



(12)发明专利

(10)授权公告号 CN 104885087 B

(45)授权公告日 2018.12.11

(21)申请号 201380068395.2

(22)申请日 2013.12.26

(65)同一申请的已公布的文献号
申请公布号 CN 104885087 A

(43)申请公布日 2015.09.02

(30)优先权数据
61/745,833 2012.12.26 US

(85)PCT国际申请进入国家阶段日
2015.06.26

(86)PCT国际申请的申请数据
PCT/IB2013/061334 2013.12.26

(87)PCT国际申请的公布数据
W02014/102726 EN 2014.07.03

(73)专利权人 皇家飞利浦有限公司

地址 荷兰艾恩德霍芬

(72)发明人 P·吉尼 M·P·B·伊利卡尔
W·D·格鲁贝 T·兰德尔

(74)专利代理机构 永新专利商标代理有限公司
72002

代理人 李光颖 王英

(51)Int.Cl.
G16H 40/67(2018.01)

(56)对比文件
US 2008/0021834 A1,2008.01.24,
CN 1427344 A,2003.07.02,

审查员 申晓科

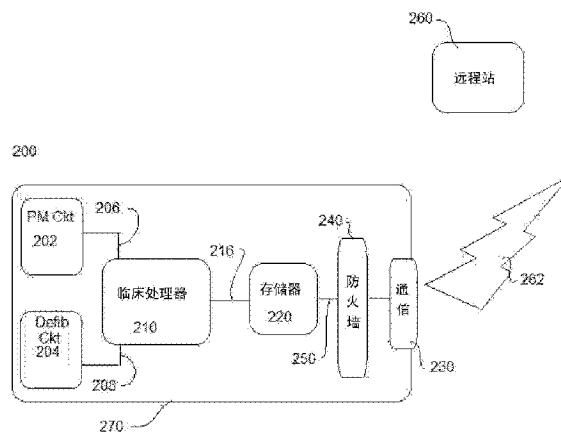
权利要求书2页 说明书8页 附图5页

(54)发明名称

监测器除颤仪远程医疗服务器

(57)摘要

描述一种将除颤仪、患者监测器和远程医疗服务器进行组合的系统和设备(200)。所述设备实现了一种方法,藉由该方法外部系统或远程站可以从所述设备“拉取”数据,而无需操作者动作或介入。通过防火墙电路(240)维持所述设备(200)中的安全关键性特征和非安全关键性特征分开,使得所述远程站不能对所述设备写入数据。



1. 一种具有集成的远程医疗服务器的监测器除颤仪,所述集成的监测器除颤仪远程医疗服务器包括:

患者监测电路(202);

除颤治疗电路(204);

临床处理器(210),其能够从所述患者监测电路和所述除颤治疗电路收集患者数据;

存储器(220),其能够从所述临床处理器接收所述患者数据,并以通用文件格式来存储接收到的患者数据;

通信接口(230),其被设置为与所述存储器只读通信,并且还能够将所述通用文件格式的所述患者数据传输到远程站;

防火墙电路(240),其被设置在所述存储器与所述通信接口之间并且能够防止从所述通信接口接收到的任何数据对所述存储器的写入;以及

统一外壳(270),其用于容纳所述患者监测电路、所述除颤治疗电路、所述临床处理器、所述存储器、所述通信接口以及所述防火墙电路中的每个。

2. 如权利要求1所述的监测器除颤仪,其中,所述通信接口还能够将所述患者数据单向传输到所述远程站。

3. 如权利要求1所述的监测器除颤仪,其中,所述通信接口包括从包括蓝牙、WiFi和蜂窝电话的组中选择的无线通信接口。

4. 如权利要求1所述的监测器除颤仪,其中,所述通信接口包括有线以太网接口。

5. 如权利要求1所述的监测器除颤仪,其中,所述通用文件格式是从包括可扩展标示语言(XML)、便携式文档格式(PDF)以及后记码(PS)文件格式的组中选择的。

6. 如权利要求1所述的监测器除颤仪,其中,所述通信接口还能够自动地将所述患者数据传输到所述远程站,而无需操作者动作。

7. 如权利要求1所述的监测器除颤仪,其中,所述存储器还能够将接收到的患者数据存储在通过事件标题识别的文件夹中。

8. 如权利要求7所述的监测器除颤仪,其中,接收到的患者数据被存储在通过所述数据被收集的日期/时间来布置的所述文件夹中。

9. 如权利要求1所述的监测器除颤仪,还包括具有多个被安全地分离的子处理器的单核处理器,其中,所述临床处理器和所述防火墙电路分别能够被设置在所述多个子处理器中的一个上。

10. 如权利要求9所述的监测器除颤仪,其中,所述临床处理器还能够执行安全关键性功能和非安全关键性功能,并且其中,所述安全关键性功能还能够被设置在所述多个子处理器中作为实时操作系统(RTOS)的一个上。

11. 一种用于将患者数据从监测器除颤仪提供到远程站的系统,包括:

远程医疗服务器(510),其具有临床处理器、可隔离存储器、防火墙电路以及通信接口,其中,所述远程医疗服务器被与监测器除颤仪电路集成以获得所述患者数据;以及

收发器(520),其被定位在所述远程站处与所述通信接口通信,其中,所述远程医疗服务器响应于来自所述远程站的针对数据的请求而将所述患者数据传输到所述远程站,并且其中,所述防火墙电路被设置在所述可隔离存储器与所述通信接口之间并且能够防止由所述通信接口从所述远程站接收到的任何数据对所述可隔离存储器的写入。

12. 如权利要求11所述的系统,其中,所述远程医疗服务器能够防止从所述远程站接收的外部数据被写入到所述可隔离存储器。

13. 如权利要求11所述的系统,其中,所述患者数据被以通用文件格式存储在所述可隔离存储器中。

14. 如权利要求11所述的系统,还包括与所述远程医疗服务器通信的患者监测电路和除颤治疗电路,所述患者监测电路和所述除颤治疗电路每个与所述远程医疗服务器一起被共同定位在统一外壳中,并且其中,所述患者监测电路和所述除颤治疗电路还能够生成所述患者数据。

15. 如权利要求11所述的系统,其中,所述远程医疗服务器还能够在获得所述患者数据时将所述患者数据传输到所述收发器。

监测器除颤仪远程医疗服务器

技术领域

[0001] 本发明涉及一种用于从在远程站处使用的监测器除颤仪获得患者数据的经改进的装置和方法。所述监测器除颤仪被与远程医疗服务器集成,使得外部系统可以使用标准通信接口和只读通信协议来获得数据。

背景技术

[0002] 监测器除颤仪从跨越从健康到危重症的范围的宽泛的患者频谱收集临床数据。许多这样的监测器除颤仪被在远离健康护理设施的位置处的急救医疗系统 (EMS) 护理者所采用。普遍认为,当由EMS收集的临床数据在患者到达之前被传输到健康护理设施时,患者结果得以改善。

[0003] 临床数据从监测器除颤仪到健康护理设施的传输有多重目的。传输提醒护理设施到来的患者的临床病况。数据的分享允许现场医生与在护理设施处的护理者之间的会诊。再者,临床数据到中央位置的例行传输实现了对电子患者护理记录 (ePCR) 的集合与归档存储。

[0004] 最近的健康护理改革的努力也已经提出了关于对EMS护理者管理并传输与EMS患者护理相关联的数据的需求的更大重视。准确且全面的患者护理记录被认为是优质护理的经改善的责任性、更有效的结算流程以及减少 (源自具有负面结果的医疗响应的) 诉讼的前提条件。

[0005] 将患者数据从患者的位置传输到医院处的中央位置的必要性已经产生了具有集成的遥测电路的若干医学设备。Roznov的2007年11月1日公开的题为“Internet-Protocol Based Telemetry Patient Monitoring System”的美国专利公开No.2007/0255120A1描述了这样的标准患者遥测系统。如图1中图示的,Roznov描述了一种具有多个便携式遥测设备12-18的系统,便携式遥测设备12-18与访问点20无线通信。便携式遥测设备12-18经由有线网络的连接24与信息系统22双向处理IP数据包。数据包典型地是实时生理和控制信息。

[0006] 便携式遥测设备12-18例如经由连接28通过访问点20与有线网络上的设备 (例如平板计算机26) 进行通信。任选的访问点控制器34控制并引导信号经由连接32通过访问点20。

[0007] 在Gordner等的2003年3月27日公开的题为“Health Monitoring System”的国际公开W0 03/025826A2中描述了类似的发明。其中,患者监测系统由与中央应用服务器1无线通信的患者监测器2构成,中央应用服务器1存储患者数据以用于由多个工作站4访问。所述患者监测器可以与除颤仪相关联。

[0008] 在Moore等的2006年7月6日公开的题为“Providing Data Destination Information to a Medical Device”的国际公开W0 2006/071711中描述了另一类似的监测发明。Moore等教导了一种可以被配置为将医学事件信息传输到选定的数据目的地的医学设备。在传输之前,用户必须选择并以“推”的方式启动数据传输。Moore等的医学设备可以是外部除颤仪。

[0009] 在Hansen等的2010年9月30日公开的题为“Portable Device and Method of Communication Medical Data Information”的美国专利公开2010/0250697中描述了将医学设备部分和单独的通信部分两者并入同一外壳内的发明。Hansen等的电路旨在将复杂的通信功能从关键医学应用中分开。医学设备部分控制其与通信部分之间的全部数据流。

[0010] 在Chen等的2006年8月24日公开的题为“Method and Apparatus for Two-Way Transmission of Medical Data”的美国专利公开2006/190999A1中描述了另一防火墙相关的发明。Chen等教导了一种被定位在健康护理提供者与第三方之间的安全防火墙,以用于在两者之间安全地共享患者图像数据。所述防火墙被设计为利用推拉式控制机制实现双向数据流。

[0011] 前述引用中的每个都以类似的方式操作。每个均提供了电路设计以及相关关联的用户界面,所述用户界面相对复杂并且因此是次优的。具体而言,每个医学监测设备的用户都必须采取特定行动以设置和/或配置所述设备,以将数据从设备“推”到远程站。每个引用的设备都需要操作者设置监测器除颤仪电路以选定的格式向选定的位置传输,或者必须经由用户界面来启动传输本身。这些系统和方法可以适用于临床诊断环境,但它们在紧急心脏患者处置协议中分散注意力并可能令人困惑,在紧急心脏患者处置协议中,节省的每一刻都提高积极的患者结果的机会。收集并传输患者数据的必要的动作可能将注意力从即刻的患者护理步骤转移开,并且可能引入在传输或救治中的错误的可能性。第三,所记载的引用每个都需要驻留在设备和远程站两者处的定制接口软件,以便于使数据链的两侧一致并解码来自患者医学设备的临床数据。针对医学应用的对接口的开发和认证是昂贵的,这必须在每次修改接口时被重复以满足不断演进的通信标准。定制接口软件还对系统优化的定制格式来保存患者数据。除非外部系统含有相同的软件,否则不能读取数据。

[0012] 因此,需要的是一种用于以避免现有技术存在的问题的方式容易地将由诸如监测器除颤仪的医学设备获得的患者信息与外部系统共享的方法和装置。

发明内容

[0013] 根据本发明的原理,描述了一种经改进的医学设备装置,所述医学设备装置包括具有集成的远程医疗服务器的医学监测器除颤仪。所述装置包括患者监测电路和除颤治疗电路,所述患者监测电路和除颤治疗电路收集患者数据并将其传达到临床处理器。存储器从所述临床处理器接收所述患者数据并且以通用文件格式存储接收到的患者数据。通信接口被设置为与所述存储器只读通信并且将所述患者数据传输到远程站。防火墙电路防止从所述通信接口接收到的任何数据对所述存储器的写入。所述电路元件中的每个都被容纳在统一外壳中。

[0014] 根据本发明的原理,还描述了一种包括具有集成的远程医疗服务器的监测器除颤仪的系统,所述远程医疗服务器与被定位在远程站处的收发器通信。所述系统被设置为使得所述远程医疗服务器响应于来自所述远程站的对数据的请求而将所述患者数据传输到所述远程站,即对数据流的“拉取”方法。所述系统因此实现了无需操作者的动作或介入的对数据的传输。通过经由标准通信接口并以通用格式对存储在隔离的远程医疗服务器存储器中的所述数据进行布置,消除了对用于与设备接合并解码数据的定制软件的需要。因此实现了较低的成本和较大的可靠性。

[0015] 根据本发明的原理的还是一种用于使用与以上描述的类似的系统将患者数据从具有患者监测电路和除颤治疗电路的监测器除颤仪远程医疗服务器传输到远程站的改进的方法。所述方法包括响应于来自所述远程站的请求而自动地将所述患者数据从所述远程医疗服务站传输到所述远程站的步骤。

[0016] 本发明的范围覆盖了具有通信能力的医学设备。具体而言,诸如由医院的人员使用但与中央服务器分开的医院内监测器除颤仪、以及由在远离医院的位置处的紧急医疗服务(EMS)人员使用的入院前监测器除颤仪的设备可以得益于该创新性的特征。

[0017] 本发明的另一目的是总体上描述一种除颤仪监测器,所述除颤仪监测器将非安全关键性应用和安全关键性应用一起执行,而不影响安全关键性功能的安全性、可靠性和性能。除颤仪监测器设备的安全关键性功能包括为患者提供关键治疗(例如起搏、CPR和除颤治疗)和/或对患者进行监测(例如ECG、血液监测(例如氧、二氧化碳和压力))。非安全关键性功能和应用包括电子患者护理记录(ePCR)应用、事件总结回顾、以及事件后分析。具体而言,本发明采用运行两种功能的多核处理器。实时操作系统(RTOS)和存储器管理单元(MMU)在所述多核处理器的单独的核上运行。非安全关键性功能在所述多核处理器的不同的核上运行。因此在安全关键性功能与非安全关键性功能之间建立了安全防火墙分离。

附图说明

[0018] 附图中:

[0019] 图1图示了根据现有技术的医学患者遥测系统。

[0020] 图2图示了根据本发明的优选实施例的除颤仪监测器远程医疗服务器的方框图。

[0021] 图3图示了与根据本发明的优选实施例的除颤仪监测器远程医疗服务器一起使用的患者数据文件存储系统的一个实施例。

[0022] 图4是根据本发明的实施例的除颤仪监测器远程医疗服务器的外部视图。

[0023] 图5图示了根据本发明的另一实施例的除颤仪监测器远程医疗服务器和远程站系统的方框图。

[0024] 图6图示了示出该创新性方法的优选实施例的流程图。

[0025] 图7图示了根据本发明的一个实施例的防火墙电路,在所述防火墙电路中公用的多核处理器内共享诸如除颤仪监测器远程医疗服务器的设备内的安全关键性功能和非安全关键性功能。

具体实施方式

[0026] 现在转到图示,图2是本发明的示范性除颤仪监测器远程医疗服务器200的功能性方框图。除颤仪监测器远程医疗服务器200的某些功能部分被定义为安全关键性的,所述功能部分总体上由与患者护理直接相关的硬件和软件组成。安全关键性特征包括被直接用于感测和监测患者的状况的那些电路。这样的范例是心电图(ECG)、心率、血压和血氧,以及呼吸监测。安全关键性特征也包括被用于向患者提供治疗的那些电路。这样的范例是心脏除颤与起搏电路。由于安全关键性电路的故障可能导致患者受伤或死亡,因此安全关键性电路在它们的设计与制造上必须符合可靠性、性能和安全性的严格标准。

[0027] 除颤仪监测器远程医疗服务器200也包括非安全关键性的功能部分。诸如电子患

者护理记录应用、事件总结回顾数据存储、以及事件后分析电路的功能并不直接影响患者护理。非安全关键性功能一般在它们的设计性能和制造上需要较少的严苛性。

[0028] 图2中所示的除颤仪监测器远程医疗服务器200的主要元件包括:临床处理器210,其从患者监测电路202和除颤治疗电路204获得患者及事件数据;可隔离存储器220;防火墙电路240;以及通信接口230,其提供针对外部系统的只读访问以读取存储在存储器220中的临床数据。图2并不旨在描绘或排除任意特定的硬件或软件实施方式。

[0029] 在图2的实施例中,除颤仪监测器远程医疗服务器200的安全关键性部分包括患者监测电路202、除颤治疗电路204、以及临床处理器电路210。患者监测电路202包括大体上实时获得患者医学参数并经由患者监测数据路径206将获得的数据传送到临床处理器210的传感器。除颤治疗电路204为患者提供除颤和/或起搏治疗。除颤治疗电路204经由除颤治疗数据路径208将有关感测到的患者参数以及与事件相关的除颤/起搏操作的数据传达到临床处理器210。

[0030] 在优选的实施例中,临床处理器210控制DMTS 200的监测功能和治疗功能的全部。在该实施例中,临床处理器210、患者监测电路201和除颤仪治疗电路204的全部功能可以由单个处理器来执行。临床处理器210也能够借助于到临床处理器的麦克风和/或相机输入(图2中未示出)来捕捉对救治事件的记录。

[0031] 在备选的实施例中,临床处理器210、患者监测电路201和除颤仪治疗电路204每个都是单独的物理处理器。在另一个备选实施例中,患者监测电路201和除颤仪治疗电路204独立于临床处理器210操作。临床处理器210因此具有两个主要功能。临床处理器210能够计算并递送治疗。临床处理器210还能够从电路收集数据并将数据处理为临床数据,并且接着存储经处理的临床数据以供进一步使用。

[0032] 临床处理器210优选地将来自患者监测电路201和除颤仪治疗电路204的数据处理成被以通用文件格式布置的经处理的临床数据。通用文件格式是能由广泛可用的软件程序读取的那些格式。这样的通用文件格式的当前范例包括但不限于可扩展标示语言(.xml)、便携式文档格式(.pdf)和/或后记码(.ps)。外部系统因此可以访问这样布置的临床数据而无需任何特定的软件。

[0033] 较不优选的实施例将临床数据布置为定制文件格式。在该实施例中,在DMTS 200外部的任何系统都将需要特殊软件以解码文件信息。

[0034] 临床处理器210经由读写通信路径216将经处理的临床数据保存到可隔离存储器空间220。注意到,临床处理器210可以要求对来自存储器220的临床数据的取读访问,以供DMTS 200内部的功能(例如显示和用户指示)使用。

[0035] 图3图示了针对被存储在可隔离存储器220中的经处理临床数据的优选布置。旨在用于外部系统访问的数据文件优选地符合针对患者临床数据记录建立的标准,例如国家EMS信息系统(NEMIS)。如图3所示,患者数据记录300与识别数据的性质的患者数据文件名称一起被存储在患者数据文件320中。患者数据文件320继而被布置在患者数据文件夹310中,患者数据文件夹310可以通过事件名称、日期和时间而被识别。患者数据文件夹310在存储器220中的目录优选地对于外部系统能只读访问,只要DMTS 200通电并有效。

[0036] 可以通过若干方法在以上布置中获得对患者保密规则的符合。临床处理器210可以被使得能够在存储器220中存储之前使患者数据匿名。也可以采用密码或其他合适的安

全方法来限制外部系统对患者数据文件夹310的访问。

[0037] 返回图2,可以由外部系统260经由通信接口230来访问位于可隔离存储器220中的临床患者数据。优选地,通信接口230是无线接口,所述无线接口的类型包括但不限于蓝牙.TM、Wi-Fi或蜂窝电话接口。通信接口230也可以是有线接口,所述有线接口的类型包括但不限于通用串行总线(USB)和以太网。通信接口230与外部系统260之间的传输路径优选地是只读的,即响应于来自外部系统的对患者数据的请求从通信接口230传输到外部系统260。

[0038] 防火墙电路240被沿可隔离存储器220与通信接口230之间的防火墙通信路径250设置。防火墙电路240能够允许在通信接口230处对位于存储器220中的患者临床数据的只读访问。防火墙电路240还能够阻挡从通信接口230接收到的任何数据对存储器220的写入。防火墙电路240因此消除了破坏安全关键性软件程序和数据的任何外源性途径。防火墙电路240因此将DMTS 200的安全关键性功能与非安全关键性功能分离。

[0039] 图4图示了DMTS 200的一个外部视图。统一外壳270容纳患者监测电路202、除颤治疗电路204、临床处理器210、存储器220以及防火墙电路240中的每个。示出的被安装在外壳270的外表面上的是通信接口230。这仅是为了图示,因为应当理解通信接口电路230被容纳在外壳内,并且仅天线或通信端口被设置在外部。优选地,通信接口230的全部部件都被容纳在外壳270里面。在图示的实施例中,从设备的只读传输路径是无线传输。

[0040] 图5中示出的图示了根据本发明另一实施例的除颤仪监测器远程医疗服务器与远程站系统500的方框图。系统500包括与监测器除颤仪一起被集成在公共的统一外壳中的远程医疗服务器510,以及被设置在远程位置处的中央监测站处的收发器520。远程医疗服务器510的内部布置和部件可以与如前文描述的图2的实施例相似。具体而言,远程医疗服务器510可以包括由防火墙电路240保护的可隔离存储器220。患者数据被存储在服务器存储器220中。优选地,如前文讨论的,患者数据被以通用文件格式存储。

[0041] 远程医疗服务器510和收发器520经由只读传输路径262通信链接。因此,远程医疗服务器510响应于来自远程站的对数据的请求而将患者数据传输到远程站收发器520。远程医疗服务器510优选地被设置成为了执行数据传输,除了请求之外什么都不需要,而没有对先前的设定或本地用户动作的任何需要。远程医疗服务器510和收发器520中的通信接口230每个都可以是无线的或者可以一起是有线的。

[0042] 远程医疗服务器510也能够阻挡或防止外部数据(包括对应于来自远程站的请求的数据)被写入到内部服务器存储器220。防火墙电路240防止对系统的安全关键性部分(例如包括患者监测电路202和除颤治疗电路204)的破坏。电路202和204继而能够生成患者数据。

[0043] 源于远程医疗服务器系统500的益处通过对其操作的描述而变得清楚。通过将非安全关键性的通信部分和安全关键性的患者监测与治疗部分共同定位在远程医疗服务器外壳270内,设备一被开启操作者就具有与远程站的即时的电信能力。服务器不需要在用于传输数据的操作之前的设定,这是因为其可以在每次被开启时自动地从任何可用的网络获得互联网识别符。此时,服务器可以自动地将其识别符传输到固定在服务器存储器内的预定网站。接着服务器仅等待启动对存储在存储器中的数据的传输的授权请求。远程医疗服务器510也可以被设置为一获得患者数据就将患者数据传输到先前授权的远程收发器520。

[0044] 该创新性系统也更容易随着电信协议随时间的变化而被修改。众所周知,安全关键性医学系统在设计过程中需要高度的严苛性,并且经受严格的检验和确认过程,以便于明确可用。通过利用防火墙240将安全关键性医学系统部分与电信部分分开,发明人已创建了这样的医学设备,其通信电路可以被修改而几乎不需要或者不需要对安全关键性部分的再验证,即使全部电路都位于同一统一外壳中。

[0045] 图6图示了示出用于将患者数据从监测器除颤仪传送到远程站的方法600的流程图。第一步骤610包括在患者位置处提供被集成在监测器除颤仪的外壳内的远程医疗服务器(610)。所集成的远程医疗服务器包括临床处理器,所述临床处理器能够从患者监测电路和除颤治疗电路收集患者数据。服务器还包括存储器,所述存储器能够从临床处理器接收患者数据并以通用文件格式存储接收到的患者数据。与外部系统的服务器接口包括:通信接口,其被设置为与存储器只读通信,并且还能够将通用文件格式的患者数据传输到远程站;以及防火墙电路,其被设置在存储器与通信接口之间,并且能够防止从通信接口接收到的任何数据对存储器的写入。

[0046] 为了完成通信设定,第二步骤620包括提供在远程站处的收发器,并在所述收发器与通信接口之间建立通信路径。该第二步骤620可以是在远程医疗服务器在前一提供步骤中被开启时使用服务器中的通信参数自动完成的,所述通信参数是在工厂预载入的或者在对服务器的之前使用期间先期建立的。

[0047] 在提供步骤610完成之后,将监测器除颤仪投入使用以处置患者。患者数据在收集步骤630中由临床处理器自动收集,并且在存储步骤640中被以通用文件格式存储在服务器存储器中。存储步骤640可以任选地包括以符合针对患者临床数据建立的标准的方式来存储患者数据。

[0048] 方法600还预期在步骤620中建立通信路径之前进行收集步骤630和存储步骤640。这种状况可能出现服务器与远程站之间不存在可用的有线或无线连接的患者位置中。

[0049] 远程站收发器在请求步骤650中开始对来自远程医疗服务器的患者数据的“拉取”。远程医疗服务器经由通信路径接收请求,并自动地确定请求者是否被授权数据共享。此外,服务器中的防火墙电路阻挡来自收发器的任何数据被写入用于存储患者数据的同一存储器。

[0050] 图6中从请求步骤650到收集步骤630的输出的上虚线指示最优方法,在所述最优方法中开启远程医疗并且建立通信路径,但其中,患者尚未被设备处置。在这种状况下,收集步骤630可以在从收发器接收到请求步骤650之后开始。

[0051] 在做出远程站是经授权的数据接收者的确定之后,远程医疗服务器经由在传输步骤660中建立的通信路径将患者数据传输到远程站。传输步骤660优选地仅响应于请求步骤650自动地发生。

[0052] 图7图示了防火墙电路的另一实施例,在该实施例中诸如除颤仪监测器远程医疗服务器的设备内的安全关键性功能和非安全关键性功能由单独的处理器模块来执行。单独的处理器模块在物理上是分开的,但位于单个多核处理器400内。可以为存储器管理单元的防火墙电路430被设置在单独的子处理器408中的一个上。子处理器中的另一个402操作安全关键性的临床处理器420。临床处理器420可以在子处理器402中的RTOS上运行。子处理器中的又一个404操作通用的非安全关键性程序440,例如通信程序。防火墙电路430提供从临

床处理器420到外部存储器406的读写能力。防火墙电路430还阻挡从非安全关键性程序440到存储器406中的任何写入能力。因此,建立了安全关键性功能与非安全关键性功能之间的安全的分区防火墙410。

[0053] 以上描述的实施例使得监测器除颤仪设备能够同时在单个硬件单元上运行安全关键性应用和ePCR应用。该实施例也可以利用多核处理器中的硬件辅助虚拟化特征以及RTOS的安全虚拟化支持。该实施例间接的使用处理器的RTOS和存储器管理单元(MMU)的资源管理与保护能力来创建安全的分区防火墙,以用于同时地并安全地运行安全关键性应用以及非安全关键性应用。

[0054] 可以以多种方式来设置以上描述的实施例。一种安全地隔离关键性功能与非关键性功能的方式是在单独的处理器模块上运行它们,所述单独的处理器模块在物理上是分开的,但位于单个硬件单元或设备中。安全关键性应用在处理器中具有专用CPU、存储器和其他所需设备和外围设备的一个中的实时操作系统(RTOS)上运行。非关键性应用在单独的处理器中的通用操作系统上运行,而不允许影响安全关键性应用的资源。显示、记录和存储器存储单元/模块将来自关键性应用和非关键性应用两者的输出合并。安全关键性用户界面控制被直接映射到安全关键性应用,以便于不受非安全关键性应用的可靠性、安全性或性能问题的影响。因此将安全关键性应用从非安全关键性应用保护起来,即使它们位于同一设备中。因此,安全关键性应用将正常起作用,即使非关键性应用未能正确地起作用。

[0055] 在备选的但更有效且更便宜的实施方式中,安全关键性应用直接在被映射到多核处理器的一个或多个专用核的RTOS上运行。非安全关键性应用一起运行,但是使用由RTOS提供的安全虚拟化技术在处理器中被映射到通用操作系统(例如Windows.TM)的其他核上运行。针对该实施方式选择的多核处理器将支持硬件辅助虚拟化特征,使得RTOS虚拟化实施方式可以利用得到的效率和经改进的性能。

[0056] 也可以在位于患者位置处的单独的功能单元上进行对从关键性应用和非关键性应用两者生成的数据的显示、记录和存储、以及用户界面控制。如果显示是在单独的单元上而不是在运行所述应用的单元上,则数据和控制请求可以在线缆上或无线地被传输到显示单元或从显示单元传输。无论是集成的还是单独的显示器,都可以使用单次按钮按下或对屏幕的触摸来实现除颤仪/监测器与ePCR应用之间的切换。除颤仪和监测器功能将具有最高优先级。设备因此保留自动地切换到除颤仪/监测器功能或者在需要临床注意的情况下警告用户从非安全相关的功能切换到除颤仪/监测器功能的能力。

[0057] 对如以上描述的设备、方法和显示的修改也被包括在本发明的范围内。例如,对满足所描述的发明的目的的临床处理器电路的各种配置落入权利要求的范围内。外部设备外壳的具体外观和布置也可以是不同的。

[0058] 应理解,尽管已经按照医学应用描述了本发明,但本发明的教导要宽泛的多并且适用于非医学应用及用途。另外,如本领域普通技术人员鉴于本文中提供的教导将意识到的,本公开/说明书中描述的和/或附图中描绘的特征、元件、部件等可以被以硬件和软件的各种组合来实现,并提供可以被组合在单个元件或多个元件中的功能。例如,可以通过使用专用硬件以及能够与合适的软件相关联地执行软件的硬件来提供附图中示出/图示/描绘的各个特征、元件、部件等的功能。当由处理器来提供功能时,可以由单个专用处理器、由单个共享处理器,或由其中一些能够被共享和/或复用的多个独立处理器来提供功能。此外,

对术语“处理器”或“控制器”的明确的使用不应被解释为排他地指代能够执行软件的硬件，并且能够暗含地包括但不限于，数字信号处理器(“DSP”)硬件、用于存储软件的只读存储器(“ROM”)、随机存取存储器(“RAM”)、非易失性存储器、以及虚拟的能够(和/或可配置为)执行和/或控制过程的任何装置和/或机器(包括硬件、软件、固件及其组合等)。

[0059] 此外，本文记载原理、方面和本发明的实施例及其具体范例的所有陈述旨在包括其结构等价方案和功能等价方案两者。此外，旨在使这样的等价方案包括目前已知的等价方案以及将来发展出的等价方案(例如发展出的可以执行相同或基本相似的功能的任何元件，而不论其结构如何)两者。因此，例如，本领域技术人员鉴于本文中提供的教导应当意识到本文提出的方框图表示说明性系统部件的概念性视图和/或实现本发明的原理的电路图。相似地，本领域技术人员鉴于本文中提供的教导应当意识到任何流程图表、流程图等表示各个过程，这些过程可以基本在计算机可读存储媒体中表示并且因此由这样的计算机或处理器执行，不论是否明确示出了这样的计算机或处理器。

[0060] 此外，本发明的示范性实施例可以采取能够从计算机可用或计算机可读存储介质访问的计算机程序产品的形式，所述计算机可用或计算机可读存储介质提供由计算机或任何指令执行系统使用或结合计算机或任何指令执行系统使用的程序代码。根据本公开，计算机可用或计算机可读存储介质能够是可以包括、存储、传送、传播或输送由指令执行系统、装置或设备使用或结合指令执行系统、装置或设备使用的程序的任何装置。这样的示范性介质可以是电子、磁性、光学、电磁、红外线或半导体系统(或装置或设备)或者传播介质。计算机可读介质的范例包括半导体或固态存储器、磁带、可移动计算机磁盘、随机存取存储器(RAM)、只读存储器(ROM)、硬磁盘和光盘。光盘的当前的范例包括只读光盘(CD-ROM)、读/写光盘(CD-R/W)和DVD。另外，应当理解今后可能发展出的任何新的计算机可读介质也应被认为是根据本发明和公开的示范性实施例可以使用或指代的计算机可读介质。

[0061] 已经描述了根据本发明的系统、设备和方法的优选且示范性的实施例(所述实施例旨在是说明性的而不是限制性的)，注意到本领域技术人员鉴于本文中(包括附图)提供的教导可以做出对这样的示范性实施例的修改和变型。因此应当理解，可以在本发明和本文中公开的示范性实施例的范围内，对本公开优选且示范性的实施例做出这样的变化。

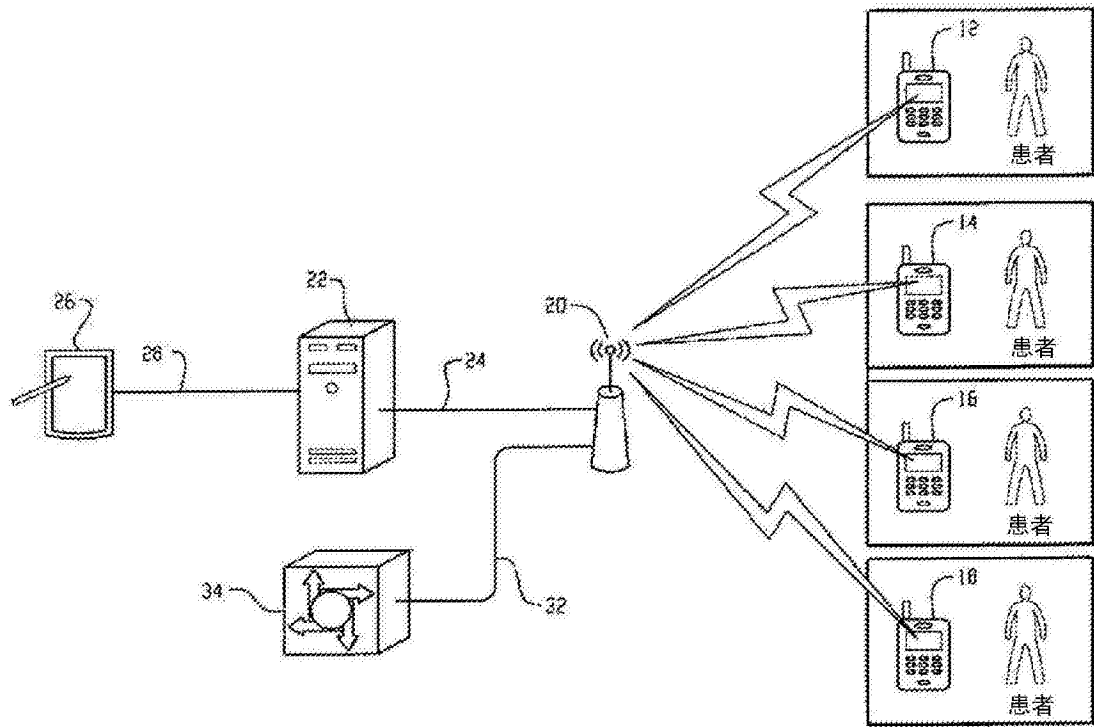


图1现有技术

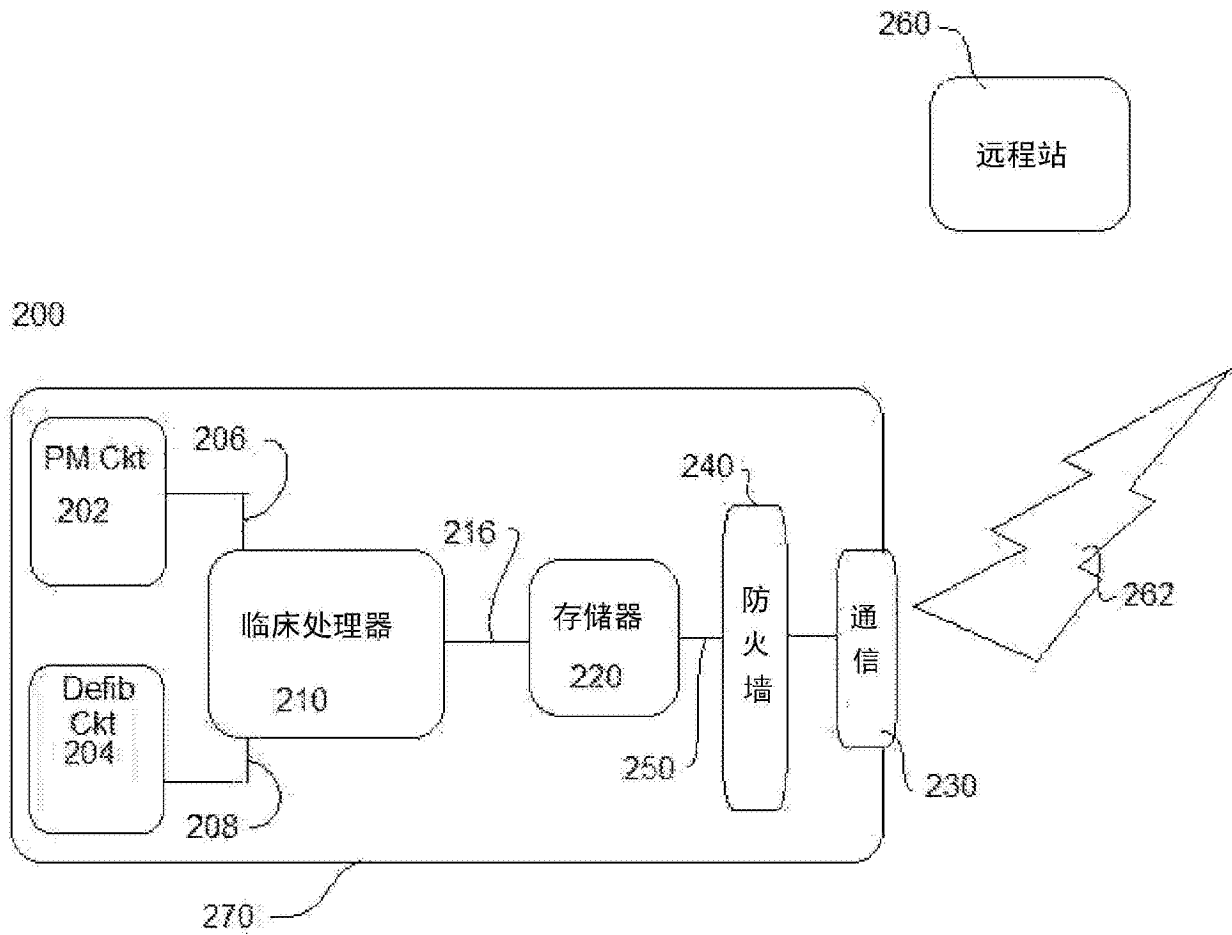


图2

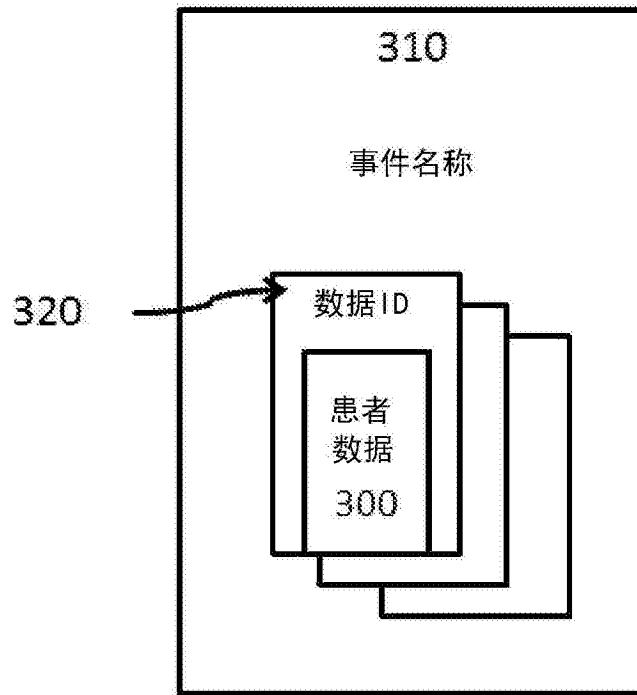


图3

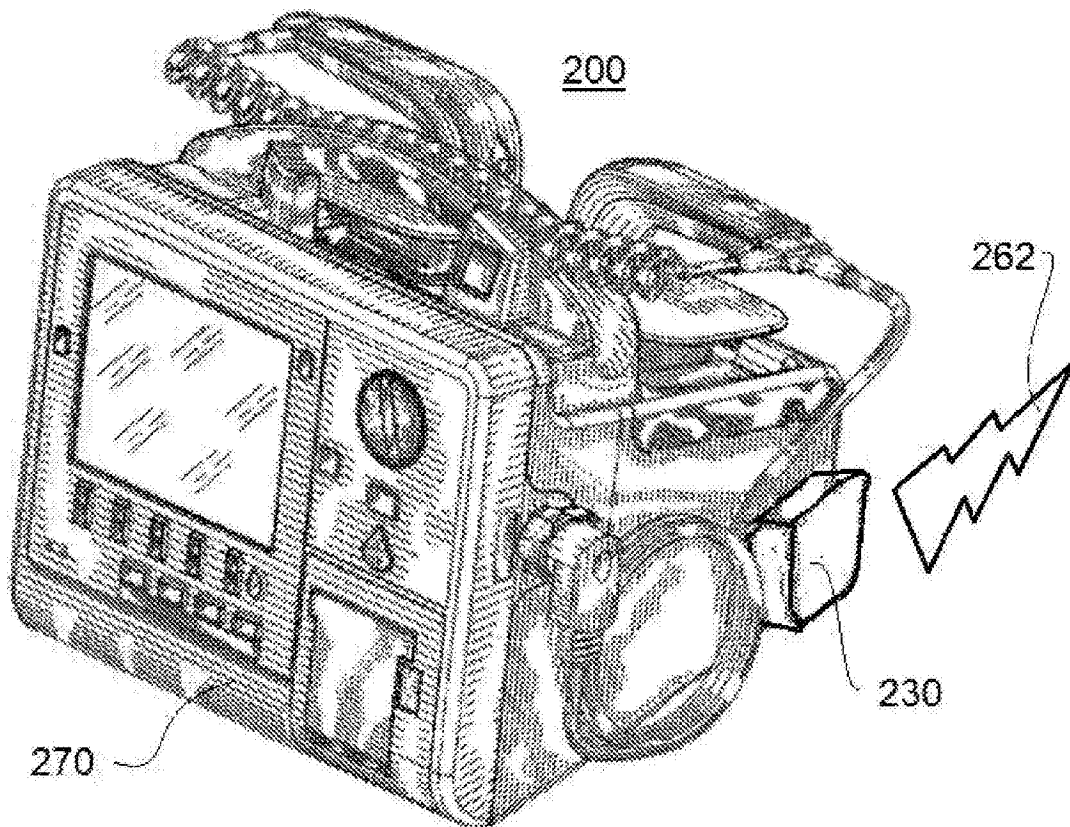


图4

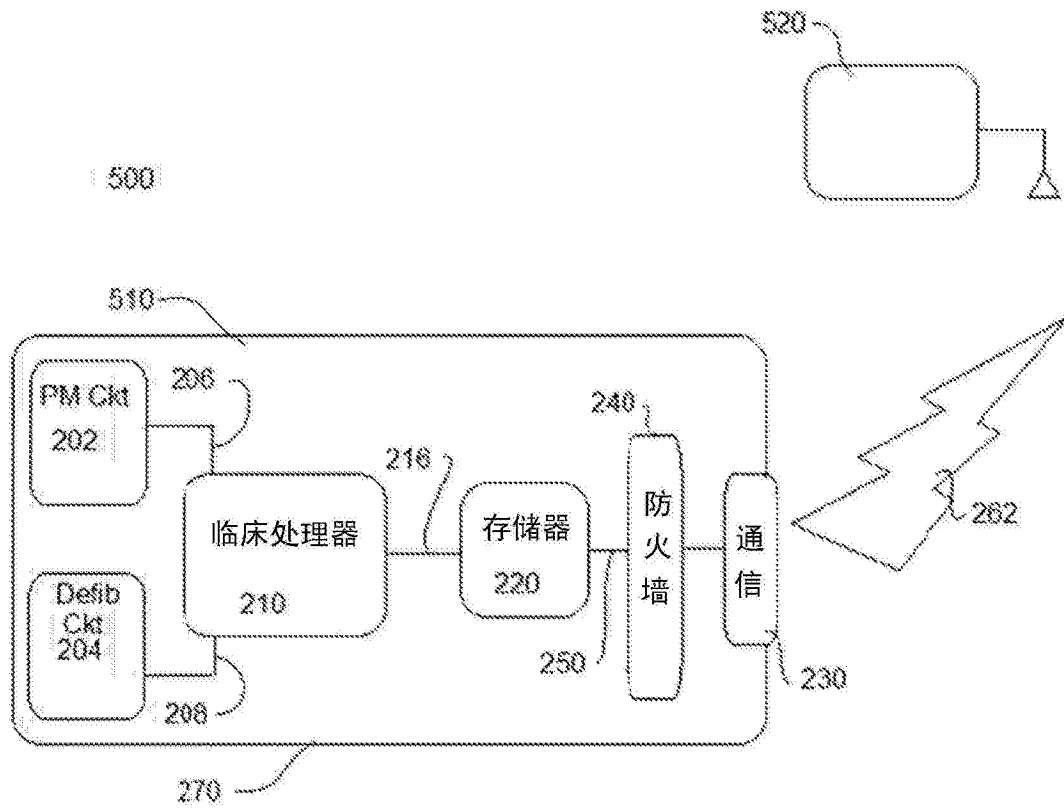


图5

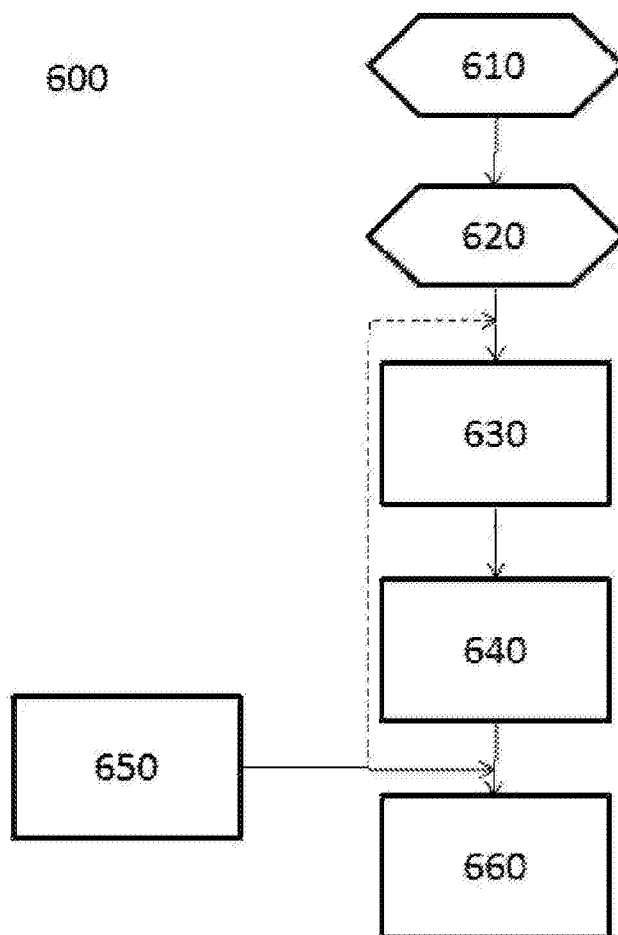


图6

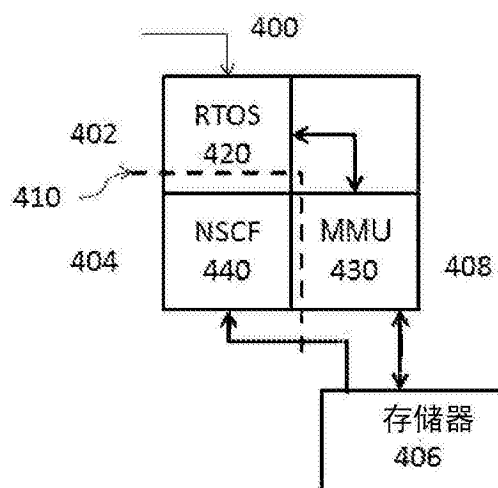


图7