[19] 中华人民共和国国家知识产权局

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

[12] 发明专利申请公布说明书

[21] 申请号 200780033989.4

[43] 公开日 2009 年 8 月 26 日

[11] 公开号 CN 101517549A

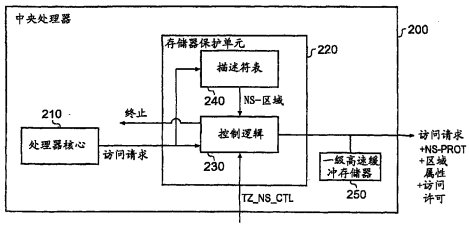
[22] 申请日 2007.8.8
[21] 申请号 200780033989.4
[30] 优先权
[32] 2006. 9.13 [33] GB [31] 0618042.6
[86] 国际申请 PCT/GB2007/003010 2007.8.8
[87] 国际公布 WO2008/032011 英 2008.3.20
[85] 进入国家阶段日期 2009.3.13
[71] 申请人 ARM 有限公司
地址 英国剑桥郡
[72] 发明人 D·柯萧 S·D·贝尔斯
[74] 专利代理机构 中国专利代理(香港)有限公司
代理人 王 岳 王丹昕
权利要求书 3 页 说明书 14 页 附图 5 页

[54] 发明名称

存储器访问安全管理

[57] 摘要

本发明提供一种用于产生访问请求的数据处理设备及方法。 所提供的总线主控器可依据自其外部接收的信号而在数据处理设备的安全域或非安全域中操作。 在总线主控器的正常操作期间把该信号生成为固定。 当总线主控器装置在安全域中操作时，所提供的控制逻辑依据默认存储器映射或安全定义的存储器区域描述符，可操作以产生与由总线主控器核心产生的访问请求相关联的域指定信号，该域指定信号指示是安全访问还是非安全访问。 因此，在安全域中操作的总线主控器可产生安全访问及非安全访问，而无须其本身能在安全及非安全操作间切换。



1. 一种具有多个域的数据处理设备，该数据处理设备的若干装置可操作在该多个域中，多述多个域包含至少一个非安全域及至少一个安全域，在该安全域中所述装置能够访问从非安全域中所不能访问的安全数据，该数据处理设备包含:

总线主控器装置，其固定在特定域中并且当需要访问数据时可操作以发布访问请求，该访问请求指定所述数据的地址;

总线，通过该总线所述访问请求被路由至从属装置，通过该总线所路由的每个访问请求具有与其相关联的域安全性信号，该域安全性信号识别关于该访问请求的域; 及

所述总线主控器装置具有域控制逻辑，其可操作以接收在该总线主控器装置外部产生的域指定信号，以识别该总线主控器装置固定在其中的域，若该域指定信号指示该总线主控器装置固定在该安全域中，则该域控制逻辑依据由所述访问请求指定的所述地址，可操作以选择性地产生待与所述访问请求相关联的非安全域安全性信号。

2. 如权利要求 1 中所述的数据处理设备，其中所述域控制逻辑能够访问存储器映射和该域安全性信号的指示，该存储器映射识别对于许多存储器区域的每个的访问控制信息，若指定该存储器区域中的地址的访问请求是由该总线主控器装置操作在该安全域中时发布的，则该域安全性信号的指示应该结合该访问请求来发布。

3. 如前述任一项权利要求中所述的数据处理设备，其中所述域控制逻辑能够访问区域描述符，每个区描述符与存储器区域相关联并且提供用于该存储器区域的区域安全性指示，所述区域描述符可由在该安全域中执行的预定软件编程，所述域控制逻辑可操作以从所述域指定信号及用于含有由该访问请求指定的地址的该存储器区域的该区域描述符的所述区域安全性指示的组合中导出用于每个访问请求的所述域安全性信号。

4. 如权利要求 3 中所述的数据处理设备，其中当所述域指定信号指示该总线主控器装置固定在该安全域时，该域控制逻辑依据所述区域安全性指示可操作地产生所述域安全性信号。

5. 如权利要求 3 或权利要求 4 中所述的数据处理设备，当其从属于权利要求 2 时，其中若所述地址是在具有区域描述符的存储器区域

中，则所述域安全性信号从所述区域安全性指示及所述域指定信号的所述组合中导出，否则所述域安全性信号从自所述存储器映射获得的所述访问控制信息中导出。

6. 如前述任一项权利要求中所述的数据处理设备，其中当所述域指定信号指示该总线主控器装置固定在该非安全域时，所述域控制逻辑可操作以使所述域安全性信号总产生为非安全。

7. 如前述任一项权利要求中所述的数据处理设备，其中所述域指定信号是输入到所述总线主控器装置的静态输入。

8. 如前述任一项权利要求中所述的数据处理设备，进一步包括安全性控制逻辑，其可操作以产生所述域指定信号。

9. 如前述任一项权利要求中所述的数据处理设备，其中所述域指定信号仅当所述总线主控器装置复位时才可改变。

10. 如权利要求 8 中所述的数据处理设备，其中所述总线主控器装置可在启动时开始操作在该安全域中，所述安全性控制逻辑可操作以稍后在启动过程中切换为产生非安全域指定信号，并且所述安全性控制逻辑此后可操作以仅产生非安全域指定信号直到出现重新启动。

11. 一种具有多个域的数据处理设备，该数据处理设备的若干装置可操作在该多个域中，所述多个域包含至少一个非安全域及至少一个安全域，在该安全域中所述装置能够访问从非安全域中所不能访问的安全数据，该数据处理设备包含：

总线主控器构件，其固定在特定域中并且当需要访问数据时用于发布访问请求，该访问请求指定所述数据的地址；

总线构件，通过该总线构件所述访问请求被路由到从属装置构件，通过该总线构件路由的每个访问请求具有与其相关联的域安全性信号，该域安全性信号识别关于该访问请求的域；和

所述总线主控器构件具有域控制逻辑构件，其用于接收在该总线主控器构件外部产生的域指定信号，以识别该总线主控器构件固定在其中的域，若该域指定信号指示该总线主控器构件固定在该安全域中，则该域控制逻辑构件依据由所述访问请求指定的所述地址，选择性地产生待与所述访问请求相关联的非安全域安全性信号。

12. 一种在具有多个域的数据处理设备中产生访问请求的方法，该数据处理设备的若干装置可操作在该多个域中，所述多个域包含至

少一个非安全域及至少一个安全域，在该安全域中所述装置能够访问从非安全域中所不能访问的安全数据，该方法包含以下步骤：

在总线主控器装置外部产生域指定信号，以识别该总线主控器装置固定在其中的域；

当需要访问数据时自所述总线主控器装置发布访问请求，所述访问请求指定所述数据的地址；

将域安全性信号与所述访问请求相关联，识别关于该访问请求的域；和

若所述域指定信号指示所述总线主控器装置固定在所述安全域中，则依据所述地址选择性地产生待与所述访问请求相关联的非安全域安全性信号。

存储器访问安全管理

技术领域

本发明涉及数据处理设备及方法，并且特别涉及对存储器中的安全与非安全数据的访问进行管理。

背景技术

通常情况下，由在处理器上运行的至少一个应用程序所使用的数据项(如指令或数据值)是敏感数据项，它们不应被可在处理器上运行的其它应用程序访问。其中的一个例子是数据处理设备是智能卡而应用程序之一使用敏感数据(如安全密钥)来执行检验、验证、解密等的安全应用程序。在这种状况下显然重要的是，确保那些敏感数据安全以致它们不会被其它应用程序－例如为试图访问那些安全数据而加载到该数据处理设备上的黑客应用程序－访问。

在已知系统中，操作系统开发人员的典型任务是确保该操作系统提供足够的安全性以确保一个应用程序的安全数据不能被在该操作系统控制下运行的其它应用程序访问。然而，随着系统变得更加复杂，通常的趋势是使操作系统变得更大更复杂，在这种状况下确保操作系统本身中足够的安全性就变得日益困难。

因此，为了试图减轻对操作系统安全性的依赖，已知的是提供一种在其中数据处理设备配有分离域的系统，这些域提供一种用于在硬件层次处理安全性的机制。例如在共同转让的共同待决的美国专利申请10/714,561号中描述了这种系统(其内容纳入此处作为参考)，该申请描述了一种具有安全域及非安全域的系统。在该系统中，非安全域及安全域实际上建立分离的世界，其中安全域提供通过硬件强制边界与其它执行空间分开的可信执行空间，而同样地非安全域提供不可信执行空间。在指定的非安全域中执行的程序不能访问被识别为安全的数据。每个访问请求则具有与其相关联的识别该访问是安全访问还是非安全访问的域安全性信号。

若该数据处理设备含有对于在安全或非安全域中执行的程序可访问的存储装置(如高速缓冲存储器)，则需要适当的机制以确保存储在这

种装置中以供在安全域中操作的程序访问的数据对于在非安全域中操作的程序是不可访问的。共同转让的美国专利申请10/714,481号(其内容纳入此处作为参考)中描述了一种数据处理设备，其中在高速缓冲存储器线中设定额外标志以指示对应数据的安全性。当高速缓冲存储器线的数据值被写入该高速缓冲存储器(典型作为线填充程序的一部分)时，相关标志被设定以识别该数据是属于安全存储器访问还是属于非安全存储器访问。对该高速缓冲存储器中的数据项的访问则是参考该标志限制的，这样其域安全性信号指示其是安全访问的访问请求仅能参考由相关(多个)标志所指示的安全高速缓冲存储器线，而类似地其域安全性信号指示其是非安全访问的访问请求仅能参考由相关(多个)标志所指示的非安全高速缓冲存储器线。因此，这种方法防止在非安全域中操作的程序访问高速缓冲存储器中其相关标志指示其含有安全数据的任何条目。这一设置避免了在访问该高速缓冲存储器的处理器从安全域操作转换到非安全域操作之前刷新该高速缓冲存储器的需要。

当这种系统用来保护安全数据的安全性时，事实上可能的情况是希望在安全域和非安全域之间共享一些数据。这种情况的一个实例是解密程序，其本身必须在安全域中操作，但产生对于非安全域程序可能是适合进行访问的解密数据。这种数据应被写入非安全存储器区域，从该区域中该数据可被非安全程序访问。

已知的是提供可在安全域及非安全域两者中操作的处理器(具有用于管理从一个域至另一个域的转换的特殊监控代码)。在一个这样的系统中，在安全域中操作的程序可向非安全存储器发布访问请求，并且把该数据访问请求标为非安全，即使该数据访问请求是从安全域中发布的。这使得安全程序能将数据写入非安全存储器栈，并且若该数据被保持在高速缓冲存储器中对于将相关高速缓冲存储器线的标志标为非安全，则可使得在该处理器(或事实在一不同处理器)上执行的后续非安全程序可以从该高速缓冲存储器中访问该数据。

然而，支持安全域及非安全域二者的处理器的复杂性不仅对于许多应用程序不必要而且可能出现潜在安全隐患，因为其在安全域或非安全域中执行程序的能力可能是黑客攻击的对象。再者，避免必须提供与处理器在安全域及非安全域二者中操作的能力相关的额外逻辑将是有利的。然而，固定在一个安全性域(即安全域)中的处理器将不具有

产生不同域安全性信号的能力，并且事实上一般不会知道该系统中的多个域。因此，若由该固定域处理器使用的数据要与另一个域中操作的另一个处理器共享时，则会产生问题。举例来说，假设固定的域处理器已在安全域中操作，所有自其发出的访问请求可自外部标记为安全访问。若数据要与非安全程序共享，则这种安全访问将需要被允许以访问非安全存储器区域。然而，即使这样的访问被允许，若使用高速缓冲存储器，仍会产生问题，因为存储在高速缓冲存储器中作为固定安全处理器的动作的结果的任何数据将会具有对应的标为安全的高速缓冲存储器线标志，因此对于非安全程序将是不可见的。这个问题的一个解决方案是使该处理器使用非安全存储器的不可高速缓存区域，该不可高速缓存区域将允许安全访问及非安全访问，然而该解决方案丧失了使用高速缓冲存储器的速度增益及省电益处。

因此，希望提供一种技术，其使得简化的处理器能在本身不具备在安全性域间转换的能力的情况下操作，同时仍保持在其中存在安全及非安全域和数据的数据处理设备内的灵活操作。

发明内容

从第一方面来看，本发明提供一种具有多个域的数据处理设备，该数据处理设备的若干装置可操作在这多个域中，所述多个域包含至少一个非安全域及至少一个安全域，在该安全域中所述装置能够访问从非安全域中所不能访问的安全数据，该数据处理设备包含：总线主控器装置，其固定在特定域中并且当需要访问数据时可操作以发布访问请求，该访问请求指示所述数据的地址；总线，通过该总线所述访问请求被路由至从属装置，通过该总线路由的每个访问请求具有与其相关联的域安全性信号，该域安全性信号识别关于该访问请求的域；并且所述总线主控器装置具有域控制逻辑，其可操作以接收在该总线主控器装置外部产生的域指定信号从而识别总线主控器装置所固定在其中的域，若该域指定信号指示该总线主控器装置固定在该安全域中，则该域控制逻辑依据由所述访问请求指定的所述地址可操作以选择性地产生待与所述访问请求相关联的非安全域安全性信号。

依据本发明，该数据处理设备具有至少一个安全域及一个非安全域，其中在数据处理设备内标示为安全的数据对于在非安全域中执行

的程序是不可访问的。总线主控器装置接收外部线上的信号，其确定总线主控器装置操作在安全域还是非安全域中。该信号“固定”总线主控器以在安全域或非安全域中操作。当该总线主控器装置发布将通过总线路由到从属装置的访问请求时，域控制逻辑可操作以产生与该访问请求相关联的域指定信号。若该总线主控器装置是在安全域中操作，则该域控制逻辑依据由所述访问请求指定的地址可产生非安全域指定信号。

让安全性域由外部信号指定，这就简化了必须在该总线主控器装置内提供的逻辑。再者，因为其安全性域未在总线主控器装置内部指定，所以可以信任该总线主控器装置会按照系统设计人员所预期的那样工作，原因在于不论黑客可能意图在总线主控器装置上执行什么样的恶意代码，切换安全性域(尤其自非安全切换至安全)都非选项。同时，藉由其域控制逻辑，对于安全(从而因此可信)程序，被选定的访问请求可以用地址相关的方式标示为非安全，尽管其来源于安全域。这样使得该安全程序能够将数据写至被定义为非安全位置的存储器位置，或将数据存储在共享资源(诸如高速缓冲存储器)中，并且将其标示为非安全数据，从而使得后续非安全程序可访问该数据。

在一个实施例中，该域控制逻辑能够访问存储器映射和该域安全性信号的指示，该存储器映射识别用于许多存储器区域的每个的访问控制信息，若指定存储器区域中的地址的访问请求是由该总线控制器装置操作在该安全域时发布的，则该域安全性信号的指示应结合该访问请求来发布。

因此，当该总线主控器装置在安全域中操作时，参考该存储器映射，访问请求不仅可以被成功地发布至被指定为安全的存储器区域，而且也可以被成功地发布至被指定为非安全的那些存储器区域，该存储器映射允许总线主控器“知道”该存储器映射的所有区域的正确的安全性。

在另一个实施例中，该域控制逻辑能够访问区域描述符，每个区描述符与存储器区域相关联并提供用于该存储器区域的区域安全性指示，所述区域描述符可由在安全域中执行的预定软件编程，所述域控制逻辑可操作以从所述域指定信号和用于含有由该访问请求指定的地址的存储器区域的区域描述符的区域安全性指示的组合中导出用于每

个访问请求的所述域安全性信号。

因此，存储器的特定区域可具有由对应区域描述符指定的区域属性及其访问许可，其可以由可信软件编辑。用于特定存储器区域的区域描述符典型地将提供一个或更多区域属性，识别例如对该区域的访问是否可高速缓存、可缓冲等；并且此外典型地将指定一个或更多访问许可，例如识别所讨论的区域是否仅当处理器核心处于预定操作模式时才可被访问，并且若其可被访问，是否允许读取访问及写入访问或者是否仅允许读取访问等。依此方式，存储器的特定区域的安全性状态可根据在数据处理设备的操作期间的需要而动态地改变。

在优选实施例中，当所述域指定信号指示该总线主控器装置固定在安全域中时，该域控制逻辑依据所述区域安全性指示来可操作地产生所述域安全性信号。依此方式，该总线主控器装置依据对应的区域描述符来适应伴随其访问请求的域安全性信号的安全性的能力，仅在安全域中操作时才被调用。

同时应了解上述用于产生域安全性信号的机制的相对优先级是可变化，在优选实施例中若所述地址在具有区域描述符的存储器区域中，则所述域安全性信号自所述区域安全性指示及所述域指定信号的所述组合中导出，否则所述域安全性信号从自所述存储器映射中获得的所述访问控制信息中导出。

在优选实施例中，当所述域指定信号指示该总线主控器装置固定在非安全域中时，所述域控制逻辑可操作以将所述域安全性信号恒产生为非安全。因此，仅有在安全域中操作的总线主控器装置能调整伴随其访问请求的域安全性信号的安全性。

在一个实施例中，该域指定信号是输入到该总线主控器装置的静态输入。因此，该总线主控器装置被永久地硬连接成处于一个特定安全性域中，且无法切换至另一个安全性域。

同时应了解存在可产生该域指定信号的许多方式，在一个实施例中该数据处理设备进一步包含安全性控制逻辑，其可操作以产生所述域指定信号。因此，该安全性控制逻辑已控制该总线主控器装置被固定在其中进行操作的安全性域并且依据可信的系统设计人员规定的规则指导该安全性域的定义。这种可信的规则由一个实施例说明，其中该域指定信号仅在所述总线主控器装置复位时才可改变。

应了解该总线主控器装置被固定在特定安全域中意味着在其操作期间不能在安全域及非安全域间转换。然而在非常有限的情况下，从安全域至非安全域的单一转换是可能的。尤其在一个实施例中，该总线主控器装置在启动时开始操作在安全域中，所述安全性控制逻辑可操作以稍后在启动过程中切换为产生非安全域指定信号，并且所述安全性控制逻辑此后可操作以仅产生非安全域指定信号，直至重新启动。

依此方式，当该数据处理设备启动时，该总线主控器装置可暂时在安全域中操作，同时执行可信的启动代码，但接着在启动代码完成时或之前，该总线主控器装置进入非安全模式，并且在没有重新启动的情况下不能切换回安全模式。这确保了在该时间期间该总线主控器被允许操作在安全域中(在启动时为了设置目的允许其暂时如此可能是有利的)，这并未显现出弱点，因为仅有可信启动代码在被执行，并且该总线主控器装置在该启动代码完成之前是不可逆地切换到非安全域。

在一个实施例中，该总线主控器装置本身能够经由系统内的再多些可信元件(例如在安全域内的处理器上执行的代码)来起动重启程序。在这些有限的情况中，该总线主控器装置可起动经验证的重启以使得从非安全域转换至安全域。总线主控器装置验证所用的可信代码用来确保该功能仅能由有效的未受黑客侵犯的代码起动。

从第二方面来看，本发明提供一种具有多个域的数据处理设备，该数据处理设备的若干装置可操作在该多个域中，所述多个域包含至少一个非安全域及至少一个安全域，在该安全域中所述装置能够访问从非安全域中所不能访问的安全数据，该数据处理设备包含：总线主控器构件，其固定在特定域中并且当需要访问数据时用于发布访问请求，该访问请求指定所述数据的地址；总线构件，通过该总线构件所述访问请求被路由至从属装置构件，通过该总线构件路由的每个访问请求具有与其相关联的域安全性信号，该域安全性信号识别关于该访问请求的域；且该总线主控器构件具有域控制逻辑构件，其用于接收在该总线主控器构件外部产生的域指定信号，以识别该总线主控器构件固定在其中的域，若该域指定信号指示该总线主控器构件固定在安全域中，则该域控制逻辑构件依据由所述访问请求指定的所述地址选择性地产生将与所述访问请求相关联的非安全域安全性信号。

从第三方面来看，本发明提供一种在具有多个域的数据处理设备中产生访问请求的方法，该数据处理设备的若干装置可操作在该多个域中，所述多个域包含至少一个非安全域及至少一个安全域，在该安全域中所述装置能够访问从非安全域中所不能访问的安全数据，该方法包含以下步骤：在总线主控器装置外部产生域指定信号，以识别该总线主控器装置固定在其中的域；当需要访问数据时自所述总线主控器装置发布访问请求，所述访问请求指定所述数据的地址；将域安全性信号与所述访问请求相关联，以识别关于该访问请求的域；以及若所述域指定信号指示所述总线主控器装置固定在所述安全域中，则依据所述地址选择性地产生将与所述访问请求相关联的非安全域安全性信号。

附图说明

参考附图中所示的具体实施例，仅以举例的形式进一步描述本发明，其中：

图 1 是依据本发明的一个实施例的数据处理设备的方框图；

图 2 示意性地示出了依据本发明的一个实施例的数据高速缓冲存储器；

图 3 是依据本发明的一个实施例的总线主控器装置的方框图；

图 4 示意性地示出了依据本发明的一个实施例的存储器地址空间的一部分；和

图 5 是示出了依据本发明的一个实施例的图 3 的控制逻辑的操作的流程图。

具体实施方式

图1是依据本发明的一个实施例的数据处理设备的方框图。总线10连接数据处理设备的各种组件并且允许它们彼此通讯，这种通讯具体而言是通过将数据访问请求自主控器装置传送至从属装置以及或者将待写入的数据项自主控器装置传送至从属装置或者自从属装置将请求的读取数据项返回至主控器装置。可切换安全性处理器20是可发布访问请求的总线主控器装置的实例。此外，可切换安全性处理器20可在安全域或非安全域中操作。当在安全域中操作时，其能访问数据处理

设备内的标示为安全数据的数据。用于数据处理设备内的数据项的主存储位置是存储器30，其经由系统高速缓冲存储器40连接至总线10。“固定式”安全性总线主控器50也可在安全域或非安全域中操作。然而，该总线主控器本身不控制其操作所处的安全性域，使其安全性域由从安全性控制逻辑60接收的信号TZ_NS_CTL定义。

安全性控制逻辑60确保TZ_NS_CTL信号在总线主控器50的正常操作期间保持不变，实际上在一个实施例中，TZ_NS_CTL被“硬连接”为高或低(即永久的非安全域或安全域操作)。更一般而言，安全性控制逻辑60由通过路径75发送信号给安全性控制逻辑60的系统控制器70所控制。

在一个实例中，总线主控器50可以是将服务提供给另一“主控器”处理器的“协助器”处理器，例如加密编码或译码。在该实例中，因为总线主控器正在处理诸如加密密钥的敏感数据，所以该总线主控器将持续操作在安全域中。因此，安全性控制逻辑60将提供连续的TZ_NS_CTL=0(安全)信号。

在另一实例中，虽然总线主控器50的安全域可在其正常操作期间被固定，但可能在非常有限的情况下允许总线主控器50的单个单向安全性域的转换可能是有用的。例如，总线主控器50可在数据处理设备的启动期间在安全域中操作，但其后在该数据处理设备的正常操作期间总线主控器50可在非安全域中继续操作。为了确保这种转换是单向的，在该实例中安全性控制逻辑60被配置成使得在启动期间仅有一个在路径75上被接收的安全性域转换信号(其指示从安全至非安全的转换)被响应，并且此后安全性控制逻辑60将产生连续且不变的非安全TZ_NS_CTL信号而不管路径75上信号的改变，直至在路径80上从系统控制器70接收复位信号。

当总线主控器50在安全域中操作(例如在数据处理设备启动例程期间)时，允许总线主控器50将其本身的转换发送信号给非安全域可能是有利的。由于该原因，临时路径85仅在启动时期可用，以使得总线主控器50可直接触发来自安全性控制逻辑60的TZ_NS_CTL信号的改变。因此，一旦总线主控器50不再需要在安全域中操作(例如一旦其已完成启动例程序)，其可立即切换至非安全操作。接着再切换至安全操作是不可能的，直至系统控制器70复位该安全性控制逻辑60及总线主控器

50。

图2示出了诸如图1的系统高速缓冲存储器40之类的高速缓冲存储器。这种高速缓冲存储器将被典型地分成几路(100、110、120等)。各路可将数据存储在阵列中，该阵列一般将被分成标记(TAG)阵列130及数据阵列140。存储在存储器30中的数据项的复本存储在数据阵列140的条目中，而与那些数据项相关联的额外信息存储在TAG阵列130中。这些相关的信息条典型地可包含TAG 150、修改位160、有效位170及NS位180。TAG对应于数据阵列140中对应数据项目的存储器地址的一部分。修改位160及有效位170分别指示对应数据项自初始被存储在该高速缓冲存储器线以来是否被更新以及该高速缓冲存储器线中的数据项是否仍有效。NS位对应于与该高速缓冲存储器线相关的安全性域。因此，由作为安全访问对象的数据所填充的高速缓冲存储器线将使NS位设定为0，而由作为非安全访问对象的数据所填充的高速缓冲存储器线将使NS位元设定为1。这使该高速缓冲存储器能由安全域及非安全域共享，而不会有非安全程序可访问安全数据的风险。这是因为来自特定安全性域的数据访问请求将仅能访问高速缓冲存储器中的其NS位匹配该安全性域的高速缓冲存储器线。

图3示出了总线主控器50内的中央处理器(CPU)200。在CPU 200内，处理器核心210发布访问请求，并且发送或接收作为访问请求对象的数据。来自处理器核心210的访问请求被传送至存储器保护单元(MPU)220内的控制逻辑230。由安全性控制逻辑60产生的TZ_NS_CTL信号由控制逻辑230接收。在MPU 220内，描述符表240也传送由处理器核心210发出的访问请求。由于处理器核心210不接收该域指定信号TZ_NS_CTL，所以处理器核心本身不具有安全性域意识，而是由MPU 220依据自处理器核心210接收的访问请求、域指定信号TZ_NS_CTL及存储在描述符表240中的信息来创建域安全性指示。产生域安全指示(NS-prot)所依据的逻辑总结在表1中。

依据表1所示的逻辑，非安全=0而安全=1。当TZ_NS_CTL=1(即CPU 200设定为在非安全域中操作)时，所产生的安全性指示(NS-prot)恒为1，这意味着在非安全域中操作的核心仅能产生非安全访问。可替换地，若存储器保护单元停用(MPU使能=0)，而该核心设定为在安全域(TZ_NS_CTL=0)中操作，则依据表2所示的默认存储器映射确定安全性

指示NS_Port(下面描述)。然而，若CPU设定为在安全域(TZ_NS_CTL=0)中操作而MPU被使能(MPU使能=1)，则依据量NS-区域的值确定安全性指示NS-prot。

TZ_NS_CTL	MPU使能	NS-区域	NS-prot	说明
0	0	X	0/1	依据表2中的地址范围的安全/非安全访问
0	1	0	0	安全访问
0	1	1	1	非安全访问
1	X	X	1	非安全访问

表1

描述符表240存储存储器地址区域及其对应的NS-区域值的列表。与落入给定存储器地址区域内的地址对应的数据访问请求将使得描述符表240产生与该列表中所储存的地址对应的NS-区域的值。然而应了解存储在描述符表240中的列表可采取各种形式，在一个实施例中NS-区域是MPU区域访问控制寄存器的属性。这些寄存器被配置成复位至逻辑值零，即按照在安全域中的默认操作将产生安全访问。应注意到在一个实施例中，表1中定义的NS-prot的切换仅应用于数据访问请求。在此类实施例中，指令访问请求总是匹配该安全性域的安全性。这确保仅有数据而非指令可在安全域和非安全域之间共享。因此控制逻辑230将访问请求自处理器核心210传送至总线10，并附加合适的NS-prot值。控制逻辑230也可传送及/或附加区域属性及访问许可至访问请求(视情况而定，如读/写许可，(不)可高速缓存等等)。

仍如图1所示，CPU 200可包含一级高速缓冲存储器250，其可以为统一的指令及数据高速缓冲存储器或者可以形成为分离的指令及数据高速缓冲存储器。典型地，对于可高速缓存的访问请求，控制逻辑230将使查找程序在访问请求被传播至总线10之前在一级高速缓冲存储器250中执行，并且若该一级高速缓冲存储器250含有作为访问请求对象的一个或多个数据项，则该访问请求依据该一级高速缓冲存储器250进行而无须将访问请求传播至总线10上。若由该访问请求指定的地址与存储器的回写式区域有关，则该更新能发生在一级高速缓冲存储器中而无须同时在系统高速缓冲存储器40及/或存储器30中执行该更新，尽

管修改位(类似于图2的修改位160)将被设定以指示稍后需要用该高速缓冲存储器内的条目来更新系统高速缓冲存储器40/存储器30中的条目。然而若该地址与直写式(write through)区域有关，则该更新典型地将发生在一级高速缓冲存储器250中，并且同时该访问请求也将经由总线10传播至系统高速缓冲存储器40/存储器30以使该更新发生在系统高速缓冲存储器/存储器中。

表2示出了示例性默认存储器映射。这种默认存储器映射定义了当TZ_NS_CTL=0(即安全域操作)时对于存储器的特定区域的访问请求的安全状态应该是什么样，并且还定义了其它访问属性(参见下文)。默认存储器映射可用于不实施MPU的中央控制单元或者用于确实具有如下MPU的中央控制单元：该MPU被停用(参见表1的第一行)或者用于其地址未由区域描述符涵盖的访问请求(因此NS-区域值未被定义)。

地址范围	TZ_NS_CTL=0时之NS-prot	指令存储器类型		数据存储器类型		执行
		I高速缓冲存储器使能	I高速缓冲存储器停用	D高速缓冲存储器使能	D高速缓冲存储器停用	
0xE0000000至0xFFFFFFFF	非安全	N/A	NA	强有序	强有序	永不执行
0xC0000000至0xDFFFFFFF	安全					
0xB0000000至0xBFFFFFFF	非安全	N/A	NA	共享装置	共享装置	永不执行
0xA0000000至0xAFFFFFFF	安全					
0x90000000至0x9FFFFFFF	非安全	N/A	NA	非共享装置	非共享装置	永不执行
0x80000000至0x8FFFFFFF	安全					
0x70000000至0x7FFFFFFF	非安全	正常，WT可高速缓存，非共享	正常，不可高速缓存，非共享	正常，不可高速缓存，共享	正常，不可高速缓存，共享	指令执行允许
0x60000000至0x6FFFFFFF	安全					
0x50000000至0x5FFFFFFF	非安全	正常，WT可高速缓存，非共享	正常，非可高速缓存，非共享	正常，WT可高速缓存，非共享	正常，不可高速缓存，共享	指令执行允许
0x40000000至0x4FFFFFFF	安全					
0x20000000至0x3FFFFFFF	非安全	正常，WT可高速缓存，非共享	正常，不可高速缓存，非共享	正常，WBWA可高速缓存，非共享	正常，不可高速缓存，共享	指令执行允许
0x00000000至0x1FFFFFFF	安全					

表2

在以上表2中，在一个实施例中非安全的NS-prot值由逻辑1值给定而安全的NS-prot值由逻辑0值给定。

在表2的示例性存储器映射中，上方六个存储器地址范围仅被分配给数据存储器，而下方六个存储器地址区域被分配给指令存储器或数据存储器。对于唯数据存储器，不可能对存储的数据项执行，并且对该区域内的地址的指令访问请求将终止。该唯数据存储器被细分成强有序的(即非高速缓存的)及共享/非共享的(即分别能或不能服从多处理器装置内的硬件一致性方案)多个区域。

下方六个存储器地址区域允许指令执行。这些存储器区域具有已定义的其它访问属性，如共享/非共享以及或不可高速缓存、直写式(WT)可高速缓存或回写写分配式(WBWA)可高速缓存。

图4示意性地示出了存储器地址空间300的区域，其中存在存储在描述符表240中的区域描述符的地址的三个子区域310、320及330被定义。存储器地址空间300的其余部分由不存在区域描述符(即未定义NS-区域值)的存储器地址区域组成，并且对于这些区域，可使用默认存储器映射(表2)(或可替换地，对此类区域的访问导致终止)。

图5是示出了依据本发明的一个实施例的图3的控制逻辑230的操作的流程图。在步骤400中，控制逻辑230等待将从处理器核心210接收的数据访问请求。一旦在步骤410接收到数据访问请求，执行描述符表240中的查找。若接着在步骤420确定命中（hit）未发生，则在步骤430检查默认存储器映射条目是否可用于该对应地址。若不可用，则发布终止(步骤440)。若对于该地址存在默认存储器映射条目，则从该信息产生NS-prot(步骤450)，并且该地址连同该NS-prot值及请求的许可一并输出。若在步骤420存在命中，则检查(步骤460)在描述符表中是否发生多于一个命中。在该实施例中这是可能的，其中多个重叠的区域描述符是可能的，例如为特定存储器装置中的所有地址定义的普通区域描述符以及还为该装置的某些地址定义的特定区域描述符。若存在多于一个命中，则在步骤470应用优先级准则以选择最高优先级命中，即在为给定地址定义的所有区域描述符中，选取具有最高优先级的那个命中。在步骤480控制逻辑230依据已接收的TZ_NS_CTL值及选定的区域描述符的NS-区域值，产生NS-prot值。最后在步骤490处，数据访问请求(视需要)连同相关的NS-prot值及许可一并输出至总线10上或直接进

入一级高速缓冲存储器250。

总之，从本发明的实施例的以上描述中，应了解已提供一种用于产生访问请求的数据处理设备和方法。所提供的总线主控器可依据自总线主控外部接收的信号，在数据处理设备的安全域或非安全域中操作。在总线主控器的正常操作期间把该信号生成为固定。提供控制逻辑，当总线主控器装置在安全域中操作时，所述控制逻辑依据默认存储器映射或安全定义的存储器区域描述符是可操作的以产生与由总线主控器核心产生的访问请求相关联的域指定信号，该域指定信号指示是安全访问还是非安全访问。因此，在安全域中操作的总线主控器可产生安全访问及非安全访问，而无须其本身能在安全及非安全操作间切换。

尽管这里已描述了特定实施例，应了解本发明不受其限制并且在本发明的范畴内可进行许多修改及增加。例如，在不脱离本发明的范畴下，可进行所附从属权利要求的特征及独立权利要求的特征的各种结合。

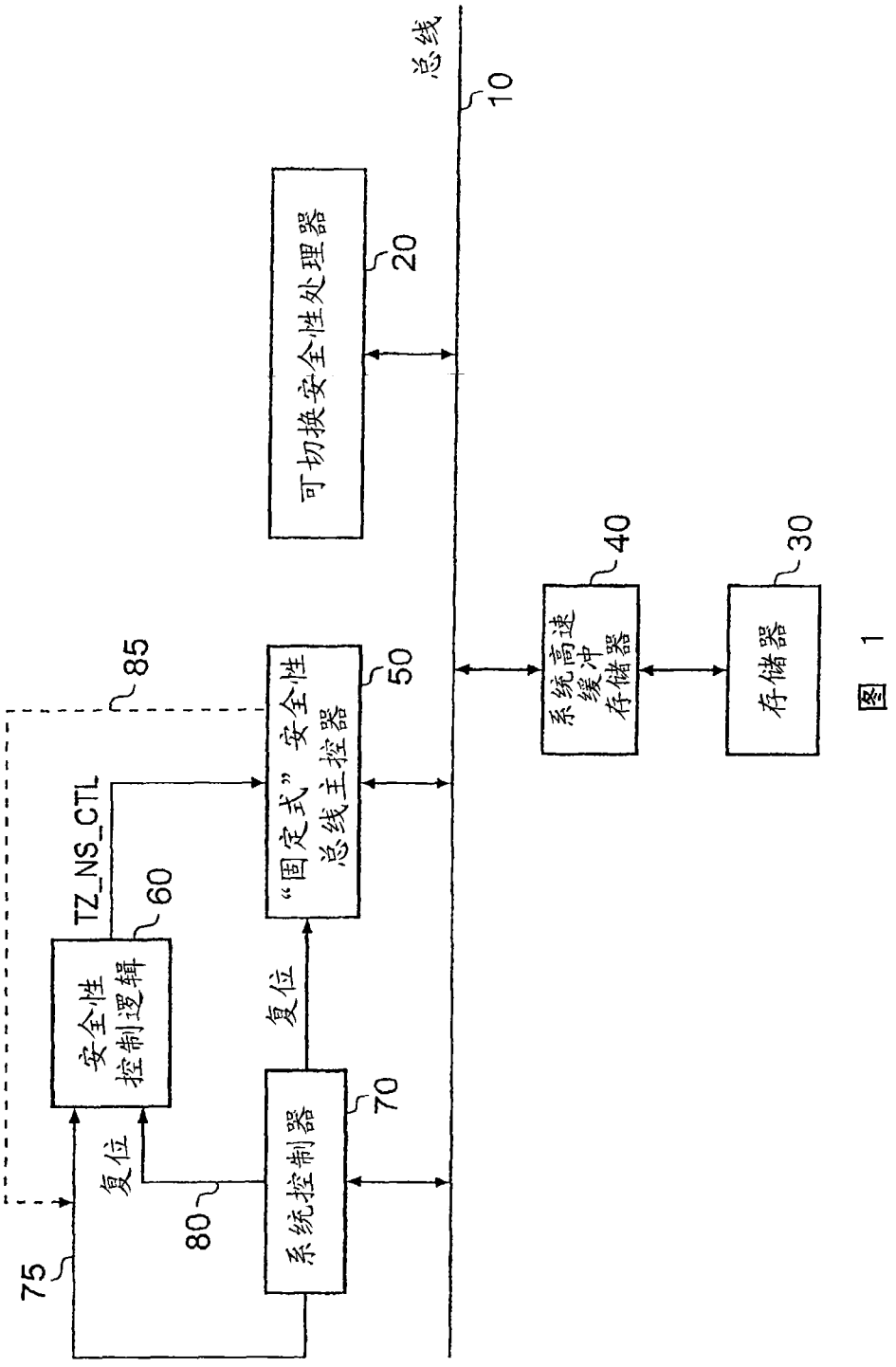

总线
10
可切换安全性处理器
20
40
30
系统高速缓冲存储器
存储器
85
50
"固定式"安全性总线主控器
TZ_NS_CTL
60
安全性控制逻辑
复位
复位
70
系统控制器
80
75

图 1

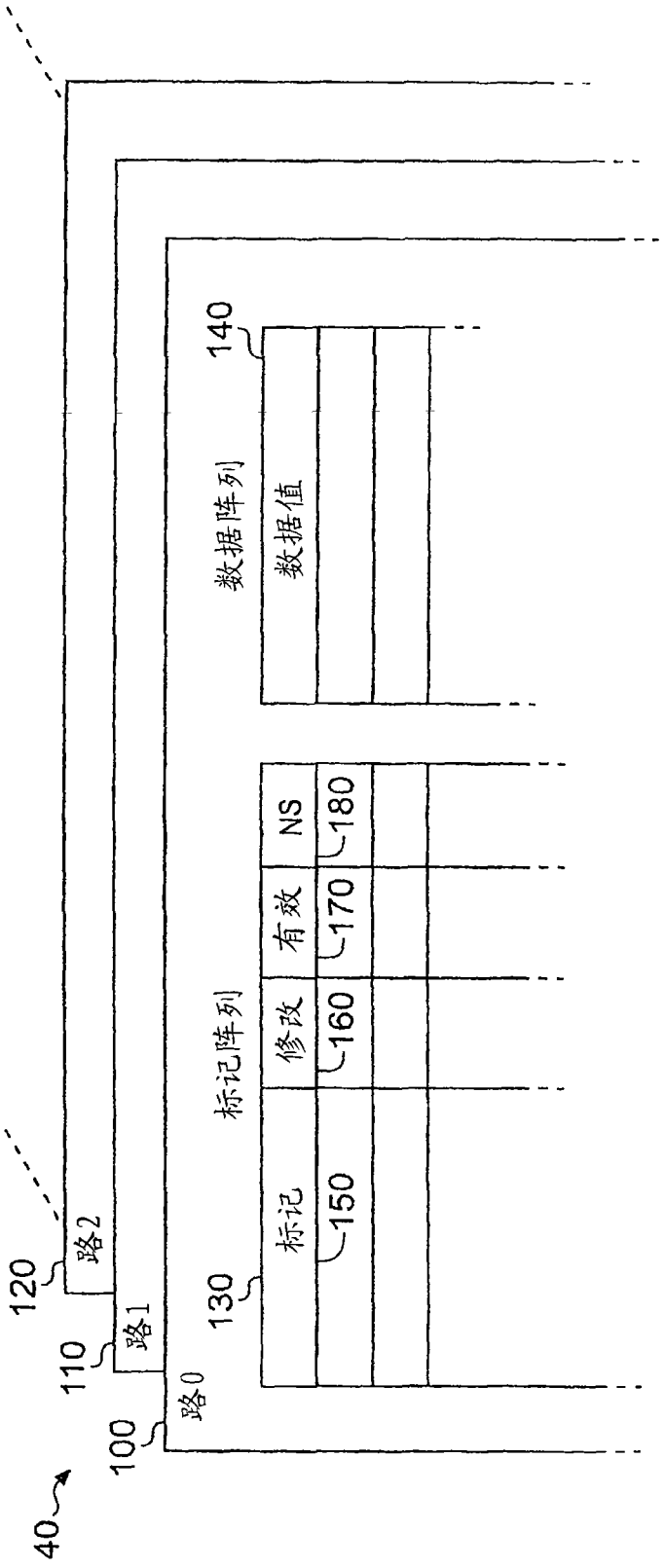

40
100
路0
110
路1
120
路2
130
标记阵列
标记
修改
有效
NS
150
160
170
180
140
数据阵列
数据值

图 2

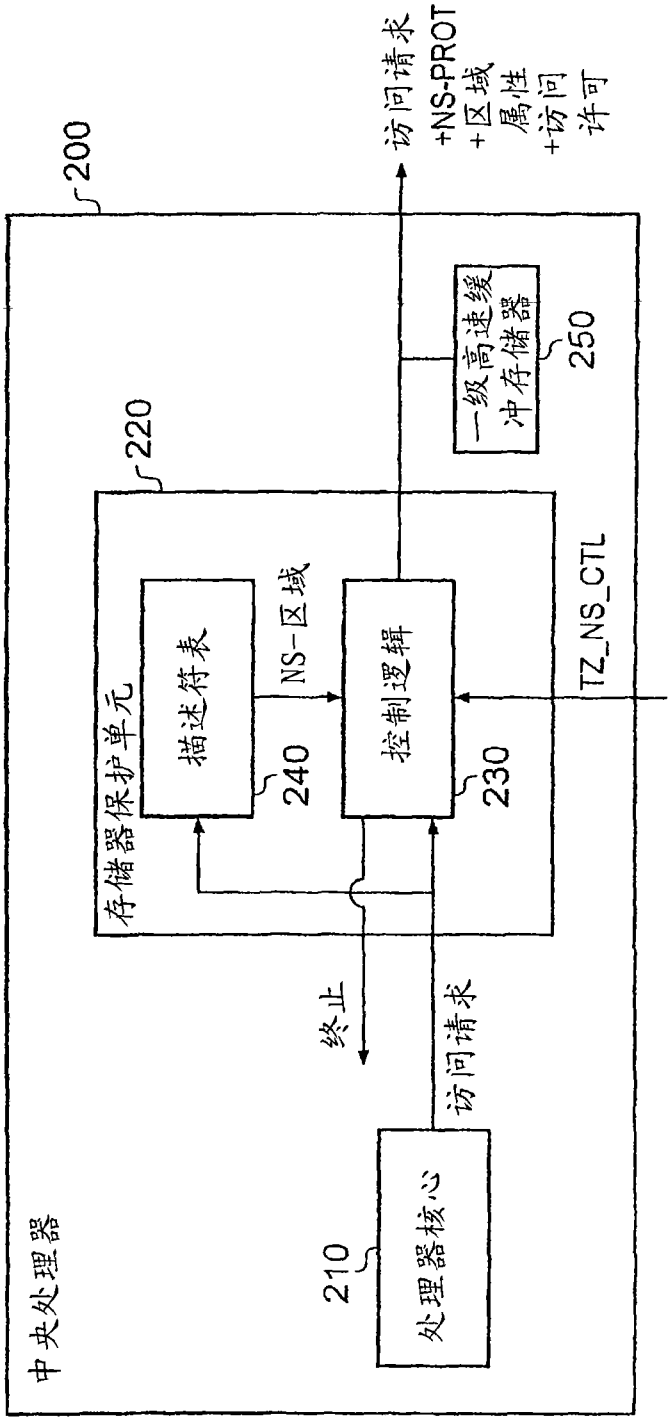

中央处理器
200
处理器核心
210
访问请求
终止
存储器保护单元
220
描述符表
240
NS-区域
控制逻辑
230
TZ_NS_CTL
一级高速缓冲存储器
250
访问请求
+NS-PROT
+区域
属性
+访问
许可

图 3

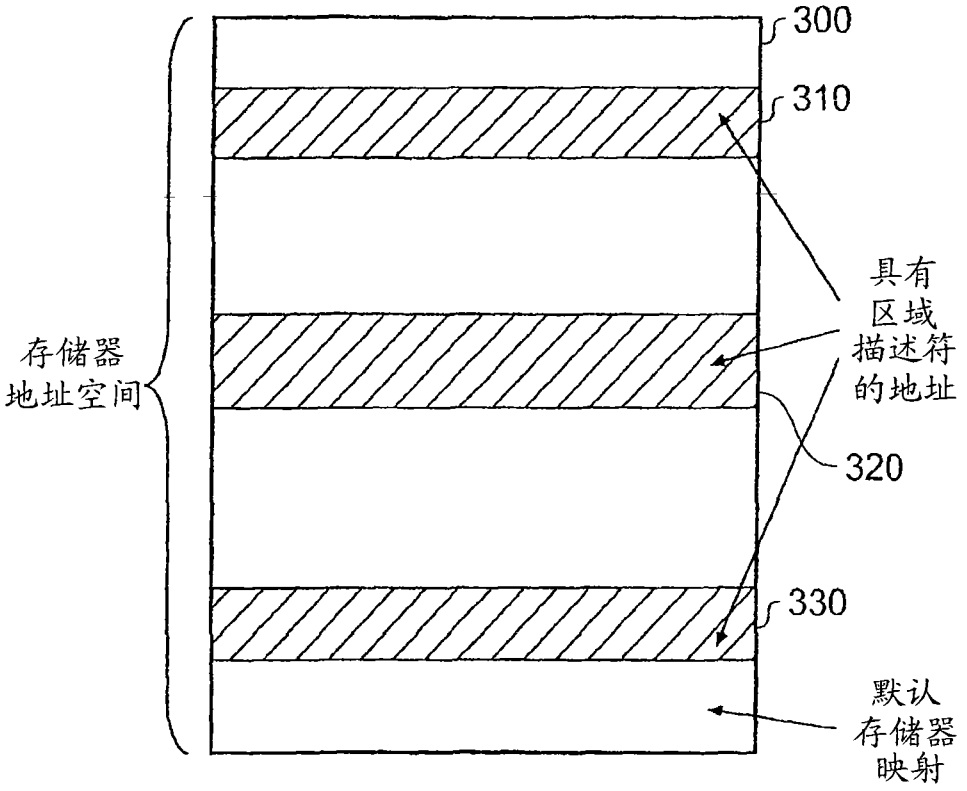


图 4

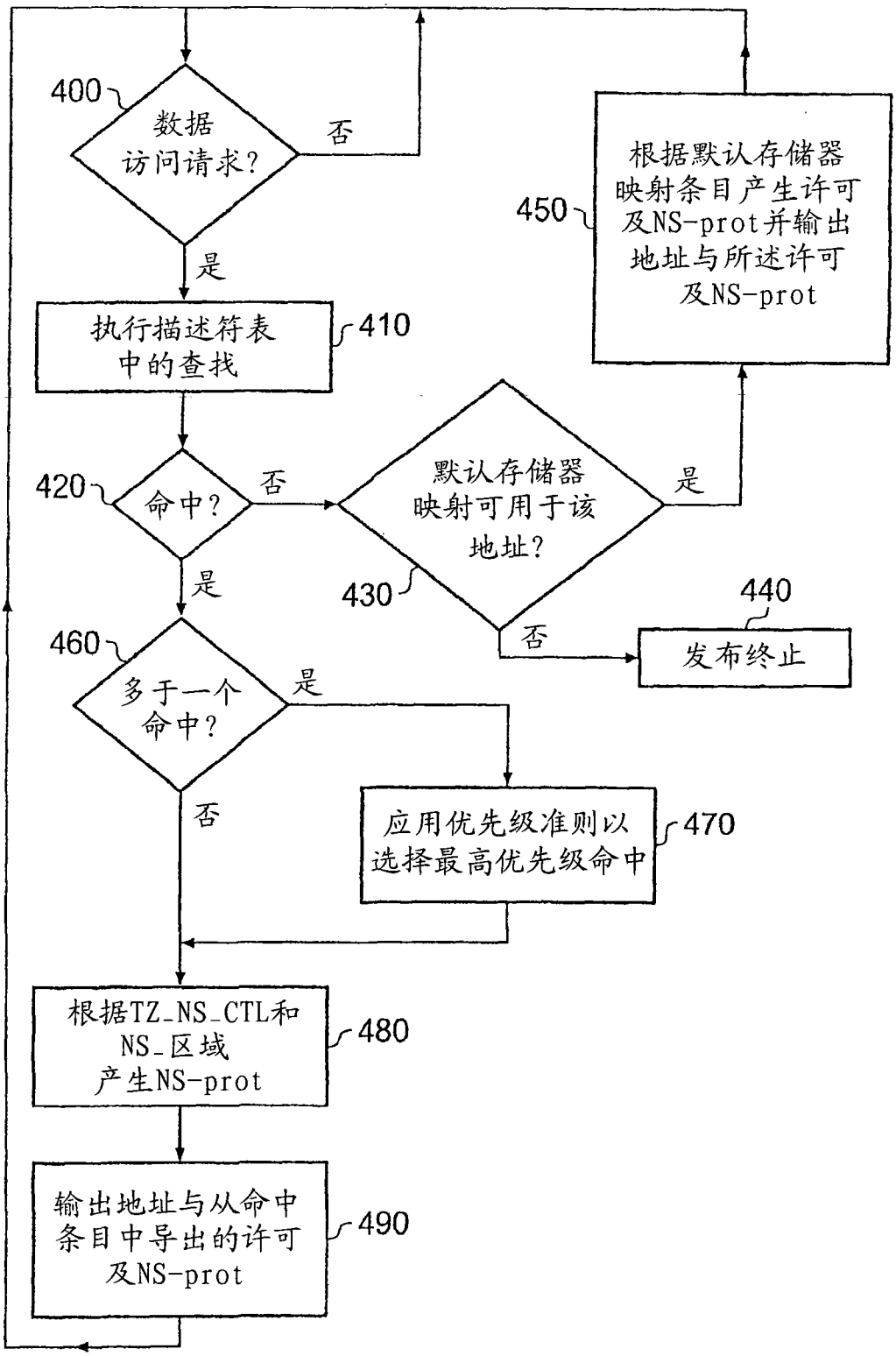

400
数据
访问请求?
否
是
执行描述符表
中的查找
410
420
命中?
否
是
默认存储器
映射可用于该
地址?
是
否
430
根据默认存储器
映射条目产生许可
及NS-prot并输出
地址与所述许可
及NS-prot
450
440
发布终止
460
多于一个
命中?
是
否
应用优先级准则以
选择最高优先级命中
470
根据TZ_NS_CTL和
NS_区域
产生NS-prot
480
输出地址与从命中
条目中导出的许可
及NS-prot
490

图 5