

(19) World Intellectual Property Organization  
International Bureau



(43) International Publication Date  
27 November 2008 (27.11.2008)

PCT

(10) International Publication Number  
**WO 2008/144103 A1**

(51) International Patent Classification:

H04M 11/04 (2006.01)

(21) International Application Number:

PCT/US2008/057458

(22) International Filing Date: 19 March 2008 (19.03.2008)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:

11/749,572 16 May 2007 (16.05.2007) US

(71) Applicant (for all designated States except US): **AZOS AI, LLC** [US/US]; P.O. Box 526, Gainesville, VA 20156 (US).

(72) Inventor; and

(75) Inventor/Applicant (for US only): **BURGESS, Shelia, Jean** [US/US]; 5627 Tournament Drive, Haymarket, VA 20169 (US).

(74) Agent: **PARISI, Joseph, A.**; Nixon Peabody LLP, 401 9th Street, N.W., Suite 900, Washington, DC 20004 (US).

(81) Designated States (unless otherwise indicated, for every kind of national protection available): AE, AG, AL, AM,

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

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

Declaration under Rule 4.17:

— as to applicant's entitlement to apply for and be granted a patent (Rule 4.17(ii))

[Continued on next page]

(54) Title: COMMUNICATIONS CONTROLLER AND PROTOCOL

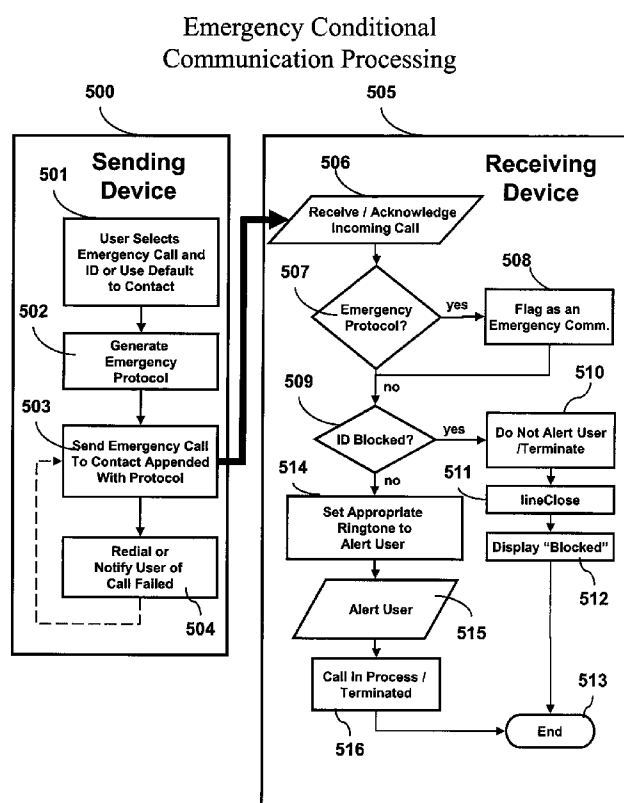


Figure 5

(57) Abstract: A communications controller and protocol are provided for empowering the user of a communications device, such as a telephone or other device, to assume intelligent control of communications. The communications controller provides conditional processing of incoming communication from a plurality of conditions comprising at least an emergency condition and a normal condition. Each caller is identified by unique originating source criteria associated with an incoming communication type. The user of the device may select to block callers based on their identification and the conditional type of the communication. The user also selects if the device is put into a unique mode where only emergency communication can alert the user. While in this mode "normal" communication will not alert the user of the communications device. Sensor data such as location of the sending device may be provided to the receiving party.



---

**Published:**

— *with international search report*

## COMMUNICATIONS CONTROLLER AND PROTOCOL

### SPECIFIC DATA RELATED TO THE INVENTION

[001] This application claims the benefit of U.S. application number 11/749,572 filed May 16, 2007.

### BACKGROUND OF THE INVENTION

[002] This invention relates in general to apparatus and methodology for controlling communications devices. More particularly, the invention relates to apparatus and methodology for intelligent conditional control incoming communications supplied to a communications device such as a mobile phone in one example.

[003] Today's consumer is being constantly bombarded and sometimes harassed by an ever-increasing volume of untimely and unwanted incoming communication (e.g., phone calls and messages (e.g., emails, Short Message Service (SMS) text messages, Instant Messages (IMs), etc.). Fundamentally, some incoming communication is not desired at all while others are extremely urgent and important as in the case of receiving an emergency communication from a loved one that needs your help immediately and that might be in a panic situation! The party receiving an *emergency* communication needs a way of distinguishing these communications to respond immediately. Right now, all communication whether it is a normal call or an emergency all ring the receiving communication device the same way—a special alert is needed to let the receiving party know the condition of the incoming communication.

[004] It is very desirable to provide users with smart communication solutions with the capability of distinguishing the criticality of incoming communication—to know that they should not just let the call go to voicemail, but take the call immediately, especially in an emergency situation. This situational awareness or conditional communication is needed to stay connected to loved ones when seconds count. The world in which we live is dangerous filled with natural and manmade disasters, even our schools are unsafe. We cannot predict when and where we will be when either we have an emergency situation and need help immediately or when someone else desperately needs us.

[005] There exists a need for enterprise-to-person and person-to-person intelligent emergency communications using conditional processing. Not all emergencies are suited for calling 911 especially when they are an emergency of a personal nature. One conventional approach to this problem is the combined telephone/answering machine which permits the user to listen to the caller and then make a real time decision as to whether or not to pick up the telephone receiver and engage the caller. This is referred to as "call screening" in its most basic form. Of course, the user also has the option of listening to the caller's message at a later time and then making a decision as to whether or not to call back. This response could be very untimely in a critical situation. Also, this approach would not be effective if the receiving party is in an environment that requires their attention (e.g., in a meeting, theater, etc. where they are required to turn their cell phones "off") so they will most likely let their answering service take the call. Having a device mode that only lets emergency communication alert the user would be helpful in these environments/situations so the user can "stay available" in case of an emergency.

[006] It would also be helpful for the receiving party to know the location of the caller in case there is a situation that the caller cannot talk, their location can be pinpointed and they can get help immediately.

[007] All communication is received the same way. Some messages are sent out by the Government to mobile devices such as the Amber Alerts. However, these messages are also received as just another incoming communication and do not use any special logic or processing to distinguish the communication from any other.

#### SUMMARY OF THE INVENTION

[008] Accordingly, one object of the present invention is to provide a method and apparatus for limiting a communications device user's exposure to undesired communications by employing advanced control mechanisms implemented in or near the communications device.

[009] Another object of the invention is to provide communications device control methodology and apparatus which permit the consumer to proactively take control of how, when, and if the customer responds to incoming communications.

[0010] Yet another object of the invention is to provide a methodology and apparatus for transforming a communications device (e.g., telephone, mobile device, computer, gateway/server, internet device, and/or television) from a passive device to a controllable device that incorporates individual conditional management values and customized consumer priorities.

[010] Yet another object of the invention is to provide communications device control methodology and apparatus with a special mode where only emergency conditional communication can alert the receiving party.

[011] Yet another object of the invention is to provide communications device control methodology and apparatus the capability to record communication upon an emergency conditional communication being received.

[012] Yet another object of the invention is to provide a methodology and apparatus for enterprise-to-person / person-to-person smart emergency communication. This smart emergency communication may be considered a protocol. This smart emergency communication comprises the exchange of an emergency conditional communication indication, the originating party data, and the originating party's location.

[013] Yet another object of the invention is to provide a methodology and apparatus for conditional processing of communication wherein the conditional processing comprises an emergency condition and a normal condition.

[014] Another object of the invention is to automate the conditional communication processing where conditional communication processing is comprised of conditions such as an emergency condition, a priority condition from a plurality of possible priorities (i.e., emergency, high priority, normal, low priority, etc.), a sending party specified condition that can be used to process incoming communication.

[015] In accordance with one embodiment of the present invention, a system and method is provided for processing conditional communication wherein a calling party sends a conditional communication to a receiving party's communication device. The method comprises a plurality of conditional communication consists at a minimum, of an emergency conditional communication type and a normal conditional communication type. Upon a sending party initiating an emergency communication (e.g., placing a call) to a receiving party, a communication link is established between

the calling party's device and the receiving communication device. Then an emergency protocol or emergency conditional communication indication is sent from the sending party's device to the receiving party's device. The receiving party's device checks to determine if the incoming communication emergency communication protocol or emergency conditional communication indication is present. If present, the incoming communication is "flagged" as an emergency communication.

[016] This system and method includes optional processing to determine if the identification of the communication originating source is blocked from placing a conditional communication to the receiving party. This includes the step of searching a blocker database of a plurality of identification records to determine if the source (e.g., caller) is blocked. If the source is blocked, then the communication is terminated. If the source is not blocked, the method sets a distinct ringtone used to alert the user of an incoming emergency conditional communication. The receiving party is intelligently alerted they are receiving an emergency communication and not just another call. If the source is not blocked for a normal conditional communication, the method sets a regular ringtone used to alert the user of another incoming communication.

[017] The disclosed method includes the step of storing a communication source identification database including a plurality of records. Each record includes the originating source identification (e.g., caller ID) information corresponding to a particular contact/source along with the conditional communication type to be blocked.

[018] This method includes a special mode which the user can select in their communication device. This mode selectively filters incoming communication by on permitting conditional communication of an emergency to alert the receiving party and then with a distinct emergency alert. All other incoming communication (e.g., normal conditional communication) is blocked from alerting the receiving party while the receiving device is in this mode.

[019] This method also includes the option of providing the GPS latitude and longitude in the conditional communication protocol of the calling party to be received and displayed by the receiving device.

[020] This method also includes the option of recording all communication upon establishing an emergency communication link between the sending and receiving communication devices.

#### BRIEF DESCRIPTION OF THE DRAWINGS

[021] The features of the invention believed to be novel are specifically set forth in the appended claims. However, the invention itself, both as to its structure and method of operation, may best be understood by referring to the following description and accompanying drawings.

[022] Figure 1 is a functional block diagram showing the overall Communications System.

[023] Figure 2 is a functional block diagram showing the overall relationship of the disclosed Communications Controller relative to other telecommunication device functions.

[024] Figure 3 is a block diagram of the hardware needed to support the Communications Controller. The implementation of the hardware can either be as a standalone unit that interfaces to Instantaneous Response Device, Messaging Response Device, and Caller Identification Device functions or an integrated element/feature set.

[025] Figure 4 depicts a Communications Controller implementation of a user interface.

[026] Figure 5 is a flow diagram depicting the conditional communication operations and logic.

[027] Figure 6 is a flow diagram depicting the setting up of the instant blocker function.

[028] Figure 7 depicts the look-up-table structure, which provides operational settings that are consequential functions related to the incoming caller blocking conditions.

[029] Figure 8 depicts notional Protocol Fields as they relate to the Emergency Protocol.

## DETAILED DESCRIPTION OF THE INVENTION

[030] The disclosed Communications Controller virtually aids the receiving party to instantly distinguish an incoming emergency communication from the constant disruptions of all other incoming communications (e.g., phone calls, emails, SMS text messages, IM, spam and/or electronic media). Advantageously, the disclosed communication controller enables consumers to regain value-added control of their personal time and be alerted of critical situations.

[031] For purposes of illustration only, and not to limit generality, the Communications Controller will be explained with reference to its use in processing incoming telephone calls as one example of its application. However, this logic can apply to any media type of incoming communications. The Communications Controller includes automated control logic that intelligently integrates communication routing and screening functions. The controller manages and controls incoming communications depending on the automated condition/situation determined by the controller logic, the calling party or originating communication source criteria, and the current mode the receiving party's communication device. The originating source criteria are comprised of appropriate identification of the party, device or entity such as Caller ID, email address, broadcast source, Internet Protocol. address source, website source, internet source, text source, messaging source, Voice-over-Internet Protocol (VoIP) source, account identifier, etc.)

[032] The disclosed Communications Controller enables the consumer to effectively control the conditional notification and if it is permitted to ring/announce an incoming communication to alert the receiving party. It permits the consumer to establish critical/emergency notification for incoming calls. If desired, all normal incoming phone calls (e.g., from solicitors and harassers) will not even ring. Therefore, at the option of the receiving party, the receiving party is not disturbed while staying available for only emergency communication. The disclosed controller advantageously transforms the telephone into a controllable device which provides efficient and effective



timely, value-added communication. It also puts a tool in the user's hands for time-critical emergency situations that are not of a 911 Service nature.

[033] The disclosed communications controller is first described as it functionally relates to other telecommunication device functions. Later, representative hardware for implementing the controller is described in detail along with a description of the processing control logic.

[034] More particularly, Figure 1 is a functional block diagram showing the overall relationship of the disclosed Communications System 100 which is comprised of the Originating Communication Device or Gateway (Incoming Communication source) 101, the Telecommunications Network Service Provider's Central Office Facility (Communications Network) 102, and the Receiving Communication Device or Gateway (Incoming Communication Destination) 103. A Gateway may comprise a mass notification system capability which could broadcast an emergency alert to one or more receiving parties. A Gateway may also be comprised of a PBX, VoIP, Transmission Control Protocol/Internet Protocol ("TCP/IP"), Hub, Server, Call Center, etc. wherein a Gateway is defined as the function that provides call management/control for multiple users. In this embodiment, the Gateway will be able to process conditional communication as the controller will reside in it as well.

[035] The processing provided to a particular incoming telephone call by the Communications Controller is originating source, conditional, and current receiving device mode setting dependent. It is noted that the Communications Controller and associative control logic can be applied and implemented as a consumer product along with other consumer communication devices (e.g. telephones, answering machines/services, Caller ID devices, computers, telephone/television/ internet solutions, and mobile/radio devices, network equipment and/or devices such as servers, gateways, PBXs, etc.). The Communications Controller can also be implemented at the telephone service switch at the Central Office Facility 102 and provided to the consumer as a communication service.

[036] In one embodiment depicted, the Instantaneous Response Device Functions 201, Messaging Response Functions 202, and Caller Identification Functions

203 may be implemented as an integrated device or independently to support the Communications Controller Functions 200 as indicated in Figure 2.

[037] The Instantaneous Response Device Functions 201 (e.g., telephone device) provides the interactive support needed for a communications device such as a mobile device/telephone. Examples of the support this device provides are ring/announce, call forward, call waiting, and paging the user for immediate response to the incoming call.

[038] The Messaging Response Functions 202 (e.g., answering machine/service, recorders) provides the passive support needed for a communications device. Examples of the support this device provides are to play, store, and record message/data (e.g., voicemail, email, video, multimedia) to which the user can respond at their convenience but not necessarily during the time the call/contact is being placed or made. The communications line 204 (e.g., a telephone line or cable) that connects to other communication devices is coupled to the Caller Identification Functions 203. For a mobile device, the communications line 204 would not be present.

[039] The Originating Identification (ID) Function 203 sends incoming communications identification data or originating source criteria such as Caller ID data supplied to the Communications Controller 200. Communications Controller 200 processes incoming communications using for example, the Caller ID data received. The interface 205 supports communications to transmit and route data among the above described system functions in Figure 2.

[040] Originating source criteria can also be originating device dependent (identifier associated to the call origination device) or caller/user dependent (identifier associated to the individual caller/person/account). Consumer products for the Caller Identification Functions 203 using today's technology are device dependent – they provide the caller's phone number and/or name. However, depending on the implementation of the Communications Controller 200, this data could be the I.P. Address of a node on a network, a network identifier, or other device identifier data. Conversely, caller dependent Caller ID data can utilize such elements as:

- 1) Caller personal account data (e.g., account number, email address, Internet address, etc.);
- 2) Speaker dependent voice data – person identifying themselves by speaking their name in order to capture their temporal phonic signal data; and
- 3) Video data – a video frame of a caller's unique identifiers (e.g., biometrics, the caller's face, retinal scan, finger/thumb print, etc.)

[041] In this embodiment, the Communications Controller 200 is not dependent on the Caller ID data/media type. Rather, controller 200 merely conforms to the data type being used by the Originating Identification (ID) Function 203 (e.g., Caller Identification Functions), which is an external interface to Communications Controller 200. Communications Controller 200 merely utilizes this data associated with the caller regardless of its type (e.g., device dependent or caller dependent) to determine the communication processing dependent on the originating source criteria (e.g., the caller). (Communications Controller 200 uses the incoming Caller ID data to attempt to match this data with the Caller ID data stored in its Blocker Function Database of Figure 8 for a call processing determination.)

[042] The operations of the communications device include the Originating Identification Functions 203, Messaging Response Functions 202, and Instantaneous Response Functions 201. Some of these operations comprise but are not limited to the following:

- Provide a specified ring alert (of multiple ring alert options) wherein alerts may be aural, visual, and/or tactical
- Provide a specified ring pattern distinct for emergency conditional communication
- Provide a specified announcement for a particular caller
- Provide a specified OGM with or without an opportunity for the caller to leave a message (of multiple OGM options)

- Terminate the call (e.g., hang-up without ringing the telephone device)
- Call Forwarding/paging upon a call being routed to ring and the user pre-selecting this option
- Call waiting will transmit a beep signal for the user while on the phone. This beep could be mapped to a priority level beep type to inform the user of the importance of the call prior to them disrupting their present conversation
- Recording an emergency conditional communication

[043] For the purpose of discussion, and not for the purpose of limitation, Figure 3 depicts a high-level hardware implementation of the Figure 2 Communications Controller as Communications Controller 300. Controller system 300 employs a microcomputer (MCU). Utilization of a MCU for this type of application is a typical solution/implementation. However, the functions indicated in Figure 2 can be integrated together or packaged separately in numerous configurations. These configurations can range from MCU's to Personal Computer/Internet Systems, personal appliances/devices, or a Radio/ Telephony/Television Systems.

[044] To clearly describe the hardware support functions required for the Communications Controller 300 of Figure 3, the following example of the steps performed upon receiving a call is explained along with details as they relate to the hardware of Communications Controller 300. Communications Controller 300 is coded with software according to the flow diagrams of Figures 5 and 6. This software code is stored in memory within controller 300 in one embodiment. When executed by controller 300, this software causes controller to implement the steps set forth in the flow diagrams of Figures 5 and 6.

[045] Data is received and transmitted across the Bus 305 to permit the Instantaneous Response Hardware 301 (e.g. a telephone), the Messaging Response Hardware 302 (e.g. an answering machine) the Caller Identification hardware 303, and Communications Controller 300 to communicate.

[046] Upon receiving a call via the communications line/service 304, the Caller Identification hardware 303 receives the incoming Caller ID data. An interrupt is then

generated from the Caller Identification Hardware 303 and sent to the Communications Controller Watchdog/IRQ 310. This Watchdog/IRQ 310 (e.g. an interrupt controller) monitors for reception of an interrupt that designates a communication is being received. After this interrupt, the Caller ID data is transmitted from the Caller Identification Hardware 303 via the bus 305 to the Communications Controller MCU Input port(s) 309. The data is transmitted via the internal Bus 311 to the MCU RAM 307.

[047] This Caller ID data is then compared against data stored in ROM 308 to obtain processing information as explained in the description of Figure 5 and 6 flow diagrams. CPU 306 performs the processing software execution, which in turn provides the control logic for the controller according to the described flow diagrams. The RAM/ROM 307/308 provides the memory necessary to support the load of the executable code and memory to support the real-time processing. The ROM 308 provides the storage necessary to support the memory requirements for the database fields of Figure 7. The internal bus 311 is used to support "local" communications among the various functions within the Communications Controller 300.

[048] In one embodiment, input values such as user selected blocking and setting of the device mode are provided to Communications Controller 300 by the user inputting such selections to the Instantaneous Response Hardware 301 (e.g. telephone/mobile device). These values are then transmitted to Communications Controller 300 for storage in the memory therein. Alternatively, an input device such as a keyboard device or personal computer can be coupled to communications controller 300 at input port 312 to provide input for such values.

[049] The Communications Controller 200 leverages a special mode or status of the communications device that supports special conditional processing called emergency mode. This mode only permits the reception of an emergency conditional communication to alert the user. For example, if the receiving party selected emergency mode, only an incoming emergency conditional communication would be permitted to ring the device. This ring may be distinctive so the receiving party knows instantly they are receiving an *emergency* communication. All other communication (e.g., "normal" communication) is processed as if the intended receiving party did not

intercept the communication. The emergency mode may be selected from a plurality of modes provided in the communication device or the selection of the emergency mode may be a toggle setting.

[050] For the purpose of discussion, and not for the purpose of limitation, Figure 4 depicts a mobile device 400 that has the Communication Controller 300 embedded in it. For example of the user interface design, the soft keys 401, 403 may be programmed to support the functionality of the Communication Controller 200. Pressing soft key 401 permits the user to toggle the emergency mode function on/off. The current mode 402 of the device is displayed on the device screen 405 above the soft key 401.

[051] Programmable key 403 may be used to initiate an emergency call. The Communication Controller 200 functionality for placing an emergency call can be programmed to soft key 403. This functionality is displayed 404 for the user. In a panic situation, the user can merely press or press and hold the Make Emergency Call 403/404 soft key to send an emergency conditional communication. The press and hold function would send a communication to a default/stored contact. A contact list could be used with a scroll capability to allow for easy selection from multiple contacts. Upon just pressing the Emergency Call soft key 403/404 (i.e., not press and hold), an opportunity is presented to the user of the device to select or input the phone number / contact information of the party they wish to send an emergency communication. The sending and the receiving devices and/or gateways require the Communication Controller 200 functionality to process an emergency conditional communication as the conditional filtering protocol is used to establish conditional communication between them.

[052] Figures 5 and 6 together form a flow diagram depicting the flow of operations carried out by the Communications Controller 200 system. The steps shown in Figures 5 and 6 provide an example of the control logic necessary to send and receive communication. Operation commences in the Sending Device 500 where the user places an Emergency Conditional Call 501 achieved by the process described for Figure 4. Upon selecting the key programmed to send an emergency condition call 403, the Emergency Protocol 502 is generated to be appended to the communication.

The call is placed over the network to of at least one or multiple of the selected contact(s) 503. One means to transmit the emergency protocol is to establish a communication connection between the Receiving Device/Gateway 505 and the Sending Device/Gateway and perform a TAPI (telephone application program interface) acknowledgement that the communication connection has been accepted then append the communication by sending the Emergency Protocol that was generated 502 to the receiving device 505. TAPI defines standards for simple call control and for manipulating call content. Other means may include sending SMS (Short Message Service) messages back and forth between the devices or leveraging Voice over Internet Protocol (VoIP)/ TCPIP protocols. Yet another approach might be to generate a signal such as a DTMF string unique to the emergency protocol to be transmitted upon a connection acknowledged from the receiving unit. If the Sending Device 500 does not receive an acknowledgement that the communication has been successfully established with the intended Receiving Device 505, then attempts may be made to redial or just notify the user (i.e., calling party) that the call failed 504.

[053] Upon the Receiving Device 505 receiving a communication, it waits for several cycles (enough time to permit a protocol to be received) then checks to see if the Emergency Conditional Protocol 507 was received. If received, the call is "flagged" as an Emergency Conditional Communication 508. Then, the originating source criteria which in this embodiment example is Caller ID is used in conjunction with the lookup table of Figure 7 to determine the device operational function to perform 701, 702 based on the type of communication being received (i.e., normal communication or emergency conditional communication). If a match of the Caller ID is found in the lookup table 700 for the type of communication being received, then the Caller ID is Blocked 508 so the communication will not alert the user and will terminate 509. Note that the communication could also be forwarded and/or go to voicemail. The TAPI lineClose is performed to terminate the call 510, the Caller ID and "Blocked" are displayed on the receiving party's communication device screen 511, 405 and the Communication Controller 200 process terminates 513.

[054] If the Caller ID is not "Blocked" then, the appropriate alert will be used to notify the receiving of the incoming communication 514. If the incoming communication

was flagged as an emergency communication then the Alert User 515 functional process will be a distinct alert uniquely used for only emergency conditional communications (tactical, aural, visual). For example, use a special ringtone that is uniquely played only for emergency communications. If no emergency protocol was received, then the incoming communication is considered "normal" and a "normal" (non-emergency) alert will be used to notify 515 the receiving party of the incoming communication event. The Communication Controller 200 process ends upon the call being terminated 516, 513.

[055] Additionally, the Emergency Conditional Communication Processing may comprise of sending location data such as GPS latitude and longitude data from the sending device to the receiving device as part of an emergency communication protocol. This data pinpoints the location of the party in an emergency situation and can be provided to the receiving party in case the sending party is unable to speak. The latitude and longitude data can be displayed on a map in the receiving party's device screen 405.

[056] A communication device enabled with the Communication Controller 200 has an Instant Blocker Function comprised of a flow diagram depicted in Figure 6. The Instant Blocker function supports the user interface to permit the user to select and set which originating sources are to be blocked for what conditions. For example, upon the Caller ID (ID) being displayed on the communication device screen 600, 405 a soft key is programmed to display "Block" 601. Another means to access the Instant Blocker Function may be via an icon displayed on the communication device screen 602, 405. Upon the User Selecting the Block Function 603 of the Communication Controller 200, a Block Dialog Box appears on the display screen 405 along with the current originating source criteria (e.g., the current Caller ID) with the option to select having only "normal" calls blocked or blocking all calls which includes emergency conditional communication 604. Once this option is selected, another dialog box presents the user of the device the option of toggling the blocking function of the selected condition and Caller ID originating source criteria "ON" or "OFF" 606, 610. If the user selects "ON" 606, store the Current Caller ID and blocking conditions 607 in the Blocker Function Database of Figure 7, set Caller ID Alert to "OFF" 608 and display the Caller ID and Blocked Status



to the user 609, 405. On the other hand, if the user selects "OFF" 610, store the Current Caller ID and blocking conditions 611 in the Blocker Function Database of Figure 7, set Caller ID Alert to "ON" 612 and display the Caller ID and Unblocked Status to the user 612, 405. The Instant Blocker Function is terminated 613 after the Caller ID Blocked status is displayed 608, 612.

[057] Figure 7 depicts a representative lookup table structure employed in the disclosed Communications Controller 200. This table is used to determine if a conditional communication (e.g., normal or emergency condition) for a particular communication originating source or ID 700 is blocked thus not permitted it to disturb the receiving party. The lookup table structure is used by test 508 of Figure 5 to obtain the consequential operation control data for the integrated communications device functions. These consequences are based on conditional results being present. In particular, the lookup table structure includes a plurality of records 703 designated 1...p, which is dependent on the number of ID's employed in a particular embodiment of Communications Controller 700. In the disclosed embodiment, the ID is comprised of the originating source criteria such as the Caller ID.

[058] With the combined conditions of the call being placed as an emergency conditional communication and the incoming ID being blocked 702, the desired consequential operation of the communication device is defined as blocked. Again, with the combined conditions of the call being placed as a normal communication and the ID of the incoming call being blocked 701, the desired consequential operation of the telephone device is defined as blocked. If the communication is defined as blocked, it will not be permitted to alert the receiving party that they are receiving an incoming communication. This function permits the receiving party to control which originating source/caller can "ring" their communications device, thus alerting them. If the ID 700 of the originating source is not present in the Blocker Function Database, it is considered acceptable to alert or "ring" the receiving party notifying them of the incoming communication.

[059] Figure 8 depicts notional protocol fields 800 to support the Sending Device logic of "Generate Emergency Protocol" 502. These fields may comprise but not be limited to the Sending ID 801 for the originating source identification; the Receiving ID

802 for the intended party's identification data; the Condition and / or Priority of the communication 803 wherein there may be various levels of emergency or priority communication (e.g., emergency-highest priority, high priority-middle priority, normal-no priority); Sensor Data 804 for readings of sensors data wherein a sensor may be a GPS so the location and/or NEMA data would be used in the sensor filed; Situation Data 805 where situation awareness information may be embedded (e.g., red alert-school is in lock-down); and an Append Field 806 wherein additional data may be added to the protocol.

[060] In summary, the disclosed method and apparatus advantageously limits a communications device user's exposure to undesired communications by employing advanced control mechanisms implemented at or near the communications device in one embodiment. The control methodology and apparatus permits the consumer to proactively take control of how, to what conditions, and if the customer responds to incoming communications. Advantageously, the disclosed methodology transforms the communications device (e.g., telephone, computer, internet device, and/or television) from a passive device to a "smart" controllable device that incorporates individual time management values and customized consumer priorities. It empowers the user to know instantly that they are not just receiving another "normal" communication but an "emergency" condition communication. Incoming communications are managed and controlled depending on the originating source criteria, the condition of the communication, and the current mode of the communications device. A special mode exists wherein only emergency condition communication can alert the receiving party while all other communication is silenced/terminated. In this manner, the user is empowered to take control over incoming communications and always stay selectively/intelligently connected in case an emergency or critical situation arises. This is especially useful in situations where it is desired to have your mobile device turned "OFF".

[061] While only certain preferred features of the invention have been shown by way of illustration, many modifications and changes will occur to those skilled in the art. It is, therefore, to be understood that the present claims are intended to cover all such modifications and changes which fall within the true spirit of the invention.

**CLAIMS**

What is claimed is:

1. A method for processing conditional communication from a sending communication device to a receiving communication device comprising the steps of:  
generating emergency indication criteria in the sending communication device;  
establishing a communication link between the sending communication device and the receiving communication device;  
sending the emergency indication criteria from the sending communication device to the receiving device; and  
processing the emergency indication criteria and originating source criteria in the receiving device to determine the operational functions to perform wherein operational functions comprise blocking the communication, using a distinctive alert for reception of the emergency conditional communication, using a non-emergency alert or alerts for reception of a non-emergency conditional communication, using a non-emergency alert or alerts for reception of a non-conditional communication, and terminating the communication.
2. The method of claim 1 further comprising the steps of:  
searching a database comprising a plurality of records of originating source identification criteria for said source to block for conditional communications; and  
upon an originating source identification criteria match, blocking the communication from alerting the receiving party.
3. The method of claim 1 further comprising the step of processing the emergency conditional communication indication comprising an emergency protocol.
4. The method of claim 3 further comprising the step of processing the emergency protocol as a flag set to acknowledge the current communication is an emergency.

5. The method of claim 3 further comprising the step of processing the emergency protocol which includes sensor data.

6. The method of claim 5 further comprising the step of processing the emergency protocol which includes the location of the sending device.

7. The method of claim 6 further comprising the step of processing the location of the sending device comprising the latitude and longitude.

8. The method of claim 3 further comprising the step of processing the emergency protocol which includes activating recording of the communication.

9. The method of claim 3 further comprising the step of processing the emergency conditional communication indication comprising an emergency protocol.

10. The method of claim 1 further comprising the step of selecting, by the user, the respective originating source identification to be blocked for emergency conditional communication stored in the database.

11. The method of claim 1 further comprising the step of sending the emergency indication criteria as a unique DTMF signal indication.

12. The method of claim 1 further comprising the step of:  
sending the emergency indication criteria as a unique SMS (Short Message Service) text message to the said receiving device; and  
reading the said SMS text message to determine the emergency conditional communication.

13. The method of claim 1 further comprising the step of sending the emergency indication criteria leveraging TCP/IP protocol between the said sending device and the said receiving device.

14. The method of claim 1 wherein the sending communication device broadcasts the emergency indication criteria to a plurality of receiving devices simultaneously.

15. A method for processing incoming communication from a sending party sent to a communications device of the receiving party comprising the steps of:

setting the receiving party's communication device mode to the conditional communication mode from a plurality of device modes wherein the said mode is for emergency conditional communication;

receiving an incoming communication that is not an emergency conditional communication; and

blocking the communication that is not an emergency conditional communication from alerting the receiving party;

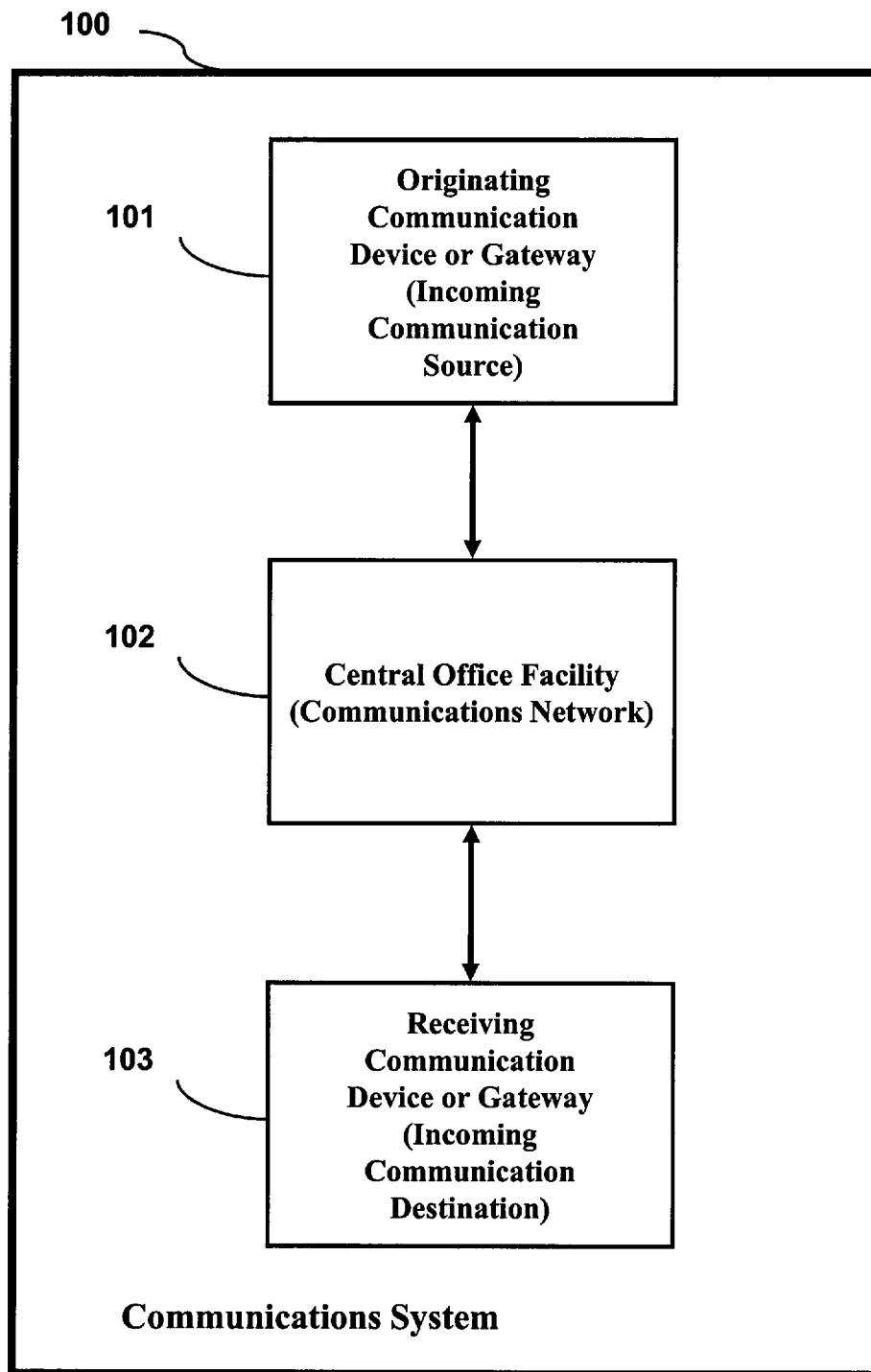


Figure 1

2/7

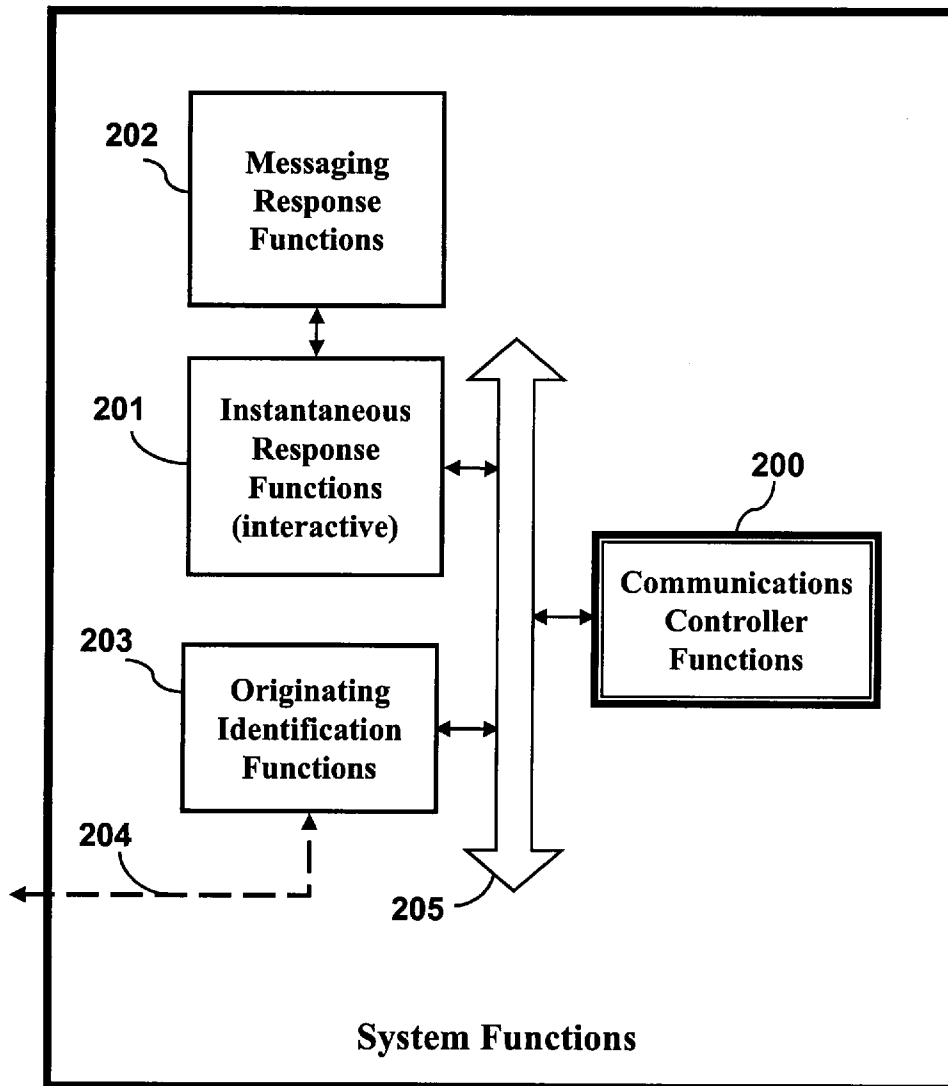


Figure 2

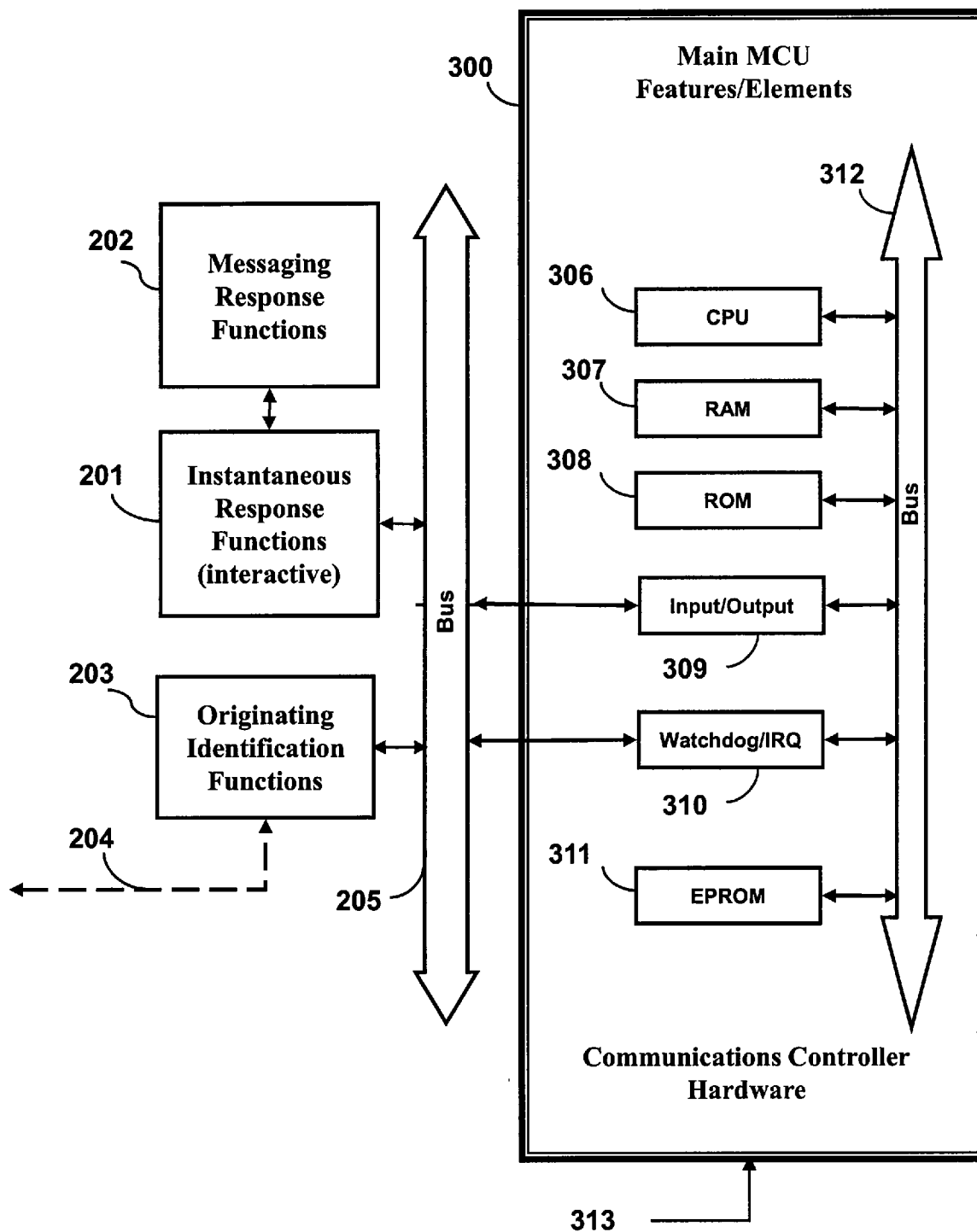


Figure 3



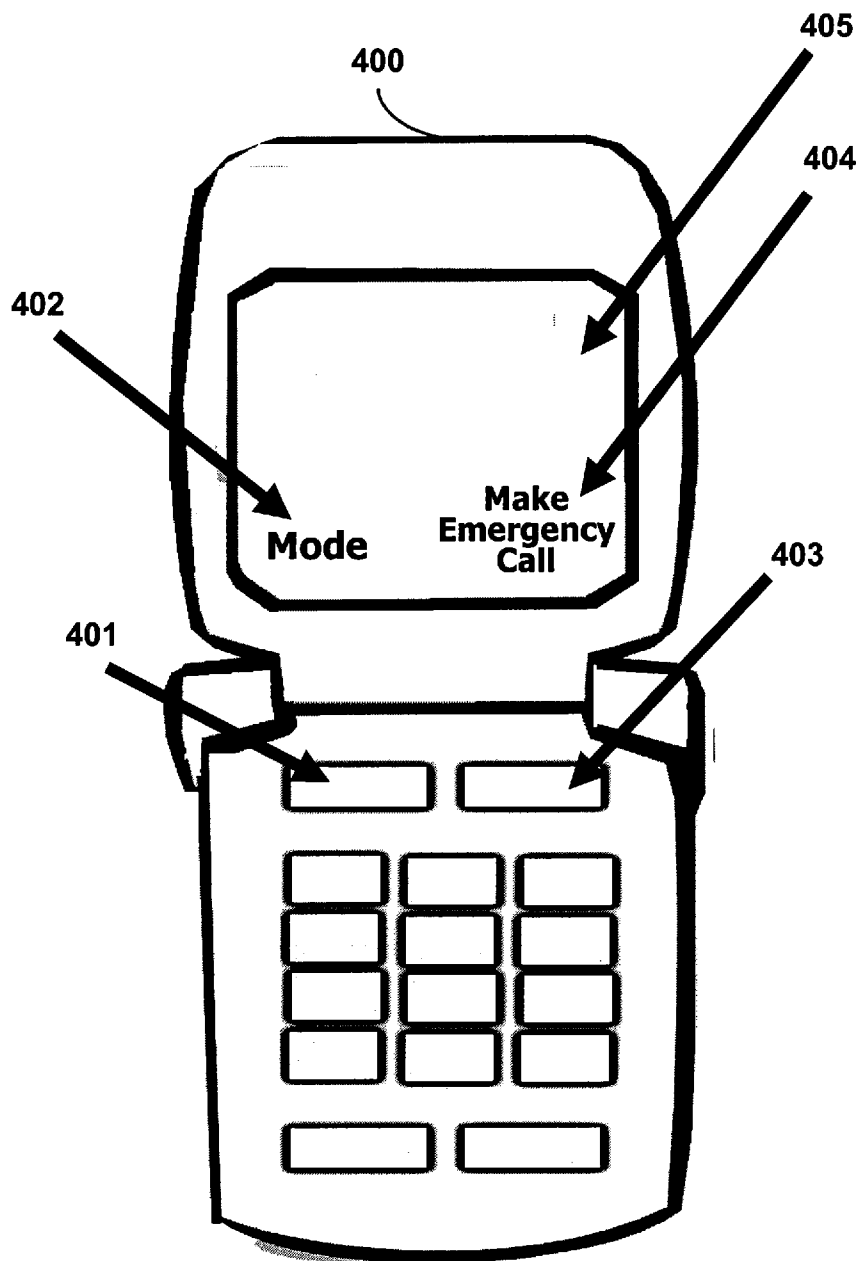


Figure 4

5/7

## Emergency Conditional Communication Processing

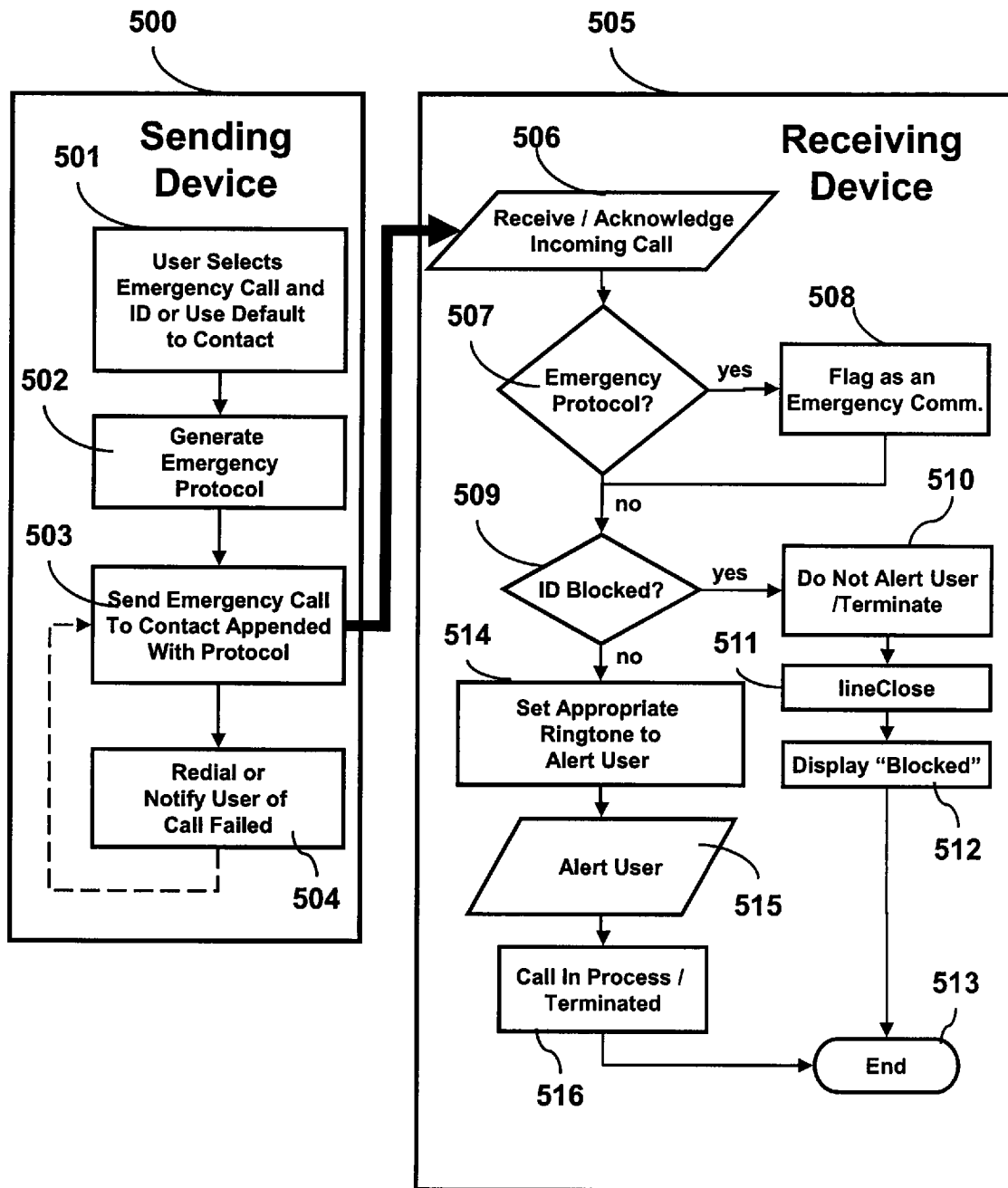


Figure 5

6/7

## Instant Blocker Function

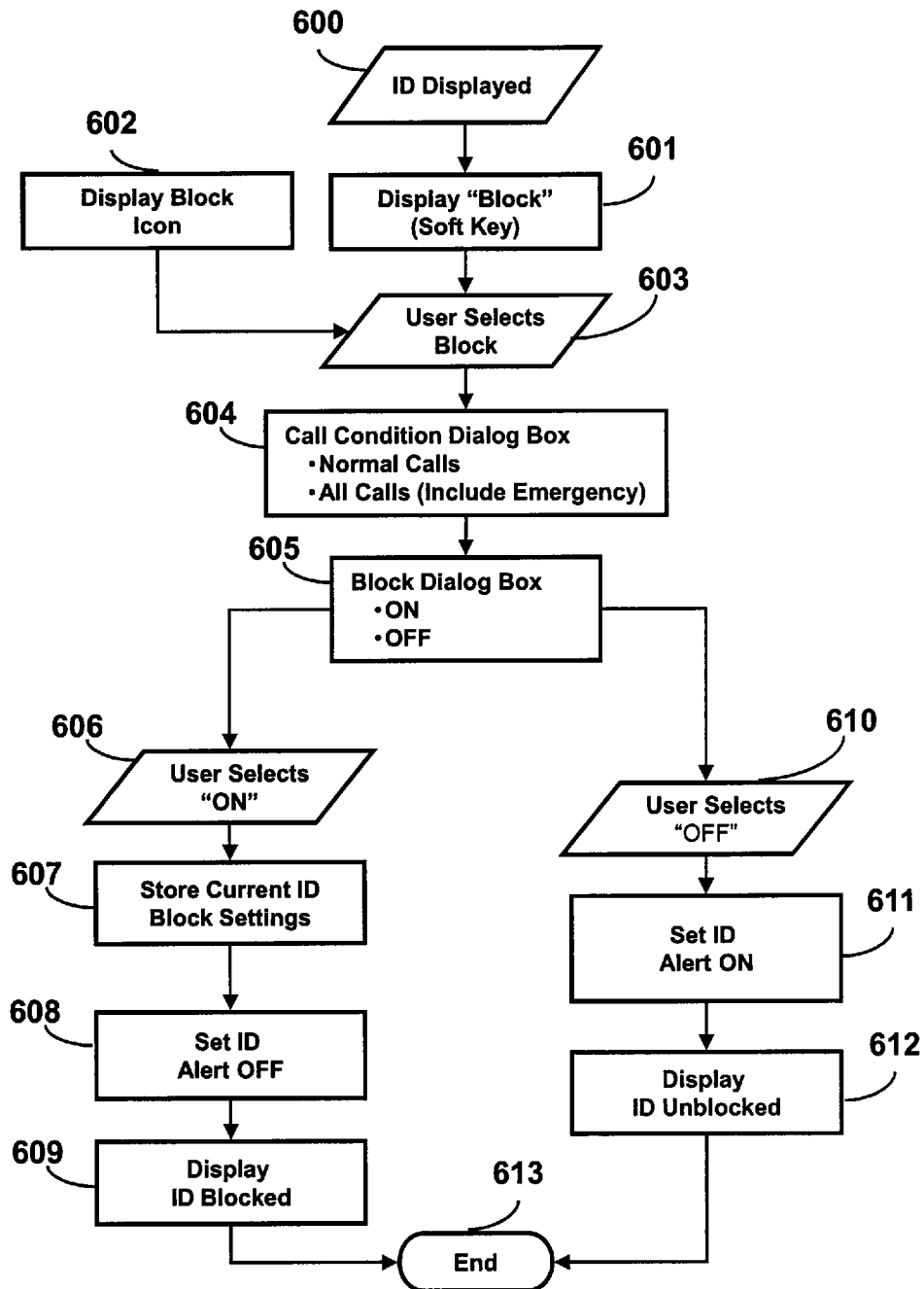


Figure 6

7/7

700	701		702
	Normal	Emergency	
ID 1			703
ID 2			703
⋮			703
ID <i>p</i>			703

Blocker Function Database

Figure 7

800	
Protocol Field	
801	1 Sending ID
802	2 Receiving ID
803	3 Condition/Priority
804	4 Sensor Data
805	5 Situation Data
806	6 Append Field

Figure 8

## INTERNATIONAL SEARCH REPORT

International application No.

PCT/US 08/57458

## A. CLASSIFICATION OF SUBJECT MATTER

IPC(8) - H04M 11/04 (2008.04)

USPC - 455/404.1

According to International Patent Classification (IPC) or to both national classification and IPC

## B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC(8): H04M 11/04 (2008.04)

USPC: 455/404.1

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

USPC: 455/404.1, 414.1, 415, 416, 379/201.01, 379/201.11, 379/211.01

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

PubWest (USPB, USPT, USOC, EPAB, JPAB); GoogleScholar

Search Terms: method processing conditional sending receiving emergency communications controller establishing link blocking alert non-emergency terminating searching database records identification block match protocol flag acknowledge sensor etc

## C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 2006/0223492 A1 (Chin et al.), 05 October 2006 (05.10.2006), para [0011]-[0014]; [0016]; [0020]-[0023]	1-15
Y	US 2005/0143048 A1 (Binning), 30 June 2005 (30.06.2005), para [0026]-[0029]; [0035]-[0038]	1-15
Y	US 2005/0288035 A1 (Wang), 29 December 2005 (29.12.2005), para [0065]-[0068]; [0071]; [0085]; [0087]; [0105]; [0107]; [0134]	1-15
A	US 2006/0040639 A1 (Karl et al.), 23 February 2006 (23.02.2006), entire document	1-15
A	US 2005/0282518 A1 (D'Evelyn et al.), 22 December 2005 (22.12.2005), entire document	1-15
A	US 2004/0105529 A1 (Salvucci et al.), 03 June 2004 (03.06.2004), entire document	1-15

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

\* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T"

later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X"

document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y"

document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&amp;"

document member of the same patent family

Date of the actual completion of the international search

15 May 2008 (15.05.2008)

Date of mailing of the international search report

30 JUN 2008

Name and mailing address of the ISA/US

Mail Stop PCT, Attn: ISA/US, Commissioner for Patents

P.O. Box 1450, Alexandria, Virginia 22313-1450

Facsimile No. 571-273-3201

Authorized officer:

Lee W. Young

PCT Helpdesk: 571-272-4300

PCT OSP: 571-272-7774