

Securing equipment of a person and associated system

The present invention relates to a personal security equipment unit for securing a person. The present invention also relates to an associated security system.

5 In the field of security, there are numerous personnel involved and they are required to make decisions rapidly and with very few information elements.

In fact, the cause of many of the incidents and accidents involving these personnel groups have to do with an inappropriate decision made by the personnel. For example, during a roadside check stop, routine behaviour is not appropriate if the car being checked is a stolen vehicle. In such a situation, the thief, sensing that they have been discovered, might retaliate with a violent reaction that could place the lives of the personnel performing the traffic check in danger.

It is therefore desirable to enhance the safety and security of the personnel involved in these checks.

15 For this purpose, it is a known practice to use body armour or bullet proof vests. A bulletproof vest is gear that is primarily designed to protect the chest, abdomen and the back against the shooting of firearms by absorbing the impact. The vests are manufactured with tightly woven fibres, mainly Kevlar. This type of vest can thus protect the person wearing it against projectiles shot from handguns and rifles, as well as shrapnel from certain explosive devices such as grenades.

However, although such equipment provides the ability to effectively protect personnel in the case of direct attack, such equipment is difficult to camouflage. As a result, for a mission involving stealthily following a target individual, the use of such equipment is ill-suited and leads, in certain circumstances to placing the personnel in danger.

25 There is therefore a need for personal securing equipment to secure a person that makes it possible to enhance the safety and security of personnel in all situations.

In order to do this, a personal security equipment unit for securing a person has been described. The security equipment comprises a wristband that is suitable to be wrapped around a wrist of a person, a box casing held by the wristband, the whole assembly of the box casing and the wristband being portable by the person. The box casing includes a receiver capable of receiving data, a processor capable of associating with each data item a given degree of dangerousness for the person, the processor being capable of sending the data to be communicated to the person and being capable of transmitting the data to be transmitted. The box casing also includes an interface capable of communicating to the person the data sent by the processor, and a transmitter capable

of transmitting the data transmitted by the processor. The security equipment unit is capable of operating in accordance with at least two modes of operation, in particular three modes of operation, with each mode of operation being associated in a one-to-one manner with a threshold degree of dangerousness, the data that the processor is capable to send in one mode of operation is the data associated with a degree of dangerousness that is greater than or equal to the threshold degree of dangerousness of the mode of operation considered.

According to some particular embodiments, the personal security equipment unit for securing a person includes one or more of the following characteristic features taken into consideration in isolation or in accordance with all technically possible combinations:

- the interface is capable of vibrating when the receiver receives data whereof the degree of dangerousness is greater than or equal to the threshold degree of dangerousness that is the highest of all the threshold degrees of dangerousness.

- the security equipment unit includes, in addition, a toggle switch button, the operation of the toggle switch button modifying the mode of operation of the security equipment unit.

- the security equipment unit comprises, in addition, an alert-alarm button, the activation of the alert-alarm button being a data item to be transmitted.

- the receiver is capable of receiving data originating from a global communication network and a local communication network, the local communication network grouping together the security equipment unit and at least one other security equipment unit such as previously described, the transmitter is capable of transmitting data over the global communication network and the local communication network, and the box casing includes in addition, an accessibility detector for detecting accessibility to the network, the detector being capable of detecting access to the global communication network, the receiver receiving the data coming from the local communications network and the transmitter transmitting the data over the local communication network when the detector detects that the global communication network is not accessible for the security equipment unit.

- the data are selected in the group including:

- + data originating from other equipment units belonging to the person;

- + data using the geographical position of the person;

- + data related to the geographical position of the person relative to the geographical position of the other equipment units; and

- + data related to the geographical position of the person relative to a geographic sectioning of an area.

- a maximal distance is defined between two security equipment units, one data item being that the other security equipment unit that is located closest is found at a distance greater than the maximal distance.

- the interface has a screen that is capable of displaying the data sent by the processor and a vibration unit that is capable of generating vibrations so as to communicate to the person, data sent by the processor.

A security system for securing a group of persons has also been described. The system includes, for each person, at least one security equipment unit such as previously described.

According to one particular embodiment, the security system comprises, in addition, a central server, each security equipment unit being capable of exchanging data with the central server via a global communication network and each security equipment unit being capable of exchanging data with another security equipment unit via a local communication network that groups together the security equipment units of the system.

Other characteristic features and advantages of the invention will become apparent upon the review of the description that follows of the embodiments of the invention, given only by way of example and with reference being made to the drawings, which are as follows:

- Figure 1, a schematic view of an example of a security system for securing a group of people, each person being equipped with a personal security equipment unit for securing a person;
- Figure 2, schematic view of a personal security equipment unit for securing a person as shown in figure 1; and
- Figure 3, a schematic view of a usage scenario for using the security system according to figure 1.

A security system 10 for securing group of persons is presented schematically in figure 1.

In the case of figure 1, the group of persons includes three police officers. In the remaining sections, the first police officer is denoted by P1, the second police officer is denoted by P2, and the third police officer is denoted by P3.

In this particular case, as indicated in the bracket in figure 1, the three police officers P1, P2 and P3 form a patrol team.

The system 10 is capable of enhancing the safety and security of the police officers P1, P2, and P3 over their area of intervention.

The system 10 includes a central server 12 and, for each of the police officers P1, P2 and P3, a set of equipment units 14.

The central server 12 is suitable for communicating with the set of equipment units 14.

The central server 12 is a server that is capable of collecting various security related data.

The collection of data is carried out by receiving of the information items originating from the databases or from dedicated equipment units such as cameras or the set of equipment units 14.

The data are, for example, data from video protection systems, amber alerts or abduction alerts, or official reports and recordings of thefts.

More generally, the data consist of all of the data related to the field of intervention and to the persons present over the field of intervention.

The data are to be collected either automatically or by manual entry by an operator.

The central server 12 is a remote server in relation to the patrol team and the field of intervention. This makes it possible to ensure that the central server 12 is in a secure location.

The central server 12 is capable of sending the data collected. The set of equipment units 14 varies according to the police officers P1, P2 and P3 considered.

The first police officer P1 is equipped with a security equipment unit 16 and a smart mobile handset 18. A smart mobile handset is more often referred to by the English term "smartphone".

The second police officer P2 is also equipped with a security equipment unit 16 and a smart mobile handset 18.

The third police officer P3 is equipped with a security equipment unit 16, a smart mobile handset 18, and a vehicle 19.

In this illustrated example, it is assumed, for the sake of simplification that the security equipment unit 16 is the same for each of the police officers P1, P2 and P3, in a manner such that, for example, the only difference between the security equipment unit 16 of the first police officer P1 and the security equipment unit 16 of the second police officer P2 is the name of the officer who has been equipped with the security equipment unit 16.

In similar fashion, it is assumed for the sake of simplification, that the smart mobile handset 18 is the same for each of the police officers P1, P2 and P3.

A security equipment unit 16 is illustrated more specifically in figure 2.

By way of an example, the security equipment unit 16 is the security equipment unit of the first police officer P1.

The security equipment unit 16 is a personal security equipment unit for securing of a person. Such an equipment unit provides the ability to enhance the security of the person who is equipped with the security equipment unit 16.

The security equipment unit 16 usually works in collaboration with the smartphone 18.

However, by way of a variant, the security equipment unit 16 is capable of functioning in the absence of the smartphone 18. This is in particular the case when the security equipment unit 16 includes the members for communicating via wi-fi or 3G/4G.

The security equipment unit 16 includes a wristband 20 and a box casing 22.

The wristband 20 is suitable to be wrapped or worn around a wrist of a person.

For example, the wristband 20 is made of a material that is flexible enough to adhere to the shape of the wrist.

According to the particular example illustrated in figure 2, the wristband 20 comprises two parts 24 and 26 that are attachable to one another by a tie not represented in the figure.

According to the example in figure 2, the two parts 24 and 26 are bands having an identical width.

The box casing 22 is held by the wristband 20.

In this case, each part 24 and 26 is connected to a part of the box casing 22 in a manner such as to ensure that each part 24 and 26 is positioned to face the other.

The box casing 22 has a cylindrical shaped form with a base of any type.

The term "a cylindrical form", is understood to indicate that the box casing 22 has the shape of a solid bounded by two parallel planes and by the base.

According to the example in figure 2, the base of the box casing 22 is rectangular. In this case, the box casing 22 has a parallelepiped shaped form.

By way of a variant, the base of the box casing 22 is a disc.

The box casing 22 is capable of vibrating.

The box casing 22 includes a receiver 28, a transmitter 30, a processor 32, an interface 34, a toggle switch button 36, an alarm button 38 and a detector 40.

By way of a variant, the box casing 22 includes other members.

Among these members, mention may be made of a start and stop button, a camera, a microphone, a speaker, or a heart rate sensor.

The box casing 22 also includes one or more of the aforementioned members.

The receiver 28 is capable of receiving data.

In the context of the receiving of data, such data may be qualified as "notifications".

According to the example in figure 2, the receiver 28 is an antenna.

The receiver 28 is capable of receiving data originating from a global communication network. The global network is denoted as R1 in the following sections.

The global network R1 is a network that provides the means for linking by communication the central server 12 and the entire set of equipment units 14 of each of the police officers P1, P2 and P3.

To put it another way, each the security equipment unit 16 is capable of exchanging data with the central server 12 over the global network R1.

The global network R1 is a wireless network.

For example, the global network R1 is a "wi-fi" network. The term "wi-fi network" is understood to signify that the network used is in compliance with a set of standards pertaining to wireless networks that have been developed by the Working Group 11 of the Institute of Electrical and Electronics Engineers - IEEE (IEEE 802) LAN/MAN [Local Area Network/Metropolitan Area Network] Standards Committee.

According to another example, the global network R1 is a 3G network. By way of illustration the global network R1 conforms to the standards, UMTS or CDMA 2000.

UMTS (abbreviation for the term "Universal Mobile Telecommunications System") is a standard that defines a cellphone technology whose radio part is based on a technique known as spread spectrum (the multiple access technology of W-CDMA, abbreviation for "Wideband Code Division Multiple Access" which means "multiplexing by wideband code").

The CDMA standard (abbreviation for "Code division multiple access") defines a communication technology using a system of coding of transmissions, using the technology of spread spectrum. Such technology allows several digital links to simultaneously use the same carrier frequency.

According to another example, the global network R1 is a 4G type network.

The receiver 28 is also capable of receiving data originating from a local communication network.

The local communication network is denoted as local network R2 in the following sections of this description.

The local network R2 groups together the security equipment unit 16 and at least one other security equipment unit 16.

The local network R2 groups together the three security equipment units 16 in the case of figure 1.

To put it another way, each security equipment unit 16 is capable of exchanging data with another security equipment unit 16 on the local network R2.

For example, the local network R2 is an ad - hoc network.

According to a particular case, the local network R2 is a wi-fi network whether or not secure.

The transmitter 30 is capable of transmitting data.

5 According to the example represented in figure 2, the transmitter 30 is a separate and distinct antenna from the receiver 28.

By way of a variant, the receiver 28 and the transmitter 30 are combined.

The transmitter 30 is capable of transmitting data over the global network R1.

The transmitter 30 is also capable of transmitting data over the local network R2.

10 The processor 32 plays the role of a controller of the elements of the box casing 22.

The processor 32 is, for example, a programmable logic circuit.

A programmable logic circuit, or programmable logic network, is an integrated logic circuit that may be reprogrammed after its manufacture. Such a programmable logic
15 circuit is composed of a number of elementary logic cells and freely connectable logic toggles. This type of electronic component is commonly referred to by various different English initialisms including in particular FPGA (abbreviation for "field-programmable gate array"), PLD (abbreviation for "programmable logic device"), EPLD (abbreviation for "erasable programmable logic device"), CPLD (abbreviation for "complex programmable
20 logic device"), PAL (abbreviation for "programmable array logic") or PLA (abbreviation for "programmable logic array").

By way of a variant, the processor 32 is a calculator.

According to another variant, the processor 32 is a computer processor that is capable of deploying computer program products.

25 More precisely, the processor 32 is capable of associating with each data item a degree of dangerousness for the person who is equipped with the security equipment unit 16.

For example, the processor 32 includes a memory storage that records and stores a database giving for each type of information a degree of dangerousness.

30 By way of illustrative example, if the data is the presence of a threat in the environment of the first police officer P1, the degree of dangerousness is high. The presence of a person known to the police services is an example of a threat.

The expression of the degree of dangerousness depends on the context.

35 By way of an example, although not realistic, the degree of dangerousness is binary, in such manner that the data are processed according to whether they are considered dangerous or not.

In a more complex treatment process, the degree of dangerousness includes several stages, for example, a number from 1 to 7. In such a case, by way of explanation, a degree of dangerousness of 1 corresponds to a data item relative to a neutral information item (a map for example) while a degree of dangerousness of 7 corresponds to a data item relative to an information item that is vital to the first police officer P1.

Other examples are detailed in the following sections of the description with reference to examples of use of the system 10.

The processor 32 is capable of sending the data to be communicated.

The processor 32 sends the data to be communicate to the interface 34.

The processor 32 is capable of transmitting the data to be transmitted.

The processor 32 sends the data to be transmitted to the transmitter 30.

The processor 32 is capable of controlling the receiver 28 and the transmitter 30.

In particular, when the processor 32 receives a signal from the detector 40 indicating that global network R1 is not accessible for the equipment unit 16, the processor 32 is capable of controlling the receiver 28 in order for the receiver 28 to only receive the data originating from the local network R2.

Similarly and possibly jointly, when the processor 32 receives a signal originating from the detector 40 indicating that global network R1 is not accessible to the equipment unit 16, the processor 32 is capable of controlling the transmitter 30 in order for the transmitter 30 to only transmit the data over the local network R2.

The processor 32 is also capable of controlling the operation of the security equipment unit 16.

The security equipment unit 16 is also capable of operating according to at least two modes of operation, with each mode of operation being associated in a one-to-one manner with a threshold degree of dangerousness, the data that the processor 32 is capable of sending in one mode of operation being the data associated with a degree of dangerousness that is greater than or equal to the threshold degree of dangerousness of the considered mode of operation.

The threshold degree of dangerousness is configurable by the user of the security equipment unit 16.

A convenient way to set the threshold degree of dangerousness for each mode of operation M1, M2 and M3 is that the user specifies what data they wish to know and this, according to the mode of operation M1, M2 and M3.

In this sense, the degree of dangerousness is understood to be a degree of dangerousness perceived by the user of the security equipment unit 16 and not a degree of objective danger for the user of the security equipment unit 16.

This amounts to saying that the degree of dangerousness is a means of classifying the processing treatment (in this case the display) of the data arriving at the processor 32.

By way of illustration, in the particular case represented in figure 2, the security equipment unit 16 is capable of functioning according to three modes of operation M1, M2 and M3.

For the remainder of the description, the first threshold degree of dangerousness associated with the first mode of operation M1 shall be denoted as DDS1, the second threshold degree of dangerousness associated with the second mode of operation M2 shall be denoted as DDS2 and the third threshold degree of dangerousness associated with the third mode of operation M3 shall be denoted as DDS3.

In addition, it is assumed that the first threshold degree of dangerousness DDS1 is strictly greater than the second threshold degree of dangerousness DDS2 and that the second threshold degree of dangerousness DDS2 is strictly greater than the third threshold degree of dangerousness DDS3.

Also, in the first mode of operation M1, the security equipment unit 16 displays less data than in the second mode of operation M2.

Similarly, in the second mode of operation M2, the security equipment unit 16 displays less data than in the third mode of operation M3.

According to a specific embodiment, in the first mode of operation M1, the data sent by the processor 32 are an SOS sent by another police officer P1, P2 and P3, the data relating to the restriction of a zone (for example, a zone being monitored by the police and in which it is not desired to see police officers in uniform) and the data related to a wanted person.

In the second mode of operation M2, the data sent include the data sent in the first mode of operation M1 and other data. The other data include the data related to a physical assault on a person in the proximity. The notion of proximity is defined by the user depending on the mission at hand. The other data also include data relating to a vehicle that has been reported and flagged. A reported vehicle is for example, a vehicle that has been stolen or monitored by a system of automatic reading of license plates. The other data also include the data relating to the proximity of firearms or explosives. Other data also include historical information on the area in question. For example, the data are data related to the occurrence of violent episodes in a given period of time, for example four weeks.

In the third mode of operation M3 the data sent include the data sent in the second mode of operation M2 and other information items. The other information is related to the

particular zone of the area of intervention: is the zone polluted? Is the zone a demonstration or protest zone? Where's the crowd? Are there traffic jams?

By way of a variant, the distribution of the data is different, and other data are may possibly be sent by the processor 32.

5 In addition, each mode of operation M1, M2, M3 is characterized by a specific colour.

Similarly, by way of an variant or in addition, each mode of operation M1, M2, M3 is characterized by a specific logo.

10 The interface 34 is capable of communicating to the police officer P1, P2, P3 the data sent by the processor 32.

The interface 34 has a vibration unit and a screen. Only the screen is visible in the figures.

The screen is capable of displaying the data sent by the processor 32.

The displayed data are messages, photos or images.

15 In the particular case represented, the screen has reduced dimensions.

For example, the surface area of the screen on which the data are displayed is less than or equal to 15 cm², in particular less than or equal to 11 cm².

20 Because of the size of the screen, when the data to be displayed are too large relative to the size of the screen, only a part of the data is displayed on the screen. To access all of the data, the police officer P1, P2 and P3 uses their smartphone 18 that is in communication with the security equipment unit 16.

According to one particular embodiment, the interface 34 is also an interface to enter information by the police officer P1, P2 and P3.

25 This also enables the police officer P1, P2 and P3 to interact with the interface 34, for example, to say that he will join another police officer P1, P2 and P3.

The vibration unit is capable of causing the vibrating of the box casing 22.

30 In particular, when the receiver 28 receives data in which respect the degree of dangerousness is greater than or equal to the threshold degree of dangerousness DDS1 which is the highest of all the threshold degrees of dangerousness DDS1, DDS2, and DDS3, the processor 32 causes the vibrating of the vibration unit.

The vibration unit is capable of generating different types of vibrations.

By way of an illustration, when the officer receives an SOS alarm, the vibration unit vibrates in a manner so as to transmit the letters S - O - S in 'vibrated morse code', which is 3 short vibrations followed by 3 long vibrations and then 3 short vibrations.

35 In certain modes of operation, the data sent are displayed or vibrated on an exclusive basis.

In other modes of operation, some data sent are both displayed by the screen and "vibrated" by making use of the vibration unit.

The toggle switch button 36 is, according to the example shown in figure 2, a push button.

5 By way of a variant, the toggle switch button 36 is a tactile or touch operated zone of the screen.

The operation of the toggle switch button 36 changes the mode of operation of the security equipment unit 16.

10 For example, a single press of the button serves to switch into the first mode of operation M1, pressing twice serves to switch into the second mode of operation M2, and the prolonged pressing serves to switch into the third mode of operation M3.

15 By way of a variant, a single press of the toggle switch button 36 serves to switch to the next mode. Indeed, when the equipment unit is in the first mode of operation M1, a single press of the button serves to switch into the second mode of operation M2; when the equipment unit is in the second mode of operation M2, a single press of the button serves to switch into the third mode M3, and when the equipment is in the third mode of operation M3, a single press of the button serves to switch into the first mode of operation M1.

20 The alert-alarm button 38 is, according to the example shown in figure 2, a push button.

By way of a variant, the alert-alarm button 38 is a tactile or touch operated zone of the screen.

In both these two cases, it is the double clicks that are detected to avoid false alert alarms in the event of an accidental single click.

25 The operating of the alert-alarm button 38 is a data item to be sent.

In a particular embodiment, the alert-alarm button 38 causes the changing of the status of the police officer P1, P2, P3. A police officer P1, P2 or P3 who has operated the 38 alert-alarm button will appear on a map represented by a red dot.

The detector 40 is a detector of accessibility to the network.

30 More specifically the detector 40 is capable of detecting the accessibility to the global network R1.

According to one particular embodiment, the detector 40 is part of the processor 32. The detector 40 is capable of analyzing the noise on the receiver 28 and of choosing the relevant type of communication via the global network R1 or the local network R2.

35 It is to be noted that the detector 40 is capable of promoting the use of the global network R1 in order to ensure the proper update of the processor 32.

The detector 40 transmits a signal to the processor 32. The signal transmitted is a signal that indicates that the global network R1 is not accessible to the equipment 16.

In a particular embodiment, the signal is a binary signal, a '0' indicating that the global network R1 is not accessible while a '1' indicates that the global network R1 is accessible.

The assembly of the box casing 22 and the wristband 20 are portable by the person. The use of this expression is understood to include the wristband 20 and all of the elements of the box casing 22.

For example, the weight of the assembly comprising the box casing 22 and the wristband 20 is less than 100 grams, for example less than 70 grams.

Similarly, the total overall dimension of the assembly comprising the box casing 22 and the wristband 20 is less than 40 cm³.

The functioning of the system 10 is now described in reference to several usage scenarios.

According to one example shown in figure 3, the three police officers P1, P2 and P3 are to apprehend a suspect S in a spatial zone 100. Hereinafter, it is also assumed that the suspect S has an accomplice C.

In this particular case, the three police officers P1, P2 and P3 are in plainclothes so as to avoid attracting attention.

The spatial zone 100 has four streets, 102, 104, 106 and 108 that cross each other at an intersection.

In the example provided, the spatial zone 100 is divided according to a divisional layout into seven zones: a first zone Z1, a second zone Z2, a third zone Z3, a fourth Z4, a fifth zone Z5, a sixth zone Z6 and a seventh zone Z7.

The first zone Z1 is bounded on the one hand by the first street 102 and on the other hand by a first barrier 112. Each barrier is represented by a dotted line in figure 3 and is presented in the form of a half straight line that originates at the intersection.

The second zone Z2 is bounded on the one hand by the first barrier 112 and on the other hand by the second street 104. The third zone Z3 is bounded on the one hand by the second street 104 and on the other by a second barrier 114. The fourth zone Z4 is bounded on the one hand by the second barrier 114 and by a third barrier 116. The fifth zone Z5 is bounded on the one hand by the third barrier 116 and on the other hand by the third street 106. The sixth zone Z6 is bounded on the one hand by the third street 106 and on the other hand by the fourth street 108. The seventh zone Z7 is bounded on the one hand by the fourth street 108 and on the other hand by the first street 102.

In the case illustrated, the first police officer P1 and the accomplice C are in the first zone Z1, the second police officer P2 is in the third zone Z3 and the third police officer P3 and the suspect S are in the fourth zone Z4.

For example, according to one scenario, it is assumed that the first police officer P1 identifies the accomplice C.

The first police officer P1 presses the alert-alarm button 38 of the security equipment unit 16 twice.

In this case, it is assumed that it had been agreed that pressing twice on the alert-alarm button 38 is a sign that the accomplice C has been seen.

In one such scenario, the transmitter 30 of the security equipment unit 16 transmits a data item relative to the fact that the accomplice C has been seen via the global network R1.

The central server 12 is also capable of geolocating the first police officer P1, for example, by means of a triangulation of the signal of the smartphone 18 of the first police officer P1.

The central server 12 then transmits the information items relating to the presence of the accomplice C in the first zone Z1. Such information is supposed to be a data item in respect whereof the degree of dangerousness is between the first threshold degree of dangerousness DDS1 and the second threshold degree of dangerousness DDS2.

It is assumed that the security equipment unit 16 of the second police officer P2 is in the second mode of operation M2.

The second police officer P2 is then alerted of the presence of the accomplice C in the first zone Z1 and can come so as to provide backup to the first police officer P1 or choose to modify his own position based on his intuition.

It is assumed that the security equipment unit 16 of the third police officer P3 is in the first mode of operation M1. The third police officer P3 being close to the suspect S and seeking to verify that it is indeed the latter only wants the most important data for his safety and security. In the first mode of operation M1, the third police officer P3 has not been alerted of the presence of the accomplice C in the first zone Z1.

In such a scenario, the security system 10 has made it possible to improve the level of information to be provided to the second police officer P2 without placing the third police officer P3 in danger.

According to another scenario, it is assumed that the third police officer P3 identifies the suspect S but is able to pick up only the local network R2.

The third police officer P3 presses once on the alert-alarm button 38 of the security equipment unit 16.

In this case, it is assumed that it had been agreed that pressing only once on the alert-alarm button 38 is a sign that the suspect S has been seen.

In such a scenario, the transmitter 30 of the security equipment unit 16 transmits a data item relative to the fact that the suspect S has been seen through the local network R2 (no connection to the global network R1).

The two police officers P1 and P2 both receive information that is then transmitted to the global network R1 since the first and the second police officers P1 and P2 have access to the global network R1.

The central server 12 is capable of geolocating the third police officer P3, for example, by means of a triangulation of the signal of the smartphone 18 of the third police officer P3.

The central server 12 then transmits the information items relating to the presence of the suspect S in the fourth zone Z4. Such information is supposed to be a data item in respect whereof the degree of dangerousness is greater than the first threshold degree of dangerousness DDS1.

In such a situation, the two police officers P1 and P2 are informed rapidly of the location where the suspect S may be found. From the point of view of the third police officer P3, this information is transmitted discreetly by pressing on the alert-alarm button 38. His security is enhanced due to the fact that his cover has not been compromised and that back-up (the first and the second police officers P1 and P2) will arrive quickly.

In the scenarios illustrated, use has been made of the data using the geographical position of the person concerned or of the data related to the operation of an alert-alarm button.

Other scenarios may also possibly be envisaged.

For example, the second police officer P2 may have a serious fall. Activation of the alert-alarm button 38, in particular by a double click, coupled with the geolocating of the officer makes it possible to save him quickly.

According to another example, the third police officer P3 is in his vehicle 19 and the vehicle 19 is equipped with a license plate recognition device for recognising car license registration plates. In the event that it recognises a stolen car license plate, it is possible to alert the other police officers P1 and P2.

By way of a variant, it is supposed that, for security related reasons, a maximal distance is defined between two police officers P1, P2 and P3. The system 10 provides the ability to detect that one police officer, for example the third police officer P3, has strayed away too far from the other police officers P1 and P2, and to alert him thereto. In

this case, a data item that is exchanged is the other security equipment unit 16 which is closest is located at a distance that is greater than the maximal distance.

According to another scenario, if passing through the fifth zone Z5 is prohibited, the system 10 provides the ability to discreetly alert the third police officer P3 of his proximity to such a “passage-prohibited” zone.

According to another scenario, the police officer P1, P2, P3 can take a picture of his environment in a discreet manner in order to share information about the situation on the ground with the central server 12, and with the other police officers P1, P2, P3. In this case, the box casing 22 includes a photo apparatus or a camera.

According to another scenario, the police officer P1, P2, P3 can make a recording of the ambient sound in a discreet manner in order to share information about the situation on the ground with the central server 12, and with the other police officers P1, P2, P3. In this case, the box casing 22 includes a microphone. In these different scenarios, it appears that the security system 10 makes it possible, thanks to the use of the security equipment unit 16 to improve the flow of data amongst a patrol team of three police officers P1, P2 and P3 with a good degree of discretion.

The result thereof is increased safety and security for each of the three police officers P1, P2 and P3.

In other words, the security system 10 ensures the protection of the police officers P1, P2 and P3, the through provision of information that is appropriate and provided at the right moment.

In fact, the security equipment unit 16 is connected to a central server 12 that centralizes the data and subsequently effectively feeds back the relevant data to the persons who are equipped with the security equipment unit 16. A synchronization is generated between each security equipment unit 16 and the central server 12.

This makes it possible to develop the “sixth sense” of the police officers P1, P2 and P3.

The security system 10 also provides the ability to decrease the period of transmission latency between the messages.

The security system 10 offers the possibility to function in local mode with the other members of the patrol team to which the user of the security equipment unit 16 belongs.

The security equipment unit 16 is indeed well suited for use on the move and in situations of attempting to apprehend a suspect S. More generally, the use thereof is compatible with missions in the field on account of the discretion and freedom to act afforded to the police officers P1, P2 and P3. In some modes of operation, the security

equipment unit 16 informs the officer P1, P2 or P3 by means of a simple vibration of the box casing 22.

In addition, the security system 10 makes it possible to ensure that the information and data given to the police officer P1, P2 or P3 are always updated given the linkage through a central server 12 with remote connection on each interface 34 provided that the overall network R1 is accessible.

In a general manner, in each scenario, the police officer P1, P2 or P3 has access to the data pertaining to a global view of the situation, the geolocation of the persons similarly equipped, the individuals who are part of a patrol unit, the presence of crowded zones, dangerous zones, zones having protest demonstrations or events, and information on the evolution of the current mission in progress, or bio-data.

The bio-data are the data related to the health of the police officer P1, P2 or P3. For example, the heart rate of the police officers P1, P2 or P3 are recorded.

Facilitating access to this information makes it possible to respond appropriately to the needs of the police officers P1, P2 and P3 encountered in concrete situations. Among these different situations, mention may be made of the need of help and support to a partner or teammate, the isolation of a police officer, the discrete taking of pictures, or discreet listening.

In order to further enhance the security of the officers P1, P2 and P3, the security equipment unit 16 has the appearance of an ordinary or trivial object.

For example, the security equipment unit 16 forms a watch, the box casing being in this case a watch dial 22.

In addition, one of the advantages of the security system 10 is its ability to be reconfigured.

In fact, it is possible to integrate new equipment units with ease by means of a change of the processor 32 and the central server 12.

Thus, the security system 10 has the capacity and ability to easily enhance its alert capabilities in keeping with technological evolution.

The security equipment unit 16 is applicable to any person having a need for protection and discretion.

By way of illustration, the person is part of a private or public security force.

According to another example, the person is part of emergency services teams, such as firemen.

According to still another example, the person is a celebrity.

Other embodiments may also possibly be envisaged.

In particular, in order to improve management of information recording by the police officer P1, P2 or P3, several types of display are used.

For example, a first display option is a map type display.

In one such embodiment, a map is displayed and the data are represented on the map.

For example, the data are displayed in the form of a disc having a specific colour and/or of pictograms.

By way of illustration, the directional orientation of a police officer P1, P2 or P3 is illustrated by arrows.

Additional data are also viewable such as a distance related data item allowing the police officer P1, P2 or P3 to better understand and assess the situation.

According to one embodiment, the map is displayed in a manner such that the centre of the screen corresponds to the current position of the police officer P1 who is equipped with the security equipment unit 16.

By way of a variant, the police officer P1 can interact with the map, in particular in order to enlarge (zoom in) a zone or to reduce it (zoom out) according to his needs.

A second display option is a display view that provides the ability to determine the members of the patrol team for the mission to be carried out along with their status.

For example, an interface display with nine faces is shown, the nine faces being those of the members of the patrol.

According to one embodiment, a face highlighted by a first colour indicates that the person is not participating in the mission. A face highlighted by a second colour indicates that the person is in danger.

In addition, a face framed by a first colour indicates that the person is available. A face framed by a second colour indicates that the person is in the process of going to the rescue of another person in danger.

A third display option is a display view that has been "camouflaged".

The passage from one display view to the other is effected by means of an on-screen sliding action.

Over these views, it is possible to superpose displays of messages that make it possible to interact with the police officer P1, P2 or P3.

An example of interaction consists of obtaining an information item from the officer P1, P2 or P3.

An example of a message is a need for assistance with two responses possible "no" or "I'm going there". Such a message follows a request for assistance originating from another member of the patrol unit.

Another example of interaction consists of informing the police officer P1 P2 or P3.

As an illustration, if the police officer enters into a polluted zone, the central server communicates a message of the type "entry into the prohibited zone".

5 In addition, according to one variant in some modes of operation M1, M2 or M3, the time period of display on screen of the data is limited in order to avoid compromising the position of police officer P1, P2 or P3.

In one embodiment, the mode of operation M1, M2 or M3 is considered to be a data item to be communicated to the person.

10 For example, a dedicated pictogram is displayed when a mode of operation M1, M2 or M3 is selected.

Other embodiments of the invention are obtained by combining the preceding embodiments when these embodiments are technically compatible.

19
CLAIMS

1.- A personal security equipment unit (16) for securing a person (P1, P2, P3), the security equipment unit (16) comprising:

5 - a wristband (20) that is suitable to be wrapped around a wrist of a person (P1, P2, P3).

 - a box casing (22) held by the wristband (20), the whole assembly of the box casing (22) and the wristband (20) being portable by the person (P1, P2, P3), the box casing (22) including:

10 - a receiver (28) capable of receiving data;

 - a processor (32) capable of associating with each data item a given degree of dangerousness for the person (P1, P2, P3), the processor (32) being capable of sending the data to be communicated to the person (P1, P2, P3) and being capable of transmitting the data to be transmitted;

15 - an interface (34) capable of communicating to the person (P1, P2, P3) the data sent by the processor (32); and

 - a transmitter (30) capable of transmitting the data transmitted by the processor (32);

20 the security equipment unit (16) being capable of operating in accordance with at least two modes of operation, in particular three modes of operation (M1, M2, M3), with each mode of operation (M1, M2, M3) being associated in a one-to-one manner with a threshold degree of dangerousness (DDS1, DDS2, DDS3), the data that the processor (32) is capable to send in one mode of operation (M1, M2, M3) being the data associated with a degree of dangerousness that is greater than or equal to the threshold degree of dangerousness (DDS1, DDS2, DDS3) of the mode of operation (M1, M2, M3) considered.

30 2.- A security equipment unit according to claim 1, in which the interface (34) is capable of vibrating when the receiver (28) receives data whereof the degree of dangerousness is greater than or equal to the threshold degree of dangerousness that is the highest (DDS1) of all the threshold degrees of dangerousness (DDS1, DDS2, DDS3).

35 3.- A security equipment unit according to claim 1 or 2, in which the security equipment unit (16) includes, in addition, a toggle switch button (36), the operation of the toggle switch button (36) modifying the mode of operation (M1, M2, M3) of the security equipment unit (16).

4.- A security equipment unit according to any one of claims 1 to 3, in which the security equipment unit (16) comprises, in addition, an alert-alarm button (38), the activation of the alert-alarm button (38) being a data item to be transmitted.

5.- A security equipment unit according to any one of claims 1 to 4, in which:

- the receiver (28) is capable of receiving data originating from a global communication network (R1) and a local communication network (R2), the local communication network (R2) grouping together the security equipment unit (16) and at least one other security equipment unit (16) according to any one of claims 1 to 4;

- the transmitter (30) is capable of transmitting data over the global communication network (R1) and the local communication network (R2), and

- the box casing (22) includes, in addition, an accessibility detector (40) for detecting accessibility to the network, the detector (40) being capable of detecting access to the global communication network (R1), the receiver (28) receiving the data coming from the local communication network (R2) and the transmitter (30) transmitting data over the local communication network (R2) when the detector (40) detects that the global communication network (R1) is not accessible for the security equipment unit (16).

6.- A security equipment unit according to any one of claims 1 to 5, in which the data are selected in the group including:

- data originating from other equipment units (14) belonging to the person (P1, P2, P3);

- data using the geographical position of the person (P1, P2, P3);

- data related to the geographical position of the person (P1, P2, P3) relative to the geographical position of the other equipment units (14), and

- data related to the geographical position of the person (P1, P2, P3) relative to a geographic sectioning of an area.

7.- A security equipment unit according to any one of claims 1 to 6, in which a maximal distance is defined between two security equipment units (16), one data item being that the other security equipment unit (16) that is located closest is found at a distance greater than the maximal distance.

8. - A security equipment unit according to any one of claims 1 to 7, in which the interface 34 has a screen that is capable of displaying the data sent by the processor (32)

and a vibration unit that is capable of generating vibrations so as to communicate to the person (P1, P2, P3), data sent by the processor (32).

5 9.- A security system (10) for securing a group of persons (P1, P2, P3), the system including, for each person (P1, P2, P3), at least one security equipment unit (16) according to any one of claims 1 to 8.

10 10.- A security system (10) according to claim 9, the security system (10) comprising, in addition, a central server (12), each security equipment unit (16) being capable of exchanging data with the central server (12) via a global communication network (R1) and each security equipment unit (16) being capable of exchanging data with another security equipment unit (16) via a local communication network (R2) that groups together the security equipment units (16) of the system (10).