(12) UK Patent Application (19) GB (11) 2472632 (13) A

(43) Date of A Publication 16.02.2011

(21) Application No: 0914196.1

(22) Date of Filing: 13.08.2009

(71) Applicant(s):
Spinnaker International Limited
(Incorporated in the United Kingdom)
Spinnaker House, Saltash Parkway, SALTASH, Cornwall, PL12 6LF, United Kingdom

(72) Inventor(s):
Christopher Kosmas
Nicholas Tripp
Anthony Westington
Nathan Clarke
Cen Tjhai

(74) Agent and/or Address for Service:
Withers & Rogers LLP
Goldings House, 2 Hays Lane, LONDON, SE1 2HW, United Kingdom

(51) INT CL:
G08B 21/18 (2006.01) ***G01S 5/00*** (2006.01)
G01S 5/14 (2006.01) ***G01S 13/74*** (2006.01)
G06Q 10/00 (2006.01) ***G08B 13/24*** (2006.01)
G08B 25/00 (2006.01) ***G08B 25/10*** (2006.01)

(56) Documents Cited:
GB 2277850 A
EP 1788749 A1
WO 2006/091192 A2
WO 2004/068160 A2
JP 2008131308 A
US 6977612 B1
US 6133687 A
US 20090174546 A1
US 20080061963 A1
US 20070222665 A1
US 20060261944 A1
US 20050207381 A1
US 20030235172 A1
EP 1975901 A1
WO 2007/028956 A1
WO 2004/102327 A2
DE 102007056354 A1
US 7418343 B1
US 6150961 A
US 5939982 A
US 20090135015 A1
US 20070262861 A1
US 20070132577 A1
US 20060192709 A1
US 20040002347 A1

(58) Field of Search:
INT CL **G01S, G01V, G06Q, G08B, G08G**
Other: **EPODOC,WPI**

(54) Title of the Invention: **A security container and security systems**
Abstract Title: **Adjusting an operating mode of a security container in response to an unexpected received radio signal**

(57) A security container 10 is provided for storing or transporting valuable items. The container 10 comprises a radio receiver 22 for receiving signals from a radio transmitter (44,fig.2) external to the container 10. An operating mode of the container 10 is adjusted if a received radio signal does not correspond to an expected signal. The operating mode may be adjusted by deactivating a locking mechanism. The receiver 22 may be arranged to decode a radio signal received from a transmitter (44,Fig.2) to retrieve an identifier associated with the transmitter, wherein the identifier may be used to determine if the security container is following a predetermined transit path. In another embodiment, a system for tracking the location of a security container is disclosed. In a further embodiment, a means for announcing the location of a security container to a central location is provided. In another embodiment, a mobile network is disclosed for tracking the location of an object.

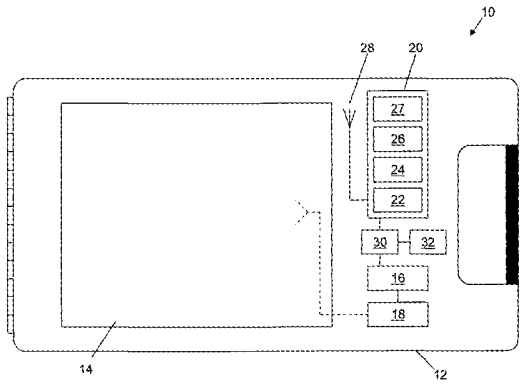

Figure 1

GB 2472632 A

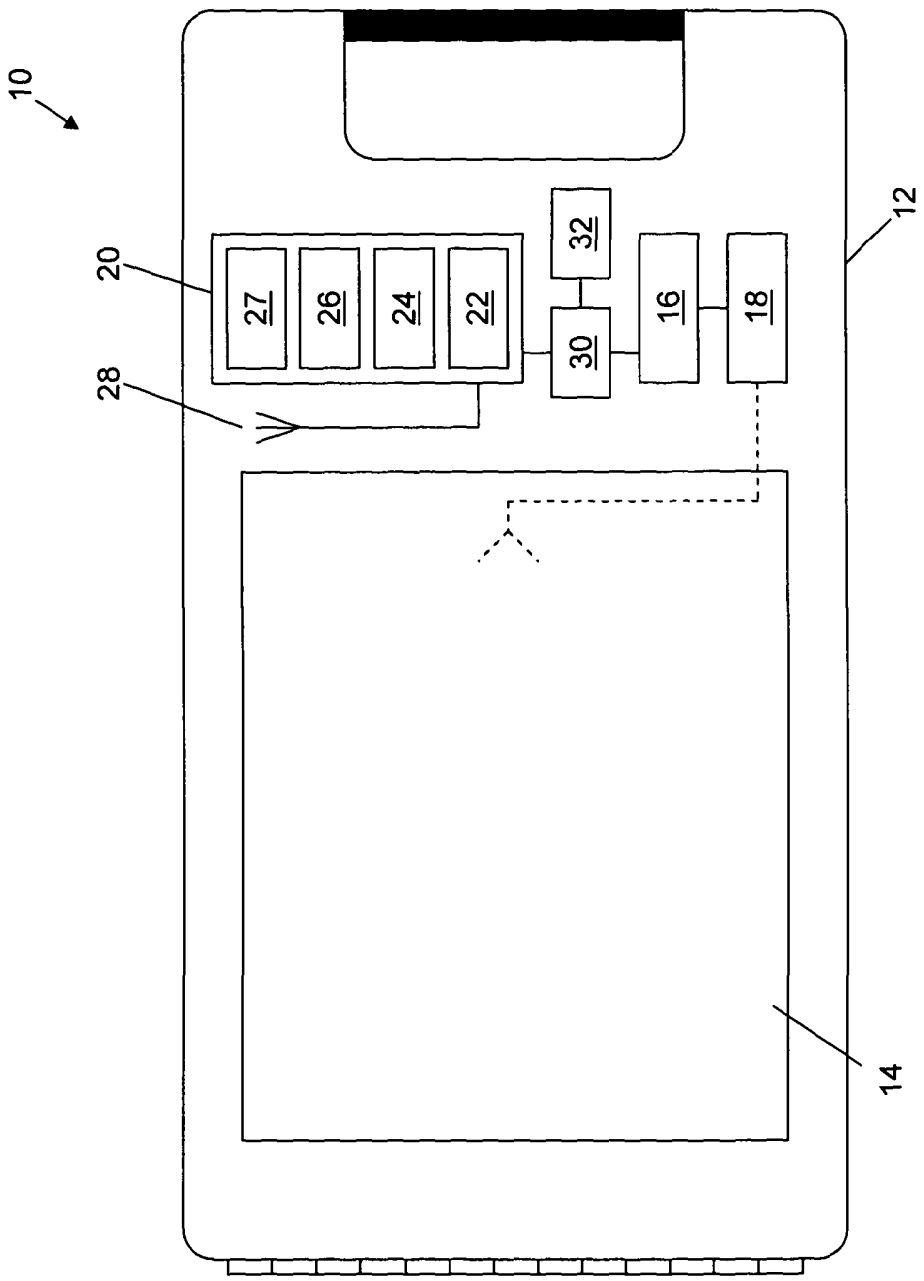

Figure 1

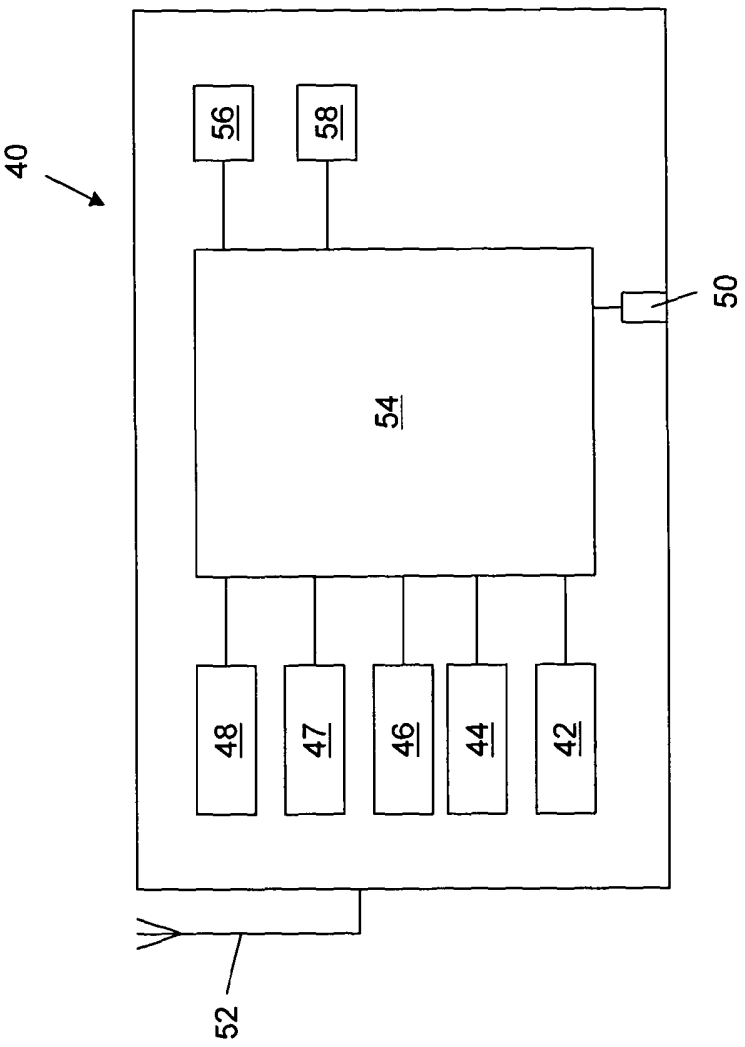

Figure 2

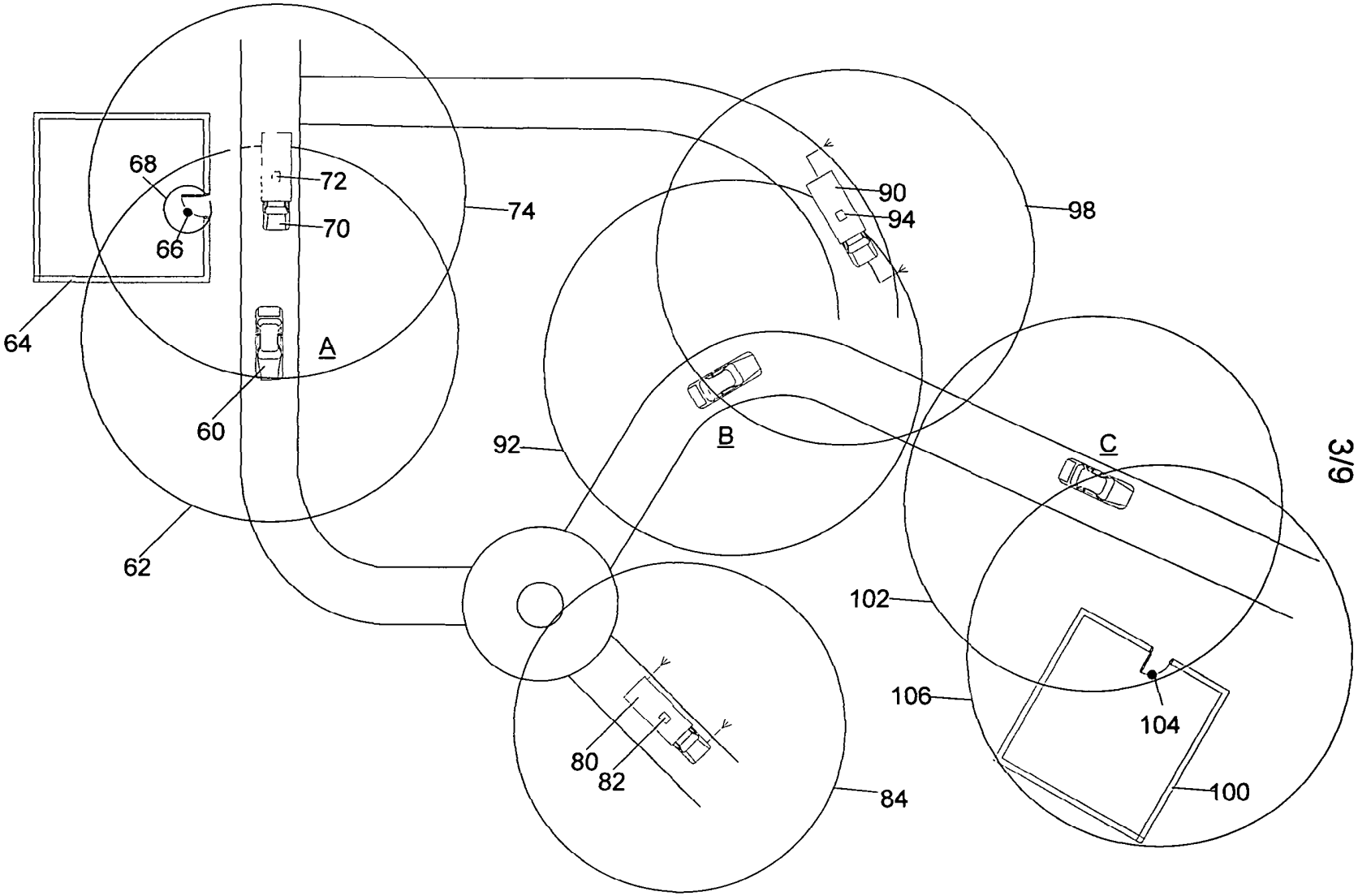

Figure 3

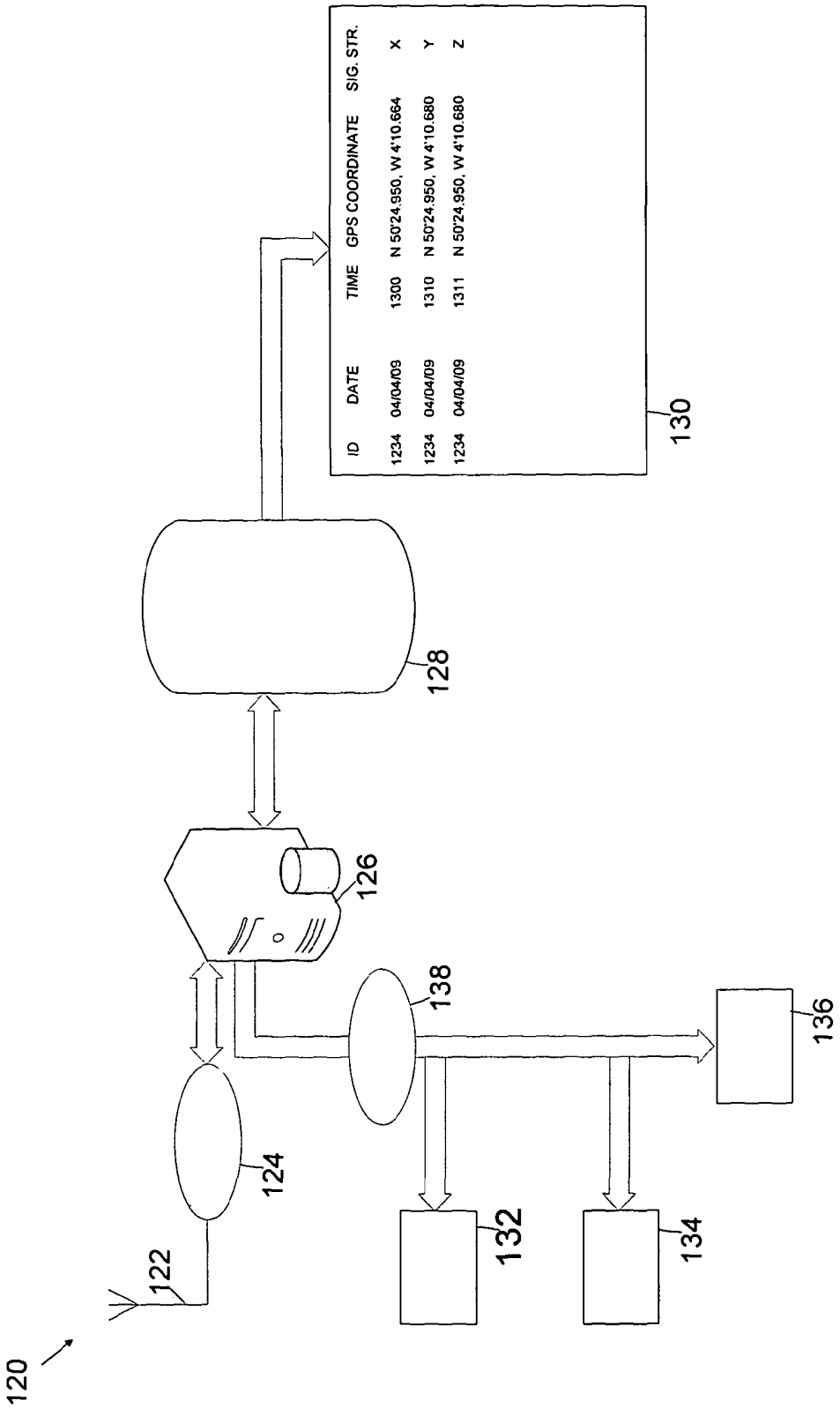
120
122
124
126
128
130
132
134
136
138
ID DATE TIME GPS COORDINATE SIG. STR.
1234 04/04/09 1300 N 50°24.950, W 4°10.664 X
1234 04/04/09 1310 N 50°24.950, W 4°10.680 Y
1234 04/04/09 1311 N 50°24.950, W 4°10.680 Z

Figure 4

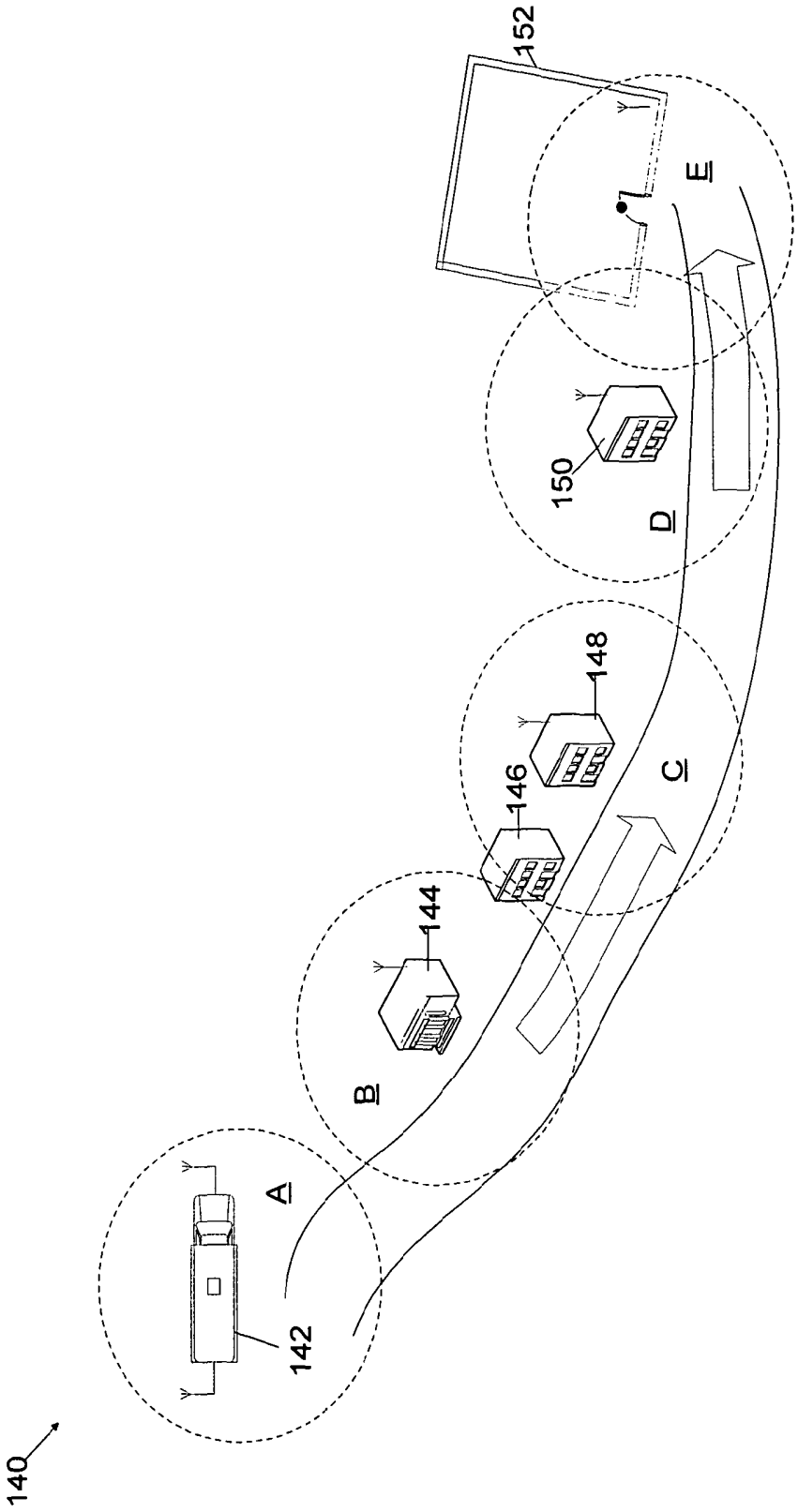

Figure 5

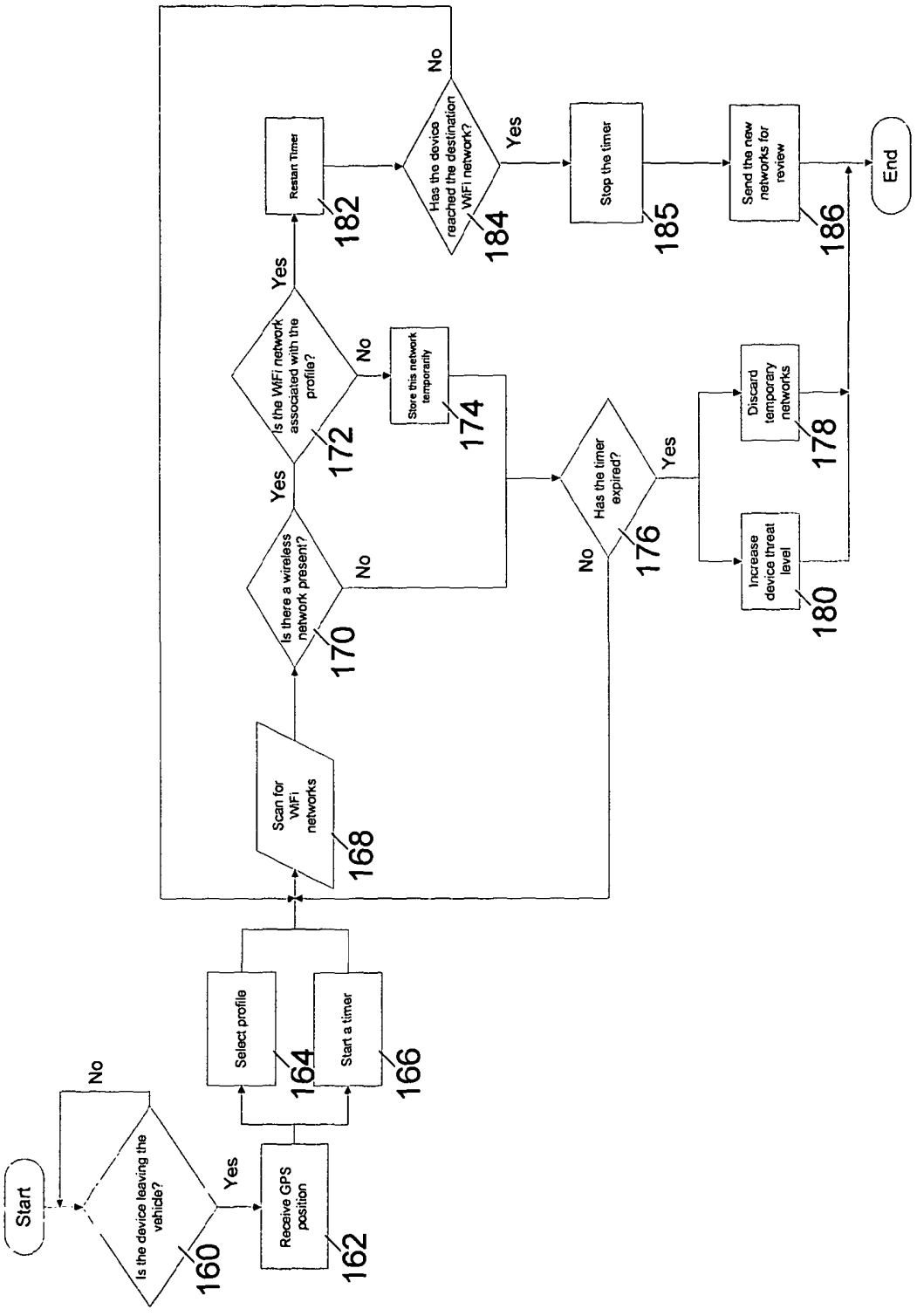
Start
Is the device leaving the vehicle?
160
No
Yes
Receive GPS position
162
Select profile
164
Start a timer
166
Scan for WiFi networks
168
Is there a wireless network present?
170
No
Yes
Is the WiFi network associated with the profile?
172
No
Yes
Store this network temporarily
174
Has the timer expired?
176
No
Yes
Discard temporary networks
178
Increase device threat level
180
Restart Timer
182
Has the device reached the destination WiFi network?
184
No
Yes
Stop the timer
185
Send the new networks for review
186
End

Figure 6

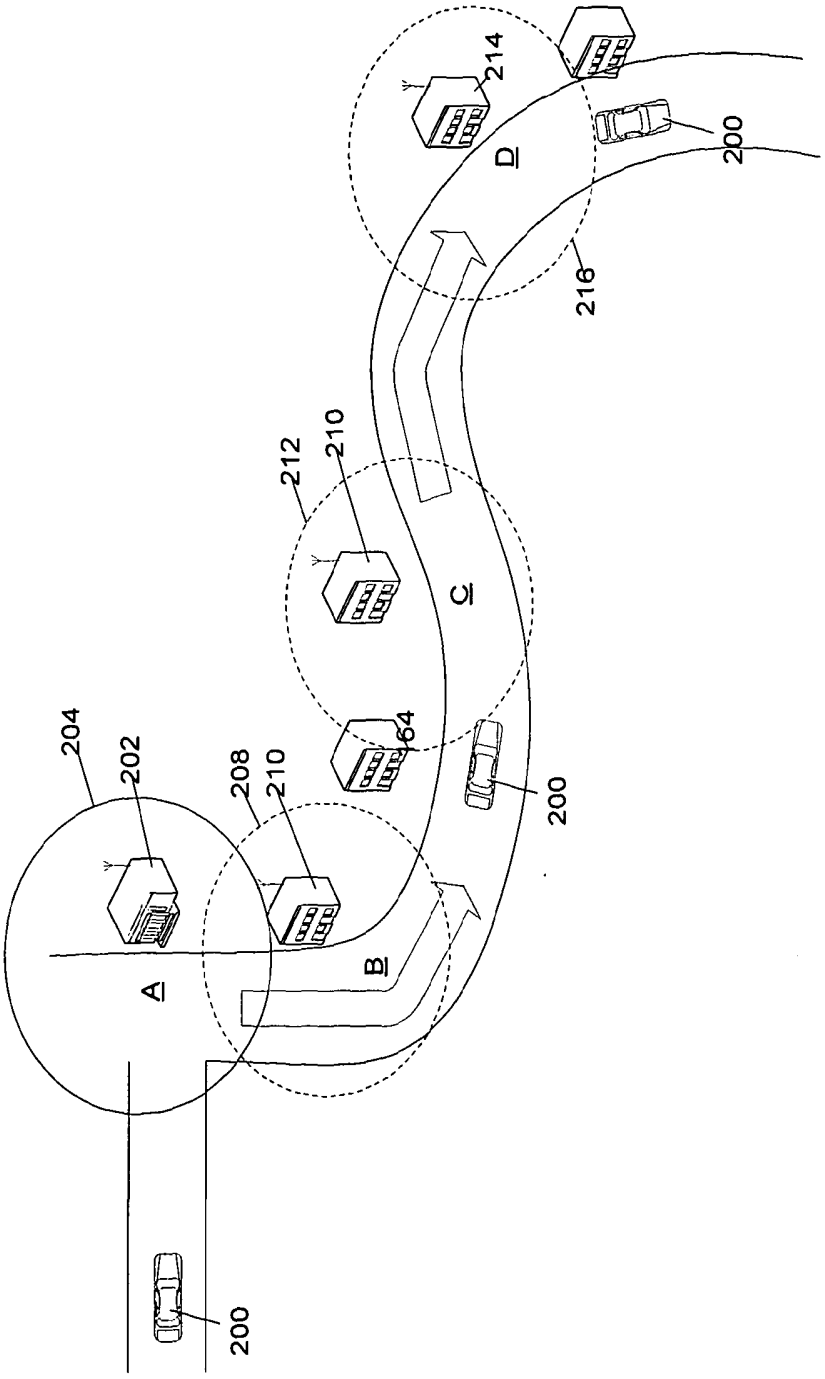

Figure 7

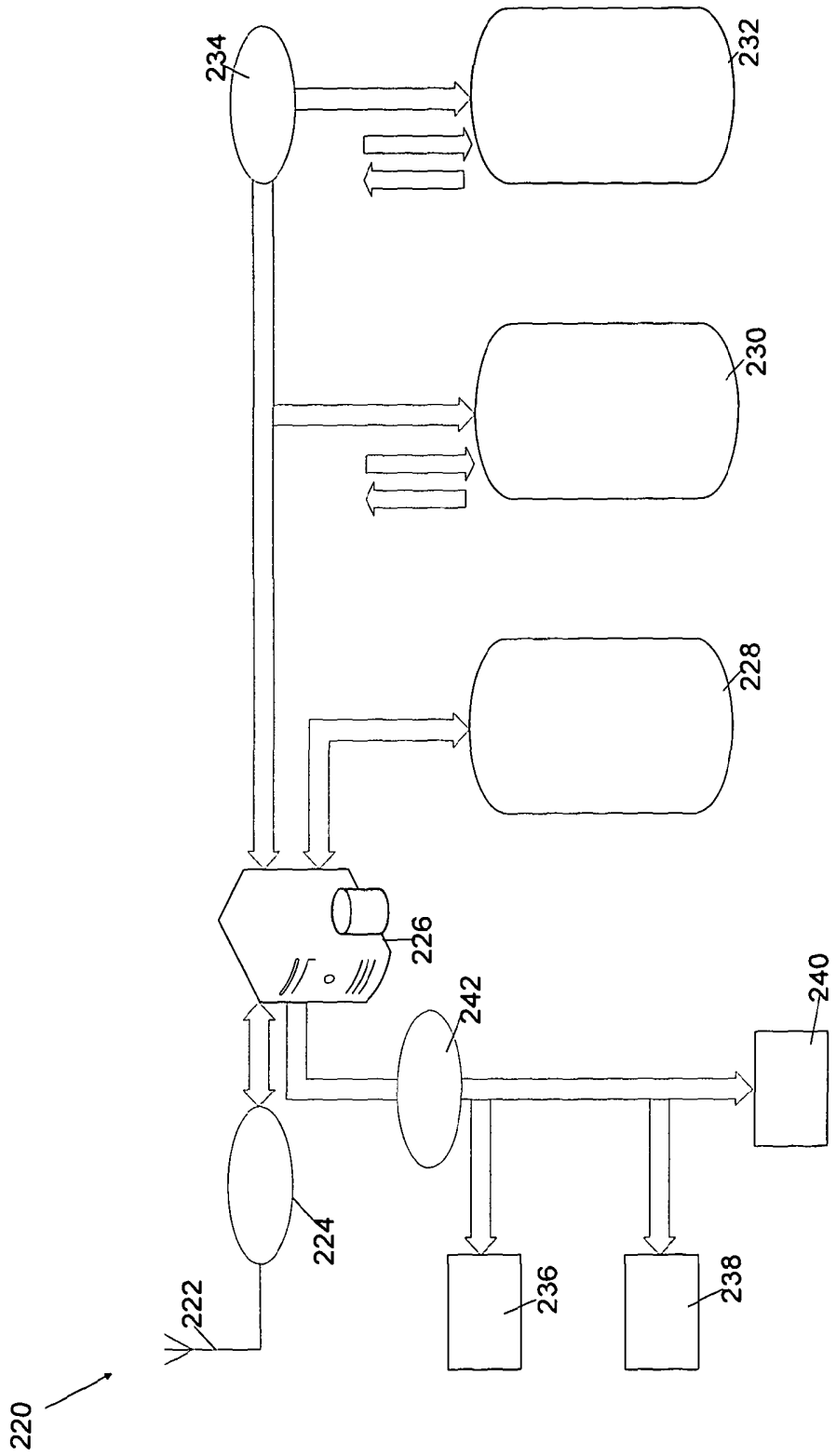

Figure 8

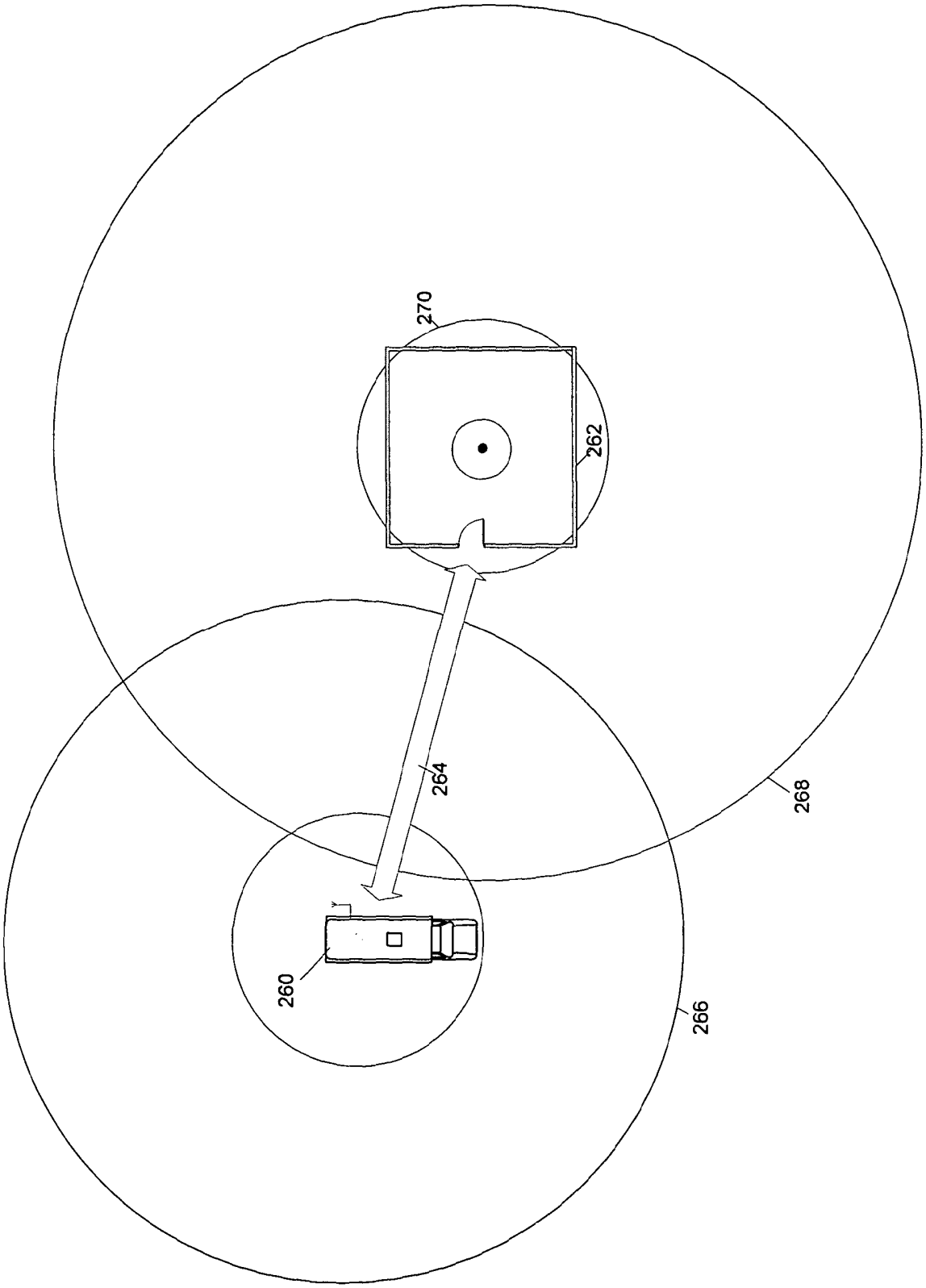

Figure 9

A SECURITY CONTAINER AND SECURITY SYSTEMS

The present invention relates to a security container, and to security systems and security methods.

It has become commonplace for valuable items such as bank notes and valuable documents to be transported to a destination in a security container equipped with a system for detecting theft or other unauthorised interference with the security container, with the detection system being configured to dispense a spoiling agent such as an indelible ink or dye onto the contents of the security container in the event of theft or unauthorised interference with the security container. Whilst such security containers provide a deterrent against theft, attacks on delivery guards still occur, and it is possible that the detection system may fail, thereby allowing a criminal to access the contents of the security container.

Moreover, in situations where a security container has been stolen it is often recovered after the spoiling agent has been dispensed and the thief has fled. Thus, the contents of the security container are spoiled and the thief may escape capture.

Accordingly, it would be desirable for security containers to provide a mechanism which could increase the likelihood of the security container and its contents being recovered intact in the event of a theft, and of the thief being apprehended whilst in possession of the security container.

According to first aspect of the invention there is provided a security container for storing or transporting valuable items, the security container comprising a radio receiver for receiving radio signals from a radio transmitter external to the security container, wherein the security container is configured to adjust an operating mode if a received radio signal does not correspond to a signal expected by the security container.

The security container of the first aspect of the invention is able to adjust its operating mode, for example by entering a high alert level mode, in response to a received radio signal, or the absence of a received radio signal, which may be indicative that the security container is

under threat of theft, or has been stolen. This allows the security container to respond to a threat before any attempt has been made to open the security container, thereby increasing the likelihood that the security container and its contents can be recovered intact.

The radio receiver may be configured to decode a radio signal received from a transmitter to retrieve an identifier associated with the transmitter and the security container may be configured to determine from the identifier whether the security container is following a predetermined transit path.

Thus, the security container is able to detect if it is deviating from an expected delivery path and to adjust its operating mode, for example by entering a high threat mode, if deviation from the expected delivery path is detected. This enables the security container to detect a theft or other threat situation very quickly, and to take appropriate action.

The security container may be configured to assess whether the signal was received within an expected time period.

The radio receiver may be configured to receive a sequence comprising signals transmitted by each of a plurality of external radio transmitters, each signal containing an identifier associated with the respective transmitter and the security container may be configured to compare the identifiers of the received sequence to a stored sequence of expected identifiers.

The security container may be configured to record an identifier contained in a signal received from an external transmitter if that identifier is not a member of the stored sequence.

In an alternative embodiment, the radio receiver may be configured to receive a first signal transmitted by a radio transmitter of a delivery vehicle and a second signal transmitted by a radio transmitter of a destination to which the security container is to be delivered, the security container being configured to adjust the operating mode if it does not receive the first and second signals in accordance with a predefined expectation.

In this embodiment the security container is able to detect a theft or other threat event very shortly after being removed from a delivery vehicle, and to take appropriate action, thereby

increasing the likelihood that the theft will be unsuccessful and that the security container and its contents will be recovered intact.

The security container may be configured to monitor the strength of the first and second signals and to adjust operating mode if the strength of the first and second signals deviates from an expected profile.

The security container may be configured to adjust the operating mode if the strength of the first or second signal falls to zero.

The security container may be configured to adjust the operating mode by increasing an alert level of the security container.

The security container may be configured to compare the strength of the second signal to a threshold value and to adjust the operating mode if the strength of the second signal meets the threshold.

The security container may be configured to adjust the operating mode only if the signal strength meets the threshold for a predetermined period of time.

The security container may be configured to adjust its operating mode on detection of a signal transmitted by a short range radio transmitter located at or near a delivery destination of the security container.

The security container may be configured to adjust the operating mode by reducing an alert level of the security container.

The security container may be configured to adjust its operating mode by deactivating a locking mechanism.

According to a second aspect of the invention there is provided a method of controlling an operating mode of a security container, the method comprising receiving radio signals from a

radio transmitter external to the security container, and adjusting the operating mode if a received radio signal does not correspond to a signal expected by the security container.

The method may further comprise decoding a radio signal received from a transmitter to retrieve an identifier associated with the transmitter and determining from the identifier whether the security container is following a predetermined transit path.

The method may further comprise assessing whether the signal was received within an expected time period.

The method may further comprise receiving a sequence comprising signals transmitted by each of a plurality of external radio transmitters, each signal containing an identifier associated with the respective transmitter, and comparing the identifiers of the received sequence to a stored sequence of expected identifiers.

The method may further comprise recording an identifier contained in a signal received from an external transmitter if that identifier is not a member of the stored sequence.

The method may further comprise receiving a first signal transmitted by a radio transmitter of a delivery vehicle and a second signal transmitted by a radio transmitter of a destination to which the security container is to be delivered and adjusting the operating mode if the first and second signals are not received in accordance with a predefined expectation.

The method may further comprise monitoring the strength of the first and second signals and adjusting the operating mode if the strength of the first and second signals deviates from an expected profile.

The method may further comprise adjusting the operating mode if the strength of the first or second signal falls to zero.

Adjusting the operating mode may comprise increasing an alert level of the security container.

The method may further comprise comparing the strength of the second signal to a threshold value and adjusting the operating mode if the strength of the second signal meets the threshold.

The method may further comprise adjusting the operating mode on detection of a signal transmitted by a short range radio transmitter located at or near a delivery destination of the security container.

Adjusting the operating mode may comprise reducing an alert level of the security container.

Adjusting the operating mode may comprise deactivating a locking mechanism of the security container.

According to a third aspect of the present invention there is provided a security system comprising a security container according to the first aspect and a radio transmitter for transmitting a signal that can be detected by the radio receiver of the security container.

According to a fourth aspect of the present invention there is provided a system for tracking the location of a security container, the system comprising a security container comprising a radio transmitter which is configured to transmit a signal containing an identifier associated with the security container and a plurality of radio receivers, each of the plurality of radio receivers being configured to receive the signal transmitted by the transmitter of the security container and to transmit the identifier and location information associated with the radio receiver to a central location.

The system of the fourth aspect of the invention allows the location of a security container to be tracked to a high level of accuracy in the event that a theft is detected. The system of the fourth aspect can also be used when a theft has not been detected to allow the owner of a security container to track its location.

Each of the plurality of receivers may comprise a positioning system receiver for providing the location information associated with the radio receiver.

Each of the plurality of radio receivers may comprise an input for receiving location information from a positioning system receiver external to the radio receiver.

Each of the plurality of radio receivers may comprise a mobile telecommunications system transmitter for transmitting the identifier and location information associated with the radio receiver to a central location.

Each of the plurality of radio receivers may be configured to monitor the strength of the signal transmitted by the transmitter of the security container and to transmit information relating to the strength of the signal to the central location with the location information associated with the radio receiver.

One or more of the plurality radio receivers may be installed in a fixed location.

One or more of the plurality of radio receivers may be installed in a vehicle.

According to a fifth aspect of the present invention there is provided a security container for use in the system of the fourth aspect, the security container comprising a radio transmitter for transmitting a signal containing an identifier associated with the security container.

According to a sixth aspect of the present invention there is provided a radio receiver for use in the system of the fourth aspect, the radio receiver being configured to receive the signal transmitted by the transmitter of the security container and to transmit the identifier and location information associated with the radio receiver to the central location.

According to a seventh aspect of the present invention there is provided a method of tracking the location of a security container, the method comprising receiving at a radio receiver a signal containing an identifier associated with the security container and transmitting the identifier and location information associated with the radio receiver to a central location. predefined expectation.

The method may further comprise receiving location information from a positioning system receiver of the radio receiver.

The method may further comprise receiving location information from a positioning system receiver external to the radio receiver.

Transmitting the identifier and location information associated with the radio receiver to a central location may be performed by a mobile telecommunications system transmitter of the radio receiver.

The method may further comprise monitoring the strength of the signal transmitted by the transmitter of the security container and transmitting information relating to the strength of the signal to the central location with the location information associated with the radio receiver.

One or more of the plurality radio receivers may be installed in a fixed location.

One or more of the plurality of radio receivers may be installed in a vehicle.

According to an eighth aspect of the present invention there is provided a security container for storing or transporting valuable items, the security container comprising a radio receiver for receiving radio signals from a radio transmitter external to the security container and a radio transmitter for transmitting data to a central location, wherein the radio receiver is configured to decode a radio signal received from a transmitter to retrieve an identifier associated with the transmitter and the radio transmitter is configured to transmit the retrieved identifier to the central location.

The security container of the eighth aspect is able actively to transmit information relating to its location to a central location to facilitate tracking of the security container in the event of theft, or in normal operation of the security container.

The security container may further comprise means for recording the date and time at which the radio signal was received by the security container, the security container being configured to transmit the date and time to the central location with the retrieved identifier.

The security container may further comprise means for recording the strength of the radio signal received from the external transmitter, the security container being configured to transmit the received signal strength to the central location with the retrieved identifier.

The security container may further comprise memory means for storing identifiers retrieved from signals received by the radio receiver transmitted by a plurality of transmitters external to the security container.

The security container may be configured to transmit the stored identifiers to the central location at a predetermined interval.

The security container may further comprise a mobile telecommunications system transmitter for transmitting the retrieved identifier to the central location.

According to a ninth aspect of the present invention there is provided a method of announcing the location of a security container, the method comprising receiving at the security container a radio signal from a radio transmitter external to the security container, decoding the received radio signal to retrieve an identifier associated with the transmitter and transmitting the identifier to a central location.

The method may further comprise recording the date and time at which the radio signal was received by the security container and transmitting the date and time to the central location with the retrieved identifier.

The method may further comprise recording the strength of the radio signal received from the external radio transmitter and transmitting the received signal strength to the central location with the retrieved identifier.

The method may further comprise storing identifiers retrieved from signals received by the radio receiver transmitted by a plurality of transmitters external to the security container.

The method may further comprise transmitting the stored identifiers to the central location at a predetermined interval.

The retrieved identifier may be transmitted to the central location by means of a mobile telecommunications system transmitter of the security container.

According to a tenth aspect of the present invention there is provided a security system for tracking the location of a security container, the security system comprising a security container according to the ninth aspect and a plurality of radio transmitters which are each configured to transmit a signal containing an identifier associated with the radio transmitter.

According to an eleventh aspect of the present invention there is provided a radio transmitter for use in the system of the tenth aspect, the radio transmitter being configured to transmit a signal containing an identifier associated with the radio transmitter.

According to a twelfth aspect of the invention there is provided a mobile network for tracking the location of an object, the mobile network comprising a plurality of transceiver modules, each transceiver module having a radio receiver for receiving information relating to an object to be tracked and a transmitter for transmitting information relating to the object to be tracked, each transceiver module being mounted on a vehicle.

Embodiments of the invention will now be described, strictly by way of example only, with reference to the accompanying drawings, of which:

Figure 1 is a schematic representation of a security container;

Figure 2 is a schematic representation of a transceiver module for use in embodiments of the system and methods of the present invention;

Figure 3 is a schematic representation illustrating a scenario in which the location of a security container can be tracked by a security system according to an embodiment of the present invention;

Figure 4 is a schematic representation of an architecture of a system for receiving and decoding signals transmitted by a security container.

Figure 5 is a schematic representation illustrating a scenario in which a security system according to an embodiment of the present invention is used to track the location of a security container along a delivery path from a delivery vehicle to a destination;

Figure 6 is a flow chart illustrating the process undertaken by a security container to detect whether the security container is deviating from an expected delivery path and to learn or update a profile of expected radio transmitter identifiers.

Figure 7 is a schematic representation illustrating a scenario in which a security system according to an embodiment of the present invention is used by a security container to notify a central location of its position to aid in tracking the security container.

Figure 8 is a schematic representation of an architecture of a system for tracking a security container in the scenario illustrated in Figure 7; and

Figure 9 is a schematic representation of a scenario in which a security container being delivered to a destination can use a security system in accordance with an embodiment of the present invention to determine whether it is being delivered to the correct destination and adjust its mode of operation accordingly.

Referring first to Figure 1, a security container is shown generally at 10 and comprises a lockable body 12 defining a compartment 14 for receiving valuable items such as bank notes or documents to be stored or transported. The security container 10 has a theft or tamper detection mechanism 16 which is linked to a spoiling mechanism 18. The spoiling mechanism 18 is configured to dispense a spoiling or degrading agent onto or towards the contents of the compartment 14 if the theft or tamper detection mechanism 16 detects theft of or other unauthorised interference with the security container 20. It will be appreciated by those skilled in the art that a number of theft or tamper detection mechanisms 16 and spoiling mechanisms 18 are suitable for use in the security container 10 and thus these elements will not be described in detail here. In this example the security container 10 is shown as being a container that can be used to transport cash or other valuable items between locations. However, it is to be understood that the security container 10 used in embodiments of systems and methods of the present invention described herein could be any type of

container, for example a cash cassette for an Automated Teller Machine (ATM) or an ATM itself, to permit tracking of the container (the ATM or ATM cassette) during transit or in the event of theft, for example.

The security container 10 includes a communications module 20 which allows the security container 10 to communicate with the outside world by means of radio signals. The communications module 20 includes a radio receiver 22 which is capable of receiving radio signals from radio transmitters external to the security container 10. For example, the radio receiver may be configured to receive signals transmitted in accordance with the IEEE 802.11 standard (sometimes referred to as Wi-Fi® signals). The communications module 20 also includes a radio transmitter 24 which is capable of transmitting radio signals such as Wi-Fi® signals.

The communications module 20 also includes a GSM transceiver 26 which is capable of transmitting signals to a GSM mobile telecommunications network. The communications module 20 has an antenna 28 which is connected to the radio receiver 22, the radio transmitter 24 and the GSM transceiver 26 by way of an appropriate multiplexer (not shown). In an alternative embodiment, a separate antenna may be provided for each of the radio receiver 22, the radio transmitter 24 and the GSM transceiver 26.

The communications module 20 may also include a high-power radio transmitter 27 which is operative to transmit a beacon signal that can be detected by suitable detection equipment, (which detection equipment may be provided with a directional antenna), allowing the location of the security container to be tracked to within metres. The transmitter 27 may transmit the beacon signal in the 433 MHz frequency band, for example.

The communications module 20 is connected to a data processor 30 which is configured to perform a variety of functions, including decoding signals received by the radio receiver 22 and encoding data to be transmitted by the radio transmitter 24 and the GSM transceiver 26. The data processor 30 is connected to the theft or tamper detection mechanism 16 such that the operating mode of the theft or tamper detection mechanism 16 can be altered in accordance with a signal received by the communications module 20. The data processor 30 can also control the operating mode of the communications module 20 and the radio receiver

22, the radio transmitter 24 and the GSM transceiver 26. The data processor 30 may be a general purpose processor integrated circuit (IC) executing appropriate instructions, or may be a bespoke processor implemented as a Field Programmable Gate Array (FPGA), Application Specific Integrated Circuit (ASIC), Digital Signal Processor (DSP) or the like.

A non-volatile memory 32 is provided which contains a unique identifier for the security container 10. The non-volatile memory 32 may be provided as part of the data processor 30 or may be a separate memory element connected to the data processor 30, as illustrated in Figure 1. The unique identifier may be, for example, an alphanumeric string, a sequence of bits, or may take any other form which enables the security container 10 to be identified by the unique identifier. The unique identifier may be permanently stored in the non-volatile memory 32, or else the non-volatile memory may be programmable with the unique identifier, such that the unique identifier can be changed if required.

Figure 2 is a schematic representation of a transceiver module for use in embodiments of the systems and methods of the present invention. The transceiver module, shown generally at 40 in Figure 2 includes a radio receiver 42 for receiving radio signals such as Wi-Fi® signals and a radio transmitter 44 for transmitting radio signals such as Wi-Fi® signals. A GSM transmitter 46 is also provided to enable the transceiver module 40 to transmit signals using a GSM mobile communications network, whilst an Ethernet port 47 allows the transceiver module 40 to connect to a network such as a Local Area Network (LAN) of a building or vehicle in which the transceiver module 40 is installed.

The transceiver module 40 may also include a receiver 48 for a positioning system such as the Global Positioning System (GPS). Additionally or alternatively the transceiver module 40 may include an input 50 for a signal from an external positioning system receiver, such as a GPS receiver installed in a vehicle.

The transceiver module 40 includes an antenna 52 which is connected to the radio receiver 42, the radio transmitter 44, the GSM transmitter 46 and the positioning system receiver 48 by means of a suitable multiplexer (not shown). Alternatively, the radio receiver 42, the radio transmitter 44, the GSM transmitter 46 and the GPS receiver 48 may each be provided with a separate antenna.

The transceiver module 40 includes a data processor 54 which is connected to the radio receiver 42, the radio transmitter 44, the GSM transmitter 46, the Ethernet port 47 and the positioning system receiver 48 and/or input 50. The data processor 54 is configured to perform a variety of functions including decoding signals received by the radio receiver 42 and generating messages to be transmitted by the radio transmitter 44, the GSM transmitter 46 and/or via the Ethernet port 47. The data processor 54 may be a general purpose processor IC executing appropriate instructions, or may be a bespoke processor implemented as an FPGA, ASIC, DSP or the like.

The transceiver module 40 may have a non-volatile memory 56. The non-volatile memory 56 may be provided as part of the data processor 54 or may be a separate memory element connected to the data processor 54, as illustrated in Figure 2. The non-volatile memory may be used to store a representation of the location of the transceiver module 40, for example as GPS co-ordinates. Thus, where the transceiver module 40 is used in a single fixed location, for example in a bank, post office or Automated Teller Machine (ATM) the coordinates of the location of the transceiver module 40 may be programmed into and stored in the non-volatile memory 56. Where the transceiver module 40 is intended for use in a fixed location the positioning system receiver 48 and the input 50 may be omitted.

The transceiver module 40 is also provided with means for determining the date and time of a signal received by the radio receiver 42. This may be a separate clock 58 which is connected to the data processor 54, or else the data processor 54 may be configured to retrieve timing information from a received signal, for example a GPS signal received by the positioning system receiver 48 or via the input 50.

Figure 3 is a schematic representation illustrating a scenario in which the location of a security container 10 can be tracked by a security system according to an embodiment of the present invention. In this example the security system uses a plurality of transceiver modules 40 of the type described above located in buildings and vehicles to track the location of the security container 10.

In the scenario illustrated in Figure 3 a security container 10 is being transported in a car 60. This may be because the security container 10 has been stolen, or it may be that it is simply being transported in the car 60 to its final destination.

Initially the car 60 is at a first location A. The radio transmitter 24 of the communications module 20 of the security container 10 is active and transmits a signal containing the unique identifier of the security container 10. This signal may be transmitted as a Wi-Fi® signal, or may be transmitted according to some other communications protocol that can be received and decoded by a transceiver module 40. The signal may be transmitted continuously or periodically. The radio transmitter 24 of the security container 10 has a limited transmission range, indicated by the circle 62. Thus, the signal transmitted by the radio transmitter 24 can only be detected by compatible receivers within the area delimited by the circle 62.

At location A the car 60 is in the vicinity of a building 64, which may be a bank, post office or the like. The building 62 is equipped with a fixed transceiver module 66 of the type described above with reference to Figure 2, whose radio receiver 42 has a limited detection range, as indicated by the circle 68. Thus, the radio receiver 42 of the transceiver module 66 can only detect signals in the area delimited by the circle 68. As the transceiver module 66 is in a fixed position, an indication of its position is stored in the non-volatile memory 56, and the positioning system receiver 48 and input 50 may be omitted from the transceiver module 66.

At location A the car 60 is also in the vicinity of a delivery vehicle 70. The delivery vehicle 70 is equipped with a transceiver module 72 of the type described above with reference to Figure 2. The radio receiver 42 of the transceiver module 72 has a limited detection range, as indicated by the circle 74. Thus, the radio receiver 42 of the transceiver module 70 can detect radio signals in the area delimited by the circle 74.

As the transceiver module 72 is mounted on a delivery vehicle 70, its location is not fixed. Thus, the transceiver module 72 may have an active positioning system receiver 48, such as a GPS receiver, or may be connected, via the input 50, to an existing positioning system receiver of the delivery vehicle 70.

At location A, the radio signal transmitted by the radio transmitter 24 of the security container 10 cannot be detected by the radio receiver 42 of the fixed transceiver module 66 located in the building 64, as the signal is outside of the detection range of that radio receiver 42, as indicated by the non-overlapping circles 62, 68.

However, the radio signal transmitted by the radio transmitter 24 of the security container 10 can be detected by the radio receiver 42 of the transceiver module 72 of the delivery vehicle, as the transmitted signal of the security container is within the detection range of the radio receiver 42 of the transceiver module 72, as indicated by the overlapping circles 62, 74. Thus, the transceiver module 72 detects the signal transmitted by the radio transmitter 24 of the security container 10.

On detection by the transceiver module 72 of the radio signal transmitted by the radio transmitter 24 of the security container 10, the data processor 54 of the transceiver module 72 decodes the received signal and extracts the unique identifier of the security container 10. The data processor 54 records the date and time at which the signal was received by extracting this information from the clock 58 or from a signal received by the positioning system receiver 48 or via the input 50, and the position of the delivery vehicle 70 when the signal was received, as reported by the positioning system receiver 48 or the vehicle's own positioning system receiver via the input 50. The data processor 54 also calculates and records the strength of the received signal.

The data processor 54 constructs a message containing the unique identifier of the security container 10, the date and time the signal from the security container 10 was received, the position of the delivery vehicle 70 at the time of receiving the signal and the strength of the received signal. This message is passed to the GSM transmitter 46 for transmission over a GSM network to a central location, at which the data is decoded and used to track the location of the security container 10, as will be described below.

As the car 60 travels towards its destination it passes through a second location B. At location B the car 60 is in the vicinity of delivery vehicles 80 and 90. The transmit range of the transmitter 22 of the security container 10 is indicated by the circle 92.

Only delivery vehicle 90 can detect the signal transmitted by the radio transmitter 24 of the security container 10, since the receive range (indicated by circle 84) of the radio receiver 42 of a transceiver module 82 of the delivery vehicle 80 is not great enough, as shown by the non-overlapping circles 84, 92. The receive range of the radio receiver 42 of a transceiver module 94 of the delivery vehicle 90 is indicated by the circle 96, and as this overlaps with the circle 92 the signal transmitted by the radio transmitter 24 of the security container 10 can be detected by the transceiver module 94 of the delivery vehicle 90.

As before, on detection by the transceiver module 94 of the delivery vehicle 90 of the signal transmitted by the radio transmitter 24 of the security container 10, the data processor 54 decodes the received signal to recover the unique identifier of the security container 10 and constructs a message containing this unique identifier, the date and time at which the signal was received, the location of the delivery vehicle 90 at the time of receiving the signal and the received signal strength. This message is passed to the GSM transmitter 46 of the transceiver module 94 for transmission over a GSM network to the central location, where the data is decoded and used to track the location of the security container 10.

It will be appreciated that the transceiver module equipped delivery vehicles 70, 90 form a mobile network of transceiver modules 40 which can be used to track the location of the security container 10. This mobile network of transceiver modules 40 can also be used for other tracking purposes and applications, as will be appreciated by those skilled in the art.

The car 60 then passes through a location C, at which it is in the vicinity of a building 100. The transmit range of the radio transmitter 24 of the security container 10 is indicated by the circle 102. The building 100 has a fixed transceiver module 104 of the type described above with reference to Figure 2. The radio receiver 42 of the transceiver module 104 has a limited receive range, as indicated by the circle 106.

As the circles 102, 106 overlap, the signal transmitted by the radio transmitter 24 of the security container 10 is within range of the radio receiver 42 of the transceiver module 104, and thus the signal can be detected by the transceiver module 104.

On detection by the transceiver module 104 of the signal transmitted by the radio transmitter 24 of the security container 10, the data processor 54 of the transceiver module 104 decodes the received signal to retrieve the unique identifier of the security container 10. The strength of the received signal is calculated by the data processor 54, and the date and time at which the signal was received is recorded, based on information retrieved by the data processor 54 from the clock 58. As the transceiver module 104 is in a fixed location, its location is stored in the non-volatile memory 56. This information is retrieved by the data processor 54 and used to create a message containing the unique identifier of the security container 10, the date and time on which the signal was received, the strength of the received signal and the location of the transceiver module 104. This message is passed to the GSM transmitter 46 for transmission via the GSM network to the central location where it is decoded and used to track the location of the security container 10. Alternatively, the message may be passed to the Ethernet port 47 with appropriate routing instructions to allow it to be transmitted to a network such as a LAN of the building 100 for onward transmission, via the Internet or a fixed telephone network to the central location.

The radio transmitter 24 of the security container 10 may be permanently active, to permit tracking of the security container 10 at any time. Alternatively, the radio transmitter 24 may be activated only in certain circumstances, such as if the theft or tamper detection mechanism 16 detects theft of or other unauthorised interference with the security container 20, or if theft of the security container 10 is detected by another mechanism.

Referring now to Figure 4, an architecture of a system for receiving and decoding signals transmitted by the GSM transmitter 46 of a security container to the central location is shown generally at 120. The system 120 allows the owners of security containers 10 to track the location of their containers 10 using an Internet based system, as will be described below.

The system 120 has an antenna 122 through which incoming GSM signals are received. Received signals are decoded by a GSM data processor 124 to extract the unique identifier, date, time, position and received signal strength contained in the signal transmitted by the GSM transmitter 46 of the security container 10. These details are passed to a secure server 126 which stores these data in a database 128. The secure server 126 compares the unique identifier contained in each received signal to a look up table containing a list of unique

identifiers for security containers 10 and the owners of those security containers, so as to associate each received signal with the correct owner of the corresponding security container 10. Alternatively, a common prefix or suffix may be provided in the unique identifier to identify security containers 10 belonging to each particular owner. For example, security containers 10 belonging to a first owner may be prefixed with the string "1234", whilst those of a second owner may be prefixed with the string "5678". Thus in this example the secure server 126 can associate each received signal with the correct owner by examining the prefix of the unique identifier of each received signal. An exemplary database record for a particular owner of security containers is shown at 130, and contains entries for the unique identifier, date, time, position and received signal strength of a security container 10 belonging to that particular owner at different time points.

The secure server 126 can be accessed by users 132, 134, 136 by means of an Internet interface 138. A user 132, 134, 136 accessing the secure server 126 is required to enter identification details such as a username and password before any information relating to the security containers 10 is presented. Once the secure server 126 has ascertained the user 132, 134, 136 is a legitimate authorised user of the system 120, it retrieves the data associated with that user's security containers 10 and causes the data to be displayed on the user's computer screen. This may be as "raw" data, or the position of the user's security containers 10 may be displayed on a map view, with the received signal strength information being used to estimate the distance of the security containers 10 from the reported positions of the transceiver modules 40, such that approximate current and previous positions, for example, for the or each security container 10 can be displayed on the map display on the user's computer.

Figure 5 is a schematic representation illustrating a scenario in which a security system according to an embodiment of the present invention is used to track the location of a security container 10 along a delivery path from a delivery vehicle to a destination to ensure that it is following an expected path. If the security container 10 deviates from this path it may infer that it is being stolen or otherwise interfered with and may thus adjust its mode of operation accordingly.

In this scenario a delivery vehicle 142 stops at a location A which is some distance away from a delivery destination E, and a delivery guard removes the security container 10 from

the delivery vehicle 142 to deliver it on foot to the delivery destination E. The delivery vehicle is equipped with a transceiver module 40 of the type described above.

Before the security container 10 is removed from the delivery vehicle 142, the delivery vehicle 142 informs the security container 10 of the location of the delivery vehicle 142. This may be achieved, for example, by transmitting a signal containing GPS co-ordinates reported by the positioning system receiver 48 of the transceiver unit 40 of the delivery vehicle 142, or provided to the transceiver unit 40 via the input 50, to the communications module 20 of the security container 10. The delivery vehicle 142 may also transmit a signal containing GPS coordinates or other location information associated with the destination E, or this information may be provided to the security container 10 at a dispatch facility prior to delivery.

On receiving the location of the delivery vehicle 142, the security container obtains a profile listing identifiers associated with radio signals that are expected to be present on the delivery path from the delivery vehicle 142 to the destination E. The identifiers may be, for example, identifiers for Wi-Fi® networks which are present in the vicinity of the delivery path. This profile may be stored in a database in the non-volatile memory 32 of the security container 10 and retrieved by using the location information of the delivery vehicle 142 and the destination E as references for a look-up table. Alternatively, the security container 10 may transmit a signal containing the location information of the delivery vehicle 142 and the destination E to a central location using the GSM transceiver 26, such that the appropriate profile can be transmitted to the security container 10 in a response signal sent over the GSM network. Once the appropriate profile has been obtained by the security container 10, the radio receiver 22 is activated so as to receive radio signals from transmitters along the delivery path.

In the example illustrated in Figure 5, the security container 10 travels from the location A, in which it receives a radio signal such as a Wi-Fi® signal transmitted by the radio transmitter 42 of the transceiver module 40 of the delivery vehicle 142. The security container then moves into a location B in the vicinity of a building 144 which is equipped with a transceiver module 40 of the type described above, or with another radio transmitter such as a wireless network hub transmitting Wi-Fi® signals. The radio receiver 22 of the security container detects the radio signal transmitted by the radio transmitter of the building 144 and the data

processor 30 decodes the signal to extract an identifier of the radio transmitter. The data processor 30 then compares this identifier to the profile to determine whether the security container 10 is following an expected delivery path.

The comparison of the received identifier with the profile may be performed in a number of ways. In a simple embodiment the data processor 30 simply compares the received identifier to all of the identifiers listed in the profile and takes no further action if the received identifier matches one of the identifiers in the profile. Alternatively, the data processor 30 may assess whether the received identifier has been received in an expected position, by comparing a sequence of received identifiers (in this example the identifier for the delivery vehicle 142 and the identifier for the building 144) to the profile. If the received identifier sequence matches the sequence of identifiers in the profile the data processor 30 may take no further action. The data processor 30 may also assess whether the received identifier was received within an expected period of time since the security container 10 left the delivery vehicle 142. If this is the case the data processor 30 may take no further action.

If the received identifier does not correspond to the expected identifier contained in the profile the data processor 30 takes action to adjust the operating mode of the security container 10. The action taken by the data processor 30 may depend upon the number of identifiers received or the time at which the or each identifier was received. For example, if the security container 10 has received only two identifiers in a time period in which three identifiers were expected to be received, the data processor 30 may take no action, since it is possible that one of the expected radio transmitters in the delivery path is not functional and thus the security container 10 is not deviating from the expected delivery path, or may set the operating mode of the security container 10 to a low level of alert, for example by readying the theft or tamper detection mechanism 16 or the spoiling mechanism 18 for activation. However, where the sequence of received identifiers deviates more from the expected sequence, for example if only two identifiers are received in a time period in which five identifiers are expected to be received, the data processor 30 may take action to set the operating mode of the security container 10 to a higher level of alert, for example by activating the theft or tamper detection mechanism 16 or the spoiling mechanism 18, or by entering a tracking mode such as that described above with reference to Figures 3 and 4, in

which the radio transmitter 24 of the security container 10 is activated to permit the location of the security container to be tracked.

The scenario described above makes use of a security system in which transceiver modules 40 are provided at fixed locations. However, where a location is provided with a radio transmitter such as a Wi-Fi® access point, this could be used in place of the transceiver module 40, provided that the signal transmitted by the radio transmitter is sufficiently strong to be detected by the radio receiver 22 of the security container 10.

The security container 10 is able to learn a profile of expected radio transmitters on a delivery path, and can update or self-heal an existing profile by removing redundant transmitter identifiers from the profile and replacing them with newly-active transmitter identifiers, provided that the newly-active transmitter identifiers pass a test, such as a peer review based test conducted by a secure server at a central location such as a dispatch depot, or by the data processor 30 of the security container 10.

Figure 6 is a flow chart illustrating the process undertaken by the data processor 30 of the security container 10 to detect whether the security container is deviating from an expected delivery path and to learn or update a profile of expected radio transmitter identifiers.

The process begins at step 160, where a test is made to determine if the security container is leaving the delivery vehicle 142. If not, the process returns to the start. If the data processor 30 determines that the security container 10 is leaving the delivery vehicle 142 it receives location information from the delivery vehicle 142, for example in the form of GPS coordinates, and selects a stored profile on the basis of the location information at step 164, as is described above. Timing information is recorded at step 166, for example by starting a timer which runs on the data processor 30.

The radio receiver 22 of the security container 10 is activated at step 168 and performs a scan for active radio transmitters such as Wi-Fi® transmitters in the vicinity of the security container 10. At step 170 a test is performed to determine if a radio transmitter has been identified. If so, a further test is performed at step 172 to compare the identifier of the radio transmitter to the profile to determine whether the identified transmitter is one of the expected

transmitters on the delivery path. If the transmitter identifier does not appear in the profile it is stored temporarily, for example in the non-volatile memory 32 of the security container, at step 174.

At step 176 a test is made to see if a predetermined period of time has expired, for example by checking the timer running on the data processor 30. If it has, the stored transmitter identifier is discarded (at step 178) and the operating mode of the security container is adjusted to a higher level of alert at step 180, as described above. This is because an expected radio transmitter has not been identified within a given time period, so the data processor 30 determines that the security container 10 may be at risk of theft.

If the test at step 172 determines that the received radio transmitter identifier corresponds to an identifier contained in the profile, the timer running on the data processor 30 is restarted, or an alternative action is taken by the data processor 30, such as recording the current time, to initialise the countdown of a predetermined time period (step 182). A test is then performed at step 184 to assess whether the security container 10 has reached its destination, by comparing the identifier of the received signal to a known identifier associated with a radio transmitter at the destination. If the result of this test is negative the data processor 30 returns to step 168 and a new scan for active radio transmitters is performed. If the result of this test is positive the timer started at step 166 is stopped at step 185 (or an equivalent action is taken to stop the countdown of the predetermined time period) and any new network identifiers stored by the security container are transmitted, at step 186, to a central location by the GSM transceiver 26 for review to determine whether the relevant profile should be updated.

Turning now to Figure 7, a scenario is illustrated in which a security system according to an embodiment of the present invention is used by a security container 10 of the type described above to notify a central location of its position to aid in tracking the security container 10, for example in the event of theft of the security container 10.

In this scenario, the theft and tamper detection mechanism 16 of the security container 10 has determined that the security container 10 has been stolen, and the data processor 30 has thus set the operating mode of the security container 10 into a high alert mode in which the radio

receiver 22 of the security container 10 is activated so as to detect radio signals transmitted by radio transmitters in the vicinity of the security container 10. It will be appreciated, however, that this mode of operation can also be used to aid in the tracking of a security container 10 in normal use, that is to say when it has not been deemed stolen.

In this example the security container is being transported in a car 200. The car 200 passes through a location A in the vicinity of a building 202 which is equipped with a transceiver module 40 of the type described above. The radio transmitter 44 of the transceiver module 40 is active and transmits an identifier which can be used to identify the transceiver module 44. The transmit range of the transmitter 44 of the transceiver module 40 of the building 202 is indicated by the circle 204. When the car enters location A, the radio receiver 22 of the security container 10 is within range of the transmitter 44 and thus receives the signal transmitted by the transmitter 44. The identifier associated with the transceiver module 40 of the building 202 is retrieved by the data processor 30 from the received signal and is recorded by the security container 10, for example in the non-volatile memory 32, for later use. The time at which the signal was received by the radio receiver 22 and the strength of the received signal are also calculated by the data processor 30 and recorded and associated with the identifier of the transceiver module 40 of the building 202.

As the car 200 passes through locations B, C and D in the vicinity of buildings 206, 210, 214 respectively, each of which is equipped with a transceiver module 40, the security container 10 retrieves and records the unique identifiers associated with the transceiver modules 40 of the buildings 206, 210, 214, as well as the date and time on which they were received and the strength of the received signals, in the manner described above. As the security container 10 approaches location B it is still able to detect signals from the transceiver module 40 of building 202, as well as signals from the transceiver module 40 of building 206. Thus, at this point the identifiers associated with the transceiver modules 40 of both building 202 and building 206 are recorded, along with the time at which the signals from those transceiver modules 40 were received and the strength of the received signals.

At a predefined interval the data processor 30 constructs a message containing the identifiers associated with the transceiver modules 40 of the buildings 202, 206, 210, 214 in the locations A, B, C, D through which the car 200 has passed, the date and time at which signals

containing these identifiers were received by the security container 10, the strength of the respective received signals and the unique identifier of the security container 10 itself. This message is transmitted over the GSM network by the GSM transceiver 26 of the security container 10 to a central location at which the message is received and decoded to enable the location of the security container 10 to be tracked.

The scenario described above make use of a security system in which transceiver modules 40 are provided at fixed locations. However, where a location is provided with a radio transmitter such as a Wi-Fi® access point, this could be used in place of the transceiver module 40, provided that the signal transmitted by the radio transmitter is sufficiently strong to be detected by the radio receiver 22 of the security container 10.

An architecture of a system for tracking a security container in the scenario illustrated in Figure 7 is shown generally at 220 in Figure 8. The system 220 has an antenna 222 for receiving incoming GSM signals. Received signals are decoded by a GSM data processor 224 to extract the unique identifier of the security container 10, the location identifiers (i.e. the identifiers of the transceiver modules 40 associated with the locations through which the security container 10 has travelled), the signal strength of the signals received by the security container 10 and the date and time associated with each of these identifiers. These details are passed to a secure server 226 which in turn stores them in a database 228. The secure server 226 also passes the location identifiers to a database containing location data for the transceiver modules 40. This location information database may be an internal database 230 or may be an external database 232 which is accessed by a web interface 234.

The location information databases 230, 232 contain identifiers of transceiver modules 40 at a large number of locations, including the locations A, B, C and D of the example illustrated in Figure 7. Each identifier in the database 230, 232 is associated with location information such as GPS coordinates of the transceiver module 40 identified by the location identifier.

The location information database 230, 232 returns the location data, for example GPS coordinates, associated with the location identifiers passed to it by the secure server 226, and the secure server 226 uses the location data to construct a trace of the approximate location of the security container 10 over time, using the data and time information associated with each

location identifier in the received signal. The secure server 226 may refine the approximate location using the received signal strength of the signals received by the security container. For example, the received signal strength of a signal received by the security container 10 can be used to determine an approximate distance of the security container 10 from the transceiver module 40 associated with the location data at the time that the signal was received by the security container 10. Thus, for each location identifier reported by the security container 10 to the secure server 226 the secure server 226 can determine the location of the transceiver module 40 associated with the location identifier and an approximate distance of the security container 10 from that transceiver module 40, thus defining a generally circular area whose radius is equal to the approximate distance of the security container 10 from the identified transceiver module 40 in which the security container is likely to be located.

The strength or other characteristics of the GSM signal received at the central location may also be used to refine or further refine the approximate location calculated by the secure server 226 on the basis of the location identifiers and the received signal strength information transmitted by the security container 10. For example, the secure server 226 may receive from the GSM network data indicative of the area in which the security container 10 was located at the time of transmitting the GSM message constructed by the data processor 26. This area data is calculated by the GSM network using a triangulation method which will be familiar to those skilled in the relevant art and will thus not be described in detail here. The area data provided by the GSM network can be used by the secure server 226 to refine the calculation of the approximate location of the security container 10, for example by disregarding locations calculated by the secure server 226 which do not overlap with areas indicated by the area data provided by the GSM network, or locations calculated by the secure server 226 which are greater than a predetermined distance from the areas indicated by the area data provided by the GSM network.

The secure server 226 can be accessed by external users 236, 238, 240 by means of an Internet interface 242. A user 236, 238, 240 accessing the secure server 226 is required to enter identification details such as a username and password before any information relating to the security containers 10 is presented. Once the secure server 226 has ascertained the user 236, 238, 240 is a legitimate authorised user of the system 220, it retrieves the data associated

with that user's security containers 10 and causes the data to be displayed on the user's computer screen. This may be as "raw" data, or the position of the user's security containers 10 may be displayed on a map view, giving approximate current and previous positions, for example, for the security container 10. As in the example illustrated in Figure 4, details of the movements of a particular user's security container(s) 10 can be retrieved by the secure server 226 by selecting from the database 228 only those records where the stored unique identifier of the security container 10 is associated with that particular user. The secure server 226 may, for example, consult a look up table or examine a prefix or suffix of the stored unique identifier of the security container 10 to select the appropriate record(s) from the database 228.

Figure 9 is a schematic representation of a scenario in which a security container 10 being delivered to a destination can use a security system in accordance with an embodiment of the present invention to determine whether it is being delivered to the correct destination and adjust its mode of operation accordingly.

In the scenario illustrated in Figure 9 a security container 10 of the type described above is being transported from a delivery vehicle 260 to a destination 262, which may be a bank, for example, along a delivery path 264. The delivery vehicle 260 is parked close to the destination 262, and is equipped with a transceiver module 40 of the type described above. The destination 262 is also equipped with a transceiver module 40 of the type described above.

Before the security container 10 is removed from the delivery vehicle 260, information relating to the location of the delivery vehicle 260 is passed to the security container 10. This information may be in the form of GPS coordinates provided by a positioning system receiver 48 of the transceiver module 40 of the delivery vehicle 260 or by a positioning system receiver of the delivery vehicle 260 via the input 50 of the transceiver module 40 of the delivery vehicle 260. The location information may, for example, be transmitted by the radio transmitter 44 of the transceiver module 40 and may be received by the radio receiver 22 of the security container 10.

On receiving the location information from the delivery vehicle 260 the security container retrieves an identifier associated with the transceiver module 40 of the destination 262 from a database. The database may be stored in the non-volatile memory 32 of the security container 10 and accessed by the data processor 30, or may be a remote database accessed by the security container 10 using the GSM transceiver 26. The retrieved identifier allows the security container 10 to recognise radio transmissions from the transceiver module 40 of the destination 262.

The radio receiver 22 of the security container 10 is activated so as to receive radio signals from transmitters in the vicinity of the security container 10. The radio transmitter 44 of the transceiver module 40 of the delivery vehicle 260 is also activated to transmit a radio signal (such as a Wi-Fi®) signal containing a unique identifier identifying the transceiver 40 of the delivery vehicle.

When the security container 10 is removed from the delivery vehicle 260 it can detect the signal transmitted by the transceiver module 40 of the delivery vehicle, which has a range indicated by the circle 266. It can also detect the signal transmitted by the transceiver module 40 of the destination 262, which has a range indicated by the circle 268.

As the security container 10 moves along the delivery path 264, it moves away from the delivery vehicle 260 and towards the destination 262. Thus, the strength of the signal received by the security container 10 from the transceiver module 40 of the delivery vehicle 260 reduces as the security container 10 moves along the delivery path 264, whilst the strength of the signal received by the security container 10 from the transceiver module 40 of the destination 262 increases.

The data processor 30 of the security container 10 monitors the strength of these received signals to determine whether the security container 10is moving in the correct direction. If the received signal strength deviates from an expected profile (which may be stored in the non-volatile memory 32 of the security container 10), for example if one or both of the signals from the transceivers 40 of the delivery vehicle 260 and the destination 262 can no longer be detected, such as if the strength of one or both of the received signals falls to zero, the data processor 30 may infer that the security container 10 is being stolen or otherwise interfered

with and may thus adjust its mode of operation accordingly. For example, the data processor 30 may set the operating mode of the security container 10 to a first, relatively low level of alert, for example by readying the theft or tamper detection mechanism 16 for activation, or to a higher level of alert, for example by activating the theft or tamper detection mechanism, or by entering a tracking mode such as those described above with reference to Figures 3, 4 and 7, in which the radio receiver 22 and/or the radio transmitter 24 of the security container 10 are activated to permit the location of the security container 10 to be tracked.

When the security container 10 is very close to the transceiver module 40 of the destination 262 the strength of the signal received by the security container 10 is very high, and the data processor 30 may be configured to recognise this as an indication that the security container 10 has arrived safely at the destination 262, and take action to reduce the level of alert of the security container 10, since the risk of theft has decreased. The data processor 30 may be configured to compare the strength of the signal received from the transceiver module 40 of the destination 262 to a threshold and to adjust the operating mode of the security container 10 by reducing its level of alert if the received signal strength meets or exceeds the threshold. In order to reduce the possibility of false signal strength readings causing the data processor 30 incorrectly to reduce the alert level of the security container 10, the data processor 30 may be configured only to reduce the alert level if the strength of the signal received from the transceiver module 40 at the destination 262 meets or exceeds the threshold for a predetermined length of time, for example three minutes or more.

The scenario described above makes use of a security system in which a transceiver module 40 is provided at the destination 262. However, if the destination 262 is provided with a radio transmitter such as a Wi-Fi® access point, this could be used in place of the transceiver module 40, provided that the signal transmitted by the radio transmitter is sufficiently strong to be detected by the radio receiver 22 of the security container 10.

In an alternative embodiment, a short-range radio transmitter such as a Wi-Fi® access point having a range of around 5 to 10 metres may be provided a the destination 262 (for example as part of the transceiver module 40 of the destination 262), and the security container 10 may be configured to adjust its operating mode on detection of the signal transmitted by the short-range radio transmitter, for example by reducing its level of alert or by deactivating a

locking mechanism, since detection of this signal is indicative that the security container 10 has reached the destination 262.

Although in the examples described above the radio receiver 22 and the radio transmitter 24 of the security container 10 and the radio receiver 44 and radio transmitter 42 of the transceiver module have been described as being capable of receiving and transmitting Wi-Fi® signals it will be appreciated that any other communications standard or protocol could equally be employed. Similarly, the GSM transceivers 26, 46 in the security container 10 and the transceiver module may be replaced with transceivers operating in accordance with an alternative standard such as TETRA, although GSM is a convenient system to use because of the ubiquity of GSM networks.

CLAIMS

1. A security container for storing or transporting valuable items, the security container comprising a radio receiver for receiving radio signals from a radio transmitter external to the security container, wherein the security container is configured to adjust an operating mode if a received radio signal does not correspond to a signal expected by the security container.

2. A security container according to claim 1 wherein the radio receiver is configured to decode a radio signal received from a transmitter to retrieve an identifier associated with the transmitter and the security container is configured to determine from the identifier whether the security container is following a predetermined transit path.

3. A security container according to claim 1 or claim 2 wherein the security container is configured to assess whether the signal was received within an expected time period.

4. A security container according any one of the preceding claims wherein the radio receiver is configured to receive a sequence comprising signals transmitted by each of a plurality of external radio transmitters, each signal containing an identifier associated with the respective transmitter and the security container is configured to compare the identifiers of the received sequence to a stored sequence of expected identifiers.

5. A security container according to claim 3 or claim 4 wherein the security container is configured to record an identifier contained in a signal received from an external transmitter if that identifier is not a member of the stored sequence.

6. A security container according to claim 1 wherein the radio receiver is configured to receive a first signal transmitted by a radio transmitter of a delivery vehicle and a second signal transmitted by a radio transmitter of a destination to which the security container is to be delivered, the security container being configured to adjust the operating mode if it does not receive the first and second signals in accordance with a predefined expectation.

7. A security container according to claim 6 wherein the security container is configured to monitor the strength of the first and second signals and to adjust operating mode if the strength of the first and second signals deviates from an expected profile.

8. A security container according to claim 7 wherein the security container is configured to adjust the operating mode if the strength of the first or second signal falls to zero.

9. A security container according to any one of the preceding claims wherein the security container is configured to adjust the operating mode by increasing an alert level of the security container.

10. A security container according to claim 7 wherein the security container is configured to compare the strength of the second signal to a threshold value and to adjust the operating mode if the strength of the second signal meets the threshold.

11. A security container according to claim 10 wherein the security container is configured to adjust the operating mode only if the signal strength meets the threshold for a predetermined period of time.

12. A security container according to any one of claims 1 to 11 wherein the security container is configured to adjust its operating mode on detection of a signal transmitted by a short range radio transmitter located at or near a delivery destination of the security container.

13. A security container according to claim 10 or claim 11 wherein the security container is configured to adjust the operating mode by reducing an alert level of the security container.

14. A security container according to any one of claims 11 to 13 wherein the security container is configured to adjust its operating mode by deactivating a locking mechanism.

15. A method of controlling an operating mode of a security container, the method comprising receiving radio signals from a radio transmitter external to the security container, and adjusting the operating mode if a received radio signal does not correspond to a signal expected by the security container.

16. A method according to claim 15 further comprising decoding a radio signal received from a transmitter to retrieve an identifier associated with the transmitter and determining from the identifier whether the security container is following a predetermined transit path.

17. A method according to claim 15 or claim 16 further comprising assessing whether the signal was received within an expected time period.

18. A method according any one of claims 15 to 17 further comprising receiving a sequence comprising signals transmitted by each of a plurality of external radio transmitters, each signal containing an identifier associated with the respective transmitter, and comparing the identifiers of the received sequence to a stored sequence of expected identifiers.

19. A method according to claim 17 or claim 18 further comprising recording an identifier contained in a signal received from an external transmitter if that identifier is not a member of the stored sequence.

20. A method according to claim 15 further comprising receiving a first signal transmitted by a radio transmitter of a delivery vehicle and a second signal transmitted by a radio transmitter of a destination to which the security container is to be delivered and adjusting the operating mode if the first and second signals are not received in accordance with a predefined expectation.

21. A method according to claim 20 further comprising monitoring the strength of the first and second signals and adjusting the operating mode if the strength of the first and second signals deviates from an expected profile.

22. A method according to claim 21 further comprising adjusting the operating mode if the strength of the first or second signal falls to zero.

23. A method according to any one of claims 15 to 22 wherein adjusting the operating mode comprises increasing an alert level of the security container.

24. A method according to claim 23 further comprising comparing the strength of the second signal to a threshold value and adjusting the operating mode if the strength of the second signal meets the threshold.

25. A method according to any one of claims 15 to 24 further comprising adjusting the operating mode on detection of a signal transmitted by a short range radio transmitter located at or near a delivery destination of the security container.

26. A method according to claim 24 or claim 25 wherein adjusting the operating mode comprises reducing an alert level of the security container.

27. A method according to any one of claims 24 to 26 wherein adjusting the operating mode comprises deactivating a locking mechanism of the security container.

28. A security system comprising a security container according to any one of claims 1 to 14 and a radio transmitter for transmitting a signal that can be detected by the radio receiver of the security container.

29. A system for tracking the location of a security container, the system comprising a security container comprising a radio transmitter which is configured to transmit a signal containing an identifier associated with the security container and a plurality of radio receivers, each of the plurality of radio receivers being configured to receive the signal transmitted by the transmitter of the security container and to transmit the identifier and location information associated with the radio receiver to a central location.

30. A system according to claim 29 wherein each of the plurality of receivers comprises a positioning system receiver for providing the location information associated with the radio receiver.

31. A system according to claim 29 or claim 30 wherein each of the plurality of radio receivers comprises an input for receiving location information from a positioning system receiver external to the radio receiver.

32. A system according to any one of claims 29 to 31 wherein each of the plurality of radio receivers comprises a mobile telecommunications system transmitter for transmitting the identifier and location information associated with the radio receiver to a central location.

33. A system according to any one of claims 29 to 32 wherein each of the plurality of radio receivers is configured to monitor the strength of the signal transmitted by the transmitter of the security container and to transmit information relating to the strength of the signal to the central location with the location information associated with the radio receiver.

34. A system according to any one of claims 29 to 33 wherein one or more of the plurality radio receivers is installed in a fixed location.

35. A system according to any one of claims 29 to 34 wherein one or more of the plurality of radio receivers is installed in a vehicle.

36. A security container for use in the system of any one of claims 29 to 35, the security container comprising a radio transmitter for transmitting a signal containing an identifier associated with the security container.

37. A radio receiver for use in the system of any one of claims 29 to 36, the radio receiver being configured to receive the signal transmitted by the transmitter of the security container and to transmit the identifier and location information associated with the radio receiver to the central location.

38. A method of tracking the location of a security container, the method comprising receiving at a radio receiver a signal containing an identifier associated with the security container and transmitting the identifier and location information associated with the radio receiver to a central location.

39. A method according to claim 38 further comprising receiving location information from a positioning system receiver of the radio receiver.

40. A method according to claim 38 or claim 39 further comprising receiving location information from a positioning system receiver external to the radio receiver.

41. A method according to any one of claims 38 to 40 wherein transmitting the identifier and location information associated with the radio receiver to a central location is performed by a mobile telecommunications system transmitter of the radio receiver.

42. A method according to any one of claims 38 to 41 further comprising monitoring the strength of the signal transmitted by the transmitter of the security container and transmitting information relating to the strength of the signal to the central location with the location information associated with the radio receiver.

43. A method according to any one of claims 38 to 42 wherein one or more of the plurality of radio receivers is installed in a fixed location.

44. A method according to any one of claims 38 to 43 wherein one or more of the plurality of radio receivers is installed in a vehicle.

45. A security container for storing or transporting valuable items, the security container comprising a radio receiver for receiving radio signals from a radio transmitter external to the security container and a radio transmitter for transmitting data to a central location, wherein the radio receiver is configured to decode a radio signal received from a transmitter to retrieve an identifier associated with the transmitter and the radio transmitter is configured to transmit the retrieved identifier to the central location.

46. A security container according to claim 45 further comprising means for recording the date and time at which the radio signal was received by the security container, the security container being configured to transmit the date and time to the central location with the retrieved identifier.

47. A security container according to claim 45 or 46 further comprising means for recording the strength of the radio signal received from the external transmitter, the security

container being configured to transmit the received signal strength to the central location with the retrieved identifier.

48. A security container according to any one of claims 45 to 47 further comprising memory means for storing identifiers retrieved from signals received by the radio receiver transmitted by a plurality of transmitters external to the security container.

49. A security container according to claim 48 wherein the security container is configured to transmit the stored identifiers to the central location at a predetermined interval.

50. A security container according to any one of claims 45 to 49 further comprising a mobile telecommunications system transmitter for transmitting the retrieved identifier to the central location.

51. A method of announcing the location of a security container, the method comprising receiving at the security container a radio signal from a radio transmitter external to the security container, decoding the received radio signal to retrieve an identifier associated with the transmitter and transmitting the identifier to a central location.

52. A method according to claim 51 further comprising recording the date and time at which the radio signal was received by the security container and transmitting the date and time to the central location with the retrieved identifier.

53. A method according to claim 51 or claim 52 further comprising recording the strength of the radio signal received from the external radio transmitter and transmitting the received signal strength to the central location with the retrieved identifier.

54. A method according to any one of claims 51 to 53 further comprising storing identifiers retrieved from signals received by the radio receiver transmitted by a plurality of transmitters external to the security container.

55. A method according to claim 54 further comprising transmitting the stored identifiers to the central location at a predetermined interval.

56. A method according to any one of claims 51 to 55 wherein the retrieved identifier is transmitted to the central location by means of a mobile telecommunications system transmitter of the security container.

57. A security system for tracking the location of a security container, the security system comprising a security container according to any one of claims 45 to 50 and a plurality of radio transmitters which are each configured to transmit a signal containing an identifier associated with the radio transmitter.

58. A radio transmitter for use in the system of claim 57, the radio transmitter being configured to transmit a signal containing an identifier associated with the radio transmitter.

59. A mobile network for tracking the location of an object, the mobile network comprising a plurality of transceiver modules, each transceiver module having a radio receiver for receiving information relating to an object to be tracked and a transmitter for transmitting information relating to the object to be tracked, each transceiver module being mounted on a vehicle.

60. A security container substantially as hereinbefore described with reference to the accompanying drawings.

61. A method substantially as hereinbefore described with reference to the accompanying drawings.

62. A security system substantially as hereinbefore described with reference to the accompanying drawings.

Application No: GB0914196.1 **Examiner:** Richard Kerslake

Claims searched: 1-28 **Date of search:** 4 December 2009

Patents Act 1977: Search Report under Section 17

Documents considered to be relevant:

Category	Relevant to claims	Identity of document and passage or figure of particular relevance
X	1 & 15 at least	US5939982 A (GAGNON et al.) See abstract
X	1 & 15 at least	WO2006/091192 A2 (CONCHA et al.) See abstract & page 5, lines 13-26
X	1 & 15 at least	US2006/0261944 A1 (NG et al.) See abstract
X	1 & 15 at least	WO2004/102327 A2 (LAMBRIGHT et al.) See abstract
X	1 & 15 at least	WO2004/068160 A2 (NAGELI et al.) See abstract
X	1 & 15 at least	US2009/0135015 A1 (DOBSON et al.) See abstract

Categories:

X	Document indicating lack of novelty or inventive step	A	Document indicating technological background and/or state of the art.
Y	Document indicating lack of inventive step if combined with one or more other documents of same category.	P	Document published on or after the declared priority date but before the filing date of this invention.
&	Member of the same patent family	E	Patent document published on or after, but with priority date earlier than, the filing date of this application.

Field of Search:

Search of GB, EP, WO & US patent documents classified in the following areas of the UKC^{X} :

Worldwide search of patent documents classified in the following areas of the IPC

G01S; G06Q; G08B; G08G

The following online and other databases have been used in the preparation of this search report

EPODOC,WPI

International Classification:

Subclass	Subgroup	Valid From
G08B	0021/18	01/01/2006
G06Q	0010/00	01/01/2006
G08B	0013/24	01/01/2006

Application No: GB0914196.1 **Examiner:** Richard Kerslake

Claims searched: 29-44 **Date of search:** 18 May 2010

Patents Act 1977
Further Search Report under Section 17

Documents considered to be relevant:

Category	Relevant to claims	Identity of document and passage or figure of particular relevance
X	29-31,33,34,37-40,42 & 43 at least	US2009/0174546 A1 (LIAN et al.) See whole document
X	29,33,34,36-38,42 & 43 at least	US2006/0192709 A1 (SCHANTZ et al.) See whole document
X	29,33,34,37,38,42 & 43 at least	US2007/0132577 A1 (KOLAVENNU) See whole document
X	29,32,34,37,38,41, & 43 at least	US2004/0002347 A1 (HOCTOR et al.) See whole document
X	29,32,34,35,37,38, 43 & 44 at least	US2003/0235172 A1 (WOOD) See whole document
X	29,31,34,37,38,40 & 43 at least	US6977612 B1 (BENNETT) See whole document
X	38,40,41 & 43 at least	US2008/0061963 A1 (SCHNITZ et al.) See whole document
X	29,33,34,37,38,42 & 43 at least	US2005/0207381 A1 (ALJADEFF et al.) See whole document
X	38,40,41 & 43 at least	US2007/0262861 A1 (ANDERSON et al.) See whole document
X	38 & 40 at least	WO2004/068160 A2 (MIRAFIN et al.) See abstract

Categories:

X	Document indicating lack of novelty or inventive step	A	Document indicating technological background and/or state of the art.
Y	Document indicating lack of inventive step if combined with one or more other documents of same category.	P	Document published on or after the declared priority date but before the filing date of this invention.
&	Member of the same patent family	E	Patent document published on or after, but with priority date earlier than, the filing date of this application.

Field of Search:

Search of GB, EP, WO & US patent documents classified in the following areas of the UKC[X] :

Worldwide search of patent documents classified in the following areas of the IPC

G01S; G01V; G06Q; G08B; G08G

The following online and other databases have been used in the preparation of this search report

EPODOC,WPI

International Classification:

Subclass	Subgroup	Valid From
G08B	0021/18	01/01/2006
G01S	0005/00	01/01/2006
G01S	0005/14	01/01/2006
G06Q	0010/00	01/01/2006
G08B	0013/24	01/01/2006
G08B	0025/00	01/01/2006
G08B	0025/10	01/01/2006

Application No: GB0914196.1 **Examiner:** Richard Kerslake

Claims searched: 45-58 **Date of search:** 20 May 2010

Patents Act 1977
Further Search Report under Section 17

Documents considered to be relevant:

Category	Relevant to claims	Identity of document and passage or figure of particular relevance
X	45,48,49,51,54,55,57 & 58 at least	WO2007/028956 A1 (THOMAS) See whole document
X	45,47,48,51,53,54,57,58 at least	GB2277850 A (ANDERSON) See whole document

Categories:

X	Document indicating lack of novelty or inventive step	A	Document indicating technological background and/or state of the art.
Y	Document indicating lack of inventive step if combined with one or more other documents of same category.	P	Document published on or after the declared priority date but before the filing date of this invention.
&	Member of the same patent family	E	Patent document published on or after, but with priority date earlier than, the filing date of this application.

Field of Search:

Search of GB, EP, WO & US patent documents classified in the following areas of the UKC^{X} :

Worldwide search of patent documents classified in the following areas of the IPC

G01S; G01V; G06Q; G08B

The following online and other databases have been used in the preparation of this search report

EPODOC,WPI

International Classification:

Subclass	Subgroup	Valid From
G08B	0021/18	01/01/2006
G01S	0005/00	01/01/2006
G01S	0005/14	01/01/2006
G01S	0013/74	01/01/2006
G06Q	0010/00	01/01/2006
G08B	0013/24	01/01/2006
G08B	0025/00	01/01/2006

Subclass	Subgroup	Valid From
G08B	0025/10	01/01/2006

Application No:	GB0914196.1	**Examiner:**	Richard Kerslake
Claims searched:	59	**Date of search:**	21 May 2010

Patents Act 1977
Further Search Report under Section 17

Documents considered to be relevant:

Category	Relevant to claims	Identity of document and passage or figure of particular relevance
X	59	US6150961 A (ALEWINE et al.) See abstract
X	59	DE102007056354 A1 (WAGENHUBER et al.) See WPI abstract
X	59	EP1788749 A1 (OSAFUNE) See paragraph 20
X	59	US2007/0222665 A1 (KOENEMAN) See abstract
X	59	US6133687 A (EBERWINE et al.) See Column 1, line 37 - column 2, line 6
X	59	US7418343 B1 (MCGRAW et al.) See abstract
X	59	JP2008131308 A (MASUDA et al.) See EPO abstract
X	59	EP1975901 A1 (TOROK et al.) See abstract

Categories:

X	Document indicating lack of novelty or inventive step	A	Document indicating technological background and/or state of the art.
Y	Document indicating lack of inventive step if combined with one or more other documents of same category.	P	Document published on or after the declared priority date but before the filing date of this invention.
&	Member of the same patent family	E	Patent document published on or after, but with priority date earlier than, the filing date of this application.

Field of Search:

Search of GB, EP, WO & US patent documents classified in the following areas of the UKC^{X} :

Worldwide search of patent documents classified in the following areas of the IPC
The following online and other databases have been used in the preparation of this search report
EPODOC,WPI

International Classification:

Subclass	Subgroup	Valid From
G08B	0021/18	01/01/2006
G01S	0005/00	01/01/2006
G01S	0005/14	01/01/2006
G01S	0013/74	01/01/2006
G06Q	0010/00	01/01/2006
G08B	0013/24	01/01/2006
G08B	0025/00	01/01/2006
G08B	0025/10	01/01/2006