



[12] 发明专利说明书

专利号 ZL 200580008775.2

[45] 授权公告日 2008 年 11 月 19 日

[11] 授权公告号 CN 100435063C

[22] 申请日 2005.3.3

审查员 冯慧萍

[21] 申请号 200580008775.2

[74] 专利代理机构 北京市金杜律师事务所

[30] 优先权

代理人 吴立明

[32] 2004.3.19 [33] US [31] 10/804,852

[86] 国际申请 PCT/IB2005/000567 2005.3.3

[87] 国际公布 WO2005/091109 英 2005.9.29

[85] 进入国家阶段日期 2006.9.19

[73] 专利权人 赫基亚有限公司

地址 芬兰埃斯波

[72] 发明人 L·帕特罗

[56] 参考文献

WO9914881A 1999.3.25

CN1342007A 2002.3.27

US2004225885A1 2004.11.11

WO0201328A2 2002.1.3

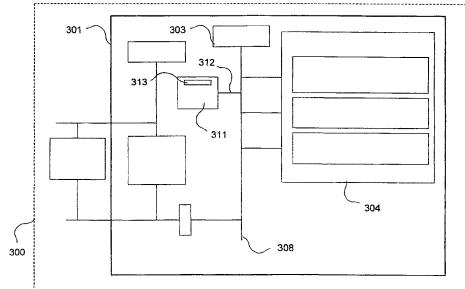
权利要求书 2 页 说明书 8 页 附图 4 页

[54] 发明名称

带加密协处理器的装置

[57] 摘要

本发明涉及一种其中提供了加速数据处理操作的电子装置(301)，该装置包括控制访问的安全执行环境。本发明的基本思想是要提供一种用于加速数据处理操作的装置(311)（“加速器”）。尤其是，使用加速器加速加密数据操作，从而对通过第一逻辑接口(312)提供给加速器的数据执行加密操作。借助于通过第二安全逻辑接口(312)提供给加速器的加密/解密密钥，执行加密操作。



1、一种电子装置(301)，其中提供了数据处理操作的加速，该装置包括限制访问的安全执行环境 (304)，并所述装置进一步包括：

用于加速数据处理操作的加速器 (311)，该加速器配置有：

第一逻辑接口，通过该第一逻辑接口提供待处理的数据，以及

第二安全逻辑接口，通过该第二安全逻辑接口提供在处理所述待处理的数据的操作中使用的密钥。

2、根据权利要求 1 所述的装置 (301)，其中，将加速器 (311) 配置使得第一逻辑接口和第二安全逻辑接口共享相同的物理接口。

3、根据权利要求 2 所述的装置 (301)，其中，加速器 (311) 进一步包括：

配置寄存器 (313)，配置成用来向加速器指示在所述装置中设置的处理器 (303) 设置了安全模式还是普通模式。

4、根据权利要求 3 所述的装置 (301)，其中，进一步设置配置寄存器 (313)，使得可将其设置成多个可能的加密模式中的一种，加速器 (311) 在配置寄存器中设置的加密模式下进行操作。

5、根据权利要求 1 所述的装置，其中，将加速器配置使得通过各个物理接口提供第一逻辑接口和第二安全逻辑接口。

6、根据权利要求 1 所述的装置 (301)，其中，将加速器的第一逻辑接口配置使得可被任一应用程序访问，而将加速器的第二安全逻辑接口配置成仅能被受保护应用程序访问。

7、根据权利要求 6 所述的装置 (301)，该装置进一步配置成使得受保护应用程序可以防止其它应用程序访问加速器 (311)。

8、根据权利要求 6 所述的装置 (301)，其中，受保护应用程

序是允许在安全执行环境（304）下执行的应用程序。

9、根据上述任一权利要求所述的装置，进一步包括：

存储电路（105，106，107），配置有至少一个存储区，涉及装置安全的受保护数据位于所述存储区，以及

处理器（103），可以将其设置为至少两个不同操作模式中的一种；以及；该装置进一步配置成：

当设置成安全处理器操作模式时，处理器访问所述存储区，所述受保护数据位于所述存储区中，

当设置成普通处理器操作模式时，拒绝处理器访问所述存储区；以及

当设置成安全处理器操作模式时，处理器能够访问加速器（311）的第二安全逻辑接口。

10、根据权利要求9所述的装置，其中，所述处理器（103）进一步配置成使得受保护的应用程序来控制处理器操作模式。

11、一种移动通信终端（300），包括根据上述任一权利要求所述的装置（301）。

12、一种用于加速数据处理操作的装置（311），该装置包括：
第一逻辑接口，通过该接口提供待处理的数据；以及
第二安全逻辑接口，通过该接口提供在处理所述数据的操作中使用的密钥。

13、根据权利要求12所述的装置（311），其中，将该装置配置使得第一逻辑接口和第二安全逻辑接口共享相同的物理接口。

14、根据权利要求13所述的装置（311），其中，该装置进一步包括：

配置寄存器（313），其被配置成用来指示所述装置设置为安全模式还是普通模式。

带加密协处理器的装置

发明的技术领域

本发明涉及一种提供了加速数据处理操作的电子装置，该装置包括控制访问的安全执行环境。本发明进一步涉及一种移动通信终端，该终端包括该电子装置和用于加速数据处理操作的装置。

背景技术

多种电子装置，例如移动电信终端、便携计算机及 PDA，需要访问安全相关组件，例如应用程序、密钥、密钥数据素材、中间加密计算结果、密码、外部下载数据的认证方式等。典型地，这些组件及其处理必需在电子装置内部保密。理想地，这些组件应尽可能不为人知，因为如果知道了装置的安全相关组件，可能会篡改装置。访问这类组件可能会帮助存有恶意企图操作终端的攻击者。

因此，提出了一种安全执行环境，在这种环境下，电子装置中的处理器能访问安全相关组件。应谨慎地限制对安全执行环境的访问、处理及退出。现有技术中包括这种安全环境的硬件常常是封装在抗篡改的外壳中。由于不能在这类硬件上探查或执行测量和测试，从而可能导致安全相关组件及其处理的泄密。

为了保护装置中的数据，应对驻留在永久的，即非易失性，存储器中的数据加密。由于一旦心存恶意的人访问到该装置，可能会企图访问装置中的敏感数据，例如通过盗取敏感数据，因此数据保护是非常必要的。另一种尝试访问敏感数据的情况是装置中包含一个数字权利管理（DRM）系统。这个 DRM 系统存储版权保护内容以及与确定用户采用何种访问形式访问内容的相关数字权利。这样，DRM 系统被用来保护内容不被未授权用户访问、误用和/或错误地分配。由于内容和权利具有经济价值，所以用户可能企图绕过 DRM 控制功能来访问内容。加密驻留在永久存储器中的数据应该是安全、有效和低成本的。如上文提到的，在当前的装置结构中，可以安全地处理安全执行环境中的安全相关组件。然而，这可能是有问题的，并且由于执行加密操作时，必须保证安

全进入和退出安全执行环境，因而导致在数据和控制信号传递方面出现相当高昂的开销。

另一方面，通过在安全环境外部使用现有技术中的硬件加速器，可以非常有效地进行加密。然而，由于组件是不受阻碍的，窃听者可能控制了来自加速器的安全组件，例如加密/解密密钥，因而出现了另一个问题。这可以通过在装置中引入安全测量来解决，但很可能需要额外的硬件和软件，从而产生无法承受的装置成本的提高。

发明概要

因此，本发明的目的是以一种使加速装置中使用的保密密钥不被装置用户或未授权的第三方所知的方式，在装置中提供加速数据处理操作，但在安全执行环境的外部，从而减少数据处理所需要的时间。

通过根据权利要求 1 所述的包括可以限制访问的安全执行环境的电子装置，在该装置中提供了加速数据处理操作，根据权利要求 11 所述的包括电子装置的移动通信终端，以及根据权利要求 12 所述的用于加速数据处理操作的装置，来实现该目的。

本发明的基本思想是要提供一种用于加速数据处理操作的装置（“加速器”）。尤其是，将加速器用来加速加密数据操作。为了克服现有技术中加速器的不足之处，必须提供一种加速器，它被配置使得通过第一逻辑接口向它提供的数据执行加密操作。借助于通过第二安全逻辑接口提供给加速器的加密/解密密钥，执行加密操作。为了防止每次进入/退出安全执行环境都要加密/解密数据，将加速器安置在安全环境的外部。

第二安全逻辑接口的使用，使得密钥不对装置用户或未授权的第三方公开。术语“逻辑”暗示加速器的第一和第二接口是隔离的，但不必进行物理隔离。它们逻辑上隔离就足够了，从而使在第二安全逻辑接口上进行传递时不可以访问第一逻辑接口。

理想地，仅允许所谓的受保护应用程序处理保密密钥，这种受保护应用程序往往是用于执行安全执行环境内部安全关键操作的小规模应用程序。受保护应用程序是由可信赖的提供商发布的应用程序，在这种情况下，这些应用程序必须被认证，但也可以由任意第三方发布，无论该第三方是否可信赖。在后一种情况下，不需要认证。必须从特定上下文确定，受保护应用程序是否必须由

可信赖的提供商发布。一般来说，被配置成具有或给予破坏装置安全性的能力的应用程序是可信赖的。

受保护应用程序应认为是在安全环境外部执行的“普通”应用程序的一部分。受保护应用程序也可以包括用来实现装置中标准功能的应用程序。例如，利用受保护应用程序来引导装置并在其中加载操作系统。所期望的是，即使装置用户无法被看作是未授权第三方，装置用户也不能访问保密密钥。可能的话，在装置中实现 DRM 系统，因为依靠 DRM 系统提供的数字内容—以及相关的数字权利—具有经济价值，所以用户企图通过绕过 DRM 控制功能来访问内容。当然，还有其它不让用户访问密钥的理由；例如必须把通用安全方面纳入考虑范围之内。

在普通装置操作模式下，装置处理器不访问位于安全环境中的安全相关数据。安全数据包括加密密钥和算法、用于引导电路的软件，诸如用作加密密钥素材的随机数之类的保密数据、应用程序等。对这些安全数据进行的访问和处理是受限制的。当测试和/或调试通常位于移动通信终端中的装置时，不允许访问安全相关数据。为此原因，将处理器设置成普通、或“不安全”操作模式，在这种模式下，处理器不再访问安全环境中的受保护数据。从而，在普通模式下，处理器及其执行的相应应用程序不访问加速器的密钥。

本发明是有利的，因为可以安全地控制加密/解密密钥的提供，而加密操作的初始化可以由在安全执行环境外部执行的普通应用软件执行。实际上，普通应用程序把加速器看成按需解密和/或加密数据的普通硬件外围设备。然而，普通应用程序无法获取与加速器相关联的敏感安全组件，例如正在使用的密钥。

此外，根据本发明的实施方案，受保护应用程序可以防止普通应用程序在任何时候以任何被视为必需的理由来访问加速器。例如，如果发现普通应用程序已被篡改时。

根据本发明的实施方案，装置处理器可以设置成至少两种不同操作模式中的一种。在所述装置中，存储电路配置成至少一个存储区，涉及装置安全的受保护数据位于所述存储区。当安全处理器操作模式被设置时，处理器访问存储区；当普通处理器操作模式被设置时，拒绝处理器访问所述存储区。根据处理器及其执行的应用程序访问或不访问存储区的事实来定义实际操作模式。当安

全处理器操作模式被设置时，处理器能够进一步访问加速器的第二安全逻辑接口。

存储电路中存储区的访问定义了处理器的安全操作模式。在安全执行模式下操作时，处理器可以访问的存储区被视为安全执行环境。如前面所提及的，这些存储区包括安全相关组件，例如应用程序、密钥、密钥数据素材、中间加密计算结果、密码、用于外部下载数据的认证方式等。在安全执行模式下，处理器能够访问加速器的安全接口，通过该接口提供密钥。这样，处理器能够把密钥加入加速器，或者更改加速器中的密钥。因为施加在普通、不安全处理模式下的装置上的安全限制是很严格的，因此这是重要的，也是非常有利的。

根据本发明的另一个实施方案，加速器的第一接口可被任意应用程序访问，而加速器的第二安全接口仅能被受保护应用程序访问。典型地，装置处理器中执行的普通应用程序、装置的数字信号处理器或者装置中的一些其它处理设备，不受阻碍地把数据发送到加速器，加速器用从安全环境接收的保密密钥加密数据，并将加密后的数据返回给普通应用程序。因此，这意味着处理器在普通操作模式下。在普通操作模式下，普通应用程序可以使用涉及数据加密/解密的加速器服务。也可能是受保护应用程序想使用这些服务。这些受保护应用程序有这么做的权利，并且普通应用程序和受保护应用程序可以交替请求来自加速器的加密服务。然而，当处理器在安全执行模式下运作时，仅允许执行受保护应用程序。这样，为了访问第二安全逻辑接口，处理器必须在安全模式下运作并执行受保护的应用程序。

仍然根据本发明的另一个实施方案，加速器进一步包括配置寄存器，其被设置用来指示加速器，通过处理器来设置安全操作模式或普通操作模式，并且在这种配置寄存器中还可能设置成多种可能的加密模式中的一种，加速器配置成在寄存器中设置的加密模式下运作。由于加速器本质上在可能的操作模式之间是有区别的，因此不必每次将要执行所请求的加密操作时请求来自装置处理器的模式验证，所以，使用加速器配置寄存器是有利的。该寄存器也可以将加速器配置成具有提供第一和第二逻辑接口的一个物理接口。此外，因为可以迅速确定将使用例如密码分组链接（CBC）模式、电子源码书（EBC）模式、密码反馈（CFB）模式、明文反馈（PFB）模式或者其它加密模式，因此可以设置成不同加密模式的事实是有利的。

研究附加的权利要求和下列描述后，本发明的进一步特点和优势将是显而易见的。本领域的技术人员认识到本发明的不同特征可以进行组合，从而构造除了下列描述之外的其它实施方案。

附图简述

参照下列附图，对本发明作更详细地描述，其中，

图 1 示出了用于提供数据安全的装置结构的示意图，其中在该结构中有利应用本发明；

图 2 示出了用于提供数据安全的装置结构的示意图，该装置可进一步配置有可移动智能卡，其中在该结构中有利应用本发明；

图 3 示出了图 1 装置结构中实现的根据本发明实施方案的加速器的示意图；以及

图 4 示出了图 1 装置结构中实现的根据本发明的另一个实施方案的加速器的示意图。

本发明优选实施方案的描述

图 1 示出了用于提供数据安全的装置结构。在该申请人的国际专利申请公开 WO2004/015553 中进一步公开了该系统，该申请在此引入作为参考。用于提供数据安全的电路以 ASIC（特定用途集成电路）101 的形式实现。该结构的处理部分包括 CPU 103 和数字信号处理器（DSP）102。ASIC 101 包含在电子设备 100 中，例如移动电信终端、便携式计算机、PDA 等，ASIC 101 被视为设备 100 的“大脑”。

安全环境 104 包括引导 ASIC 101 的 ROM 105。该 ROM 105 包括引导应用软件和操作系统。位于安全环境 104 中的某些应用程序优先于其它应用程序。在配置了 ASIC 101 的移动电信终端中，应该存在引导软件，该软件包括终端的主要功能。没有该软件，则不能把终端引导到普通操作模式。这带来了如下优点，即通过控制该引导软件，也能控制每个终端的初始激活。

安全环境 104 还包括 RAM 106，RAM 106 存储数据和应用程序，即受保护数据。RAM 106 优选存储所谓的受保护应用程序，该程序的规模较小，用于执行安全环境 104 内部的安全关键操作，但也存储诸如密钥、中间加密计算结果和密码之类的对象。通常，采用受保护应用程序的方式是让“普通”应用程序请求来自某一特定受保护应用程序的服务。可以在任何时候把新的受保护应

用程序下载到安全环境 104 中，如果应用程序在 ROM 中，则不是这样。安全环境 104 软件控制受保护应用程序的下载和执行。受保护应用程序可以访问安全环境 104 中的任何资源，也可以为了提供安全服务而它们和普通应用程序通信。

在安全环境 104 中，包括熔丝存储器（fuse memory）107，该存储器包含一个在制造过程中生成并编程到 ASIC 101 中的唯一随机数。该随机数用作特定 ASIC 101 的身份，并进一步用来获取加密操作中的密钥。此外，以安全控制寄存器形式的存储电路访问控制装置被配置在安全环境 104 中。安全控制寄存器的目的是依靠寄存器中设定的模式，让 CPU 103 访问安全环境 104，或者防止 CPU 103 访问安全环境 104。CPU 103 的操作模式可以通过应用程序软件在寄存器中设置，这样，该结构不必依赖外部信号。从安全观点看，这是优选的，因为通过控制应用程序软件，也可以控制处理器模式的设置。也可能将外部信号（未示出）连接到 ASIC 101，通过这种外部信号可以设置安全控制寄存器。通过采用外部信号，可以轻松快捷地执行模式变换，这在测试环境中更有利。组合这两种模式设置方式，即应用程序软件和外部信号，是切实可行的。

该结构进一步包括用来限制总线 108 上的数据可见性的标准桥接电路 109。该结构应密封在抗篡改外壳中。不能在这类硬件上探查或执行测量和测试，这可能导致安全相关组件以及其处理的泄密。DSP 102 可以访问其他外围设备 110，例如可以在 ASIC 101 的外部提供的直接存储器存取（DMA）单元、RAM、闪存、附加处理器。

图 2 示出了用于提供数据安全的装置结构的另一个实施方案，其中对应的附图标记表示如图 1 中描述的相应元件。与图 1 所示结构相比，图 2 中示出的结构的区别点在于电子设备 200 配置有可移动智能卡 211，例如 SIM 卡，这也能够看作是安全环境。出于安全目的，移动终端 200 和智能卡 211 存储由可信赖的鉴定机构（CA）颁发的数字证书。证书用来确保与移动终端 200 和/或智能卡 211 进行通信的参与者，即特定证书持有者，已经由相应的可信赖 CA 授权。CA 签署证书，并且证书持有者必须拥有和 CA 的私钥相对应的公钥，从而验证 CA 签署的证书是有效的。注意不同装置可以拥有不同 CA 颁发的证书。在这种情形下，不同的 CA 必须相互之间进行一些通信，例如交换他们自己的公钥。证书为那些本领域的技术人员所熟知，并且一种众所周知的标准证书是包

括在 CCITT 建议 X.509 中的证书。

图 3 示出了如图 1 中描述的装置结构，于此实现了加速器 311。对应的附图标记再次表示如图 1 中描述的相应元件。在该实施方案中，加速器配置有一个物理接口 312。当处理器 303 的普通、不安全执行模式被设置时，该物理接口充当第一逻辑接口，在其上提供了待加密/解密的数据。而当处理器的安全执行模式被设置时，物理接口充当第二安全逻辑接口，在其上提供了加密/解密数据操作中使用的密钥。此外，在该实施方案中，加速器配备了配置寄存器 313，该寄存器被设置以指示加速器，处理器设置了安全操作模式还是普通操作模式。这个寄存器位于总线 308 上的地址中，如果启动安全执行模式，则仅允许处理器写到该地址。因此，仅允许受保护应用程序设置、改变或修改该寄存器。如果以适当方式设置寄存器 313，即对寄存器设置预定代码，则可以把密钥写入加速器。

最初，当对实施在诸如移动通信终端 300 之类的电子设备中的 ASIC 301 进行引导时，处理器在其安全执行模式下操作，并且受保护应用程序恰当地设置了配置寄存器，因此，受保护应用程序通过物理接口 312 可以为加速器 311 提供一个（或多个）密钥，物理接口 312 从而充当了第二安全逻辑接口。在初始化之后，受保护应用程序改变配置寄存器 313，从而使在给定配置下，不能修改或更改加速器中的密钥。此外，受保护应用程序把处理器 303 设置为普通执行模式，并把装置 301 的操作移交给普通应用程序。因此，物理接口 312 充当第一逻辑接口，并且处理器可以把要进行加密处理的数据提供给加速器。在 ASIC 301 运作期间，可以通过在安全执行模式下执行的处理器来改变密钥。

在配置寄存器中，更可能的是设置多种可能的加密模式（CBC, EBC, CFB 等）中的一种，加速器在上述加密模式下运作。

图 4 示出了如图 1 中描述的装置结构，此处实现了加速器 411 的另一个实施方案。对应的附图标记再次表示如图 1 中描述的相应元件。在该实施方案中，加速器配置有两个物理接口 412、414。当处理器 403 的普通、不安全执行模式被设置时，第一物理接口充当第一逻辑接口 412，在其上提供待加密/解密的数据。而当处理器的安全执行模式被设置时，第二物理接口充当第二安全逻辑接口 414，在其上提供加密/解密数据操作中使用的密钥。第二安全逻辑接口和处理器直接相连，处理器仅允许在启动安全执行模式时写入第二接口。因此，仅

允许受保护应用程序设置、改变或修改密钥。

在加速器 411 的这个实施方案中，最初，当引导 ASIC 401 时，使处理器在其安全执行模式下运转，并且受保护应用程序通过第二安全逻辑接口 414 设置密钥。在初始化之后，受保护应用程序把处理器 403 设置为普通执行模式，并把装置 401 的操作移交给普通应用程序。于是，处理器可以通过第一逻辑接口 412 把要进行加密处理的数据提供给加速器。

在加速器的这个实施方案中，加速器也可以配置有配置寄存器（未示出），其中可以设置为多种可能的加密模式（CBC，EBC，CFB 等）中的一种，加速器在上述加密模式下运作。这个寄存器可以通过第二安全逻辑接口 414 由处理器 403 进行设置。

即使已经参考本发明的特定示例性实施方案描述了本发明，但是对于本领域的技术人员来说，许多不同的改变、修改等也是显而易见的。因此，所描述的实施方案不用来限定如所附权利要求所定义的本发明的范围。

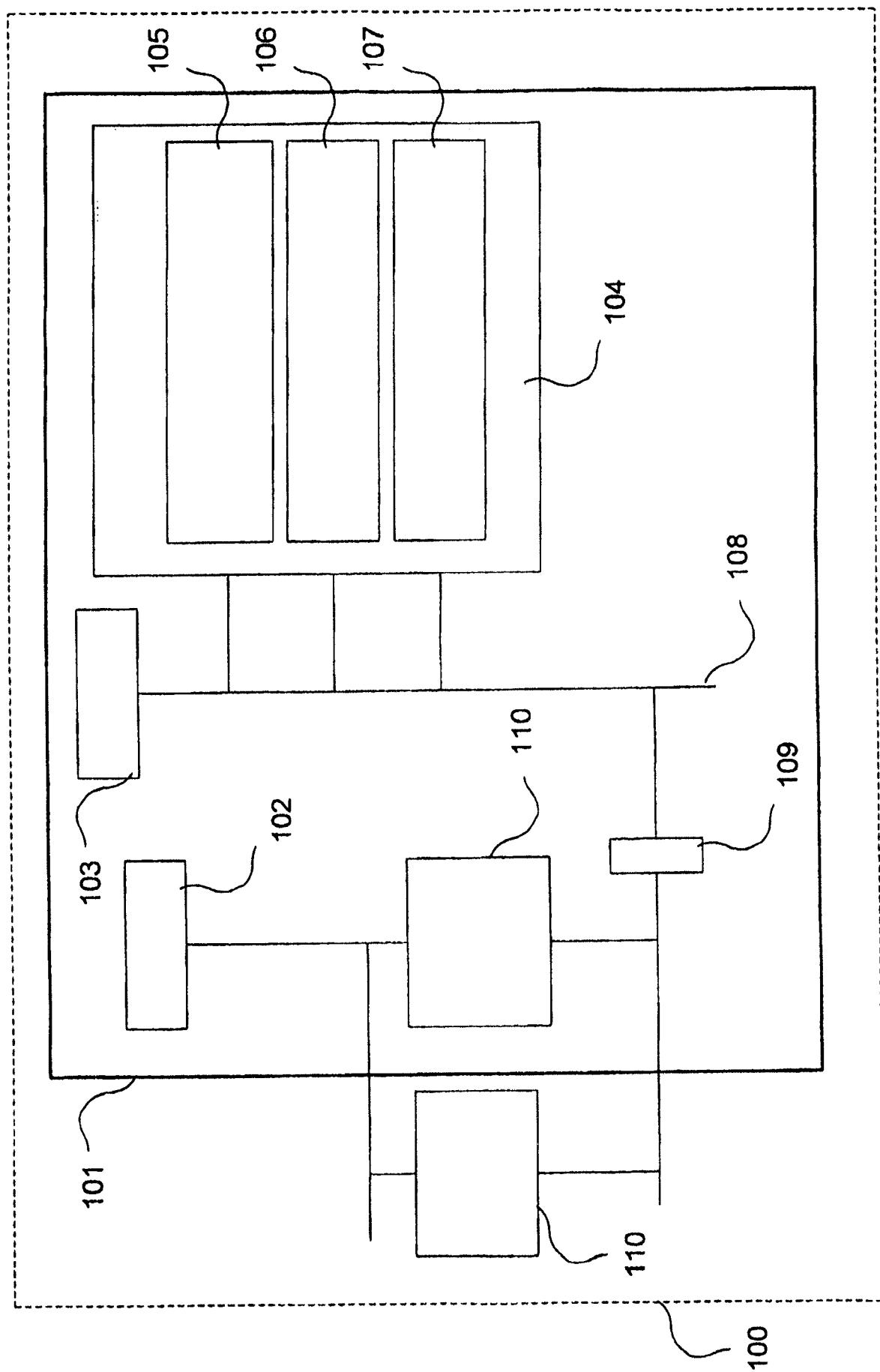


图 1

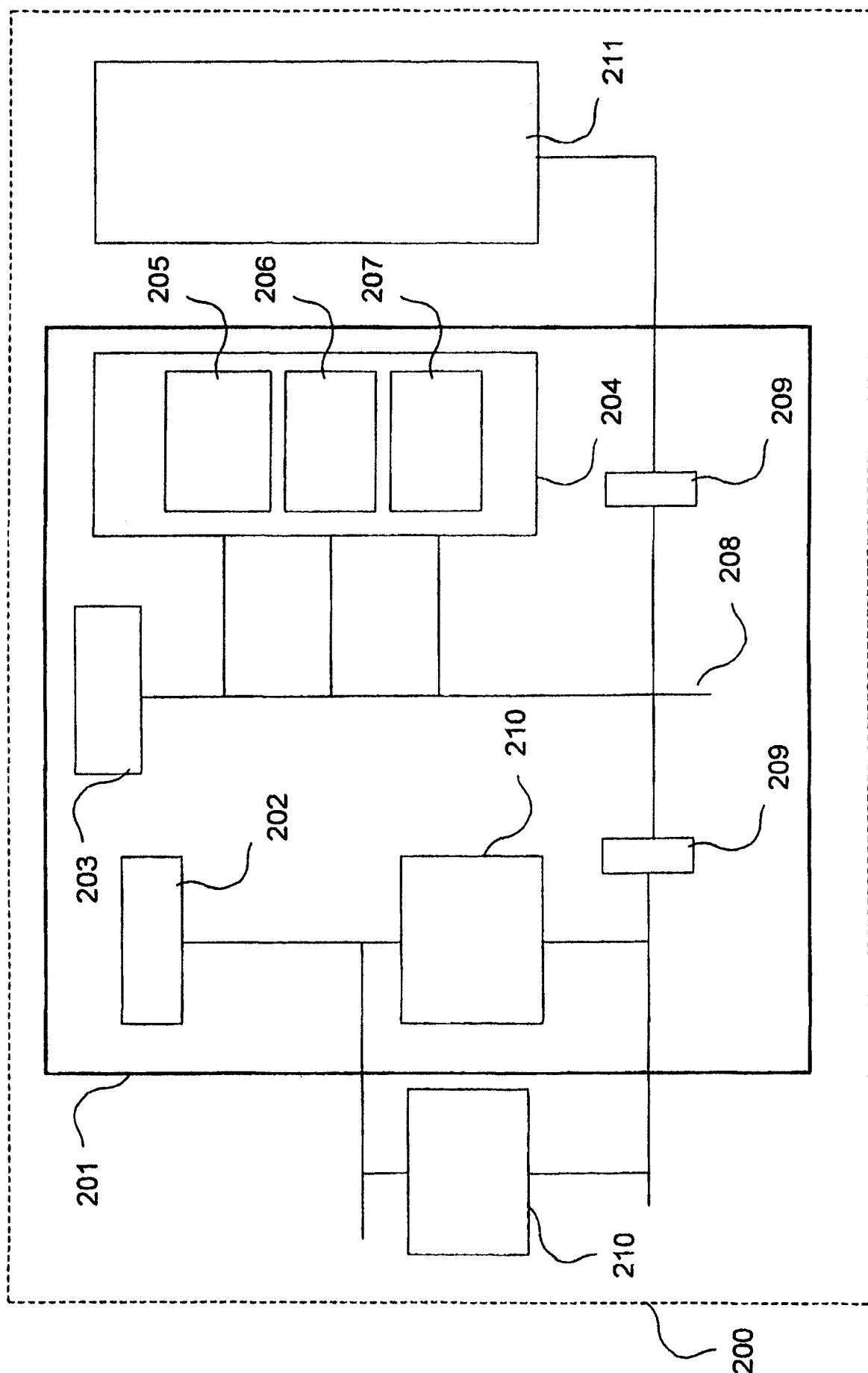


图 2

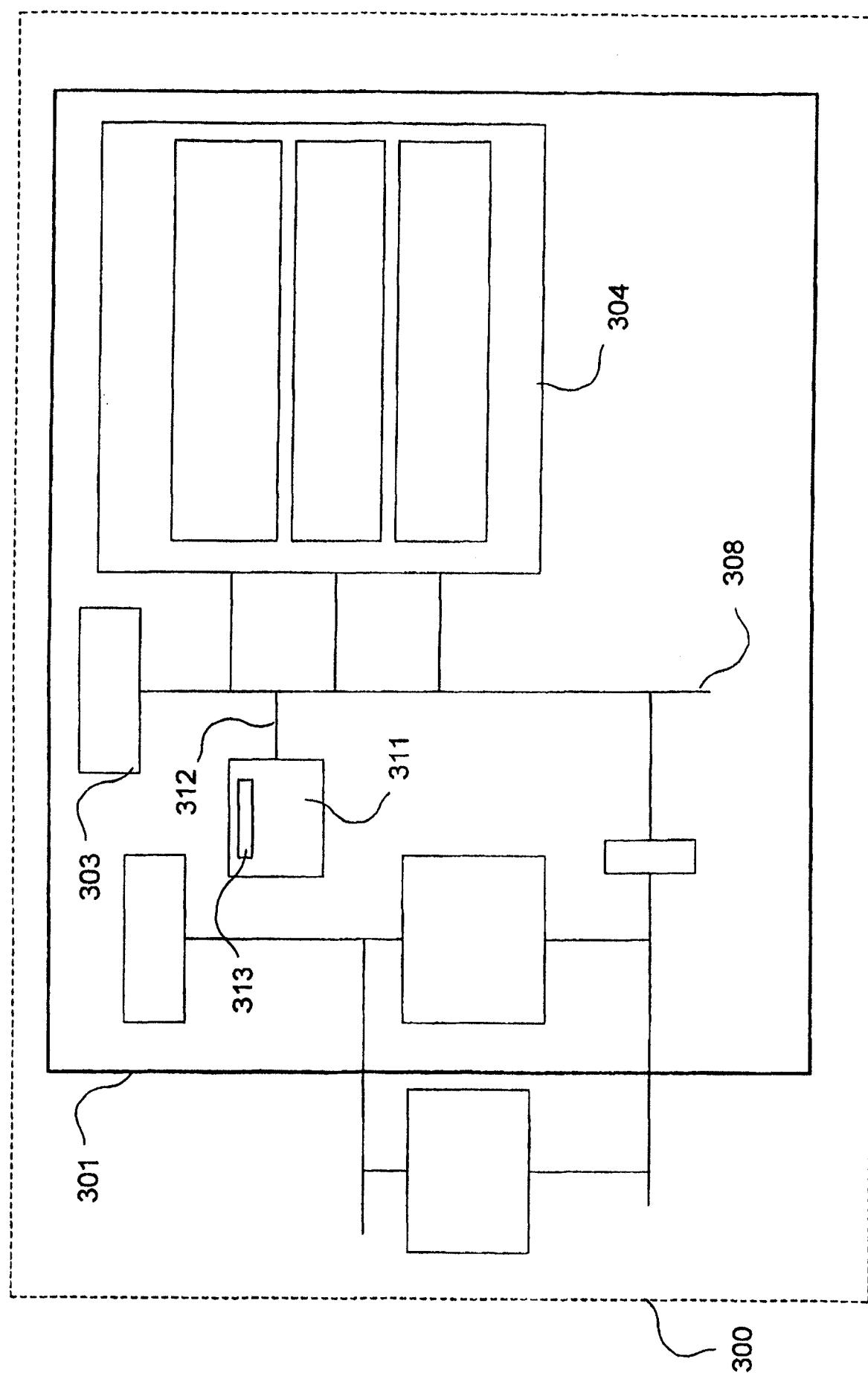


图 3

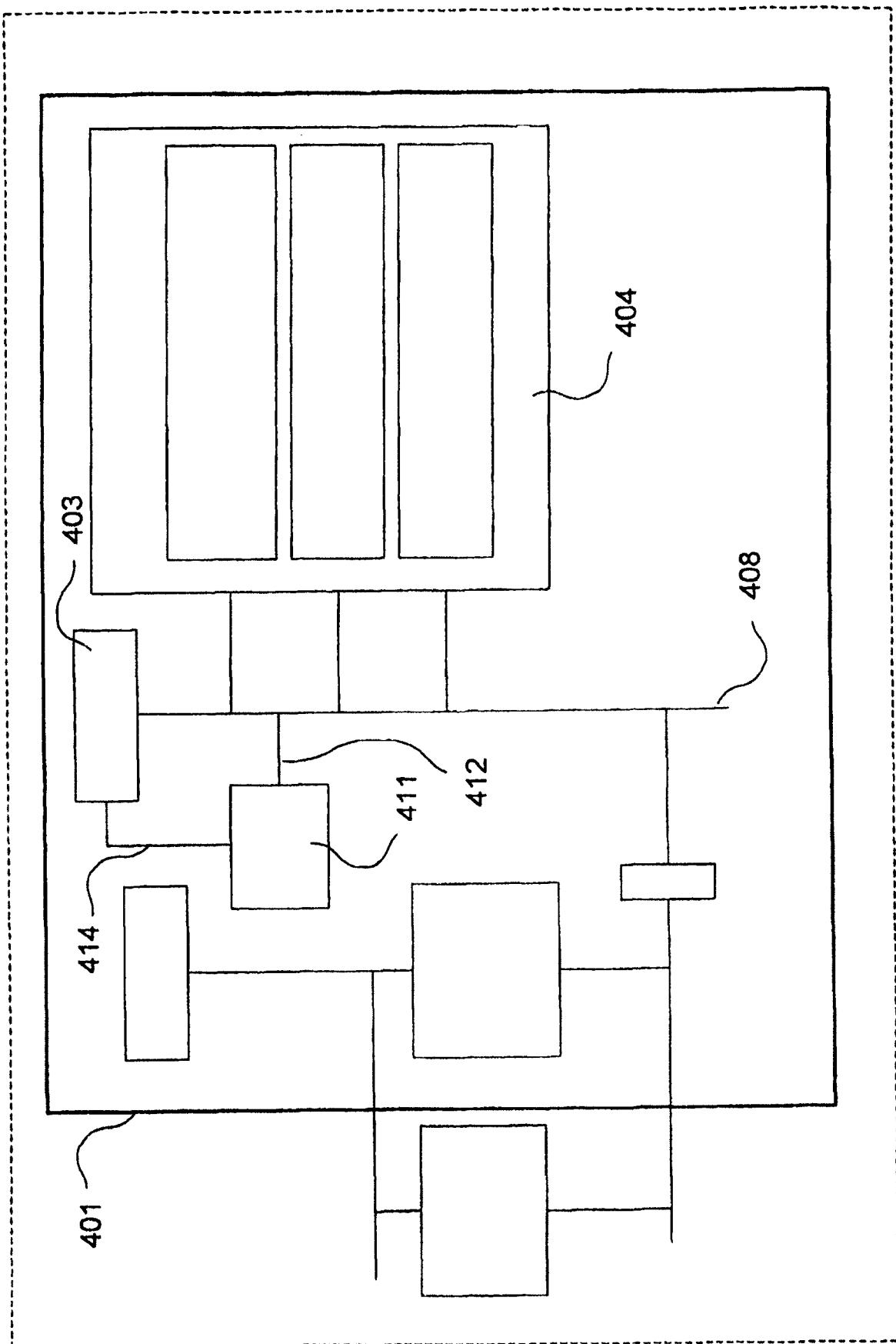


图 4