(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 110532789 B
(45)授权公告日 2021.04.06

(21)申请号 201910743535.0

(22)申请日 2019.08.13

(65)同一申请的已公布的文献号
申请公布号 CN 110532789 A

(43)申请公布日 2019.12.03

(73)专利权人 南京芯驰半导体科技有限公司
地址 210000 江苏省南京市江北新区星火路17号创智大厦B座610室

(72)发明人 张力航 孙鸣乐 谢俊

(74)专利代理机构 北京德崇智捷知识产权代理有限公司 11467
代理人 王金双

(51)Int.Cl.
G06F 21/60(2013.01)

(56)对比文件
CN 106713332 A,2017.05.24
CN 102970164 A,2013.03.13
CN 103873463 A,2014.06.18
US 2012215901 A1,2012.08.23
CN 101030946 A,2007.09.05

审查员 江梓琴

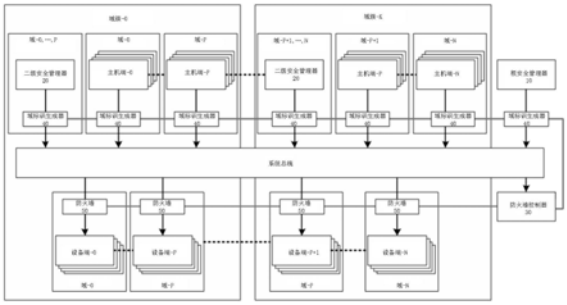
权利要求书2页 说明书7页 附图1页

(54)发明名称

一种层次化的系统防火墙及配置方法

(57)摘要

一种层次化的系统防火墙，包括，根安全管理器、二级安全管理器、防火墙控制器，以及防火墙，其中，所述根安全管理器，为每个域簇指定二级安全管理器、分配系统资源；为域簇之间提供防火墙配置方案；所述二级安全管理器，为域簇的主机以及设备添加域标识符，并为每个域提供防火墙配置方案；所述防火墙控制器，为系统中的主机以及设备添加域簇标识号、为所述二级安全管理器添加标识；为当前域簇中的主机以及设备分配域标识；为当前域簇中每一个设备端的防火墙进行访问权限的配置；所述防火墙，为来自不同域或不同域簇的主机对当前设备的访问进行权限控制。本发明还提供一种层次化的系统防火墙的配置方法，简化了系统的设计，提高了系统的安全性。



CN 110532789 B

1.一种层次化的系统防火墙，其特征在于，包括，根安全管理器、二级安全管理器、防火墙控制器，以及防火墙，其中，

所述根安全管理器，其为每个域簇指定二级安全管理器、分配系统资源；为域簇之间提供防火墙配置方案；

所述二级安全管理器，为域簇的主机以及设备添加域标识，并为域簇中每个域提供防火墙配置方案；

所述防火墙控制器，其为系统中的主机以及设备添加域簇标识、为所述二级安全管理器添加标识；为当前域簇中的主机以及设备分配域标识；为当前域簇中每一个设备端的防火墙进行访问权限的配置；

所述防火墙，其为来自不同域或不同域簇的主机对当前设备的访问进行权限控制。

2.根据权利要求1所述的层次化的系统防火墙，其特征在于，所述系统资源，包括，主机、设备和域资源。

3.根据权利要求1所述的层次化的系统防火墙，其特征在于，还包括域标识生成器，所述域标识生成器，根据所述根安全管理器的配置为系统中的每一个主机生成域簇标识；根据所述根安全管理器和所述二级安全管理器的配置为系统中的每一个主机生成域标识。

4.根据权利要求1所述的层次化的系统防火墙，其特征在于，所述防火墙控制器，其依据所述根安全管理器的配置为系统中的主机以及设备添加域簇标识、为所述二级安全管理器添加标识；接受所述根安全管理器或所述二级安全管理器的配置，为当前域簇中的主机以及设备分配域标识；接受所述根安全管理器或所述二级安全管理器的配置，为当前域簇中每一个设备端的防火墙进行访问权限的配置。

5.根据权利要求1所述的层次化的系统防火墙，其特征在于，所述防火墙，其根据所述根安全管理器或本域簇的所述二级安全管理器的配置，为来自不同域或不同域簇的主机对当前设备的访问进行权限控制。

6.一种层次化的系统防火墙的配置方法，包括以下步骤：

1)为每一个域簇分配系统资源，并指定二级安全管理器；

2)为系统中的主机和设备添加域簇标识、为二级安全管理器添加标识，并为域簇之间提供防火墙配置方案；

3)为域簇中的主机和设备添加域标识后分配到不同域中，并为每个域提供防火墙配置方案；

4)为当前域簇中每一个设备端的防火墙进行访问权限的配置；

5)为来自不同域或不同域簇的主机对当前设备的访问进行权限控制；

所述步骤1)进一步包括，

根安全管理器为每一个域簇分配主机、设备，以及域资源，同时为每一个域簇指定二级安全管理器；

所述步骤3)进一步包括，

防火墙控制器接受根安全管理器或二级安全管理器的配置，为当前域簇中的主机以及设备分配域标识；

二级安全管理器根据自身安全的需求，为域簇所有的主机以及设备添加域标识，并为每个域提供防火墙配置方案。

7.根据权利要求6所述的层次化的系统防火墙的配置方法，其特征在于，所述步骤2)进一步包括，

防火墙控制器根据根安全管理器的配置，为系统中的每一个主机和设备添加域簇标识、为二级安全管理器添加标识；

根安全管理器为域簇之间提供防火墙配置方案。

8.根据权利要求6所述的层次化的系统防火墙的配置方法，其特征在于，所述步骤4)进一步包括，防火墙控制器接受根安全管理器或二级安全管理器的配置，为当前域簇中每一个设备端的防火墙进行访问权限的配置。

9.根据权利要求6所述的层次化的系统防火墙的配置方法，其特征在于，所述步骤5)进一步包括，防火墙根据根安全管理器或二级安全管理器的配置，为来自不同域或不同域簇的主机对当前设备的访问进行权限控制。

10.一种计算机可读存储介质，其上存储有程序，其特征在于，所述程序可被处理器执行权利要求6-9任一项所述的层次化的系统防火墙的配置方法的步骤。

一种层次化的系统防火墙及配置方法

技术领域

[0001] 本发明实施例涉及片上系统(SoC)技术领域,尤其涉及片上系统的防火墙。

背景技术

[0002] 片上系统中的硬件防火墙(Firewall),其作用主要包括:

[0003] 为各个子系统提供可靠的数据隔离;

[0004] 为各个子系统之间,以及子系统内部主机与设备间提供可靠的数据交互通道

[0005] 保护安全世界敏感信息;

[0006] 为全以及非安全世界提供安全的数据交互通道。

[0007] 现有硬件防火墙设计,多采用单一层次的管理结构,即由单一的管理器对整个系统的安全策略进行管理。而随着系统中子系统数目的不断增加,为了满足各个子系统不同的安全需求,单一的管理器结构安全策略设计的复杂度急剧增加。

发明内容

[0008] 为了解决现有技术存在的不足,本发明提供一种层次化的系统防火墙及配置方法,简化了系统安全应用的功能设计,提高系统整体以及子系统的安全性。

[0009] 为实现上述目的,本发明至少一个实施例提供一种层次化的系统防火墙,包括,根安全管理器、二级安全管理器、防火墙控制器,以及防火墙,其中,

[0010] 所述根安全管理器,其为每个域簇指定二级安全管理器、分配系统资源;为域簇之间提供防火墙配置方案;

[0011] 所述二级安全管理器,为域簇的主机以及设备添加域标识,并为域簇中每个域提供防火墙配置方案;

[0012] 所述防火墙控制器,其为系统中的主机以及设备添加域簇标识、为所述二级安全管理器添加标识;为当前域簇中的主机以及设备分配域标识;为当前域簇中每一个设备端的防火墙进行访问权限的配置;

[0013] 所述防火墙,其为来自不同域或不同域簇的主机对当前设备的访问进行权限控制。

[0014] 进一步地,所述系统资源,包括,主机、设备和域资源。

[0015] 进一步地,还包括域标识生成器,所述域标识生成器,根据所述根安全管理器的配置为系统中的每一个主机生成域簇标识;根据所述根安全管理器和所述二级安全管理器的配置为系统中的每一个主机生成域标识。

[0016] 进一步地,所述防火墙控制器,其依据所述根安全管理器的配置为系统中的主机以及设备添加域簇标识、为所述二级安全管理器添加标识;接受所述根安全管理器或所述二级安全管理器的配置,为当前域簇中的主机以及设备分配域标识;接受所述根安全管理器或所述二级安全管理器的配置,为当前域簇中每一个设备端的防火墙进行访问权限的配置。

[0017] 更进一步地，所述防火墙，其根据所述根安全管理器或本域簇的所述二级安全管理器的配置，为来自不同域或不同域簇的主机对当前设备的访问进行权限控制。

[0018] 为实现上述目的，本发明至少一个实施例还提供了一种层次化的系统防火墙的配置方法，包括以下步骤：

[0019] 1)为每一个域簇分配系统资源，并指定二级安全管理器；

[0020] 2)为系统中的主机和设备添加域簇标识、为二级安全管理器添加标识，并为域簇之间提供防火墙配置方案；

[0021] 3)为域簇中的主机和设备添加域标识后分配到不同域中，并为每个域提供防火墙配置方案；

[0022] 4)为当前域簇中每一个设备端的防火墙进行访问权限的配置；

[0023] 5)为来自不同域或不同域簇的主机对当前设备的访问进行权限控制；

[0024] 所述步骤1)进一步包括，

[0025] 根安全管理器为每一个域簇分配主机、设备，以及域资源，同时为每一个域簇指定二级安全管理器；

[0026] 所述步骤3)进一步包括，

[0027] 防火墙控制器接受根安全管理器或二级安全管理器的配置，为当前域簇中的主机以及设备分配域标识；

[0028] 二级安全管理器根据自身安全的需求，为域簇所有的主机以及设备添加域标识，并为每个域提供防火墙配置方案。

[0029] 进一步地，所述步骤2)进一步包括，

[0030] 防火墙控制器根据根安全管理器的配置，为系统中的每一个主机和设备添加域簇标识、为二级安全管理器添加标识；

[0031] 根安全管理器为域簇之间提供防火墙配置方案。

[0032] 进一步地，所述步骤4)进一步包括，防火墙控制器接受根安全管理器或二级安全管理器的配置，为当前域簇中每一个设备端的防火墙进行访问权限的配置。

[0033] 更进一步地，所述步骤5)进一步包括，防火墙根据根安全管理器或二级安全管理器的配置，为来自不同域或不同域簇的主机对当前设备的访问进行权限控制。

[0034] 为实现上述目的，本发明至少一个实施例提供一种计算机可读存储介质，其上存储有程序，所述程序可被处理器执行，实现上述层次化的系统防火墙的配置方法的步骤。

[0035] 本发明的层次化的系统防火墙及配置方法，解决了多子系统处理器由于子系统数目不断增加导致的安全策略设计复杂度急剧提升的问题。与现有技术相比较，具有如下的技术效果：

[0036] 1)简化了系统(特别是带虚拟化的异构系统)中安全应用的功能设计；

[0037] 2)降低了不同子系统之间安全策略管理的耦合性，使得每个子系统可独立开发安全应用；

[0038] 3)层次化设计，减少了各个子系统之间的干扰提高了整体以及子系统的安全性

[0039] 本发明的其它特征和优点将在随后的说明书中阐述，并且，部分地从说明书中变得显而易见，或者通过实施本发明而了解。

附图说明

[0040] 附图用来提供对本发明的进一步理解，并且构成说明书的一部分，并与本发明的内容和实施例一起，用于解释本发明，并不构成对本发明的限制。在附图中：

[0041] 图1为根据本发明的层次化的系统防火墙结构框图；

[0042] 图2为根据本发明的层次化的系统防火墙配置方法流程图。

具体实施方式

[0043] 以下结合附图对本发明的优选实施例进行说明，应当理解，此处所描述的实施例仅用于说明和解释本发明，并不用于限定本发明。

[0044] 在附图的流程图示出的步骤可以在诸如一组计算机可执行指令的计算机系统中执行。并且，虽然在流程图中示出了逻辑顺序，但是在某些情况下，可以以不同于此处的顺序执行所示出或描述的步骤。

[0045] 本发明至少一个实施例中，访问权限的管理是基于域(Domain)以及域簇(DomainGroup)来进行的，其中，

[0046] 域，为系统中一个访问规则的空间。所有被分配到该空间的主机以及设备遵循相同的访问规则。该空间的规则只能被该空间内或者上层的管理器控制，不受其他域管理器控制。

[0047] 域簇，为系统中多个访问规则空间的集合。所有被分配到该空间的主机以及设备可以被域簇管理器分配到域簇内的各个域空间当中。

[0048] 实施例1

[0049] 图1为根据本发明的层次化的系统防火墙结构框图，如图1所示，本发明的层次化的系统防火墙，包括，根安全管理器10、二级安全管理器20、防火墙控制器30、域标识生成器40，以及多个防火墙50，其中，

[0050] 根安全管理器(Root Security Manager)10，其为每一个域簇指定二级安全管理器(2nd Level Security Manger)20、分配主机(Master)、设备(Slave)资源，以及域资源；为域簇之间提供初始的防火墙配置方案，例如完全隔离。

[0051] 本发明的一个实施例中，根安全管理器10将系统资源(包括主机、设备以及域资源)根据应用需求分配到不同域簇中，并为域簇之间提供完全隔离防火墙配置方案。

[0052] 二级安全管理器(2nd Level Security Manager)20，其为所属域簇中所有的主机以及设备添加域标识符，并为本域簇中各个域提供防火墙配置方案。该防火墙配置方案，为当前域簇中不同域的主机对指定的域中的设备访问权限的设置。

[0053] 本发明的一个实施例中，二级安全管理器20根据自身的安全需求，将所属域簇中的主机和设备资源分配到不同的域之中，并为本域簇中各个域提供防火墙配置方案。

[0054] 防火墙控制器(FWC)30，其为系统中的主机以及设备添加域簇标识号和二级安全管理器的标识；为当前域簇中的主机和设备分配域标识；为当前域簇中每一个设备端的防火墙进行访问权限的配置，包括，

[0055] 1)为不同域簇以及该域簇中不同域针对当前设备的访问权限进行不同的设置；

[0056] 2)访问权限的类型在不同的系统中可能略有不同，主要包括：

[0057] 是否允许读访问；

[0058] 是否允许写访问；

[0059] 是否允许安全的读访问；

[0060] 是否允许安全的写访问；

[0061] 是否允许特权模式的读访问；

[0062] 是否允许特权模式的写访问。

[0063] 本发明的一个实施例中，防火墙控制器30，在初始状态下依据根安全管理器10的配置，为系统中的主机以及设备添加域簇标识号和二级安全管理器的标识；在根安全管理器10的配置结束后，接受根安全管理器10或者二级安全管理器20的配置，为当前域簇中的主机以及设备分配域标识；接受根安全管理器10或者二级安全管理器20的配置，为当前域簇中每一个设备端的防火墙进行访问权限的配置。

[0064] 所述访问权限的配置，可基于当前访问的主机的域簇标识符或域标识符、访问的读写类型、是否为安全的访问或是否为特权模式的访问等。

[0065] 域标识生成器(DIDA)40，其为系统中的每一个主机生成域簇标识和域标识。

[0066] 本发明的一个实施例中，域标识生成器40，根据根安全管理器10的配置，为系统中的每一个主机和设备生成域簇标识；根据根安全管理器10和二级安全管理器20的配置，为系统中的每一个主机生成域标识。

[0067] 防火墙(Firewall)50，其为来自不同域或不同域簇的主机对当前设备的访问进行权限控制。所述访问权限的控制，可基于当前访问的主机的域簇标识符或域标识符、访问的读写类型、是否为安全的访问或是否为特权模式的访问等。

[0068] 本发明的一个实施例中，防火墙50根据根安全管理器10或二级安全管理器20的配置，为来自不同域或不同域簇的主机对当前设备的访问进行权限控制。

[0069] 实施例2

[0070] 图2为根据本发明的层次化的系统防火墙配置方法流程图，下面将参考图2，对本发明的层次化的系统防火墙配置方法进行详细描述。

[0071] 首先，在步骤201，为每一个域簇分配系统资源，并指定二级安全管理器。

[0072] 本发明的一个实施例中，根安全管理器10为每一个域簇分配主机、设备资源，以及域资源，同时为每一个域簇指定二级安全管理器20。

[0073] 在步骤202，为系统中的主机和设备添加域簇标识号、为二级安全管理器添加标识，为域簇之间提供初始的防火墙配置方案。

[0074] 本发明的一个实施例中，防火墙控制器30根据根安全管理器10的配置，为系统中的每一个主机和设备添加域簇标识、为二级安全管理器的标识；根安全管理器10为域簇之间提供完全隔离的防火墙配置方案。

[0075] 在步骤203，为域簇中的主机和设备添加域标识符后分配到不同域中，并为每个域提供防火墙配置方案。

[0076] 本发明的一个实施例中，防火墙控制器30接受根安全管理器10或者二级安全管理器20的配置，为当前域簇中的主机以及设备分配域标识；二级安全管理器20根据自身安全的需求，为域簇所有的主机以及设备添加域标识符，并为每个域提供防火墙配置方案。

[0077] 在步骤204，为当前域簇中每一个设备端的防火墙进行访问权限的配置。

[0078] 本发明的一个实施例中，防火墙控制器30接受根安全管理器10或者二级安全管理

器20的配置,为当前域簇中每一个设备端的防火墙进行访问权限的配置。

[0079] 在步骤205,为来自不同域或不同域簇的主机对当前设备的访问进行权限控制。

[0080] 本发明的一个实施例中,防火墙50根据根安全管理器10或二级安全管理器20的配置,为来自不同域或不同域簇的主机对当前设备的访问进行权限控制。所述访问权限的控制,可基于当前访问的主机的域簇标识符或域标识符、访问的读写类型、是否为安全的访问或是否为特权模式的访问等。

[0081] 本发明一实施例提供一种计算机可读存储介质,所述计算机可读存储介质存储有程序,所述程序可被处理器执行,以实现任一实施例所述的层次化的系统防火墙配置方法的步骤。

[0082] 所述计算机可读存储介质包括:U盘、只读存储器(ROM,Read-Only Memory)、随机存取存储器(RAM,Random Access Memory)、移动硬盘、磁碟或者光盘等各种可以存储程序代码的介质。

[0083] 应用实例

[0084] 以下通过应用示例对本发明实施例进行清楚详细的说明,应用示例中仅以系统运行两个操作系统为例进行陈述本发明,并不用于限定本发明的保护范围,例如系统在运行多个操作系统时,同样可以采用本发明构建多层次的系统防火墙。

[0085] 本发明的一个应用示例中,一个虚拟化的系统同时运行了两个操作系统OS_A(例如安卓系统)和OS_B(例如FreeRTOS):

[0086] 初始化的过程当中,根安全管理器(例如一级启动的处理器),将系统资源(包括主机、设备以及域资源)根据应用需求分配到两个域簇DomainGroup_A(为OS_A使用)和DomainGroup_B(为OS_B使用)当中,同时为两个域簇指定二级安全管理器(例如两个操作系统的启动处理器CPU_A和CPU_B);

[0087] 初始化完成后,各个操作系统各自启动后,其二级安全管理器(启动处理器),根据自身的安全需求,将该域簇当中的主机和设备资源分配到不同的域之中,同时为分属于不同域的设备的防火墙设置访问策略。

[0088] 设置完成后,系统域、主机、设备以及访问策略的配置如表格一。表格中R/W表示支持读写访问;R表示只支持读访问;W表示只支持写访问;表格中SR/SW表示支持安全的读写访问;SR表示只支持安全的读访问;SW表示只支持安全的写访问;“-”表示读写访问均不支持。本例中只列举了几种常见的访问策略。

[0089] 表格一

[0090]

域簇编号			域簇A （安卓系统）				域簇B （FreeRTOS）		
		主机	CPU_A	CMOS传感器	人脸识别单元	显示控制器	CPU_B	加密引擎	以太网控制器
	设备	域编号	0	1	2	0	8	9	10
域簇A	内存0	0	R/W	R/W	R/W	R/W	-	-	-
	内存1	1	SR/SW	-	-	SR	-	-	-
	内存2	2	-	W	R	-	-	-	-
域簇B	内存3	8	-	-	-	-	R/W	R/W	R/W
	内存4	9	-	-	-	-	SW	R/W	-
	内存5	10						W	R

[0091] 根据设置，安卓系统以及FreeRTOS系统进行了完全的隔离，即两个系统中的主机都不能访问对方的设备。

[0092] 1、安卓系统中

[0093] 1)域0为普通的非安全域；

[0094] 2)域1为安全域，如密码键盘应用运行于此域。CPU_A通过安全的访问在内存1中绘制乱序的密码键盘，显示控制器安全的访问将内存1中的密码键盘读出并显示。由于系统中别的主机均不能访问密码键盘的内容，用户输入的密码得以保护；

[0095] 3)域2为另外一个安全域。该域用于人脸解锁应用。初始状态下用户通过CMOS传感器模块将人脸特征录入内存2当中；当人脸识别启动后，人脸识别模块读取CMOS传感器模块写入内存0的人脸数据同时于内存2中的人脸特征数据进行比对来判断是否解锁。由于只有人脸识别单元能读取内存2中的人脸特征数据，人脸特征数据的安全性得到了保证。

[0096] 2、FreeRTOS系统中

[0097] 1)域8为普通的非安全域；

[0098] 2)域9为安全域，在加密通信的应用中CPU_B通过安全的访问将明文写入内存4当中；加密引擎将内存4中的明文读出并且进行加密产生密文存储于内存5当中；以太网控制器将密文从内存5读出而后进行传输；

[0099] 3)在此过程当中只有加密引擎能够读取明文，明文的信息安全得到了保证。

[0100] 由于本发明实施例中采用了层次化的控制结构，各个操作系统可独立维护自己安全策略，各个操作系统安全策略的开发得以简化；各个操作系统在运行时与根安全管理器

的交互大大减少，简化了根安全管理器的设计；各个操作系统安全策略的耦合性大大降低，操作系统见得干扰得以大大降低，系统的整体安全性得以提升。

[0101] 本领域普通技术人员可以理解：以上所述仅为本发明的优选实施例而已，并不用于限制本发明，尽管参照前述实施例对本发明进行了详细的说明，对于本领域的技术人员来说，其依然可以对前述各实施例记载的技术方案进行修改，或者对其中部分技术特征进行等同替换。凡在本发明的精神和原则之内，所作的任何修改、等同替换、改进等，均应包含在本发明的保护范围之内。

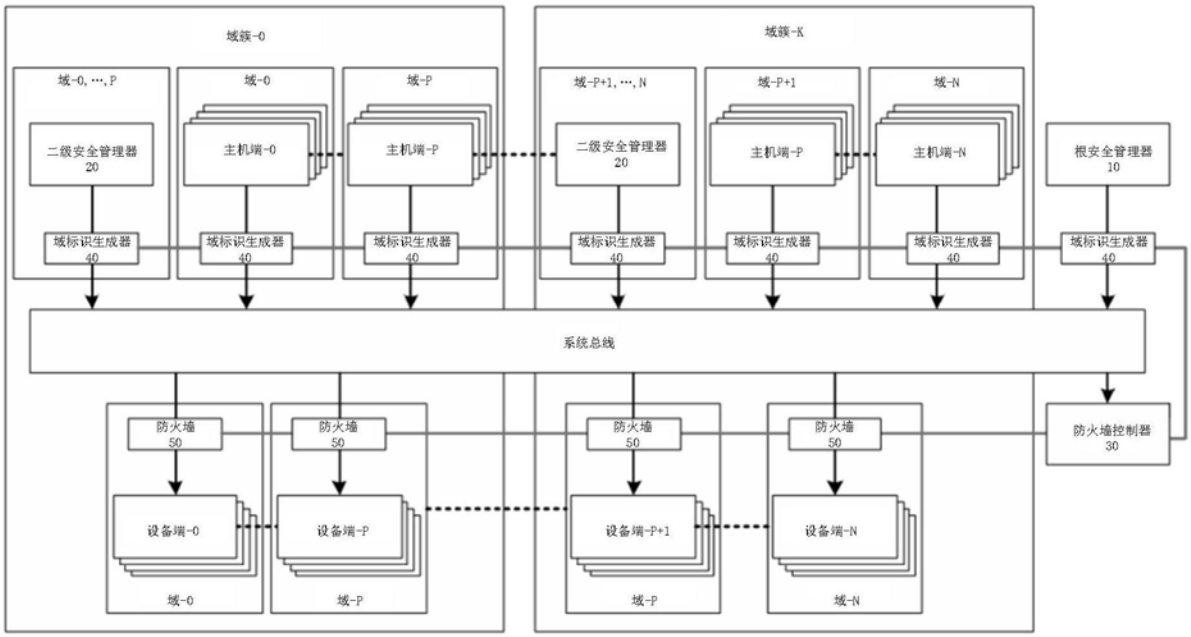

域簇-0
域簇-K
域-0,…,P
域-0
域-P
域-P+1,…,N
域-P+1
域-N
二级安全管理器 20
主机端-0
主机端-P
二级安全管理器 20
主机端-P
主机端-N
根安全管理器 10
域标识生成器 40
域标识生成器 40
域标识生成器 40
域标识生成器 40
域标识生成器 40
域标识生成器 40
域标识生成器 40
系统总线
防火墙 50
防火墙 50
防火墙 50
防火墙 50
防火墙控制器 30
设备端-0
设备端-P
设备端-P+1
设备端-N
域-0
域-P
域-P
域-N

图1

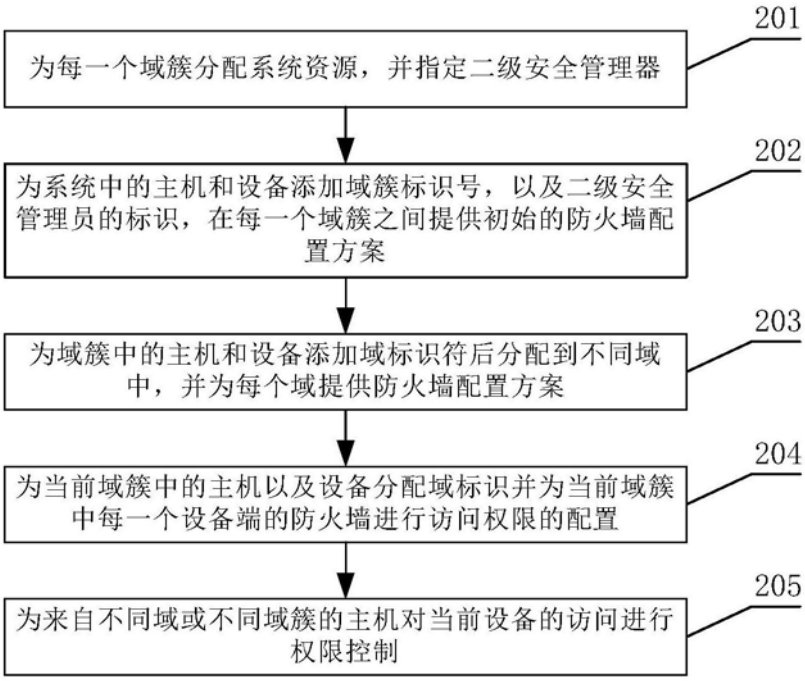

201
为每一个域簇分配系统资源，并指定二级安全管理器
202
为系统中的主机和设备添加域簇标识号，以及二级安全管理员的标识，在每一个域簇之间提供初始的防火墙配置方案
203
为域簇中的主机和设备添加域标识符后分配到不同域中，并为每个域提供防火墙配置方案
204
为当前域簇中的主机以及设备分配域标识并为当前域簇中每一个设备端的防火墙进行访问权限的配置
205
为来自不同域或不同域簇的主机对当前设备的访问进行权限控制

图2