



Office de la Propriété
Intellectuelle
du Canada

Un organisme
d'Industrie Canada

Canadian
Intellectual Property
Office

An agency of
Industry Canada

CA 2896417 A1 2014/07/03

(21) **2 896 417**

(12) **DEMANDE DE BREVET CANADIEN**
CANADIAN PATENT APPLICATION

(13) **A1**

(86) **Date de dépôt PCT/PCT Filing Date:** 2013/12/26
(87) **Date publication PCT/PCT Publication Date:** 2014/07/03
(85) **Entrée phase nationale/National Entry:** 2015/06/25
(86) **N° demande PCT/PCT Application No.:** IB 2013/061334
(87) **N° publication PCT/PCT Publication No.:** 2014/102726
(30) **Priorité/Priority:** 2012/12/26 (US61/745,833)

(51) **Cl.Int./Int.Cl. G06F 19/00** (2011.01)

(71) **Demandeur/Applicant:**
KONINKLIJKE PHILIPS N.V., NL

(72) **Inventeurs/Inventors:**
GUINEY, PATRICK, NL;
ILLIKKAL, MASHOOD PUTHAN BEETIL, NL;
GRUBE, WILLIAM DOUGLAS, NL;
LANDER, TODD, NL

(74) **Agent:** SMART & BIGGAR

(54) **Titre : MONITEUR, DEFIBRILLATEUR ET SERVEUR DE TELEMEDECINE**

(54) **Title: MONITOR DEFIBRILLATOR TELEMEDICINE SERVER**

(57) Abrégé/Abstract:

A system and device (200) which combines a defibrillator, patient monitor and a telemedicine server is described. The device enables a method whereby an external system or remote station may "pull" data from the device without the need for operator action or intervention. Safety-critical and non-safety-critical features in the device (200) are maintained separate by a firewall circuit (240) such that the remote station cannot write data to the device.

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

(19) World Intellectual Property Organization
International Bureau



(10) International Publication Number

WO 2014/102726 A1

(43) International Publication Date
3 July 2014 (03.07.2014)

(51) International Patent Classification:
G06F 19/00 (2011.01)

(21) International Application Number:
PCT/IB2013/061334

(22) International Filing Date:
26 December 2013 (26.12.2013)

(25) Filing Language:
English

(26) Publication Language:
English

(30) Priority Data:
61/745,833 26 December 2012 (26.12.2012) US

(71) Applicant: KONINKLIJKE PHILIPS N.V. [NL/NL];
High Tech Campus 5, NL-5656 AE Eindhoven (NL).

(72) Inventors: GUINEY, Patrick; c/o High Tech Campus 5, NL-5656 AE Eindhoven (NL). ILLIKKAL, Mashhood Puthan Beetil; c/o High Tech Campus 5, NL-5656 AE Eindhoven (NL). GRUBE, William Douglas; c/o High Tech Campus 5, NL-5656 AE Eindhoven (NL). LANDER, Todd; c/o High Tech Campus 5, NL-5656 AE Eindhoven (NL).

(74) Agents: STEFFEN, Thomas et al.; High Tech Campus Building 5, NL-5656 AE Eindhoven (NL).

(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, BN, 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, IR, IS, JP, KE, KG, 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, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, 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, LR, LS, MW, MZ, NA, RW, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ, TM), European (AL, 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, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

Published:

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



WO 2014/102726 A1

(54) Title: MONITOR DEFIBRILLATOR TELEMEDICINE SERVER

(57) Abstract: A system and device (200) which combines a defibrillator, patient monitor and a telemedicine server is described. The device enables a method whereby an external system or remote station may "pull" data from the device without the need for operator action or intervention. Safety-critical and non-safety-critical features in the device (200) are maintained separate by a firewall circuit (240) such that the remote station cannot write data to the device.

Monitor Defibrillator Telemedicine Server

[0001] The invention relates to an improved apparatus and method for obtaining patient data from a monitor defibrillator for use at a remote station. The monitor defibrillator is integrated with a telemedicine server, such that external systems may use a standard communications interface and a read-only communications protocol to obtain the data.

[0002] Monitor defibrillators collect clinical data from a wide spectrum of patients that span the range from healthy to critically ill. Many such monitor defibrillators are employed by emergency medical system (EMS) caregivers at locations away from healthcare facilities. It is widely acknowledged that patient outcomes are improved when the clinical data collected by EMS is transmitted to the healthcare facility before the arrival of the patient.

[0003] Transmission of clinical data from monitor defibrillators to healthcare facilities serves multiple purposes. The transmission alerts the care facility to the clinical condition of the incoming patient. Sharing of the data allows consultation between the field medic and the caregiver at the care facility. Also, routine transmission of clinical data to a central location enables the assembly and archival storage of electronic patient care records (ePCRs).

[0004] Recent healthcare reform efforts have also prompted a greater emphasis on the need for EMS caregivers to manage and transmit the data associated with EMS patient care. Accurate and comprehensive patient care records are acknowledged to be a prerequisite for improved accountability of quality care, more efficient billing

procedures, and reduced litigation that results from medical responses that have negative outcomes.

[0005] The necessity to transmit patient data from the patient's location to a central location at the hospital has given rise to a number of medical devices having integrated telemetry circuits. U.S. Pat. Publication No. 2007/0255120A1, entitled "Internet-Protocol Based Telemetry Patient Monitoring System ", published on November 1, 2007 to Roznov, describes such a standard patient telemetry system. Roznov, as illustrated in FIGURE 1, describes a system having a plurality of portable telemetry devices 12-18 which are in wireless communication with an access point 20. Portable telemetry devices 12-18 transact IP data packets, bi-directionally, with an information system 22 via a connection 24 of the wired network. The data packets are typically real-time physiological and control information.

[0006] Portable telemetry devices 12-18 communicate with devices, e.g., tablet PC 26 on the wired network, e.g., via connection 28, through an access point 20. An optional access point controller 34 controls and directs the signals through access point 20 via a connection 32.

[0007] A similar invention is described in International Publication WO 03/025826A2, entitled "Health Monitoring System", published on 27 March 2003 to Gordner et al. There, a patient monitoring system is comprised of patient monitors 2 which are in wireless communication with a centralized application server 1, which stores the patient data for access by multiple workstations 4. The patient monitor could be associated with a defibrillator.

[0008] Another similar monitoring invention is described in International Publication WO 2006/071711, entitled "Providing Data Destination Information to a Medical Device", published on 6 July 2006 to Moore et al. Moore et al. teach a medical device which may be configured to transmit medical event information to a selected data destination. Prior to transmission, the user must select and initiate the data transmission in a "push" fashion. The Moore et al. medical device may be an external defibrillator.

[0009] An invention which incorporates both a medical device part and a separate communication part within the same housing is described in U.S. Patent Publication 2010/0250697, entitled "Portable Device and Method of Communication Medical Data Information", published on 30 September, 2010 to Hansen et al. The Hansen et al. circuit is intended to separate the complex communications functionality from the critical medical application. The medical device part controls all data flow between it and the communication part.

[0010] Another firewall-related invention is described in U.S. Patent Publication 2006/190999A1, entitled "Method and Apparatus for Two-Way Transmission of Medical Data", published on 24 August 2006 to Chen et al. Chen et al. teach a secure firewall located between a healthcare provider and a third party for securely sharing patient image data between the two. The firewall is designed to allow bidirectional data flow with a push-pull control mechanism.

[0011] Each of the afore-described references operates in a similar manner. Each offers a circuit design and associated user interface which is relatively complicated and therefore suboptimal. In particular, the user of each medical monitoring device must take specific action to set-up and/or configure the device to "push" data from the device to the remote

station. Each referenced device requires the operator to either set up the monitor defibrillator circuitry to transmit to a chosen location in a chosen format, or must initiate the transmission itself via the user interface. These systems and methods may be appropriate for use in a clinical diagnostic environment, but they are distracting and potentially confusing during an urgent cardiac patient treatment protocol where every moment saved improves the chance for a positive patient outcome. Actions necessary to collect and transmit patient data may divert attention away from the immediate patient care steps, and can introduce a potential for error in either the transmission or the rescue. Third, the recited references each require custom interface software residing both at the device and at the remote station in order to reconcile both sides of the data link and to decode the clinical data from the patient medical device. The interface is expensive to develop and certify for medical use, which must be repeated each time that the interface is modified to meet evolving communications standards. The custom interface software also holds patient data in a customized format which is optimized to the system. Unless the external system contains the same software, the data cannot be read.

[0012] Thus what is needed is a method and apparatus for easily sharing patient information obtained by a medical device such as a monitor defibrillator with external systems in a way which avoids the problems presented by the prior art.

[0013] In accordance with the principles of the present invention, an improved medical device apparatus is described which consists of a medical monitor defibrillator having an integrated telemedicine server. The apparatus includes a patient monitoring circuit and defibrillation therapy circuit which collect patient data and convey it to a clinical processor. A memory receives the patient data from the clinical processor and stores the

received patient data in a generic file format. A communications interface is disposed in read-only communication with the memory and transmits the patient data to a remote station. A firewall circuit prevents the writing of any data received from the communications interface to the memory. Each of the circuit elements is contained in a unitary housing.

[0014] Also in accordance with the principles of the present invention, a system is described which comprises a monitor defibrillator having an integrated telemedicine server in communications with a transceiver located at a remote station. The system is disposed such that the telemedicine server transmits the patient data to the remote station in response to a request for data from the remote station, i.e. in a “pull” method of data flow. The system thus enables the transmission of data without the need for the operator’s action or intervention. By arranging the data stored in the isolated telemedicine server memory via a standard communications interface and in a generic format, the need for customized software to interface with the device and decode the data is eliminated. Lower cost and greater reliability are thus realized.

[0015] Also in accordance with the principles of the present invention is an improved method for transferring patient data from a monitor defibrillator telemedicine server having a patient monitoring circuit and a defibrillation therapy circuit to a remote station using a system similar to that described above. The method includes a step of transmitting the patient data from the telemedicine server to the remote station automatically in response to a request from the remote station.

[0016] The scope of the invention encompasses medical devices having communications capabilities. In particular, devices such as in-hospital monitor defibrillators used by

hospital personnel but separated from a central server and pre-hospital monitor defibrillators used by emergency medical services (EMS) personnel at locations remote from the hospital may benefit from the inventive features.

[0017] Another object of the invention is to describe generally a defibrillator monitor which performs non-safety-critical applications and safety-critical applications together, without affecting the safety, reliability and performance of the safety critical functions. Safety critical functions of a defibrillator monitor device include providing critical therapy to a patient (e.g., pacing, CPR and defibrillation therapy) and/or monitoring of a patient (e.g., ECG, blood monitoring such as oxygenation, carbon dioxide and pressure). Non-safety-critical functions and applications include electronic patient care record (ePCR) applications, event summary review and post event analysis. In particular, the invention employs a multi-core processor which runs both functions. A real time operating system (RTOS) and the memory management unit (MMU) run on separate cores of the multi-core processor. Non-safety critical functions run on different cores of the multi-core processor. Thus is established a secure firewalled separation between safety-critical and non-safety critical functions.

[0018] IN THE DRAWINGS:

[0019] FIGURE 1 illustrates a medical patient telemetry system according to the prior art.

[0020] FIGURE 2 illustrates a block diagram of a defibrillator monitor telemedicine server according to a preferred embodiment of the invention.

[0021] FIGURE 3 illustrates one embodiment of a patient data file storage system for use with the defibrillator monitor telemedicine server according to a preferred embodiment of

the invention.

[0022] FIGURE 4 is an external view of a defibrillator monitor telemedicine server according to an embodiment of the invention.

[0023] FIGURE 5 illustrates a block diagram of a defibrillator monitor telemedicine server and remote station system according to another embodiment of the invention.

[0024] FIGURE 6 illustrates a flow chart showing a preferred embodiment of the inventive method.

[0025] FIGURE 7 illustrates a firewall circuit in which safety-critical and non-safety-critical functions within a device such as a defibrillator monitor telemedicine server are shared within a common multi-core processor, according to one embodiment of the invention.

[0026] Now turning to the illustrations, FIGURE 2 is a functional block diagram of an exemplary defibrillator monitor telemedicine server 200 of the present invention. Certain functional portions of the defibrillator monitor telemedicine server 200 are defined as safety-critical, which generally consists of hardware and software that relate directly to patient care. Safety-critical features include those circuits used directly for sensing and monitoring a patient's condition. Electrocardiogram (ECG), heart rate, blood pressure and oxygenation, and respiration monitoring are such examples. Safety-critical features also include those circuits used to provide therapy to the patient. Cardiac defibrillation and pacing circuits are such examples. Because the failure of a safety-critical circuit can lead to a patient's injury or death, safety-critical circuits must comply with heightened standards of reliability, performance, and security in their design and manufacture.

[0027] Defibrillator monitor telemedicine server 200 also includes functional portions that are non-safety critical. Functions such as electronic patient care record applications, event summary review data storage, and post event analysis circuits do not directly affect patient care. Non-safety critical functions generally require a lessened rigor in their design performance and manufacture.

[0028] The main elements of the defibrillator monitor telemedicine server 200 shown in FIGURE 2 include a clinical processor 210 which obtains patient and event data from a patient monitoring circuit 202 and a defibrillation therapy circuit 204, an isolable memory 220, a firewall circuit 240, and a communications interface 230 that provides read-only access for external systems to read clinical data stored in memory 220. FIGURE 2 is not intended to depict or preclude any specific hardware or software implementation.

[0029] In the FIGURE 2 embodiment, the safety-critical portions of defibrillator monitor telemedicine server 200 include a patient monitoring circuit 202, a defibrillation therapy circuit 204, and a clinical processor circuit 210. The patient monitoring circuit 202 includes sensors which obtain patient medical parameters, generally in real time, and communicate the obtained data to the clinical processor 210 via a patient monitoring data path 206. The defibrillation therapy circuit 204 provides defibrillation and/or pacing therapy to the patient. Defibrillation therapy circuit 204 conveys data regarding sensed patient parameters and defibrillation/pacing operations that are related to the event to clinical processor 210 via defibrillation therapy data path 208.

[0030] In a preferred embodiment, clinical processor 210 controls all of the monitoring and therapy functions of DMTS 200. In this embodiment, all functions of clinical

processor 210, patient monitoring circuit 201 and defibrillator therapy circuit 204 may be performed by a single processor. The clinical processor 210 may also be operable to capture a record of a rescue event by means of a microphone and/or camera input, not shown in FIGURE 2, to the clinical processor.

[0031] In an alternate embodiment, clinical processor 210, patient monitoring circuit 201 and defibrillator therapy circuit 204 are each separate physical processors. In another alternate embodiment, patient monitoring circuit 201 and defibrillator therapy circuit 204 operate independently from clinical processor 210. Clinical processor 210 thus has two primary functions. Clinical processor 210 may be operable to calculate and deliver therapy. Also, clinical processor 210 is operable to collect and process data from the circuits into clinical data, and then to store that processed clinical data for further use.

[0032] Clinical processor 210 preferably processes the data from the patient monitoring circuit 201 and defibrillator therapy circuit 204 into processed clinical data that is arranged in generic file formats. The generic file formats are ones that are readable by widely-available software programs. Current examples of such generic file formats include, but are not limited to, extensible mark-up language (.xml), portable document format (.pdf), and/or postscript (.ps). External systems may thus access the clinical data so arranged without requiring any special software.

[0033] A less preferred embodiment arranges the clinical data into a custom file format. In this embodiment, any system external to the DMTS 200 will require special software to decode the file information.

[0034] Clinical processor 210 saves the processed clinical data to an isolable memory space 220 via a read-write communications path 216. It is noted that clinical processor

210 may require read-access to the clinical data from memory 220 for use with functions, e.g. displays and user indications, internal to the DMTS 200.

[0035] FIGURE 3 illustrates a preferred arrangement for the processed clinical data files as stored in isolable memory 220. The data files that are intended for external system access preferably conform to an established standard for patient clinical data records, such as the National EMS Information System (NEMESIS). As shown in FIGURE 3, patient data records 300 are stored in patient data files 320 with a patient data file name that identifies the nature of the data. The patient data files 320 are in turn arranged in a patient data folder 310, which may be identified by the event name, date and time. The directory of patient data folders 310 in memory 220 is preferably read-only accessible to external systems as long as the DMTS 200 is powered on and active.

[0036] Compliance with patient confidentiality rules can be obtained in the above arrangement through a number of methods. Clinical processor 210 may be enabled to anonymize patient data prior to storage in memory 220. Passwords and other appropriate security methods may also be employed to restrict access to the patient data folders 310 by external systems.

[0037] Turning back to FIGURE 2, the clinical patient data which resides in isolable memory 220 may be accessed by external systems 260 via a communications interface 230. Preferably, communications interface 230 is a wireless interface of a type which includes but is not limited to Bluetooth.TM, Wi-Fi, or cellular telephone interfaces. Communications interface 230 may also be a wired interface of a type which includes but is not limited to Universal Serial Bus (USB) and Ethernet. The transmission path between the communications interface 230 and the external system 260 is preferably read-only,

i.e. transmitted from the communications interface 230 to external system 260 in response to the requesting of patient data from the external system.

[0038] A firewall circuit 240 is disposed along a firewalled communications path 250 between isolable memory 220 and communications interface 230. The firewall circuit 240 is operable to allow read-only access at the communications interface 230 to the patient clinical data residing in memory 220. Firewall circuit 240 is further operable to block the writing of any data received from communications interface 230 to memory 220. The firewall circuit 240 thus eliminates any externally-originated avenue for corrupting safety-critical software programs and data. Firewall circuit 240 thus separates the safety critical and non-safety-critical functions of DMTS 200.

[0039] FIGURE 4 illustrates one external view of a DMTS 200. A unitary housing 270 contains each of the patient monitoring circuit 202, the defibrillation therapy circuit 204, the clinical processor 210, the memory 220, and the firewall circuit 240. Shown mounted on the external surface of the housing 270 is the communications interface 230. This is for illustration only, as it is understood that the communications interface circuitry 230 is contained within the housing, and that only the antennae or communications port is disposed externally. Preferably, all components of communications interface 230 are contained inside housing 270. In the illustrated embodiment, the read-only transmission path from the device is a wireless transmission.

[0040] Shown in FIGURE 5 illustrates a block diagram of a defibrillator monitor telemedicine server and remote station system 500 according to another embodiment of the invention. System 500 includes a telemedicine server 510 which is integrated in a common unitary housing with a monitor defibrillator, and a transceiver 520 which is

disposed at a central monitoring station at a remote location. The internal arrangement and components of the telemedicine server 510 may be similar to the FIGURE 2 embodiment as previously described. In particular, telemedicine server 510 may include isolable memory 220 protected by a firewall circuit 240. The patient data is stored in the server memory 220. Preferably, the patient data is stored in a generic file format as previously discussed.

[0041] Telemedicine server 510 and transceiver 520 are communicatively linked via a read-only transmission path 262. Thus, telemedicine server 510 transmits patient data to the remote station transceiver 520 in response to a request for data from the remote station. The telemedicine server 510 is preferably disposed to require nothing more than the request, without any need for a previous setup or local user action, to perform the data transmission. The communications interface 230 in the telemedicine server 510 and the transceiver 520 may each be wireless or may be wired together.

[0042] Telemedicine server 510 is also operable to block, or prevent, external data including that corresponding to the request from the remote station from being written to the internal server memory 220. The firewall circuit 240 prevents the corruption of the safety-critical portions of the system, including for example, the patient monitoring circuit 202 and the defibrillation therapy circuit 204. Circuits 202 and 204 in turn are operable to generate the patient data.

[0043] The benefits resulting from the telemedicine server system 500 become clear by description of its operation. By co-locating the non-safety critical communications portions and the safety-critical patient monitoring and therapy portions within the telemedicine server housing 270, the operator has instant telecommunications capability

with a remote station as soon as the device is turned on. The server requires no setup prior to operation for transmitting data, because it can obtain an internet identifier automatically from any available network each time it is turned on. At that time, the server can automatically transmit its identifier to a predetermined website fixed within the server memory. Then the server merely awaits an authorized request that initiates the transmission of data stored in memory. The telemedicine server 510 may also be disposed to transmit the patient data to a previously authorized remote transceiver 520 as soon as the patient data is obtained.

[0044] The inventive system is also easier to modify as telecommunications protocols change over time. It is well known that safety-critical medical systems require heightened rigor in the design process and are subject to rigorous verification and validation processes in order to be cleared for use. By separating the safety-critical medical systems portions from the telecommunications portions with a firewall 240, the inventors have created a medical device whose communications circuits may be modified with little or no re-validation required of the safety-critical portions, even if all circuits reside in the same unitary housing.

[0045] FIGURE 6 illustrates a flow chart showing a method 600 for transferring patient data from a monitor defibrillator to a remote station. The first step 610 includes providing at the patient location a telemedicine server (610) integrated within the housing of the monitor defibrillator. The integrated telemedicine server includes a clinical processor operable to collect patient data from a patient monitoring circuit and a defibrillation therapy circuit. The server also includes a memory operable to receive the patient data from the clinical processor and to store the received patient data in a generic file format.

The server interface with external systems includes a communications interface disposed in read-only communication with the memory and further operable to transmit the patient data in the generic file format to the remote station, and a firewall circuit disposed between the memory and the communications interface and operable to prevent the writing of any data received from the communications interface to the memory.

[0046] In order to complete the communication setup, a second step 620 includes providing a transceiver at a remote station, and establishing a communications path between it and the communications interface. This second step 620 may be automatically completed when the telemedicine server is turned on in the previous providing step, using communications parameters in the server that are either pre-loaded at the factory, or previously established during prior uses of the server.

[0047] After the providing step 610 is completed, the monitor defibrillator is put into use to treat a patient. Patient data is automatically collected by the clinical processor at collecting step 630 and stored in the server memory in the generic file format at storing step 640. Storing step 640 may optionally include storing the patient data in a format which conforms to an established standard for patient clinical data.

[0048] The method 600 also contemplates that collecting step 630 and storing step 640 are conducted prior to the establishing of a communications path at step 620. This situation may arise in patient locations in which there is no wired or wireless connectivity available between the server and the remote station.

[0049] The remote station transceiver begins the “pull” of patient data from the telemedicine server at requesting step 650. The telemedicine server receives the request via the communications path and automatically determines whether the requester is

authorized for data sharing. In addition, the firewall circuit in the server blocks any data from the transceiver to be written in the same memory used to store the patient data.

[0050] The upper dashed line in FIGURE 6 from requesting step 650 to the output of the collecting step 630 indicates an optional method in which the telemedicine is turned on and a communications path is established, but wherein a patient is not yet being treated by the device. In this situation, the collecting step 630 may begin after the requesting step 650 is received from the transceiver.

[0051] After the determination is made that the remote station is an authorized recipient of data, the telemedicine server transmits the patient data to the remote station via the established communication path at transmitting step 660. Transmitting step 660 preferably occurs automatically and solely in response to the requesting step 650.

[0052] FIGURE 7 illustrates another embodiment of a firewall circuit in which safety-critical and non-safety-critical functions within a device such as a defibrillator monitor telemedicine server are performed by separate processor modules. The separate processor modules are physically separated but reside within a single multi-core processor 400. A firewall circuit 430, which may be a memory management unit, is disposed on one of the separate sub-processors 408. Another of the sub-processors 402 operates a safety-critical clinical processor 420. The clinical processor 420 may run on an RTOS in the sub-processor 402. Yet another of the sub-processors 404 operates a general purpose, non-safety-critical program 440 such as a communications program. The firewall circuit 430 provides read-write capability from the clinical processor 420 to external memory 406. Firewall circuit 430 also blocks any write capability from the non-safety critical program

440 into memory 406. Thus, a secure partition firewall 410 between safety-critical and non-safety critical functions is established.

[0053] The above-described embodiment enables a monitor defibrillator device to run safety-critical applications and ePCR applications simultaneously on a single hardware unit. The embodiment may also take advantage of the hardware-assisted virtualization features in a multi-core processor and the secured virtualization support of an RTOS. The embodiment indirectly uses the resource management and protection capabilities of the RTOS and the memory management unit (MMU) of the processor to create a secured partition firewall for running safety-critical applications simultaneously and safely alongside non-safety-critical applications.

[0054] The above-described embodiment may be disposed in several ways. One way to safely isolate critical and non-critical functions is to run them on separate processor modules that are physically separated but reside in a single hardware unit or device. Safety-critical applications run on a real time operating system (RTOS) in one of the processors with dedicated CPU, memory and other required devices and peripherals. Non-critical applications run on a general purpose operating system in a separate processor, without the permission of affecting the resources of the safety-critical applications. Display, recording and memory storage unit/module incorporate outputs from both critical and non-critical applications. Safety-critical user interface controls are mapped directly to the safety-critical application in order to be unaffected by reliability, security or performance problems of the non-safety-critical application. Safety-critical applications are thus protected from non-safety-critical applications even though they

reside in the same device. Hence the safety-critical applications will function normally even if a non-critical application fails to function correctly.

[0055] In an alternate but more efficient and less expensive implementation, the safety-critical applications run directly on an RTOS mapped to one or more dedicated cores of a multi-core processor. The non-safety-critical applications run alongside but on the other cores of the processor mapped to a general purpose operating system, such as Windows.TM, using a secure virtualization technique provided by the RTOS. The multi-core processor chosen for the implementation would support hardware-assisted virtualization features so that the RTOS virtualization implementation can take advantage of the resultant efficiency and improved performance.

[0056] Display, recording and storage of data generated from both critical and non-critical applications and the user interface control could also be conducted on separate functional units residing at the patient location. If the display is on a separate unit than where the application is running, then the data and control requests can be transmitted over to/from the display unit over a cable or wirelessly. Regardless of an integrated or separate display, switching between defibrillator/monitor and ePCR applications could be implemented using a single button press or touch of a screen. Defibrillator and monitor functions would be of the highest priority. The device thus retains the capability to automatically switch to defibrillator/monitor functions or alert the user to switch to defibrillator/monitor functions from non-safety related functions if clinical attention is needed.

[0057] Modifications to the device, method, and displays as described above are encompassed within the scope of the invention. For example, various configurations of

the clinical processor circuits which fulfill the objectives of the described invention fall within the scope of the claims. Also, the particular appearance and arrangement of the external device housing may differ.

[0058] It should be understood that, while the present invention has been described in terms of medical applications, the teachings of the present invention are much broader and are applicable for non-medical applications and uses. Further, As one having ordinary skill in the art will appreciate in view of the teachings provided herein, features, elements, components, etc. described in the present disclosure/specification and/or depicted in the appended Figures may be implemented in various combinations of hardware and software, and provide functions which may be combined in a single element or multiple elements. For example, the functions of the various features, elements, components, etc. shown/illustrated/depicted in the Figures can be provided through the use of dedicated hardware as well as hardware capable of executing software in association with appropriate software. When provided by a processor, the functions can be provided by a single dedicated processor, by a single shared processor, or by a plurality of individual processors, some of which can be shared and/or multiplexed. Moreover, explicit use of the term “processor” or “controller” should not be construed to refer exclusively to hardware capable of executing software, and can implicitly include, without limitation, digital signal processor (“DSP”) hardware, memory (e.g., read only memory (“ROM”) for storing software, random access memory (“RAM”), non volatile storage, etc.) and virtually any means and/or machine (including hardware, software, firmware, combinations thereof, etc.) which is capable of (and/or configurable) to perform and/or control a process.

[0059] Moreover, all statements herein reciting principles, aspects, and embodiments of the invention, as well as specific examples thereof, are intended to encompass both structural and functional equivalents thereof. Additionally, it is intended that such equivalents include both currently known equivalents as well as equivalents developed in the future (e.g., any elements developed that can perform the same or substantially similar function, regardless of structure). Thus, for example, it will be appreciated by one having ordinary skill in the art in view of the teachings provided herein that any block diagrams presented herein can represent conceptual views of illustrative system components and/or circuitry embodying the principles of the invention. Similarly, one having ordinary skill in the art should appreciate in view of the teachings provided herein that any flow charts, flow diagrams and the like can represent various processes which can be substantially represented in computer readable storage media and so executed by a computer, processor or other device with processing capabilities, whether or not such computer or processor is explicitly shown.

[0060] Furthermore, exemplary embodiments of the present invention can take the form of a computer program product accessible from a computer-readable and/or computer-readable storage medium providing program code and/or instructions for use by or in connection with, e.g., a computer or any instruction execution system. In accordance with the present disclosure, a computer-readable or computer readable storage medium can be any apparatus that can, e.g., include, store, communicate, propagate or transport the program for use by or in connection with the instruction execution system, apparatus or device. Such exemplary medium can be, e.g., an electronic, magnetic, optical, electromagnetic, infrared or semiconductor system (or apparatus or device) or a

propagation medium. Examples of a computer-readable medium include, e.g., a semiconductor or solid state memory, magnetic tape, a removable computer diskette, a random access memory (RAM), a read-only memory (ROM), flash (drive), a rigid magnetic disk and an optical disk. Current examples of optical disks include compact disk – read only memory (CD-ROM), compact disk – read/write (CD-R/W) and DVD. Further, it should be understood that any new computer-readable medium which may hereafter be developed should also be considered as computer-readable medium as may be used or referred to in accordance with exemplary embodiments of the present invention and disclosure.

[0061] Having described preferred and exemplary embodiments of systems, devices and methods in accordance with the present invention (which embodiments are intended to be illustrative and not limiting), it is noted that modifications and variations in/to such exemplary embodiments can be made by persons skilled in the art in light of the teachings provided herein (including the appended Figures). It is therefore to be understood that such changes which can be made in/to the preferred and exemplary embodiments of the present disclosure are within the scope of the present invention and the exemplary embodiments disclosed herein.

CLAIMS:

1. A monitor defibrillator having an integrated telemedicine server comprising:
 - a patient monitoring circuit (202);
 - a defibrillation therapy circuit (204);
 - a clinical processor (210) operable to collect patient data from the patient monitoring circuit and the defibrillation therapy circuit;
 - a memory (220) operable to receive the patient data from the clinical processor and to store the received patient data in a generic file format;
 - a communications interface (230) disposed in read-only communication with the memory and further operable to transmit the patient data in the generic file format to a remote station;
 - a firewall circuit (240) disposed between the memory and the communications interface and operable to prevent the writing of any data received from the communications interface to the memory; and
 - a unitary housing (270) for containing each of the patient monitoring circuit, the defibrillation therapy circuit, the clinical processor, the memory, the communications interface, and the firewall circuit.
2. The monitor defibrillator of Claim 1, wherein the communications interface is further operable to transmit the patient data unidirectionally to the remote station.
3. The monitor defibrillator of Claim 1, wherein the communications interface comprises a wireless communications interface selected from the group consisting of Bluetooth, WiFi, and cellular telephone.
4. The monitor defibrillator of Claim 1, wherein the communications interface comprises a wired Ethernet interface.

5. The monitor defibrillator of Claim 1, wherein the generic file format is selected from the group consisting of an extensible markup language (XML), portable document format (PDF), and postscript (PS) file format.

6. The monitor defibrillator of Claim 1, wherein the communications interface is further operable to transmit the patient data automatically to the remote station without operator action.

7. The monitor defibrillator of Claim 1, wherein the memory is further operable to store the received patient data in a folder identified by an event title.

8. The monitor defibrillator of Claim 7, wherein the received patient data is stored in the folder arranged by the date/time in which the data was collected.

9. The monitor defibrillator of Claim 1, further comprising a single core processor having a plurality of securely separated sub-processors, wherein the clinical processor and the firewall circuit are operably disposed respectively on one of the plurality of sub-processors.

10. The monitor defibrillator of Claim 9, wherein the clinical processor is further operable to perform safety-critical functions and non-safety-critical functions, and further wherein the safety-critical functions are operably disposed on one of the plurality of sub-processors as a real-time operating system (RTOS).

11. A system for providing patient data from a monitor defibrillator to a remote station comprising:

a telemedicine server (510) having a clinical processor, an isolable memory, a firewall circuit, and a communications interface, wherein the telemedicine server is integrated with the monitor defibrillator circuitry to obtain the patient data; and

a transceiver (520) located at the remote station in communication with the communications interface, wherein the telemedicine server transmits the patient data to the remote station in response to a request for data from the remote station.

12. The system of Claim 11, wherein the telemedicine server is operable to prevent external data received from the remote station from being written to the isolable memory.

13. The system of Claim 11, wherein the patient data is stored in the isolable memory in a generic file format.

14. The system of Claim 11, further comprising a patient monitoring circuit and a defibrillation therapy circuit in communication with the telemedicine server, each co-located in a unitary housing with the telemedicine server, and further wherein the patient monitoring circuit and the defibrillation therapy circuit are operable to generate the patient data.

15. The system of Claim 11, wherein the telemedicine server is further operable to transmit the patient data to the transceiver as the patient data is obtained.

16. The system of Claim 11, wherein the transceiver is a wireless transceiver and the communications interface comprises a second wireless transceiver.

17. A method for transferring patient data from a monitor defibrillator having a patient monitoring circuit and a defibrillation therapy circuit to a remote station comprising the steps of:

providing a telemedicine server (610) integrated within the housing of the monitor defibrillator, the telemedicine server including

a clinical processor operable to collect patient data from the patient monitoring circuit and the defibrillation therapy circuit,

a memory operable to receive the patient data from the clinical processor and to store the received patient data in a generic file format,

a communications interface disposed in read-only communication with the memory and further operable to transmit the patient data in the generic file format to the remote station, and

a firewall circuit disposed between the memory and the communications interface and operable to prevent the writing of any data received from the communications interface to the memory;

establishing a communications path (620) between a transceiver at the remote station and the communications interface;

collecting (630) the patient data at the clinical processor;

storing the patient data (640) in the memory in the generic file format;

requesting the patient data (650) from the transceiver to the telemedicine server; and

transmitting the patient data (660) from the telemedicine server to the remote station automatically in response to the requesting step.

18. The method of Claim 17, wherein the transmitting step is solely in response to the requesting step.

19. The method of Claim 17, wherein the storing step further comprises storing the patient data in a format which conforms to an established standard for patient clinical data.

20. The method of Claim 17, wherein the collecting step begins after the requesting step.

1/7

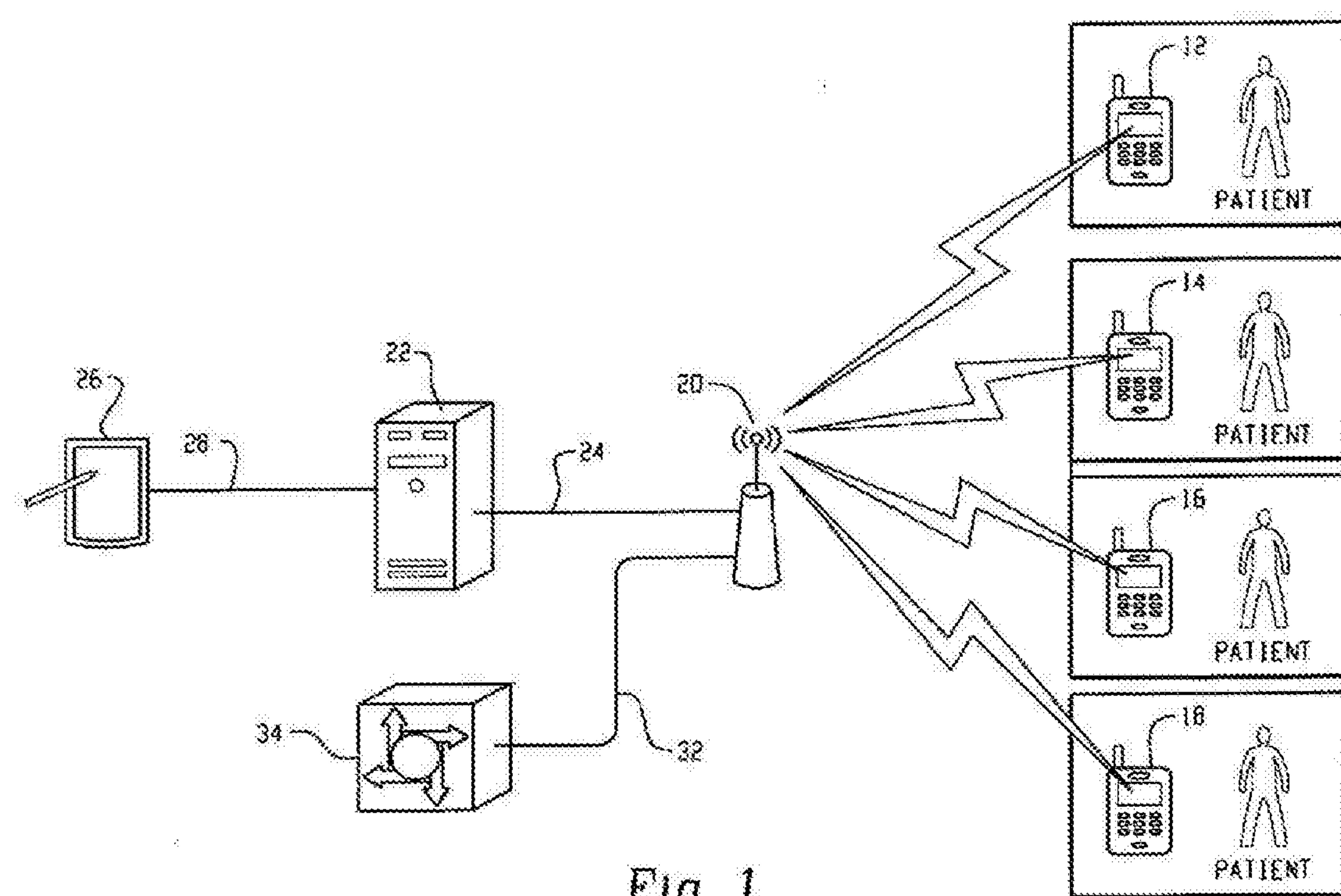
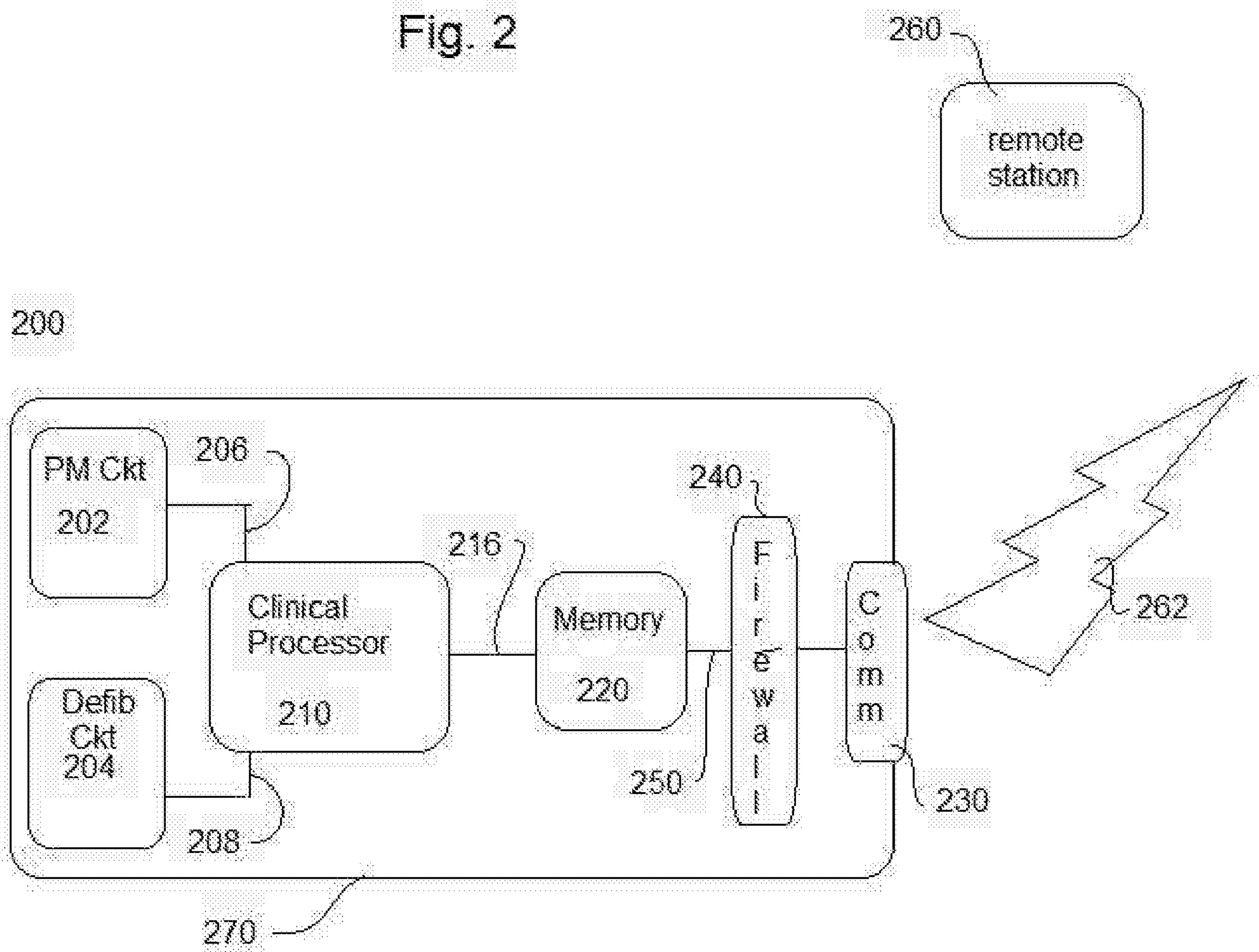


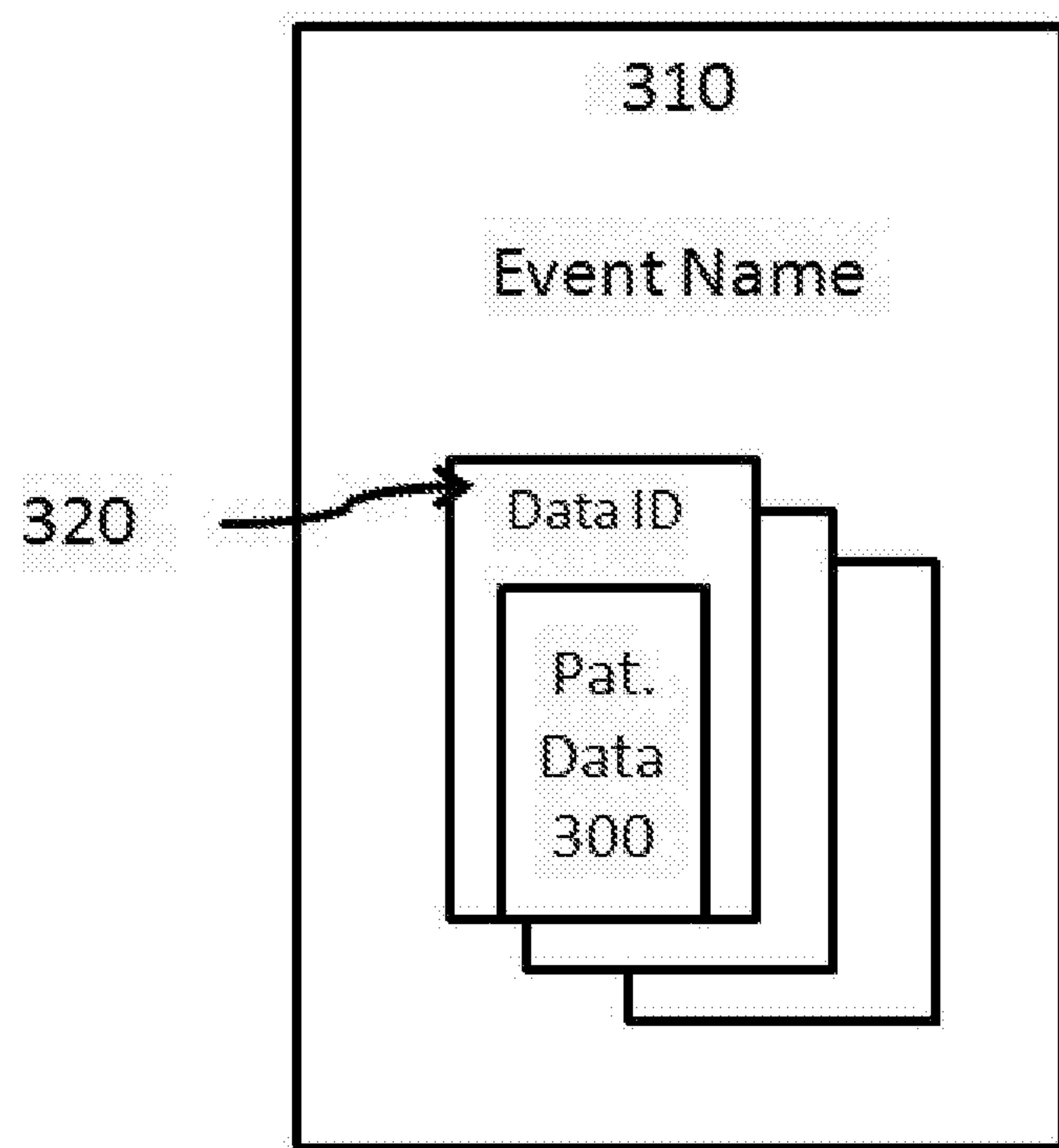
Fig. 1
Prior Art

Fig. 2



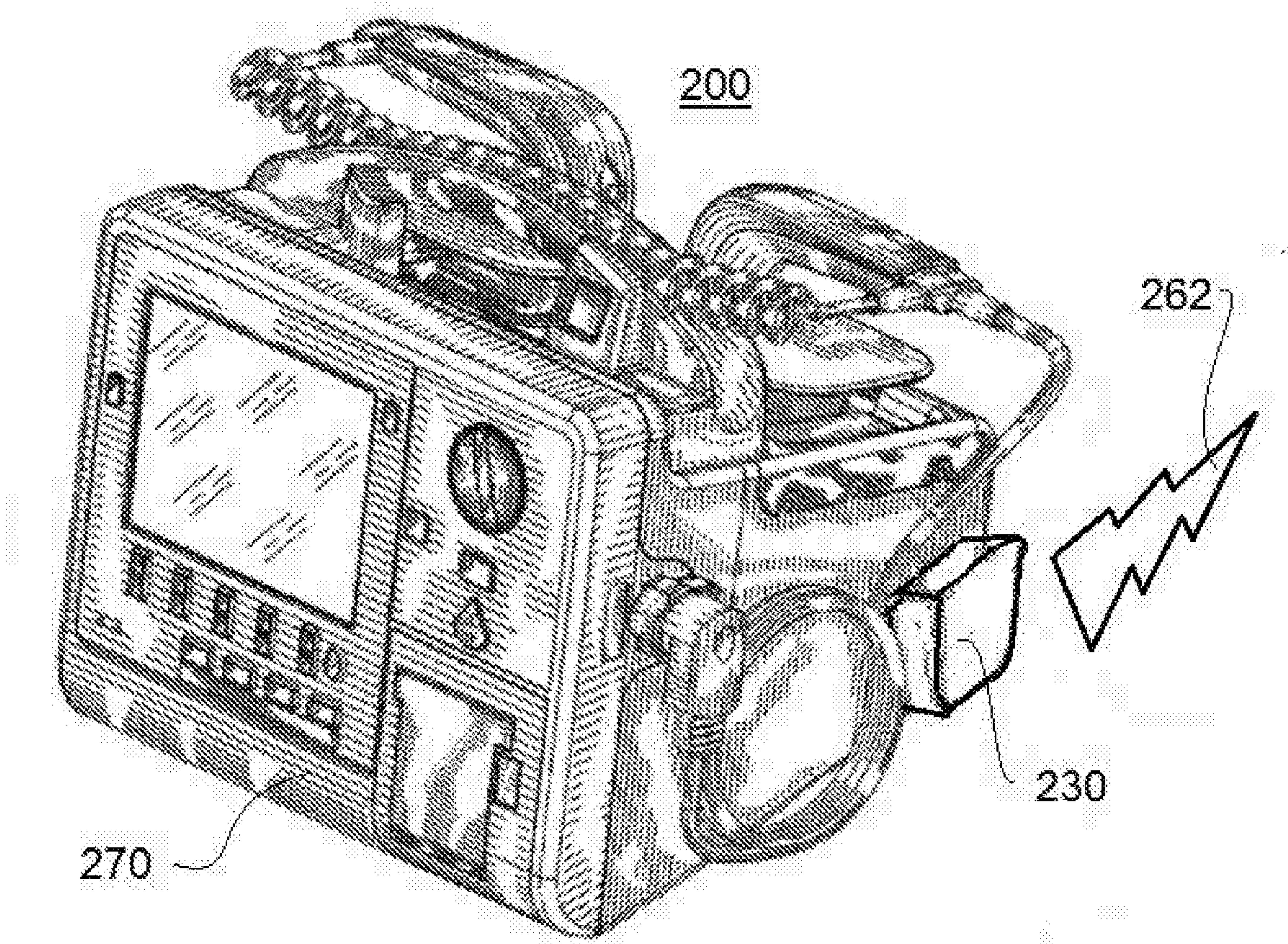
3/7

Fig. 3

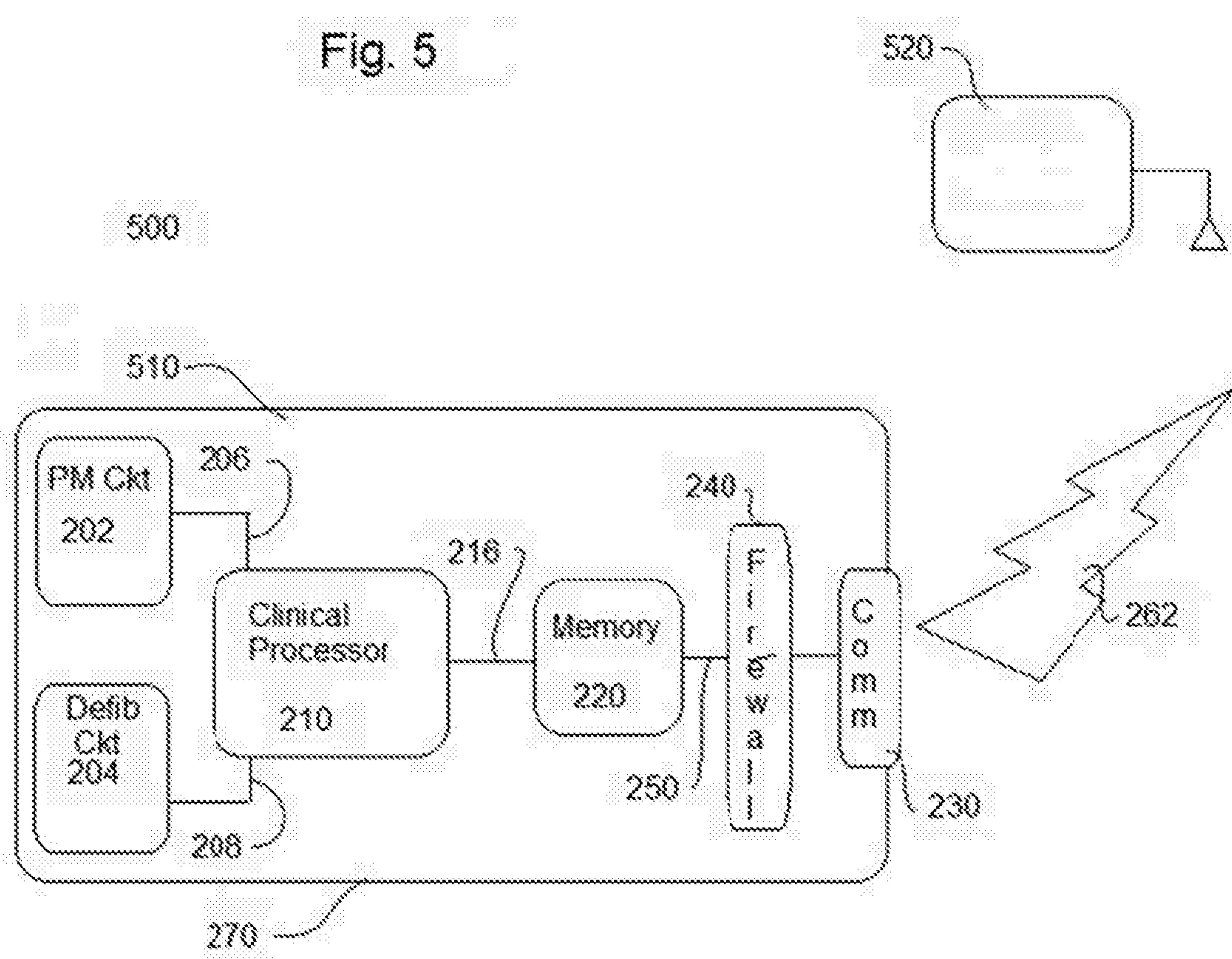


4/7

Fig. 4

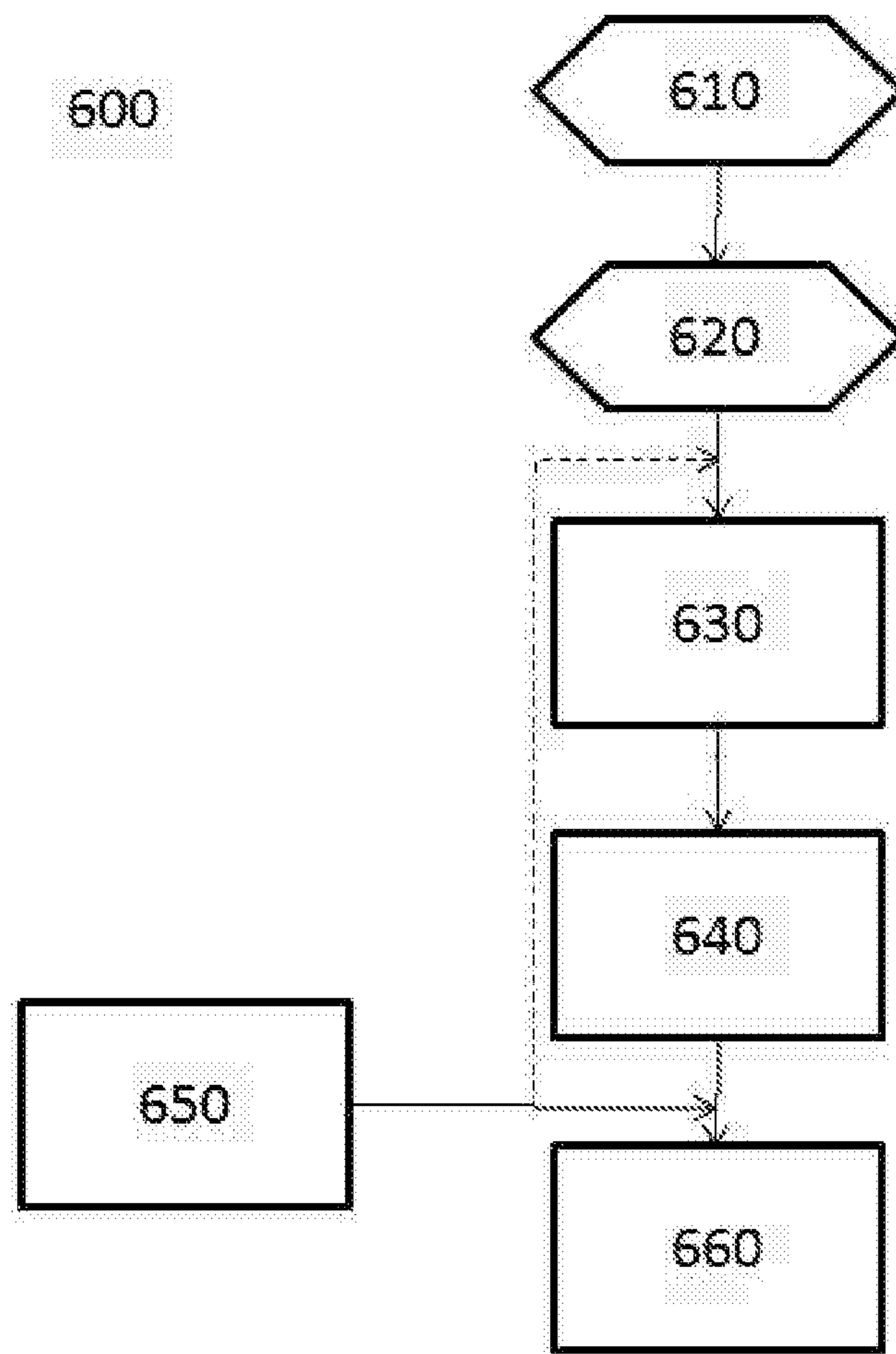


5/7



6/7

Fig. 6



7/7

Fig. 7

