



(11) **EP 1 599 847 B1**

(12) **EUROPEAN PATENT SPECIFICATION**

(45) Date of publication and mention of the grant of the patent:  
**15.08.2007 Bulletin 2007/33**

(51) Int Cl.:  
**G08B 21/02** <sup>(2006.01)</sup> **H04M 11/04** <sup>(2006.01)</sup>  
**A61B 5/00** <sup>(2006.01)</sup> **G01S 5/00** <sup>(2006.01)</sup>

(21) Application number: **04711657.9**

(86) International application number:  
**PCT/GB2004/000640**

(22) Date of filing: **17.02.2004**

(87) International publication number:  
**WO 2004/072918 (26.08.2004 Gazette 2004/35)**

(54) **A TRACKING AND MONITORING APPARATUS AND SYSTEM**

VORRICHTUNG UND SYSTEM ZUR VERFOLGUNG UND ÜBERWACHUNG

APPAREIL ET SYSTEME DE SURVEILLANCE ET DE SUIVI

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

(72) Inventor: **DOUGLAS, Raymond**  
**Newcastle BT33 0PP (GB)**

(30) Priority: **17.02.2003 GB 0303586**  
**09.01.2004 GB 0400428**

(74) Representative: **Hanna, John Philip et al**  
**MacLachlan & Donaldson**  
**47 Merrion Square**  
**Dublin 2 (IE)**

(43) Date of publication of application:  
**30.11.2005 Bulletin 2005/48**

(56) References cited:  
**WO-A-02/32098** **US-A- 4 952 928**

(73) Proprietor: **Kinderguard Limited**  
**Hollywood BT18 9HF (GB)**

**EP 1 599 847 B1**

Note: Within nine months from the publication of the mention of the grant of the European patent, any person may give notice to the European Patent Office of opposition to the European patent granted. Notice of opposition shall be filed in a written reasoned statement. It shall not be deemed to have been filed until the opposition fee has been paid. (Art. 99(1) European Patent Convention).

## Description

**[0001]** The present invention relates to a tracking and monitoring apparatus and system and in particular to an apparatus and system for tracking and monitoring people who operate in a plurality of different environments.

**[0002]** The price of GPS units has dropped dramatically over the last number of years to such an extent that modern automobiles and watercraft have GPS units installed to assist the operator with navigation. Due to the increase in reported cases of child abduction in recent years as a result of the globalisation of large media companies in addition to the increase in popularity of so-called dangerous sports, such as mountain-climbing or off-piste skiing, which generally require remote locations, it has also become desirable to provide people with GPS tracking units. These units are particularly useful if the person wearing the unit is in distress and is able to generate a distress signal by activating an alarm on the unit.

**[0003]** The distress signal can be transmitted from the unit and a search and rescue team are able to accurately identify the whereabouts of the person in distress before attempting a rescue

**[0004]** One disadvantage associated with tracking devices of the prior art is that they are dependent upon the host to transmit distress signals. The GPS tracking units of the prior art are passive devices which interact with satellites only. In addition to this, there is a significant risk that if the tracking unit falls off a host and generates a distress signal as it hits the ground or is later interfered with by someone else or a wild animal, for example, the distress signal does not provide an accurate indication of the current location of the host but instead gives the location of the unit itself.

**[0005]** The closest prior art is outlined in W0 02/32098 which discloses a method for operating a wireless communication system having steps of operating a set of vital signs sensors that are affixed to a user; transmitting sensor-generated information to a wireless communicator such as a cellular/PCS telephone; comparing, in the wireless communicator, the sensor-generated information to a set of thresholds stored in or accessible by the wireless communicator and, upon an occurrence of sensor-generated information falling outside of a threshold, initiating an emergency call from the wireless communicator to an emergency response center. The emergency call includes at least some of the sensor-generated information and information describing a current location of the wireless communicator. The emergency call can further include other information that is descriptive of a medical condition of the user, such as the user's medical history and medications that are taken by the user. The other information can also be provided for use by the emergency services personnel, along with updated sensor-generated information that continues to be transmitted from the wireless communicator while the emergency services personnel are in route to the user. A physician's station can be provided for downloading the set of thresh-

olds and the optional other information into a memory that is accessible by the wireless communicator.

**[0006]** US 4,952,928 discloses a personnel monitoring system including a transmitting or transponding unit that is worn or carried by the individual being monitored, and which periodically, or upon request, transmits a uniquely encoded signal that identifies the person being monitored, as well as information about the condition or activities or the person being monitored as sensed by sensors, coupled to the transmitting unit. The system also includes a field monitoring device (FMD), that is positioned near the person being monitored, or at a location where the person being monitored should be found and a central processing unit (CPU), that automatically, or by request, receives and interprets data from the FMD. A communication link between the FMD and the CPU may be by way of existing telephone lines or other telecommunicative links.

**[0007]** It is an object of the present invention to obviate or mitigate the problems of prior art tracking units outlined above.

**[0008]** Accordingly, the present invention provides a programmable mobile unit for a portable host, such as a person, comprising a microcontroller in communication with each of

a detachable free space communication module for communication with a control centre,  
a GPS unit for communication with at least a GPS satellite system, and  
a biometric sensor, the biometric sensor and the microcontroller being configured to monitor and uniquely identify the host from biometric data specific to the host

**[0009]** Preferably, a set of communication modules are provided for use with the mobile unit and each module is configured to interface with different wireless protocols.

**[0010]** Ideally, the protocols include GPS, GSM, GPRS, Mode, 3G-UMTS and IEEE 802.11 WLAN. Advantageously, this allows various different types of mobile unit to be deployed in different situations such as enclosed theme parks, chemical plants or outdoor pursuits.

**[0011]** Preferably, the microcontroller has a control program stored thereon for receiving information from the GPS unit and the biometric sensor and storing the information in a local memory.

**[0012]** Ideally, the microcontroller has a database of acceptable behaviour parameters for the host stored in the memory of the unit. This database defines the boundaries of acceptable behaviour for the host including acceptable geographical locations for the host in addition to acceptable biological values such as body temperature and/or heart rate and/or bioelectrical impedance at any given point in time.

**[0013]** Preferably, the microcontroller has a control program stored thereon for comparing information re-

ceived from the GPS unit and the biometric sensor against the behaviour parameters database stored in on-board memory for a given host at any given time.

**[0014]** Ideally, the microcontroller is pre-programmed to periodically monitor and download up-to-date information from the GPS unit and the biometric sensor.

**[0015]** Preferably, the control program loaded in the memory of the microcontroller runs the information received from the GPS unit and the biometric sensor against the behaviour parameters database every time new location and biometric information is captured and downloaded from both the biometric sensor and the GPS unit.

**[0016]** Ideally, exception values falling outside allowable tolerances defined in the database are detected by an interpretation program also stored in the memory of the microcontroller.

**[0017]** Preferably, the interpretation program has means for prioritising these exception values and has means for selecting values which indicates that the host is encountering significant difficulties.

**[0018]** Ideally, the microcontroller transmits these selected values via the communications module to a control centre.

**[0019]** Alternatively, the microcontroller transmits these selected values via the GPS unit.

**[0020]** Ideally, the behaviour parameters database is remotely programmable to take new activities and routines of the host into account.

**[0021]** Preferably, the biometric sensor comprises a power source and a plurality of body contacting elements.

**[0022]** Ideally, the body contacting elements provide information indicative of activity of the host such as, body temperature, heart rate and respiration.

**[0023]** Preferably, the biometric sensor and the microcontroller communicate using bluetooth technology.

**[0024]** Ideally, the biometric sensor and microcontroller are configured to uniquely identify the host from biological data specific to the host during a learning phase when the sensor is first placed on the host and the unit is initially powered up.

**[0025]** Preferably, this unique identification is a biometric signature for the host and is used to benchmark subsequent data feeds from the biometric sensor.

**[0026]** Ideally, the biometric sensor is provided by a flexible multi-sensor patch which monitors ECG, temperature and respiration rate continuously. The sensor-based patch is disposable, low cost and user friendly, similar to current disposable ECG electrodes. The sensor patch is small and low profile, capable of being worn in a completely non-invasive manner.

**[0027]** Preferably, the device integrates patented screen printable ECG electrode technology with new micro-thermistors and piezo-electric based respiration sensors.

**[0028]** The patch is easily applied and remotely monitorable utilising freespace based communications such as Bluetooth. It is capable of connectivity with the micro-

controller either directly via a serial interface as part of an integrated solution, or using Bluetooth as part of an optional upgrade solution.

**[0029]** Preferably, the biometric sensor is provided with flexible circuitry to allow the sensor to adapt to the shape of the host's body.

**[0030]** In another embodiment of biometric sensor, the microcontroller has means for generating and transmitting signals into the body of the host and means for receiving and analysing the signals from the host's body via the biometric sensor, the signals being attenuated by bioelectrical impedance of the host's body whereby in use the analysis of the attenuated signals by the controller provides a bioelectrical impedance signature capable of uniquely identifying the host.

**[0031]** Bioelectrical impedance is measurable with simple technical instruments which facilitates the ability to miniaturise the biometric sensing technology to a degree suitable for implementation.

**[0032]** Ideally, the biometric sensor comprises two or more electrodes disposed on the host's skin.

**[0033]** Preferably, the means for generating and analysing signals comprises a software control module stored on the memory of the microcontroller, being executable on the processor.

**[0034]** Live biometric data describes information obtained from the person the sensor is currently mounted on as opposed to information from the person whose biometric data was originally recorded during a learning phase when the mobile unit is first put on.

**[0035]** Preferably, a host's bioelectrical impedance signature is stored on the memory of the mobile unit, this signature being recorded during initial enrolment and primary data calibration in a secure environment or during the learning phase as for the other biometric signatures.

**[0036]** Ideally, the software control module is capable of comparing the live bioelectrical impedance signature recorded with the bioelectrical impedance signature recorded during enrolment or learning phase.

**[0037]** Ideally, the software control module has error identifying means comprising robustly designed algorithms taking into account skin resistivity, sweat, geographical regionality, weight, age, gender, current, voltage measurement and frequency range.

**[0038]** Preferably, the biometric sensor has circuitry capable of generating a range of analogue signals of varying currents and frequency.

**[0039]** Essentially, the currents are of a magnitude to ensure safe passage through a hosts body.

**[0040]** Ideally, the currents are in the range of 100 $\mu$ A to 900 $\mu$ A.

**[0041]** Preferably, the frequency of the signals is in the range of 1 to 1350 KHZ.

**[0042]** Ideally, the software control module has means for identifying bioelectrical impedance characteristics representative of fat mass, body cell mass, extracellular water and skeletal mass.

**[0043]** Preferably, the software control module is ca-

pable of generating, transmitting, receiving and analysing signals in a time interval in the range of a few seconds to provide a host identified or host not identified output.

**[0044]** Ideally, the time interval is approximately one second.

**[0045]** Ideally, the biometric sensor circuitry has means for reading attenuated signals from one or more electrodes.

**[0046]** Preferably, the sensor circuitry has means for filtering the signal, converting the analogue signal to a digital signal and passing the signal to the processor for analysis.

**[0047]** Preferably, the algorithms have means of generating a unique bioelectrical impedance signature for a specific host from a full set of data including skin resistivity, sweat, geographical regionality, weight, age, gender, current, voltage measurement and frequency range. The algorithms may combine the impedance with other biometric data as may be required.

**[0048]** Ideally, the algorithms are capable of reducing the time required to identify a live host by utilising a subset of data selected from any combination of the above variables.

**[0049]** The present invention also provides a method of uniquely identifying a host comprising the steps of a controller generating and transmitting signals into the body of a host, the controller receiving signals from the host's body after they have been attenuated by the bioelectrical impedance of the host's body, the controller analysing the attenuated signals to produce a bioelectrical impedance signature capable of uniquely identifying the host.

**[0050]** Ideally, the method also comprises the step of the controller comparing a bioelectrical impedance signature of a host recorded during secure enrolment or the learning phase with a live bioelectrical impedance signature recorded from the current host's body for identification purposes.

**[0051]** Preferably, the method comprises generating and transmitting an electrical current over a range of frequencies into the host's body via at least one electrode and receiving the attenuated signal via the or each electrode, the sensor circuitry reading the resulting voltage drop for each frequency of the signal, filtering the attenuated signal, converting the signal from analogue to digital and passing the digital signal to the processor.

**[0052]** Preferably, the host wears the programmable mobile unit as jewellery or clothing with the electronic components incorporated therein. This type of equipment is commonly referred to as smart clothing.

**[0053]** Preferably, the mobile unit includes a Wide Area Augmentation System (WAAS). WAAS is a twelve channel receiver for improving the accuracy and integrity of GPS signals.

**[0054]** Ideally, the mobile unit has means for shielding itself from electromagnetic interference and other environmental signal interference sources.

**[0055]** Ideally, the mobile unit supports an Application

Programmers Interface (API) scripting language and graphical user interface (GUI). Advantageously, these features allow the definition of the acceptable behaviour rules regarding geographical location of the host relative to time and the upper and lower tolerances of the biometric data.

**[0056]** The present invention also provides a system for monitoring and tracking a host, such as a person, comprising a control centre in freespace communication with a mobile unit and a GPS satellite system, the mobile unit comprising a microcontroller in communication with each of

a detachable freespace communication module for communication with the control centre, a GPS unit for communication with at least a GPS satellite system, and a biometric sensor, the biometric sensor and the microcontroller being configured to monitor and uniquely identify the host from biometric data specific to the host.

**[0057]** Preferably, the control centre of the system and interested third parties are in communication via fixed / freespace communication protocols.

**[0058]** Ideally, the protocols include GPS, I EEE 802.11, GSM, iMode, ISDN, Internet, PSTN and Bluetooth.

**[0059]** Ideally, the mobile unit communicates with the control centre using freespace communication protocols.

**[0060]** Preferably, the protocols include GPS, I EEE 802.11, GSM, iMode and Bluetooth.

**[0061]** Ideally, an earth transceiver station is provided for communicating signals between the satellite system and the control centre.

**[0062]** Preferably, the acceptable behaviour database is also stored at the control centre for further analysis of exception values reported from the mobile unit.

**[0063]** Ideally, the system includes a web-based interface to a database driven secure environment for dynamic creation and modification of the acceptable behaviour database stored in the control centre and the mobile unit.

**[0064]** Preferably, the control centre includes means for alerting custodians and interested third parties of exception values via chosen fixed / freespace communication protocols.

**[0065]** Ideally, the behaviour rules are defined in software agents via a web-based GUI and downloaded to the mobile unit.

**[0066]** Preferably, the system has means for identifying that the mobile unit is no longer functioning or the mobile unit has lost contact with the host. Separation is recognised as the biometric sensor takes readings every 30 seconds and if no biosignals are received for an extended period of time then either the biosensor is no longer attached to the host or there is a malfunction with the mobile unit's communication system.

**[0067]** The present invention also provides a second

programmable mobile unit for tracking and monitoring a portable host comprising a microcontroller, a database stored in a memory of the microcontroller containing acceptable behaviour data for the host, a GPS location unit in communication with the microcontroller, a control program loaded in the memory of the microcontroller for detecting when signals from the GPS unit contain exception values which fall outside the parameters defined in the acceptable behaviour database.

**[0068]** Preferably, the database contains acceptable geographical location data and acceptable biological data as a function of time for a specific host.

**[0069]** Ideally, the second mobile unit also has a biometric sensor in communication with the microcontroller.

**[0070]** Preferably, the control program detects when signals from the biometric sensor contain exception values which fall outside the acceptable biological parameters defined in the acceptable behaviour database.

**[0071]** Ideally, the second programmable mobile unit is suitable for use with the system described above.

**[0072]** Preferably, both mobile units have means for supporting European Geostationary Navigation Overlay Service (EGNOS).

**[0073]** The present invention further provides a control program for controlling the operation of the monitoring and tracking system having means for generating and transmitting signals, interrogation means for receiving signals from a plurality of input means, interpretation means for analysing signals received from the interrogation means and alarm generating means operable in response to identification of exception values by the interpretation means.

**[0074]** Ideally, the signals received from input means include GPS input data and biometric input data.

**[0075]** Preferably, the interpretation means comprises a database of acceptable biological and geographical data for a host as a function of time and a set of encoded instructions for processing information captured from the GPS input data and biometric input data against the database to check for biological and geographical exception values falling outside acceptable tolerances defined by the database.

**[0076]** Ideally, the means for generating, transmitting and receiving signals includes encoded instructions for controlling the GPS transceiver and the communications module via a microprocessor.

**[0077]** Preferably, the set of encoded instructions of the interpretation means are terminate and stay resident software agents communicable between the mobile unit and the control centre.

**[0078]** The invention will now be described with reference to the accompanying drawings, which show by way of example only one embodiment of a programmable mobile unit and one embodiment of a system for monitoring and tracking a host wearing the mobile unit. In the drawings:

Figure 1 is a schematic drawing of the architecture

of a programmable mobile unit; Figure 2 is a pictorial drawing of a system for monitoring and tracking a host wearing the mobile unit; and

Fig. 3 is a schematic representation of the process of scripting the behaviour rules.

**[0079]** Referring to the drawings and initially to Figure 1 there is shown a programmable mobile unit indicated generally by the reference numeral 4. The unit 4 has a central microprocessor 10 (ARM) processing signals received by the unit 4. The processor 10 has a clock 21 and a power source 19 which also provides power for the GPS transmitter / receiver pair 28. The level of the power source 19 is constantly monitored by a power level sensor 18. A solar cell 20 is connected to the power source 19 providing an effective back-up storage supply in the event that the power source 19, such as a battery, runs flat. The processor 10 is able to sense the power level of the power source 19 and initiate a reduced power mode when appropriate.

**[0080]** A local memory 14 is provided for storing data obtained from a biometric sensor 23 and information received from the GPS receiver 28. The biometric sensor 23 has a power source 22 and includes a number of detectors 24, 25, 26 and 27 for receiving various information representing physical attributes of the hosts body such as skin type 24, body temperature 25, ECG 26 and respiration 27.

**[0081]** A logic and control unit 15 is in communication with the local memory 14 and the processor 10 and the logic and control unit 15 is also in communication with software 16 (terminate and stay resident agents TSR's). A database 17 is also stored in the memory 14 of the unit 4 containing a predetermined set of acceptable behaviour parameters which are used to benchmark the dynamic information received from the biometric sensor 23 and the

**[0082]** GPS receiver 28.

**[0083]** Microprocessor 10 is also in communication with and controls the operation of a communications module 9 and a GPS transmitter / receiver pair 28. A manually actuatable alarm 12 is located on the unit 4 allowing a host to transmit a distress signal via either the GPS transmitter 28 or the communication module 9. If the alarm 12 is activated by accident or the event causing the distress has passed, the host can de-activate the alarm by pressing the alarm disarm button 11. The mobile unit 4 also includes a radio frequency pulse generator 13 connected to the processor 10. This generator 13 facilitates close quarter detection.

**[0084]** In use, prior to normal operation of the mobile unit 4 the biometric sensor 23 is calibrated against the physical attributes of the specific host. At initiation, the biometric sensor 23 detects a number of key parameters including skin type 24, ECG 26, body temperature 25 and body respiration 27. After an initial learning period the biometric sensor 23 enters normal operation mode. During the learning period, the biometric sensor 23 issues

signals to the processor 10 of the mobile unit 4 using bluetooth technology. Within processor 10 there is logic and control to process the biometric data during these 30-60 seconds of the learning period. After this period has elapsed, the processor 10 creates a packet data unit (PDU) and transmits the combined biometric signals as a biometric signature 29 of the host to a control centre (see Fig. 2). Thereafter, the biometric signature 29 is used to monitor subsequent data feeds from the host and identifies potential/real exception conditions as a function of mapping the current biometric data feeds against the original biometric signature 29.

**[0085]** In normal operation, there is a high degree of mapping and adherence of current biometric data to that of the original biometric signature 29 derived during calibration. Any significant deviation from any/all parameters is identified as a potential exception value. The cause of this could vary from a change in activity application (from rest to exertion) or a change in environment (temperature, respiration). A real exception value is a result of a change in host (skin definition 24, ECG 26) or an unscheduled missing signal.

**[0086]** Such deviations in biometric signature 29 form part of the acceptable behaviour parameters which are constructed and profiled for any host.

**[0087]** The mobile unit 4 follows the following top-level sequence of operations during active mode:-

**[0088]** While power is available

- take local biometric readings every 30 seconds
- verify local storage 14 is available- delete data over 5 minutes old
- store biometric data as current signature 29
- verify signature data 29 against original calibrated signature 29
- compute GPS co-ordinates every 5 minutes
- verify GPS data in accordance with behaviour rules TSR Agent 16
- If any exception conditions exist then
- Create PDU with biometric, operational and GPS data
- Send PDU to a control centre 33 (see Figure 2) via relevant communications module 9

**[0089]** The mobile unit 4 follows the following sequence of operation during passive mode:-

**[0090]** While power is available

- If a request for a PDU from a control centre is received or a Local Alarm signal activated then
- take local biometric readings
- verify local storage 14 is available
- store biometric data as current signature 29
- compute GPS co-ordinates
- Create PDU with biometric, operational and GPS data
- Send PDU to the control centre 33 via a relevant communications module 9

**[0091]** On receipt of the relevant PDU from the unit 4 the control centre 33 determines if any attribute of the PDU represents an exception condition based on:

- host alarm signal activated manually
- host alarm signal activated automatically (tamper)
- host raised exception condition (spatial rule violation)
- host raised exception condition (biometric calibration violation)

**[0092]** The unit 4 either discovers that the exception condition has occurred on GPS or biometric attributes and informs the control centre 33, or the passive mode will return a PDLT and the control centre 33 processes the data against its behaviour rule database for this host. If the data passes the TSR agent 16 then the operational mode is maintained as normal.

**[0093]** The host has the ability to switch off the unit 4 and remove the biosensor 23 at pre-determined locations and events (including when at home, sleeping, travelling by train/aeroplane, swimming), In all these situations, the transition to either power-off or the switching off of key components of the device in order to reduce power consumption is pre-programmed into the behaviour rules TSR agent 16.

**[0094]** The power consumption level is monitored and reported under operational data as part of the PDU which is sent back to the control centre 33. The unit 4 raises an exception condition on the level of battery life available if the status become critical (i.e. less than 25% power level is reached). In such an event, the control centre 33 processes the PDU and forwards the status to the relevant contact point for this host. In order to conserve power under normal operational conditions, the unit 4 will use trickle power mode of operation when applicable.

**[0095]** Referring now to Figure 2, there is shown a pictorial representation of a system of the invention indicated generally by the reference numeral 31. The system 31 has a mobile unit 4 secured on the wrist of a child 32. The mobile unit 4 is in freespace communication with a control centre 33 and a GPS satellite 34. The control centre 33 and a parent/guardian or interested third party 35 are in communication via the internet through an ISP 37. Other apparatus and modes of communication between the control centre 33 and a third party 35 include interactive TV 38 via ADSL, mobile phones 39 via GSM and PDA's 36 via GPRS. An earth transceiver station 41 is shown in freespace communication with both the GPS satellite 34 and the control centre 33.

**[0096]** In the normal mode of operation, a GPS unit 28 (see Figure 1) in the mobile unit 4 is turned off and the system for communication with the control centre 33 is placed in listening mode similar to a GPRS-enabled mobile device.

**[0097]** When the control centre 33 communicates with the mobile unit 4, either as a systems check or because the parent/guardian 35 wishes to determine the state of

the child 32, the control centre 33 initiates a communications channel with the unit 4 using a wireless circuit via GSMGPRS/802.1 1, cellular, MIP, which relays the signal to the mobile unit 4. In receipt of such a signal from the control centre 33, the mobile unit 4 executes a TSR 16 which allows it to return a signal indicating the unit 4 is active containing:-

- spatial location data
- operational status/battery power level
- biometric signature data

The GPS transceiver 28 on the mobile unit 4 can calculate its spatial co-ordinates via a GPS satellite 34 as a function of time and space and pass this back as spatial location data.

**[0098]** Should the child 32 be out of range of normal wireless protocols, the system 31 can use GPS to provide the transmit/receive flow from/to the control centre 33 from the mobile unit 4. In situations where the host 32 is at sea, in mountainous terrain, in desert surroundings, it is necessary to provide satellite communications only so that the mobile unit 4 can be uniquely identified, addressed and accessed. The same TSR 16 is executed by the mobile unit 4 on receipt of the request from the control centre 33. Without such intervention the mobile unit 4 is out of range. The mobile unit 4 sends periodic data feeds in accordance with the attributes of the unit 4 itself.

**[0099]** Depending on the activity and the physical location of the host 32, the control centre 33 communicates with the host 32 via GPS modules 28 or other communications interfaces 9 using IEEE 802.11, 3G, GPRS, GSM, Bluetooth. The mobile unit 4 responds to the control centre 33 accordingly under the control of the processor 10 of the microcontroller.

**[0100]** In general, when the unit 4 detects an exception condition locally it uses mobile communications to initiate a communications session with the control centre 33. The GPS unit 28 performs the location function utilising signals from the GPS satellite 34 nearby. Under normal operations, the GPS module 28 is powered off unless either the unit 4 has detected a biometric exception condition, the host has issued an alarm 12 or the control centre 33 requests a status update. In such events, the GPS modules 28 are turned on and the location process is executed under the control of the processor 10. The GPS components 34, 28 may combine other data from the control centre 33 to verify and refine the results. Such aiding data may include approximate location data, an almanac ephemeris, a frequency offset, doppler, previous spatial reference, time, etc. The GPS components 34, 28 provide the spatial location data computed using the GPS satellite 34 in connection with the GPS unit 28 and the processor 10. This data is then combined with the biometric signature 29 and sent as a structured PDU to the control centre 33 via appropriate communications protocols. Operational data concerning power source

levels of the power sources 19, 22 (see Figure 1) is also included. Upon receipt of the PDU the control centre 33 verifies the values of the PDU attributes in accordance with the behaviour rules database 17 for that target host at that specific point in time and space.

**[0101]** If the PDU came from the unit 4 as a result of a user-initiated Alarm 12, then the control centre 33 expedites the alarm condition to the named contact person/organisation on the database who is to be contacted in an emergency. If, however, the PDU came from the mobile unit 4 in either a response to an earlier request from a control centre 33, or as a potential exception condition detected by the unit 4 itself, the control centre 33 verifies the PDU attributes in accordance with the behaviour rules database 17 for that target host 1 at that specific point in time and space and responds accordingly.

**[0102]** Referring now to Fig. 3, the behaviour rules are defined via a scripting language and programmed via a web-based graphical upper interface (GUI) by the control centre 33 or the parent/guardian 35 of the host 32. The spatial and biometric rules that define the acceptable movement and status of the host 32 as a function of time, space and activity are programmed as follows. The method by which the behavioural rules are structured, defined and expressed is by means of a script 52 which is written in either C or Java and verified through a script compiler 53. Essentially, the script 52 is a means by which the assumed location and activity of the host are defined as a function of time of day and activity. The script 52 is combined with the status of the host 32 in terms of their key biometric readings. Such biometric parameters will relate to body temperature, dermis, ECG attributes. Each script 52 will also contain the parameter values for:-

- Date (date)
- time (24 hour clock) (numeric)
- x, y co-ordinates from the national grid (numeric)
- location descriptor (text)

- i. home
- ii. School
- iii. Holiday
- iv. Shopping
- v. Work
- vi. etc.

- activity descriptor (text)

- i. field sport
- ii. Swimming
- iii. Climbing
- iv. Skiing
- v. indoor sport
- vi. leisure
- vii. school
- viii. work
- ix. etc..

- appointed trustee (if any)
- mode of transport
  - i. (on foot, car, bicycle, surface train, plane, ship, underground, etc.)
- biometric attributes
  - i. body temperature
  - ii. ECG parameters
  - iii. Skin type
  - iv. Perspiration level
  - v. Tec.

**[0103]** For each physical communication protocol which is emulated within the host 32, there will be associated with it a range of scripts 52 which will be sent to the unit 4 via a script dispatcher 51 and executed by the unit 4 and subsequently used to enter into a dialogue with the control centre 33.

**[0104]** These are then assembled into executable mobile agent code for transmission to the unit 4 as a TSR 16. Mobile client-server protocols are enabled to provide for the call-set-up, agent communications and TSR 16 verification between the control centre 33 and the unit processor 10. The behavioural rules database 17 is then populated with these values. Subsequent local datafeeds from GPS 28 and Biometric sensor 23 are compared against the behavioural database 17 and the rules that were defined in the TSR 16. A Data warehouse will be maintained at the control centre 33 to keep a profile of the host behaviour for future reference and prediction.

**[0105]** Variations and modifications can be made without departing from the scope of the invention described above and as hereinafter defined in the appended claims.

## Claims

1. A programmable mobile unit (4) for a portable host, such as a person (32), comprising a microcontroller in communication with each of
  - a detachable freespace communication module (9) for communication with a control centre (33),
  - a GPS unit (28) for communication with at least a GPS satellite system (34), and a biometric sensor (23), the biometric sensor (23) and the microcontroller being configured to monitor and uniquely identify the host from biometric data specific to the host.
2. A programmable mobile unit (4) as claimed in claim 1, wherein the detachable freespace communication module (9) is selectable from a set of communication modules and each module is configured to interface with different freespace communication protocols.
3. A programmable mobile unit (4) as claimed in claim 1 or claim 2, wherein the microcontroller has a database (17) of acceptable behaviour parameters for the host (32) stored in a memory (14) of the unit (4).
4. A programmable mobile unit (4) as claimed in claim 3, wherein the database (17) defines the boundaries of acceptable geographical locations and acceptable biological values as a function of time for the host (32).
5. A programmable mobile unit (4) as claimed in claim 3 or 4, wherein the database (17) is remotely programmable to take new activities and routines of the host into account.
6. A programmable mobile unit (4) as claimed in any preceding claim, wherein original identification takes place when the biometric sensor (23) is first attached to the host (32) and the mobile unit (4) is initially powered up.
7. A programmable mobile unit (4) as claimed in claim 6, wherein the identification provides a reproducible, identifiable biometric signature (29) for the host (32).
8. A programmable mobile unit (4) as claimed in any one of the preceding claims, wherein the biometric sensor (23) comprises a power source (22) and a flexible multi-sensor patch which continuously monitors the host's ECG (26), body temperature (25) and respiration rate (27).
9. A programmable mobile unit (4) as claimed in any one of the preceding claims, wherein the biometric sensor (23) is provided with flexible circuitry allowing the sensor (23) to adapt to the shape of the host's body.
10. A programmable mobile unit (4) as claimed in any one of the preceding claims, wherein the biometric sensor (23) and the microcontroller communicate using bluetooth technology.
11. A programmable mobile unit (4) as claimed in any one of the preceding claims, wherein the microcontroller is pre-programmed to periodically monitor and download up-to-date information from the GPS unit (28) and the biometric sensor (23).
12. A system (31) for monitoring and tracking a host, such as a person (32), comprising a control centre (33) in freespace communication with a mobile unit (4) and a GPS satellite system (34), the mobile unit (4) comprising a microcontroller in communication with each of a detachable freespace communication module (9) for communication with the control centre (33), a GPS unit (28) for communication with at least

- a GPS satellite system (34) and a biometric sensor (23), the biometric sensor (23) and the microcontroller being configured to monitor and uniquely identify the host from biometric data specific to the host.
13. A system (31) as claimed in claim 12, wherein the mobile unit (4) and the control centre (33) periodically communicate with each other using freespace communication protocols.
14. A system (31) as claimed in claim 12 or 13, wherein an acceptable behaviour database (17) is stored at the control centre (33) and on the mobile unit (4).
15. A system (31) as claimed in claim 14, wherein the system includes a web-based interface to a database driven secure environment for dynamic creation and modification of the acceptable behaviour database (17) stored in the control centre(33) and the mobile unit (4).
16. A system (31) as claimed in any one of claims 12 to 15, wherein the control centre (33) of the system and third parties are in communication using predetermined communication protocols.
17. A system (31) as claimed in any one of claims 12 to 16, wherein the control centre (33) includes means for alerting custodians and third parties of exception values via predetermined communication protocols.
18. A system (31) as claimed in claim 16 or 17, wherein the third parties and the control centre (33) have means for contacting the mobile unit (4) via predetermined communication protocols.

#### Patentansprüche

- Freiraum-Kommunikationsprotokollen verbunden ist.
3. Eine programmierbare mobile Anlage (4) gemäß Anspruch 1 oder Anspruch 2, bei der der Mikrocontroller eine Datenbank (17) mit für den Host (32) akzeptierbaren Verhaltensparametern besitzt, die in einem Speicher (14) der Anlage gespeichert sind.
4. Eine programmierbare mobile Anlage (4) gemäß Anspruch 3, bei der die Datenbank (17) die Grenzen der akzeptierbaren geografischen Orte und der akzeptierbaren biologischen Werte als eine Zeitfunktion für den Host (32) bezeichnet.
5. Eine programmierbare mobile Anlage (4) gemäß Anspruch 3 oder 4, bei der die Datenbank (17) auf Entfernung programmiert werden kann, um neue Aktivitäten und Routinen des Hosts zu berücksichtigen.
6. Eine programmierbare mobile Anlage (4) gemäß der vorhergehenden Ansprüche, bei der die ursprüngliche Identifizierung stattfindet, wenn der biometrische Sensor (23) erstmalig mit dem Host (32) verbunden wird und die mobile Anlage (4) erstmalig in Betrieb genommen wird.
7. Eine programmierbare mobile Anlage (4) gemäß Anspruch 6, bei der die Identifizierung für den Host (32) eine wiederholbare, identifizierbare biometrische Signatur (29) bietet.
8. Eine programmierbare mobile Anlage (4) gemäß der vorhergehenden Ansprüche, bei der der biometrische Sensor (23) eine Stromquelle (22) und einen flexiblen Multisensor-Patch besitzt, der das EKG (26), die Körpertemperatur (25) und die Atmungsrate (27) des Hosts kontinuierlich überwacht.
9. Eine programmierbare mobile Anlage (4) gemäß der vorhergehenden Ansprüche, bei der der biometrische Sensor (23) einen flexiblen Schaltkreis besitzt, der dem Sensor (23) die Möglichkeit bietet, sich der Körperform des Hosts anzupassen.
10. Eine programmierbare mobile Anlage (4) gemäß der vorhergehenden Ansprüche, bei der der biometrische Sensor (23) und der Mikrocontroller über Bluetooth Technologie miteinander kommunizieren.
11. Eine programmierbare mobile Anlage (4) gemäß der vorhergehenden Ansprüche, bei der der Mikrocontroller zur periodischen Überwachung und zum Herunterladen aktueller Informationen von der GPS Anlage (28) und dem biometrischen Sensor (23) vorprogrammiert ist.
12. Ein System (31) zur Überwachung und zum Verfol-

gen eines Hosts, d.h. einer Person (32), bestehend aus einem Kontrollzentrum (33), das in Freiraum-Kommunikation mit einer mobilen Anlage (4) und einem GPS Satellitensystem (43) steht und bei der die mobile Anlage (4) einen Mikrocontroller in Kommunikation mit jedem der abnehmbaren Freiraum-Kommunikationsmodule (9) zur Kommunikation mit dem Kontrollzentrum (33), eine GPS Anlage (28) zur Kommunikation mit mindestens einem GPS Satellitensystem (34) und einen biometrischen Sensor (23) besitzt, wobei der biometrische Server (23) und der Mikrocontroller zur Überwachung und speziellen Identifizierung des Hosts durch biometrische Daten, die speziell den Host betreffen, konfiguriert sind.

13. Ein System (31) gemäß Anspruch 12, bei dem die mobile Anlage (4) und das Kontrollzentrum (33) periodisch durch Verwendung von Freiraum-Kommunikationsprotokollen miteinander kommunizieren.

14. Ein System (31) gemäß Anspruch 12 oder 13, bei dem eine Datenbank akzeptabler Verhaltensformen (17) im Kontrollzentrum (33) und in der mobilen Anlage gespeichert wird.

15. Ein System (31) gemäß Anspruch 14, mit einer Web-Verbindung zu einer von der Datenbank bestimmten sicheren Umgebung für die dynamische Schaffung und Modifizierung der Datenbank akzeptabler Verhaltensformen (17), die im Kontrollzentrum (33) und in der mobilen Anlage (4) gespeichert wird.

16. Ein System (31) gemäß der Ansprüche 12 bis 15, bei dem das Kontrollzentrum (23) des Systems und Dritte unter Verwendung von vorbestimmten Kommunikationsprotokollen kommunizieren.

17. Ein System (31) gemäß der Ansprüche 12 bis 16, bei dem das Kontrollzentrum (33) Möglichkeiten zur Warnung von Aufsichtspersonen und Dritten über ungewöhnliche Werte via vorbestimmte Kommunikationsprotokolle mit einschließt.

18. Ein System (31) gemäß Anspruch 16 oder 17, bei dem Dritte und das Kontrollzentrum (33) Möglichkeiten haben, die mobile Anlage (4) über vorbestimmte Kommunikationsprotokolle zu benachrichtigen.

## Revendications

1. Une unité mobile programmable (4) pour un hôte mobile, tel une personne (32), composé d'un microcontrôleur communiquant avec chaque module de communication amovible dans un espace libre (9), lui-même relié à un centre de contrôle (33), une unité GPS (28) capable de communiquer avec au moins un système satellite GPS (34), et un senseur biomé-

trique (23), le serveur biométrique (23) et le microcontrôleur configuré afin de contrôler et d'identifier l'hôte de manière unique à partir de données biométriques spécifiques à cet hôte en particulier.

2. Une unité mobile programmable (4) comme spécifié dans la revendication (1), où le module de communication libre amovible (9) peut être choisi parmi une gamme de modules de communication et où chaque module est configuré pour s'interfacer avec différents protocoles de communication dans un espace libre.

3. Une unité mobile programmable (4) comme spécifié dans les revendications (1) ou (2), où le microcontrôleur possède une base de données (17) de paramètres comportementaux acceptables de la part de l'hôte (32) sauvegardés dans la mémoire (14) de l'unité (4).

4. Une unité mobile programmable (4) comme spécifié dans la revendication (3), où la base de données (17) définit la limite des positions géographiques et des valeurs biologiques acceptables pour l'hôte, en fonction du temps.

5. Une unité mobile programmable (4) comme spécifié dans les revendications (3) ou (4), où la base de données (17) est programmable à distance afin de prendre en considération les nouvelles activités ou routines effectuées par l'hôte.

6. Une unité mobile programmable (4) comme spécifié dans les revendications précédentes, où l'identification initiale s'effectue lorsque le senseur biométrique (23) est fixé pour la première fois sur l'hôte (32) et lorsque l'unité mobile (4) est mise en marche pour la première fois.

7. Une unité mobile programmable (4) comme spécifié dans la revendication (6), où l'identification permet d'identifier l'hôte (32) grâce à une signature biométrique reproductible et identifiable (29).

8. Une unité mobile programmable (4) comme spécifié dans les revendications précédentes, où le senseur biométrique (23) comprend une source d'énergie (22) et un patch flexible multi sensoriel qui mesure de façon continue l'activité cérébrale (26), la température corporelle (25) et le rythme respiratoire (27).

9. Une unité mobile programmable (4) comme spécifié dans les revendications précédentes, où le senseur biométrique (23) est fourni avec un ensemble de circuits flexibles permettant au senseur (23) de s'adapter à la forme du corps de l'hôte.

10. Une unité mobile programmable (4) comme spécifié

dans les revendications précédentes, où le capteur biométrique (23) et le microcontrôleur communiquent grâce à la technologie Bluetooth.

11. Une unité mobile programmable (4) comme spécifié dans les revendications précédentes, où le microcontrôleur est préprogrammé afin d'effectuer des mesures périodiques et de télécharger des informations mises à jour à partir de l'unité GPS (28) et du capteur biométrique (23). 5  
10
12. Un système (31) de contrôle et de suivi de l'hôte, tel une personne (32), comprenant un centre de contrôle (33) en communication dans un espace libre avec une unité mobile (4) et un système satellite GPS (34), l'unité mobile (4) comprenant un microcontrôleur communiquant avec chacun des modules de communication dans un espace libre (9) afin de communiquer avec le centre de contrôle (33), une unité GPS (28) afin de communiquer avec au moins un système satellite (34) et un capteur biométrique (23), le serveur biométrique (23) et le microcontrôleur configurés afin de contrôler et d'identifier uniquement l'hôte auquel il est relié à partir de données biométriques spécifiques à cet hôte. 15  
20  
25
13. Un système (31), comme spécifié dans la revendication 12, où l'unité mobile (4) et le centre de contrôle (33) communiquent périodiquement entre eux par le biais de protocoles de communication dans un espace libre. 30
14. Un système (31), comme spécifié dans les revendications (12) et (13), avec une base de données de comportements acceptables (17) qui se trouve dans le centre de contrôle (33) et dans l'unité mobile (4). 35
15. Un système (31), comme spécifié dans la revendication (14), où le système comprend une interface web vers une base de données pilotée par un environnement sécurisé pour créer et modifier dynamiquement la base de données des comportements acceptables (17) mémorisée dans le centre de contrôle et dans l'unité mobile (4). 40  
45
16. Un système (31), comme spécifié dans les revendications de (12) à (15), où le centre de contrôle (33) du système et des tierces parties sont en communication grâce à des protocoles de communication prédéterminés 50
17. Un système (31), comme spécifié dans les revendications de (12) à (16), où le centre de contrôle (33) comprend les moyens d'alerter le porteur et les tierces parties d'éventuelles anomalies par le biais de protocoles de communication prédéterminés. 55
18. Un système (31), comme spécifié dans les revendications de (16) et (17), où les tierces parties et le centre de contrôle(33) ont la possibilité d'entrer en contact avec l'unité mobile (4) par le biais de protocoles de communication prédéterminés.

cations de (16) et (17), où les tierces parties et le centre de contrôle(33) ont la possibilité d'entrer en contact avec l'unité mobile (4) par le biais de protocoles de communication prédéterminés.

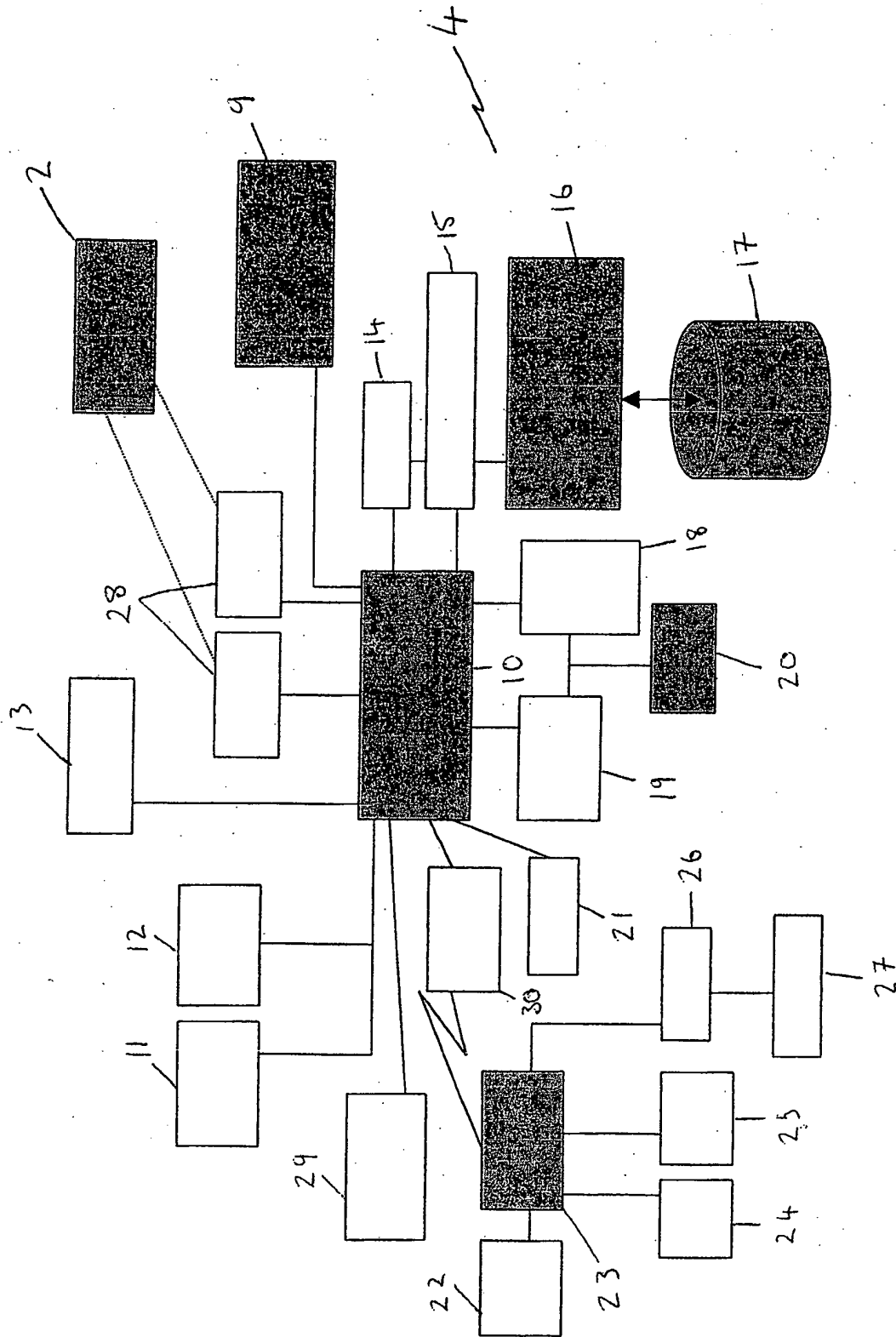


Figure 1

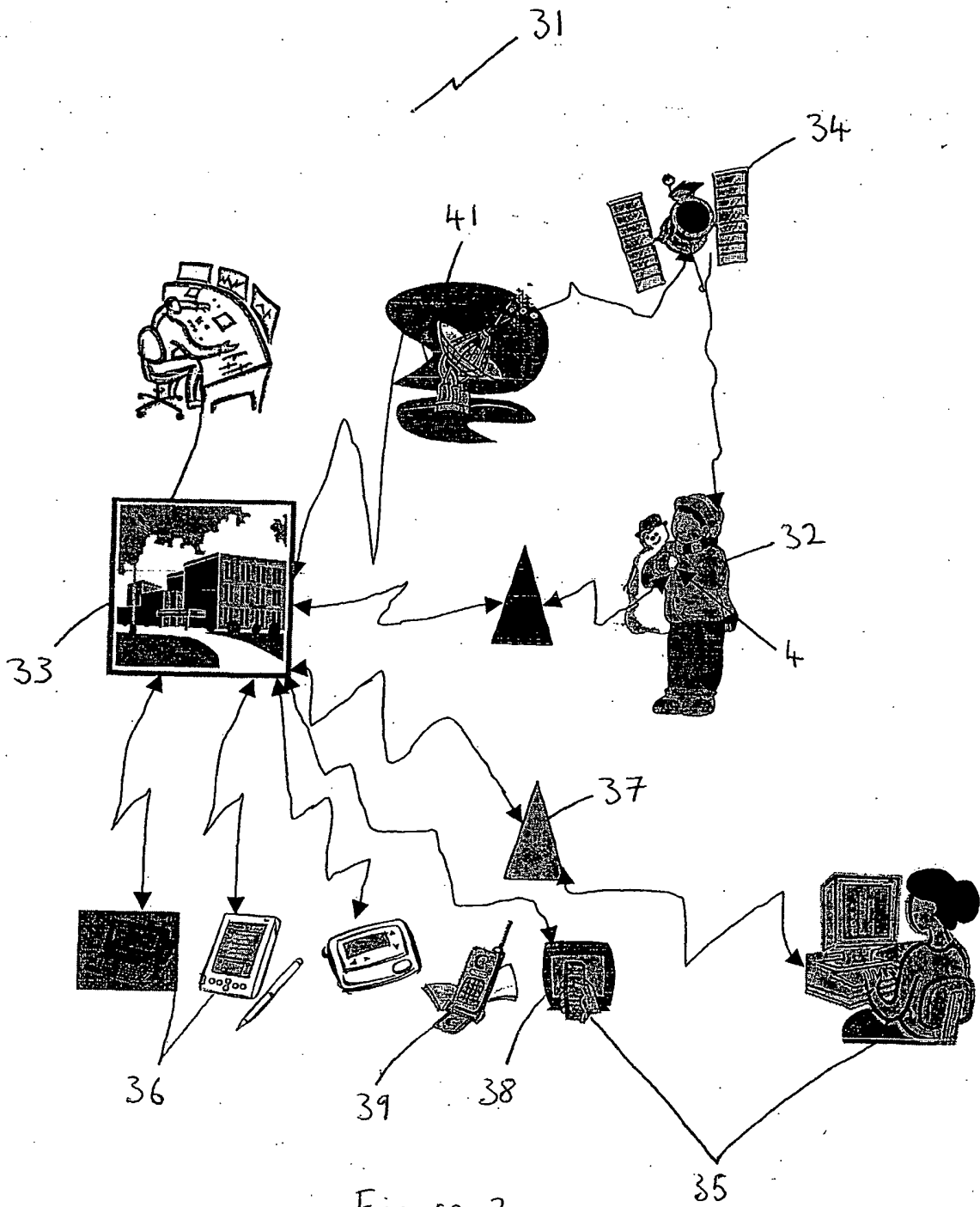
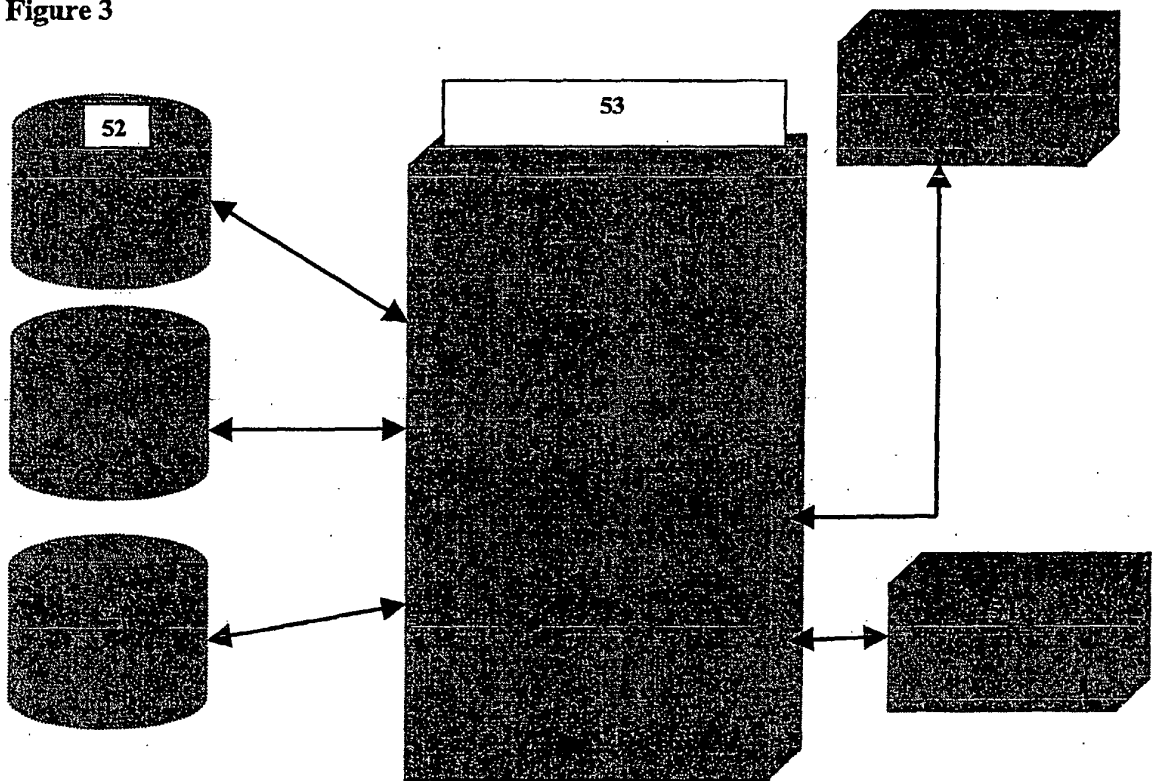


Figure 2

Figure 3



**REFERENCES CITED IN THE DESCRIPTION**

*This list of references cited by the applicant is for the reader's convenience only. It does not form part of the European patent document. Even though great care has been taken in compiling the references, errors or omissions cannot be excluded and the EPO disclaims all liability in this regard.*

**Patent documents cited in the description**

- WO 0232098 A [0005]
- US 4952928 A [0006]

专利名称(译)	跟踪和监视设备和系统		
公开(公告)号	<a href="#">EP1599847B1</a>	公开(公告)日	2007-08-15
申请号	EP2004711657	申请日	2004-02-17
[标]申请(专利权)人(译)	KINDERGUARD		
申请(专利权)人(译)	KINDERGUARD有限公司		
当前申请(专利权)人(译)	KINDERGUARD有限公司		
[标]发明人	DOUGLAS RAYMOND		
发明人	DOUGLAS, RAYMOND		
IPC分类号	G08B21/02 H04M11/04 A61B5/00 G01S5/00 A61B5/0205 A61B5/08 H04L12/26		
CPC分类号	G08B21/18 A61B5/0006 A61B5/02055 A61B5/0816 G01S5/00 G08B21/0211 G08B21/0261 G08B21/0269		
优先权	2004000428 2004-01-09 GB 2003003586 2003-02-17 GB		
其他公开文献	EP1599847A2		
外部链接	<a href="#">Espacenet</a>		

摘要(译)

一种用于便携式主机 ( 32 ) 的可编程移动单元 ( 4 ) , 例如人, 包括与可拆卸自由空间通信模块 ( 9 ) 中的每一个通信的微控制器, 用于与控制中心 ( 33 ) , GPS单元 ( 28 ) 用于与至少一个GPS卫星系统 ( 34 ) 和生物识别传感器 ( 23 ) 进行通信, 以监测和识别主机 ( 32 ) 。

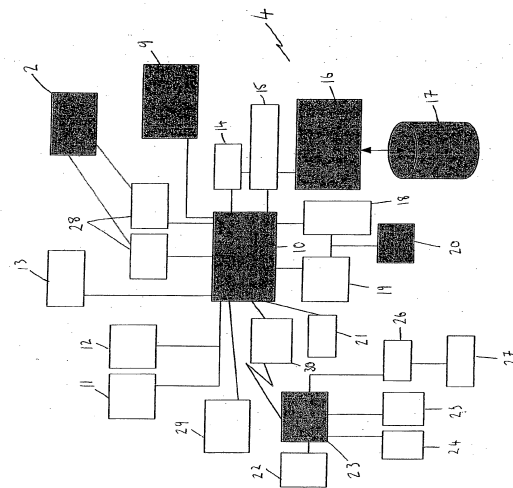


Figure 1