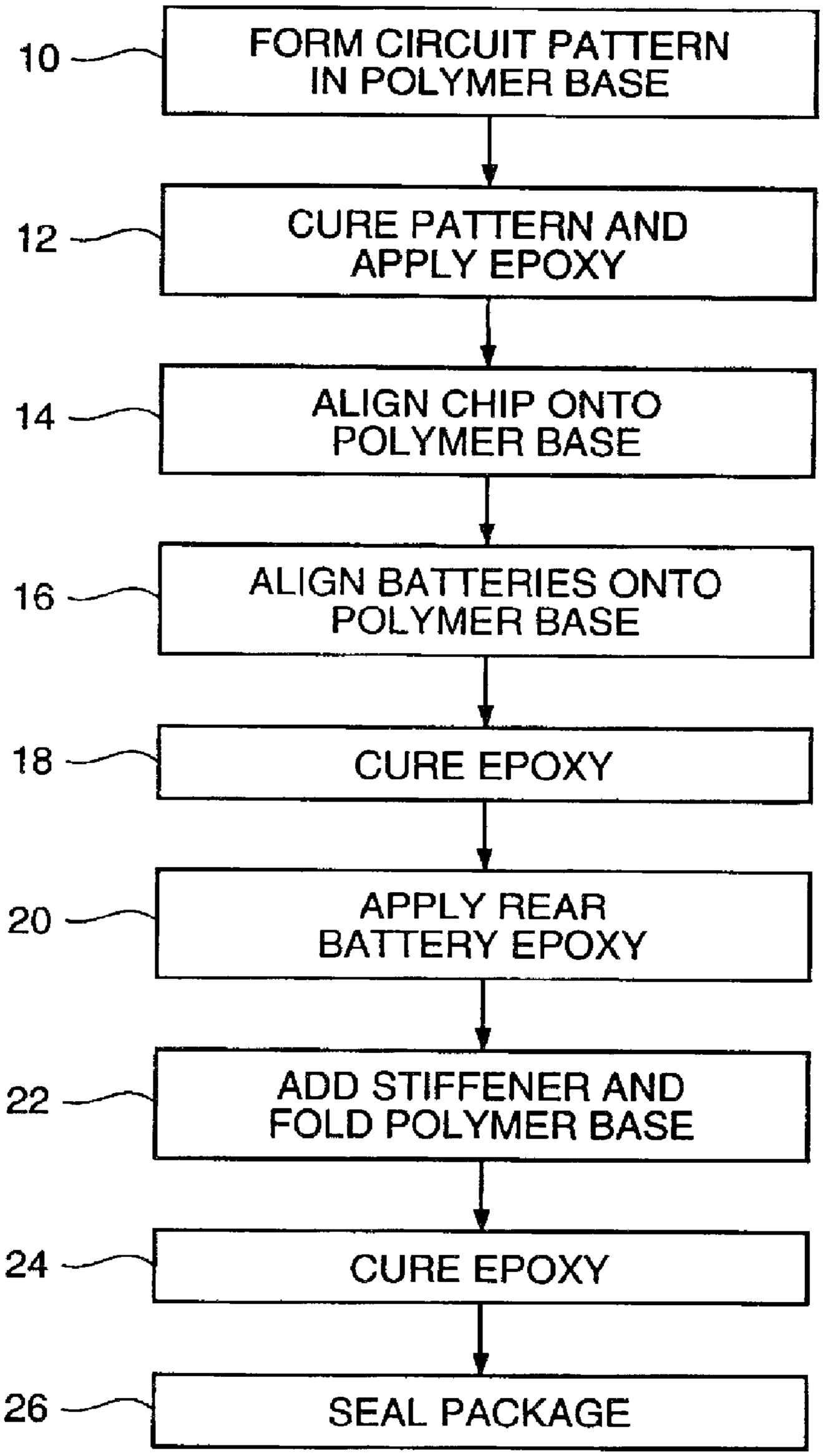

10
FORM CIRCUIT PATTERN IN POLYMER BASE
12
CURE PATTERN AND APPLY EPOXY
14
ALIGN CHIP ONTO POLYMER BASE
16
ALIGN BATTERIES ONTO POLYMER BASE
18
CURE EPOXY
20
APPLY REAR BATTERY EPOXY
22
ADD STIFFENER AND FOLD POLYMER BASE
24
CURE EPOXY
26
SEAL PACKAGE

FIG. 1

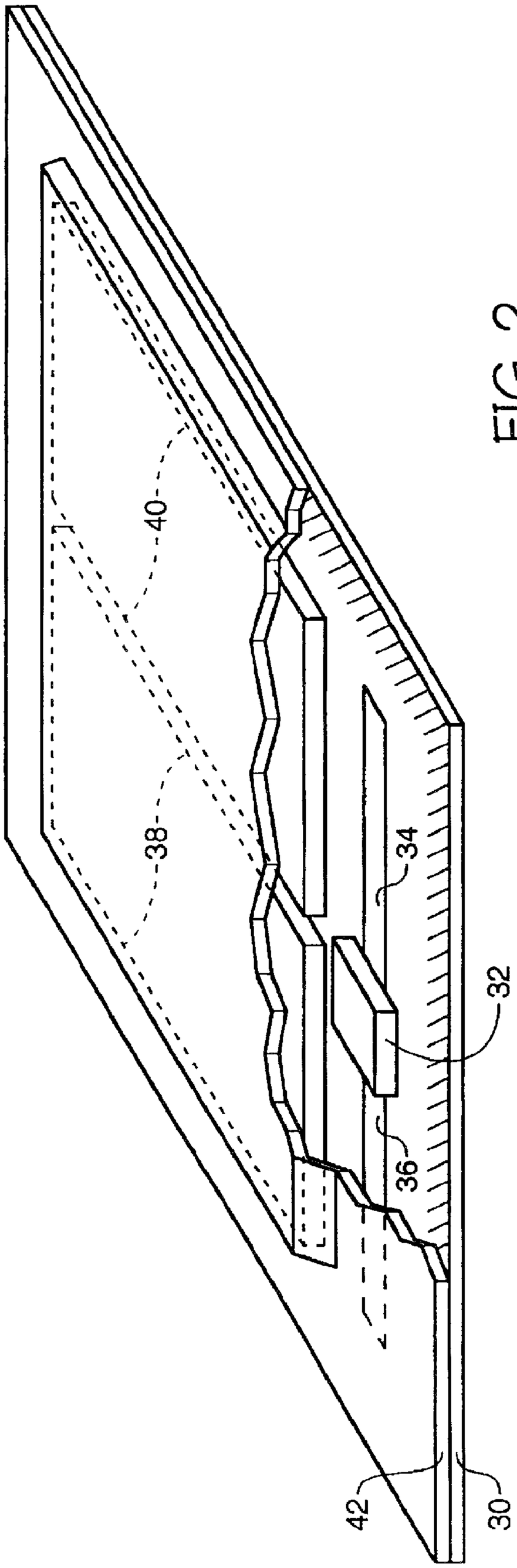


FIG. 2

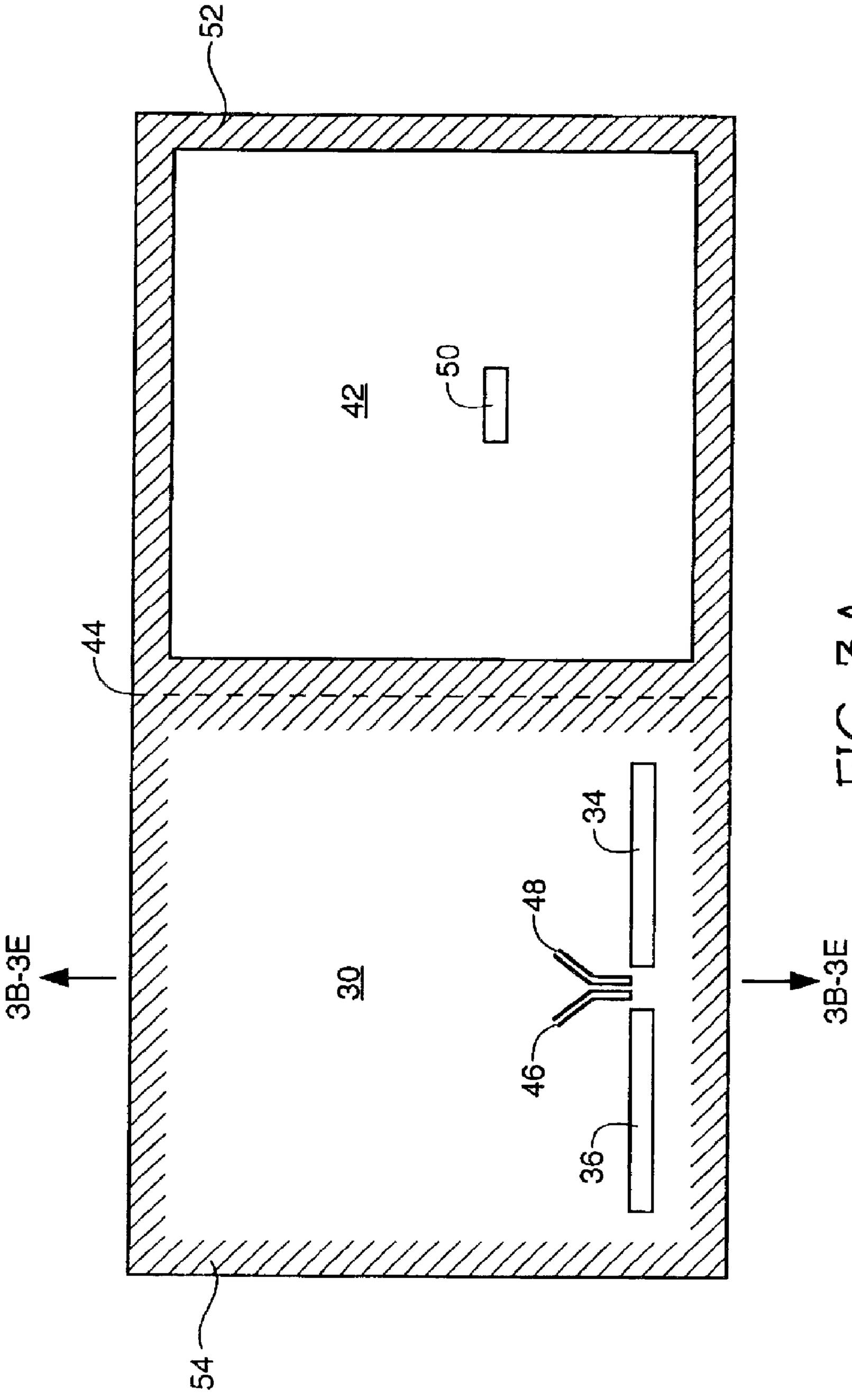


FIG. 3A

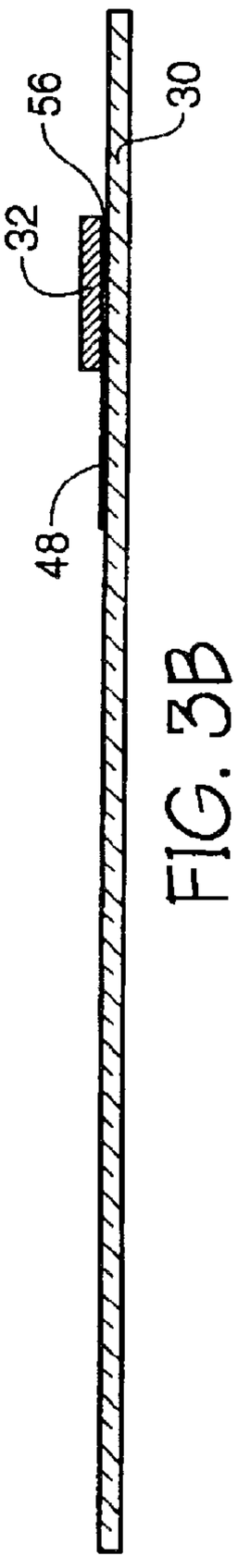


FIG. 3B

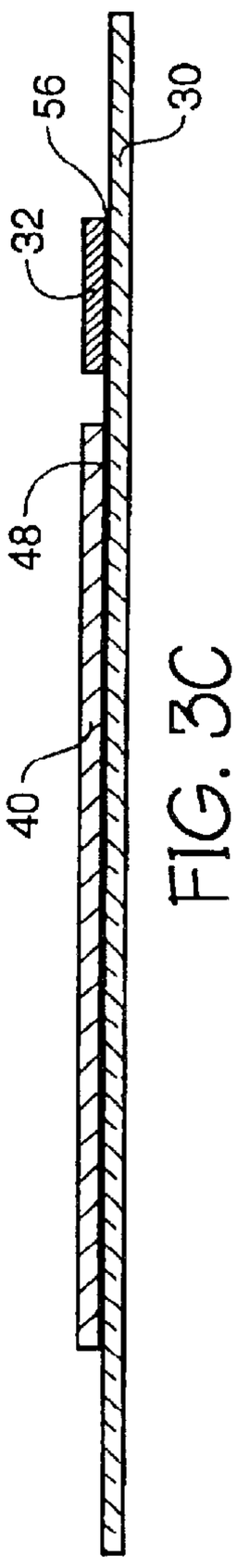


FIG. 3C

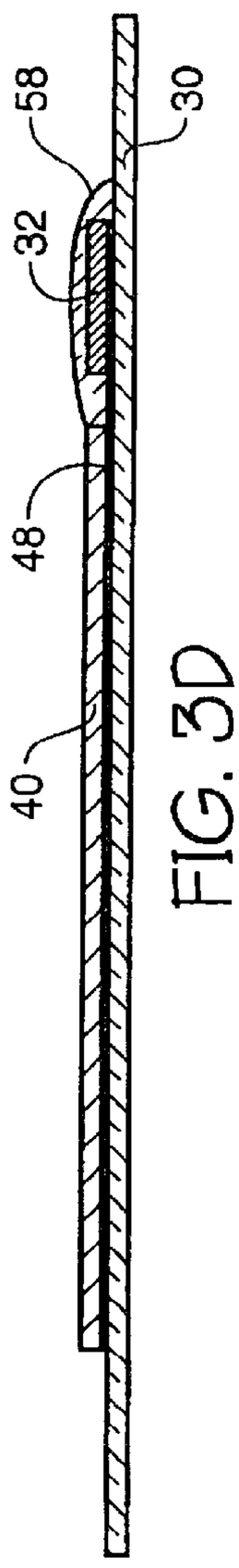


FIG. 3D

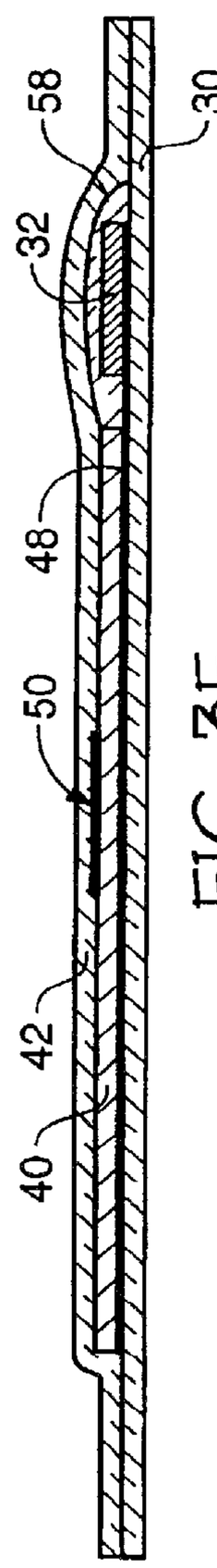


FIG. 3E

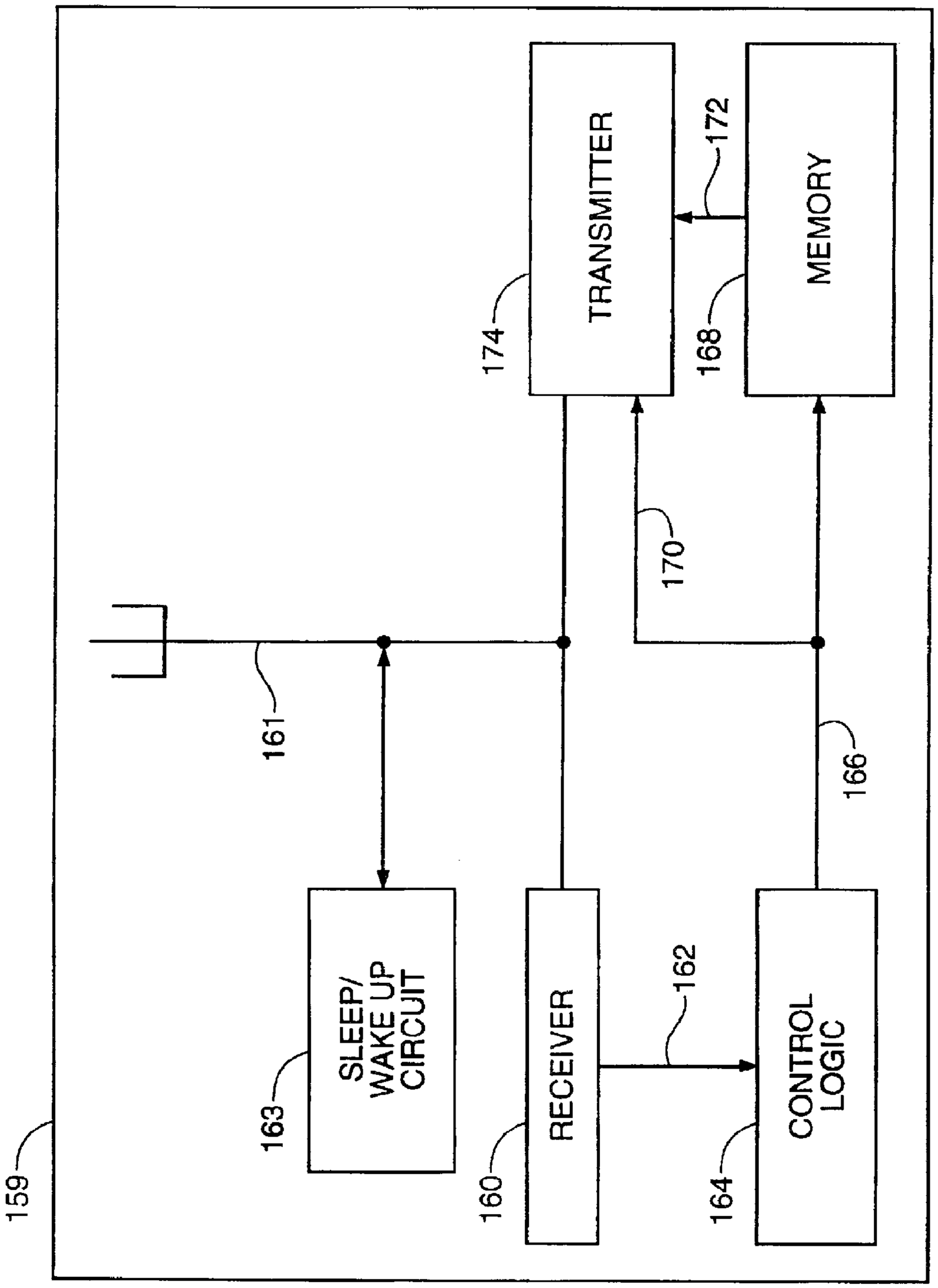

TRANSMITTER
MEMORY
172
174
168
170
166
161
SLEEP/
WAKE UP
CIRCUIT
RECEIVER
CONTROL
LOGIC
162
163
160
164
159

FIG. 4

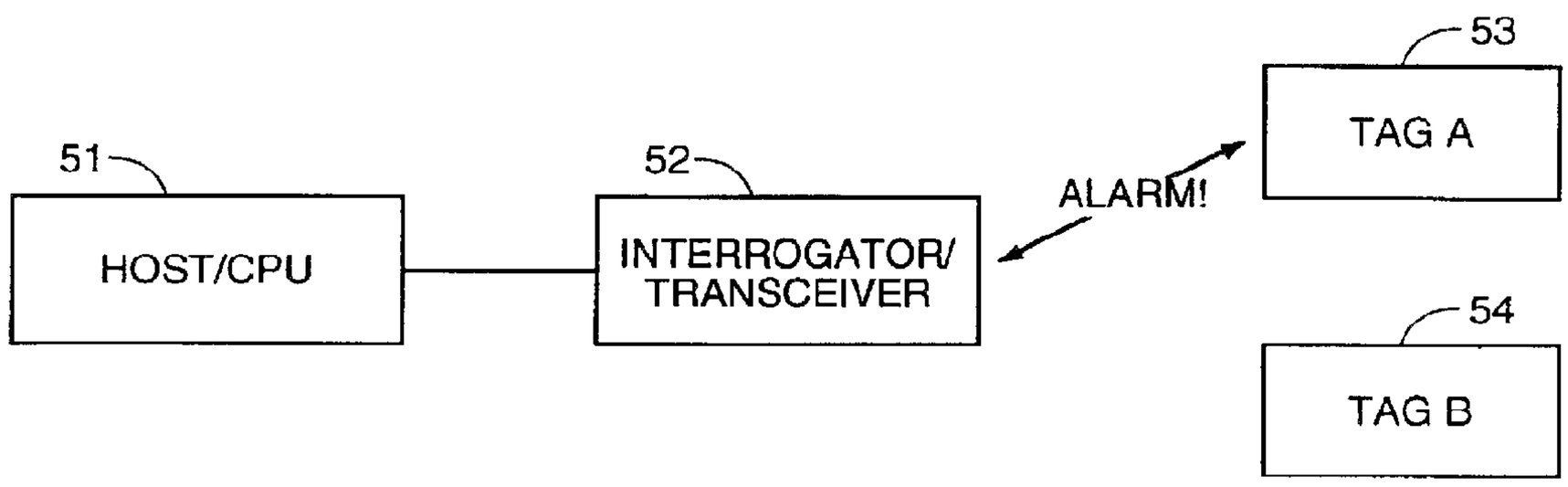

51
HOST/CPU
52
INTERROGATOR/
TRANSCEIVER
ALARM!
53
TAG A
54
TAG B

FIG. 5

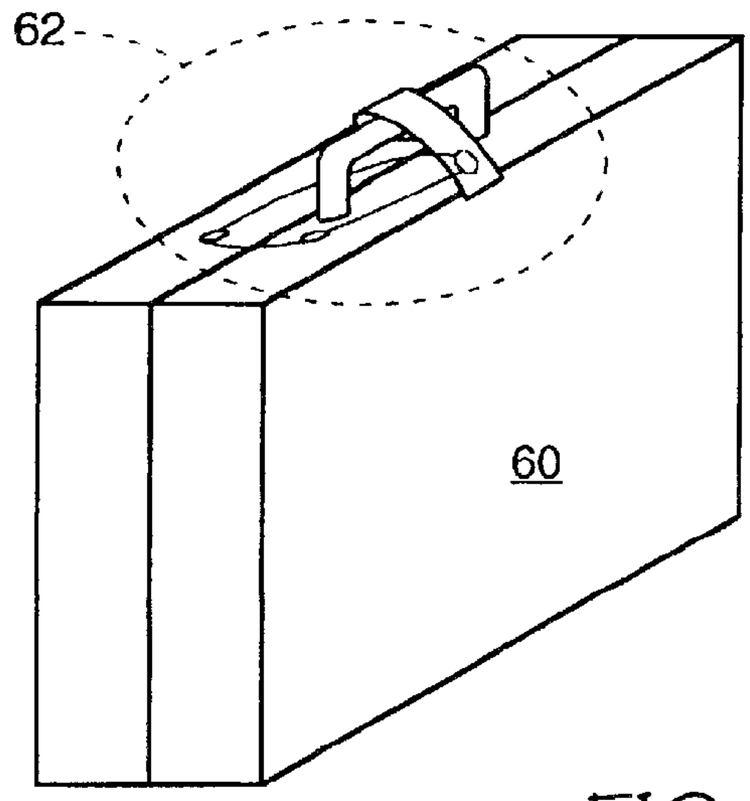


FIG. 6

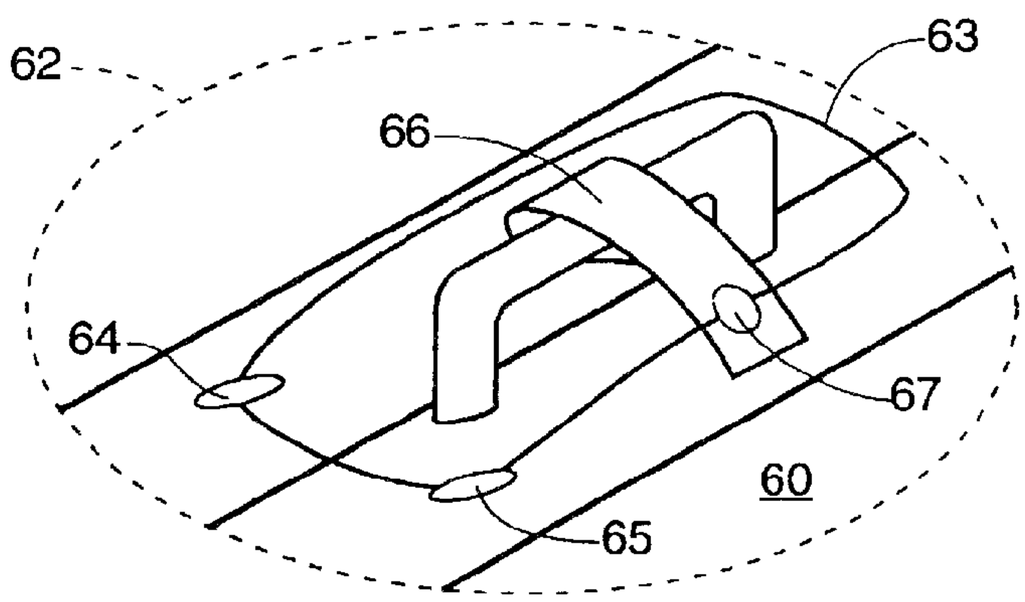


FIG. 6A

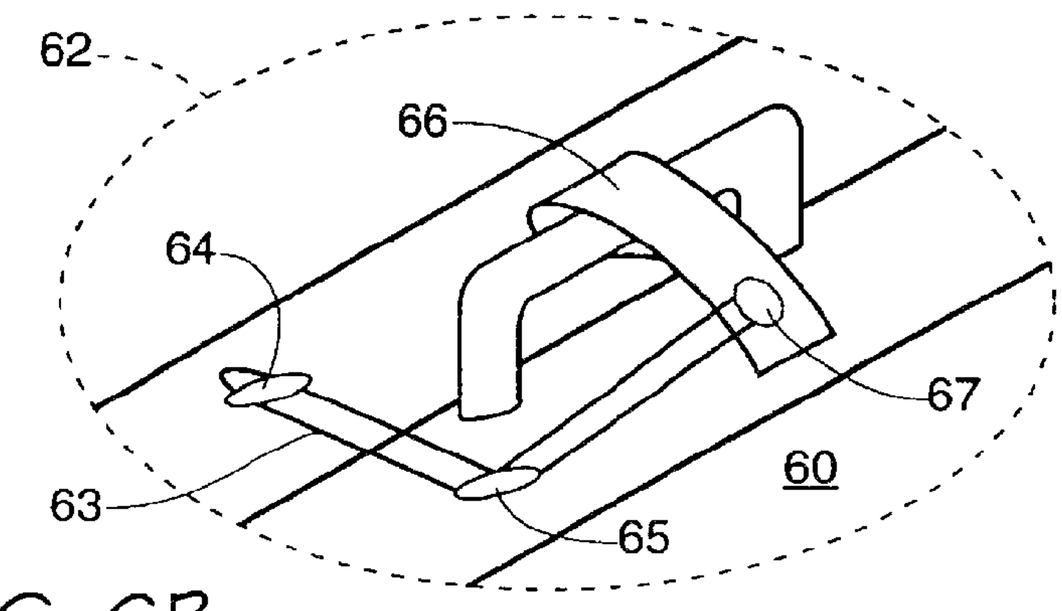


FIG. 6B

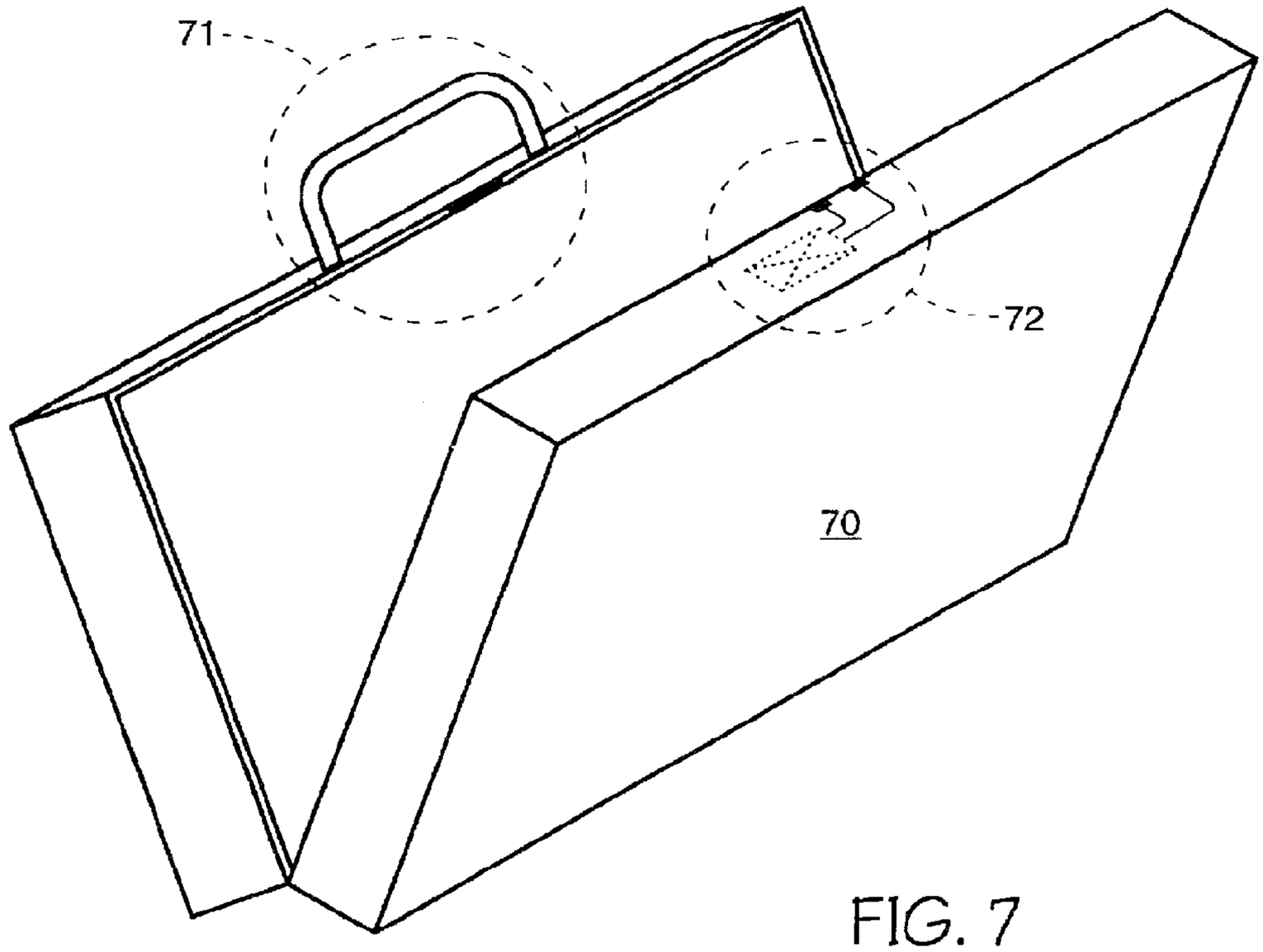


FIG. 7

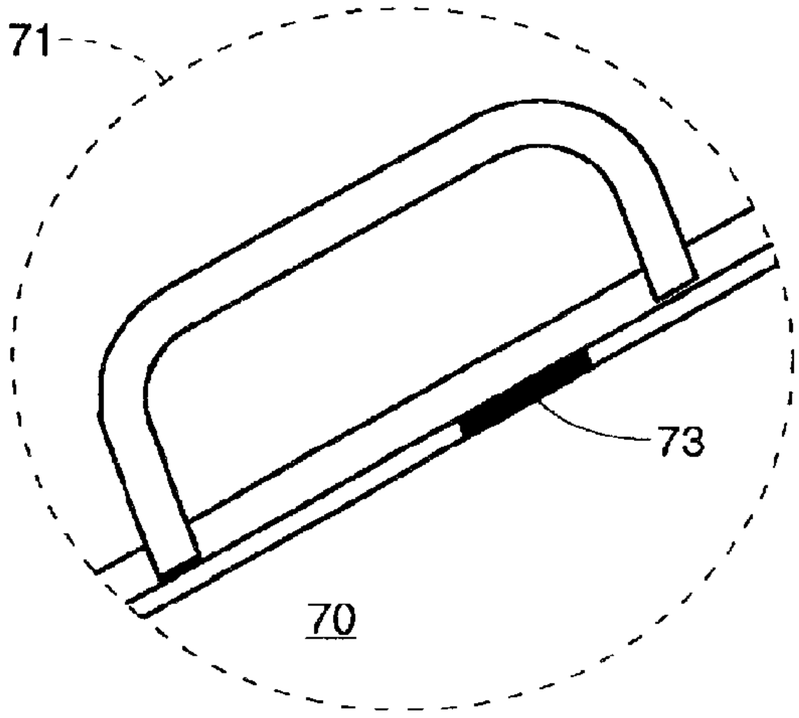


FIG. 7A

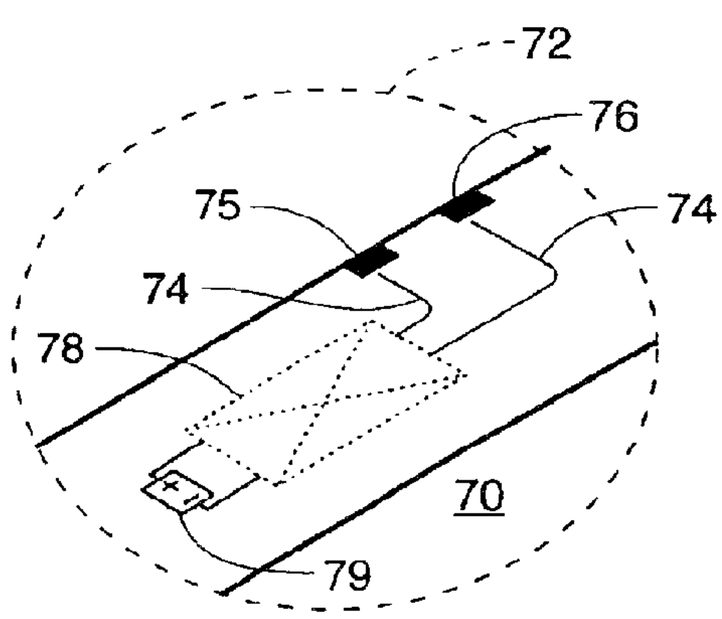


FIG. 7B

ANTI-THEFT METHOD FOR DETECTING THE UNAUTHORIZED OPENING OF CONTAINERS AND BAGGAGE

Matter enclosed in heavy brackets [ ] appears in the original patent but forms no part of this reissue specification; matter printed in italics indicates the additions made by reissue.

CROSS-REFERENCE TO RELATED APPLICATION

[This application] *More than one reissue application has been filed for the reissue of U.S. Pat. No. 5,831,531, which reissue applications are the present reissue application Ser. No. 12/038,473, filed Feb. 27, 2008, and a reissue continuation application Ser. No. 12/057,270, filed Mar. 27, 2008, which is a continuation application of the present reissue application, which is a reissue of U.S. Pat. No. 5,831,531, granted from U.S. patent application Ser. No. 08/827,037 filed Mar. 25, 1997, which* is a continuation [of] application *of U.S. patent application* Ser. No. 08/421,571 filed Apr. 11, 1995, now U.S. Pat. No. 5,646,592, *which is a continuation application of U.S. Pat. application Ser. No. 08/151,599 filed Nov. 12, 1993, now U.S. Pat. No. 5,406,263,* which is a continuation-in-part of application Ser. No. 07/921,037 filed Jul. 27, 1992, now abandoned.

FIELD OF THE INVENTION

This invention relates generally to anti-theft devices and in particular to a method for detecting unauthorized opening of containers and baggage.

BACKGROUND OF THE INVENTION

Protecting personal property has become a major industry from a security system standpoint. Security systems today can be as elaborate as those installed to protect banking institutions, equipped with video cameras, hooked-up as alarms to the local police station and security guards, or be as simple as a car alarm that is sounded when the door is forced open.

Likewise, the shipping industry is faced with an increasingly growing security problem in that containers, packages, baggage, luggage and mail (all of which may be referred to as simply "shipping container" hereinafter) are vulnerable to being opened by unauthorized personnel, who might steal the contents. As this problem increases it becomes necessary to protect these articles in order to protect the customer's property.

Due to the smaller size and larger quantity of the shipping articles mentioned above, the protection system used must be compact for concealment purposes, and somewhat simple in operation, thereby making them easy to produce and install in mass quantities while being fairly easy to monitor and operate.

The anti-theft method of the present invention conveniently addresses all of these issues to provide a workable and fairly inexpensive solution to securing safe transportation of articles shipped in some type of enclosed shipping container.

SUMMARY OF THE INVENTION

The present invention introduces a method for protecting against the unauthorized opening of shipping containers which is disclosed in the several embodiments following.

A first embodiment comprises a simple trip-wire or magnetic circuit that provides continuity, which is detected electrically. Simply, if continuity is disabled by a forced entry of the container, electrical detection means, such as a radio-frequency-identification (RFID) transceiver tag (or simply RFID tag), will alert the owner or monitoring station. The trip-wire concept would require the replacing of a broken trip wire (resulting from forced entry), while the magnetic circuit concept can be reused repetitively.

A second embodiment comprises the magnetic circuit approach of the first embodiment by having the magnetic circuit and the detection device embedded into the shipping article during manufacturing. The preferred detection device, and RFID tag, could also be a battery backed transceiver type on which a replaceable or rechargeable battery could be mounted on the inside of the shipping container during manufacturing. The RFID tag would communicate with an interrogator unit, which could be connected to a host computer. The interrogator and/or the host computer would then monitor the shipping container's status (opened or closed) . The RPID tag could also have an output that changes state upon alarm, so that another device could be connected to indicate the alarm via sound, flashing lights or other means.

Implementation of the present invention will become readily understandable to one skilled in the art in the detailed descriptions that follow.

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. **1** is a process flow diagram showing the major processing stations and fabrication stages used in an overall manufacturing process of an RFID tag;

FIG. **2** is an enlarged perspective view of an RFID tag as constructed in accordance with the process flow of FIG. **1**;

FIGS. **3**A through **3**E are cross sectional views of FIG. **2** showing the major processing steps used to construct the RFID tag;

FIG. **4** is a functional block diagram showing the major signal processing stages within the RFID integrated circuit chip described herein and also within the interrogation unit used to interrogate the chip;

FIG. **5** is a functional block diagram showing the communication between several RFID tags and interrogation unit;

FIGS. **6**, **6**A and **6**B depict a shipping container (luggage) on which a first embodiment of the present invention has been installed; and

FIGS. **7**, **7**A and **7**B depict a shipping container (luggage) on which a second embodiment of the present invention has been installed.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

Referring now to FIG. **1**, the process flow diagram shown in this figure includes nine (9) major processing stations or fabrication stages which are used in the overall manufacturing process steps that may be used to fabricate an RFID (radio frequency indentification) tag unit used in the anti-theft method of the present invention. These stages are described in more detail below with reference to FIGS. **2** and **3**A through **3**E. Initially, a circuit pattern is formed on a polymer base material in station **10**, whereafter the circuit pattern is cured and an epoxy conductive material is applied to station **12** before aligning an integrated circuit chip onto the polymer base in station **14**. Next, batteries (batteries added to the RFID package is optional) are aligned onto the polymer base in station **16** whereafter the epoxy is cured in station **18**.

In the next step, the rear battery epoxy is applied in station **20** before adding a stiffener and then folding the polymer base over onto the top cover as indicated in station **22**. The epoxy material is then cured in station **24** before providing a final sealing step in stage **26** to complete the package as described in more detail below.

Referring now to FIG. **2**, an RFID tag is depicted that includes a base support member **30** upon which an integrated circuit chip **32** is disposed on the near end of the device and connected to a dipole antenna consisting of metal strips **34** and **36** extending laterally from the chip **32** and typically screen printed on the upper surface of the base support member **30**.

A pair of rectangular shaped batteries **38** and **40** are positioned as shown adjacent to the IC chip **32** and are also disposed on the upper surface of the base support member **30**. The two rectangular batteries **38** and **40** are electrically connected in series to power the IC chip **32** in a manner more particularly described below. The device or package shown in FIG. **2** is then completed by the addition of an outer or upper cover member **42** which is sealed to the exposed edge surface portions of the base member **30** to thereby provide an hermetically sealed and completed package. The integrated chip **32** has transmitter, memory, logic, and receiver stages therein and is powered by the two batteries **38** and **40** during the transmission and reception of data to and from an interrogator to provide the interrogator with the various above identified information parameters concerning the article or person to which the RFID tag **30** is attached. The integrated chip may be designed to contain the needed circuitry one skilled in the art needs to accomplish the desired task and therefore may or may not contain all the circuitry listed above.

Referring now to FIG. **3**A, there is shown a plan view of the geometry of the base support member **30** and the cover member **42** which, during the initial manufacturing stage, are joined at an intersecting line **44**. The dipole antenna strips **34** and **36** shown positioned on each side of the IC chip **32**, and the two conductive strips **46** and **48** serve to connect the tops of the batteries **38** and **40** into the IC chip **32**. A conductive strip **50** is provided on the upwardly facing inside surface of the top cover **42**, so that when the cover **42** is folded by 180° C., its outer boundary **52** is ready to be sealed with the outer boundary **54** of the base support member **30**, and simultaneously the conductive strip **50** completes the series electrical connection used to connect the two batteries **38** and **40** in series with each other and further in the series circuit with the integrated circuit chip **32** through the two conductors **46** and **48**.

Referring now to FIGS. **3**B through **3**E, FIG. **3**B shows in cross section the IC chip **32** bonded to the base support member **30** by means of a spot button of conductive epoxy material **56**. The conductive strip **48** is shown in cross section on the upper surface of the base support member **30**. This figure would correspond generally to the fabrication stations **10**, **12**, and **14** in FIG. **1**.

Referring now to FIG. **3**C, the battery **40** is aligned in place as indicated earlier in FIG. **2** and has the right hand end thereof connected to the upper surface of the conductive strip **48**. FIG. **3** would therefore correspond to stations **16** and **18** in FIG. **1**.

Referring now to FIG. **3**D, a stiffener material **58** is applied as shown over the upper and side surfaces of the IC chip **32**, to provide a desired degree of stiffness to the package as completed. FIG. **3**D would therefore correspond to stations **20** and **22** in FIG. **1**.

Next, a conductive epoxy is applied to the upper surfaces of the two batteries **38** and **40**, and then the polymer base material **30** with the batteries thereon are folded over onto the cover member **42** to thus complete and seal the package in the configuration shown in FIG. **3**E and corresponding to the remaining stations **24** and **26** in FIG. **1**.

Referring now to FIG. **4**, the rectangular outer boundary **159** in this figure defines the active area on the integrated circuit chip in which the integrated circuit transceiver has been formed using state of the art MOS planar processing techniques. These MOS planar processing techniques are well known in the art and are, therefore, not described in detail herein. Within the chip active area there is provided an RF receiver stage **160** which is connected to an antenna **161** and via one or more lines or circuit connections **162**, to a control logic stage **164**. The control logic stage **164** is in turn connected via one or more integrated circuit connections or lines **166** to a memory stage **168**. The control logic stage **164** is further connected via a line **170** to a transmitter stage **174**, and the memory stage **168** is also connected via line **172** to the trasmitter stage **174**. The memory stage **168** is operative to provide input data to the transmitter stage **174** upon request, and functions in a manner operationally described in the example given below.

FIG. **5** is a functional block diagram showing a method of communication between several RFID tags and an interrogation unit in light of the anti-theft detection units later described in FIGS. **6** and **7**. Referring now to FIG. **5**, Host/CPU **51** interacts with interrogator/transceiver unit **52** and instructs unit **52** to interrogate RFID tags A (**53**) and B (**54**) for alarm data. If interrogator **52** receives no reply from either tag A or tag B the host **51** continues to instruct unit **52** to interrogate tags A and B as often as internal software demands it. However, if tag A responds (in an alarm state) the interrogator unit **52** communicates that information to the host **51** and an appropriate alarm is sounded to notify personnel that unauthorized opening of a container has just taken place.

By using the communication approach taken in FIG. **5**, a first embodiment of an "unauthorized opening detection device" is shown in FIG. **6** with variations of this embodiment shown in expanded views of FIG. **6** presented in FIGS. **6**A and **6**B.

Referring now FIG. **6**, shipping container **60** (luggage in this case) is adorned with an "unauthorized opening detection unit" enclosed by outlined dashed circle **62**. Expanded view **6**A of dashed circle **62** shows a continuous wire **63** attached to both sides of container **60** at a first connection node **64**, then to second connection node **65**, continuing to RFID tag **67** (which is affixed to label **66**) onto which wire **63** is attached. Wire **63** then completes its continuity path by attaching tag **67** to starting point node **64**. If continuity is disrupted (wire **63** breaks by unauthorized opening of container **20**) tag **67** would then signal the interrogator or some other device to sound an alarm and alert the owner or possibly security personnel in case of airline luggage transportation. Disarming the detection unit may be done by command from the interrogator or by the software at a given site, say at the container's destination, which may simply ignore the "opened" signal.

Expanded view of FIG. **6**B shows a second means of installing a detection device wherein continuous wire **63** attaches to a first connection node **64**, continues to a second connection node **65**, routes to RFID tag **67** (which is affixed to label **66**) and routes back to node **65** and finally to node **64**.

Both attaching methods serve as examples of how the opening detection unit may be attached to containers or doors that open. It would be preferred to have the wire attached so that it is not easily detected by casual observance and not easily broken by accident. Tag **67** could be affixed to label **66**

with tag **67** itself being adhered to a self-adhesive paper, such as stamp, and then applied to the label.

A second embodiment of an "unauthorized opening detection device" is shown in FIG. **7** with this embodiment shown in expanded views **7**A and **2**B.

Referring now to FIG. **7**, shipping container **70** (luggage in this case) is adorned with an "unauthorized opening detection unit" enclosed by outlined dashed circles **71** and **72**. In expanded view **7**A of dashed circle **71**, in the edge of container **70** a magnetic contact **73** is embedded. This magnetic contact **73** is preferably located in close proximity to a latch of container **70**, or magnetic contact **73** may also function as half the latching mechanism to the container. In expanded view **7**B of dashed circle **72**, an RFID tag **78** is affixed to the top face of container **70**. Electrical connections **74** extend from RFID tag **70** and attached to magnetic contacts **75** and **76**. Magnetic contacts **75** and **76** may also function as the other half of the latching mechanism to the container. When container **70** is closed, contacts **75** and **76** mate with contact **73**, thereby completing an electrical circuit. Unless disabled by the owner, should the container be forced open and continuity between contacts **73**, **75** and **76** be disrupted, an alarm state bit is set in (in the alarm flagging circuitry) tag **78** which will signal the interrogator or other controlling device to sound an alarm to alert the owner or security personnel. Tag **78** will remain in an alarm state until the alarm state bit is reset by the interrogator/controlling unit.

The detection device of FIG. **7**A could be further enhanced by providing a replaceable battery **79**, a power enabling means, for powering tag **78**. It would be logical to have the battery only accessible from the inside of container **70** which would mean tag **78** would need to be embedded into container **70** and preferably embedded during the manufacturing of container **70**. With a replaceable battery powered tag, tag **78** would now have the capability to send an alert signal to an interrogator unit or other device (such as a computer controlled transceiver unit) which would monitor the status of container **70** over its entire lifetime.

The methods of the embodiments discussed above, can easily be implemented into security systems. For example, by attaching the RFID tag and continuity completing circuitry to span between an entry/exit door and the framework supporting the door, unauthorized entry can now be monitored by activating the system when the door is to remain closed. Other such security schemes could also use the monitoring methods of the present invention.

It is to be understood that although the present invention has been described in several embodiments, various modifications known to those skilled in the art, such as applying these techniques to any kind of containers (mail, freight, etc.) or by various methods of attaching the detection device to the container, may be made without departing from the invention as recited in the several claims appended hereto.

I claim:

[1. For an apparatus having an aperture capable of being closed and opened by moving first and second closure members together and apart, respectively, an improved security device for signalling whether the aperture is opened, comprising:

(a) an elongated electrical conductor having first and second ends, the conductor extending between the two closure members and being attached to both the first closure member and the second closure member so that the two closure members cannot be moved apart more than a predetermined amount to open the aperture without breaking the conductor; and

(b) an RFID transceiver, connected to the two ends of the conductor, including an electrical circuit for detecting when electrical continuity between the two ends of the conductor is broken and subsequently transmitting a radio frequency alarm signal.**]**

[2. A security device according to claim **1**, wherein said apparatus is a container and the first and second closure members are external walls of the container.**]**

[3. A security device according to claim **2**, wherein the RFID transceiver is embedded within a wall of the container.**]**

[4. A security device according to claim **1**, wherein said apparatus is a suitcase and the first and second closure members are external walls of the suitcase.**]**

[5. For an apparatus having an aperture capable of being closed and opened by moving first and second closure members together and apart, respectively, an improved security device for signalling whether the aperture is opened, comprising:

(a) an electrical device, mounted on the apparatus adjacent the aperture, for detecting whether the aperture is open or closed; and

(b) an RFID transceiver which transmits a radio frequency alarm signal after said device detects the aperture has been opened.**]**

[6. A security device according to claim **5**, wherein the electrical device includes a magnet.**]**

[7. A security device according to claim **5**, wherein the electrical device includes an elongated electrical conductor having first and second ends, the conductor extending between the two closure members and being attached to both the first closure member and the second closure member so that the two closure members cannot be moved apart a substantial amount to open the aperture without breaking the conductor.**]**

[8. A security device according to claim **5**, wherein said apparatus is a container and the first and second closure members are external walls of the container.**]**

[9. A security device according to claim **8**, wherein the RFID transceiver is embedded within a wall of the container.**]**

[10. A security device according to claim **5**, wherein said apparatus is a suitcase and the first and second closure members are external walls of the suitcase.**]**

[11. For an apparatus having an aperture which is selectably closed and opened by moving first and second closure members together and apart, respectively, an improved security device for signalling whether the aperture is opened, comprising:

(a) an electrical device, mounted on the apparatus adjacent the aperture, for detecting whether the aperture is open or closed, wherein the electrical device includes:

(i) first and second electrical contacts mounted on the first closure member, and

(ii) a third electrical contact mounted on the second closure member at a position such that, when the two closure members are moved together so as to close the aperture, the third electrical contact mates with both the first and the second contacts so as to complete an electrical continuity between the first and second contacts; and

(b) an RFID transceiver which transmits a radio frequency alarm signal in response to said electrical continuity being broken.**]**

[12. A secure apparatus for signalling whether an aperture of the apparatus is opened, comprising:

an apparatus having first and second closure members and having an aperture capable of being closed and opened by moving the two closure members together and apart, respectively;

an electrical device, mounted on the apparatus adjacent the aperture, for detecting whether the aperture is opened; and

an RFID transceiver which transmits an alarm signal after said device detects the aperture has been opened.]

[**13**. Apparatus according to claim **12**, wherein the electrical device includes an elongated electrical conductor having first and second ends, the conductor extending between the two closure members and being attached to both the first closure member and the second closure member so that the two closure members cannot be moved apart more than a predetermined amount to open the aperture without breaking the conductor.]

[**14**. Apparatus according to claim **13**, further comprising:

a hinge mounted on a first end of each closure member;

wherein the conductor extends between the two closure members at a second end of each closure member opposite the hinge.]

[**15**. Apparatus according to claim **14**, further comprising:

a handle mounted on the second end of one of the closure members; and

a strap encircling the handle;

wherein the RFID transceiver is mounted on the strap.]

[**16**. Apparatus according to claim **12**, wherein:

the electrical device includes

first and second electrical contacts mounted on the first closure member, and

a third electrical contact mounted on the second closure member at a position such that, when the two closure members are moved together so as to close the aperture, the third contact mates with both the first and second contacts so as to complete an electrical continuity between the first and second contacts; and

the RFID transceiver transmits said radio frequency alarm signal in response to said electrical continuity being broken.]

[**17**. Apparatus according to claim **16**, wherein the first, second and third electrical contacts respectively comprise first, second and third magnetic contacts.]

[**18**. Apparatus according to claim **12**, wherein the electrical device includes a magnetic device.]

[**19**. Apparatus according to claim **12**, wherein said apparatus is a container and the first and second closure members are external walls of the container.]

[**20**. Apparatus according to claim **19**, wherein the RFID transceiver is embedded within a wall of the container.]

[**21**. Apparatus according to claim **12**, wherein:

said apparatus is a suitcase; and

the first and second closure members are external walls of the suitcase.]

[**22**. Apparatus according to claim **12**, wherein:

said apparatus is a doorway;

the first closure member is a door frame; and

the second closure member is a door.]

[**23**. A method for signalling whether an aperture is opened, comprising the steps of:

providing an apparatus having first and second closure members and having an aperture capable of being closed and opened by moving the first and second closure members together and apart, respectively;

detecting whether the aperture is opened; and

in response to detecting that the aperture is opened, transmitting a radio frequency alarm signal.]

[**24**. A method according to claim **23**, wherein the detecting step comprises:

mounting adjacent the aperture an electrical detecting device having an electrical condition responsive to whether the aperture is opened; and

detecting whether the aperture is opened by detecting the electrical condition of the detecting device.]

[**25**. A method according to claim **24**, wherein:

the step of mounting an electrical detecting device comprises extending between the two closure members an elongated electrical conductor having first and second ends, and attaching the conductor to both the first closure member and the second closure member so that the two closure members cannot be moved apart more than a predetermined amount to open the aperture without breaking the conductor; and

the step of detecting whether the aperture is opened comprises detecting whether electrical continuity between the two ends of the conductor is broken.]

[**26**. A method according to claim **24**, wherein the step of mounting an electrical detecting device comprises mounting a magnet adjacent the aperture.]

[**27**. A method according to claim **23**, wherein the providing step comprises:

providing a container having first and second external walls, wherein said apparatus is the container and said first and second closure members are the first and second external walls of the container, respectively.]

[**28**. A method according to claim **27**, further comprising the step of:

embedding an RFID transceiver within a wall of the container;

wherein the transmitting step comprises the RFID transceiver transmitting the radio frequency alarm signal.]

[**29**. A method according to claim **28**, further comprising the steps of:

mounting a replaceable battery within the container so as to be accessible only from the interior of the container; and

connecting the battery to the RFID transceiver.]

[**30**. A method according to claim **27**, wherein the step of providing a container comprises:

providing a suitcase as said container.]

[**31**. A method according to claim **23**, wherein the transmitting step further comprises:

receiving radio frequency interrogation signals; and

transmitting said radio frequency alarm signal only after receiving a radio frequency interrogation signal subsequent to said detecting that the aperture is opened.]

32. A method for signalling whether an aperture is opened, comprising the steps of:

providing a shipping container having at least one hinge, first and second closure members, and an aperture capable of being closed and opened by moving, via the at least one hinge, the first and second closure members together and apart, respectively;

providing an unauthorized opening detection unit attached to the shipping container adjacent the aperture, the detection unit comprising an RFID device storing data concerning the shipping container and a detection circuit;

detecting whether the aperture is opened using the detection circuit;

generating a detection signal if the aperture is opened, wherein, in response to the detection signal, alarm data is stored in the detection unit to indicate that the aperture is opened; and

in response to detecting that the aperture is opened, transmitting a radio frequency alarm signal from the RFID device if the aperture is detected to be opened.

33. A method according to claim 32, wherein the radio frequency alarm signal is transmitted to an interrogator in response to the interrogator interrogating the RFID device.

34. A method according to claim 33, further comprising communicating an alarm status to a host computer coupled to the interrogator if the interrogator receives the radio frequency alarm signal from the RFID device.

35. A method according to claim 33, wherein the radio frequency alarm signal is transmitted to the interrogator in response to the interrogator interrogating a plurality of RFID devices including the RFID device.

36. A method according to claim 35, wherein the interrogator continually interrogates the RFID device in accordance with software running on a host computer coupled to the interrogator.

37. A method according to claim 32, further comprising continually interrogating the RFID device using an interrogator to continually monitor for an alarm.

38. A method according to claim 32, wherein the alarm data is stored in the detection unit until reset.

39. A method according to claim 38, further comprising transmitting a reset command from an interrogator to the RFID device to reset the alarm data.

40. A method according to claim 39, further comprising providing a battery only accessible from inside the shipping container when the aperture is closed to power the detection unit.

41. A method according to claim 32, further comprising providing a replaceable battery hermetically sealed within a compartment containing the RFID device.

42. A method according to claim 32, wherein the detecting of whether the aperture is opened comprises electrically detecting continuity between two electrical contacts.

43. A method according to claim 32, wherein the detection unit spans the aperture.

44. A method according to claim 32, further comprising monitoring a status of the aperture of the shipping container as being either opened or closed via a host computer.

45. A method according to claim 32, further comprising transmitting an audible sound from the detection unit.

46. A method according to claim 45, wherein the transmitting of the audible sound is in response to detecting that the aperture is opened.

47. A method according to claim 32, further comprising transmitting a visible light signal from the detection unit.

48. A method according to claim 47, wherein the transmitting of the visible light signal is in response to detecting that the aperture is opened.

49. A method according to claim 32, wherein the first closure member is a door.

50. A method according to claim 49, wherein the second closure member is a door frame.

51. A method according to claim 32, wherein the RFID device is hermetically sealed within a compartment of the detection unit.

52. A method according to claim 32, wherein the detection circuit comprises a magnet.

53. A method according to claim 32, wherein the detection unit is coupled to a latching mechanism of the shipping container to hold the aperture closed.

54. For a shipping container having an aperture, an improved security device for signalling whether the aperture is opened, comprising:

(a) an electrical detection device, mounted on the shipping container adjacent the aperture, for detecting whether the aperture is open or closed, the shipping container having first and second closure members, the aperture capable of being closed and opened by moving the first and second closure members together and apart, respectively, the detection device to generate a detection signal if the aperture is opened; and

(b) an RFID transceiver device which transmits a radio frequency alarm signal after the electrical device detects the aperture has been opened, the RFID transceiver device coupled to the detection device and storing data concerning the shipping container;

wherein, in response to the detection signal, alarm data is stored in the security device to indicate that the aperture has been opened.

55. A security device according to claim 54, wherein the RFID transceiver device comprises memory, transmitter, logic, and receiver stages, and an antenna coupled to the transmitter and receiver stages, the memory to store information identifying the shipping container and to store the alarm data in response to the detection signal.

56. A security device according to claim 55, wherein the memory, the transmitter, logic, and receiver stages are integrated on an integrated circuit chip.

57. A security device according to claim 55, wherein when the receiver stage of the RFID device receives an interrogation command from an interrogator through the antenna, the transmitter stage of the RFID device is to transmit the information identifying the shipping container and to transmit the radio frequency alarm signal according to the alarm data.

58. A security device according to claim 57, wherein when the receiver stage of the RFID device receives a reset command from an interrogator through the antenna, the RFID device is to reset the alarm data in the memory.

59. A security device according to claim 55, further comprises a battery to power the RFID device, wherein the RFID device and the battery are hermetically sealed within a compartment.

60. A security device according to claim 55, wherein the radio frequency alarm signal is transmitted in response to an interrogator interrogating plurality of RFID devices including the RFID device.

61. A security device according to claim 55, further comprising a device connected to indicate an alarm via at least audio or visual signals, in response to the detection signal.

62. A security device according to claim 55, further comprising a device connected to emit audible sound.

63. A security device according to claim 55, further comprising a device connected to emit visible light.

64. A security device according to claim 55, wherein the detection circuit comprises a magnet.

65. A security device according to claim 54, wherein the detection device is coupled to a latching mechanism of the shipping container for holding the aperture closed.

66. A security device according to claim 65, wherein at least a portion of the detection device is part of the latching mechanism of the shipping container.

67. A security device according to claim 65, wherein the shipping container has at least one hinge; and the aperture is capable of being closed and opened by moving, via the at least one hinge, the first and second closure members together and apart, respectively.

68. A security device according to claim 65, wherein the detection device is to generate a detection signal if the aperture is opened without authorization.

69. A secure apparatus for signalling whether an aperture of the apparatus is opened, comprising:

a shipping container having first and second closure members, and an aperture capable of being closed and opened by moving the first and second closure members together and apart, respectively;

an electrical detection device, mounted on the shipping container adjacent the aperture, for detecting whether the aperture is open or closed and for generating a detection signal if the aperture is opened; and

an RFID transceiver device which transmits a radio frequency alarm signal after the electrical device detects the aperture has been opened, the RFID transceiver device coupled to the electrical detection device and storing data concerning the shipping container;

wherein, in response to the detection signal, alarm data is stored in the RFID device to indicate that the aperture has been opened.

70. A secure apparatus according to claim 69, wherein the RFID device comprises memory, a transmitter, a logic stage, a receiver and an antenna coupled to the transmitter and the receiver, the memory to store the data concerning the apparatus and to store the alarm data in response to the detection signal.

71. A secure apparatus according to claim 70, wherein the memory, transmitter, logic stage and receiver are integrated on an integrated circuit chip.

72. A secure apparatus according to claim 70, further comprising a battery to power the RFID device; wherein the RFID transceiver tag, the battery and at least a portion of the detection device are sealed inside a package.

73. A secure apparatus according to claim 70, further comprising an interrogator wirelessly coupled to the RFID device via radio frequency signals, the RFID device to transmit the alarm signal to the RFID interrogator according to the alarm data in response to an interrogation command transmitted from the interrogator to the RFID device.

74. A secure apparatus according to claim 73, further comprising an alarm device coupled to the interrogator to indicate an alarm via at least sound or light, in response to the alarm signal.

75. A secure apparatus according to claim 73, wherein the alarm signal is transmitted to the interrogator in response to the interrogator interrogating a plurality of RFID devices including the RFID device.

76. A secure apparatus according to claim 75, wherein the interrogator continually interrogates the RFID device in accordance with software running on a host computer coupled to the interrogator.

77. A secure apparatus according to claim 75, wherein the interrogator continually interrogates the RFID device to continually monitor for an alarm.

78. A secure apparatus according to claim 70, further comprising an interrogator wirelessly coupled to the RFID device via radio frequency signals, the RFID device to reset the alarm data in response to a radio frequency reset command from the interrogator to the RFID device.

79. A secure apparatus according to claim 70, wherein the detection device spans the aperture.

80. A secure apparatus according to claim 70, wherein the first closure member is a door and the second closure member is a door frame.

81. A secure apparatus according to claim 69, wherein the detection device is coupled to a latching mechanism of the shipping container.

82. A secure apparatus according to claim 69, wherein the shipping container has at least one hinge; and the aperture is capable of being closed and opened by moving, via the at least one hinge, the first and second closure members together and apart, respectively.

83. A secure apparatus according to claim 69, further comprising a device connected to emit audible sound.

84. A secure apparatus according to claim 69, further comprising a device connected to emit visible light.

85. A method for signalling whether an aperture is opened, comprising the steps of:

providing an apparatus having first and second closure members including a door, and having an aperture capable of being closed and opened by moving, via the door, the first and second closure members together and apart, respectively;

providing an RFID device to wirelessly identify the apparatus to an interrogator;

after the door is closed, applying an unauthorized opening detection unit to form a continuity circuit, wherein a change in the continuity circuit indicates that the door is opened;

detecting whether the aperture is opened using the detection unit; and

in response to detecting that the aperture is opened, transmitting a radio frequency alarm signal from the RFID device to the interrogator if the aperture is detected to be opened.

86. A method according to claim 85, further comprising continually interrogating the RFID device via radio frequency signals using the interrogator to continually monitor for an alarm.

87. A method according to claim 85, wherein the applying of the detection unit comprises attaching a wire to form the continuity circuit.

88. A method according to claim 87, wherein the wire is attached across the closure members.

89. A method according to claim 85, wherein the detection unit is coupled to a latching mechanism for keeping the aperture closed.

90. For an apparatus having an aperture, an improved security device for signalling whether the aperture is opened, comprising:

(a) an electrical device, mounted on the apparatus adjacent the aperture, for detecting whether the aperture is open or closed, the apparatus having first and second closure members including a door, the aperture capable of being closed and opened by moving, via the door, the first and second closure members together and apart, respectively, the electrical device comprising a conductor to form a continuity circuit which when disrupted generates a signal indicating that the aperture is opened; and

(b) a RFID transceiver tag coupled to the electrical device to monitor the continuity circuit, the RFID transceiver tag having memory to store identification information of the RFID transceiver tag and to store status information indicating whether the aperture has been opened, wherein the RFID transceiver tag transmits the identification information and transmits a radio frequency alarm signal according to the status information stored in the memory after the electrical device detects the aperture has been opened.

91. A security device according to claim 90, wherein the conductor extends between the closure members to form the continuity circuit.

92. A security device according to claim 90, wherein the RFID transceiver tag comprises transmitter, logic, and receiver stages integrated on an integrated circuit chip; the

RFID transceiver tag further comprises an antenna coupled to the transmitter and receiver stages, the receiver stage of the RFID transceiver tag is configured to receive an interrogation command from an interrogator via radio frequency signals; and the transmitter stage is configured to transmit the identification information and the radio frequency alarm signal in response to the interrogation command.

93. A security device according to claim 90, wherein the RFID transceiver tag is to reset the status information in the memory when the receiver stage of the RFID transceiver tag receives a reset command over the antenna.

94. A security device according to claim 90, further comprising a replaceable battery to power the RFID tag, wherein the RFID tag is sealed inside a package.

95. A secure apparatus for signalling whether an aperture of the apparatus is opened, comprising:

an apparatus having first and second closure members comprising a door and having an aperture capable of being closed and opened by moving, via the door, the two closure members together and apart, respectively;

an electrical device, mounted on the apparatus adjacent the aperture, for detecting whether the aperture is opened, the electrical device comprises a conductor, continuity of the conductor to be changed when the aperture is opened, when continuity of the conductor is changed the electrical device to generate an signal indicating that the aperture is opened;

an RFID transceiver tag coupled to the electrical device, the RFID transceiver tag having memory to store data concerning the apparatus and to store, in response to the signal generated by the electrical device, status information indicating whether the aperture has been opened; and

an interrogator wirelessly coupled to the RFID transceiver tag via radio frequency signals, wherein in response to an interrogation command received from the interrogator, the RFID tag transmits an alarm signal to the interrogator, according to the status information stored in the memory, after said device detects the aperture has been opened.

96. A secure apparatus according to claim 95, wherein the conductor spans across the aperture to form a continuity circuit.

97. A secure apparatus according to claim 95, further comprising a battery to power the RFID transceiver tag and the electrical device; wherein the RFID transceiver tag and the battery are sealed inside a package.

98. A secure apparatus according to claim 95, further comprising an alarm device coupled to the interrogator, the alarm device to be activated to indicate alarm via at least sound or light in response to the interrogator receiving the alarm signal.

99. A secure apparatus according to claim 95, wherein the electrical device is coupled to a latching mechanism of the apparatus for keeping the aperture closed.

* * * * *