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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
4 November 2010 (04.11.2010)

PCT

(10) International Publication Number
WO 2010/124358 A1

(51) International Patent Classification:
*G08C 17/00* (2006.01) *H02J 9/00* (2006.01)
*G05D 7/06* (2006.01) *H04W 84/18* (2009.01)
*H02J 7/00* (2006.01)

(21) International Application Number:
PCT/CA2009/001433

(22) International Filing Date:
9 October 2009 (09.10.2009)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
61/173,840 29 April 2009 (29.04.2009) US

(71) Applicant *(for all designated States except US)*: **GWS COMMUNICATION SYSTEMS INC.** [CA/CA]; 202-11 Burbidge Street, Coquitlam, British Columbia V3K 7B2 (CA).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **WOOD, Raymond** [CA/CA]; 2927 Pinetree Close, Coquitlam, British Columbia V3E 2Z5 (CA). **HANRAHAN, Michael Wayne** [CA/CA]; 201-2285 Welcher Ave., Port Coquitlam, British Columbia V3C 1X2 (CA).

(74) Agent: **SMITHS IP**; Suite 330 - 1508 West Broadway, Vancouver, British Columbia V6J 1W8 (CA).

(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, CL, 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, PE, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, SE, SI, SK, SM,

*[Continued on next page]*

(54) Title: NETWORK-ENABLED VALVE MANAGEMENT SYSTEM

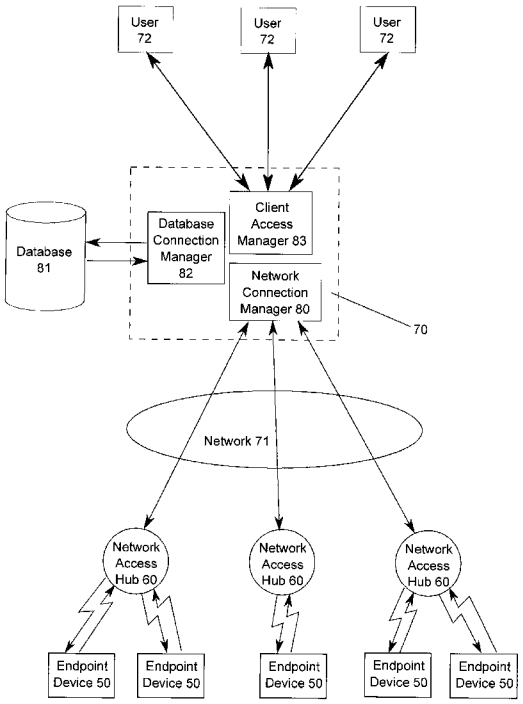


Figure 3

(57) Abstract: A system for remotely operating endpoint devices, such as valves for utility services, comprises a server, one or more network access hubs, and one or more endpoint devices. The network access hubs communicate with the server through a network and communicate wirelessly with the endpoint devices. The network access hubs transmit instructions to the endpoint devices to control the operation of the endpoint devices. The network access hubs may also comprise earthquake detection circuits to detect possible earthquakes and transmit instructions to the endpoint devices to close valves accordingly.

WO 2010/124358 A1

TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

— *with amended claims (Art. 19(1))*

**Published**:

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

# TITLE OF THE INVENTION

Network-Enabled Valve Management System

## FIELD OF THE INVENTION

The present invention relates to automatic control of valves. In particular, the present invention relates to automatic control of valves for gas, oil, water or other fluids.

## BACKGROUND OF THE INVENTION

Valves are typically used to control utility service (such as gas or water) to customers. For example, quarter-turn valves are commonly used for gas and water connections. Such valves are usually operated manually, with a technician turning a handle to control the flow of the utility service.

Traditionally, to stop or restore gas, water, or other utility service to a customer, a utility company would send a technician to the location to manually unlock and open, or close and lock a valve. There are a number of costs associated with this approach, including labour cost (including time required for travel and for completing the job) and vehicle cost (including fuel and maintenance cost).

## SUMMARY OF THE INVENTION

The objectives of the present invention include the following: (1) eliminate the need for service visits to stop, limit, or restore gas, water, or utility service; (2) provide mass emergency utility shut-off capabilities; (3) provide automatic utility shutoff in an earthquake; (4) provide a network of earthquake detectors that can operate independently and collectively; (5) provide a means for rationing utility service; (6) provide a means for automatic utility "prepaid" service; and (7) provide automatic "intermittent" or time-limited utility service.

In one aspect of the invention, a system for remotely operating endpoint devices comprises a server, one or more network access hubs, and one or more endpoint

devices. Each of the network access hubs comprises a network interface for communication with the server over a network, a microprocessor, a hub transmitting means, and a hub power supply. Each of the endpoint devices comprises an endpoint receiving means for receiving wireless communications comprising instructions from the hub transmitting means of one or more of the network access hubs in wireless communications range, a microcontroller for processing the instructions and executing the instructions, and an endpoint power supply.

In another aspect, the endpoint devices further comprise a valve motor for controlling one or more valves and a motor driver, wherein the motor driver receives electrical signals from the microcontroller upon execution of the instructions by the microcontroller and wherein the motor driver effects movement of the valve motor in accordance with the electric signals. The valves may be used to restrict the flow of one of the following utility services: gas, oil, and water.

In yet another aspect, the one or more network access hubs further comprise an earthquake detection circuit, wherein the earthquake detection circuit sends an earthquake warning to the microprocessor upon detection of a possible earthquake.

In a further aspect, one or more of the endpoint devices comprises a light source for use in street lighting.

In another aspect, a method of remotely controlling endpoint devices comprises the steps of a server communicating with one or more network access hubs through a network, the one or more network access hubs wirelessly transmitting instructions to one or more endpoint devices through a hub transmitting means, the one or more endpoint devices receiving the instructions from the network access hubs through an endpoint receiving means, and the one or more endpoint devices implementing the instructions.

In a further aspect, a method of remotely controlling a valve in an endpoint device in response to a possible earthquake comprises the steps of a server communicating with a network access hub through a network, the network access hub detecting a possible earthquake through an earthquake detection circuit, the network access hub

transmitting information regarding the possible earthquake to the server through the network, the network access hub wirelessly transmitting instructions to the endpoint device through a hub transmitting means, wherein the instructions comprises instructions regarding control of the valve in response to the possible earthquake, the endpoint device receiving the instructions from the network access hub through an endpoint receiving means, and the endpoint device controlling the valve in accordance with the instructions.

The foregoing was intended as a broad summary only and of only some of the aspects of the invention. It was not intended to define the limits or requirements of the invention. Other aspects of the invention will be appreciated by reference to the detailed description of the preferred embodiment and to the claims.

## BRIEF DESCRIPTION OF THE DRAWINGS

Fig. 1 is a schematic diagram of a valve of the present invention in accordance with the preferred embodiment;

Fig. 2 is a schematic diagram of a network access hub of the present invention in accordance with the preferred embodiment;

Fig. 3 is a schematic diagram showing the network structure of the present invention in accordance with the preferred embodiment;

Fig. 4 is a schematic diagram showing an alternative network structure of the present invention; and

Fig. 5 is a schematic diagram showing a second alternative network structure of the present invention.

## DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENT

Referring to Figs. 1 and 2, the present invention comprises one or more endpoint devices 50 and one or more network access hubs 60. Referring in particular to Fig. 1,

the endpoint device 50 is preferably a valve for controlling gas, oil, water, or some other utility service. In the preferred embodiment, the endpoint device 50 is an electrically operated, battery-powered valve, although the valve may also be pneumatically actuated instead. The valve is preferably a quarter-turn ball valve or a butterfly valve with a position sensor consisting of limit switches and rotary encoder for accurate position determination. In the case where the endpoint device 50 is a valve, it comprises a transceiver 4, a motor driver 6, a valve motor 7, a microcontroller 3, and a power supply 1.

The transceiver 4 is preferably a two-way radio that provides a secure two-way wireless radio link between the endpoint device 50 and the network access hub 60. Preferably, this link is encrypted to prevent eavesdropping and to ensure that there is no unauthorized access to either the endpoint device 50 or the network access hub 60. It is possible to use a receiver only, instead of the transceiver 4, in which case the endpoint device 50 would only be able to receive data from the network access hub 60, and not transmit.

The microcontroller 3 is preferably a low-power processor pre-programmed with firmware to manage and control the operation of the endpoint device 50, based on instructions and communications received from the network access hub 60 via the transceiver 4. The valve motor 7 causes the physical operation of the valve. For gas and water connections, the valve is typically a quarter-turn ball valve, although butterfly valves may also be used. The motor driver 6 comprises circuitry to translate the logic-level signal from the microcontroller 3 into movement of the valve motor 7. For an electrically driven valve, this would include power conditioning to achieve proper isolation from the power supply 1 and to achieve the desired voltage and frequency. The motor driver 6 further comprises circuitry to control the direction of valve motor 7 rotation. For a stepper-motor, the microcontroller 3 comprises circuitry to control the rotation sequence to allow for precise control over the setting of the angle of the valve.

The power supply 1 is preferably a battery, but any other means for providing power is suitable.

The endpoint device 50 may also comprise a valve position detection circuit 8. The valve position detection circuit 8 may provide an accurate indication of the rotation of the valve by incorporating a resistive element that varies a known resistance as the valve turns. The valve position detection circuit 8 may also contain a pulse counter or a rotary encoder in combination with limit switches at the open and closed positions. The limit switches provide an absolute reference for the open and closed positions and provide a calibration reference for the variable position sensor.

The endpoint device 50 may also comprise a tamper detection circuit 10 to alert the system to unauthorized access to the physical hardware. This may be accomplished in 3 ways. The first method is to employ an electro-mechanical switch and/or an optical sensor that will trigger an intrusion alarm message to a server if the valve enclosure is opened. The second method is to employ a motion sensor in the valve to respond to unexpected motion that could indicate attempted removal of the valve. The third method is for the server to monitor the valve and report an error message when the valve stops responding to information requests.

The endpoint device 50 may also comprise a temperature sensor 9 to monitor the temperature of the endpoint device 50.

Further, the endpoint device 50 may comprise a battery management circuit 2. It maintains safety and reliability by limiting current to protect the power supply 1 from a short circuit. It may also provide the necessary isolation between the various power supply rails so that excessive noise or ringing on one supply will not interfere with other supplies. It will also monitor the battery voltage to report back to the server, and if the battery voltage ever drops below a certain threshold, it will send an alert to the server.

In addition to valves, the endpoint device 50 may also comprise metering equipment, sensors (for monitoring flow, motion, temperature, etc.), signalling equipment (sirens, lights, etc.), fans, other motors, solenoids, pumps, or barriers. It may also comprise a light source that may be used for street lighting. The operation of the metering equipment, sensors, signalling equipment, fans, solenoids, pumps, barriers, and/or light source would be controlled through communications with the network access

hub 60.

Each endpoint device 50 is preferably provided with a unique identifier, which could be used to identify the type of endpoint device (e.g. valve, signalling device, pumps, etc.). If the endpoint device 50 is a sensor or meter, it would operate in a very similar way to a valve. However, instead of primarily receiving instructions through the transceiver 4 from the network access hub 60, it would be primarily transmitting data through the transceiver 4 to the network access hub 60. This data would comprise of the information collected by the sensor or meter. Other endpoint devices would behave as valves would. For example, a command normally interpreted as "OPEN" by a valve could be interpreted as "START" by a signalling device (and it would start flashing a light, sounding a siren, etc.). Similarly, a command normally interpreted as "CLOSE" by a valve could be interpreted as "STOP" by the signalling device (stopping the flashing of the light, stopping the siren, etc.).

Referring to Fig. 2, the network access hub 60 is a low-power DC device that can draw its power from a variety of DC power sources. A hub power supply 100, such as a switching AC – DC power supply, is included with the network access hub 60; however, any power source capable of providing enough DC power to the unit may be used instead or as a backup power source. Such sources could include any combination of batteries, solar cells, wind turbines, fuel cells, and generators.

The network access hub 60 also comprises a hub transceiver 400, a network interface 700, and a microprocessor 600. The hub transceiver 400 provides a secure two-way wireless radio link between the endpoint device 50 and the network access hub 60. Preferably, this link is encrypted to prevent eavesdropping and to ensure that there is no unauthorized access to either the endpoint device 50 or the network access hub 60. It is possible to use a transmitter only, instead of the hub transceiver 400, in which case the network access hub 60 would only be able to transmit data to the endpoint device 50, and not receive. The data comprises instructions from the network access hub 60 to the endpoint device 50 regarding the operation of the endpoint device 50.

The network interface 700 provides a secure connection to a data network. Since the network access hubs 60 are likely to be distributed over a large geographical area, a

mobile data solution is preferably used. This would be either a satellite modem, or a mobile data (GSM/GPRS/EDGE, etc.) modem connected to the Internet, or directly to a private network to which the server is also connected. Depending on the network configuration, this could also be some other wireless configuration (e.g. Wi-Fi, Wi-Max, Zigbee, etc.) or a hard-wired configuration (e.g. Ethernet, SCADA, etc.).

The microprocessor 600 comprises the firmware that manages the network access hub 60. It manages its own functions and keeps track of the endpoint devices 50 within its range, so it preferably has more computing power and memory than the microcontroller 3 that would be found in the endpoint devices 50.

The network access hub 60 may also comprise an earthquake detection circuit 800. It uses an accelerometer to measure the magnitude, direction, and frequency of ground oscillations. Oscillations that fall within the limits set by the ASCE 25-06 standard will be considered an earthquake and trigger a broadcast command that will cause all endpoint devices 50 controlled by the network access hub 60 to close automatically. ASCE 25-06 is one example of a common "local standard" for earthquake-actuated valve closure. Because the limits are set in software, these can be easily reconfigured to meet any other limits required for other jurisdictions or applications, and also easily updated to meet any other current or future earthquake detection standards that are based on measuring any combination of magnitude, direction, and/or frequency (period) of ground movement. A message is also sent back to inform the server of the situation. The server can analyze these messages and when enough network access hubs 60 report an earthquake, the server can take the proactive step of telling all network access hubs 60 within the affected geographic area to shut their respective endpoint devices 50 before the earthquake arrives. Alternatively, firmware can be configured so that the accelerometer will respond only to oscillations that fall within the limits set by other standards, or as required in specific cases.

The earthquake detection circuit 800 also incorporates P-wave identification and early warning capability. It will identify P-waves and compare the horizontal and vertical components of a ground oscillation to distinguish them from low-energy S-waves. This will provide an advance warning of an incoming earthquake. The network access hub 60 can use this information to automatically actuate valves or other

systems (e.g. sirens, lights, door openers, etc.) in endpoint devices 50 before the damaging S-waves arrive.

The network access hub 60 may also comprise a power management circuit 200 to manage the hub power supply 100 and any backup power supplies that may be required. Circuitry within the network access hub 60 are typically 12 VDC or less, so the incoming main power supply can be from a mains power supply "brick" with a 9-12 VDC output, from a solar panel, or any other source that can provide 9-12 VDC. The circuitry in the power management circuit 200 will handle any voltage monitoring or conditioning required by the network access hub 60. It will also handle the switch-over from the hub power supply 100 to any backup power supply when required. In the case where the backup power supply is a battery, the power management circuit 200 will maintain the appropriate charge method for the chemistry of the battery chosen.

The network access hub 60 may also comprise a backup power supply 300, which may be used in the event that the hub power supply 100 fails. Its operation would be controlled by the power management circuit 200 as needed.

Further, the network access hub 60 may comprise a tamper detection circuit 1000. It may comprise any combination of limit switches, optical sensors, and/or motion sensors. If any of these devices detect unauthorized "tampering", they will cause a fault condition in the microprocessor 600, which will immediately inform the server and alert any users logged into the system.

Limit switches are configured in such a way that the switch arm is normally held in by the enclosure of the network access hub 60 and will be released if the enclosure is opened, causing a state change within the switch.

Optical sensors may be configured in three ways. The first method is to provide a certain logic state dependent on the ambient light that is detected. The first state, low-light, would exist when the enclosure is closed. Opening the enclosure in most environments would cause a different light condition that would result in a change in logic state from the sensor. The second method is to utilize a beam source directed at

the optical sensor with a barrier integrated into the enclosure that would either break or make the beam when the enclosure is tampered with, resulting in a change in logic state from the sensor. The third method also employs a beam, but utilizes a reflective surface integrated into the enclosure in such a way that the beam is normally directed back to the sensor, but if the enclosure is tampered with, the reflective surface would no longer direct the beam back to the sensor.

Motion sensors would detect unexpected, non-earthquake movement to the enclosure and cause a tamper fault. This could be a separate vibration sensor or switch (e.g. a mercury switch or similar). The integrated accelerometer for the earthquake detection circuitry 800 could also be utilized in this manner in addition to its earthquake detection role.

Alternatively, the network access hub 60 could exist not as a physical device but as a virtual machine. The core functions of the network access hub 60 would be integrated into software running on a computer. The hub transceiver 400 may either be a piece of dedicate hardware connected to the computer through a standard connection or as an "expansion card" for a standard bus-type (PCI, PCMCIA, etc.). The endpoint devices 50 could also be reconfigured to use a standard wireless networking configuration (e.g. Wi-Fi), in which case the computer could access its endpoint devices 50 through a standard wireless access point connected on a LAN/WAN or even directly through an integrated (or addon) wireless network adapter. The earthquake detection circuitry 800 could also exist as a piece of dedicated hardware attached to the computer, or it could exist as a separate device. This setup would provide a potential means for the user to access and control his or her own "subnet" of valves, sensors, or other endpoint devices over a network (e.g. Internet). When configured as part of the larger network, this virtual machine setup would be transparent to the central server. The message transactions between the virtual machine and the real hardware version of the network access hub 60 would be identical.

A typical application would see network access hubs 60 deployed in a "cellular" grid in a geographic area to maximize the wireless coverage for the endpoint devices 50. Within each grid, the endpoint devices 50 would be installed on main water and/or gas

supply lines to buildings. Software running in a central location would allow an authorized user to access each valve individually to open or close it as required.

Referring to Fig. 3, the system may also comprise a server 70 at a central location. The server communicates with the network access hubs 60 and comprises a network connection manager 80, a database 81, a database connection manager 82, and a client access manager 83.

The network access manager 80 maintains the routing information, authorization, and data encryption between the server 70 and the network access hubs 60. This communication may be through a network 71, which may be a public or private network. The network 71 may be the Internet, a WAN, a LAN, or some other form of network. It attempts to reestablish dropped connections and provides a listening port to which the network access hubs 60 can reconnect on their own.

The database connection manager 82 maintains a link to the database 81. It allows the user to use an existing database or to provide a new blank database. The database 81 cross-references system-specific data (valve/hub serial numbers, valve/hub relationships, etc.) with customer-specific information. This could include physical address of the location where the endpoint device 50 is installed, GPS co-ordinates (this information could also come directly from the endpoint device 50), customer name, customer account information (account number, billing, usage history, etc.)

The client access manager 83 authenticates clients attempting to log into the server 70 and restricts access to information or operations based on permissions.

The server 70 may also comprise core software that contains core operations for the server 70. It is "wrapped" by the network access manager 80, the database connection manager 82, and the client access manager 83 as a security measure to provide isolation from the outside world.

Preferably, the system further comprises client access software to provide a user interface for the end-user. It may include a graphical user interface to display information provided by the server 70, allow for control of the endpoint devices 50

and the network access hubs 60, and access the database 81. Different client applications can be developed for various platforms (PC, Mac, handheld computer, smart-phone, etc.) or for specific applications with limited functionality (e.g. emergency services).

A typical transaction would see a user log into the system from client software. After the user is authenticated, the user can retrieve information and perform operations on the endpoint devices 50 or access the database 81.

For example, if a user 72 wished to close a valve, the transaction would proceed as follows:

1. The user 72 would pull up a customer record from the database 81 and then issue a "close valve" command on this record.

2. The server 70 would pass this information to the network connection manager 80, which would pull the routing information from the database 81 and then issue the command across the network to the correct network access hub 60.

3. The network access hub 60 instructs the valve of the appropriate endpoint device 50 to close. When the valve is closed, it may report back to the network access hub 60, which reports back to the network access manager 80, which in turn passes it along to the server 70. The database 81 is updated, and the server 70 broadcasts an update message to all users logged in that the valve status has changed to closed.

An alternate network structure is illustrated in Fig. 4, where the server-hub-valve relationship is maintained, but remote open/close capabilities of the valve are also accessible by a local subnet of devices through a local interface 73 to automatically shut the valve off in an emergency, or to allow the user to open and close the valve whenever the service is not required as a safety and/or conservation measure. The local interface 73 may also incorporate an alarm monitoring panel interface so that it may be controlled by a third party monitoring company or configured to automatically close the valve when the alarm for the site is armed in "away" mode, and to

automatically reopen the valve when the alarm is disarmed. The local interface 73 may also be used to communicate and/or control local devices 74. Examples of local devices 74 would be fire alarms, carbon monoxide detectors, gas leak detectors, water leak sensors, etc. In this scenario, the server may maintain master control over the system and can override, or lock out, commands from local sources if required. This may be accomplished by giving instructions from the server with higher priority than instructions from the local devices 74.

A third network structure is illustrated in Fig. 5, where the server-hub-valve relationship is removed entirely, leaving each valve as separate network on its own. Each of the remote devices communicates only with the local interface in its own network, which in turn maintains operation of the valve. The network is simplified by removing the local interface and allows each remote device to communicate directly with the valve.

The present invention provides many advantages. The present invention allows a utility service to be controlled remotely. In addition, because of the client-server nature of the system, a unique client can be made that would allow emergency services personnel responding to a fire or other emergency the ability to shut off gas or water to a particular site or area. The client software would be granted a unique login/password by the owner of the system and would provide a limited amount of information. Typically, this information would be limited to the address, GPS co-ordinates (which could in-turn be used with other GPS software to provide routing information), and the ability to close the valve.

Furthermore, acting independently, each network access hub 60 can detect an earthquake and instruct all endpoint devices 50 under its control to shut. The alarm threshold would be set according to local jurisdictional requirements (e.g. ASCE 25-06). The network access hub 60 could also instruct other devices, such as horns, signal lights, or barriers to activate as well.

Alternatively, separate wireless devices incorporating earthquake detection could be paired with individual valves or a specific subset of valves relating to the same site. In this case, the valve(s) would respond only to its paired "earthquake detector" rather

than to a hub on the network.

The network access hubs 60, as part of a larger network, can communicate their "earthquake" status to the server 70. The server 70 can, in turn, make a decision based on the number or pattern of network access hubs 60 reporting in to instruct other network access hubs 60, which have not yet experienced the earthquake to automatically shut their valves or trigger signalling devices. Since earthquake waves have a finite speed as they propagate outward from the epicentre, but data transmission across a network is nearly instantaneous, the system can spread the message of the impending earthquake faster than the earthquake itself.

By incorporating metering equipment into the system, the network can monitor the usage of a utility (e.g. gas, water, oil, street lighting) at a location, and automatically restrict, or stop, service when a preset quota is reached. This quota can be daily, weekly, monthly, yearly, or arbitrarily set to match a billing cycle or other schedule. For example, a water utility in a desert community could set a daily limit on how much water a location can use, especially during times of drought. If a site reaches its daily quota, then the software can automatically stop service, or restrict the service to 10% to still allow for emergency usage (e.g. enough water to drink, but not enough to run appliances or water the garden). One scenario could see the utility have a soft quota and a hard quota. Reaching the soft quota would trigger a limited service, while reaching the hard quota would trigger a complete shutdown. When the quota period is over, the system would then automatically restore service to all sites that had previously violated the quota.

Furthermore, with metering equipment installed, the system can be set up so that the end customer prepays for its utility service. The software can be configured to provide an automated email, or other electronic message, to the customer when the prepaid service is nearly expired to remind them to prepay for more service, and automatically stop or limit service when the prepaid amount expires.

The system also can be set to provide service for a limited time by date and/or time, or it can be set to only provide service during preset time periods. For example, a construction site that requires gas service but only for a few days can have the service

automatically turned on at the start, and then automatically turned off a few days later automatically. Or a utility can offer a service to commercial sites where they would use the system to automatically shut off service after business hours, and restore it during business hours.

A local interface provides access to a singular valve, or specific valves. These valves would still be accessible to the utility over the network; however, through the use of a local interface, the enduser would also be granted a degree of control over his valves without affecting other nearby valves or devices on the main network. This feature can be locked out by the utility so that the customer would be unable to re-open a closed valve without the utility's consent. Sources of actuation could include gas-leak detection, fire alarms, carbon monoxide detection, water leak detection, earthquake detection, and remote opening/closing of device.

This allows the end-user to integrate a safety system at his or her site that takes advantage of the automatic open/close capabilities of the valve without impairing the utility's ability to control the level of service to that site. It also provides peace of mind by providing a means for the end-user to easily close his or her valve when the end-user leaves the site.

Alternatively, the network may be removed leaving the local interface and safety system as the sole controller for the valve. The local interface for the valve can also be integrated into each of the devices on the safety system, allowing each to access the valve independently.

It will be appreciated by those skilled in the art that the preferred and alternative embodiments have been described in some detail but that certain modifications may be practiced without departing from the principles of the invention.

## CLAIMS

1. A system for remotely operating endpoint devices, said system comprising:

a server;

one or more network access hubs, wherein each of said one or more network access hubs comprises:

a network interface for communication with said server over a network;

a microprocessor;

a hub transmitting means; and

a hub power supply; and

one or more endpoint devices, wherein each of said one or more endpoint devices comprises:

an endpoint receiving means for receiving wireless communications from said hub transmitting means of one or more of said network access hubs in wireless communications range, said wireless communications comprising instructions;

a microcontroller for processing said instructions and executing said instructions; and

an endpoint power supply.

2. The system of claim 1, wherein said hub transmitting means comprise a transceiver.

3. The system of claim 1, wherein said endpoint receiving means comprise a transceiver.

4. The system of claim 1, wherein one or more of said endpoint devices further comprise:

a valve motor for controlling one or more valves; and

a motor driver, wherein said motor driver receives electrical signals from said microcontroller upon execution of said instructions by said microcontroller and wherein said motor driver effects movement of said valve motor in accordance with said electric signals.

5. The system of claim 4, wherein said one or more valves restrict the flow of one of the following utility services: gas, oil, and water.

6. The system of claim 5, wherein said endpoint devices further comprise a valve position detection circuit to send data to said microcontroller regarding position of said one or more valves.

7. The system of claim 1, wherein one or more of said endpoint devices further comprise one or more of the following: sensors, meters, signaling devices, fans, and pumps.

8. The system of claim 1, wherein said one or more network access hubs further comprise an earthquake detection circuit, wherein said earthquake detection circuit sends an earthquake warning to said microprocessor upon detection of a possible earthquake.

9. The system of claim 1, wherein one or more of said endpoint devices further comprise an endpoint tamper detection circuit to send an endpoint tamper warning to said microcontroller upon detection of possible tampering with said endpoint device.

10. The system of claim 1, wherein one or more of said network access hubs further comprise a hub tamper detection circuit to send a hub tamper warning to said microprocessor upon detection of possible tampering with said network access hub.

11. The system of claim 1, wherein one or more of said endpoint devices further comprise a temperature sensor.

12. The system of claim 1, wherein said endpoint power supply comprises a battery.

13. The system of claim 12, wherein said endpoint device further comprises a battery management circuit to send a battery warning to said microcontroller upon detection of a possible failure of said battery.

14. The system of claim 1, wherein one or more of said network access hubs further comprise a backup power supply.

15. The system of claim 14, wherein said network access hubs further comprise a power management circuit to send a power warning to said microprocessor upon detection of a possible failure of said hub power supply or said backup power supply.

16. The system of claim 1, further comprising a database in communication with said server, said database storing information in relation to operation of said system.

17. The system of claim 1, wherein one or more of said endpoint devices comprises a light source for use in street lighting.

18. A method of remotely controlling endpoint devices, said method comprising the steps of:

a server communicating with one or more network access hubs through a network;

said one or more network access hubs wirelessly transmitting instructions to one or more endpoint devices through a hub transmitting means;

said one or more endpoint devices receiving said instructions from said network access hubs through an endpoint receiving means; and

said one or more endpoint devices implementing said instructions.

19. A method of controlling endpoint devices, said method comprising the steps of:

a server communicating with one or more network access hubs through a network;

said one or more network access hubs wirelessly transmitting instructions to one or more endpoint devices through a hub transmitting means;

said one or more endpoint devices receiving said instructions from said network access hubs through a endpoint receiving means;

said one or more endpoint devices receiving other instructions from a local interface connected to said endpoint devices;

said one or more endpoint devices implementing either said instructions or said other instructions, depending on priority of said instructions and said other instructions.

20. A method of remotely controlling a valve in an endpoint device in response to a possible earthquake, said method comprising the steps of:

a server communicating with a network access hub through a network;

said network access hub detecting a possible earthquake through an earthquake detection circuit;

said network access hub transmitting information regarding said possible earthquake to said server through said network;

said network access hub wirelessly transmitting instructions to said endpoint device through a hub transmitting means, said instructions comprising instructions regarding control of said valve in response to said possible earthquake;

said endpoint device receiving said instructions from said network access hub through an endpoint receiving means; and

said endpoint device controlling said valve in accordance with said instructions.

AMENDED CLAIMS
received by the International Bureau on 30 August 2010 (30.08.2010)

## CLAIMS

1. A system for remotely operating endpoint devices, said system comprising:

a server;

one or more network access hubs, wherein each of said one or more network access hubs comprises:

a network interface for communication with said server over a network;

a microprocessor;

a hub transmitting means;

an earthquake detection circuit, wherein said earthquake detection circuit sends an earthquake warning to said microprocessor upon detection of a possible earthquake; and

a hub power supply; and

one or more endpoint devices, wherein each of said one or more endpoint devices comprises:

an endpoint receiving means for receiving wireless communications from said hub transmitting means of one or more of said network access hubs in wireless communications range, said wireless communications comprising instructions;

a microcontroller for processing said instructions and executing said instructions; and

an endpoint power supply.

2. The system of claim 1, wherein said hub transmitting means comprise a transceiver.

3. The system of claim 1, wherein said endpoint receiving means comprise a transceiver.

4. The system of claim 1, wherein one or more of said endpoint devices further comprise:

a valve motor for controlling one or more valves; and

a motor driver, wherein said motor driver receives electrical signals from said microcontroller upon execution of said instructions by said microcontroller and wherein said motor driver effects movement of said valve motor in accordance with

said electric signals.

5. The system of claim 4, wherein said one or more valves restrict the flow of one of the following utility services: gas, oil, and water.

6. The system of claim 5, wherein said endpoint devices further comprise a valve position detection circuit to send data to said microcontroller regarding position of said one or more valves.

7. The system of claim 1, wherein one or more of said endpoint devices further comprise one or more of the following: sensors, meters, signaling devices, fans, and pumps.

8. (Cancelled)

9. The system of claim 1, wherein one or more of said endpoint devices further comprise an endpoint tamper detection circuit to send an endpoint tamper warning to said microcontroller upon detection of possible tampering with said endpoint device.

10. The system of claim 1, wherein one or more of said network access hubs further comprise a hub tamper detection circuit to send a hub tamper warning to said microprocessor upon detection of possible tampering with said network access hub.

11. The system of claim 1, wherein one or more of said endpoint devices further comprise a temperature sensor.

12. The system of claim 1, wherein said endpoint power supply comprises a battery.

13. The system of claim 12, wherein said endpoint device further comprises a battery management circuit to send a battery warning to said microcontroller upon detection of a possible failure of said battery.

14. The system of claim 1, wherein one or more of said network access hubs further comprise a backup power supply.

15. The system of claim 14, wherein said network access hubs further comprise a power management circuit to send a power warning to said microprocessor upon detection of a possible failure of said hub power supply or said backup power supply.

16. The system of claim 1, further comprising a database in communication with said server, said database storing information in relation to operation of said system.

17. The system of claim 1, wherein one or more of said endpoint devices comprises a light source for use in street lighting.

18. A method of remotely controlling endpoint devices, said method comprising the steps of:

a server communicating with one or more network access hubs through a network;

said one or more network access hubs wirelessly transmitting instructions to one or more endpoint devices through a hub transmitting means;

said one or more endpoint devices receiving said instructions from said network access hubs through an endpoint receiving means; and

said one or more endpoint devices implementing said instructions.

19. A method of controlling endpoint devices, said method comprising the steps of:

a server communicating with one or more network access hubs through a network;

said one or more network access hubs wirelessly transmitting instructions to one or more endpoint devices through a hub transmitting means;

said one or more endpoint devices receiving said instructions from said network access hubs through a endpoint receiving means;

said one or more endpoint devices receiving other instructions from a local interface connected to said endpoint devices;

said one or more endpoint devices implementing either said instructions or said other instructions, depending on priority of said instructions and said other instructions.

20. A method of remotely controlling a valve in an endpoint device in response to a possible earthquake, said method comprising the steps of:

a server communicating with a network access hub through a network;

said network access hub detecting a possible earthquake through an earthquake detection circuit;

said network access hub transmitting information regarding said possible earthquake to said server through said network;

said network access hub wirelessly transmitting instructions to said endpoint device through a hub transmitting means, said instructions comprising instructions regarding control of said valve in response to said possible earthquake;

said endpoint device receiving said instructions from said network access hub through an endpoint receiving means; and

said endpoint device controlling said valve in accordance with said instructions.

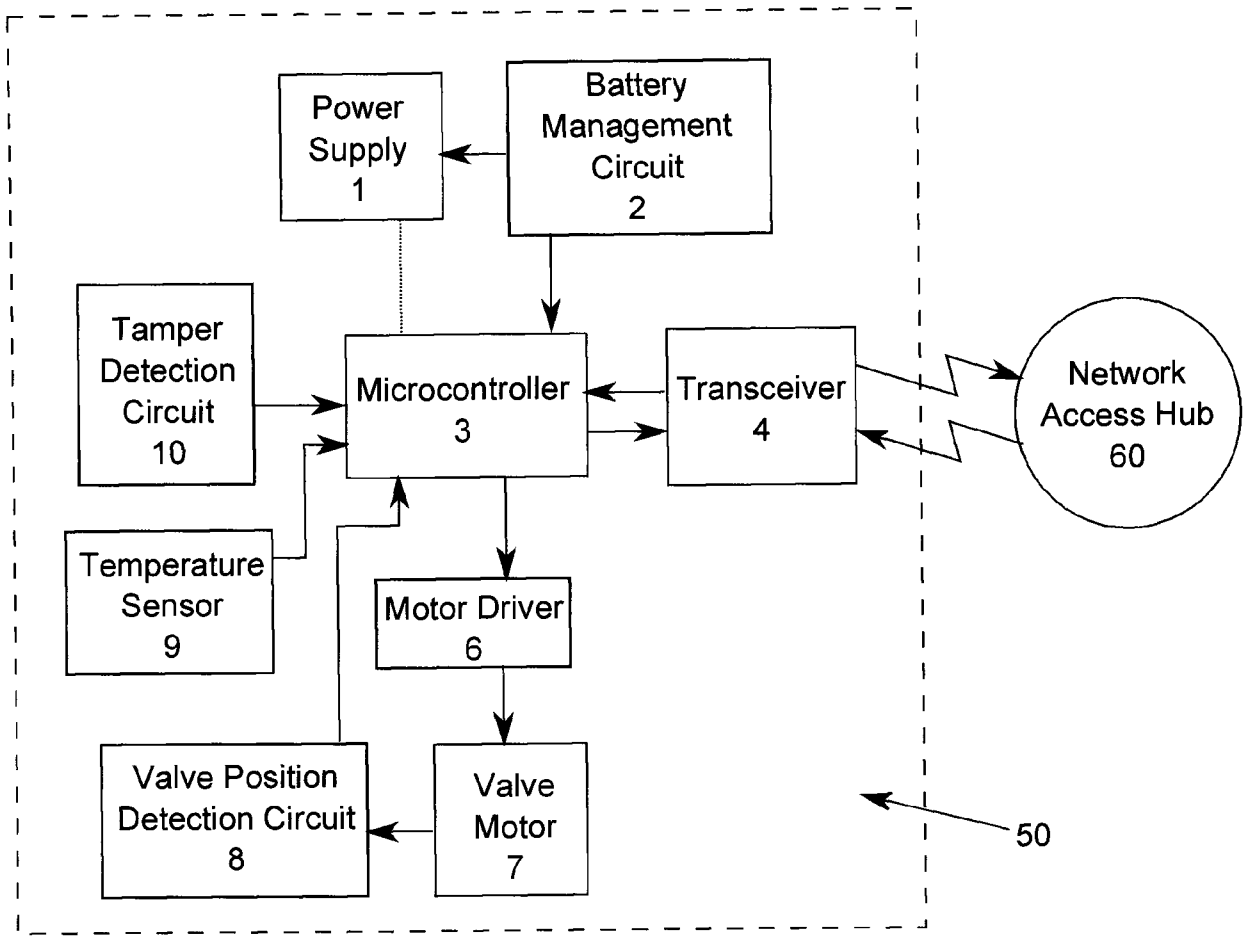
Power Supply 1
Battery Management Circuit 2
Tamper Detection Circuit 10
Microcontroller 3
Transceiver 4
Network Access Hub 60
Temperature Sensor 9
Motor Driver 6
Valve Position Detection Circuit 8
Valve Motor 7
50

Figure 1

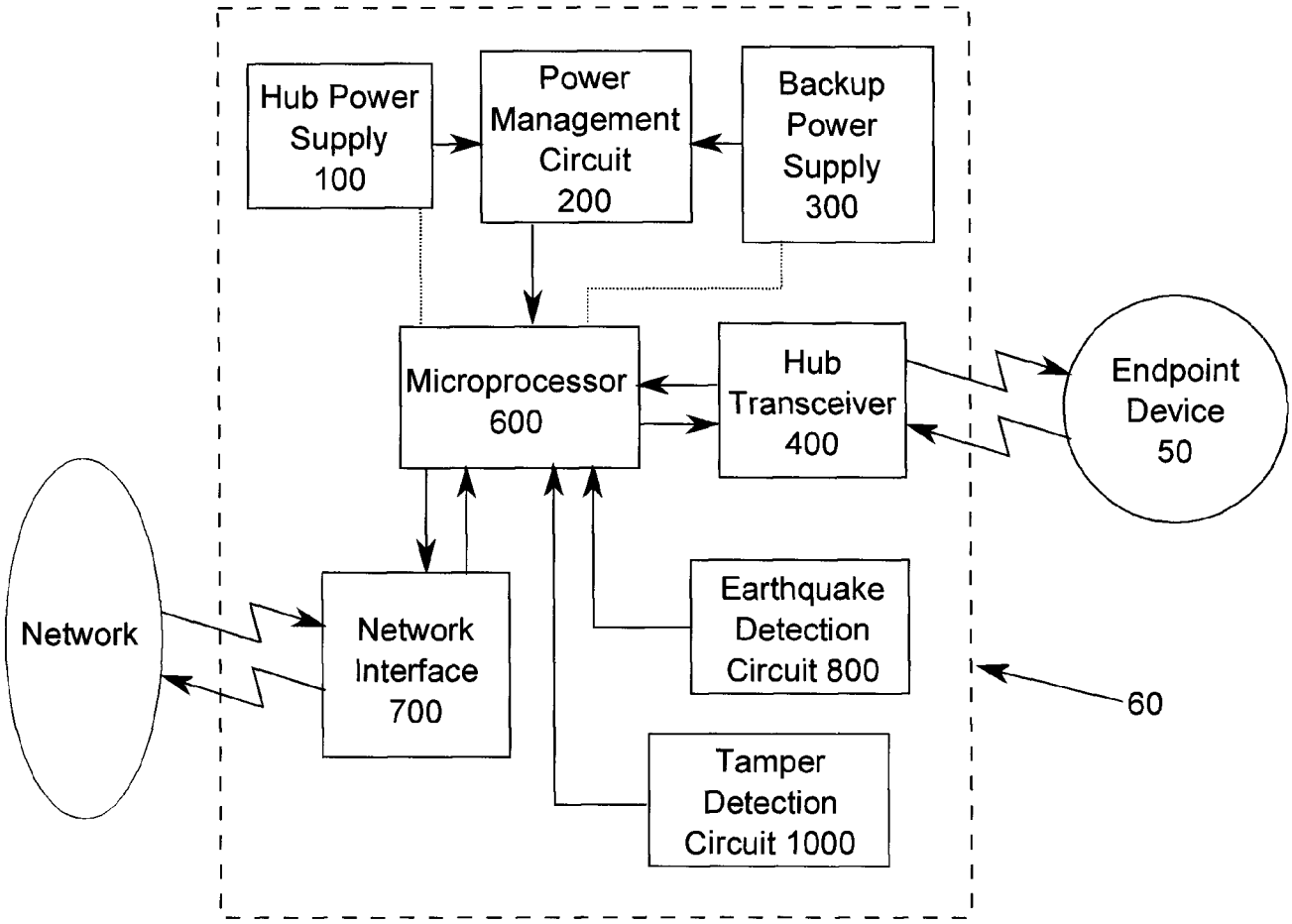
Hub Power Supply 100
Power Management Circuit 200
Backup Power Supply 300
Microprocessor 600
Hub Transceiver 400
Endpoint Device 50
Network
Network Interface 700
Earthquake Detection Circuit 800
Tamper Detection Circuit 1000
60

Figure 2

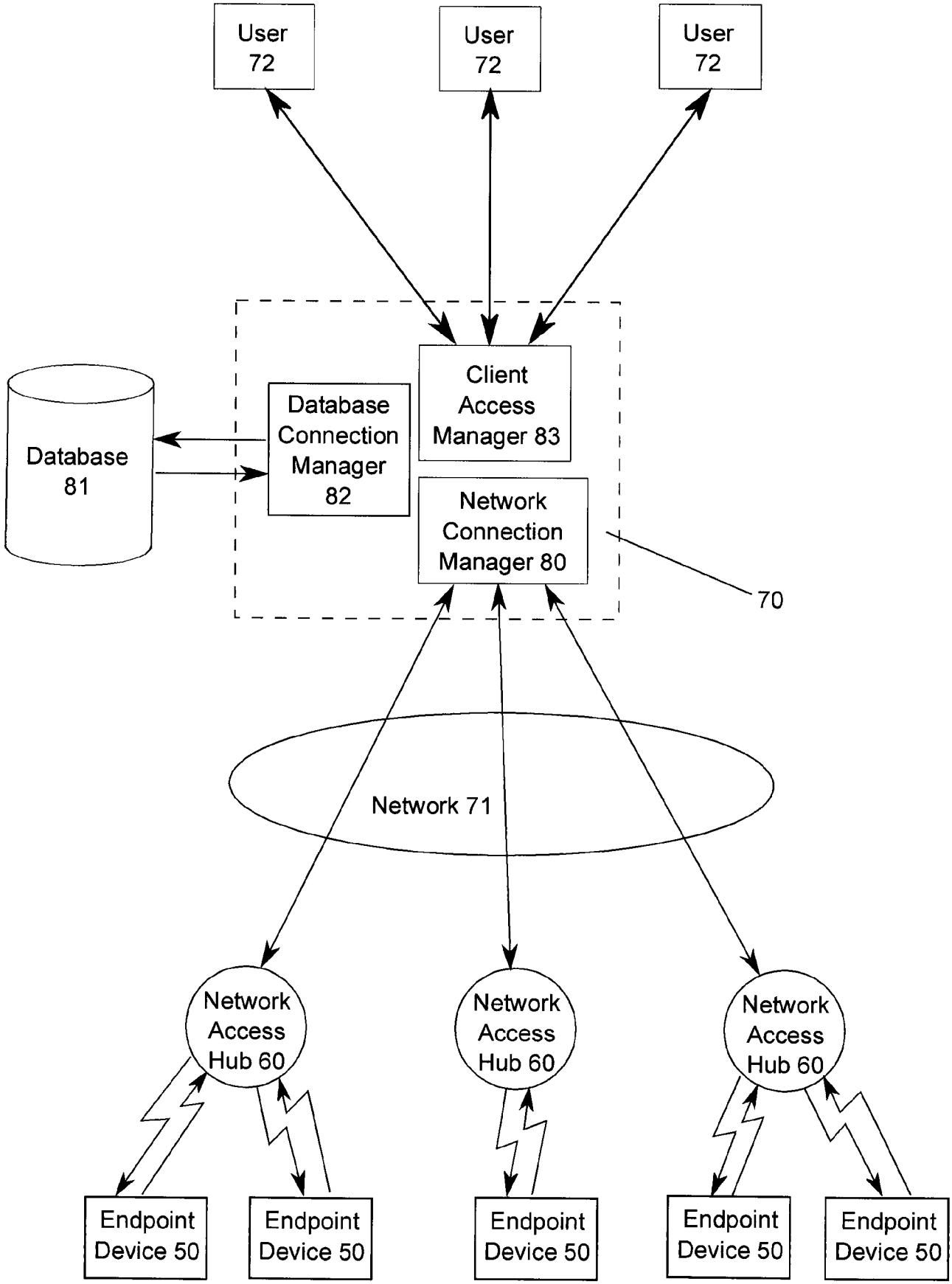
User 72
User 72
User 72
Client Access Manager 83
Database Connection Manager 82
Database 81
Network Connection Manager 80
70
Network 71
Network Access Hub 60
Network Access Hub 60
Network Access Hub 60
Endpoint Device 50
Endpoint Device 50
Endpoint Device 50
Endpoint Device 50
Endpoint Device 50

Figure 3

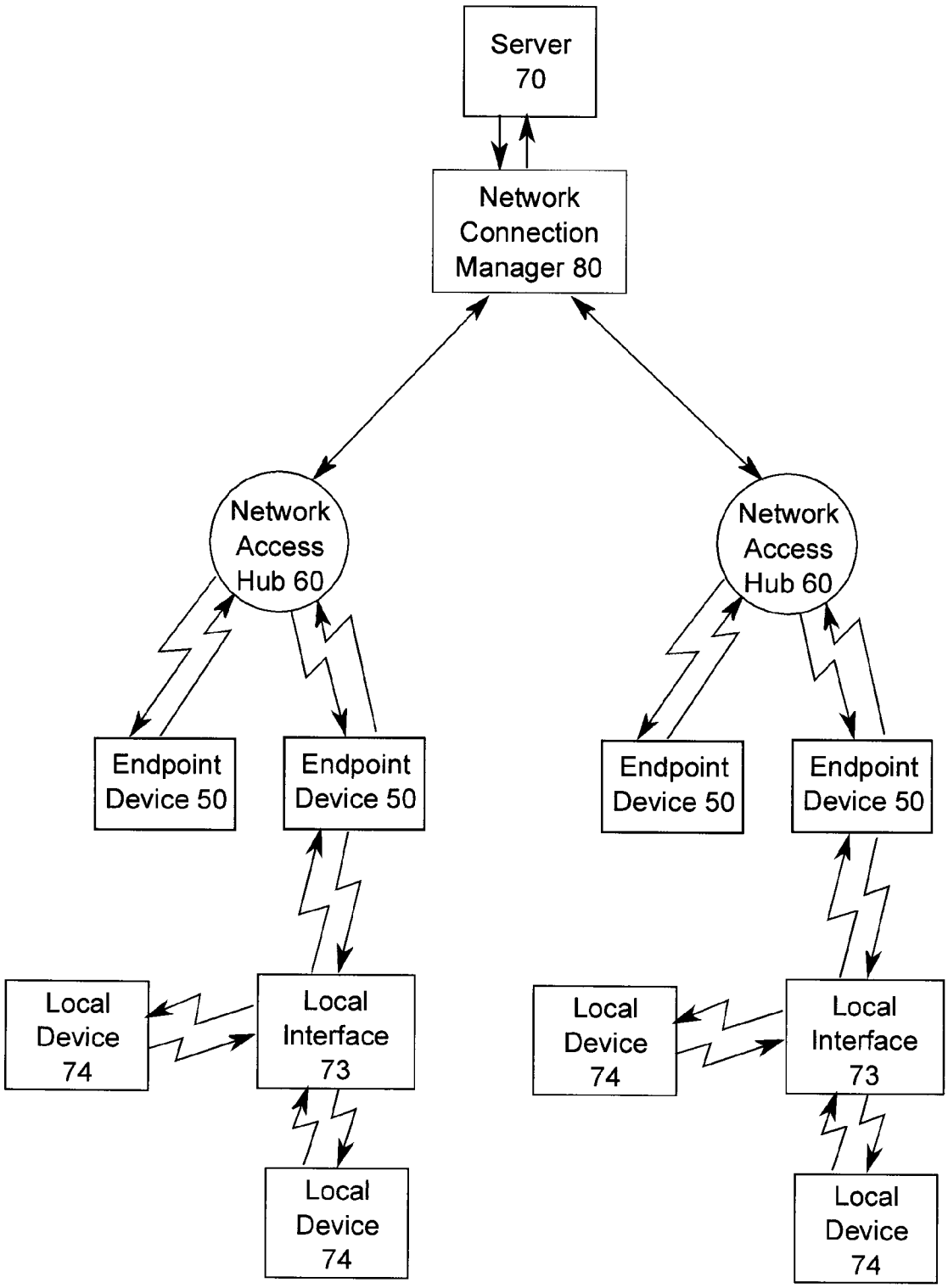
Server 70
Network Connection Manager 80
Network Access Hub 60
Network Access Hub 60
Endpoint Device 50
Endpoint Device 50
Endpoint Device 50
Endpoint Device 50
Local Device 74
Local Interface 73
Local Device 74
Local Interface 73
Local Device 74
Local Device 74

Figure 4

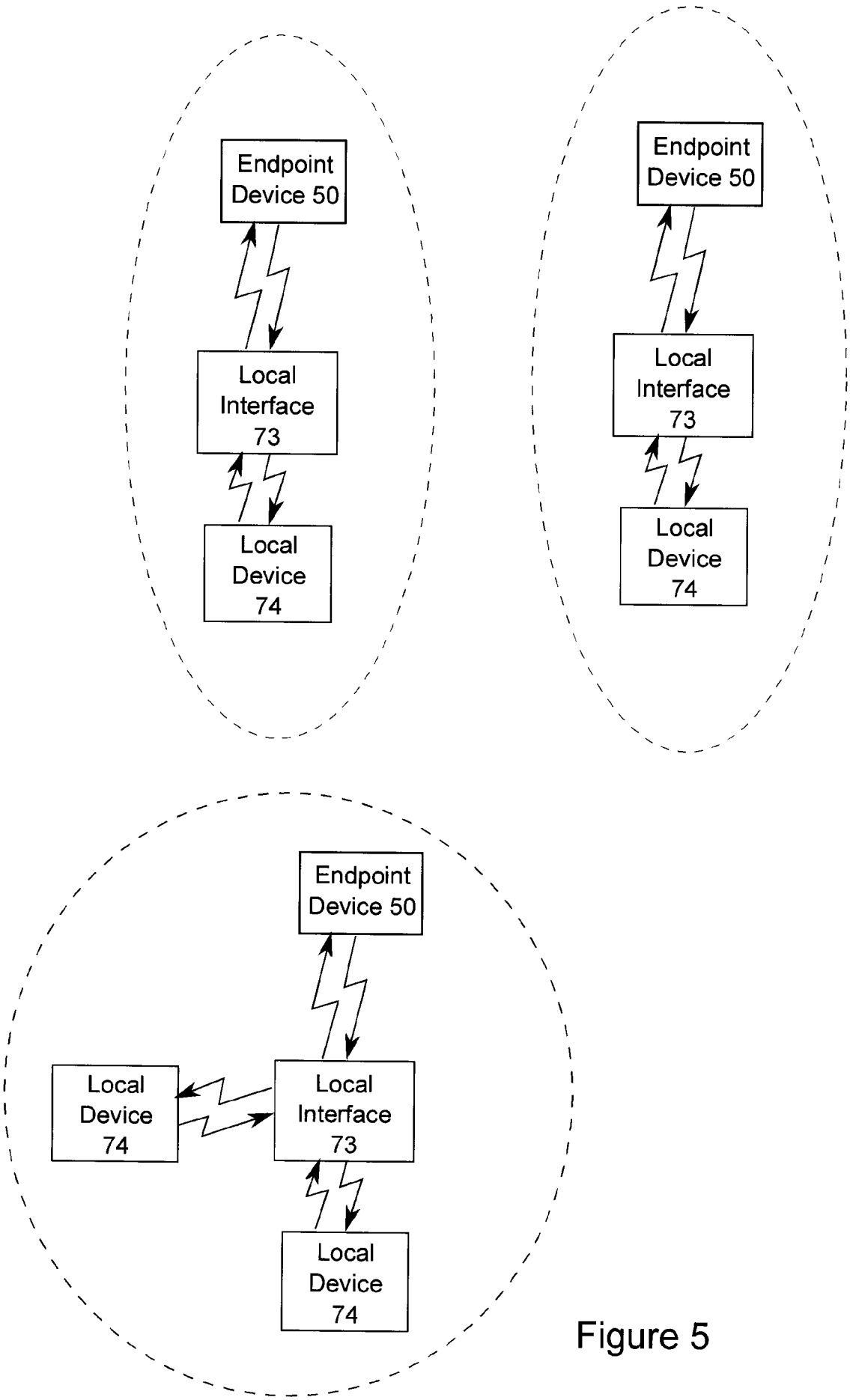
Endpoint Device 50
Local Interface 73
Local Device 74
Endpoint Device 50
Local Interface 73
Local Device 74
Endpoint Device 50
Local Device 74
Local Interface 73
Local Device 74

Figure 5

**INTERNATIONAL SEARCH REPORT**

International application No.
PCT/CA2009/001433

A. CLASSIFICATION OF SUBJECT MATTER

IPC: ***G08C 17/00*** (2006.01) , ***G05D 7/06*** (2006.01) , ***H02J 7/00*** (2006.01) , ***H02J 9/00*** (2006.01) , ***H04W 84/18*** (2009.01) , *H04W 4/00* (2009.01)

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 (2006.01): G08C, G05D, H02J, H04W

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

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

Canadian patent database, IEEE Xplore, Delphion: system, remote control, operating, endpoint, device, meter, valve, utility, service, server, network access hub, wireless, instructions, control, operation, earthquake, tamper, detection circuits, automatic control, gas, oil, water, emergency shut-off, rationing, prepaid, intermittent, network interface, microprocessor, power supply, position detection, tamper detection, temperature sensor, broadcast command, database, memory, light source, power failure, battery management, monitor, telemetry, data collection, mesh network, local interface and all such related terms.

C. DOCUMENTS CONSIDERED TO BE RELEVANT

| Category* | Citation of document, with indication, where appropriate, of the relevant passages | Relevant to claim No. |
|---|---|---|
| X<br>---<br>Y | US 2007/ 063866 A1 WEBB 22 March 2007 (22-03-2007)<br><br>Paragraphs 14, 81 to 83, 86 to 99, 102 to 107, 112, 113, 116, 119, 131, 132, 140 to 156, 161 to 163, 165, 168, 171 to 175, Claims 1 to 8 and Figures 1 to 6 | 1 to 16, 18, 20<br>---<br>17, 19 |
| X<br>---<br>Y | US 2007/284293 A1 PITCHFORD et al. 13 December 2007 (13-12-2007)<br><br>Paragraphs 24 to 29, 31, 34 to 37, 47, 51 to 53, 55, 56, Claims 1 to 20 and Figures 1, 2, 4, 5, 10 | 1 to 7, 11 to 16, 18<br>---<br>8, 9, 10, 17, 19, 20 |
| Y | US 4414994 A HOGAN 15 November 1983 (15-11-1983)<br><br>Columns 1 to 4, Claims 1 to 7 and Figures 1 to 3 | 8, 20 |

[ ] Further documents are listed in the continuation of Box C. [X] See patent family annex.

* Special categories of cited documents :

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

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

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

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

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

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

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

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

"&" document member of the same patent family

| Date of the actual completion of the international search | Date of mailing of the international search report |
|---|---|
| 28 January 2010 (28-01-2010) | 17 February 2010 (17-02-2010) |

| Name and mailing address of the ISA/CA | Authorized officer |
|---|---|
| Canadian Intellectual Property Office<br>Place du Portage I, C114 - 1st Floor, Box PCT<br>50 Victoria Street<br>Gatineau, Quebec K1A 0C9<br>Facsimile No.: 001-819-953-2476 | Salvatore Ginese (819) 934-4888 |

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

| Category* | Citation of document, with indication, where appropriate, of the relevant passages | Relevant to claim No. |
|---|---|---|
| Y | WO 01/ 82028 A2 DUNCAN et al. 01 November 2001 (01-11-2001)<br><br>Page 7, lines 15-24, page 11, lines 6-9, Claim 1 and Figure 2 | 9, 10 |
| Y | WO 00/39770 A1 MORAND 06 July 2000 (06-07-2000)<br><br>Entire document | 9, 10 |
| Y | EP 1192793 B1 CROOKHAM et al. 27 October 2004 (27-10-2004)<br><br>Claims 1, 6 to 8 | 17<br><br>1 to 20 |
| A | WO 2009/143287 A1 SABERI et al. 26 November 2009 (26-11-2009)<br><br>Entire document | 1 to 20 |
| A | US 2009/096605 A1 PETITE et al. 16 April 2009 (16-04-2009)<br><br>Entire document | 1 to 20 |
| | WO 03/088737 A1 CROFT 30 October 2003 (30-10-2003)<br><br>Entire document | |

| Patent Document Cited in Search Report | Publication Date | Patent Family Member(s) | Publication Date |
|---|---|---|---|
| US2007063866A1 | 22-03-2007 | None | |
| US2007284293A1 | 13-12-2007 | CA2653092A1 | 21-12-2007 |
| | | EP2032231A2 | 11-03-2009 |
| | | MX2008015316A | 02-03-2009 |
| | | US7605485B2 | 20-10-2009 |
| | | US2008143109A1 | 19-06-2008 |
| | | US2009058088A1 | 05-03-2009 |
| | | WO2007146121A2 | 21-12-2007 |
| | | WO2007146121A3 | 24-04-2008 |
| US4414994A | 15-11-1983 | None | |
| WO0182028A2 | 01-11-2001 | AU5564801A | 07-11-2001 |
| | | AU7784401A | 07-11-2001 |
| | | CA2407512A1 | 01-11-2001 |
| | | EP1390578A2 | 25-02-2004 |
| | | US6551583B2 | 22-04-2003 |
| | | US6670810B2 | 30-12-2003 |
| | | US2002043969A1 | 18-04-2002 |
| | | US2002044954A1 | 18-04-2002 |
| | | WO0181248A2 | 01-11-2001 |
| | | WO0181248A3 | 04-04-2002 |
| | | WO0182028A3 | 11-12-2003 |
| WO0039770A1 | 06-07-2000 | AU5246399A | 31-07-2000 |
| | | CA2353631A1 | 06-07-2000 |
| | | EP1147503A1 | 24-10-2001 |
| | | EP1147503A4 | 09-07-2003 |
| | | US6232886B1 | 15-05-2001 |
| EP1192793B1 | 27-10-2004 | AU780583B2 | 07-04-2005 |
| | | AU5908900A | 22-01-2001 |
| | | AU2005211531A1 | 13-10-2005 |
| | | CA2378318A1 | 11-01-2001 |
| | | CA2378318C | 23-05-2006 |
| | | EP1192793B1 | 27-10-2004 |
| | | GB0200060D0 | 20-02-2002 |
| | | GB2371394A | 24-07-2002 |
| | | US6681110B1 | 20-01-2004 |
| | | US2004056775A1 | 25-03-2004 |
| | | WO0103414A1 | 11-01-2001 |
| | | WO0103414A9 | 09-08-2001 |
| WO2009143287A1 | 26-11-2009 | None | |

| | | | |
|---|---|---|---|
| US2009096605A1 | 16-04-2009 | AT352805T | 15-02-2007 |
| | | AU777215B2 | 07-10-2004 |
| | | AU1604601A | 06-06-2001 |
| | | AU2474901A | 06-09-2001 |
| | | AU3592300A | 04-10-2000 |
| | | AU7924101A | 18-02-2002 |
| | | AU7924901A | 18-02-2002 |
| | | AU8121401A | 18-02-2002 |
| | | AU8475901A | 18-02-2002 |
| | | BR0015528A | 25-02-2003 |
| | | CA2338388A1 | 01-09-2001 |
| | | CA2391372A1 | 17-05-2001 |
| | | CA2434642A1 | 26-09-2002 |
| | | DE60033178D1 | 15-03-2007 |
| | | DE60033178T2 | 15-11-2007 |
| | | EP1169690A2 | 09-01-2002 |
| | | EP1236075A2 | 04-09-2002 |
| | | EP1236075A4 | 28-07-2004 |
| | | EP1236075B1 | 24-01-2007 |
| | | EP1370958A1 | 17-12-2003 |
| | | EP1370958A4 | 15-04-2009 |
| | | FR2805897A1 | 07-09-2001 |
| | | FR2805897B1 | 08-12-2006 |
| | | GB0104849D0 | 18-04-2001 |
| | | GB2365529A | 20-02-2002 |
| | | GB2365529B | 10-03-2004 |
| | | MXPA02004732A | 14-10-2003 |
| | | MXPA03005348A | 20-04-2004 |
| | | US5926531A | 20-07-1999 |
| | | US6028522A | 22-02-2000 |
| | | US6218953B1 | 17-04-2001 |
| | | US6233327B1 | 15-05-2001 |
| | | US6430268B1 | 06-08-2002 |
| | | US6437692B1 | 20-08-2002 |
| | | US6522974B2 | 18-02-2003 |
| | | US6618578B1 | 09-09-2003 |
| | | US6628764B1 | 30-09-2003 |
| | | US6747557B1 | 08-06-2004 |
| | | US6836737B2 | 28-12-2004 |
| | | US6891838B1 | 10-05-2005 |
| | | US6914533B2 | 05-07-2005 |
| | | US6914893B2 | 05-07-2005 |
| | | US7053767B2 | 30-05-2006 |
| | | US7079810B2 | 18-07-2006 |
| | | US7103511B2 | 05-09-2006 |
| | | US7137550B1 | 21-11-2006 |
| | | US7209840B2 | 24-04-2007 |
| | | US7263073B2 | 28-08-2007 |
| | | US7295128B2 | 13-11-2007 |
| | | US7346463B2 | 18-03-2008 |
| | | US7397907B2 | 08-07-2008 |
| | | US7468661B2 | 23-12-2008 |
| | | US7650425B2 | 19-01-2010 |
| | | US2001002210A1 | 31-05-2001 |
| | | US2001024163A1 | 27-09-2001 |
| | | US2002010545A1 | 24-01-2002 |
| | | US2002012323A1 | 31-01-2002 |
| | | US2002013679A1 | 31-01-2002 |
| | | US2002019712A1 | 14-02-2002 |
| | | US2002019725A1 | 14-02-2002 |
| | | US2002027504A1 | 07-03-2002 |
| | | US2002031101A1 | 14-03-2002 |
| | | US2002125998A1 | 12-09-2002 |
| | | US2003067889A1 | 10-04-2003 |
| | | US2004053639A1 | 18-03-2004 |
| | | US2004183687A1 | 23-09-2004 |
| | | US2005043059A1 | 24-02-2005 |
| | | US2005190055A1 | 01-09-2005 |
| | | US2005201397A1 | 15-09-2005 |

| | | | |
|---|---|---|---|
| | | US2005243867A1 | 03-11-2005 |
| | | US2006181406A1 | 17-08-2006 |
| | | US2007208521A1 | 06-09-2007 |
| | | US2009068947A1 | 12-03-2009 |
| | | US2009243840A1 | 01-10-2009 |
| | | WO0055825A1 | 21-09-2000 |
| | | WO0055825A8 | 15-03-2001 |
| | | WO0135190A2 | 17-05-2001 |
| | | WO0135190A3 | 13-12-2001 |
| | | WO0135190B1 | 10-01-2002 |
| | | WO0213036A1 | 14-02-2002 |
| | | WO0213412A1 | 14-02-2002 |
| | | WO0213413A1 | 14-02-2002 |
| | | WO0213413A8 | 11-07-2002 |
| | | WO0213414A1 | 14-02-2002 |
| | | WO02075565A1 | 26-09-2002 |
| WO03088737A1 | 30-10-2003 | AU2003224867A1 | 03-11-2003 |
| | | CA2475980A1 | 30-10-2003 |
| | | CA2475980C | 15-04-2008 |
| | | EP1496736A1 | 19-01-2005 |
| | | EP1496736A4 | 20-08-2008 |
| | | US6491062B1 | 10-12-2002 |