(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 106455940 B
(45)授权公告日 2020.06.05

(21)申请号 201580018788.1

(22)申请日 2015.04.08

(65)同一申请的已公布的文献号
申请公布号 CN 106455940 A

(43)申请公布日 2017.02.22

(30)优先权数据
61/977,169 2014.04.09 US

(85)PCT国际申请进入国家阶段日
2016.10.09

(86)PCT国际申请的申请数据
PCT/US2015/024953 2015.04.08

(87)PCT国际申请的公布数据
WO2015/157436 EN 2015.10.15

(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 J·霍夫曼 J·斯潘塞

(74)专利代理机构 永新专利商标代理有限公司 72002
代理人 王英 刘炳胜

(51)Int.Cl.
A61B 1/012(2006.01)
A61B 1/00(2006.01)

(56)对比文件
WO 2005/091546 A3,2005.11.17,
US 7840268 B2,2010.11.23,
CN 101208037 A,2008.06.25,
CN 1883369 A,2006.12.27,
WO 2006/067377 A1,2006.06.29,
US 2007/0083111 A1,2007.04.12,
US 2006/0161054 A1,2006.07.20,

审查员 王歆媛

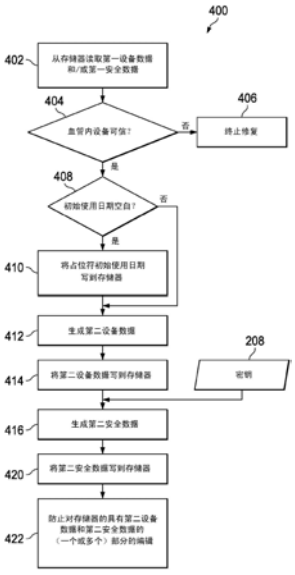
权利要求书2页 说明书12页 附图3页

(54)发明名称

用于认证的血管内设备使用和重新使用的设备、系统和方法

(57)摘要

提供了用于修复血管内设备以用于重新使用的设备、系统和方法。所述方法包括:从血管内设备的存储器读取第一安全数据;确定所述血管内设备是否是可信的;当所述血管内设备是可信的时,生成第二安全数据;并且将所述第二安全数据写到所述血管内设备的存储器。提供了用于对血管内设备进行验证以供使用的设备、系统和方法。所述方法包括:使血管内设备与计算设备通信,所述血管内设备包括存储器;确定第一安全数据是否是可信的;当所述第一安全数据是可信的时,确定所述血管内设备是否已经被修复;当所述血管内设备已经被修复时,确定所述第二安全数据是否是可信的;并且当所述第二安全数据是可信的时,允许在临床流程中使用所述血管内设备。



CN 106455940 B

1.一种针对血管内设备的授权的使用和/或重新使用的方法,包括:

从所述血管内设备的存储器读取第一安全数据;

基于所述第一安全数据来确定所述血管内设备是否是可信的;

通过当所述血管内设备是可信的时生成第二安全数据,并且将所述第二安全数据写到所述血管内设备的所述存储器来允许对所述血管内设备的修复以供在临床流程中重新使用,

其中,所述第一和第二安全数据包括消息认证码。

2.根据权利要求1所述的方法,还包括:

对所述血管内设备进行消毒。

3.根据权利要求1所述的方法,还包括:

评估所述血管内设备的性能特性;并且

基于所述性能特性来生成针对所述血管内设备的重新使用指令。

4.根据权利要求1所述的方法,还包括:

从所述血管内设备的所述存储器读取第一设备数据,所述第一设备数据包括以下中的至少一项:序列号、制造日期、配置信息、初始参数、性能参数、版本号以及过期日期,其中,所述配置信息包括系统配置设置。

5.根据权利要求4所述的方法,还包括:

生成第二设备数据,所述第二设备数据包括以下中的至少一项:序列号、额外的配置信息、与所述初始参数相对应的额外的参数、修复日期、重新使用指令、性能参数、版本号以及过期日期,其中,所述额外的配置信息包括系统配置设置;并且

将第二设备数据写到所述血管内设备的所述存储器。

6.根据权利要求1所述的方法,还包括:

使所述血管内设备与计算设备通信,所述存储器能由所述计算设备访问,所述存储器在其上存储有第一设备数据、第二设备数据、所述第一安全数据和第二安全数据;

基于所述第一设备数据来确定所述第一安全数据是否是可信的;

当所述第一安全数据是可信的时,基于所述第二设备数据来确定所述血管内设备是否已经被修复;

当所述血管内设备已经被修复时,基于所述第二设备数据来确定所述第二安全数据是否是可信的;并且

当所述第二安全数据是可信的时,允许在所述临床流程中使用所述血管内设备。

7.根据权利要求6所述的方法,还包括:

基于所述第一设备数据和所述第二设备数据中的至少一个来确定所述血管内设备是否在授权的使用时段之内;并且

当所述血管内设备在所述授权的使用时段之内时,允许在所述临床流程中使用所述血管内设备。

8.一种血管内系统,包括:

与血管内设备通信的计算设备,所述计算设备被配置为通过以下操作来修复所述血管内设备以供在临床流程中重新使用:

从所述血管内设备的存储器读取第一安全数据;

基于所述第一安全数据来确定所述血管内设备是否是可信的;并且

通过以下操作来对所述血管内设备进行修复以供在临床流程中重新使用:

当所述血管内设备是可信的时生成第二安全数据,并且将所述第二安全数据写到所述血管内设备的所述存储器,

其中,所述第一和第二安全数据包括消息认证码。

9.根据权利要求8所述的血管内系统,其中,所述计算设备还被配置为:

评估所述血管内设备的性能特性;并且

基于所述性能特性来生成针对所述血管内设备的重新使用指令。

10.根据权利要求8所述的血管内系统,其中,所述计算设备还被配置为:

从所述血管内设备的所述存储器读取第一设备数据,所述第一设备数据包括以下中的至少一项:序列号、制造日期、配置信息、初始参数、性能参数、版本号以及过期日期,其中,所述配置信息包括系统配置设置;

生成第二设备数据,所述第二设备数据包括以下中的至少一项:序列号、额外的配置信息、与所述初始参数相对应的额外的参数、修复日期、重新使用指令、性能参数、版本号以及过期日期,其中,所述额外的配置信息包括系统配置设置;并且

将第二设备数据写到所述血管内设备的所述存储器。

11.根据权利要求10所述的血管内系统,其中,所述计算设备还被配置为通过生成所述消息认证码来生成所述第二安全数据。

12.根据权利要求11所述的血管内系统,其中,所述计算设备还被配置为通过使用密钥、所述第二设备数据和所述序列号来生成所述第二安全数据。

13.根据权利要求8所述的血管内系统,其中,

所述计算设备还被配置为通过以下操作来对所述血管内设备进行认证以供在所述临床流程期间使用:

基于存储在所述存储器上的第一设备数据来确定存储在所述存储器上的所述第一安全数据是否是可信的;

当所述第一安全数据是可信的时,基于存储在所述存储器上的第二设备数据来确定所述血管内设备是否已经被修复;

当所述血管内设备已经被修复时,基于所述第二设备数据来确定存储在所述存储器上的第二安全数据是否是可信的;并且

当第二安全数据是可信的时,允许在所述临床流程中使用所述血管内设备。

14.根据权利要求13所述的血管内系统,其中,所述计算设备还被配置为:

基于所述第一设备数据和所述第二设备数据中的至少一个来确定所述血管内设备是否在授权的使用时段之内;并且

当所述血管内设备在所述授权的使用时段之内时,允许在所述临床流程中使用所述血管内设备。

15.根据权利要求13所述的血管内系统,其中,所述第一安全数据是使用密钥、第一设备数据和所述存储器的序列号来生成的,并且所述第二安全数据是使用密钥、第二设备数据和所述存储器的所述序列号来生成的。

用于认证的血管内设备使用和重新使用的设备、系统和方法

技术领域

[0001] 本公开总体涉及具有存储器的血管内设备，以实施加密算法而仅允许在临床流程中对所述血管内设备的授权的使用和/或重新使用。

背景技术

[0002] 血管内设备，诸如引导丝、导管、引导导管等，能够被配置用于成像、流量测量和/或压力测量以及其他功能。这样的血管内设备通常是一次性设备。此外，制造商通常针对单次使用来评价血管内设备。亦即，制造商针对单次使用确保血管内设备的安全性和/或血管内设备收集的数据的完整性。在临床流程中在患者的脉管系统内使用之后，所述血管内设备被舍弃。

[0003] 近来，未被制造商授权的第三方已经收集使用后的血管内设备。所述使用后的血管内设备之后被消毒、重新包装和销售以用于将来在临床流程中的使用。这给患者带来了显著的风险。这些血管内设备尚未被验证和确认，并且因此，不能够确保或者期望满足必要的安全性以及可信血管内设备的效力标准。当血管内设备被不适当地重新使用时，其能够将患者直接暴露于经由污染的危害。当一次性血管内设备被用于比其被设计进行安全操作更长的时间时，其也会将患者暴露于误诊的可能性。除了患者安全性问题，当消费者购买重新包装、使用后的血管内设备而非授权的血管内设备时，制造商还遭受财务损失。

[0004] 先前已经做出一些努力来确保仅授权的血管内设备被用在临床流程中。这些努力包括防止使用其板上数据未通过临床环境中的计算设备执行的某种核查的血管内设备。然而，第三方已经能够篡改板上数据，使得计算设备将所述血管内设备对待为可信的。

[0005] 此外，尽管第三方在没有对血管内设备的详细了解的情况下不适合重新加工或者修复使用后的血管内设备，但制造商或授权方却是适于这样做的。

[0006] 因此，仍然存在对全面地防止未授权的、欺骗性的和/或以其他方式篡改的血管内设备的使用的认证系统的需求。当制造商或授权方修复使用后的血管内设备时，认证系统也需要允许该设备在临床流程中使用。

发明内容

[0007] 本公开的实施例提供了一种针对血管内设备通过仅允许在临床流程期间授权的使用和/或重新使用的经改进的安全系统。所述血管内设备包括存储器。使用所述存储器实施加密。经改进的安全性也允许经恰当地修复的使用后的血管内设备以在临床流程中重新使用。

[0008] 在示范性的方面中，本公开涉及一种修复血管内设备以用于在临床流程期间重新使用的方法。所述方法包括从血管内设备的存储器读取第一安全数据；基于所述第一安全数据来确定所述血管内设备是否是可信的；当所述血管内设备是可信的时，生成第二安全数据；并且将所述第二安全数据写到所述血管内设备的存储器。

[0009] 在一方面中，所述方法还包括当所述血管内设备被确定为不是可信的时终止所述

修复。在一方面中，所述方法还包括对所述血管内设备进行消毒。在一方面中，所述方法还包括评估所述血管内设备的性能特性；并且基于所述性能特性来生成针对所述血管内设备的重新使用指令。在一方面中，所述方法还包括从所述血管内设备的存储器读取第一设备数据，所述第一设备数据包括以下中的至少一项：序列号、制造日期、配置信息、初始参数、生产日期、性能参数、版本号、过期日期以及系统配置设置。在一方面中，所述方法还包括生成第二设备数据，所述第二设备数据包括以下中的至少一项：序列号、额外的配置信息、额外的参数、修复日期、重新使用指令、性能参数、版本号、过期日期以及系统配置设置；并且将所述第二设备数据写到所述血管内设备的存储器。在一方面中，所述第一安全数据和所述第二安全数据包括消息认证码。在一方面中，所述第一安全数据是使用密钥、所述第一设备数据和所述序列号来生成的。在一方面中，所述第二安全数据是使用密钥、所述第二设备数据和所述序列号来生成的。

[0010] 在另一示范性方面中，本公开涉及一种血管内系统。所述系统包括与血管内设备通信的计算设备，所述计算设备被配置为通过以下方式来修复所述血管内设备以用于在临床流程期间的重新使用：从血管内设备的存储器读取第一安全数据；基于所述第一安全数据来确定所述血管内设备是否是可信的；当所述血管内设备是可信的时，生成第二安全数据；并且将所述第二安全数据写到所述血管内设备的存储器。

[0011] 在一方面中，所述计算设备还被配置为：评估所述血管内设备的性能特性；并且基于所述性能特性来生成针对所述血管内设备的重新使用指令。在一方面中，所述计算设备还被配置为：从所述血管内设备的存储器读取第一设备数据，所述第一设备数据包括以下中的至少一项：序列号、制造日期、配置信息、初始参数、生产日期、性能参数、版本号、过期日期以及系统配置设置；生成第二设备数据，所述第二设备数据包括以下中的至少一项：序列号、额外的配置信息、额外的参数、修复日期、重新使用指令、性能参数、版本号、过期日期以及系统配置设置；并且将第二设备数据写到所述血管内设备的存储器。在一方面中，所述计算设备还被配置为通过生成消息认证码来生成所述第二安全数据。在一方面中，所述计算设备还被配置为通过使用密钥、所述第二设备数据和所述序列号来生成第二安全数据。

[0012] 在另一示范性方面中，本公开涉及一种对血管内设备进行认证以用于在临床流程期间重新使用的方法。所述方法包括使血管内设备与计算设备通信，所述血管内设备包括能由所述计算设备访问的存储器，所述存储器在其上存储有第一设备数据、第二设备数据、第一安全数据和第二安全数据；基于所述第一设备数据来确定第一安全数据是否是可信的；当所述第一安全数据是可信的时，基于所述第二设备数据来确定所述血管内设备是否已经被修复；当所述血管内设备已经被修复时，基于所述第二设备数据来确定所述第二安全数据是否是可信的；并且当所述第二安全数据是可信的时，允许在临床流程中使用所述血管内设备。

[0013] 在一方面中，所述方法还包括基于所述第一设备数据和所述第二设备数据中的至少一个来确定所述血管内设备是否在授权的使用时段之内；并且当所述血管内设备处在授权的使用时段之内时，允许在临床流程中对所述血管内设备的使用。在一方面中，所述第一安全数据和所述第二安全数据包括消息认证码，其中，所述第一安全数据是使用密钥、第一设备数据和存储器的序列号来生成的，而所述第二安全数据是使用密钥、第二设备数据和存储器的序列号来生成的。

[0014] 在另一示范性方面中，本公开涉及一种血管内系统。所述系统包括与具有存储器的血管内设备通信的计算设备，所述计算设备被配置为通过以下操作来对所述血管内设备进行认证以用于在临床流程期间使用：基于存储在所述存储器上的第一设备数据来确定存储在所述存储器上的第一安全数据是否是可信的；当所述第一安全数据是可信的时，基于存储在所述存储器上的第二设备数据来确定所述血管内设备是否已经被修复；当所述血管内设备已经被修复时，基于所述第二设备数据来确定存储在所述存储器上的第二安全数据是否是可信的；并且当第二安全数据是可信的时，允许在临床流程中对所述血管内设备的使用。

[0015] 在一方面中，所述计算设备还被配置为：基于所述第一设备数据和所述第二设备数据中的至少一个来确定所述血管内设备是否在授权的使用时段之内；并且当所述血管内设备处在授权的使用时段之内时，允许在临床流程中对所述血管内设备的使用。在一方面中，所述第一安全数据和所述第二安全数据包括消息认证码，其中，所述第一安全数据是使用密钥、第一设备数据和存储器的序列号来生成的，而所述第二安全数据是使用密钥、第二设备数据和存储器的序列号来生成的。

[0016] 根据下文的详细描述，本公开的另外的方面、特征和优点将变得显而易见。

附图说明

[0017] 将参考附图来描述本公开的例示性实施例，在附图中：

[0018] 图1是根据本公开的各方面的在制造环境中的血管内系统的图解示意图；

[0019] 图2是根据本公开的各方面的对血管内设备进行初始调节以用于在临床流程期间使用的方法的流程图；

[0020] 图3是根据本公开的各方面的在修复环境中的血管内系统的图解示意图；

[0021] 图4是根据本公开的各方面的修复血管内设备以用于在临床流程期间重新使用的方法的流程图；

[0022] 图5是根据本公开的各方面的在临床环境中的血管内系统的图解示意图；

[0023] 图6是根据本公开的各方面的对血管内设备进行认证以用于在临床流程期间使用和/或重新使用的方法的流程图。

具体实施方式

[0024] 出于促进对本公开的原理的理解的目的，现在将参考在附图中图示的实施例，并且特定的语言将被用于描述相同的内容。然而，应当理解，并不旨在限制本公开的范围。对所描述的设备、系统和方法的任何更改和进一步修改以及本公开的原理的任何其他应用被完全预期并且包括在本公开之内，如对于本公开相关的本领域技术人员通常将进行的。具体而言，完全预期，关于一个实施例描述的特征、部件和/或步骤可以与关于本公开的其他实施例描述的特征、部件和/或步骤进行组合。然而，出于简洁的目的，将不单独描述这些组合的众多的迭代。

[0025] 本文中所描述的设备、系统和方法涉及对血管内设备的授权的使用和/或重新使用。所述血管内设备包括存储器。本文中所描述的认证方案使用存储器实施加密。认证能够使用被写到血管内设备的存储器的一个或多个加密代码来实现。本文中所描述的认证方案

使用关于存储在存储器上的血管内设备的数据以及加密代码来综合地防止未授权的设备使用和/或重新使用。新数据(例如,关于血管内设备和/或加密代码)能够被写到存储器以进一步保护血管内设备。例如,新数据能够在对所述血管内设备的使用、重新使用、消毒和/或修复之前、期间和/或之后被写到所述存储器。在临床环境中的计算设备和/或远程设备能够使用关于血管内设备的数据和/或加密代码来验证所述血管内设备是可信的并且被授权在临床流程期间使用。

[0026] 本文中所描述的认证算法通过在使用之前验证血管内设备的完整性和状态来防止过期的和/或未授权的血管内设备的使用。当血管内设备正在被不恰当地重新使用时,或者因为所述血管内设备是制造商的设备的未授权的克隆,则所述设备会是未授权的。作为所述血管内设备的存储器的部分实施的加密方案使得伪造有效的血管内设备以使得其将被不正确地处置为可信的在计算上是不可行的。

[0027] 本文所描述的设备、系统和方法能够应用于任何一次性或有限使用的血管内设备,包括被配置用于血管内超声(IVUS)、光学相干断层摄影(OCT)、前向查看IVUS(FLIVUS)、前向查看心脏内回声(FLICE)、流量测量、压力测量和/或其组合。

[0028] 图1是根据本公开的各方面在制造环境中的血管内系统100的图解示意图。血管内系统100包括血管内设备102,诸如导管、引导丝或引导导管。在一些实施例中,血管内设备102被配置为使用一种或多种成像模态(例如,IVUS、OCT等)来对血管的腔进行成像。在一些实施例中,血管内设备102被配置为测量通过血管的血液的压力和/或流量。用于成像、压力测量和/或流量测量的一个或多个部件能够被定位在血管内设备102的远端部分处。

[0029] 血管内设备102包括存储器104。存储器104能够是一次写入存储器或者可再写/可再编程存储器。例如,利用可重写/可编程存储器,存储器104的部分在被初始编程之后能够被重写或再编程,而不使存储器和/或血管内设备102退化。在各种实施例中,存储器104能够是电可擦除可编程只读存储器(EEPROM)、闪速存储器、硬盘和/或其他合适的存储设备。存储器104具有足够的容量以存储关于血管内设备102的数据(例如,存储器的唯一的序列号、配置信息、初始参数、重新使用指令、制造数据、重新加工数据、临床使用数据等)以及安全或加密数据(例如,一个或多个消息认证码)。

[0030] 血管内设备102是一次性或有限使用的设备。例如,制造商能够针对一次、两次、三次、四次或更多次有限次数的使用确保血管内设备102的安全性和/或使用血管内设备102收集的数据的完整性。血管内设备102也能够是重复使用的设备,其在使用之间是可消毒的(例如,使用高压灭菌流程)。由此,血管内设备102能够在多个流程中使用。在一些实施例中,血管内设备102仅在被消毒后重复使用。在一些实施例中,血管内设备102在被修复之后(例如,在被消毒和经受进一步的处理两者以准备血管内设备102进行重新使用之后)重复使用。关于图3和图4论述了修复流程的示范性实施例。血管内设备102能够被配置用于在制造和/或修复之后的特定时间段之内使用和/或重新使用。

[0031] 图1图示了制造环境,在所述制造环境中,血管内设备102被初始地组装、调节和/或编程。关于血管内设备的数据能够通过制造系统110写到存储器104。制造系统110包括计算设备,所述计算设备被配置为与血管内设备102通信并且利用初始参数、安全数据和其他合适的数据对血管内设备102进行编程,以允许血管内设备102在临床环境中被使用。关于图2论述初始调节流程的示范性实施例。

[0032] 制造系统110能够被配置为直接访问、读取和/或写存储器104。在制造环境中，在制造系统110与血管内设备102之间的信号的通信能够包括将来自制造系统110的初始参数、安全数据和其他合适的数据传送到血管内设备102。在一些实施例中，制造系统110不直接访问存储器104，而是额外的部件(例如，类似于图5的患者接口模块(PIM))便于在制造系统110与血管内设备102之间的通信。在一些实施例中，额外的部件的功能是通过制造系统110和/或血管内设备102执行的，使得不利用额外的部件。

[0033] 图2是根据本公开的各方面初始地调节血管内设备以用于在临床流程期间使用的方法200的流程图。方法200的一个或多个步骤能够通过制造系统110执行，从而准备血管内设备102以供在患者的脉管中使用。作为方法200的结果，血管内设备102能够连同认证算法一起实施，从而仅允许对血管内设备102的授权的使用和/或重新使用。

[0034] 在步骤202，方法200包括生成第一设备数据。第一设备数据能够包括例如存储器104的唯一序列号、配置信息、初始参数、制造日期、性能参数、版本号、过期日期、系统配置设置以及关于血管内设备102的其他数据。所述第一设备数据能够基于血管内设备102的特定部件(包括存储器104和用于成像、压力测量和/或流量测量的(一个或多个)部件)来生成。在一些实施例中，工厂/制造提供的唯一序列号能够被写在存储器104的只读存储器(ROM)部分。

[0035] 在步骤204，方法200包括将所述第一设备数据写到存储器104。例如，能够使血管内设备102与制造系统110进行通信，使得制造系统110能够对存储器104进行访问和编程。所述第一设备数据能够被写到存储器的具体部分(例如，页0和1)。

[0036] 在步骤206，方法200包括生成第一安全数据。在一些实施例中，所述第一安全数据(以及第二、第三、第四和其他安全数据)能够包括消息认证码(MAC)或其他合适的加密工具，诸如哈希函数、分组密码等。在一些实施例中，所述第一安全数据是使用第一设备数据、存储器104的唯一的序列号以及密钥208作为输入来生成的。密钥208能够是在认证算法中使用的参数，其仅对血管内设备102的制造商或授权方可知。

[0037] 在示范性实施例中，认证算法利用消息认证码(CMAC)或者具有128位先进加密标准(AES)的基于密码的一键CBC MAC1(OMAC1)。在http://tools.ietf.org/html/rfc4493上可获得的The Internet Society,The AES-CMAC Algorithm(2006)中描述了示范性认证算法，在此通过引用将其全文并入。在不同实施例中，可以利用其他合适的认证方案，诸如数据认证算法(DAC)、密码分组链消息认证码(CBC-MAC)、有密钥的哈希消息认证码(HMAC)、可并行的MAC(PMAC)、VMC、基于通用哈希的消息认证码(UMAC)、Poly1305-AES等。

[0038] 能够如下生成针对本文所描述的设备、系统和方法的一个或多个MAC以用于基于CMAC的认证算法。以k表示由制造商随机、一致地选取的128位密钥作为密钥，并且以k_1、k_2作为从k导出的128位子密钥作为下文的GenerateSubKey算法的输出。以$E_k(x)$和$E_k^{-1}(x)$作为使用键k分别在128位字符串x上的128位AES加密和解密函数。以$msb_l(x)$表示x的最为重要(或者最左侧)的位或者在l被省略时的最为重要的位。左位移由<<表示，并且异或由⊕表示。

[0039] GenerateSubKey算法能够如下所述地定义。GenerateSubKey算法能够采取128位(16字节)字符串并且返回两个128位字符串以被用作GenerateSubKey算法中的子密钥。

GenerateSubKey (k:uint128):(uint128, uint128)

$C \leftarrow$ (uint128)0x87

$k_0 \leftarrow E_k$((unit128)0)

[0040]

if $msb(k_0) = 0$

$k_1 \leftarrow k_0 \ll 1$

else

$k_1 \leftarrow (k_0 \ll 1) \oplus C$

if $msb(k_1) = 0$

$k_2 \leftarrow k_1 \ll 1$

[0041]

else

$k_2 \leftarrow (k_1 \ll 1) \oplus C$

return(k_1, k_2)

[0042] GenerateMac算法能够如下所述地定义。GenerateMac算法利用128位密钥k、包含消息的字节阵列D以生成CMAC以及D中的字节的长度n。返回值是128位CMAC。

GenerateMac (k:uint128, D:byte[n], n:int):uint128

$(k_1, k_2) \leftarrow$ GenerateSubKey(k)

if $n = 0$

return *ERROR*

$m \leftarrow [n/16]$ *{m 是要处理的分组的数量}*

B:unit128[m] *{B 作为 16 字节分组的消息}*

for i in [0, $m - 1$]

$B[i] \leftarrow D[i * 16]$

if $n \equiv 0$ (mod 16)

[0043] $B[m-1] \leftarrow B[m-1] \oplus k_1$

else *{利用位 100...00 填充上一分组}*

lastBlock:uint128

$\text{lastBlock} \leftarrow D[((m-1) * 16) \ldots n] \| 0x80 \| 0^{16-(n-16(m-1))-1}$

$B[m-1] \leftarrow \text{lastBlock} \oplus k_2$

$x \leftarrow$ (unit128)0

for i in [0, $m - 1$]

$y \leftarrow x \oplus B[i]$

$x \leftarrow E_k(y)$

return x

[0044] 在步骤210，方法200包括将第一安全数据写到存储器104。所述第一安全数据能够被写到存储器104的具体部分(例如，页1)。

[0045] 在步骤212，方法200包括防止利用第一设备数据和第一安全数据对存储器104的(一个或多个)部分进行编辑。例如，存储器104能够包括锁页功能，其锁定存储器104的指定的部分并且防止那些部分被编辑。

[0046] 在基于方法200被初始地调节(condition)之后，血管内设备和认证算法能够如关于图5和图6描述的在临床环境中实施。在一次或多次使用之后，血管内设备能够通过由制造商或授权方修复以供随后的使用。这是参考图3和图4描述的。

[0047] 图3是根据本公开的各方面在修复环境中的血管内系统300的图解示意图。图3图示了修复环境，在修复环境中，在血管内设备102已经被用在一个或多个临床流程中使用之后，血管内设备102被准备用于重新使用。计算设备(例如，修复系统310)能够评估血管内设备102的性能特性，以识别源自较早的使用的任何改变，并且生成重新使用指令，其补偿所识别的改变。修复系统310也能够将第二安全数据、修复日期等写到存储器104，使得临床系统将认识到血管内设备102已经被恰当的修复并允许重新使用。在一些实施例中，修复系统310能够被配置为直接访问、读取和/或写存储器104。在一些实施例中，制造系统110不直接

访问存储器104，而是额外的部件便于在制造系统110与血管内设备102之间的通信。在一些实施例中，修复系统310能够是制造系统110(图1)。例如，制造系统110能够被配置为执行关于图2描述的初始调节流程以及关于图4描述的修复流程。

[0048] 图4是根据本公开的各方面修复血管内设备以用于在临床流程期间重新使用的方法400的流程图。方法400的一个或多个步骤能够由制造商或授权方使用修复系统310执行。作为方法400的结果，血管内设备102能够连同认证算法一起实施，从而仅允许在临床环境中对修复的血管内设备102的授权的重新使用。

[0049] 在步骤402，方法400包括从存储器104读取第一设备数据和/或第一安全数据。在步骤404，方法400包括确定血管内设备102是否是可信的。例如，修复系统310能够使用本文所描述的认证算法来确定血管内设备102是可信的。使用从存储器104读取的第一设备数据(步骤402)，修复系统310能够确定从存储器104读取的第一安全数据(步骤402)是可信的。如果血管内设备102不是可信的，在步骤406，方法400能够包括终止所述修复流程。这样的情况会在制造商未初始地修复血管内设备102时，存储器104被篡改等时出现。在这样的情况中，血管内设备102的使用可以防止对患者的健康风险，并且血管内设备102能够被舍弃。在一些实施例中，如果所述血管内设备不是可信的情况下，能够执行额外的处理以消除对患者的健康风险、对血管内设备进行重新认证等。在这样的实施例中，被确定为不可信的血管内设备不被舍弃并且经受修复流程。

[0050] 当血管内设备102是可信的时，在步骤408，方法400包括确定存储器104的初始使用日期字段是否是空白的。例如当先前未使用的血管内设备102被引入到修复环境时会出现这样的情况。当血管内设备102是先前使用的时，存储器104的初始使用字段也能够是空白的，但是通过某种错误初始使用字段未被由临床环境中的计算设备填充。尽管非标准事件能够使初始使用日期字段为空白的，但是那些事件不像是需要终止修复流程，因为血管内设备的可信性(步骤404)已经被验证。当所述初始使用日期字段是空白的时，在步骤410，占位符初始使用日期能够被写到存储器104的具体部分(例如，页3)。

[0051] 当初始使用日期字段已经利用占位符填充时或者当初始使用日期字段不是空白的时，在步骤412，方法400能够包括生成第二设备数据。在一些实施例中，所述第二设备数据能够包括第一设备数据的所有或一些部分。所述第二设备数据能够包括：序列号、额外的配置信息、额外的参数、修复日期、重新使用指令、性能参数、版本号、过期日期、系统配置设置以及关于血管内设备102的其他数据。

[0052] 在一些实施例中，方法400能够包括评估血管内设备(例如，血管内设备102的用于成像、压力测量和/或流量测量的一个或其他部件)的性能特性。血管内设备102的性能能够如使用的自然结果而劣化。方法400因此能够包括基于所述性能特性而生成重新使用指令。所述重新使用指令例如能够指定由血管内设备102收集的数据应当如何在临床环境中处理。重新使用指令能够是在初始使用期间数据如何被处理的修改，并且能够补偿血管内设备102的任何劣化。在步骤414，方法400包括将第二设备数据写到存储器104。所述第二设备数据能够被写到存储器的(一个或多个)指定部分(例如，页2)。

[0053] 在步骤416，方法400包括生成第二安全数据。在一些实施例中，所述第二安全数据能够第二MAC。能够以与上文描述的第一MAC相似的方式生成第二MAC。例如，能够使用第二设备数据、第一设备数据的所有或某部分、存储器104的唯一序列号以及密钥208作为输入

来生成第二MAC。在步骤420，方法400包括将第二安全数据写到存储器104。所述第二安全数据能够被写到存储器的指定部分(例如，页2)。在一些实施例中，所述第二安全数据替换所述第一安全数据。例如，存储器104的包括第一MAC的指定部分被写入以包括第二MAC。在一些实施例中，存储器104包括第一安全数据和第二安全数据两者。在步骤422，方法400包括使用存储器104的锁页功能来防止利用第二设备数据和第二安全数据对存储器104的(一个或多个)部分进行编辑。

[0054] 在基于方法400被修复之后，血管内设备和认证算法能够如参考附图5和图6在临床环境中实施。

[0055] 图5是根据本公开的各方面在临床环境中的血管内系统500的图解示意图。图5图示了临床环境，在所述临床环境中，在临床流程期间使用和/或重新使用血管内设备102。例如，血管内设备102能够与临床系统510一起使用以进行血管内成像、压力测量和/或流量测量。临床系统510能够包括与血管内设备102通信的计算设备并且被配置为确定血管内设备102是否被授权用于使用和/或重新使用。

[0056] 临床系统510和血管内设备102在一些实施例中能够与患者接口模块(PIM)520进行通信。PIM 520方便临床系统510与血管内设备102之间的信号的通信。在一些实施例中，PIM 520供应高压和低压DC功率以支持血管内设备102的操作，包括用于成像、压力测量和/或流量测量的(一个或多个)部件。在一些实施例中，PIM 520被配置为基于例如来自临床系统510的指令来访问、读取和/或写存储器104。在其他实施例中，临床系统510能够被配置为在无PIM 520的情况下直接访问、读取和/或写存储器104。

[0057] 图6是根据本公开的各方面对血管内设备进行认证以用于在临床流程期间使用和/或重新使用的方法600的流程图。方法600的一个或多个步骤能够通过使用临床系统510来执行。方法600能够允许用于血管内设备102的授权的初始使用、血管内设备102的授权的重新使用、修复的血管内设备102的授权的初始使用和/或修复的血管内设备102的授权的重新使用。

[0058] 在步骤602，方法600包括使血管内设备102与PIM 520和/或临床系统510通信。例如，导管能够被物理地插入到PIM 520中。在其他实施例中，血管内设备102与PIM 520和临床系统510无线地通信。

[0059] 在步骤604，方法600包括确定第一安全数据是否是可信的。例如，临床系统510能够使用第一设备数据来确定第一MAC是否是可信的。如果所述第一安全数据不是可信的，则血管内设备102被确定为未被授权使用。当例如存储器104的数据是伪造的和/或以其他方式被篡改时，所述第一安全数据可以是不可信的。当所述第一安全数据不是可信的，在步骤606，方法600包括向用户提供血管内设备102未被授权用于临床使用的指示。临床系统510也能够将诊断代码写到存储器104，指示血管内设备102是不可信的，因为安全数据不是可信的。例如，临床系统510将修改存储器104的第一未使用的使用日期字段、将临床系统510的序列号写到存储器、和/或将诊断代码写到存储器104。未授权的血管内设备102的未来尝试的重新使用能够在临床系统读取诊断代码时被防止。在步骤608，方法600包括拒绝对血管内设备102的使用。

[0060] 当第一安全数据是可信的时，在步骤610，方法600包括确定存储器104的初始使用日期字段是否已经被修改。当初始使用日期字段尚未被修改时，临床系统510确定血管内设

备102是新的、未使用的设备。为了确定血管内设备102是否被授权初始使用，在步骤612，方法600包括确定血管内设备102是否已经过期。步骤612能够包括从存储器104读取制造日期字段和/或授权的使用时段字段。临床系统510能够确定当前日期与制造日期相比是否在授权的使用时段之内。如果血管内设备102被确定为过期，那么血管内设备102是未授权的。在步骤614，方法600包括向用户提供血管内设备102未被授权用于临床使用的指示。临床系统510也能够将诊断代码写到存储器104，指示血管内设备102是未授权的，因为血管内设备102已经过期。例如，临床系统510将修改存储器104的第一未使用的使用日期字段、将临床系统510的序列号写到存储器、和/或写入诊断代码。未授权的血管内设备102的未来尝试的重新使用能够在临床系统读取所述诊断代码时被防止。在步骤608，方法600包括拒绝对血管内设备102的使用。

[0061] 当血管内设备102尚未过期时，临床系统510确定血管内设备102未被授权初始使用。在步骤616，方法600包括将当前日期写到存储器104的初始使用日期字段。步骤616也能够包括将临床系统510的序列号写到存储器104，作为关于血管内设备102的使用的另外的信息。在步骤618，方法600包括允许对血管内设备102的使用。

[0062] 如果临床系统510在步骤610确定存储器104的初始使用字段已经被修改，那么在步骤620，方法600包括确定血管内设备102是否已经被修复或重新加工。例如，临床系统510能够确定第二设备数据是否已经被写到存储器、存储器104的重新加工日期字段是否已经被填充等。当血管内设备102尚未被修复时，临床系统510确定血管内设备102正在被重新使用。在步骤622，方法600包括确定血管内申请102是否处在授权进行重新使用的时间段(例如，重新使用窗口)之内。步骤622能够包括从存储器104读取制造日期字段、初始使用日期字段和/或授权重新使用时段字段。临床系统510能够确定当前日期与制造日期和/或初始使用日期相比是否在授权重新使用时段之内。如果试图在授权重新使用的时段之外重新使用，那么血管内设备102是未授权的。在步骤624，方法600包括向用户提供血管内设备102未被授权用于临床使用的指示。临床系统510也能够将诊断代码写到存储器104，指示血管内设备102是未授权的，因为针对血管内设备102的重新使用的窗口已经过期。例如，临床系统510将修改存储器104的第一未使用的使用日期字段、将临床系统510的序列号写到存储器104、和/或写入诊断代码。未授权的血管内设备102的未来尝试的重新使用能够在临床系统读取所述诊断代码时被防止。在步骤608，方法600包括拒绝对血管内设备102的使用。

[0063] 当血管内设备102在重新使用窗口之内时，临床系统510确定血管内设备102被授权重新使用。方法600能够包括将当前日期写到存储器104的重新使用日期字段。方法600也能够包括将临床系统510的序列号写到存储器104，作为关于血管内设备102的重新使用的另外的信息。在步骤618，方法600包括允许对血管内设备102的使用。

[0064] 如果临床系510在步骤620确定血管内设备102已经被修复或重新加工，那么在步骤626，方法600包括确定第二安全数据是否是可信的。例如，临床系统510能够使用第二设备数据来确定第二MAC是否是可信的。在一些实施例中，使用第一设备数据和/或第二设备数据的所有或某部分确定第二MAC是可信的。如果第二安全数据不是可信的，则血管内设备102被确定为未被授权使用。类似于第一安全数据，当例如存储器104的数据是伪造的和/或以其他方式被篡改时，所述第二安全数据能被确定为不是可信的。当所述第二安全数据不是可信的，在步骤606，方法600包括向用户提供血管内设备102为被授权用于临床使用的指

示，如上文所描述的。在步骤608，方法600包括拒绝对血管内设备102的使用。

[0065] 当第二安全数据是可信的，在步骤628，方法600包括确定存储器104的修复或重新加工使用日期字段是否已经被修改。当修复使用日期字段尚未被修改时，临床系统510确定血管内设备102自被修复起尚未使用的设备。为了在被修复之后确定血管内设备102是否被授权初始使用，在步骤630，方法600包括确定血管内设备102是否已经过期。步骤630能够包括从存储器104读取制造日期字段、修复日期字段和/或授权的使用时段字段。临床系统510能够确定当前日期与制造日期和/或修复日期相比是否在授权的使用时段之内。如果血管内设备102被确定为过期，则血管内设备102是未授权的。在步骤614，方法600包括向用户提供血管内设备102未被授权用于临床使用的指示，如上文所描述的。在步骤608，方法600包括拒绝对血管内设备102的使用。

[0066] 当在步骤630处确定血管内设备102尚未过期时，临床系统510确定血管内设备102未被授权在修复之后的初始使用。在步骤632，方法600包括将修复的使用日期写到存储器104。步骤632也能够包括将临床系统510的序列号写到存储器104，作为关于血管内设备102的使用的进一步的信息。在步骤618，方法600包括允许对血管内设备102的使用。

[0067] 在步骤628，如果存储器104的修复的使用日期字段已经被修改，那么临床系统510确定修复的血管内设备102正在被重新使用。在步骤622，方法600包括确定血管内设备102是否在授权用于重新使用的时间段之内。步骤622能够包括从存储器104读取制造日期字段、初始使用日期时段、修复使用日期字段和/或授权重新使用时段字段。临床系统510能够确定当前日期与制造日期、初始使用日期和/或修复使用日期相比是否在授权重新使用时段之内。如果试图在授权重新使用的时段之外重新使用，那么血管内设备102是未授权的。在步骤624，方法600包括向用户提供血管内设备102未被授权用于临床使用的指示，如上文所描述的。在步骤608，方法600包括拒绝对血管内设备102的使用。

[0068] 在步骤622，当血管内设备102在重新使用窗口之内时，临床系统510确定修复的血管内设备102被授权重新使用。方法600能够包括将重新使用日期写到存储器104。方法600也能够包括将临床系统510的序列号写到存储器104，作为关于修复的血管内设备102的重新使用的另外的信息。在步骤618，方法600包括允许对血管内设备102的使用。

[0069] 尽管方法600描述了重新使用的一个实例和修复的一个实例，但是应当理解，血管内设备102能够被重新使用和/或修复一次、两次、三次、四次或更多次。这样，第三、第四和其他设备数据和/或安全数据能够被写到存储器104。血管内设备102能够被授权以与相对于方法600描述的相似的方式使用。

[0070] 本文所描述的设备、系统和方法使用MAC来防止伪造并检测存储在存储器104上的数据中的误差。为了确定血管内设备102是否是可信的，临床系统105考虑存储器104的内容，作为从制造商发送到临床系统510的加密的消息。认证算法允许血管内设备102和/或计算设备(例如制造系统110、修复系统310和/或临床系统)免受一个或多个伪造。例如，所述认证算法能够防止回放攻击，在回放攻击中，相同的消息被发送两次并且两次都被接受为可信的。这能够例如在来自修复的设备的MAC/存储器内容被拷贝到尚未被修复的设备的情况下发生。如上文所描述的，存储器104能够根据制造包括具有唯一序列号的ROM。通过包括唯一序列号作为输入之一以生成MAC，MAC被关联到特定的存储器104，其仅以微不足道的冲突的机会写入。

[0071] 认证算法能够防止更改，其中，消息中的一些被修改并且被接受为可信的。当存储器104在制造期间或者在修复期间被写入时，部分被锁定以防止任何其他改变。另外，如果值以某种方式被改变，则攻击者将在没有密钥208的情况下降不能够生成新的有效的MAC。为了防止更改，MAC能够被配置为使得在输入数据中的单个位的改变引起MAC大致一半的位以计算上不可行的方式改变(例如，如针对加密基元所提供的，诸如分组密码和哈希函数)。

[0072] 所述认证算法能够防止无消息攻击，在无消息攻击中，基于其他有效消息的知识(例如，自适应选取的消息攻击)来生成有效消息/MAC对。密钥208是必要的以生成可信的MAC。密钥208保持是秘密的并且能够在必要时改变。这样的改变能够利用针对临床系统510的制造商软件版本进行协调。例如，临床系统510能够访问密钥的阵列，以基于存储器104上包含的序列号对血管内设备102进行授权。制造商能够利用每个新的软件版本(例如来自临床系统510)来改变密钥208并且要求所有更新的设备(例如，具有高于截止值的序列号)具有基于要认为可信的被写到存储器104的新的密钥的MAC。制造商或授权的第三方能够协调血管内设备102的销售，使得具有新的序列号的设备被售卖到具有已经具有新软件的临床系统510的区域。另外，能够针对临床系统510提供自动软件更新，其允许改变密钥的额外的灵活性。对CMAC和AES-128的暴力攻击当前被认识是计算上不可行的。因此，针对伪造的安全能够依赖于密钥208的安全。

[0073] 本领域技术人员将认识到，上文所描述的装置、系统和方法能够以不同的方式进行修改。相应地，本领域技术人间将意识到，本公开包含的实施例并不限于上文所描述的具体示范性实施例。在这一方面，尽管已经示出并描述了例示性实施例，在前述公开中包含宽范围的修改、改变和替换。应当理解，可以对前述内容做出这样的变型，而不偏离本公开的范围。相应地，应当意识到，随附的权利要求被宽泛地并且以与本公开一致的方式进行解释。

[0074] 尽管本公开主要参考血管内设备，本文所公开的系统也适于对任何一次性或有限适于设备的认证。本领域技术人员将意识到跨其他学科对本原理的应用。

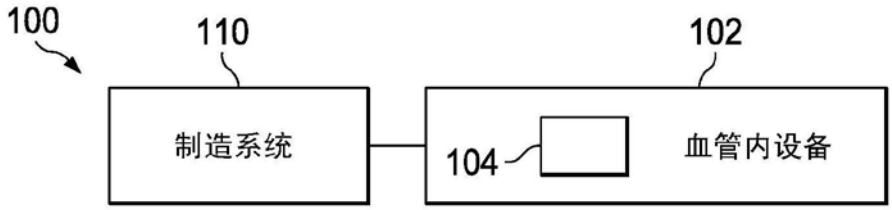

100
110
102
制造系统
104
血管内设备

图1

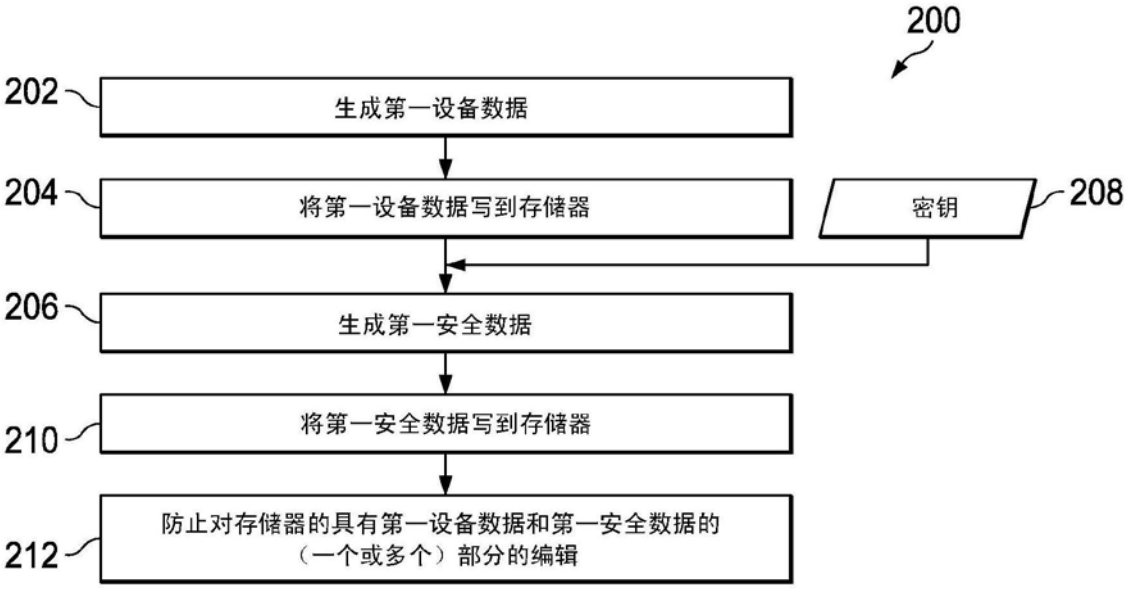

200
202
生成第一设备数据
204
将第一设备数据写到存储器
密钥
208
206
生成第一安全数据
210
将第一安全数据写到存储器
212
防止对存储器的具有第一设备数据和第一安全数据的
（一个或多个）部分的编辑

图2

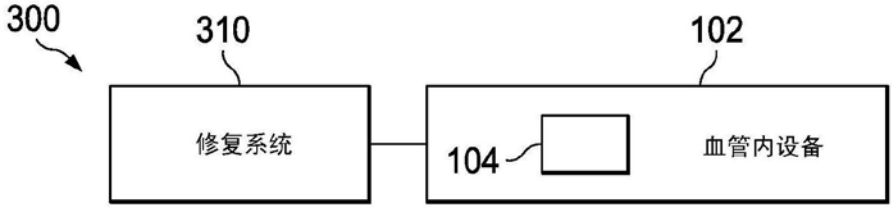

300
310
102
修复系统
104
血管内设备

图3

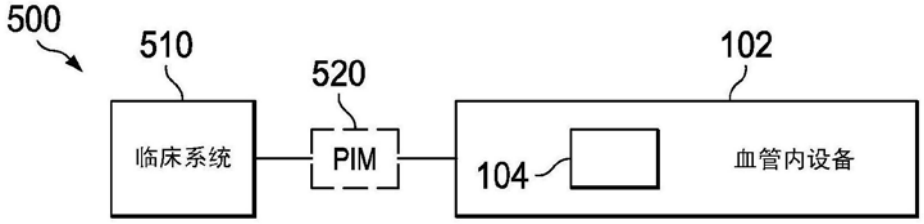

500
510
520
102
临床系统
PIM
104
血管内设备

图5

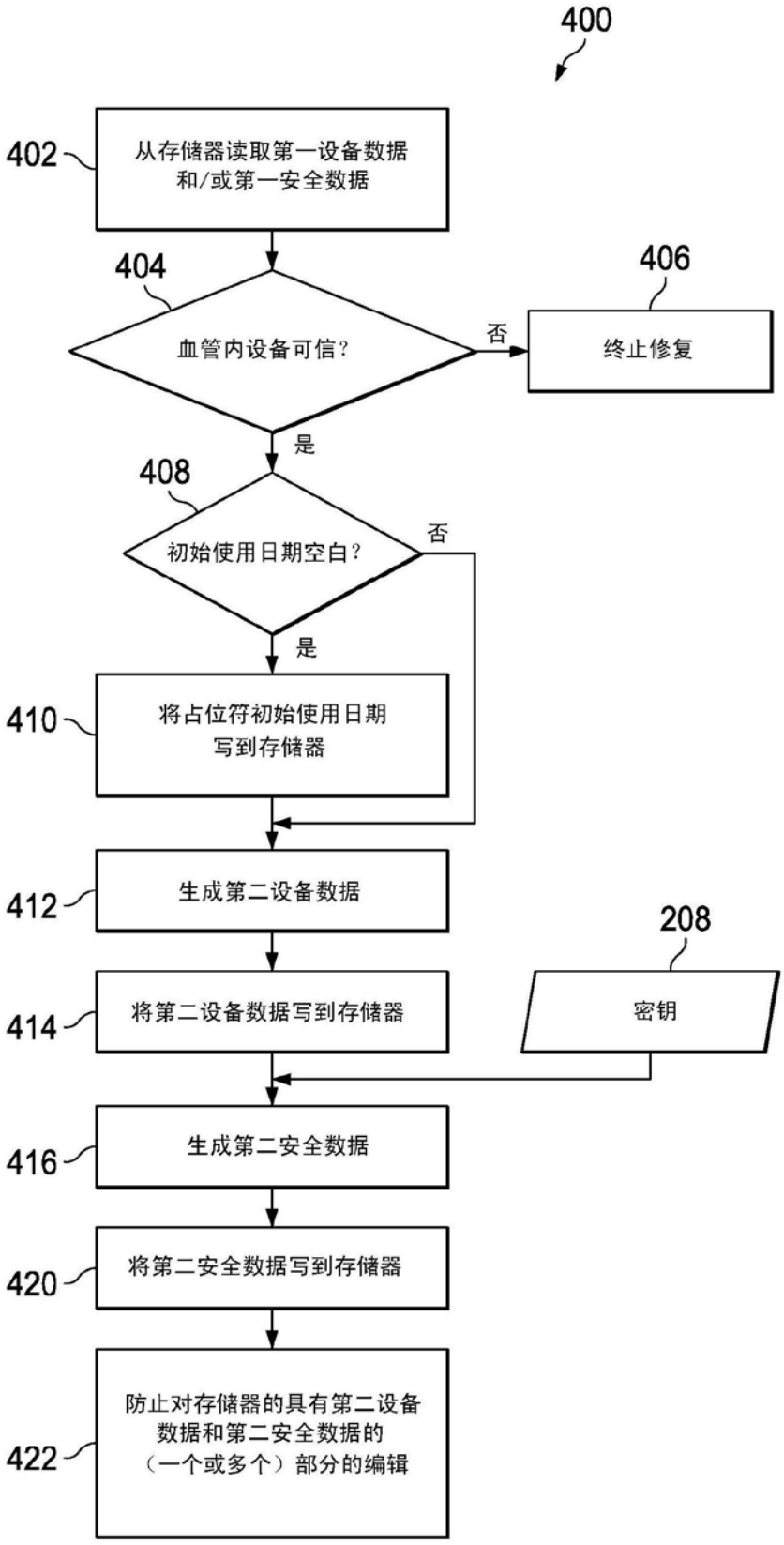

400
402
从存储器读取第一设备数据和/或第一安全数据
404
血管内设备可信？
否
406
终止修复
是
408
初始使用日期空白？
否
是
410
将占位符初始使用日期写到存储器
412
生成第二设备数据
208
密钥
414
将第二设备数据写到存储器
416
生成第二安全数据
420
将第二安全数据写到存储器
422
防止对存储器的具有第二设备数据和第二安全数据的（一个或多个）部分的编辑

图4

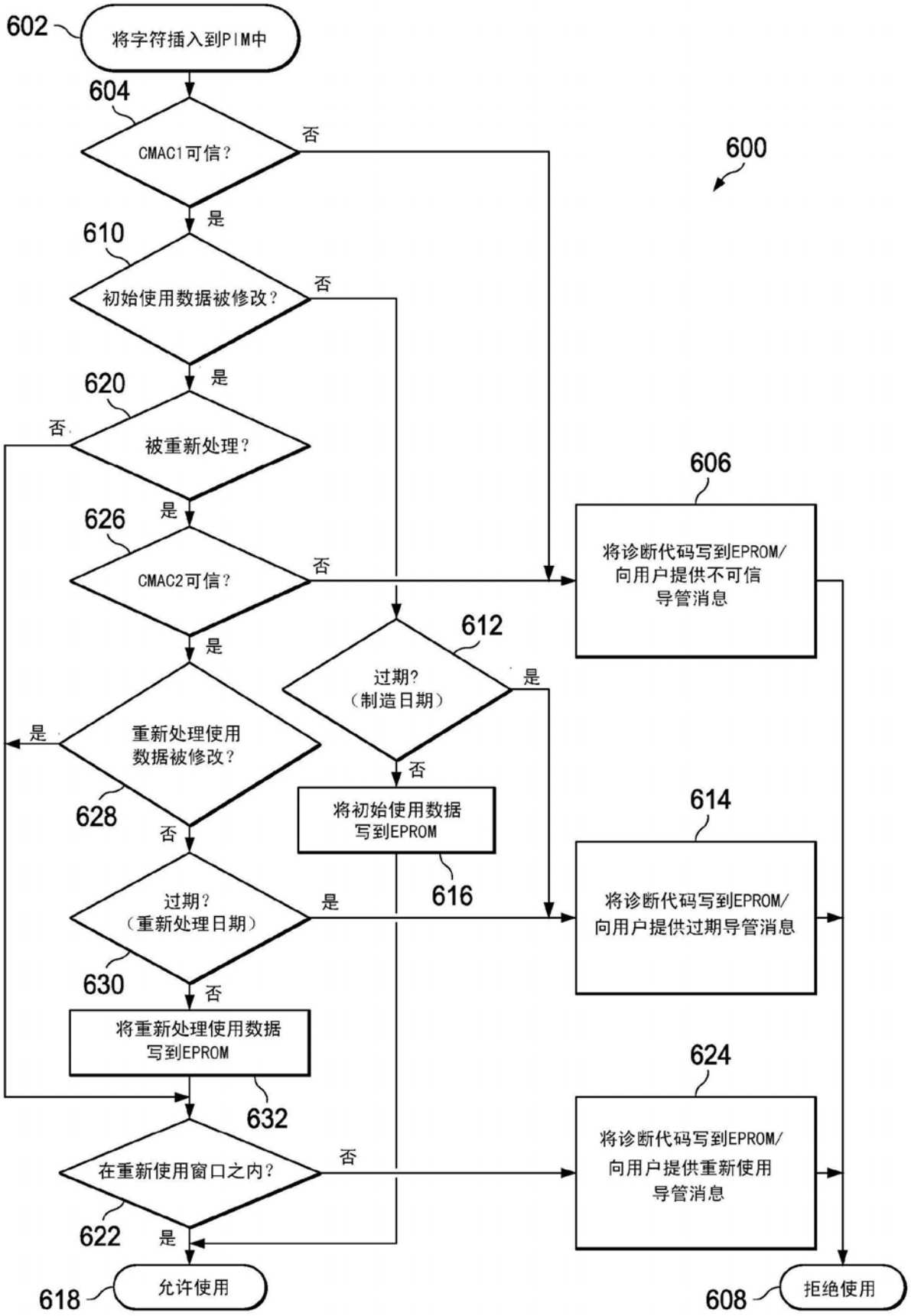

602
将字符插入到PIM中
604
CMAC1可信?
否
是
600
610
初始使用数据被修改?
否
是
620
被重新处理?
否
是
606
将诊断代码写到EPROM/
向用户提供不可信
导管消息
626
CMAC2可信?
否
是
612
过期?
(制造日期)
是
否
是
重新处理使用
数据被修改?
628
否
将初始使用数据
写到EPROM
614
616
过期?
(重新处理日期)
是
将诊断代码写到EPROM/
向用户提供过期导管消息
630
否
将重新处理使用数据
写到EPROM
624
632
在重新使用窗口之内?
否
将诊断代码写到EPROM/
向用户提供重新使用
导管消息
622
是
618
允许使用
608
拒绝使用

图6