[19] 中华人民共和国国家知识产权局

[51] Int. Cl.
G06F 12/14 (2006.01)

[12] 发明专利申请公开说明书

[21] 申请号 03826547.8

[43] 公开日 2006 年 5 月 10 日

[11] 公开号 CN 1771482A

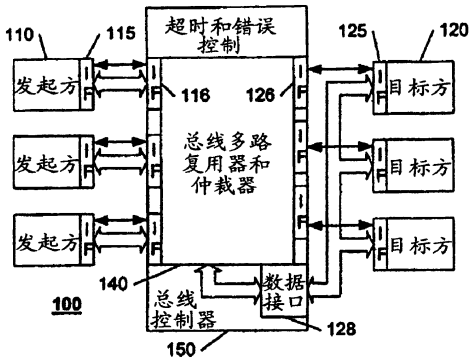
[22] 申请日 2003.5.27 [21] 申请号 03826547.8
[86] 国际申请 PCT/IB2003/002359 2003.5.27
[87] 国际公布 WO2004/107181 英 2004.12.9
[85] 进入国家阶段日期 2005.11.28
[71] 申请人 皇家飞利浦电子股份有限公司
地址 荷兰艾恩德霍芬
[72] 发明人 T·A·庞修斯 R·H·延森
T·拉贝莱尔
[74] 专利代理机构 中国专利代理(香港)有限公司
代理人 李亚非 王 勇
权利要求书 3 页 说明书 8 页 附图 1 页

[54] 发明名称

访问保护的总线系统

[57] 摘要

访问控制设备阻止未授权的发起方－目标方对之间在总线上的数据传送。 对许可矩阵进行维护以对每个相对于每个目标方的发起方的访问许可进行识别。 访问设备对总线进行监视并且确定发起方和所期望的目标方的标识。 如果发起方具有对目标方合适的访问权限，则允许进行总线通信，否则阻塞该通信并发布出错信号。 为了进一步提供安全性，对于访问控制设备而言是本地的发起方的标识符经由到每个发起方的直接有线连接被传送至访问控制设备。



1、一种总线系统(100,300)，包含:

促进信号在多个设备间传送的总线，

访问控制矩阵(160)，对所述多个设备中的一个或多个发起方(110)与一个或多个目标方(120)之间的访问权限进行识别，以及

访问控制器(140,310)，可操作地耦合至所述总线和所述访问控制矩阵(160)，它被配置为:

-对所述总线上从所述一个或多个发起方(110)中的选定发起方至所述一个或多个目标方(120)中的选定目标方的数据传送请求进行监视；以及

-根据所述选定发起方与所述选定目标方之间的访问权限，选择性地阻止在所述选定发起方与所述选定目标方之间的数据传送。

2、如权利要求1所述的总线系统(100,300)，其中，所述访问控制器(140,310)可操作地串联耦合在所述一个或多个发起方(110)与所述一个或多个目标方(120)之间。

3、如权利要求2所述的总线系统(100)，其中:

所述一个或多个发起方(110)中的每一个经由所述访问控制器(140)的多个输入端口中的一个输入端口被独立地耦合至所述访问控制器(140)；并且

所述访问控制矩阵(160)根据对应于所述一个或多个发起方(110)中每一个的输入端口，对所述一个或多个发起方(110)与所述一个或多个目标方(120)之间的所述访问权限进行识别。

4、如权利要求1所述的总线系统(100,300)，其中，所述访问控制器(140,310)向所述一个或多个目标方(120)中的每一个提供使能信号，并且经由对与所述选定目标方相关联的所述使能信号的控制，选择性地阻止在所述选定发起方与所述选定目标方之间的所述数据传送。

5、如权利要求1所述的总线系统(300)，其中，所述访问控制器(310)可操作地与所述一个或多个发起方(110)和所述一个或多个目标方(120)并联耦合。

6、如权利要求5所述的总线系统(300)，其中，所述访问控制器(310)通过在所述总线上发布信号状态来选择性地阻止所述选定发起

方与选定目标方之间的所述数据传送，所述信号状态阻止所述选定发起方改变所述总线上的信号状态。

7、如权利要求 1 所述的总线系统(100, 300)，其中，所述访问控制矩阵(160)被配置为，根据发起方分类和目标方分类中的至少一个对所述一个或多个发起方(110)与所述一个或多个目标方(120)之间的所述访问权限进行识别。

8、一种电子系统(100, 300)，包含:

多个设备(110, 120)，被配置为在相互之间传送信号;

访问控制矩阵(160)，对所述多个设备(110, 120)中的设备对之间的访问权限进行识别；以及

访问控制器(140, 310)，可操作地耦合至所述多个设备(110, 120)和所述访问控制矩阵(160)，它被配置为:

- 从所述多个设备(110, 120)中的第一设备接收数据传送请求，该数据传送请求用于实施与所述多个设备(110, 120)中的第二设备的数据传送；以及

- 根据对应于所述第一设备和所述第二设备的所述设备对(110, 120)之间的所述访问权限，选择性地阻止所述第一设备与所述第二设备之间的所述数据传送。

9、如权利要求 8 所述的电子系统(100)，其中，所述访问控制器(140)可操作地串联耦合在所述第一设备与所述第二设备之间。

10、如权利要求 9 所述的电子系统(100)，其中:

所述第一设备经由所述访问控制器(140)的多个输入端口的一个输入端口被耦合至所述访问控制器(140)；并且

所述访问控制矩阵(160)根据对应于所述第一设备的所述输入端口对所述第一设备与所述第二设备之间的所述访问权限进行识别。

11、如权利要求 8 所述的电子系统(100, 300)，其中，所述访问控制器(140, 310)经由对与所述第二设备相关联的使能信号的控制，来阻止所述第一设备与所述第二设备之间的所述数据传送。

12、如权利要求 8 所述的电子系统(300)，其中，所述访问控制器(310)经由被用来在所述第一设备与所述第二设备之间传送所述信号的总线可操作地与所述第一设备和所述第二设备并联耦合。

13、如权利要求 12 所述的电子系统(100, 300)，其中，所述访问

控制器(140,310)通过在所述总线上发布信号状态来选择性地阻止所述第一设备与所述第二设备之间的所述数据传送，所述信号状态阻止所述第一设备改变所述总线上的所述信号状态。

14、如权利要求8所述的电子系统(100,300)，其中，所述访问控制矩阵(160)被配置为，根据所述多个设备(110,120)中一个或多个设备的分类对所述设备对(110,120)之间的所述访问权限进行识别。

15、如权利要求8所述的电子系统(100,300)，其中，所述多个设备(110,120)包括下列至少一种：视频处理设备、用户识别设备、安全设备、存储器设备和处理设备。

16、一种控制访问多个目标方(120)的方法，包括：

确定试图访问所述多个目标方中的选定目标方(120)的发起方(110)的标识，

根据所述发起方(110)的标识确定所述发起方(110)与所述选定目标方(120)之间的预先定义的访问权限，以及

根据所述发起方(110)与所述选定目标方(120)之间的所述预先定义的访问权限，选择性地阻止对所述选定目标方(120)的访问。

17、如权利要求16所述的方法，其中，选择性地阻止对所述选定目标方(120)的访问包括对所述选定目标方(120)的使能信号进行控制。

18、如权利要求16所述的方法，其中，选择性地阻止对所述选定目标方(120)的访问包括在总线上发布一个信号状态，该信号状态阻止所述发起方(110)改变所述总线上的信号状态。

19、如权利要求16所述的方法，其中，根据下列中的至少一种分类来确定所述发起方(110)与所述选定目标方(120)之间的所述预先定义的访问权限：与所述发起方(110)相关联的分类和与所述选定目标方(120)相关联的分类。

访问保护的总线系统

本发明涉及电子系统领域，特别是涉及一种选择性控制对电子系统内的设备进行的访问的架构。

电子系统通常采用总线结构在系统内的部件之间传送数据。正如此处所用，总线是用于提供往返于连接至总线的设备之间的路径的信号的集合，并且该总线包括串行总线、并行总线及其组合。正如本技术领域内所知的那样，利用公共总线结构常常允许更加有效地利用设计和研发资源。经总线通信的功能块可以独立地设计，只需遵循为总线而设定的协议即可，而不是去遵循系统内的每个其它功能块形形色色的要求。因为这些独立设计的功能块可适用于其它系统配置和应用，从而可将这种可复用块的研发成本分摊到更多的产品上，所以获得进一步的效率。不管是集成电路内的局部总线，印刷电路“母板”上的总线，部件架(component rack)的背板上的总线，还是串级链(daisy-chained)的部件串中的串行总线等，都实现了总线架构和模块化设计的优点。

在总线环境下，数据传送操作的发起方一般在总线上发布(assert)数据传送指令。该指令标识出其寻址的目标设备。每个部件对总线进行监视以确定其是否为目标设备；如果特定部件是目标设备，则对数据传送指令作出响应，否则保持沉寂状态。例如，中央处理单元(CPU)可对系统总线发布读取命令，指定包含了其欲读取数据的特定的目标存储器地址。该目标存储器地址的子集通常对应于其地址范围包含该目标存储器地址的特定的 ROM 或 RAM 部件，因此发出将该特定 ROM 或 RAM 部件作为目标设备的信号。作为目标方的 ROM 或 RAM 部件响应该读取请求，其方式为在总线上发布目标存储器地址处的数据值。在更为复杂的数据传送操作中，在实际的数据传送发生之前，数据传送指令可以在发起方与目标方之间发起对话。

在许多系统和应用中，对于部分或所有的数据传送施加有限制。例如在媒体处理系统内，用户标识设备是唯一允许访问视频控制器的许可(permission)寄存器的设备。在该实例中，视频控制器被配置为

根据许可寄存器的状态允许或拒绝对选择内容材料的访问。在传统的处理系统中，这种访问控制的提供方式为通过识别数据传送指令中、或者在随后的传送前的对话中的发起方，并且将目标设备安排为对选择发起方标识的访问进行限制。根据所需的安全程度，访问控制可包括密码识别的使用。例如，当上述实例的媒体处理系统第一次被配置时，用户识别设备和视频控制器可启动传统的安全密钥交换过程，并且随后利用该安全交换后的密钥验证数据传送发起方的身份。在其它安全性无关紧要的环境中，访问控制可以仅仅是基于惯例得到认可的，或者在设计文档中得到预防性警告。例如考虑 DVD 播放机内的媒体处理系统，该 DVD 播放机提供了基于用户身份识别的家长控制(parental control)。在这种系统中，与黑客攻击有线或卫星转换器的访问控制以获取不受限的免费电影的可能性相比，黑客攻击 DVD 播放机的访问控制以破坏家长控制的可能性微乎其微。在该实例中，DVD 播放机在设计时可以仅假设或认为只有用户识别设备被配置为对许可寄存器进行访问。

但是这种访问控制技术容易被黑客和病毒攻破，或者如果有，根据所提供的安全级别，容易因偶尔的编程错误造成不适当的访问。通常情况下，访问控制系统通过伪造发起方的身份被破坏，由此获取本不打算向伪造身份的发起方开放的访问权限。如上所述，通过纳入复杂的加密验证技术可以避免这样的破坏，但是这种防护措施的成本通常基本上超出其所获得的收益。

本发明的目标是提供访问控制方法、设备和架构，其可靠地执行给予电子系统内的部件的访问权限。本发明的进一步目标是提供一种访问控制架构，其无需每个目标设备中执行访问控制。本发明的进一步目标是提供无需使用加密技术的安全的访问控制。本发明的进一步目标是在电子系统内提供可编程的访问控制。

通过提供一种阻止成对的未授权发起方－目标方之间在总线上传送数据的访问控制设备，这些和其它目标得以实现。对许可矩阵进行维护，该矩阵标识出每个发起方相对于每个目标方的访问许可。访问设备监视总线并确定发起方和欲访问的目标方的身份。如果发起方具有对目标方合适的访问权限，则该总线通信是允许进行的，否则通信

被阻止，并且发布出错信号。为了进一步提供安全性，属于访问控制设备本地的发起方的标识符经由与每个发起方的直接有线连接被传送至访问控制设备。

以下参照附图并借助实例对本发明进行详细描述，其中：

图 1 示出了按照本发明的具有访问控制的总线系统的实例方框图。

图 2 示出了按照本发明的实例访问控制矩阵。

图 3 示出了按照本发明的可替换的具有访问控制的总线系统的实例方框图。

在所有附图中，相同的参考标记指示相似或相应的特征或功能。

图 1 示出了按照本发明的具有访问控制的总线系统 100 的实例方框图。系统 100 包括多个经公共总线结构互相通信的功能性部件。为便于理解，使用总线事务的发起方 110 和与发起方 110 通信的目标方 120 的范例(paradigm)来给出本发明。功能部件可以是发起方 110 或目标方 120，或者同时是发起方 110 和目标方 120。存储器部件例如一般仅仅是目标方 120，因为存储器部件一般不会发起数据传送。同样地，存储器空间的不同区域可分别构成目标方 120。另一方面，单处理器系统中的 CPU 一般为发起方 110，因为它一般决定进行何种通信。但是如果 CPU 允许经过总线结构中断，则它将是中断发起方的目标方 120。需要注意的是，利用这种范例，作为发起方 110 和目标方 120 的角色与所期望的数据传送方向(读取/写入、发送/接收)无关。

为便于理解，本发明使用集中式的总线控制器 150 进行描述，该集中式的总线控制器 150 对总线的活动进行管理，该活动包括总线的多路复用和访问控制、超时和错误控制等等。对于本领域内普通技术人员显而易见并且下面将参照图 3 进一步讨论的是，本发明的原理可应用于具有分布式总线控制的总线结构，其中，例如通过每个部件协同配合以使总线竞争最少来实现仲裁和多路复用功能。

总线架构同时包括“广播”总线和“定向(directed)”总线。在广播总线中，多个部件共同直接连接至总线，以致出现在总线上的数据可以为每个部件获得。在定向总线中，到总线的接口经由多路复用

器，该多路复用器选择在给定时间点哪些设备被连接至总线。图 1 的实例系统 100 示出总线结构，该总线结构包括与发起方 110 进行通信的定向总线和与目标方 120 进行总线通信的广播总线，以说明本发明的原理可应用于定向总线、广播总线或者它们的组合。

系统 100 的部件 110、120 中的每一个都包括分别用于经由总线进行通信的接口适配器 115、125。经由总线的通信包括用宽箭头符号表示的数据和用单线宽度（single width）箭头符号表示的控制信号。在发起方 110 所使用的定向总线结构中，每个接口适配器 115 在总线控制器 150 处具有相应的接口模块 116。数据和控制信号都在接口 115、116 之间传送。在目标方 120 所使用的广播总线结构中，每个接口适配器 125 具有相应的控制接口模块 126 用于控制信号，但是数据接口模块 128 为与所有的目标方 120 进行的数据通信提供了公共接口。

共同未决的美国专利申请“CONFIGURABLE SYNCHRONOUS OR ASYNCHRONOUS BUS INTERFACE(可配置的同步或异步总线接口)”(Pontius 等人于 2002 年 1 月 17 日提交，序列号为 10/052,276)公开了一种总线控制结构，其允许在每个发起方 110 或目标方 120 与总线控制器 150 之间进行同步和异步通信，从而在发起方 110 与目标方 120 之间允许同步和异步通信，该专利申请作为参考文献被纳入本文。

按照本发明，总线控制器 150 包括发起方 110 与目标方 120 中的访问权限的标识。为了方便和便于理解，这里利用访问控制矩阵 160 的范例来表示访问权限的标识，该访问控制矩阵 160 被用来控制每个发起方 110 与每个目标方 120 之间的数据的传送。本领域的普通技术人员将会认识到，表示访问权限的替换形式也是可以采用的，例如列表、规则等等，但是不管访问控制信息的形式或格式如何，每种表示方式在功能上都对应于将每个发起方访问每个目标方的权限进行映射的矩阵。例如，为了减少存储的需求，可以将访问控制信息存储为仅列出禁止访问的列表，这意味着每个未被包含在该列表内的发起方－目标方对都是许可的访问。正如这里所用，术语矩阵对应于可被映射为传统的矩阵形式的任何形式的数据表示。

图 2 示出了按照本发明的实例访问控制矩阵 160。该示例性矩阵 160 中用 A、B 和 C 标记的行对应于发起方，即分别对应于图 1 中的发

起方 A、发起方 B 和发起方 C。用 1、2 和 3 标记的列对应于目标方，即分别对应于图 1 的目标方 1、目标方 2 和目标方 3。在该示例性矩阵 160 中，“a”表示被授予全部访问权限，“r”表示被授予只读权限，“w”表示被授予“只写”权限，以及“-”表示未授予访问权限。在一个更为简单的实施例中，访问权限可以只包括二元的“是”或“否”而不管数据传送的方向如何；或者所有发起方具有对所有设备的读取权限，并且访问权限仅对选择目标方进行数据写入作出限制。对于本领域内普通技术人员来说，在考虑到公开的内容之后，作出这些替换和其它替换将是显而易见的。例如，在更为复杂的一个实施例中，访问控制矩阵可包含性能指示以及权限，诸如可实现块数据传送的发起方－目标方对等等。

按照本发明的另一方面，访问控制矩阵 160 优选是可编程的，从而允许在将发起方 110 或目标方 120 加入或从系统 100 移除时创建和修改访问权限。为了对访问控制矩阵 160 的访问进行控制，访问控制矩阵包括以“0”标记的列，在该实例中该列对应于总线控制器 150，特别是对应于访问控制矩阵 160。

如在图 2 的示例性矩阵 160 中所示，发起方 B 是被允许访问目标方 3 的唯一设备，并且如在行 B 与列 3 的交汇处以“w”表示的那样，这种访问局限于将数据写入目标方 3。如在上面“背景技术”部分所述，发起方 B 例如可对应于示例性的用户识别设备，而目标方 3 可对应于示例性视频控制器的许可寄存器。

如上所述，图 1 的总线控制器 150 被配置来接收来自每个发起方 110 的数据传送请求，并且根据访问控制矩阵 160 所指示的访问权限，选择性地使能该数据传送请求的目标方 120。使用图 2 的示例性矩阵 160，如果发起方 A 或发起方 C 向目标方 3 提交数据传送请求，则总线控制器 150 根据访问控制矩阵 160 的列“3”中的条目内容“-”（无权限），将拒绝该请求，并且将不会使得目标方 3 能够实行所请求的传送。同样地，如果发起方 B 请求从目标方 3 向发起方 B 进行数据传送（即“读取”请求），则控制器 150 将拒绝该请求。另一方面，如果发起方 B 请求从发起方 B 向目标方 3 进行数据传送（即“写入”请求），则控制器 150 根据访问控制矩阵 160 中的条目内容“w”（只写），将使得目标方 3 能够接收数据。

同样地，根据图 2 的示例性访问控制矩阵 160，图 1 的总线控制器 150 将对应于在“0”列的第一行的条目内容为“a”(所有权限)允许发起方 A 对访问控制矩阵 160 进行读取或写入，但是根据“0”列的每个其它行的条目内容“-”(无权限)，将阻止每个其它发起方 110 对访问控制矩阵 160 进行访问。如此，只有发起方 A 被允许修改发起方 110 与目标方 120 之间的访问权限。

值得指出的是，通过在总线控制器 150 处维护和执行访问权限信息，免除了每个目标方 120 维护和执行访问权限的责任。还需指出的是，在图 1 的示例性实施例中，每个发起方都被分配总线控制器 150 的特定输入端口或接口 116。如果总线控制器 150 和访问控制矩阵 160 被配置为相对于输入端口来定义访问权限，则只能通过物理修改系统来假冒发起方的身份，诸如撤销授权的发起方 110 并在通向总线控制器的输入端口处用假冒的发起方替换。如果发起方 110 与总线控制器 150 之间的连接为“硬连线的”(hard-wired)、诸如部件至集成电路内的总线或印刷电路板上的总线的连接，则控制器 150 所提供的安全性相当重要。由于与修改集成电路的内部电路相关的复杂性，集成电路内的总线所提供的安全级别明显高于印刷电路板上的总线的。如果发起方 110 与总线控制器 150 之间的连接是经由插头和插座组合方式，则替换更为容易，但是仍然需要获得物理接入总线控制器 150。这样，本发明所提供的安全性实际上是不会被远程黑客或远程病毒攻破的。

图 3 示出了按照本发明的可替换的具有访问控制的总线系统 300 的实例方框图。在这个实例中，每个设备 300 在总线上互相并联。虽然未涉及数据传送，但是每个设备 320 在总线上还是保持“不活动(inactive)”状态。当设备 320 希望发起数据传送时，该设备 320 在总线上发布“激活”状态。激活和不活动状态被如此定义，以便激活状态比不活动状态占优(override)。例如逻辑高电的不活动状态是普通的，其中每个设备 320 经相对高的阻抗将总线耦合至逻辑高值。为了发布激活状态，设备 320 将总线经非常低的阻抗耦合至逻辑低值。因为耦合到逻辑低值经由非常低的阻抗而耦合至逻辑高值经由一条或多条高阻抗路径，所以总线被驱动至逻辑低值。因为如果到总线的任何输入是逻辑低值，则总线状态将是逻辑低值而不管其它到总线的输

入取值如何，由此模拟与门的功能，所以这种配置通常称为线与(Wired-AND)总线配置。线或(Wired-OR)总线配置也是常用的，其中如果到总线的任何输入是逻辑高值，则将迫使总线为逻辑高值，而不管其它到总线的输入，由此模拟或门的功能。

在本实施例中，访问控制器 310 被耦合至总线以监视来自每个设备 320、即设备 1、设备 2……设备 N 的数据传送请求。因为总线的配置是如此，以致每个设备 320 与每个其它的设备 320 并联，所以在该总线结构中发起方与目标方之间没有明确的区分。数据传送请求包括发起设备和期望的目标设备的显性(explicit)标识。另外的选择是可采用混合实施例，其中每个发起设备包含直接通过连线连接至访问控制器 310 的识别信号，用来对总线上的每次事务中的发起方进行识别，从而规定了本发明的上述物理安全特征。

访问控制器 310 根据访问权限的识别确定传送是否得到授权。在这个示例性实施例中，上述的访问控制矩阵 160 以矩阵的形式提供了预先定义的访问权限，其中行和列都与设备而非特定的发起方和目标方相关联。

如果传送未获授权，则访问控制器 310 在总线上发布一个或多个激活信号以防止数据传送。例如，如果总线协议要求传送设备 320 提供时钟信号来实现传送，则控制器 310 仅仅在时钟线上发布连续的激活状态，由此阻止了任何其它设备 320 触发该线。可替换地，控制器 310 可以仅仅在数据线上发布连续的激活状态，从而阻止任何其它设备 320 发布与不活动状态相对应的数据值。在优选的实施例中，总线协议包括“复位”状态，其对应于以延长的持续时间发布连续激活状态。按照该协议，当有任何设备 320 检测到该复位状态时，设备 320 必须终止任何数据传送并释放该总线。可选地，总线控制器 310 可以被配置为在其完成传送阻塞操作后向未授权的发起方发出出错信息，以避免该发起方继续试图进行未授权传送而被纠缠该总线。

上述描述仅仅阐释了本发明的原理。将会意识到是，本领域的技术人员将能够设计出各种装置，虽然这些装置在这里没有直截了当地进行描述或在此示出，但是体现了本发明的原理，并且因此在本发明的精神和范围内。例如并非所有的发起方和/或目标方和/或设备 320 都需要明确地被包含在访问控制矩阵 160 中。访问控制矩阵 160 可被

配置为仅仅包含远程发起方或设备，和/或访问控制矩阵160可被配置为仅包含敏感的目标方。类似地，每个发起方和/或目标方例如可以根据其地址的子集被识别为属于特定类，并且访问控制矩阵160可根据发起方的类别和/或目标方的类别识别访问权限。同样，就象一个设备可同时对应于发起方和目标方那样，一个设备也可对应于多个发起方和/或多个目标方。即，基于特定的用户、该用户正在使用的特定的应用、该设备内的特定子系统等等，设备可能具有不同的访问许可。这种替换的访问许可可通过在访问控制矩阵内实现多个条目来实现，从而在公共的物理设备内提供“虚拟设备”。例如，可以利用两组许可来编码发起方，一组代表处于“用户”模式时的发起方，而另一组代表处于“管理员”或“内核”模式时的发起方。对于本领域的普通技术人员来说，在考虑此处的公开内容之后，这些和其它系统配置和优化特征都是显而易见的，并且被包含在下列权利要求的范围之内。

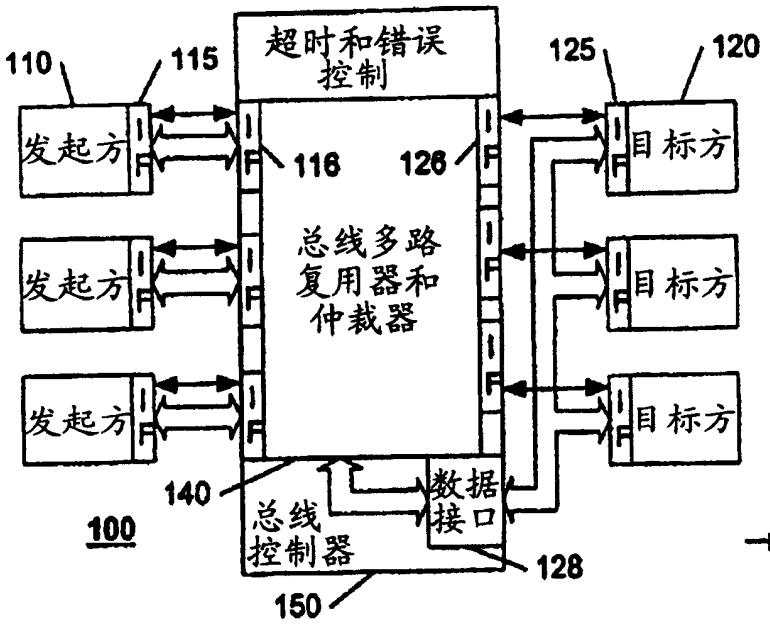

超时和错误控制
110
115
125
120
发起方
目标方
116
126
总线多路复用器和仲裁器
140
总线控制器
数据接口
128
150
100

图 1

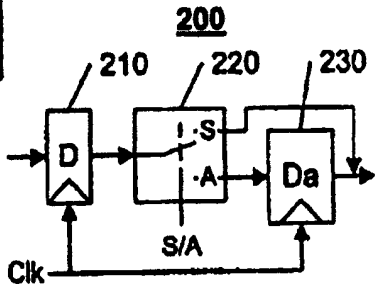

200
210
220
230
D
S
A
Da
S/A
Clk

图 2

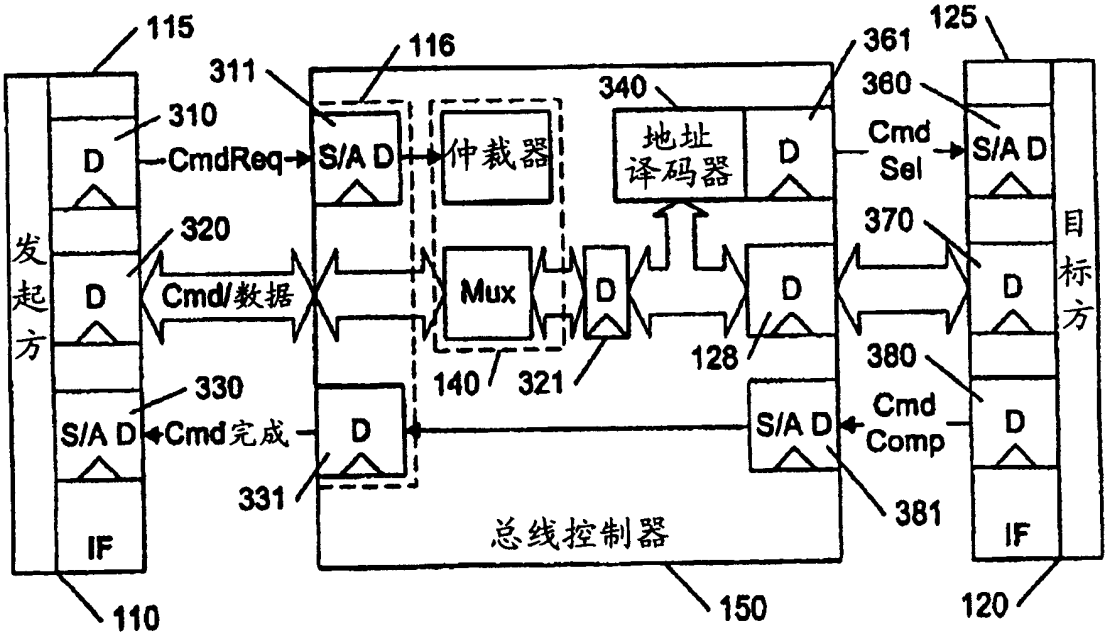

115
116
125
311
361
340
360
310
CmdReq
S/A D
仲裁器
地址译码器
D
Cmd Sel
320
370
Cmd/数据
Mux
发起方
目标方
128
380
330
Cmd完成
140
321
Cmd Comp
331
381
总线控制器
IF
110
150
120

图 3