



(51) International Patent Classification:

G16H 40/40 (2018.01) G16H 40/67 (2018.01)

(21) International Application Number:

PCT/GB2024/051694

(22) International Filing Date:

28 June 2024 (28.06.2024)

(25) Filing Language:

English

(26) Publication Language:

English

(30) Priority Data:

2309847.8 29 June 2023 (29.06.2023) GB

(71) Applicant: **CAIN MEDICAL LTD** [GB/GB]; Norfolk House, 4 Station Road, St Ives Cambridgeshire PE27 5AF (GB).

(72) Inventors: **CAIN, Stuart James**; c/o Cain Medical Ltd, Norfolk House, 4 Station Road, St Ives Cambridgeshire PE27 5AF (GB). **CAIN, Nicholas John**; c/o Cain Medical Ltd, Norfolk House, 4 Station Road, St Ives Cambridgeshire PE27 5AF (GB). **GREVE, Andrea**; c/o Cain Medical Ltd,

Norfolk House, 4 Station Road, St Ives Cambridgeshire PE27 5AF (GB).

(74) Agent: **DUNLEAVY, Christopher**; 406 Cambridge Science Park, Milton Road, Cambridge, Cambridgeshire CB4 0WW (GB).

(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, CV, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IQ, IR, IS, IT, JM, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, MG, MK, MN, MU, 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, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, WS, ZA, ZM, ZW.

(84) Designated States (unless otherwise indicated, for every kind of regional protection available): ARIPO (BW, CV, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SC, SD, SL, ST, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ,

(54) Title: A SERVER FOR EXTENDING A POINT-TO-POINT CONNECTION BETWEEN A HEALTHCARE INFORMATION SYSTEM AND AT LEAST ONE MEDICAL DEVICE

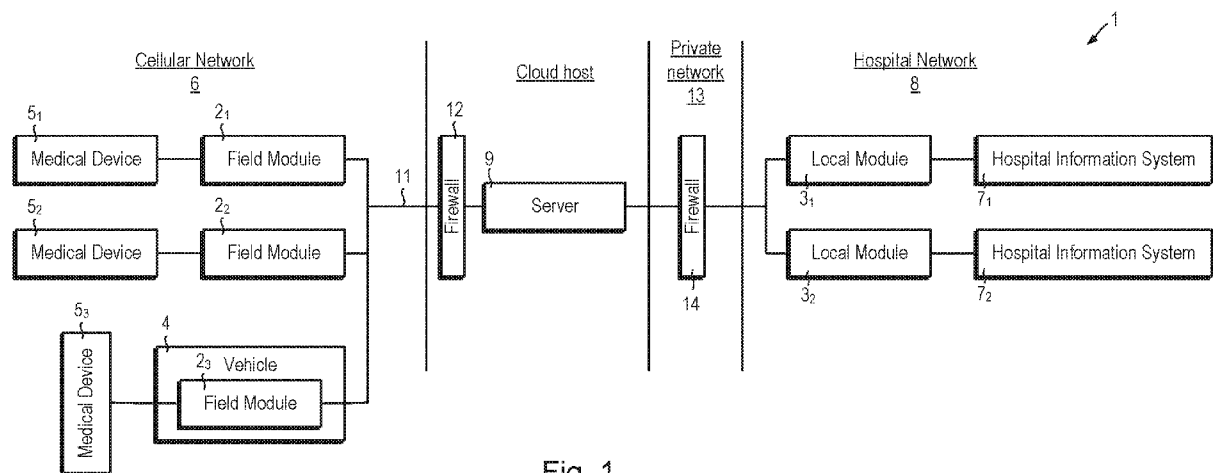


Fig. 1

(57) Abstract: A server for extending a point-to-point connection between a healthcare information system and at least one medical device is described. A server for extending a point-to-point connection between a healthcare information system and at least one medical device. The server is configured to connect to a local module via a first private network, the local module configured to connect to the healthcare information system, and to connect to a field module via a second private network, the field module configured to connect to the at least one medical device. In response to receiving data from the at least one medical device via a field module, the server is configured to verify that the data is from the at least one medical device and to send the verified data using the first private network to the local module, and/or, in response to receiving data from the local module, the server is configured to send the data to the medical device using the second private network via the field module.



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, ME, 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))*
- *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments (Rule 48.2(h))*

A server for extending a point-to-point connection between a healthcare information system and at least one medical device

Field

- 5 The present invention relates to hardware and methods for extending a point-to-point connection from inside a trusted local network to outside that network. Specifically, the invention relates to hardware and methods for extending a point-to-point connection from inside a trusted local network to a remote device, for example a field device.

10

Background

- Growing pressures on emergency departments, paramedics and emergency services have risen to concerning levels in the UK. Overcrowded hospitals make it difficult for ambulances to offload patients, non-emergency calls take up valuable resources and an aging population on places increasing demands on the medical systems with downstream consequences for ambulance services.

15

- Integrated care systems including hospital at home, emergency care services and virtual wards are able to alleviate some of these pressures by facilitating care and an effective triage of patients out in the community. To enable effective care, one critical need is to shift diagnostic testing, currently happening within hospitals, into community settings to ensure high-quality clinical care without conveying patients into hospitals. For this, medical grade Point of Care (POC) testing and patient monitoring devices can be placed into communities. However, whilst hospital grade POC devices often automate their recording of data into hospital information systems, this is only possible within hospital IT settings. Once POCs are taken out of hospitals into communities, they lose their ability to automatically communicate with hospital systems. However, 'real-time' access to POC data is critical to enable clinical experts to make time-critical clinical decisions for emergency care.

20

25

- 2 -

Summary

According to a first aspect of the invention, there is provided a server for extending a point-to-point connection between a healthcare information system and at least one medical device, the server configured: to connect to a local module via a first
5 private network, the local module configured to connect to the healthcare information system, and to connect to a field module via a second private network, the field module configured to connect to the at least one medical device; in response to receiving data from the at least one medical device via a field module, to verify that the data is from the at least one medical device and to send the
10 verified data using the first private network to the local module; and/or in response to receiving data from the local module to send the data to the medical device using the second private network via the field module.

The medical device may be a device which is remote or outside of a hospital or
15 other care-giving centre. For example, the medical device may be a point of care (POC) device, or a point of care testing (POCT) device used on a patient in community or community care setting. The local module may be a clinical-based device, for example, a hospital-based device, such as a hospital-based computer or server.

20 In this way, a remote medical device which is in the community outside of a hospital or other caregiving or care-providing centre can automatically connect to any POC device and provide secure connections reaching into hospital information systems. Paramedics are therefore able to deliver mobile, laboratory-standard test
25 results in the community with the data being communicated in 'real-time' to clinical experts in hospital pathology labs for appropriate decision-making. This enhanced communication, may reduce unnecessary hospital admissions, help guide clinical pathway decisions, accelerates time to treatment and reduces inconvenience to patients.

30 The server may be configured to connect wirelessly, for example, using broadband or narrowband radio waves, cellular connections, for example, 3G, 4G, 5G, GSM and the like.

35 Data may be in the form of a data packet.

- 3 -

The local module may be configured to connect to the same local area network as the healthcare information system.

The server may be configured to connect to the local module via a single port.

5

Thus, the healthcare information system can communicate with a medical device which may be in a location outside the hospital which houses the healthcare information system.

10 Additionally, or alternatively, the diagnostic results can be sent from the healthcare information system back to field module via the local module and the server in a readable format.

15 The server may be configured to send the data via a single port, and/or; to receive data via the single port from the local module.

The number of ports required to cross the hospital IT boundary may be minimised by mapping and remapping the message crossing the between the Server 9 and the local module. For example, many POC devices can be connected to hospital
20 information systems with opening a single port or more.

The server can direct messages to one or more local modules, for example, paramedic who servers more than one hospital in an ambulance the data will be delivered to appropriate hospital local module.

25

The data may be verified by checking the data size and/or frequency.

The verification of the data may be performed by the local module or by the server.

30 For example, the verification or check may comprise checking the maximum data size. The verification or check may comprise software on the local module or the server which performs the verification or check.

35 The data may be verified by confirming that the data conforms to a medical device data type corresponding to the medical device networked to the field module.

- 4 -

The data may be verified by confirming the medical device fixed internet protocol address or media access control address.

5 Data may be verified by waiting for confirmation before proceeding, checking one or more data packets from the medical device and/or the healthcare information system, checking the external service details (e.g., a software driver will check on the data may comprise a data size check, or packet size check, dates fields, message format for example, maximum packet size check, the check on the data fields and data structure may include a device type to confirm that the data or data
10 packet comes from the correct device.

The server may be configured to communicate with the local module or field module using the transmission protocol expected by the medical device.

15 The transmission protocol may be Transmission Control Protocol (TCP) or may be User Datagram Protocol (UDP).

The medical device may be a point of care medical device.

20 That is, the medical device may be a medical device remote from a hospital or other care-providing institution, for example, in someone's home, in a vehicle, etc. The point of care (POC) medical device may be a point of care testing (POCT) medical device, or a point of care (POC) monitoring device. For example, the POCT may be a blood gas analyser, a glucose monitor, bodily fluid antigen analyser. The
25 POC monitoring device may be a blood pressure analyser, heart rate recorder, a pulse oximetry device.

The field module may be configured to connect to a plurality of medical devices.

30 The connection between the field module and the plurality of medical devices may be a secure connection.

The server may be configured to verify and send data from a plurality of medical devices simultaneously.

35

- 5 -

The server may be configured to receive, verify and/or send data from multiple medical devices (e.g., 10, 20, 50, 100, 1000, 10,000 or more than 10,000 medical devices) at the same time.

- 5 The data received may be encrypted data, and the server is configured to decrypt the data.

The data received may be protected using a password, and the server is configured to access the data using the password.

10

The field module or server may be configured to identify a test type based on the at least one medical device type, and based on the test type, send data from a test performed on the at least one medical device to an associated local module and/or hospital information system.

15

For example, the at least one medical device may be a blood sample analyser, or a saliva sample analyser, if the medical device is a blood sample analyser, the test type is given a "blood sample" ID or flag, if the medical device is a saliva sample analyser, the test type is given a "saliva sample" ID or flag. Certain tests need to be sent to certain systems within the hospital. Therefore, the field module or server can identify the type of test and then send it to the appropriate system (local module and/or hospital information system) for record keeping or further analysis.

20

According to a second aspect of the invention, there is provided a local module for extending a point-to-point connection between a healthcare information system and at least one medical device, the local module configured: to connect to the healthcare information system; to connect to a sever via a private network; in response to receiving data from the server using the private network, to identify an inbound port on the healthcare information system to send the data to the healthcare information system; and/or in response to receiving data from the healthcare information system, to send data from the healthcare information system to the server.

25

30

The local module may connect to the same local area network as the healthcare information system.

35

- 6 -

The local module may be configured to receive data from the healthcare information system via a single port. The local module may be configured to send data from the healthcare information system to the server via a single port on the healthcare information system.

5

The local module may be configured with the single port on the healthcare information system.

10 According to a third aspect of the invention, there is provided a field module for extending a point-to-point connection between a healthcare information system and at least one medical device, the local module configured: to connect to a server via a private network; to connect to the at least one medical device; and to relay data between the at least one medical device and the server.

15 The field module may comprise a location module configured to identify the location of the field module.

20 The location module may be a satellite positioning system module (e.g., a global positioning system, GPS module, or other suitable satellite positioning system), which can identify the location of the field module. The field module may be configured to forward the location of the field module on to the local module and/or hospital information system via the server. The location module may also record the time as well as the location, and may also forward this to the local module and/or the hospital information system.

25

The location module may also be used to identify where and when the field module was used to communicate with a nearby medical device, thus providing the location and time of use of a medical device.

30 The module may comprise an interface configured to allow data input, wherein on receiving an input of data, may send the data to the hospital information system via the server.

35 The hospital information system, on receiving the input data from the file module, may generate a patient record based on the received data. The input data system also allows for manual input of novel patient record or patient medical information additional to that which can be supplied from the test.

- 7 -

The field module may be configured to: send medical device data to the healthcare information system; and receive diagnostic information from the healthcare information system based on the medical device data.

5

The field module may be configured to: send medical device data to the healthcare information system; and receive instruction information from the healthcare information system based on the medical device data.

10 The instruction information may be for initial or further patient care, for example, a video on how best to treat a patient from whom the medical device data has been collected. The instruction information may also cover information on device usage.

15 According to a fourth aspect of the invention, there is provided a system for extending a point-to-point connection between a healthcare information system and at least one medical device, the system comprising: a local module connected to the healthcare information system; a server connected to the local module via a first private network; and a field module connected to the server via a second private network.

20

The field module is configured: to connect to the at least one medical device; and to relay data between the at least one medical device and the server.

25 The server is configured: in response to receiving data from the field module, to verify that the data is from the at least one medical device and to send the verified data to the local module or receive data from the local module.

30 The local module is configured: in response to receiving data from the server to forward the data to the healthcare information system; and/or in response to receiving data from the healthcare information system, to send data from the healthcare information system to the server.

35 The system may be configured to monitor one or more of: field module location; field module data usage; field module activity; or field module data sent to the server.

- 8 -

The first or second private networks may be virtual private networks (VPN) The private network may be a dual redundant private network.

5 The server may be configured to send the verified data via a single port to the local module or receive data via the single port from the local module.

The data of the local module, the field module or the server may be encrypted data and either the server, the field module, or the local module is configured to decrypt the data.

10

The data of the local module, the field module, or the system may be protected using a password, and either the server, the field module, or the local module is configured to access the data using the password.

15 According to a fifth aspect of the invention, there is provided a server for extending a point-to-point connection between a healthcare information system and at least one field module, the server configured: to connect to a local module via a first private network, the local module configured to connect to the healthcare information system, and to connect to a field module via a second private network;
20 in response to receiving data from the local module to send the data to the field module using the second private network via the field module; and/or in response to receiving data from the at least one field module, to verify that the data is from the at least one field module, and to send the verified data using the first private network to the local module.

25

The server of the fourth or fifth aspects may be the server of the first aspect. The local module of the fourth or fifth aspects may be the local module of the second aspect. The field module of the fourth or fifth aspects may be the field module of the third aspect.

30

- 9 -

Brief description of the drawings

Certain embodiments of the present invention will now be described, by way of example, with reference to the accompanying drawings, in which:

- 5 Figure 1 is a system block diagram of a remote medical device communication system;
Figure 2 is a system block diagram of a remote medical device communication system field device;
Figure 3 is a system block diagram of a remote medical device communication
10 system local area network connected device; and
Figure 4 is a system block diagram of a remote medical device communication system server.

Detailed description of certain embodiments

15

Overview

- The inventors have developed an innovative hardware and software system, that eases the mounting pressures on emergency departments, and emergency services by remotely bringing clinical hospital level expertise into communities. With this
20 system, diagnostic testing, which patients typically attend the hospital for, can now be conducted in community settings. Medical Point of Care (POC) devices such as point of care testing, physiological monitoring, respiration and infusion devices can be operated by paramedics or other community healthcare providers or care staff, while test data is reviewed by clinical experts remotely, for example, in a hospital
25 setting. The system automatically collects and securely relays data from POC devices into hospital or healthcare information systems in real time. Examples of hospital or healthcare information systems include clinical information system (CIS), electronic patient record system (EPR), laboratory information management system (LIMS), hospital middleware (or Medical Device Data Systems) or a hospital
30 interface engine. Hospital clinical experts can use this information, for example in real-time, to make informed clinical decisions while patients and paramedics are still in the community.

- For example, the system enables paramedics to deliver mobile, laboratory-standard
35 test results in communities, combined with remote expert clinical decisions from hospital clinical experts, for example, those working in pathology labs. This integrated urgent care service looks after more patients using remote clinical

- 10 -

assessment and helps the conveyance of only those patients who require hospital care. The system can facilitate device connectivity and communication, which may reduce unnecessary hospital admissions, help guide clinical pathway decisions, and accelerate time to treatment. Most importantly, the system can reduce
5 inconvenience and risks to patients who attend hospitals, for example, hospital-acquired infections. It enables patients to receive care close to their homes, supporting their continued independent living. Overall, the system provides a sustainable solution that automates the mobile use of medical devices, complementing other community care services.

10

The system presented here bridges the gap between point of care testing (POCT) and hospital communication systems, enabling expert clinical diagnostics to be delivered into the community. The system automatically reads the data collected by POCT devices used in the community. The data are instantly and automatically
15 transmitted to a hospital where they are recorded in a Hospital Information System. Critically, the system may allow clinical experts to use the information from POCT devices in 'real-time' to make informed, clinical decisions in hospitals while patients and paramedics are still out in the community. Further, the system will support non advanced paramedics who may not have medical device diagnostics training, in
20 clinical decision making.

The system may facilitate, for example:

- support non advanced paramedics in clinical decision making;
- 25 • patients using remote clinical assessment;
- managing more patients at home or in the community;
- helping convey patients to hospital who require specialist care that can only safely be provided in hospital, whilst reducing conveyances of patients who can be treated at home;
- 30 • improving the capabilities in the pre-hospital setting that can enable patients to be cared closer to home;
- using technology to support patients care, enhance communication and improves patient safety in the initial diagnosis;
- helping diagnosis by using point of care testing and/or monitoring devices.

35

Referring to Figure 1, the system 1 is a hardware and software solution, which comprises of two modules (also referred to as devices): a Field Module 2 (also

- 11 -

referred to as "FiM", a "portable module", or a "remote module") and a local module 3 (also referred to as a hospital module, or HoM). The FiM 2 is a small, mobile router which can be, for example, carried in a paramedics' bag, their uniform or vehicle 4. The field module 2 can also be situated in a pharmacy or GP office or surgery and can be used where there is no network connection in remote locations, e.g., by using a cellular connection. The FiM 2 establishes a secure connection to any POC device 5, to read the device data and automatically send them securely to a hospital information system such as a hospital patient record, laboratory management or middleware system. The system 1 may work over a multicellular network 6, and the FiM 2 and has a power source, for example, a battery (not shown). POC device 5 results are never lost and can be resent in the event of temporary signal drop-out.

The system 1 hospital module (HoM) 3 (also referred to as a "local module" 3) is as software solution located on or connected to (e.g., via the local area network, which may be the hospital or other care-providing service's network 8) a hospital information system 7 (which may also be referred to as a hospital server). The hospital module 3 is configured to remap POC devices' 5 messages to the correct entry in the hospital information system 7. The HoM 3 can support many makes, models, and manufacturers of medical devices 5 out in the community and is securely monitored using intelligent message protection, which will be explained in more detail later, ensuring messages are delivered under a protected closed private system. The system 1 can automatically connect to any POC 5 device and provide secure connections reaching into Hospital IT systems, in line with NHS regulatory requirements.

The System 1 can direct messages to one or more HoM 3, for example, paramedic who servers more than one hospital in an ambulance the data will be delivered to appropriate hospital HoM 3.

The system 1 allows a user to:

- connect to any community-based POC device and to any hospital information system, for example, including connecting through existing hospital middleware solution, for example, Medical Device Data Systems; and
- enable hospital information systems to communicate or talk to different makes and models of POC device.

- 12 -

The system 1 is compatible with an entity's (e.g. a hospital) security and their private network, for example, NHS security, including firewalls and the Health and Social Care Network (HSCN), or other suitable private network. The system 1 may contain a dual redundant private network (e.g., a VPN) in case of system failure.

5 The system 1 includes intelligent security to allow specified medical device data to be communicated, with other data blocked. The system can prevent network attacks such as malware, denial of service, message interception and ransomware. The system 1 runs on a private dedicated network, using its own dedicated internet, which may allow the system 1 to require only one secured port into the
10 hospital to connect a plurality, (for example, tens, hundreds, or thousands) of devices 5. The system 1 has standardisation, which assures hospital information systems 7 can connect with any medical device 5 rapidly and confidently, now and at any time in the future.

15 The system 1 further comprises a server 9 hosted on a managed dedicated internet 10. The server 9 is connected to the file module(s) 2 via a private network 11, for example, a virtual private network (VPN). Optionally, there may be a firewall 12 between the field module(s) 2 and the server 9 which may be present on either the field module 4 or the server 9, or both. The server 9 is also connected to one or
20 more hospital (or local) modules 3 via a private network 13 or a dedicated network which may be a Health and Social Care Network (HSCN), or another private network, e.g., a VPN. There may also be a firewall 14 between the server 9 and the local modules 3.

25 Possible benefits of the system 1

The present system 1 has a significant impact on the health economics of the healthcare systems. The system 1 enables paramedics to deliver mobile, laboratory-standard test results in the community with the data being communicated in 'real-time' to remote clinical experts in a hospital department for
30 appropriate decision-making. This enhanced communication, can reduce unnecessary hospital admissions, help guide clinical pathway decisions, accelerate time to treatment and reduce inconvenience to patients. The system 1 can also reduce labour costs and increases productivity of the healthcare services with significant cost savings.

35

The system 1 provides an affordable and sustainable solution which can automate the mobile use of medical devices 5 including point of care devices. This enables

- 13 -

clinical decisions and care to be brought to patients' home, which facilitates continued independent living and complements other community support. For example, the system 1 facilitates community clinical professionals and response teams in their clinical decision making from within hospitals, which will support the appropriate use of ambulances and conveyances of patients into hospital.

In summary, some of the benefits provided by the system 1 are:

- improved accuracy and consistency of data collected, reducing the risk of errors, and improving patient outcomes. Accurate and consistent data can also lead to better decision-making by healthcare professionals;
- increased productivity by reducing the time required for data collection and analysis, freeing up time for other tasks such as patient care and treatment, reducing unnecessary conveyances of patients into hospital which may enhance response teams attending critical cases in need of conveyance; and
- cost savings by reducing labour requirements, improving efficiency, and reducing the risk of errors. In addition, it cuts down on journeys of paramedics to hospitals for instance to upload data.

Using a POC device 5 outside of hospitals reduces patient admittance, emergency department workloads and patient infections. For example, POC testing by paramedics a patient was directly admitted to a hospice, negating a visit to the Emergency Department for blood tests; another patient was fast-tracked directly to the intensive care unit. Streamlined patient journeys provide inherent savings to the service and benefits to patient care. Patients report high levels of satisfaction, and paramedics confirm it adds value where it was used to support decision-making.

The system 1 is capable of extending a device medical data system, which may be housed on a local module 3 within a health information system 7, or connected to the same local area network (LAN) as the health information system 7.

Many hospitals are using such a local module 3 to interface with bedside and point-of-care medical devices 5 to clinical systems in such areas as intensive care operating rooms, paediatric/Neonate ICU, patient wards, bioscience and pathology labs and emergency rooms.

- 14 -

The benefits of medical device connectivity are well documented, as it reduces transcription errors, reduces clinical staff time, and ensures the data is where it is most both in real-time and trended over time. There is increasing demand for health service providers such as the National Health Service (NHS) to connect their
5 medical devices throughout a hospital.

Medical devices are networked, and the local module 3 communication interfaces collect standardised medical data from bedside and point-of-care medical devices.

10 The local module 3, is a middleware solution, that can manage messages or data from a medical device, the medical device message or data may be measurements and waveforms such as heart rate, blood pressure, body temperature, and ECG, point of care results and/or diagnostic results. This includes alarms such as types, triggers, limits, thresholds, settings, and acknowledgements, to a common
15 standard.

The local module 3 contains medical device drivers making the system device agnostic and, therefore, can be used with many makes or manufacturers of medical devices. Including hospital legacy and newly purchased devices.

20

All medical device readings can be passed to the hospital information system 7 or Clinical Information System (CIS) or Electronic Patient Record System (EPR) or Laboratory Information Management System (LIMS) or Hospital Middleware or Hospital Interface Engine.

25

The system 1 ensures that the local module 3 is not just limited to hospital medical devices but can reach out into the community.

Technical description of the system 1

30 Referring again to Figure 1. This invention relates to transferring data from a remote medical device to a hospital or healthcare information system.

Portable medical devices 5 often provide a means to transfer test results or measurements or medical parameters to a computer, but when the device is
35 outside of the hospital environment this can prove challenging. The hospital computer network will have extensive network security to prevent unauthorised access restricting data entering or leaving the hospital, and the point-to-point

- 15 -

connectivity of mobile devices lacks the sophistication required to accommodate security protocols.

5 The mobility of the devices also means they may be operated in point of care vehicles 4 (for example, ambulances) and may require a wireless method to access a network. Preferably, the means to transfer the data may also be scalable, with medical devices installed in multiple vehicles. The present invention proposes the means to wirelessly connect the medical device to an hospital information system, while allowing the connectivity to be managed within the security mechanisms of
10 the hospital.

The system 1 has three main components:

1. A portable computing device 2, which can provide a local Wi-Fi hotspot, or other wireless connection or wired connections, to a cellular data network,
15 and a virtual portable network (VPN) client.
2. A cloud-based application server which also hosts a VPN server.
3. A hospital-based application server hosting a VPN client, and a TCP and/or UDP redirection application.

20 The portable computing device (or field module) 2 provides network connectivity to the portable medical device 5. The cloud-based application server 9 provides a bridge between the portable computing device 2 and the hospital-based application server (also referred to as the hospital module, or the local module) 3.

25 The hospital-based server 3 redirects, relays, or replicates data from the portable medical device 5 to the hospital information system.

Figure 1 shows the deployment diagram giving the relationship between the components.

30 Portable medical devices 5 connect to the Wi-Fi hotspot provided by the portable computing device 2. The portable computing devices 2 access the Internet through a cellular network 6 (which may include a cellular tower (not shown)), or multicellular network, which provides connectivity via a private network 11 (e.g., a VPN) to cloud services. A cloud-based application server 9 hosts a private network server (e.g., a VPN server) that is accessed through the hospital network 8 (or hospital trust network) by the local module 3, which can act as a local application

- 16 -

server. The local module 3 can transfer data acquired from the medical devices 5 to the hospital information system 7.

5 The portable computing device 2, cloud application server 9, and VPNs 11, 13 between the cloud application server 9 and the hospital-based hospital information system 7 allow the portable medical device 5 to directly connect to the hospital-based server 7. Software on the hospital-based server 7, for example a lookup table, can replicate the server network port(s) of the hospital information system 7 and provide one endpoint of the point to point connect from the portable medical
10 device 2. This can then manage inbound and outbound connections from multiple portable medical devices 5 and route all traffic to the hospital information system 7.

Field module 2

Referring to Figure 2, the field module software runs on a portable device 2, which
15 can be issued to each paramedic or community care staff.

The system 1 can communicate with any medical device 5 regardless of make or manufacturer, such as Abbott iSTAT, Roche Cardiac Reader, Siemens ePOC, Philips ECG/Patient monitor, LumiraDx, Drager ventilators etc.

20

The field module 2 may be carried by paramedics or their vehicle 4 and establishes a secure connection to the paramedics' medical devices 5. A field module 2 located near a community medical device 5 will automatically connect to it wirelessly. In addition, the field module 2 may have an Ethernet socket or Wi-Fi or wireless
25 dongles (not shown) which attach to community medical devices 5 that lack inbuilt wireless connectivity.

The field module 2 communicates with the VPN 11 across a multi-network internet connection (which could be any cellular network, such as 3G, 4G, 5G, etc.). If out of signal range, the field module 2 may wait for a signal before automatically
30 broadcasting the communication.

The field module 2 has an interface 16 and/or a display 17, which indicates battery usage and shows that the connection to the local module 3 is maintained. The field module 2 may also comprise a controller 18, which may comprise a processor 19,
35 volatile memory 20, non-volatile memory 21, an input output interface 22, and a bus 23 connecting these components together.

- 17 -

Local module 3

Referring to Figure 3, the local module 3 (also referred to as the Hospital Module (HoM) sits on the local area network (LAN) with the hospital information systems 7, such as the hospital's middleware, laboratory information systems or hospitals EPR.

- 5 The software installed on the module may instead be installed on a hospital server. Only one local module 3 is required for each hospital information system 7, regardless of the number of remote sites or community medical devices 5 that need to be monitored. The local module 3 may be a dedicated hardware device, and may comprise a controller 28, which may comprise a processor 29, volatile memory 30,
10 non-volatile memory 31, an input output interface 32, and a bus 33 connecting these components together. The local module 3 may also have an interface 34 and, optionally, a display 35.

- Software that enables the system 1 to run may be run as a service, for example,
15 the Microsoft™ Windows Service™, or other functionality can then manage the automatic starting of the application (for instance on server boot up). Since instantiation of the application is an automated process, the use of a GUI is not necessary, and the configuration of the application would be done through a text file.

20

The local module 3 connects devices to the required hospital information system 7 within the hospital network 8. The server 7, is configured to provide a fixed IP address accessible by the hospital network 8. The field module 2 and the local module 3 map medical devices to

- 25 the hospital system as described below.

Medical Device Drivers: Each medical devices driver will be programmed to communicate to medical device. Each driver will conform to a standardisation (e.g., Cain Medical Standardisation).

30

Logging and notifications: For each connection the following information is logged, connection status, movement of inbound and outbound packets and error messages. If required, the connection monitoring can push a notification. The following configuration defines the criteria: connect events, disconnect, bad packet
35 events, notification destination IP address/ port.

Server 9

- 18 -

Referring again to Figure 1, working between the field module 2 and the local module 3, the server 9 is configured to pass medical device messages, for example, across a dual redundant private dedicated connection hosted privately away from the public internet. In addition, the server 9 is configured to reduce the communication to a single secured hospital network port.

The server 9 may be configured to communicate out to the hospital using a peer-to-peer IPSec tunnel or private network or dedicated network on, for example, the VPN or NHS Health and Social Care Network (HSCN).

10

Referring also to Figure 4, the server 9 may have similar components to that of the field module 2 and the local module 3. For example, the server 9 may have a controller 40, which may comprise a processor 41, volatile memory 42, non-volatile memory 43, an input output interface 44, and a bus 45 connecting these components together. The local module 3 may also have an interface 46.

15

The server 9 may receive data from the medical device 5 via the field module 2 and the private network 11 through a respective port 50₁, 50₂, 50₃, ..., 50_N which may be determined by the medical device. Once the server 9 has verified the data and confirmed that the data is from an expected medical device 5, it can send the data on to the local module 3 through a single dedicated port 51 and the private network 13 or dedicated network (e.g., the Health and Social Care Network (HSCN)).

20

Medical device 5 communication configurations

The medical devices 5 communicate in two separate ways and the system 1 manages these differences as follows:

25

Community medical device which initiates connections with hospital system: medical devices that initiate connections to the hospital information systems will connect to the IP address of the local module 3 (which is on the hospital LAN). When field module 2 detects a message from the medical device 5, this is routed through the server 9 to the local module 3, which will make a corresponding UDP/TCP transfer to the hospital information system 7.

30

Hospital information systems 7 which initiates connections with community medical devices 5: medical devices 5 to which the hospital information system 7 established connections are processed differently. All medical devices 5 are configured to a

35

- 19 -

single IP address (the IP address of the local module 3 but using different TCP ports to communicate with the hospital information system 7). The local module 3 manages the multiple UDP/TCP ports that distinguish communication for each of the medical devices, and
5 requires the correct mapping to hospital system.

The system 1 allows hospital information systems to communicate with either a medical device interface (e.g., a Cain Medical's medical device interface), drivers or the existing hospital medical device interface drivers (i.e., when medical device
10 driver is already in place to communicate with internal hospital medical devices).

User Requirements

The system 1:

- 15 • enables hospital information systems 7 to communicate with one or more community-based devices 5 through a single monitored and secure port into the hospital.
- enables medical devices 5 out in the community to function and communicate in the same way as a hospital located medical device.
- 20 • securely relays data from medical devices 5 to the hospital information system 7.
- simultaneously interfaces multiple medical devices 5 of any make.
- has a simple user interface, which facilitates an easy set-up and monitoring of functionality.
- 25 • is protected against potential interception with robust end to end encryption and password protection.

The field module 2 can operate without mains supply, e.g., by the use of a battery, or local generator such as a solar panel, and can go beyond that when intermittently charged, e.g., in a paramedic vehicle - the system remains fully
30 operational while on charge.

The system 1 securely relays data without any loss of information even in the event of power or connectivity loss in the field.

35 System 1 Security Requirement

System 1 Security model:

- 20 -

Reduces the number of ports required to cross the hospital IT boundary by mapping and remapping the message crossing the between the server 9 and the local module 3 for example, many POC devices can be connected to hospital information systems with opening a single port or more. That is, the server may be configured to send the data via a single port, and/or to receive data via the same single port from the local module.

Zero Trust Network

The system 1 operates a zero-trust network model, which only lets medical devices 5 communicate with the system 1 and blocks any other users.

Stateful packet inspection (SPI) and Deep packet inspection

Message head and field attributes are intelligently monitored to ensure only legitimate medical device 5 messages are sent and received.

Drivers on the local module 3 or on the server 9 can verify the make and model of the device, reducing the risk of hacking, or other cyber security event, and ensuring that the correct device is in use.

Integrity Control

The server 9 an VPNs 11, 13 ensure medical device 5 messages are not altered or destroyed. The system 1 uses a dedicated internet service, away from any public internet.

Transmission Security

The system has the functionality to encrypt messages which are sent from the field module 2 and decrypt those messages when received by the local module 3. This creates a virtual tunnel so data cannot be intercepted by snoopers, hackers or third parties.

Audit Controls

The server 9 an VPNs 11, 13 offer network visibility by identifying and reporting risks and vulnerabilities. Activity reports provide details on which devices are communicating.

Remote IoT Gateway Management

- 21 -

Remote gateway management, using SSH can be deployed to manage the field module 2 and local module 3 devices which include updating device O/S and firmware.

5 System 1 Security details

10 The unique configuration of the field module 2 will automatically form a connection to the local module 3 via its own virtual private network 11, 13 (VPN). Two key encryption protects this peer-to-peer virtual private network 11, 13 at each end of the system. Therefore, data messages communicated over the Internet will be encrypted and only routed through the VPN 11, 13, i.e., the messages never have an unencrypted format outside the hospital. In the final step between the local module 3 and the hospital information system 7 messages are relayed in the same way as for hospital located medical devices. A hospital firewall 14 can be used in addition to the system 1 security. The firewall 14 may be on the local module 3, or
15 between the server 9 and the local module 3.

A wireless network with encryption is used to prevent local snooping in the vicinity of the medical device. Additionally, the field module 2 and local module 3 will be connected to private networks dedicated to this solution to ensure encryption of
20 patient data between the field module 2 and the local module 3.

Field Module 2 Security

Each paramedic or vehicle 4 will contain a field module 2.

25 Communication between medical device 5 and the field module 2:
Each field module 2 operates with a network (SSID) and password to communicate with any of the medical devices 5. WPA2 / AE256 protects the wirelessly communicated data when possible (WPA2, which can be encrypted with TKIP or AES256. The system 1 may use the same level of encryption of the medical device
30 5, for example, whether TKIP or AES is used may be determined by the capability of the medical device 5.

Communication between the field module 2 and the local module 3:
The field module 2 is configured to hold a SIM card with mobile data for
35 communication to the local module 3. The field module 2 wireless connection (e.g., Wi-Fi) is secured with a password, so only authorised medical devices can connect. The field module 2 connects automatically to the private network (e.g., VPN) 11, 13

- 22 -

only devices which are members of the private network (VPN) are visible to the field module 2. WEP2 / AE256 protects the wireless communication data.

Private network 11, 13 (e.g., VPN) Security

- 5 The Internet component of the solution supports the private network 11, 13 and is accessible from all field modules 2 and the local module 3. The purpose of this component is to act as an encrypted network (switch) between components.

10 A Site-to-Site private network (e.g., VPN) is a fully managed dedicated service with high availability by using two tunnels stream primary traffic through the first tunnel and use the second tunnel for redundancy — if one tunnel goes down, traffic continues to flow.

15 The system can be connected using either IPsec or on the HSCN private (or dedicated) network.

Local module 3 security

20 The local module 3 sits on the same local area network (LAN) as the hospital information systems 7. The local module 3 can use a standard operating system, for example, Windows™ 11 Pro, and can be updated automatically.

25 This traffic will only be from devices in the private network 11, 13 (VPN) on a dedicated internet service 11, 13. The port will be the same port as used by the medical device 5. All other ports can be firewalled, and therefore may not be accessible by third parties.

The local module 3 has port on the hospital local area network to connect to the hospital information system 7 via a range of TCP and UDP ports.

30 The local module 3 can be monitored, will show the status (number of results forwarded, any security issues), this includes blocked messages based on incorrect size and frequency of message and/or incorrect medical device message structure.

Port forwarding

35 A medical device 5 may be acting as a client or a server (although client is the typical case). The system 1 may be configured with the following information to forward network communication:

- Client devices:

- 23 -

- Inbound port
- Outbound port
- Protocol (TCP/UDP)
- Server devices:
 - 5 ○ Server IP Address
 - Server Port
 - Protocol (TCP/UDP)

Packet monitoring

10 The server 9 may be configured to perform checks on the inbound packet size, for example, the maximum packet size. Additional monitoring may be performed, for example, the system 1 may query a separate service to determine whether a packet matches the expected type. This would require the following configuration:

- 15
- Device type – does it match with what is expected
 - Wait for confirmation – block forwarding until positive confirmation (which may create lag in communication)
 - Check one or more, or all packets
 - External service details (i.e., address and port, or driver DLL name)

20

Since the packet checking would be specific to a device, the necessary logic may be incorporated into the driver during driver development.

Multiple forwarders

25 The extender supports multiple devices. To provide this, the extender will consist of a component that handles a single connection, and a management component that can instantiate multiple connection components. The individual connection components can also be instantiated manually to assist debugging issues.

30 Field module 2 communication

The server 9 may be used for extending a point-to-point connection between the healthcare information system and at least one field module 2. Such a configuration may allow messages, for example results, dosages, or other information to be sent from a clinical expert based in the hospital to the field module 2 to be read and
35 acted on by the community care provider (e.g., paramedic, community nurse and the like). The server 9 acts in a similar way as described earlier, but without the communication with the medical device 5.

- 24 -

For example, the server 9 is connected to a local module 3 via a first private network 13. The local module 3 is connected to the healthcare information system 7 based in the hospital. The server 9 is also connected to the field module 2 via a second private network 11. In response to receiving data from the local module 3 the server 9 sends the data to the field module 2 using the second private network 11 to the field module 2. In response to the server 9 receiving data from the field module 2, the server 9 verifies that the data is from the field module 2, and sends the verified data using the first private network 13 to the local module 3. The server 9 may also verify that the data from the local module 3 is from the local module 3 before sending it on to the field module 2. This may help prevent hacks or other cyber security breaches, and also ensures that the data received originates from the correct local module 3, and therefore the correct clinical expert.

Modifications

It will be appreciated that various modifications may be made to the embodiments hereinbefore described. Such modifications may involve equivalent and other features which are already known in the design, manufacture and use of servers configured to extend point to point connections and component parts thereof and which may be used instead of or in addition to features already described herein. Features of one embodiment may be replaced or supplemented by features of another embodiment.

The system can also track the number of results sent and received from the medical device via the field module 2, how much data has been used by the Subscriber Identity Module card (SIM card) of the field module 2, and how often the field module 2 has been used. This can increase security of the field module, server 9, local module 3, and hospital information system 7 because statistical analysis of these data will allow users to track any change in the pattern of usage of one or more of these components. These usage data may also be used to monitor outages of the system and calculate user charges or billing.

Although claims have been formulated in this application to particular combinations of features, it should be understood that the scope of the disclosure of the present invention also includes any novel features or any novel combination of features disclosed herein either explicitly or implicitly or any generalization thereof, whether or not it relates to the same invention as presently claimed in any claim and

- 25 -

whether or not it mitigates any or all of the same technical problems as does the present invention. The applicants hereby give notice that new claims may be formulated to such features and/or combinations of such features during the prosecution of the present application or of any further application derived
5 therefrom.

Claims

1. A server for extending a point-to-point connection between a healthcare information system and at least one medical device, the server configured:
 - 5 to connect to a local module via a first private network, the local module configured to connect to the healthcare information system, and to connect to a field module via a second private network, the field module configured to connect to the at least one medical device;
in response to receiving data from the at least one medical device via a field
10 module, to verify that the data is from the at least one medical device and to send the verified data using the first private network to the local module; and/or
in response to receiving data from the local module to send the data to the medical device using the second private network via the field module.
- 15 2. The server of claims 1 or 2, wherein the server is configured to send the data via a single port, and/or;
to receive data via the single port from the local module.
3. The server of claim 1 wherein the data is verified by checking the data size
20 and/or frequency.
4. The server of any of claims 1 to 3, wherein the verification of the data is performed by the local module or by the server.
- 25 5. The server of any of claims 1 or 4, wherein the data is verified by confirming that the data conforms to a medical device data type corresponding to the medical device networked to the field module.
6. The server of any of claims 1 to 5, wherein the data is verified by confirming
30 the medical device fixed internet protocol address or media access control address.
7. The server of any of claims 1 to 6 wherein the server is configured to communicate with the local module or field module using the transmission protocol expected by the medical device.
35
8. The server of any of claims 1 to 7 wherein the medical device is a point of care medical device.

- 27 -

9. The server of any of claims 1 to 8, wherein the field module is configured to connect to a plurality of medical devices.

5 10. The server of any one of claims 1 to 9 where the server is configured to verify and send data from a plurality of medical devices simultaneously.

11. The server of any of claims 1 to 10, wherein the data received is encrypted data, and the server is configured to decrypt the data.

10

12. The server of any one of claims 1 to 11, wherein the data received is protected using a password, and the server is configured to access the data using the password.

15 13. The server of any one of claims 1 to 12, wherein the field module or server is configured to identify a test type based on the at least one medical device type, and
based on the test type, send data from a test performed on the at least one medical device to an associated local module and/or hospital information system.

20

14. A local module for extending a point-to-point connection between a healthcare information system and at least one medical device, the local module configured:

25 to connect to the healthcare information system;
to connect to a sever via a private network;
in response to receiving data from the server using the private network, to identify an inbound port on the healthcare information system to send the data to the healthcare information system; and/or
in response to receiving data from the healthcare information system, to
30 send data from the healthcare information system to the server.

15. A field module for extending a point-to-point connection between a healthcare information system and at least one medical device, the local module configured:

35 to connect to a server via a private network;
to connect to the at least one medical device; and
to relay data between the at least one medical device and the server.

- 28 -

16. The field module of claim 15, comprising a location module configured to identify the location of the field module.

5 17. The field module of claim 15 or 16, wherein the module comprises an interface configured to allow data input, wherein on receiving an input of data, sends the data to the hospital information system via the server.

18. The field module of any of claims 15 to 17, wherein the field module is
10 configured to:
send medical device data to the healthcare information system; and
receive diagnostic information from the healthcare information system based on the medical device data.

15 19. The field module of any of claims 15 to 18, wherein the field module is configured to:
send medical device data to the healthcare information system; and
receive instruction information from the healthcare information system based on the medical device data.

20 20. A system for extending a point-to-point connection between a healthcare information system and at least one medical device, the system comprising:
a local module connected to the healthcare information system;
a server connected to the local module via a first private network; and
25 a field module connected to the server via a second private network, wherein the field module is configured:
to connect to the at least one medical device; and
to relay data between the at least one medical device and the server;
wherein the server is configured:
30 in response to receiving data from the field module, to verify that the data is from the at least one medical device and to send the verified data to the local module or receive data from the local module;
wherein the local module is configured:
in response to receiving data from the server to forward the data to
35 the healthcare information system; and/or
in response to receiving data from the healthcare information system, to send data from the healthcare information system to the server.

- 29 -

21. The system of claim 20, wherein the system is configured to monitor one or more of:

- 5 field module location;
field module data usage;
field module activity; or
field module data sent to the server.

22. The local module, the field module, or the system of any of claims 14 to 21,
10 wherein the data is encrypted data and either the server, the field module, or the local module is configured to decrypt the data.

23. The local module, the field module, or the system of any of claims 14 to 22,
15 wherein the data is protected using a password, and either the server, the field module, or the local module is configured to access the data using the password.

24. A server for extending a point-to-point connection between a healthcare information system and at least one field module, the server configured:
to connect to a local module via a first private network, the local module
20 configured to connect to the healthcare information system, and to connect to a field module via a second private network;
in response to receiving data from the local module to send the data to the field module using the second private network via the field module; and/or
in response to receiving data from the at least one field module, to verify
25 that the data is from the at least one field module, and to send the verified data using the first private network to the local module.

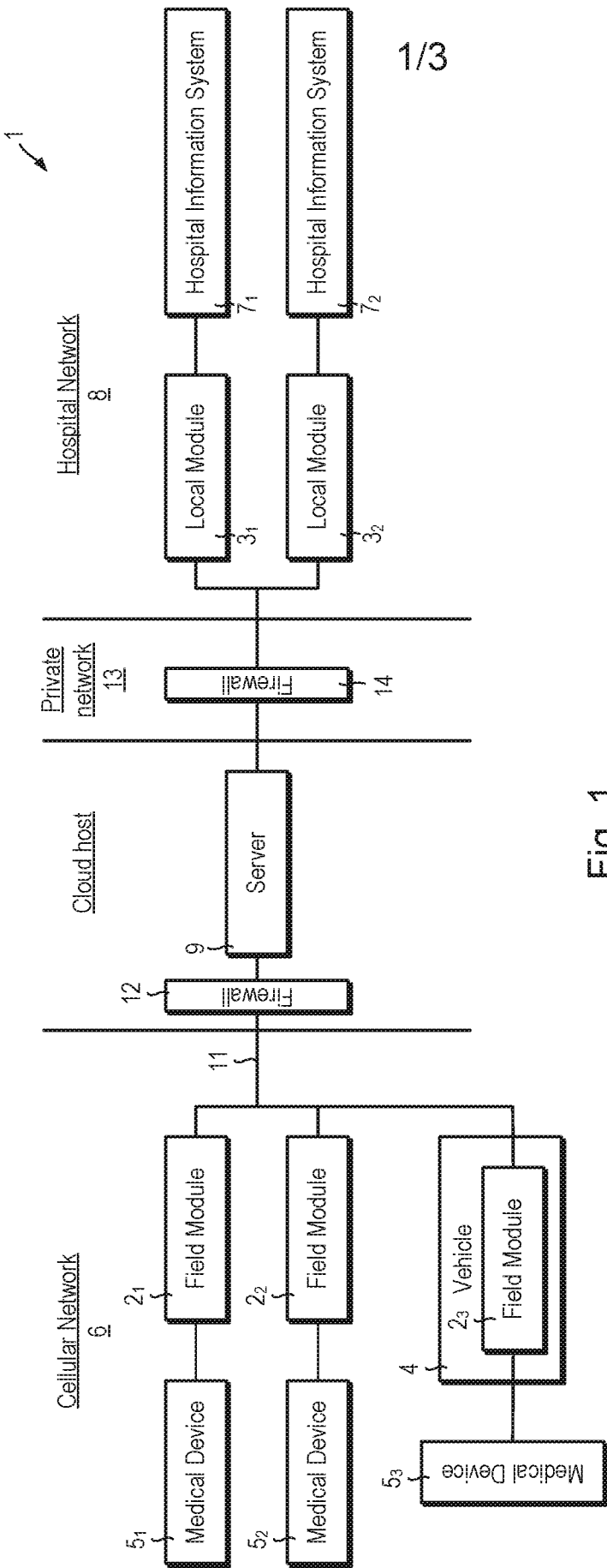


Fig. 1

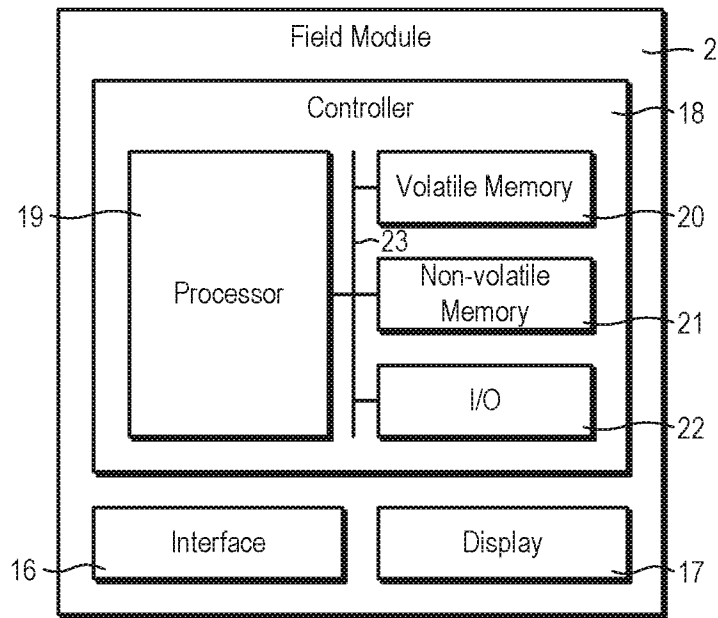


Fig. 2

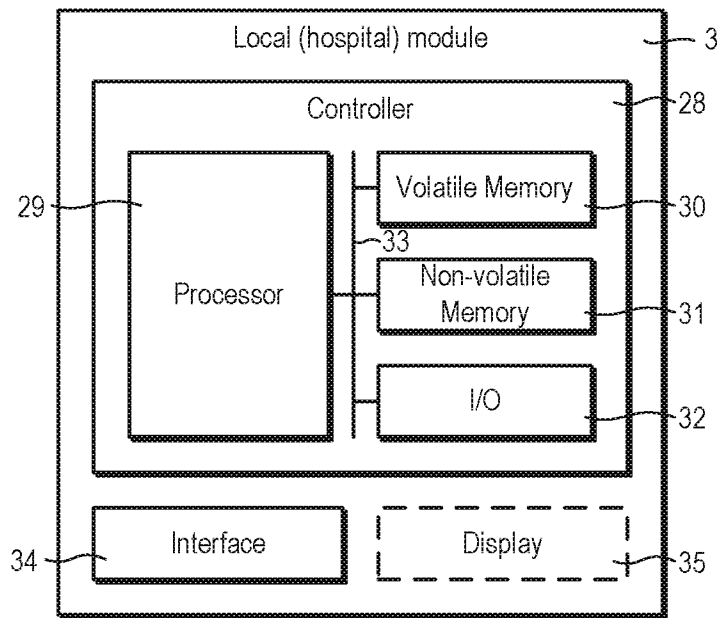


Fig. 3

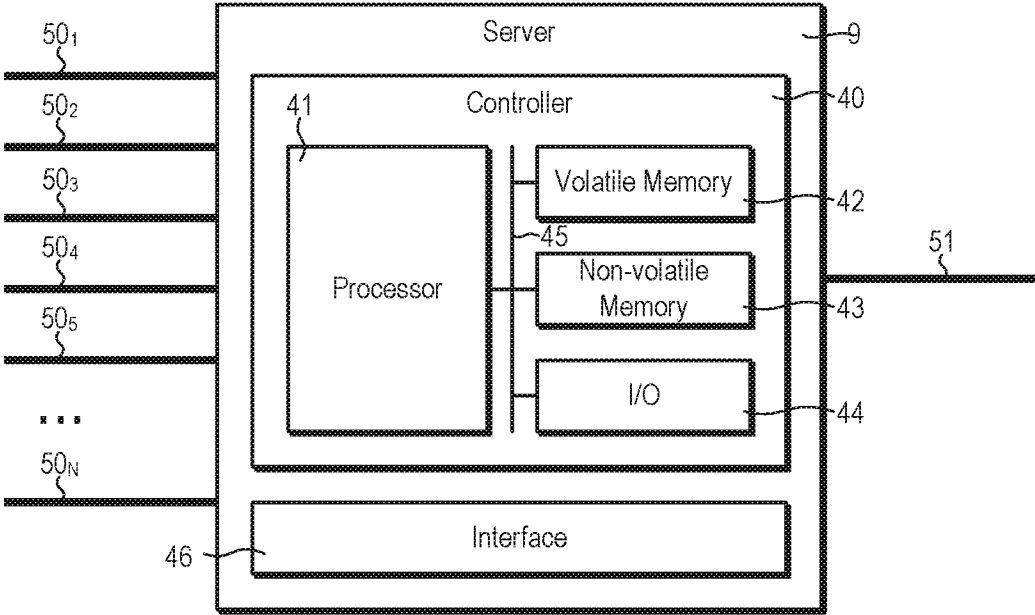


Fig. 4

INTERNATIONAL SEARCH REPORT

International application No

PCT/GB2024/051694

A. CLASSIFICATION OF SUBJECT MATTER INV. G16H40/40 G16H40/67 ADD.		
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) G16H		
Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched		
Electronic data base consulted during the international search (name of data base and, where practicable, search terms used) EPO-Internal		
C. DOCUMENTS CONSIDERED TO BE RELEVANT		
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2022/059216 A1 (LEWIS RONALD A [US]) 24 February 2022 (2022-02-24) abstract; figures 4-6 paragraph [0018] - paragraph [0043] paragraph [0095] - paragraph [0130] -----	1 - 24
☐ Further documents are listed in the continuation of Box C. ☒ 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 14 October 2024		Date of mailing of the international search report 24/10/2024
Name and mailing address of the ISA/ European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016		Authorized officer Menschner, Philipp

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No

PCT/GB2024/051694

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2022059216	A1	24-02-2022	NONE
