(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
17 September 2009 (17.09.2009)

PCT

(10) International Publication Number
WO 2009/114850 A1

(51) International Patent Classification:
G08B 29/00 (2006.01)

(21) International Application Number:
PCT/US2009/037280

(22) International Filing Date:
16 March 2009 (16.03.2009)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
61/036,623 14 March 2008 (14.03.2008) US

(71) Applicant *(for all designated States except US)*: **NEW CENTURION SOLUTIONS, INC.** [US/US]; 5005 Roberson Farm Road, Kernersville, NC 27284 (US).

(72) Inventors; and
(75) Inventors/Applicants *(for US only)*: **SHELTON, John, Travis** [US/US]; 343 Horseshoe Lane, Westfield, NC 27053 (US). **BOYETTE, Jordan, J.** [US/US]; 3504 North Carolina Highway 66 North, Westfield, NC 27053 (US). **WILLIAMS, Gregory, H.** [US/US]; 5005 Roberson Firm Rd., Kernersville, NC 27284 (US).

(74) Agent: **SOSENKO, Jessica**; Spilman Thomas & Battle PLLC, c/o CPA Global, P.O. Box 52050, Minneapolis, MN 55402 (US).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:

— *with international search report (Art. 21(3))*

(54) **Title**: PRIVATE NETWORK EMERGENCY ALERT PAGER SYSTEM

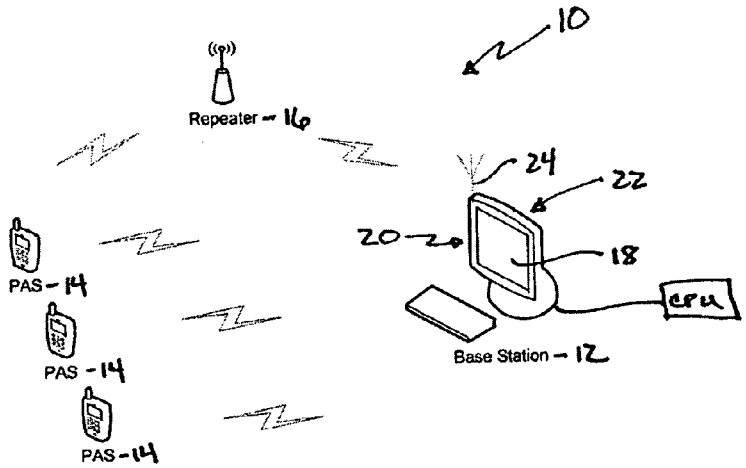


Fig. 1

(57) **Abstract**: A private network emergency pager alert system as described herein can generally utilize a plurality of personal alert pager devices and a main controller in two-way communication with each personal alert pager device. Each personal alert pager device can be provided with a transceiver for receiving alerts from the main controller and for sending alerts to the main controller, a text display for receiving alert messages, switches for sending an alert to the main controller, and a GPS receiver for providing location data of the personal alert pager device to the main controller. The personal alert pager device could additionally be provided with an RFID module and/or a key pad for sending text messages

WO 2009/114850 A1

TITLE

PRIVATE NETWORK EMERGENCY ALERT PAGER SYSTEM

BACKGROUND

The private network emergency alert pager system relates generally to an emergency alert system, and more particularly to a private network emergency alert system utilizing multiple personal alert pager devices and a monitoring station which is in two-way communication with each personal alert pager device.

"Active Shooter" events have increased dramatically in the last decade; a common problem has been the lack of technology that provides instantaneous, mass notification to potential victims in the immediate threat area. The incident at Virginia Tech increased the focus on the problem when the area in need of protection encompasses a wide area such as a sprawling campus with over 100 buildings, and when the threat is mobile. Even victims who were aware of a threat in the area were unaware of which areas contained the threat, and what area to move to for safety. The Active Shooter phenomenon has also resulted in the increased use of RFID-activated and secured doors on campuses nationwide, which are intended to provide secured areas for students and faculty/staff in emergency situations.

Accordingly, there is a need for a system which can provide a solution to the problem of mass notification, and at the same time provide personal accountability for every person in need of notification, protection, and rescue.

SUMMARY

An emergency alert pager system as described herein has the advantages of two-way communication between a Personal Alert Sentry (PAS) and a base station; individual panic alert capability; and being a stand-alone, self-contained system providing instantaneous, truly mass notification.

An emergency alert pager system as described herein can generally comprise at least one personal alert pager device, but preferably a plurality of personal alert pager devices, referred to hereinafter alternatively as either a "pod" or a "Personal Alert Sentry" (PAS), and a single main security controller, referred to herein alternatively as main controller, base station, or monitoring station. Each pod is a portable device that can be handheld or worn by a user. When a pod is activated, it sends its location to software of the main controller. The main controller shows the pod on a screen along with pertinent information. The controller can send back a message to the

individual pod or a general announcement to all pods. If any pod is unaccounted for, the pod can be polled by the main controller as to its location and status. Pods can be deployed in a wide screen search, and repeaters can be used to increase the range of the system.

An embodiment of the overall private network emergency alert pager system can generally comprise:

- 1. a main controller;
  - which can comprise a computer, one or more associated monitors for displaying data, a base antenna, and optional repeaters for better range or to deal with obstructions.

- 2. at least one pod, preferably a plurality;
  - each in 2-way communication with the base station, and each pod comprising (as described in more detail below in connection with Sheet 2/2) one or more of a transceiver and associated antenna, a GPS module and associated antenna, a text display screen, and alert buttons/switches.

Each individual pod can generally comprise:

- 1. spread spectrum transceiver
  - For example a 250 mW transceiver in the 900 MHz band.

- 2. GPS receiver and active antenna
  - To receive and decode the GPS positional signal.

- 3. movement sensor
  - To sense movement for higher resolution GPS fixes and power saving.

- 4. vibrating motor and peizo sounder
  - For audible and tactile feedback during alert.

- 5. LED display
  - For text readout of alert information.

- 6. batter control and charge circuitry

- 7. emergency alert switches
  - For activating an alert to the main controller.

- 8. microcontroller

- 9. optional keypad
  - Could permit text messages to be sent from the pod to the main controller to provide details about the threat.

- 10. optional RFID module
  - Could be utilized to gain access to safe/secure areas, buildings, etc.

As indicated above, each pod can utilize pager technology with one or more of text messaging on LCD display screens, audible alert tones, vibrating alerts, GPS technology, RFID (radio frequency identification) technology, and two way communication between the pager device and the monitoring station.

The emergency alert pager system described herein can provide a solution to the problem of mass notification, and at the same time provide personal accountability for every person in need of notification, protection, and rescue.

To the accomplishment of the foregoing and related ends, certain illustrative aspects of the emergency alert pager system are described in the following description and drawing figures. These aspects may be indicative of but a few of the various ways in which the principles of the emergency alert pager system may be employed, and which is intended to include all such aspects and any equivalents thereof. Other advantages and features of the emergency alert pager system may become apparent from the following detailed description when considered in conjunction with the drawing figures.

BRIEF DESCRIPTION OF THE DRAWING FIGURES

A more complete understanding of the emergency alert pager system described herein can be obtained by considering the following description in conjunction with the accompanying drawing figures in which:

Fig. 1 illustrates an embodiment of an emergency alert pager system as described herein;

Fig. 2 illustrates an embodiment of an emergency alert pager base station as described herein;

Fig. 3 illustrates an embodiment of an emergency alert pager device as described herein;

Fig. 4 illustrates another embodiment of an emergency alert pager device as described herein;

Fig. 5 illustrates another embodiment of an emergency alert pager device as described herein;

Fig. 6 illustrates another embodiment of an emergency alert pager base station as described herein;

Fig. 7 illustrates an embodiment of an emergency alert pager repeater as described herein;

DESCRIPTION OF CERTAIN EMBODIMENTS

The emergency alert pager system is particularly suited to college and public school campuses, groups of law enforcement resources at national events, business campus environments, and the like. The emergency alert pager system is designed to address critical incidents where mass notification of threat information has to be disseminated at extreme speed. The emergency alert pager system allows for two-way communication between individuals and a dispatch center. That is, an individual can send an alert or alert message to the dispatch center and the dispatch center can send an alert or alert message to an individual, a group of individuals, or all individuals on the system. The emergency alert pager system is preferably a stand alone system utilizing its own networks and communications equipment and protocols. Thus, there is no reliance on third party equipment and networks, allowing for faster and more reliable delivery of alerts and/or alert messages.

Using the Virginia Tech incident as an example to conceptualize the emergency alert pager system, the college used email as an alert system, but it was too slow and ineffective in notifying the student body and faculty because not everyone is looking at email at the same time. Text messaging with phones also was flawed due to numerous issues, including the fact that it took approximately 30 plus minutes to notify the 18,000 subscribers. The seriousness of the problem is more clearly seen when you realize there are over 30,000 students and faculty at Virginia Tech. Additional evidence that the cell phone / email systems are not the answer to the problem is seen in the number of universities going back in time 60 years with the adoption of tornado sirens as a band-aid solution to instantaneous, mass notification of a threat. However, an obvious deficiency is that a siren only indicates that there is "a problem." It does not tell you what the problem is, where the problem is, or where to go for safety. The emergency alert pager system does all of that, and more.

The emergency alert pager system is particularly well suited for protecting groups of people within a specified area, but is simultaneously effective for use as an alert system capable of providing individual security. In the case of Virginia Tech, for example, instead of 30 or more minutes passing by before approximately 2/3 of the university population was warned of a double homicide, the emergency alert pager system could notify all 30,000 people in less than one second of sending the message. The campus shooting rampage actually took place about two hours after the initial double homicide, but students and faculty/staff were not notified of the threat in time to avoid the ensuing tragedy.

According to the emergency alert pager system described herein, instead of a dispatch center getting numerous phone calls that are slow and cumbersome and have to be repeated, a

dispatch center equipped with the emergency alert pager system main controller / monitoring station could receive instantaneous alerts from each person equipped with a personal alert pager device in the threat area. Upon becoming aware of any threat, including upon receipt of the first alert from a personal alert pager device, the dispatch office can use the main controller to send an alert to every other person having a personal alert pager device, alerting everyone on campus in less than one second.

Each alert received by the main controller can be displayed on a monitor, preferably with each personal alert device represented by points of light on a graphical map screen representing the whole campus. As the points of light appear, as alerts are being received instantaneously, the dispatch center can alert first responders to the exact location of numerous threat origination points- the exact location being indicated by the GPS position of the personal alert pager device sending the alert. Additionally, the monitor can also "poll" each personal alert device if desired, to determine the exact location of each personal alert pager device, even such devices which have not sent an alert to the main controller.

The main controller can also send a warning alert of the threat area to every person on campus in under one second, if they have the personal alert pager device. The points of light graphically representing every alert sent from a personal alert paging device also can trace a "path" that the threat is taking, thereby speeding up the response of law enforcement. The exact location of each point of light will be displayed as the GPS coordinates of each personal alert pager device that transmits an alert to the main controller.

Additionally, RFID technology can be added to multitask with the personal alert pager device, allowing the device to be used for gaining access to buildings, secure areas, and the like which can be designated as safe areas for people to seek refuge from the threat.

As noted above, each personal alert pager device cannot only receive an alert, it can send an alert to the monitoring station. Consequently, the personal alert pager device can also serve as an individual panic alarm in the case of an attack, assault, abduction, and the like. The two-way alert capability, i.e., two-way communication between the personal alert pager device and the monitoring station, is believed to be unique to the emergency alert pager system.

Referring now to the drawing figures, an embodiment of the private network emergency alert pager system 10 is illustrated in Fig. 1. As further shown in Figs. 2 and 3, the system 10 generally comprises:

- a main controller 12;
  - which can comprise a computer 20, one or more associated monitors 22 for displaying data, a base antenna 24, an optional repeater 16 for better range or to deal with obstructions.

- a plurality of pods 14;
  - each in 2-way communication with the base station 12, and each pod 14 comprising (as described in more detail below in connection with Sheet 2/2) one or more of a transceiver 26 and associated antenna, a GPS module 28 and associated antenna, text display screen 30, and alert buttons/switches 32.

- a repeater 16.

The system is comprised of at least one portable unit 14, but preferably many portable units 14, or pods, and a single main security controller 12 (which may alternatively be referred to as a main controller, master controller, monitoring station, or base station). Each pod 14 can be handheld or wearable by a user. When a pod is activated, it sends its location to software of the main controller. The main controller shows the pod on a screen 18 along with pertinent information. The main controller can send back a message to the individual pod or a general announcement to all pods. If a pod user is missing, their pod can be polled as to its whereabouts and status. Pods can be deployed in a wide screen search, and repeaters can increase the range of the system.

The emergency alert pager system described herein can generally be comprised of the main controller that monitors and processes emergency calls from multiple sources, primarily large numbers of portable units (which may alternatively be referred to as a personal alert pager device, or a pod). The system preferably utilizes a private area wireless network, mainly for reasons of speed and robustness, and avoids all the disadvantages of public service networks. As a stand-alone system, there are no associated cellular phone costs or rental agreements to deal with. For example, the pods can number up to 250 thousand. Each pod can be roughly the size of a small cell phone, and can include, inter alia, a complete spread spectrum digital transceiver system, a high sensitivity GPS receiver, and a visual and audible alert complete with vibrating silent alert. The visual alert can comprise, for example, a two line alpha numeric display (which can be an LCD display) which can deliver detailed threat information and emergency instructions to all units in under 30 seconds.

The emergency alert pager system can use pager technology with one or more of a variety of alert notification systems, such as text messaging on LCD display screens, audible alert tones, vibrating alerts, and GPS technology as well as RFID (radio frequency identification) technology. When the system operates on a private network, it is a closed, i.e., private, system. It does not rely on a third party to wait for a dial tone, an operator in emergency operations, or

the relatively clumsy transfer of oral or typed information. Nor does law enforcement need to perform a GPS type triangulation.

The pod is unique in that it can not only receive an alert (by text, vibration alert, or audible alert) from the base or monitoring station, but can also send an alert to the monitoring station, via a spread spectrum transceiver, for example, by activation of one or more switches, buttons, or the like. An alert may be a message, for example, "emergency", "need assistance", or the like.

Each pager-like pod can also be tracked by GPS, and can thus be located by the monitoring station after an alert is sent to the base station. The GPS information from the last valid fix is transferred to the controller in under one second, along with the ID number of that pod. In a fight or flight situation, the average, untrained person could forget their own name, much less their relative position in relation to the event. Thus, the GPS position is vital information that is gathered from each pod.

In addition to receiving alerts from individual pods, the main controller can simultaneously send instructions to select individual pods, or a general broadcast to all pods, or all pods in a certain area. If desired, pods can be prioritized by groups or individuals (teachers, security staff, administration, and others). Each pod can have a unique identification code. The system can also be used for general announcements to the student body/faculty or page a specific individual in the network in under one second from the message being typed.

Each pod can also be provided with RFID keycard type system capability for ingress to buildings, as well as restricted or secure areas. The RFID capability, which functions similar to bar coding, can enable the pod to "scan" across a receiver such as a card reader to electronically unlock secure doors.

The software interface can comprise, inter alia, a database containing identification (ID) information for each device within the specified area being served by the system, and can include graphic mapping for a specified area that all the pods operate within. This can be displayed as a map on a computer monitor associated with the main controller, wherein each pod can be displayed as a "points of light" on the map. Depending on application, each pod can appear as a point of light when an alert is sent to the monitoring station, when the pod is alerted by the monitoring station, and/or when the pod is queried by the monitoring station. The main controller software can be designed to provide a dropdown window containing information including current GPS coordinates for each pod. Multiple display screens can be provided associated with the main controller, and the pod locations can be displayed simultaneously on one screen, while the main database can be displayed on a different screen, or screens.

The pod can be configured to transmit its GPS location to the main controller both when the pod sends an alert to, and when it receives an alert from, the main controller. Additionally, the main controller can "poll" or "ping" the pod to determine its GPS location. Thus, if a user/pod is unaccounted for, the pod can be pinged to activate the pod to transmit its GPS coordinates to the main controller. Each pod can also store a history of its GPS coordinates, in case there is a need for that information. Line of sight range is in excess of three (3) miles, and repeaters can be used for extended range or blind spots behind obstructions. The pods are rechargeable, and will last up to three (3) days on a single charge.

In Fig. 4, the pod 14 is broadly illustrated and can generally comprise:

- a spread spectrum transceiver 26
  - For example a 250 mW transceiver in the 900 MHz band.
- a GPS receiver 28 and active antenna
  - To receive and decode the GPS positional signal.
- a movement sensor 34
  - To sense movement for higher resolution GPS fixes and power saving.
- a vibrating motor and piezo sounder 36
  - For audible and tactile feedback during alert.
- an LED display 30
  - For text readout of alert information.
- battery control and charge circuitry 38
- emergency alert switches 32
  - For activating an alert to the main controller.
- a microcontroller 40
- an optional keypad 42
  - Could permit text messages to be sent from the pod to the main controller to provide details about the threat.
- an optional RFID module 44
  - Could be utilized to gain access to safe/secure areas, buildings, etc.

The pod can be configured to send an alert to the base station, for example, by pushing two buttons (switches) at the same time. Alternatively, a specific button sequence can also be programmable to the system or user's preference. The buttons can be recessed into the case to prevent accidental alerts.

The pod transfers information to the master controller, for example, using a state of the art, embedded spread spectrum transceiver. The transceiver preferably transmits in the 900 MHz region at a power level of approximately 250 mW. This level of power ensures a line of sight range in excess of two (2) miles. The use of spread spectrum technology rapidly changes the transmit frequency many times a second. If there is an in band signal, either noise or active jamming, this makes the transmission much less likely to be interfered with. If a transmission is received intact, an acknowledgement is sent by the master controller. If, for some reason, the transmission is not properly received, it will be resent, for example, up to 26 times, to complete transmission.

A text type keypad can be installed on the pod, which provides the capability to send more detailed information to the base station. However, in emergency situations, there typically is no time to send a text message and keeping operation as simple as possible, i.e., just pushing the buttons, can be desirable.

The latest generation of GPS chipsets uses an extremely high sensitivity and high speed correlator to decode the available GPS signals. Combined with a very reliable helically wound antenna, the system can lock onto very weak signals. The need to be outdoors, in a large field with no obstructions of the sky, is a thing of the past. Indoor fixes of position are much more reliable. The GPS unit can simultaneously track up to 20 satellites for very accurate positional information.

If the pod loses "sight" of enough satellites for a fix, it will transmit the last good fix received, along with the time of the fix. This gives the main controller (and the first responders) more information than just the pod ID number-- it provides a place to begin the search.

Under a worst case scenario, where a pod cannot get a position fix, and the last fix is very old, the pod can be tracked using RF tracking techniques to recover the pod. All pod IDs are encoded, so the possibility of an unauthorized user tracking a pod is very unlikely.

The following list of features is provided by way of example only, merely to highlight some features of the private network emergency alert pager system. This list is not an all inclusive list of every possible feature, and more features will be apparent to one of ordinary skill in the art upon reading of this disclosure.

A. This is a two-way alert system; main controller to individual pods and individual pods to main controller.

B. Alerts can be sent to one or all pods simultaneously, with audible, silent, tactile and/or text messaging format.

C. Alerts are extremely high speed, unlike typical text messaging systems relying on email or cell-phone devices.

D. Each pod is traceable by internal GPS modules in every pod.

E. The physical location of each pod can be displayed as a point of light on a computer monitor to immediately reveal the exact GPS coordinate of each pod sending or receiving an alert.

F. The points of light appearing on the main controller monitor serve as real-time threat locaters enabling real-time threat tracking, by means of each additional alert being sent to the main controller as the threat moves within the service area, such as a college campus, other compounds, or other types of areas.

G. The pods can be RFID-scanning capable for gaining entrance to safe or other secured areas.

H. The pods can be identified with individual data saved in a separate data-base that works in conjunction with the main controller; a "mouse-over" feature can be programmed to allow the controller to identify the registered user of the alerting pod as it appears as a point of light on the monitor.

Referring to Fig. 5, an embodiment of a pod 14 is illustrated. The pod 14 includes:

- μC – Microcontroller 46 – The firmware resides on this device, which provides an interface to the all of the components in the circuit and controls the user interface menus.
- Shake sensor 48 – Chatters if the unit is moved in order to facilitate power savings and GPS tracking.
- User Buttons 50 – allows the user to interact with the unit in order to scroll through menus and to signal an emergency situation.
- Accelerometer 52 – allows the unit to perform dead reckoning, which allows the system GPS to track even when in places where the GPS signal is too low to function normally as well as facilitating power savings. This would replace the shake sensor if used.
- Mini-USB Connection 54 – provides USB data interface as well as charging voltage.
- USB data lines/voltage protection 56 – this entails the use of two separate chips that protect the microcontroller and other integrated circuits from voltage spikes both on the USB data lines and input voltage (+5VDC).
- Battery charge/current limit 58– two integrated circuits work together to accomplish several functions, which are: safely charging the 4.2V lithium-ion battery, limiting the total amount of current drawn from a connected USB port to 500mA or 100mA depending on the port limitations, managing that total current by distributing it to the unit and the battery charge current, which effectively allows the unit to run while charging the battery, provides feedback to the Microcontroller about battery charge status, battery fault conditions, input power status, allows the Microcontroller to change the current limitation mode and shut down the battery charge function.
- Power regulator 60 – provides a regulated 3.0Vdc for the components in the circuit using the battery/charger voltage as an input.

- Motor 62 – serves to vibrate the unit in order to call the attention of the user.
- Display (LCD) 64 – serves as the main interface to the user, which allows the user to see pertinent information on the display as well as scroll through the user menus.
- Beeper 66 – 4 kHz Piezo buzzer serves to call attention to the unit by providing a "beep" of an arbitrarily significant volume.
- GPS module 68 – provides the current GPS coordinates to the Microcontroller.
- GPS antenna 70 – allows the GPS module to receive GPS data from the satellites.
- 900 MHz RF Module 72 – transmits and receives 900MHz frequency-hopping-spread-spectrum data, which allows the units to interface to the main hub wirelessly.
- RF Filtering/switching 74– facilitates reliable and efficient transmitting and receiving of the 900MHz wireless data.
- 900 MHz antenna 76 – radiates and receives the 900 MHz wireless data transmissions.

Referring to Fig. 6, an embodiment of a base station 12 is illustrated. The base station 12 includes:

- μC – Microcontroller 78 – The firmware resides on this device, which provides an interface to the all of the components in the circuit and controls the user interface menus.
- Mini-USB Connection 80 – provides USB data interface as well as charging voltage.
- USB data lines/voltage protection 82 – this entails the use of two separate chips that protect the microcontroller and other integrated circuits from voltage spikes both on the USB data lines and input voltage (+5VDC).
- Current limit 84 – only one integrated circuit will assure that the circuit cannot draw more than the maximum allowed by the USB port specification, which is 500 mA for most although some can be 100 mA depending on the port type.
- Power regulator 86 – provides a regulated 3.0Vdc for the components in the circuit using the battery/charger voltage as an input.
- Display (LCD) 88 – serves as the main interface to the user, which allows the user to see pertinent information on the display as well as scroll through the user menus.
- Beeper 90 – 4 kHz Piezo buzzer serves to call attention to the unit by providing a "beep" of an arbitrarily significant volume.
- GPS module 92 – provides the current GPS coordinates to the Microcontroller.
- GPS antenna 94 – allows the GPS module to receive GPS data from the satellites.
- 900 MHz RF Module 96 – transmits and receives 900MHz frequency-hopping-spread-spectrum data, which allows the units to interface to the main hub wirelessly.
- RF Filtering/switching 98 – facilitates reliable and efficient transmitting and receiving of the 900MHz wireless data.
- 900 MHz antenna 100 – radiates and receives the 900 MHz wireless data transmissions.

Referring to Fig. 7, an embodiment of a repeater 16 is illustrated. The repeater 16 includes:

- μC – Microcontroller 102 – The firmware resides on this device, which provides an interface to the all of the components in the circuit and controls the user interface menus.
- Power connection 104 – allows an external 5Vdc power source to be connected directly.

- Voltage protection 106– one chip protects the circuitry from spikes on the input voltage.
- Bat charge/current limit 108 – two integrated circuits work together to accomplish several functions, which are: safely charging the 4.2V lithium-ion battery, limiting the total amount of current drawn from a connected USB port to 500mA or 100mA depending on the port limitations, managing that total current by distributing it to the unit and the battery charge current, which effectively allows the unit to run while charging the battery, provides feedback to the Microcontroller about battery charge status, battery fault conditions, input power status, allows the Microcontroller to change the current limitation mode and shut down the battery charge function.
- Power regulator 110 – provides a regulated 3.0Vdc for the components in the circuit using the battery/charger voltage as an input.
- Display (LCD) 112 – serves as the main interface to the user, which allows the user to see pertinent information on the display as well as scroll through the user menus.
- Beeper 114 – 4 kHz Piezo buzzer serves to call attention to the unit by providing a "beep" of an arbitrarily significant volume.
- GPS module 116 – provides the current GPS coordinates to the Microcontroller.
- GPS antenna 118 – allows the GPS module to receive GPS data from the satellites.
- 900 MHz RF Module 120 – transmits and receives 900MHz frequency-hopping-spread-spectrum data, which allows the units to interface to the main hub wirelessly.
- RF Filtering/switching 122 – facilitates reliable and efficient transmitting and receiving of the 900MHz wireless data.
- 900 MHz antenna 124 – radiates and receives the 900 MHz wireless data transmissions.

What has been described above includes exemplary embodiments of a private network emergency alert pager system. It is, of course, not possible to describe every conceivable combination of components or methodologies for purposes of this description, but one of ordinary skill in the art may recognize that further combinations and permutations are possible in light of the overall teaching of this disclosure. Accordingly, the description provided herein is intended to be illustrative only, and should be considered to embrace any and all alterations, modifications, and/or variations that fall within the spirit and scope of this description, and any appended claims.

What is claimed is:

1. An emergency pager alert system, comprising:

a. at least one personal alert pager device;

b. a main controller in two-way communication with each personal alert pager device; and

c. wherein each personal alert pager device comprises:

i. a transceiver for receiving alerts from the main controller and for sending alerts to the main controller;

ii. an alert notification system;

iii. at least one switch for initiating the sending of an alert to the main controller; and

iv. a GPS module for providing location data of the personal alert pager device to the main controller.

2. The system of claim 1 wherein each personal alert pager device comprises an RFID module.

3. The system of claim 1 wherein each personal alert pager device comprises a key pad.

4. The system of claim 1 wherein the alert notification system is a display.

5. The system of claim 4 wherein the display is a text display.

6. The system of claim 1 wherein the alert notification system is a speaker.

7. The system of claim 1 wherein the alert notification system is a vibration motor.

8. The system of claim 1 wherein the system is configured to operate on a closed network system.

9. The system of claim 1 wherein the main controller comprises a screen configured to display location data of each personal alert pager device.

10. The system of claim 1 further comprising a repeater in communication with the main controller and each personal alert pager device.

11. A personal alert pager device, comprising:

a. a transceiver for receiving alerts and for sending alerts;

b. an alert notification system;

c. at least one switch for initiating the sending of an alert; and

d. a GPS module for providing location data of the personal alert pager device.

12. The device of claim 11 further comprising an RFID module.

13. The device of claim 11 further comprising a key pad.

14. The device of claim 11 wherein the alert notification system is a display.

15. The device of claim 14 wherein the display is a text display.

16. The device of claim 11 wherein the transceiver is configured to be in two-way communication with a main controller.

17. A method for emergency alerts, comprising the steps of:

providing a main controller;

providing at least one pod in two-way communication with the main controller;

sending an alert from the main controller to the at least one pod in an emergency situation; and

sending an alert from the at least one pod in an emergency situation.

18. The method of claim 17, wherein a plurality of pods are provided and further comprising the step of providing an alert from the main controller to a sub-set of the plurality of pods in an emergency situation.

19. The method of claim 17 further comprising the step of providing a location of the at least one pod to the main controller.

20. The method of claim 17 further comprising the step of using the at least one pod as a security device during an emergency situation.

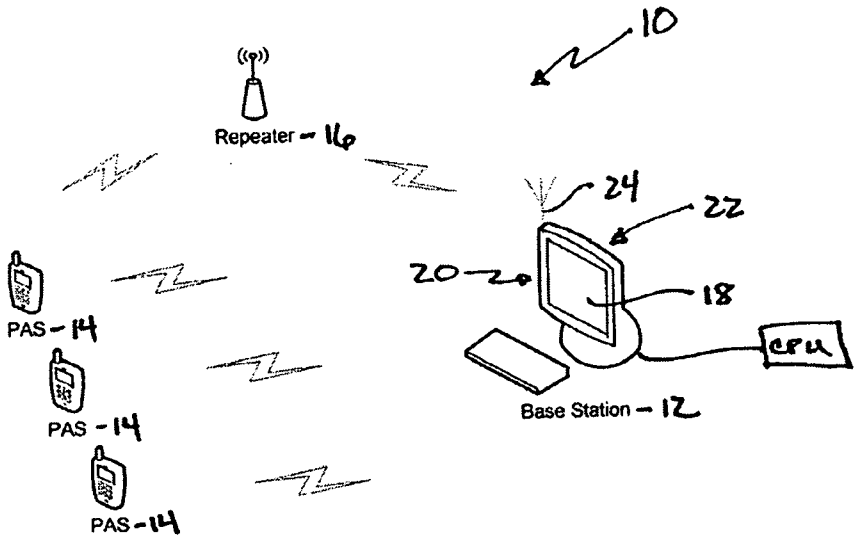
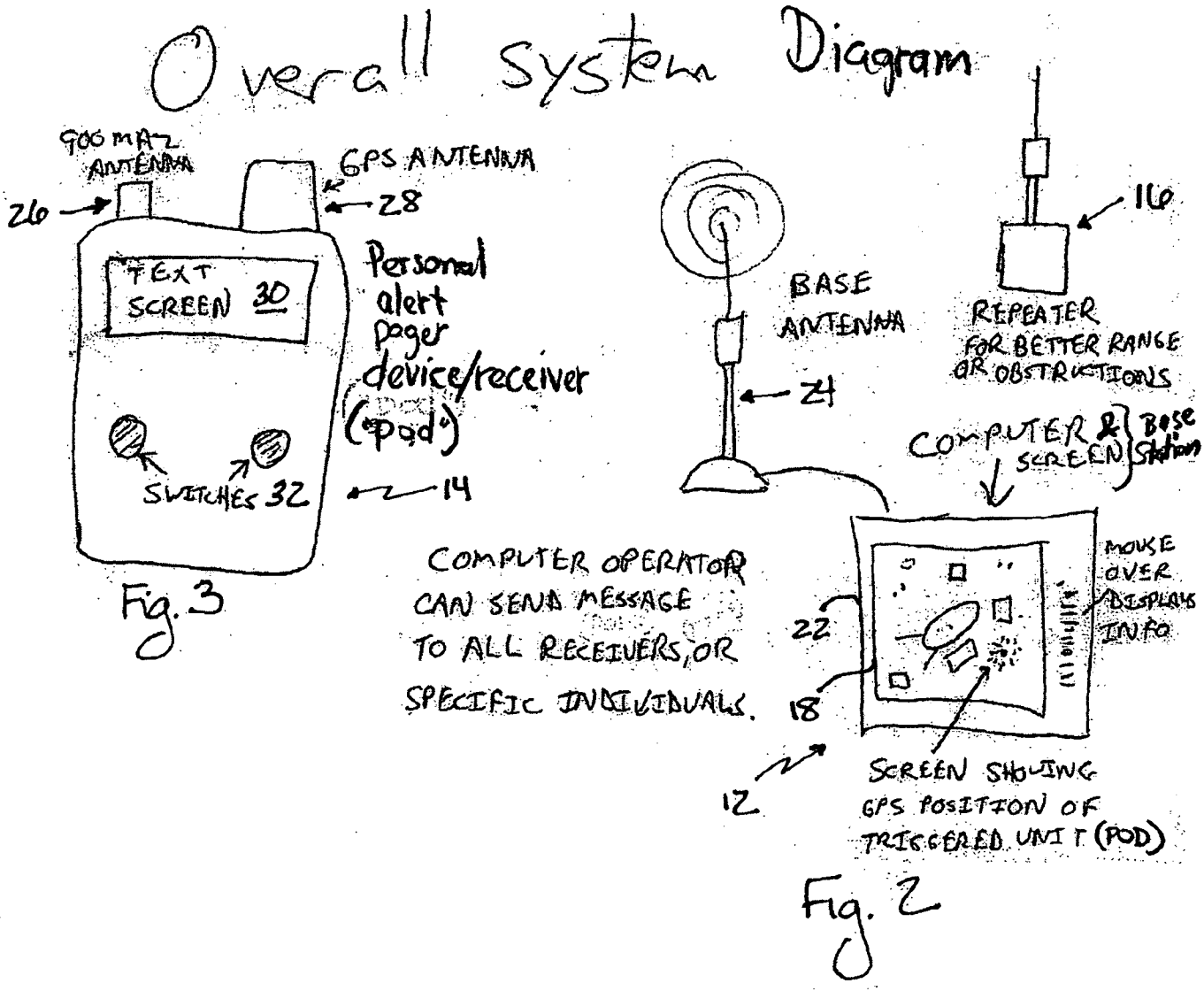

10
Repeater – 16
24
22
20
18
CPU
PAS – 14
PAS – 14
PAS – 14
Base Station – 12

Fig. 1


Overall System Diagram
900 MHz ANTENNA
GPS ANTENNA
26
28
TEXT SCREEN 30
Personal alert pager device/receiver ("pod")
SWITCHES 32
14
Fig. 3
BASE ANTENNA
24
16
REPEATER FOR BETTER RANGE OR OBSTRUCTIONS
COMPUTER & SCREEN
Base Station
COMPUTER OPERATOR CAN SEND MESSAGE TO ALL RECEIVERS, OR SPECIFIC INDIVIDUALS.
22
18
12
MOUSE OVER DISPLAYS INFO
SCREEN SHOWING GPS POSITION OF TRIGGERED UNIT (POD)
Fig. 2

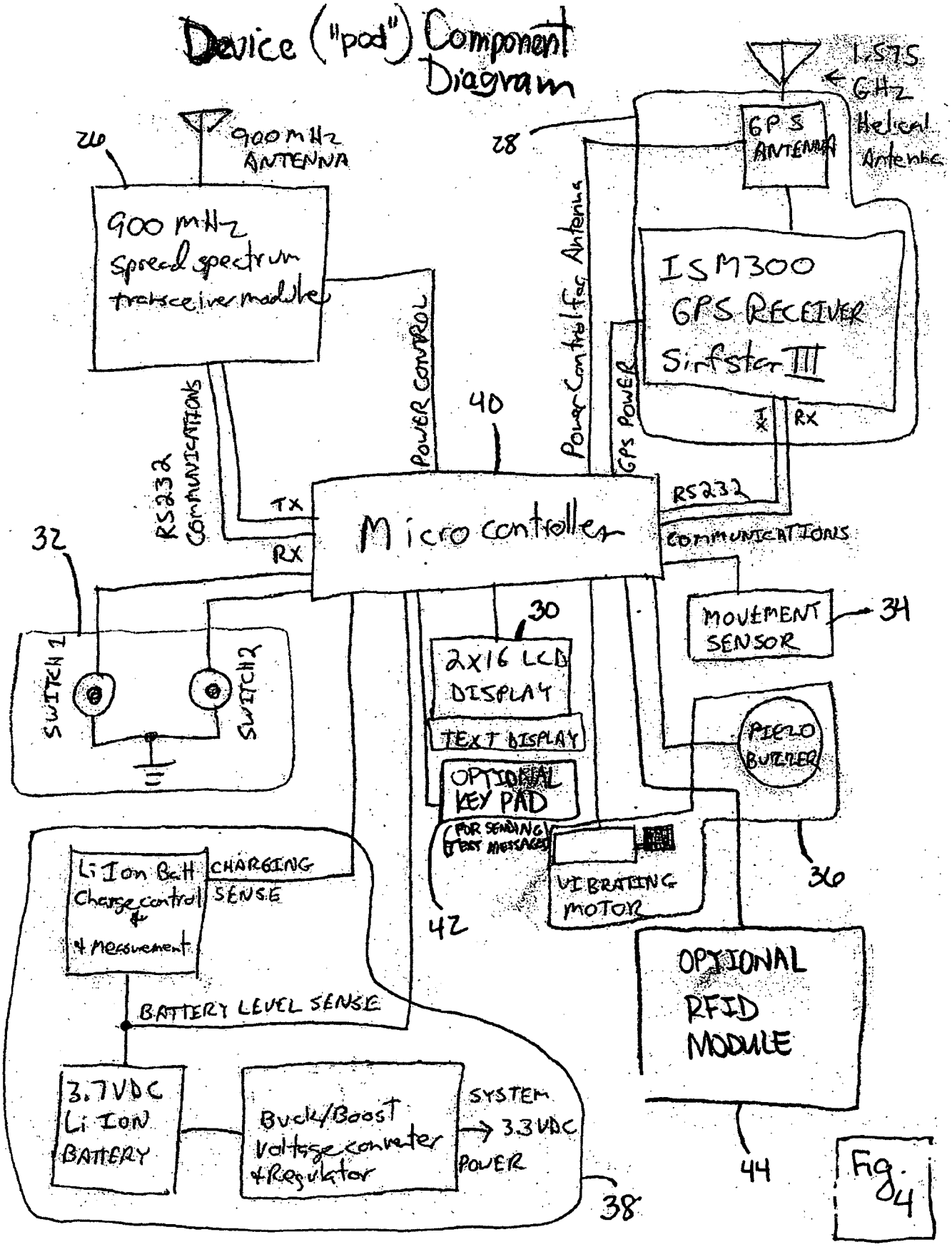

Device ("pod") Component Diagram
900 mHz ANTENNA
20
900 mHz spread spectrum transceiver module
RS232 COMMUNICATIONS
TX
RX
POWER CONTROL
40
Micro controller
32
SWITCH 1
SWITCH 2
30
2X16 LCD DISPLAY
TEXT DISPLAY
OPTIONAL KEY PAD
(FOR SENDING TEXT MESSAGES)
42
Li Ion Batt Charge control & measurement
CHARGING SENSE
BATTERY LEVEL SENSE
3.7VDC Li ION BATTERY
Buck/Boost Voltage converter & Regulator
SYSTEM 3.3VDC POWER
38
28
GPS ANTENNA
1.575 GHz Helical Antenna
Power Control for Antenna
GPS POWER
ISM300 GPS RECEIVER Sirfstar III
TX
RX
RS232 COMMUNICATIONS
MOVEMENT SENSOR
34
PIEZO BUZZER
36
VIBRATING MOTOR
OPTIONAL RFID MODULE
44

Fig. 4

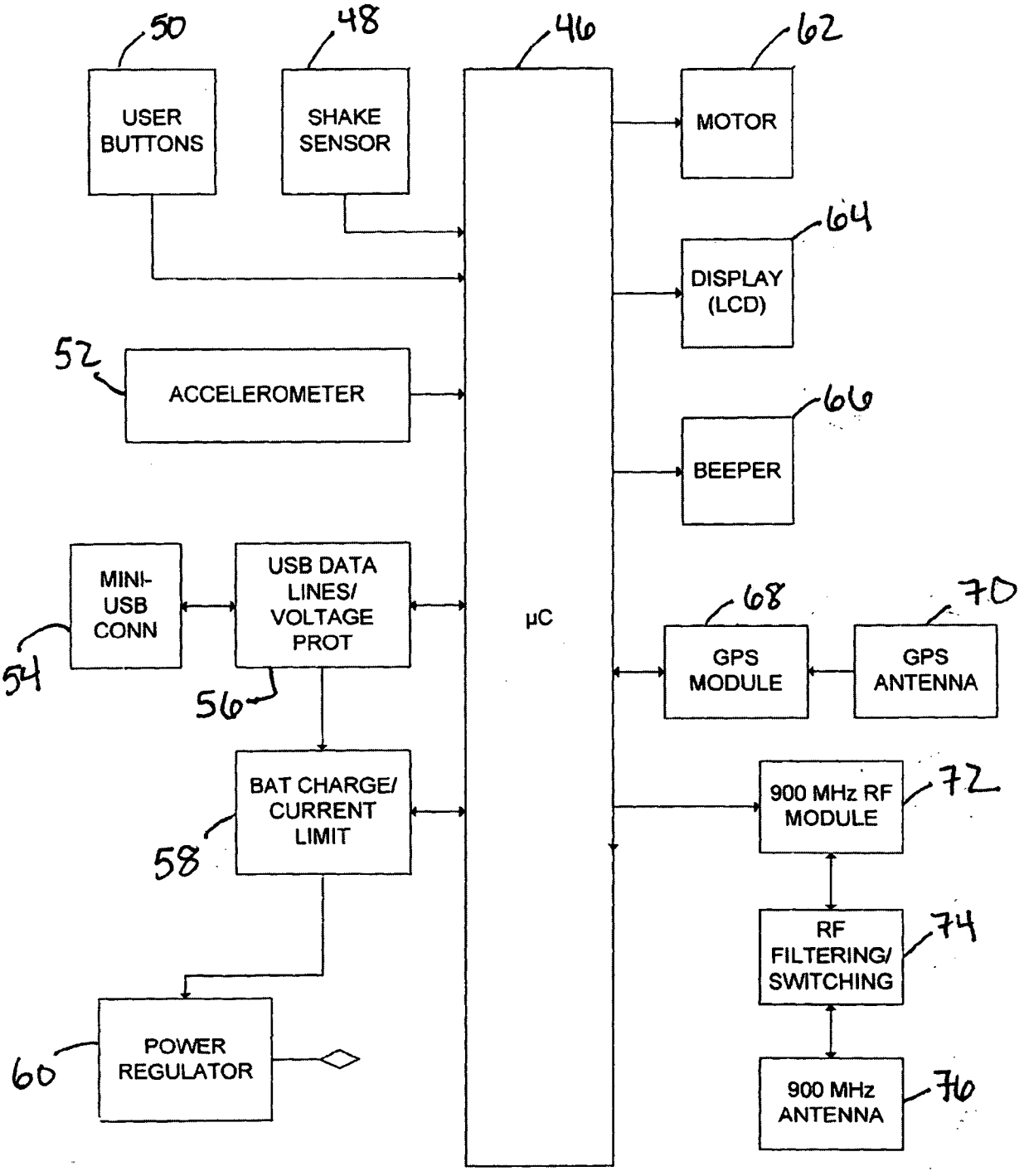

50
48
46
62
USER BUTTONS
SHAKE SENSOR
MOTOR
64
DISPLAY (LCD)
52
ACCELEROMETER
66
BEEPER
MINI-USB CONN
USB DATA LINES/ VOLTAGE PROT
µC
68
70
GPS MODULE
GPS ANTENNA
54
56
BAT CHARGE/ CURRENT LIMIT
900 MHz RF MODULE
72
58
RF FILTERING/ SWITCHING
74
60
POWER REGULATOR
900 MHz ANTENNA
76
Personal Alert Security 14

Fig. 5

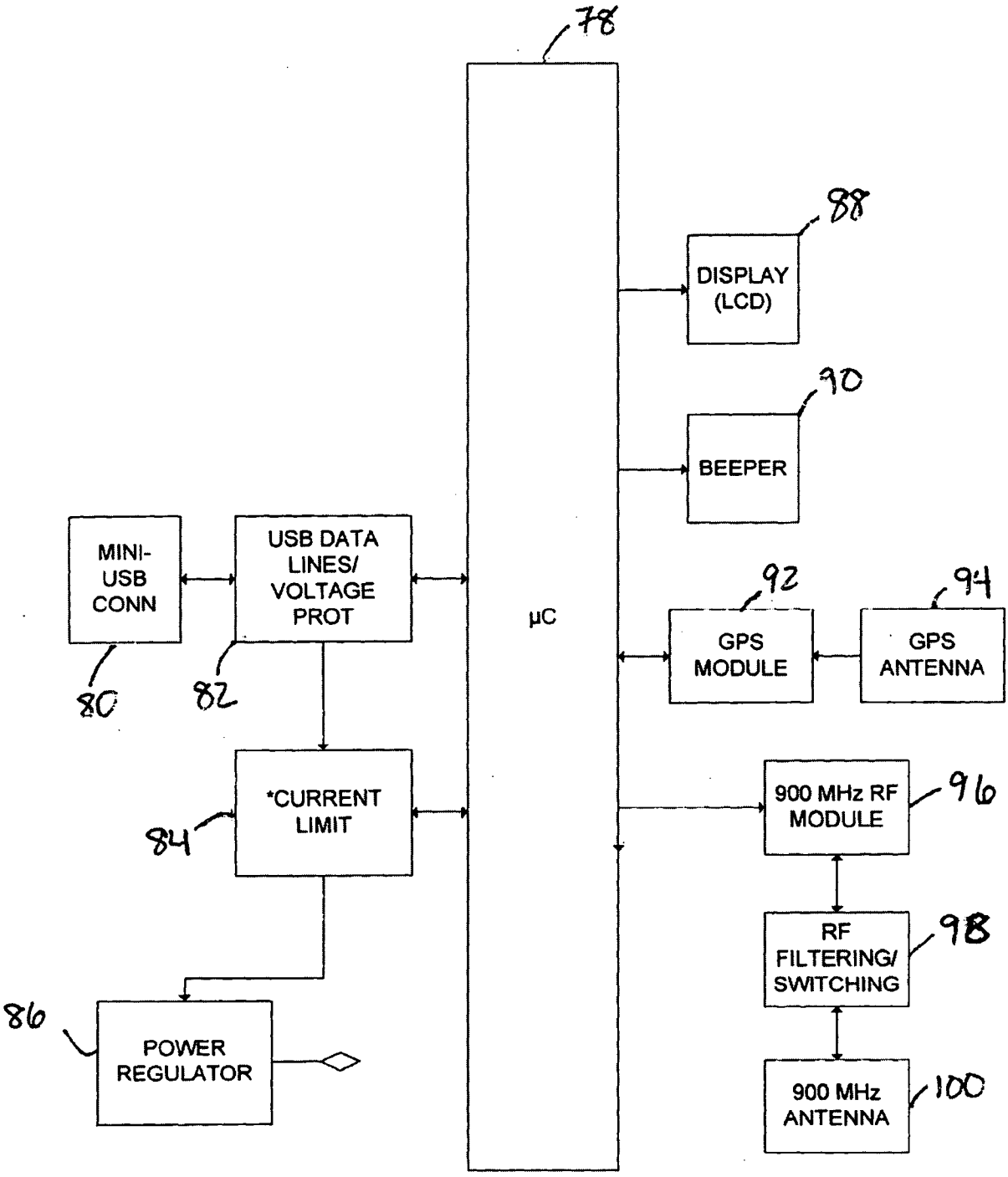

78
88
DISPLAY (LCD)
90
BEEPER
MINI-USB CONN
USB DATA LINES/ VOLTAGE PROT
μC
92
GPS MODULE
94
GPS ANTENNA
80
82
*CURRENT LIMIT
84
900 MHz RF MODULE
96
RF FILTERING/ SWITCHING
98
86
POWER REGULATOR
900 MHz ANTENNA
100
Home Base (HUB) 12

Fig. 6

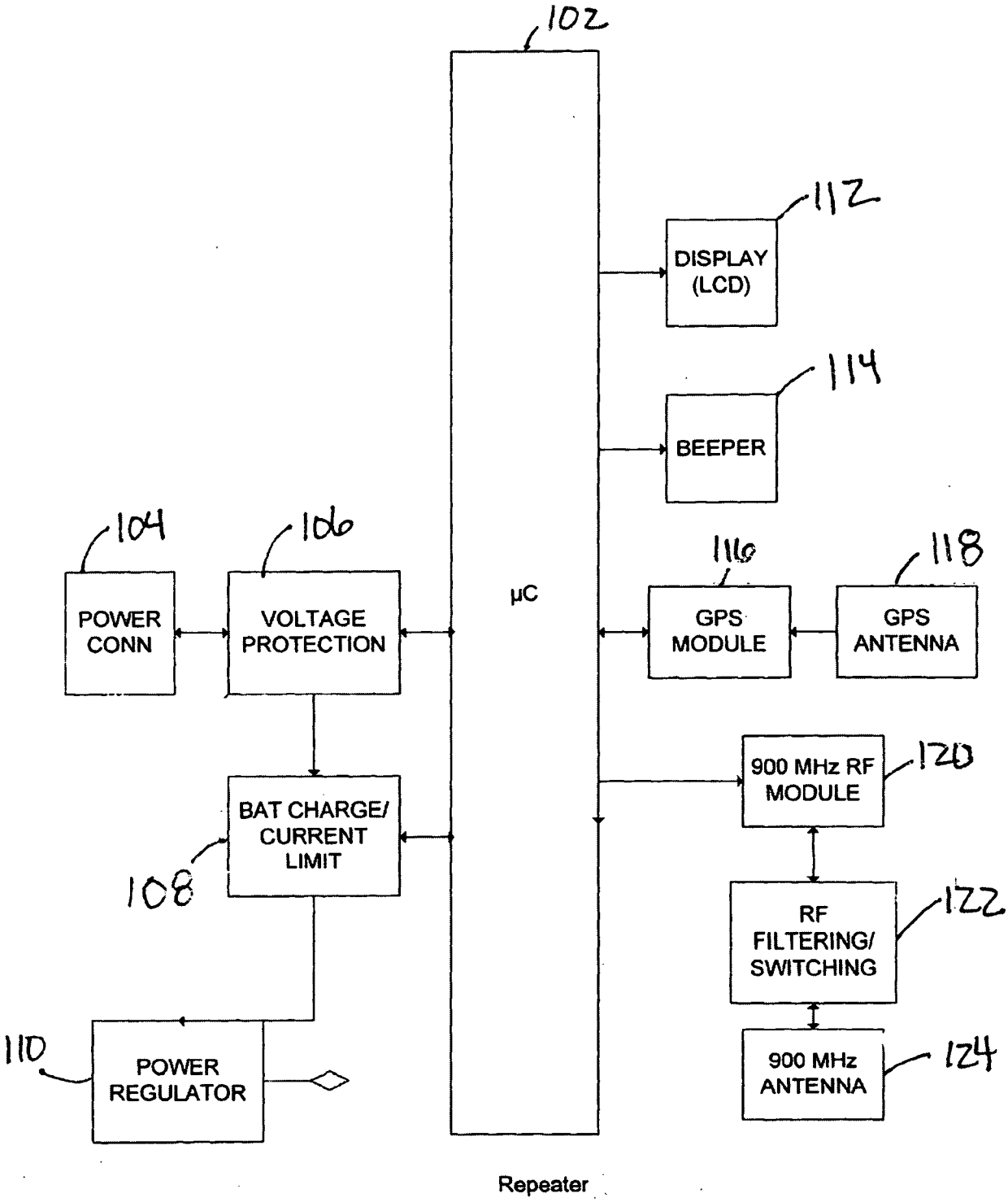

102
µC
112
DISPLAY (LCD)
114
BEEPER
104
POWER CONN
106
VOLTAGE PROTECTION
116
GPS MODULE
118
GPS ANTENNA
108
BAT CHARGE/ CURRENT LIMIT
120
900 MHz RF MODULE
122
RF FILTERING/ SWITCHING
110
POWER REGULATOR
124
900 MHz ANTENNA
Repeater

Fig. 7

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US2009/037280

A. CLASSIFICATION OF SUBJECT MATTER
IPC(8) - G08B 29/00 (2009.01)
USPC - 340/506
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC(8) - G08B 29/00 (2009.01)
USPC - 340/506

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
MicroPatent, Google Patent

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 2008/0048851 A1 (REYES et al) 28 February 2008 (28.02.2008) entire document	1-20
Y	US 2007/0293186 A1 (LEHMANN) 20 December 2007 (20.12.2007) entire docuemnt	1-20
A	US 6,774,795 B2 (ESHELMAN et al) 10 August 2004 (10.08.2004) entire document	1-20
A	US 7,245,216 B2 (BURKLEY et al) 17 July 2007 (17.07.2007) entire document	1-20

☐ Further documents are listed in the continuation of Box C. ☐

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
04 June 2009	12 JUN 2009
Name and mailing address of the ISA/US Mail Stop PCT, Attn: ISA/US, Commissioner for Patents P.O. Box 1450, Alexandria, Virginia 22313-1450 Facsimile No. 571-273-3201	Authorized officer: Blaine R. Copenheaver PCT Helpdesk: 571-272-4300 PCT OSP: 571-272-7774

Form PCT/ISA/210 (second sheet) (April 2005)