



[12] 发明专利申请公开说明书

[21] 申请号 03805171.0

[43] 公开日 2005 年 7 月 13 日

[11] 公开号 CN 1639666A

[22] 申请日 2003.3.5 [21] 申请号 03805171.0
 [30] 优先权
 [32] 2002. 3. 8 [33] US [31] 10/094,082
 [86] 国际申请 PCT/US2003/007117 2003. 3. 5
 [87] 国际公布 WO2003/077085 英 2003. 9. 18
 [85] 进入国家阶段日期 2004. 9. 3
 [71] 申请人 飞思卡尔半导体公司
 地址 美国得克萨斯
 [72] 发明人 威廉姆·C·莫耶
 迈克尔·D·菲茨西蒙斯

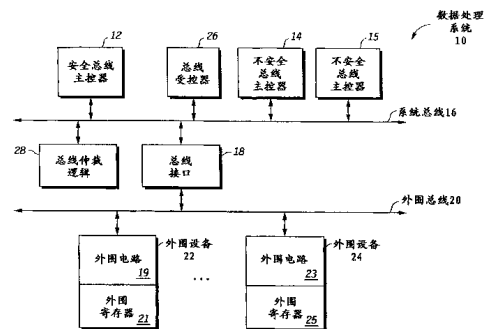
[74] 专利代理机构 中国国际贸易促进委员会专利商
 标事务所
 代理人 党建华

权利要求书 3 页 说明书 10 页 附图 3 页

[54] 发明名称 具有外围设备访问保护的数据处理系统及其方法

[57] 摘要

本发明涉及具有外围设备访问保护的数据处理系统及其方法，其中的一个实施例在数据处理系统(10)内提供柔性外围设备访问保护机构，以便获得更安全的操作环境。例如，数据处理系统包括需要访问共享外围设备(22, 24)的安全(12)和不安全总线主控器(14, 15)的组合。一个实施例允许安全总线主控器(12)动态更新每个不安全总线主控器针对每个外围设备的访问许可。从而，安全总线主控器能建立哪些不安全总线主控器具有对哪个外围设备的访问许可，以便保护数据处理系统不因在不安全总线主控器上运行的错误或敌对软件而导致恶化。通过使用总线主控器标识符(36)，基于安全总线主控器建立的许可而允许或拒绝对所请求外围设备的访问。



1. 一种用于在数据处理系统内提供外围设备访问保护的方法，包括：

启动要求访问外围设备（22，24）的总线周期；
在总线周期的至少一部分中提供总线主控制器标识符（36）；
使用总线主控制器标识符来选择总线周期的访问控制信息；以及
确定访问控制信息是否允许总线主控制器访问外围设备。

2. 如权利要求1所述的方法，进一步包括：

启动要求访问外围设备的第二总线周期；
在第二总线周期的至少一部分中提供第二总线主控制器标识符；
使用第二总线主控制器标识符来选择第二总线周期的第二访问控制信息；以及

确定第二访问控制信息是否允许第二总线主控制器访问外围设备。

3. 如权利要求1所述的方法，进一步包括：

如果访问控制信息允许总线主控制器访问外围设备，就继续总线周期并且访问外围设备；以及

如果访问控制信息不允许总线主控制器访问外围设备，就在访问外围设备之前终止总线周期。

4. 如权利要求1所述的方法，进一步包括：

启动要求访问存储电路的第二总线周期，其中，存储电路储存访问控制信息；

在第二总线周期的至少一部分中提供第二总线主控制器标识符；以及

确定第二总线主控制器标识符是否允许访问储存访问控制信息的存储电路。

5. 如权利要求1所述的方法，进一步包括：

启动要求访问外围设备的第二总线周期；

在第二总线周期的至少一部分中提供总线主控制器标识符；

使用总线主控器标识符来选择第二总线周期的第二访问控制信息；以及

确定第二访问控制信息是否允许总线主控器访问外围设备，其中，第一总线周期是读总线周期，而第二总线周期是写总线周期。

6. 如权利要求 1 所述的方法，进一步包括：

启动要求访问外围设备另一部分的第二总线周期；

在第二总线周期的至少一部分中提供总线主控器标识符；

使用总线主控器标识符和至少一个地址信号来选择第二总线周期的第二访问控制信息；以及

确定第二访问控制信息是否允许第二总线主控器访问外围设备的所述另一部分。

7. 一种数据处理系统（10），包括：

具有地址部分（42）、数据部分（40）和总线主控器标识符部分（36）的系统总线（16）；

耦合到系统总线的第一总线主控器（14）；

耦合到系统总线的第二总线主控器（15）；

外围总线（20）；

耦合到外围总线的外围设备（22, 24）；

用于把系统总线耦合到外围总线的接口电路（18）；

储存与第一总线主控器相应的第一访问控制值的第一存储电路（60）；

储存与第二总线主控器相应的第二访问控制值的第二存储电路（62）；以及

耦合到系统总线并耦合到第一和第二存储电路的总线主控器许可确定电路（50），所述总线主控器许可确定电路使用总线主控器标识符部分来选择与总线主控器标识符部分相应的第一访问控制值，该值表示第一总线主控器正在进行对外围设备的当前访问，所述总线主控器许可确定电路从第一访问控制值确定是否拒绝第一总线主控器访

问外围设备。

8. 如权利要求 7 所述的数据处理系统，其中，第一和第二存储电路包括在与外围设备不同的位置上位于数据处理系统存储器映象中的寄存器的至少一部分。

9. 如权利要求 7 所述的数据处理系统，其中，系统总线进一步包括：

耦合到总线主控制器许可确定电路的信号，该信号用于表示拒绝第一总线主控制器访问外围设备。

10. 一种用于在数据处理系统内提供外围设备访问保护的方法，包括：

提供第一总线主控制器（14 或 12）；

提供第二总线主控制器（15）；

启动要求访问外围设备（22，24）的第一总线周期；

在第一总线周期的至少一部分中提供与第一总线主控制器相应的第一总线主控制器标识符；

使用第一总线主控制器标识符来选择第一总线周期的第一访问控制信息；

使用第一访问控制信息来确定是否因为不允许第一总线主控制器访问外围设备而终止第一总线周期；

启动要求访问外围设备的第二总线周期；

在第二总线周期的至少一部分中提供与第二总线主控制器相应的第二总线主控制器标识符；

使用第二总线主控制器标识符来选择第二总线周期的第二访问控制信息；以及

使用第二访问控制信息来确定是否因为不允许第二总线主控制器访问外围设备而终止第二总线周期。

具有外围设备访问保护的 数据处理系统及其方法

技术领域

本发明涉及一种数据处理系统，并更具体地涉及一种具有外围设备访问保护的数据处理系统。

背景技术

在关于芯片上系统（SoC）的解决方案中，一般具有多个主控器，所述多个主控器具有共享的外围设备。SoC的一些主控器可以是不可信主控器。在这样的系统中，需要保护部分或全部外围设备不被不可信主控器访问，因为此访问可导致系统恶化。例如，可通过在不可信主控器上运行的软件而引入病毒，或者，不可信主控器可用于获得对系统外围设备内的安全信息的访问。而且，为了确保安全的数据处理，需要对外围设备的保护。

一个现有技术的解决方案要求系统内的每个主控器具有它自己专用的外围设备，从而，在主控器之间不共享外围设备。然而，使用专用外围设备导致需要重复许多原本可共享的外围设备，因而导致增加芯片面积和成本。而且，使用具有专用外围设备的主控器妨碍系统内处理负载均衡的使用。例如，如果不需要专用外围设备来执行传输的过程，由一个主控器执行的过程就不能传输到系统内的另一主控器，由此降低系统效率。

从而，对于数据处理系统，要求允许可信和不可信主控器共享数据处理系统内的外围设备，同时避免不可信主控器对这些共享外围设备的访问。

附图说明

本发明通过实例来说明，并且不受附图的限制，在附图中，相同的参考号代表相似的元件，其中，

图 1 以框图形式示出根据本发明一个实施例的数据处理系统；

图 2 以框图形式示出根据本发明一个实施例的图 1 总线接口的一部分；

图 3 以框图形式示出根据本发明一个实施例的访问控制寄存器；
以及

图 4 以框图形式示出根据本发明一个实施例的图 3 访问控制寄存器的一部分。

有经验的技术人员清楚：附图中的元件是为了简单和清晰起见而示出的，不必按比例绘制。例如，图中一些元件的尺寸相对其它元件被放大，这样有助于加深对本发明实施例的理解。

具体实施方式

本发明的一个实施例在数据处理系统内提供柔性外围设备访问保护机构，以便获得更安全的操作环境。例如，数据处理系统可包括需要访问共享外围设备的安全和不安全总线主控器的组合。一个实施例允许安全总线主控器动态更新每个不安全总线主控器针对每个外围设备的访问许可。从而，安全总线主控器能建立哪些不安全总线主控器具有对哪个外围设备的访问许可，以便保护数据处理系统不因在不安全总线主控器上运行的错误或敌对软件而导致恶化。通过使用总线主控器标识符，基于安全总线主控器建立的许可而允许或拒绝对所请求外围设备的访问。

图 1 示出数据处理系统 10 的一个实施例。数据处理系统 10 包括安全总线主控器 12、总线受控器 26、不安全总线主控器 14、不安全总线主控器 15、总线仲裁逻辑 28、系统总线 16、总线接口 18、外围总线 20、以及外围设备 22 和 24。安全总线主控器 12、总线受控器 26、不安全总线主控器 14、不安全总线主控器 15、总线仲裁逻辑 28 和总线接口 18 全都双向耦合到系统总线 16。总线接口 18、外围设备 22

和外围设备 24 全都双向耦合到外围总线 20。外围设备 22 包括外围电路 19 和外围寄存器 21，并且，外围设备 24 包括外围电路 23 和外围寄存器 25。尽管在图 1 中只示出两个外围设备 22 和 24，但数据处理系统 10 可包括耦合到外围总线 20 的任意数量的外围设备。同样，任意数量的安全总线主控器、不安全总线主控器和受控设备可耦合到系统总线 16，并且不局限于图 1 中所示的。而且，虽然图 1 示出总线仲裁逻辑 28 作为耦合到系统总线 16 的独立单元，但总线仲裁逻辑 28 的部分可位于耦合到系统总线 16 的每一个总线主控器（或总线主控器的一部分）中。（在现有技术中，总线仲裁逻辑 28 可作为任何已知的总线仲裁器操作。）

在一个实施例中，安全总线主控器 12、不安全总线主控器 14 和不安全总线主控器 15 可以是处理器，如微处理器、数字信号处理器等，或者可以是任何其它类型的主控设备，如直接存储器存取（DMA）单元。在一个实施例中，安全总线主控器 12 是比不安全总线主控器 14 和 15 更不易恶化的处理器。例如，安全总线主控器 12 可执行由安全总线主控器 12 制造商完全控制的指令（即，在安全总线主控器 12 上运行的软件被认为是可信软件）。也就是说，在此实例中，第三方软件不能在安全总线主控器 12 上运行，并且不允许第三方访问安全总线主控器 12。可替换地，安全总线主控器 12 的安全级别可从十分安全到更少信任变化，并且取决于数据处理系统 10 的设计，但它一般比不安全总线主控器 14 和 15 更安全。

不安全总线主控器 14 和 15 一般是更容易访问的。在一个实施例中，不安全总线主控器 14 和 15 可以是可接收和执行第三方软件（如用户开发软件）的普通应用处理器或任何其它的不可信软件（其中，一般不了解软件的内容和功能）。由于软件不可信，因此它可以是错误的或敌对的软件，试图恶化安全总线主控器 12 或外围设备 22 和 24，把病毒引入到数据处理系统 10 中，或访问安全总线主控器 12、外围设备 22 和 24 或数据处理系统 10 内的安全信息。

总线受控器 26 可以是任何受控设备，如可由安全总线主控器 12

和不安全总线主控器 14 和 15 访问的存储器。外围设备 22 和 24 可以是任何类型的外围设备，如通用异步收发器（UART）、实时时钟（RTC）、键盘控制器等。外围电路 19 允许在外围总线 20 与外围寄存器 21 之间进行通信。相似地，外围电路 23 允许在外围总线 20 与外围寄存器 25 之间进行通信。在替代实施例中，外围设备 22 可以是存储器单元，其中，外围寄存器 21 将是存储地址单元。

在操作中，安全总线主控器 12、不安全总线主控器 14 和不安全总线主控器 15 请求访问系统总线 16，以请求对耦合到系统总线 16 的其它受控设备的访问，或请求通过总线接口 18 对外围设备 22 和 24 的访问。如以下所述，总线接口 18 确定是否允许请求特定的外围设备或特定的寄存器（或寄存器组）。如果不允许，总线接口 18 可通过系统总线 16 提供总线错误响应。然而，如果允许请求，总线接口 18 就提供任何需要的总线协议，以完成该请求。在一个实施例中，由于安全总线主控器 12 是广泛可信的处理器，因此它具有对外围设备 22 和 24 的无限制访问。然而，根据安全总线主控器 12 所建立，不安全总线主控器 14 和 15 每一个都只有对外围寄存器 21 和外围寄存器 25 的有限访问权。不安全总线主控器可要求访问外围资源的子集，以便有效地操作数据处理系统 10；然而，通过限制某些总线主控器对外围设备的访问，系统完整性和安全性可维持更高的程度。

图 2 示出根据本发明一个实施例的图 1 总线接口 18 的一部分。总线接口 18 包括控制电路 44 和访问控制寄存器 30。控制电路 44 通过系统总线 16 提供和接收地址 42、数据 40 和控制 38。控制电路 44 还通过系统总线 16 接收总线主控器标识符 36。控制电路 44 包括用于对寄存器 30 进行安全总线主控器读/写（R/W）访问的电路 46，其中，控制电路 44 双向耦合到访问控制寄存器 30。控制电路 44 还包括用于访问外围设备 22、24 的电路 48。电路 48 包括从访问控制寄存器 30 接收信息的总线主控器许可确定电路 50。控制电路 48 还包括双向耦合到外围总线 20 以便向和从外围设备 22 和 24 提供和接收合适信号的信号桥接电路 52。访问控制寄存器 30 包括访问控制寄存器 32 和访问

控制寄存器 34。在一个实施例中，访问控制寄存器 30 只包括单个寄存器，或可替换地，可包括任意数量的寄存器，这在以后结合图 3 和 4 进一步描述。

在操作中，总线接口 18 基于总线主控器标识符 36 而提供对访问控制寄存器 30 的访问。总线主控器标识符 36 向控制电路 44 识别哪个总线主控器正在提供当前请求。例如，在一个实施例中，数据处理系统 10 中的每个总线主控器可具有相应的标识 (ID) 号。例如，安全总线主控器 12 具有相应的 ID 号 0，不安全总线主控器 14 具有相应的 ID 号 1，并且不安全总线主控器 15 具有相应的 ID 号 2。从而，数据处理系统 10 内的任何总线主控器可被分配唯一的 ID 号。当特定的总线主控器请求对外围设备的访问时，它相应的 ID 号可提供给可作为总线主控器标识符 36 而提供给控制电路 44。在此实例中，如果总线主控器标识符 36 为 0，就代表安全总线主控器 12。在替代实施例中，任何类型的标识系统可用于区分安全总线主控器 (或多个安全总线主控器) 和不安全总线主控器，并且用于区分不同的总线主控器。

总线接口 18 通过电路 46 确保只有安全总线主控器才能获得对访问控制寄存器 30 的 R/W 访问。电路 46 比较输入的总线主控器标识符 36，以确定安全总线主控器 12 是否正在请求对访问控制寄存器 30 的 R/W 访问或者不安全总线主控器 (如，不安全总线主控器 14 或 15) 是否正在请求对访问控制寄存器 30 的 R/W 访问。从而，在前面图形所描述的实例中，电路 46 比较总线主控器标识符 36 是否为 0，以确定是否允许对访问控制寄存器 30 的 R/W 访问。如果安全总线主控器 12 请求对寄存器 30 的 R/W 访问，那么，安全总线主控器 12 就被授权访问，并且能自由地对访问控制寄存器 30 进行读或写。以此方式，安全总线主控器 12 能通过对访问控制寄存器 30 编程而设置授与每个不安全总线主控器的访问许可。在加电时、在重置时，响应软件应用的初始化，或者在任何其它适当的时候，安全总线主控器 12 可把所述值编程到访问控制寄存器 30 中。这允许对访问控制寄存器 30 的动态访问，从而，在需要时，它们可被更新。可替换地，尽管访问控制寄

寄存器 30 内的值可被编程一次（例如通过使用只写一次存储器），但只编程有限的次数，或可被硬接线。在讨论用于访问外围设备 22、24 的电路 48 之前，结合图 3 和 4 描述访问控制寄存器 30 的内容。

图 3 示出访问控制寄存器 30 内的访问控制寄存器的一个实施例。例如，图 3 示出访问控制寄存器 32，该寄存器具有不安全总线主控器 14 外围设备访问控制位 60 和不安全总线主控器 15 外围设备访问控制位 62。在此实例中，访问控制寄存器 30 只需要单个寄存器，如图 3 的访问控制寄存器 32，其中，为每个不安全总线主控器提供外围设备访问控制位（如控制位 60 和 62）。每组外围设备访问控制位可具有一个或多个为相应不安全总线主控器提供访问控制信息的位。在一个实施例中，每组外围设备访问控制位对每个外围设备具有一位，它表示是否允许相应的不安全总线主控器对相应的外围设备进行读/写访问。可替换地，每组外围设备访问控制位对每个外围设备具有两位，其中，一位表示是否允许相应的不安全总线主控器对相应的外围设备进行读访问，另一位表示是否允许相应的不安全总线主控器对相应的外围设备进行写访问。

在另一实施例中，每个外围设备内的外围寄存器可细分为子集（或部分），其中，每个子集可包括一个或多个外围寄存器，从而，根据所请求总线主控器和访问类型而允许或拒绝对寄存器的特定子集或部分的访问。结合图 4 可更好地理解此实施例。例如，图 4 示出不安全总线主控器 14 外围设备访问控制位 60 的一个实施例，在这，控制位 60 包括用于访问外围寄存器 21 的不同部分的读和写访问控制位。例如，外围寄存器 21 读访问控制位的第一部分 64 和外围寄存器 21 写访问控制位的第一部分 66 分别提供读和写访问控制信息，所述信息由安全总线主控器 12 授与给不安全总线主控器 14，以访问外围设备 22 内的外围寄存器 21 的第一部分。相似地，外围寄存器 21 读访问控制位的第二部分 68 和外围寄存器 21 写访问控制位的第二部分 70 分别提供读和写访问控制信息，所述信息由安全总线主控器 12 授与给不安全总线主控器 14，以访问外围设备 22 内的外围寄存器 21 的第二部分。

从而，只授权对外围寄存器一部分的访问。而且，外围寄存器 21 的第一部分和第二部分可以是寄存器 21 的重叠部分，或者可以是寄存器 21 的完全不同的部分。进而，不需要对寄存器 21 每个部分的独立的读和写访问控制，从而，对寄存器 21 的特定部分允许或不允许进行读和写访问。

如果需要，不安全总线主控器 14 外围设备访问控制位 60 包括任意数量的控制位。例如，除了控制位 64、66、68 和 70 以外，还可包括用于确定对外围寄存器 25(或其部分)的读和写访问许可的控制位，作为控制位 60 的一部分。也就是说，控制位 60 包括用于确定不安全总线主控器 14 对外围总线 20 上外围设备的读和写访问许可所需的控制位。如上所述，这些许可由安全总线主控器 12 完全控制，在这，只有安全总线主控器 12 可改变它们的值。与不安全总线主控器 15 相应的控制位 62 与图 4 中为不安全总线主控器 14 所定义的控制位相似。也就是说，控制位 62 可包括用于确定不安全总线主控器 15 对外围总线 20 上外围设备的读和写访问许可所需的控制位。而且，图 3 的访问控制寄存器 32 可包括用于安全总线主控器 12 的外围设备访问控制位；然而，这一般不是必需的，因为安全总线主控器 12 一般具有对所有外围设备的完全访问。

访问控制寄存器 30 的替代实施例包括与每个不安全总线主控器相应的寄存器，所述寄存器确定每个不安全总线主控器对每个外围设备的访问许可。可替换地，访问控制寄存器 30 可包括与每个外围设备相应的寄存器，所述寄存器确定每个不安全总线主控器的访问许可。进而，在此实施例中，每个寄存器包括用于外围设备中寄存器的每个部分的不同位组以及用于每个不安全总线主控器的每个部分的相应许可。从而，可在总线接口 18 内或数据处理系统 10 内以各种方式定义并储存每个不安全总线主控器对每个外围设备的读和写访问许可（并且不局限于使用寄存器）。

返回到图 3，用于访问外围设备 22、24 的电路 48 包括总线主控器许可确定电路 50。电路 50 接收地址 42、控制 38 和总线主控器标识

符 36。从而，电路 50 接收所有必需信息，所述信息识别访问类型（读或写）、所请求的外围设备（和所请求的外围寄存器）、以及哪个总线主控器正在进行请求的标识。如上所述，使用储存在访问控制寄存器 30 中的信息，电路 50 确定当前请求不安全总线主控器是否具有必需的对特定外围寄存器或所请求寄存器的访问许可。例如，启动可由总线主控器要求访问外围设备的总线周期（此总线周期可以是读或写总线周期）。在总线周期的至少一部分中，提供总线主控器标识符 36。总线主控器标识符 36 用于从访问控制寄存器 30 选择用于总线周期的访问控制信息（与所请求总线主控器相对应）。接着，可确定访问控制信息是否允许所请求总线主控器访问所请求外围设备。

如果允许访问（意味着所请求不安全总线主控器具有对特定外围寄存器或所请求寄存器的适当访问许可），操作就继续进行（即总线周期继续），并且提供必需的总线协议，以完成操作。例如，信号桥接电路 52 向从控制 38、数据 40 和地址 42 得到的被访问外围设备提供任何适当的数据、地址和控制信号。相似地，信号桥接电路 52 通过控制 38、数据 40 和地址 42 向系统总线 16 返回任何必需的控制、数据和地址信息。

然而，如果不允许访问（意味着所请求不安全总线主控器没有对特定外围寄存器或所请求寄存器的适当访问许可），就在访问外围设备之前终止总线周期。而且，通过系统总线 16 提供表示拒绝所请求不安全总线主控器访问外围设备的信号。例如，通过系统总线 16 向所请求不安全总线主控器提供总线错误。总线错误可通过总线主控器许可确定电路 50 提供，作为控制信号 38 中之一。作为响应，不安全总线主控器可执行适当的例外处理，以从总线错误恢复。可替换地，如果不允许访问，可执行全部或部分数据处理系统 10 的重置。

如以上所讨论地，如果需要，安全总线主控器 12 可动态地改变访问控制寄存器 30 中的许可。在一个实施例中，安全总线主控器 12 可响应软件应用的初始化而改变许可。例如，不安全总线主控器 14 可警告安全总线主控器 12：它正准备开始软件应用。作为响应，安全

总线主控器 12 可更新访问控制寄存器 30，以向不安全总线主控器 14 提供对所需外围寄存器的访问，以便完成它的应用。在完成此应用时，安全总线主控器 12 可撤销先前授与的许可，从而，只是基于逐个应用地授与许可。

在替代实施例中，外围设备 22 或 24 可以是存储器单元，其中，外围寄存器 21 或 25 是存储单元。在此实施例中，访问控制寄存器 30 限定每个不安全总线主控器对特定存储单元或部分存储器单元的访问许可。

还指出，在替代实施例中，与每个外围设备相应的访问控制寄存器（即，许可信息）可位于外围设备内，而不是位于总线接口 18 内。进而，总线主控器许可确定电路也可位于外围设备内，从而，在允许访问外围设备的寄存器之前，通过外围设备而确定许可。从而，替代实施例可在数据处理系统 10 的存储器映象内的任何地方储存可由安全总线主控器 12 访问的许可信息。而且，数据处理系统 10 可包括任意数量的能更新许可信息的安全总线主控器，并且不局限于单个安全总线主控器。

现在可理解，数据处理系统 10 如何能为外围接口单元（如总线接口 18）提供柔性保护机构，以确保实现系统的安全性要求。本发明的实施例允许在外围接口单元内（例如在访问控制寄存器 30 内）动态更新许可。从而，安全总线主控器 12 能建立哪些不安全总线主控器具有对哪些外围寄存器的访问许可，从而保护数据处理系统 10 不因在不安全总线主控器上运行的错误或敌对软件而引起恶化。通过使用总线主控器标识符，基于安全总线主控器 12 建立的许可而允许或拒绝对所请求外围寄存器的访问。

应指出，尽管图 1 和 2 示出使用双向导线，但应该理解，可替代使用单向导线的组合。可替换地，可使用双向和单向导线的组合。信号可通过单根导线串行传输或通过多根导线并行传输。可替换地，信号可以在单根或多根导线上时间多路复用。

在前面的说明中，本发明已经结合特定实施例进行描述。然而，

本领域中技术人员明白：只要不偏离以下权利要求所提出的本发明范围，就可作出各种变更和变化。例如，应该理解，数据处理系统 10 可以是任何类型的可位于单个芯片或集成电路（IC）或芯片或 IC 组合上的数据处理系统。数据处理系统 10 也可应用到位于具有共享外围设备的网络（通过网络系统总线耦合）上的各种主控器和受控器。相应地，以上说明和附图是示例性的，而不是限制意义的，并且所有这些变更包括在本发明的范围内。

以上已经结合特定实施例描述好处、其它优点和对问题的解决方案。然而，好处、优点、对问题的解决方案、以及可导致任何好处、优点、或发生或变得更明显的解决方案的任何元件并不将被解释为任何或全部权利要求的关键性的、必需的、或基本的特征或元件。如在此所使用的，术语“包括”、“包含”或任何其它变化，都用于涵盖非排它性的包含物，从而，包括元件列表的过程、方法、物品或装置不仅包括这些元件，而且包括其它未明显列举的或这些过程、方法、物品或装置所固有的其它元件。

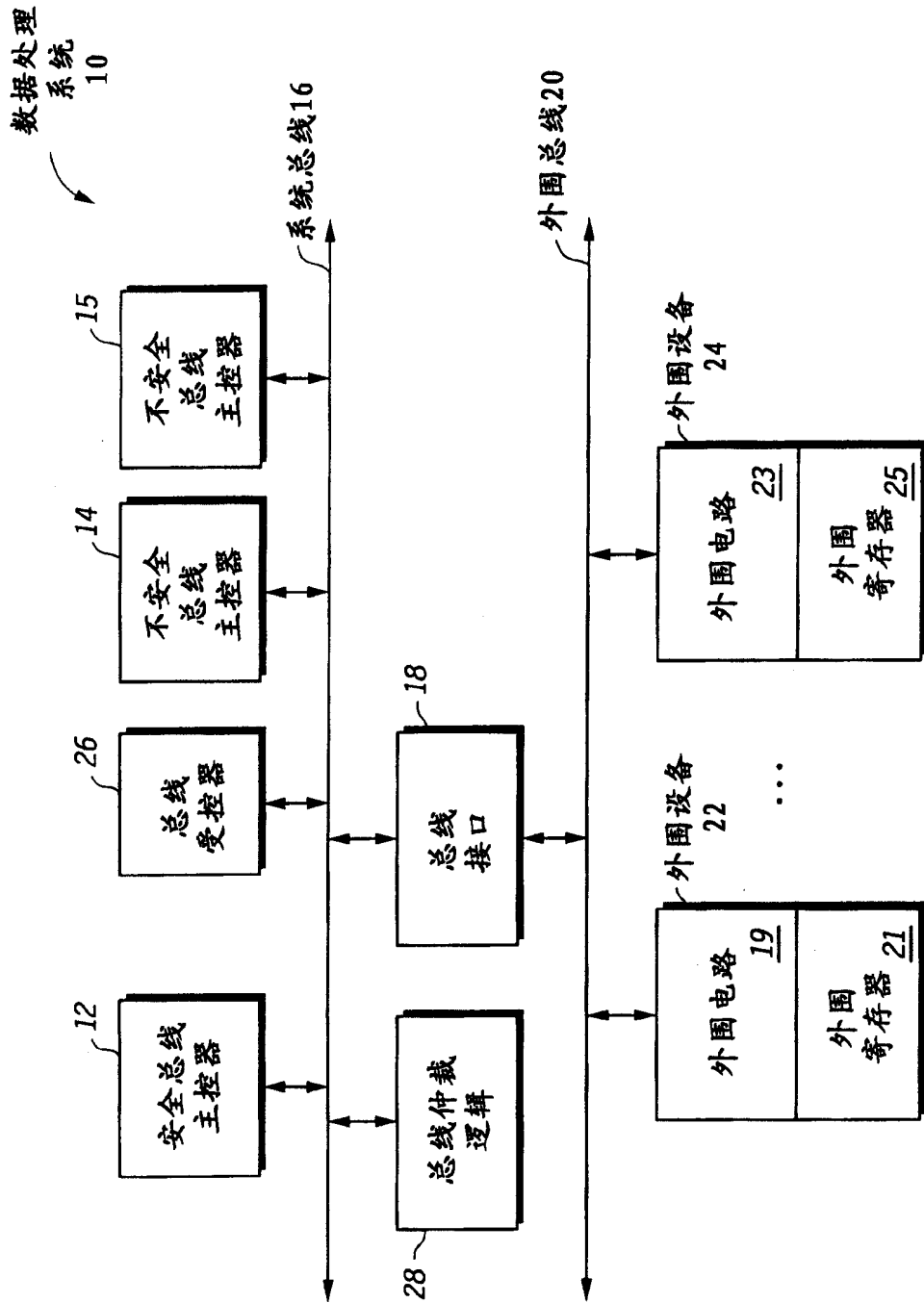


图1

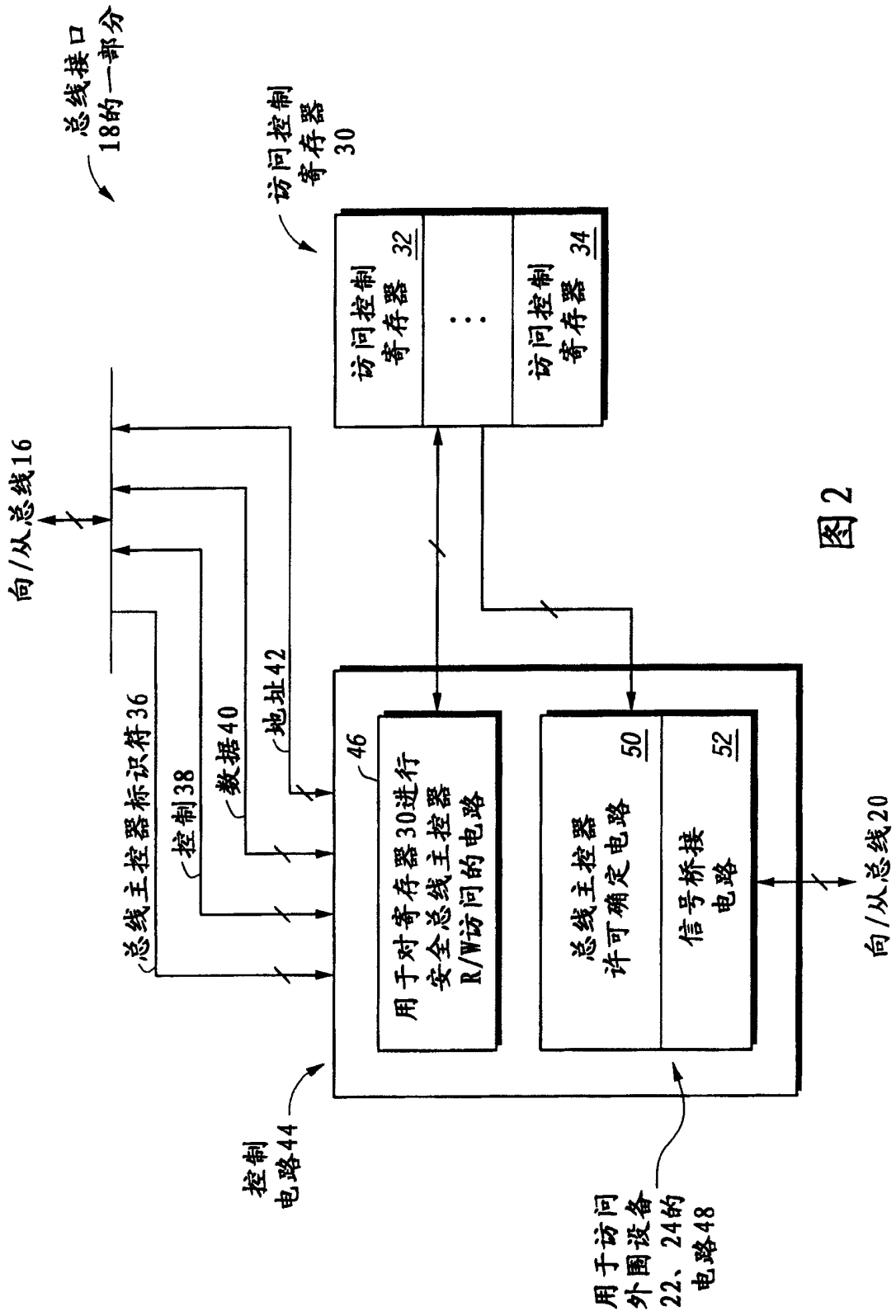


图 2

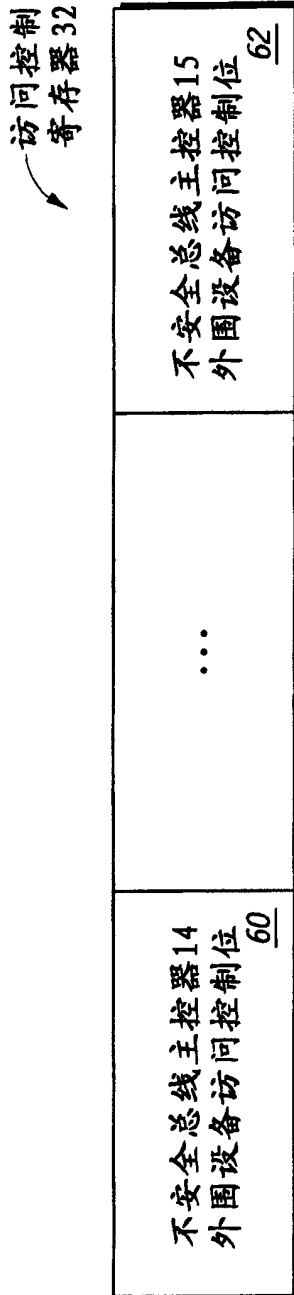


图3

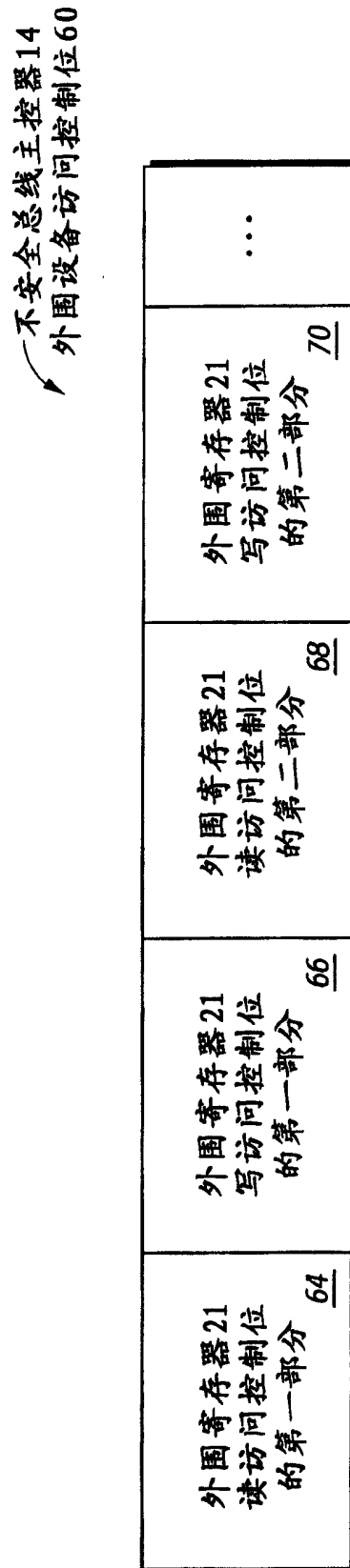


图4