

(12) 按照专利合作条约所公布的国际申请

(19) 世界知识产权组织
国际局

(43) 国际公布日
2025 年 6 月 5 日 (05.06.2025)



(10) 国际公布号
WO 2025/112463 A1

(51) 国际专利分类号:
G06F 11/00 (2006.01) **G06F 9/4401** (2018.01)

(21) 国际申请号: PCT/CN2024/099921

(22) 国际申请日: 2024 年 6 月 18 日 (18.06.2024)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
202311628371.X 2023年11月30日 (30.11.2023) CN

(71) 申请人: 苏州元脑智能科技有限公司 (SUZHOU METABRAIN INTELLIGENT TECHNOLOGY CO., LTD.) [CN/CN]; 中国江苏省苏州市吴中经济开发区郭巷街道官浦路1号9幢 215000 (CN)。

(72) 发明人: 孙秀强 (SUN, Xiuqiang); 中国江苏省苏州市吴中经济开发区郭巷街道官浦路1号9幢 215000 (CN)。 韩国志 (HAN, Guozhi); 中国江苏省苏州市吴中经济开发区郭巷街道官浦路1

号9幢 215000 (CN)。 刘宝俊 (LIU, Baojun); 中国江苏省苏州市吴中经济开发区郭巷街道官浦路1号9幢 215000 (CN)。 艾山彬 (AI, Shanbin); 中国江苏省苏州市吴中经济开发区郭巷街道官浦路1号9幢 215000 (CN)。

(74) 代理人: 北京润泽恒知识产权代理有限公司 (BEIJING RUN ZEHENG INTELLECTUAL PROPERTY LAW FIRM); 中国北京市海淀区中关村南大街甲 18 号北京国际 C 座 6 层 606 100081 (CN)。

(81) 指定国(除另有指明, 要求每一种可提供的国家保护): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CV, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IQ, IR, IS, IT, JM, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, MG, MK, MN, MU, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD,

(54) Title: ARM SECURITY FIRMWARE CONFIGURATION METHOD AND APPARATUS APPLIED TO ARM SERVER

(54) 发明名称: 应用于ARM服务器的ARM安全固件配置方法及装置

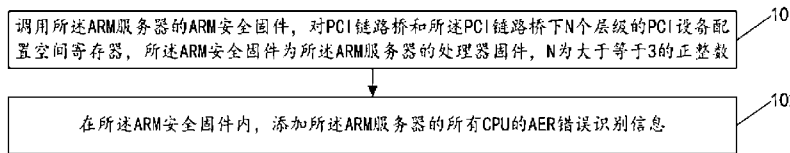


图 1

- 101 Call an ARM security firmware of an ARM server to configure a space register for a PCI link bridge and PCI devices of N levels under the PCI link bridge, wherein the ARM security firmware is a processor firmware of the ARM server, and N is a positive integer greater than or equal to 3
- 102 Add, in the ARM security firmware, AER error identification information of all CPUs of the ARM server

(57) Abstract: The present application provides an ARM security firmware configuration method and apparatus applied to an ARM server. The method comprises: calling an ARM security firmware of an ARM server to configure a space register for a PCI link bridge and PCI devices of N levels under the PCI link bridge, wherein the ARM security firmware is a processor firmware of the ARM server, and N is a positive integer greater than or equal to 3; and adding, in the ARM security firmware, AER error identification information of all CPUs of the ARM server. The embodiments of the present application can effectively solve the problem of down caused by restart of a DPU virtual cloud system or restart of PCI devices in the DPU virtual cloud system.

(57) 摘要: 本申请提供了一种应用于ARM服务器的ARM安全固件配置方法及装置。所述方法包括: 调用所述ARM服务器的ARM安全固件, 对PCI链路桥和所述PCI链路桥下N个层级的PCI设备配置空间寄存器, 所述ARM安全固件为所述ARM服务器的处理器固件, N为大于等于3的正整数; 在所述ARM安全固件内, 添加所述ARM服务器的所有CPU的AER错误识别信息。本申请实施例可以有效解决DPU虚拟云盘系统下重启或者DPU虚拟云盘系统下重启PCI设备宕机的问题。

SE, SG, SK, SL, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ,
UA, UG, US, UZ, VC, VN, WS, ZA, ZM, ZW。

- (84) 指定国(除另有指明，要求每一种可提供的地区
保护): ARIPO (BW, CV, GH, GM, KE, LR, LS, MW, MZ,
NA, RW, SC, SD, SL, ST, SZ, TZ, UG, ZM, ZW), 欧亚
(AM, AZ, BY, KG, KZ, RU, TJ, TM), 欧洲 (AL, AT, BE,
BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR,
HU, IE, IS, IT, LT, LU, LV, MC, ME, MK, MT, NL, NO,
PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF,
CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN,
TD, TG)。

本国际公布:

- 包括国际检索报告(条约第21条(3))。

应用于 ARM 服务器的 ARM 安全固件配置方法及装置

相关申请的交叉引用

本申请要求于 2023 年 11 月 30 日提交中国专利局，申请号为 202311628371.X，申请名称为“应用于 ARM 服务器的 ARM 安全固件配置方法及装置”的中国专利申请的优先权，其全部内容通过引用结合在本申请中。

技术领域

本申请涉及芯片技术领域，尤其涉及一种应用于 ARM 服务器的 ARM 安全固件配置方法及装置。

背景技术

互联网客户采购 ARM (Advanced RISC Machines) 服务器除了支持替换传统 X86 服务器的存储功能、云业务外，也支持 AI (Artificial Intelligence, 人工智能) 领域的功能替换，如基于 ARM 服务器搭配 T4 卡和 DPU (Graphics Processing Unit, 图形处理器) 卡进行物理组合的配置。在此种配置前提下，客户习惯将 DPU 设备的硬盘进行虚拟云盘安装，同时，将 ARM 服务器的所有 PCI 外设设备都在 DPU 的虚拟云盘系统中进行初始化使用，因 DPU 可以支持多个虚拟云盘的安装及使用，这就导致 ARM 服务器中的 PCI 外设设备可随时被不同的云盘系统所使用。在一个云盘系统中使用完毕时，需要对此 PCI 设备如 T4 卡进行重启，当 T4 卡重启完成后另外一个云盘系统才能正常使用这张物理 T4 卡。

然而，在 ARM 服务器的云盘系统下重启时会出现宕机导致云盘系统下的 T4 卡无法进行重启且整个 ARM 服务器也宕机无法正常使用。

发明内容

本申请实施例提供一种应用于 ARM 服务器的 ARM 安全固件配置方法及装置，以解决相关技术中在 ARM 服务器的云盘系统下重启时会出现宕机导致云盘系统下的 T4 卡无法进行重启且整个 ARM 服务器也宕机无法正常使用的问题。

为了解决上述技术问题，本申请实施例是这样实现的：

第一方面，本申请实施例提供了一种应用于 ARM 服务器的 ARM 安全固件配置方法，方法包括：

调用 ARM 服务器的 ARM 安全固件，对 PCI 链路桥和 PCI 链路桥下 N 个层级的 PCI 设备配置空间寄存器，ARM 安全固件为 ARM 服务器的处理器固件，N 为大于等于 3 的正整数；

在 ARM 安全固件内，添加 ARM 服务器的所有 CPU 的 AER 错误识别信息。

在一些实施例中，调用 ARM 服务器的 ARM 安全固件，对 PCI 链路桥和 PCI 链路桥下 N 个层级的 PCI 设备配置空间寄存器，包括：

在 ARM 安全固件加载启动过程中，调用 ARM 安全固件，对所有 CPU 进行 PCI 链路桥及 N 个层级的 PCI 设备扫描，得到扫描结果；

在扫描结果指示 PCI 链路桥下存在 N 个层级的 PCI 设备的情况下，对 PCI 链路桥下 N 个层级的 PCI 设备配置空间寄存器。

在一些实施例中，对 PCI 链路桥下 N 个层级的 PCI 设备配置空间寄存器，包括：

对 PCI 链路桥下 N 个层级的 PCI 设备进行初始化；

对PCI链路桥下N个层级的PCI设备配置空间寄存器。

在一些实施例中，在调用ARM安全固件，对所有CPU进行PCI链路桥及N个层级的PCI设备扫描，得到扫描结果之前，包括：

响应于ARM服务器启动且BIOS加载成功，加载ARM安全固件；

对ARM安全固件进行安全启动校验；

响应于ARM安全固件安全启动校验成功，对ARM安全固件进行内存初始化。

在一些实施例中，调用ARM安全固件，对所有CPU进行PCI链路桥及N个层级的PCI设备扫描，得到扫描结果，包括：

响应于ARM安全固件内存初始化完成，调用ARM安全固件，对所有CPU进行PCI链路桥及N个层级的PCI设备扫描，得到扫描结果；

在初始化的内存中配置PCI链路桥对应的PCI配置空间。

在一些实施例中，调用ARM安全固件，对所有CPU进行PCI链路桥及N个层级的PCI设备扫描，还包括：

根据PCI链路桥的拆分情况对PCI链路桥及N个层级的PCI设备进行扫描。

在一些实施例中，对PCI链路桥下N个层级的PCI设备配置空间寄存器，包括：

在PCI配置空间内，对PCI链路桥下N个层级的PCI设备分别配置空间寄存器。

在一些实施例中，在调用ARM安全固件，对所有CPU进行PCI链路桥及N个层级的PCI设备扫描，得到扫描结果之后，还包括：

在扫描结果指示PCI链路桥下的PCI设备的层级小于N的情况下，在PCI配置空间内预留PCI链路桥对应的寄存器配置空间。

在一些实施例中，在PCI配置空间内预留PCI链路桥对应的寄存器配置空间之后，还包括：

在预留的寄存器配置空间内对后续接入的N个层级的PCI设备配置空间寄存器。

在一些实施例中，在ARM安全固件内，添加ARM服务器的所有CPU的AER错误识别信息，包括：

获取ARM服务器的所有CPU下的链路桥，及所有CPU下的链路桥下的所有PCI设备；

在ARM安全固件内，添加所有CPU下的链路桥下的所有PCI设备的AER错误识别信息。

在一些实施例中，在ARM安全固件内，添加所有CPU下的链路桥下的所有PCI设备的AER错误识别信息，包括：

获取所有CPU下的链路桥的AER配置信息；

在ARM安全固件内，基于AER配置信息，对所有CPU下的链路桥下的所有PCI设备进行初始化，以添加AER错误识别信息。

在一些实施例中，在添加ARM服务器的所有CPU的AER错误识别信息之后，还包括：

检测ARM安全固件下的所有PCI链路桥下的PCI设备是否均配置完成；

响应于所有PCI链路桥下的PCI设备均配置完成，启动ARM服务器的UEFI固件，并启动加载虚拟云盘系统。

在一些实施例中，在检测ARM安全固件下的所有PCI链路桥下的PCI设备是否均配置完成之后，还包括：

响应于所有PCI链路桥下的PCI设备存在未配置的PCI链路桥，获取未配置的PCI链路桥

下的PCI设备；

依次对未配置的PCI链路桥和未配置的PCI链路桥下的PCI设备进行寄存器配置和AER错误识别信息的添加。

在一些实施例中，在启动ARM服务器的UEFI固件，并启动加载虚拟云盘系统之后，还包括：

在重启PCI设备和重启虚拟云盘系统的情况下，确定ARM服务器是否出现宕机现象；
响应于ARM服务器未出现宕机现象，确定ARM安全固件配置成功。

在一些实施例中，在重启PCI设备和重启虚拟云盘系统的情况下，确定ARM服务器是否出现宕机现象，包括：

当PCI设备未出现重启宕机问题，以及虚拟云盘操作系统也未出现重启宕机问题，则确定ARM服务器未出现宕机现象。

在一些实施例中，在确定ARM服务器是否出现宕机现象之后，还包括：
响应于ARM服务器出现宕机现象，输出宕机报警信息。

在一些实施例中，ARM服务器至少包括一个CPU。

第二方面，本申请实施例提供了一种应用于ARM服务器的ARM安全固件配置装置，装置包括：

寄存器配置模块，用于调用ARM服务器的ARM安全固件，对PCI链路桥和PCI链路桥下N个层级的PCI设备配置空间寄存器，ARM安全固件为ARM服务器的处理器固件，N为大于等于3的正整数；

AER信息添加模块，用于在ARM安全固件内，添加ARM服务器的所有CPU的AER错误识别信息。

在一些实施例中，寄存器配置模块包括：

扫描结果获取单元，用于在ARM安全固件加载启动过程中，调用ARM安全固件，对所有CPU进行PCI链路桥及N个层级的PCI设备扫描，得到扫描结果；

空间寄存器配置单元，用于在扫描结果指示PCI链路桥下存在N个层级的PCI设备的情况下，对PCI链路桥下N个层级的PCI设备配置空间寄存器。

在一些实施例中，空间寄存器配置单元包括：

PCI设备初始化子单元，用于对PCI链路桥下N个层级的PCI设备进行初始化；

空间寄存器配置子单元，用于对PCI链路桥下N个层级的PCI设备配置空间寄存器。

在一些实施例中，装置包括：

ARM安全固件加载模块，用于响应于ARM服务器启动且BIOS加载成功，加载ARM安全固件；

安全启动校验模块，用于对ARM安全固件进行安全启动校验；

内存初始化模块，用于响应于ARM安全固件安全启动校验成功，对ARM安全固件进行内存初始化。

在一些实施例中，扫描结果获取单元包括：

扫描结果获取子单元，用于响应于ARM安全固件内存初始化完成，调用ARM安全固件，对所有CPU进行PCI链路桥及N个层级的PCI设备扫描，得到扫描结果；

PCI配置空间配置子单元，用于在初始化的内存中配置PCI链路桥对应的PCI配置空间。

在一些实施例中，空间寄存器配置单元包括：

寄存器配置子单元，用于在PCI配置空间内，对PCI链路桥下N个层级的PCI设备分别配置空间寄存器。

在一些实施例中，装置还包括：

配置空间预留模块，用于在扫描结果指示PCI链路桥下的PCI设备的层级小于N的情况下，在PCI配置空间内预留PCI链路桥对应的寄存器配置空间。

在一些实施例中，AER信息添加模块包括：

PCI设备获取单元，用于获取ARM服务器的所有CPU下的链路桥，及所有CPU下的链路桥下的所有PCI设备；

AER信息添加单元，用于在ARM安全固件内，添加所有CPU下的链路桥下的所有PCI设备的AER错误识别信息。

在一些实施例中，AER信息添加单元包括：

配置信息获取子单元，用于获取所有CPU下的链路桥的AER配置信息；

AER信息添加子单元，用于在ARM安全固件内，基于AER配置信息，对所有CPU下的链路桥下的所有PCI设备进行初始化，以添加AER错误识别信息。

在一些实施例中，装置还包括：

配置完成检测模块，用于检测ARM安全固件下的所有PCI链路桥下的PCI设备是否均配置完成；

虚拟云盘系统加载模块，用于响应于所有PCI链路桥下的PCI设备均配置完成，启动ARM服务器的UEFI固件，并启动加载虚拟云盘系统。

在一些实施例中，装置还包括：

未配置设备获取模块，用于响应于所有PCI链路桥下的PCI设备存在未配置的PCI链路桥，获取未配置的PCI链路桥下的PCI设备；

PCI设备配置模块，用于依次对未配置的PCI链路桥和未配置的PCI链路桥下的PCI设备进行寄存器配置和AER错误识别信息的添加。

在一些实施例中，装置还包括：

宕机现象确定模块，用于在重启PCI设备和重启虚拟云盘系统的情况下，确定ARM服务器是否出现宕机现象；

配置成功确定模块，用于响应于ARM服务器未出现宕机现象，确定ARM安全固件配置成功。

第三方面，本申请实施例提供了一种电子设备，包括：

存储器、处理器及存储在存储器上并可在处理器上运行的计算机程序，计算机程序被处理器执行时实现上述任一项的应用于ARM服务器的ARM安全固件配置方法。

第四方面，本申请实施例提供了一种计算机非易失性可读存储介质，当所述存储介质中的指令由电子设备的处理器执行时，使得电子设备能够执行上述任一项的应用于ARM服务器的ARM安全固件配置方法。

在本申请实施例中，通过调用ARM服务器的ARM安全固件，对PCI链路桥和PCI链路桥下N个层级的PCI设备配置空间寄存器，ARM安全固件为ARM服务器的处理器固件，N为大于等于3的正整数。在ARM安全固件内，添加ARM服务器的所有CPU的AER错误识别信息。

本申请实施例通过增加PCI链路桥及PCI设备在ATF固件中的扫描层级并配置寄存器设置，同时，无论是单路还是双路服务器都需要在ATF中增加所有CPU的每个PCI链路桥及PCI设备添加AER错误信息识别功能，可以有效解决DPU虚拟云盘系统下重启或者DPU虚拟云盘系统下重启PCI设备宕机的问题。

上述说明仅是本申请技术方案的概述，为了能够更清楚了解本申请的技术手段，而可依照说明书的内容予以实施，并且为了让本申请的上述和其它目的、特征和优点能够更明显易懂，以下特举本申请的具体实施方式。

附图说明

为了更清楚地说明本申请实施例的技术方案，下面将对本申请实施例的描述中所需要使用的附图作简单地介绍，显而易见地，下面描述中的附图仅仅是本申请的一些实施例，对于本领域普通技术人员来讲，在不付出创造性劳动的前提下，还可以根据这些附图获得其他的附图。

图1为本申请实施例提供的一种应用于ARM服务器的ARM安全固件配置方法的步骤流程图；

图2为本申请实施例提供的一种空间寄存器配置方法的步骤流程图；

图3为本申请实施例提供的另一种空间寄存器配置方法的步骤流程图；

图4为本申请实施例提供的一种ARM安全固件启动方法的步骤流程图；

图5为本申请实施例提供的一种PCI配置空间配置方法的步骤流程图；

图6为本申请实施例提供的一种AER错误识别信息添加方法的步骤流程图；

图7为本申请实施例提供的另一种AER错误识别信息添加方法的步骤流程图；

图8为本申请实施例提供的一种PCI设备配置方法的步骤流程图；

图9为本申请实施例提供的一种ARM安全固件配置成功确定方法的步骤流程图；

图10为本申请实施例提供的一种ARM服务器支持系统下重启PCI设备的流程图；

图11为本申请实施例提供的一种硬件架构的示意图；

图12为本申请实施例提供的一种应用于ARM服务器的ARM安全固件配置装置的结构示意图；

图13为本申请实施例提供的一种电子设备的结构示意图。

具体实施方式

ARM架构处理器固件可以划分为两个部分，一部分是ARM架构独有的ATF（Arm Trusted Firmware，ARM安全固件）固件，另一部分是传统的UEFI固件，UEFI固件是任何架构处理器都需要支持且各种规范协议均统一，而ATF固件则是ARM架构独有的固件，ATF固件涉及ARM的安全启动校验、内存初始化、PCI（Peripheral Component Interconnect，外设部件互连标准）链路的初始化及热插拔等PCI设备的基本功能的支持，在ATF固件中对PCI链路的初始化涉及到了一层级，即对CPU（Central Processing Unit，中央处理器）的PCI链路的根桥、根桥下的PCI设备进行初始化，而在ARM服务器的DPU（Data Processing Unit，数据处理器）虚拟系统中，T4卡是在DPU虚拟云盘的系统下属于PCI设备下的二级层级的PCI设备，而不是ARM系统下的PCI链路桥下的一级PCI设备，这就导致在ARM服务器系统下非DPU虚拟云盘系统下重启T4卡是无任何宕机问题的，但是在ARM系统下的DPU虚拟云盘系统下重启T4卡则会出现宕机问题，这是T4卡在不同系统下的PCI设备层级不同，ATF的初始

化并未考虑到二级甚至三级层级的PCI重启设置的需求，此时，需要对ATF进行多级PCI设备初始化及寄存器设置使能。除了在ATF中增加PCI链路初始化层级外，还需要添加PCI设备的AER识别功能，若未添加的话则会产生AER（Advanced Error Reporting，高级错误报告）报错导致系统继续宕机，因为ARM服务器既支持单路启动也支持双路启动，若只在ATF中添加单路即CPU0的PCI AER错误识别信息的话在单路或者双路启动时使用重启T4卡设备仍旧会报错，故需要在ATF中添加双路启动时的PCI AER错误识别信息设定才行，在此基础上进行单路或者双路启动后在DPU的虚拟云盘系统下进行T4卡的重启设置则不会出现AER宕机问题，故基于上述ATF固件中的两处调整方可解决ARM服务器DPU虚拟云盘系统下重启PCI设备宕机的技术问题。

接下来，结合具体实施例对本申请实施例的技术方案进行如下详细描述。

参照图1，示出了本申请实施例提供的一种应用于ARM服务器的ARM安全固件配置方法的步骤流程图，如图1所示，该应用于ARM服务器的ARM安全固件配置方法可以包括：步骤101和步骤102。

步骤101：调用ARM服务器的ARM安全固件，对PCI链路桥和PCI链路桥下N个层级的PCI设备配置空间寄存器，ARM安全固件为ARM服务器的处理器固件，N为大于等于3的正整数。

本申请实施例可以应用于在ARM安全固件部分将CPU的PCI链路及PCI设备的扫描层级增多至多级，并将所有CPU的PCI链路桥及PCI设备添加AER错误信息识别功能，以解决系统下重启PCI设备或者系统重启时的宕机问题的场景中。

本申请实施例可以应用于ARM服务器，即执行主体为ARM服务器，其中，ARM服务器可以包括：BIOS（Basic Input Output System，基本输入输出系统），在BIOS内设置有ARM安全固件（即ATF（固件）和UEFI固件）。

在具体实现中，在ARM服务器开机启动之后，可以率先加载BIOS，然后可以加载ARM安全固件，并在ARM安全固件加载启动过程中，通过ARM安全固件对PCI链路桥和PCI链路桥下的N个层级的PCI设备配置空间寄存器。其中，N为大于等于3的正整数。

在具体实现中，可以在ARM安全固件加载启动过程中，调用ARM安全固件对所有CPU（即ARM服务器内所有的CPU，可以为单个CPU，也可以为多个CPU）进行PCI链路桥及多层级PCI设备扫描，并对扫描得到的多层级PCI设备进行空间寄存器配置。对于该实现过程可以结合图2进行如下详细描述。

参照图2，示出了本申请实施例提供的一种空间寄存器配置方法的步骤流程图。如图2所示，该空间寄存器配置方法可以包括：步骤201和步骤202。

步骤201：在ARM安全固件加载启动过程中，调用ARM安全固件，对所有CPU进行PCI链路桥及N个层级的PCI设备扫描，得到扫描结果。

在本实施例中，在加载BIOS之后，可以加载ARM安全固件，并在ARM安全固件加载启动过程中，调用ARM安全固件对所有CPU进行PCI链路桥及N个层级的PCI设备扫描，得到扫描结果。具体地，可以通过ARM安全固件扫描CPU下的所有链路桥，以及每个链路桥下的N个层级的PCI设备，从而得到扫描结果。

在具体实现中，在进行安全扫描时，可以先加载ARM安全固件并进行安全启动检验和内存初始化，然后再进行扫描。对于该实现过程可以结合图4进行如下详细描述。

参照图4，示出了本申请实施例提供的一种PCI配置空间配置方法的步骤流程图。如图4所示，该PCI配置空间配置方法可以包括：步骤401、步骤402和步骤403。

步骤401：加载ARM安全固件。

在本实施例中，在加载BIOS之后，可以加载ARM安全固件。

在加载ARM安全固件之后，执行步骤402。

步骤402：对ARM安全固件进行安全启动校验。

在加载ARM安全固件之后，可以对ARM安全固件进行安全启动的校验，以校验ARM安全固件是否安全启动。若ARM安全固件未安全启动，则结束。若ARM安全固件安全启动，则执行步骤403。

步骤403：响应于ARM安全固件安全启动校验成功，对ARM安全固件进行内存初始化。

在ARM安全固件安全启动校验成功之后，可以对ARM安全固件进行内存初始化，以为ARM安全固件配置内存空间，以便于后续空间寄存器的配置。

在完成上述安全校验和内存初始化之后，则可以调用ARM安全固件执行扫描流程，同时，可以配置PCI链路桥对应的PCI配置空间，以为后续的空间寄存器的配置提供内存。对于该实现过程可以结合图5进行如下详细描述。

参照图5，示出了本申请实施例提供的一种PCI配置空间配置方法的步骤流程图。如图5所示，该PCI配置空间配置方法可以包括：步骤501和步骤502。

步骤501：响应于ARM安全固件内存初始化完成，调用ARM安全固件，对所有CPU进行PCI链路桥及N个层级的PCI设备扫描，得到扫描结果。

在本申请实施例中，在对ARM安全固件内存初始化完成之后，可以调用ARM安全固件对所有CPU进行PCI链路桥及N个层级的PCI设备扫描，得到扫描结果。

步骤502：在初始化的内存中配置PCI链路桥对应的PCI配置空间。

然后，可以在初始的内存中配置PCI链路桥对应的PCI配置空间，该PCI配置空间可以用于进行后续的PCI设备的空间寄存器的配置。

在调用ARM安全固件对所有CPU进行PCI链路桥及N个层级的PCI设备扫描，得到扫描结果之后，执行步骤202。

步骤202：在扫描结果指示PCI链路桥下存在N个层级的PCI设备的情况下，对PCI链路桥下N个层级的PCI设备配置空间寄存器。

在调用ARM安全固件对所有CPU进行PCI链路桥及N个层级的PCI设备扫描，得到扫描结果之后，在扫描结果指示PCI链路桥下存在N个层级的PCI设备的情况下，则可以对PCI链路桥下N个层级的PCI设备配置空间寄存器。具体地，可以对PCI链路桥下N个层级的PCI设备进行初始化，并配置空间寄存器。对于该实现过程可以结合图3进行如下详细描述。

参照图3，示出了本申请实施例提供的另一种空间寄存器配置方法的步骤流程图。如图3所示，该控件寄存器配置方法可以包括：步骤301和步骤302。

步骤301：对PCI链路桥下N个层级的PCI设备进行初始化。

在本实施例中，在扫描结果指示PCI链路桥下存在N个层级的PCI设备的情况下，则可以对PCI链路桥下N个层级的PCI设备进行初始化。

步骤302：对PCI链路桥下N个层级的PCI设备配置空间寄存器。

在初始化的过程中，可以对PCI链路桥下N个层级的PCI设备配置空间寄存器。即对PCI

设备的初始过程可以将空间寄存器写入对应的空间内。

本申请通过对ATF进行多级PCI设备初始化及寄存器设置使能，可以解决在ARM服务器系统下DPU虚拟云盘系统下重启PCI设备出现宕机的问题。

在对PCI链路桥下N个层级的PCI设备分别配置空间寄存器时，由于已经在初始化的ARM安全固件的内存中配置了PCI配置空间，则可以在PCI配置空间内，对PCI链路桥下N个层级的PCI设备分别配置空间寄存器。

在本申请的一种具体实现中，在扫描结果指示PCI链路桥下的PCI设备的层级小于N的情况下，在PCI配置空间内预留PCI链路桥对应的寄存器配置空间。通过预留寄存器配置空间，可以在后续接入多层级的PCI设备时，以及时在预留的寄存器配置空间内对接入的PCI设备进行空间寄存器的配置。

在调用ARM服务器的ARM安全固件对PCI链路桥和PCI链路桥下N个层级的PCI设备配置空间寄存器之后，执行步骤102。

步骤102：在ARM安全固件内，添加ARM服务器的所有CPU的AER错误识别信息。

在调用ARM服务器的ARM安全固件对PCI链路桥和PCI链路桥下N个层级的PCI设备配置空间寄存器之后，则可以在ARM安全固件内，添加ARM服务器的所有CPU的AER错误识别信息。

本申请实施例通过对ARM服务器的所有CPU添加AER错误识别信息，在此基础上，进行单路或者双路启动后在DPU虚拟云盘系统下进行如T4卡的重启设置则不会出现AER宕机问题。

在具体实现中，在进行AER错误识别信息的添加时，可以在ARM安全固件内对所有CPU下的链路桥下的所有PCI设备均添加相应的AER错误识别信息。对于该实现过程可以结合图6进行如下详细描述。

参照图6，示出了本申请实施例提供的一种AER错误识别信息添加方法的步骤流程图。如图6所示，该AER错误识别信息添加方法可以包括：步骤601和步骤602。

步骤601：获取ARM服务器的所有CPU下的链路桥，及所有CPU下的链路桥下的所有PCI设备。

在本申请实施例中，在进行AER错误识别信息的添加时，可以获取ARM服务器的所有CPU下的链路桥。

在本示例中，ARM服务器中可以仅有一个CPU，也可以有两个CPU，或者四个CPU等，具体地，对于ARM服务器中CPU的数量可以根据实际情况而定，本实施例对此不加以限制。

在获取到ARM服务器的所有CPU下的链路桥之后，则可以对每个CPU下的链路桥进行PCI设备的扫描，以得到所有CPU下的链路桥下的所有PCI设备。

在获取到ARM服务器的所有CPU下的链路桥，及所有CPU下的链路桥下的所有PCI设备之后，执行步骤602。

步骤602：在ARM安全固件内，添加所有CPU下的链路桥下的所有PCI设备的AER错误识别信息。

在获取到ARM服务器的所有CPU下的链路桥，及所有CPU下的链路桥下的所有PCI设备之后，则可以在ARM安全固件内，添加所有CPU下的链路桥下的所有PCI设备的AER错误识

别信息。

本申请实施例中，无论是单路服务器还是双路服务器均进行AER错误识别信息的添加，从而可以解决在ARM服务器启动后在DPU虚拟云盘系统下进行如T4卡的重启设置出现AER宕机的问题。

在具体实现中，在进行AER错误识别信息的添加时，可以获取所有CPU下的链路桥的AER配置信息，并基于AER配置信息进行AER错误识别信息的添加。对于该实现过程可以结合图7进行如下详细描述。

参照图7，示出了本申请实施例提供的另一种AER错误识别信息添加方法的步骤流程图。如图7所示，该AER错误识别信息添加方法可以包括：步骤701和步骤702。

步骤701：获取所有CPU下的链路桥的AER配置信息。

在本申请实施例中，在获取到ARM服务器的所有CPU下的链路桥，及所有CPU下的链路桥下的所有PCI设备之后，可以获取所有CPU下的链路桥的AER配置信息。

在获取到所有CPU下的链路桥的AER配置信息之后，执行步骤702。

步骤702：在ARM安全固件内，基于AER配置信息，对所有CPU下的链路桥下的所有PCI设备进行初始化，以添加AER错误识别信息。

在获取到所有CPU下的链路桥的AER配置信息之后，则可以在ARM安全固件内，基于AER配置信息，对所有CPU下的链路桥下的所有PCI设备进行初始化，以添加AER错误识别信息。

本申请实施例通过结合AER配置信息对链路桥下的所有PCI设备进行AER错误识别信息的添加，可以满足多层次系统下重启PCI设备正常使用的功能。

在具体实现中，在添加ARM服务器的所有CPU的AER错误识别信息之后，则可以检测ARM安全固件下的所有PCI链路桥下的PCI设备是否均配置完成。若所有PCI链路桥下的PCI设备均配置完成，则可以启动ARM服务器的UEFI固件，并启动加载虚拟云盘系统（如DPU虚拟云盘系统等）。

若所有PCI链路桥下的PCI设备存在未配置的PCI链路桥，则对未配置的PCI链路桥继续进行配置流程。对于该实现过程可以结合图8进行如下详细描述。

参照图8，示出了本申请实施例提供的一种PCI设备配置方法的步骤流程图。如图8所示，该PCI设备配置方法可以包括：步骤801和步骤802。

步骤801：响应于所有PCI链路桥下的PCI设备存在未配置的PCI链路桥，获取未配置的PCI链路桥下的PCI设备。

在本实施例中，在所有PCI链路桥下的PCI设备存在未配置的PCI链路桥的情况下，可以获取未配置的PCI链路桥下的PCI设备。

步骤802：依次对未配置的PCI链路桥和未配置的PCI链路桥下的PCI设备进行寄存器配置和AER错误识别信息的添加。

进而，可以依次对未配置的PCI链路桥和未配置的PCI链路桥下的PCI设备进行寄存器配置和AER错误识别信息的添加。

本申请实施例通过对未配置PCI链路桥的检测，可以避免出现PCI链路桥或PCI设备的遗漏，导致PCI链路桥下的PCI设备未进行上述配置出现宕机的情况发生。

在具体实现中，在启动虚拟云盘系统之后，可以在重启PCI设备和重启虚拟云盘系统的

情况下，确定是否出现ARM服务器出现宕机现象。对于该实现过程可以结合图9进行如下详细描述。

参照图9，示出了本申请实施例提供的一种配置完成确定方法的步骤流程图。如图9所示，该配置完成确定方法可以包括：步骤901和步骤902。

步骤901：在重启PCI设备和重启虚拟云盘系统的情况下，确定ARM服务器是否出现宕机现象。

在本实施例中，在启动加载虚拟云盘系统之后，可以在ARM服务器下重启PCI设备，并重启虚拟云盘系统，以检测ARM服务器是否出现宕机现象。具体地，DPU虚拟云盘操作系统后，通过系统下PCI命令重启如PCI设备T4卡，并通过系统命令重启DPU虚拟云盘操作系统。同时检测ARM服务器是否出现宕机现象。

步骤902：响应于ARM服务器未出现宕机现象，确定ARM安全固件配置成功。

若确定出ARM服务器未出现宕机现象，则可以确定ARM安全固件配置成功，已彻底解决重启PCI设备宕机问题。

当然，若ARM服务器仍出现宕机现象，则有可能是由于其它原因造成的，此时，可以输出宕机报警信息，以提示运维人员查找产生宕机现象的原因。

对于ARM服务器支持系统下重启PCI设备的流程可以结合图10进行如下详细描述。

参照图10，示出了本申请实施例提供的一种ARM服务器支持系统下重启PCI设备的流程图。如图10所示，该流程可以包括以下步骤：

步骤1、ARM服务器（本示例中为双路启动机制的ARM服务器）开机启动，BIOS固件加载，率先加载ATF镜像固件。

步骤2、ATF加载启动过程中，当安全启动及内存初始化启动完成后，进行PCI链路初始化部分，根据PCI链路桥的拆分情况对PCI链路桥及PCI设备进行扫描并初始化。此时，ATF由扫描初始化PCI链路桥及一层级PCI设备的方案改为扫描PCI链路及多层级PCI设备的方案。若当前PCI链路存在多级设备则进行多级PCI设备扫描并初始化，若当前PCI链路不存在多级设备，则将多级扫描PCI设备空间的功能进行开启并预留，即预留寄存器配置空间。

步骤3、在完成上述步骤2之后，可以对PCI链路桥的AER表格（包含PCI链路桥的AER配置信息）进行初始化，若不初始化AER表格将导致系统下重启PCI设备宕机问题出现，初始化表格需要对两个CPU的PCI链路及PCI设备均进行初始化，若只初始化任意1个CPU的PCI链路则会出现系统下重启PCI设备宕机问题，初始化AER表格需要将PCI链路及多层级的PCI设备的AER信息进行设置，以满足多层级系统下重启PCI设备正常使用的功能。

步骤4、当ARM服务器固件初始化完成ATF固件后，则启动UEFI固件，继续启动并进入DPU虚拟云盘操作系统。

步骤5、DPU虚拟云盘操作系统后，通过系统下PCI命令重启如PCI设备T4卡未出现重启宕机问题，或者，通过系统命令重启DPU虚拟云盘操作系统也未出现重启宕机问题，故重启PCI设备宕机问题彻底解决。

步骤6、当然，在仅对两个CPU中的任意一个CPU的PCI链路桥及多层级PCI设备添加AER错误识别信息的情况下，启动加载虚拟云盘系统后，通过系统下PCI命令重启如PCI设备T4卡会出现重启宕机问题，或者，通过系统命令重启DPU虚拟云盘操作系统会出现重启宕机问题。

在本实施例中，根据ARM服务器固件的特性及DPU虚拟云盘系统下重启PCI设备或者虚拟云盘系统重启导致的系统宕机问题，通过对问题的根因定位到ATF需要支持PCI设备多层级扫描并配置管理寄存器方可。同时，因在DPU虚拟云盘系统下重启PCI设备或者重启系统导致AER错误产生且继续宕机的现象，通过在ATF中对CPU0和PCI的PCI链路桥及PCI设备添加AER错误信息识别功能，方可解决AER错误导致的宕机问题，上述2点必须同时存在才能彻底解决DPU虚拟云盘系统下重启PCI设备或者重启系统导致的系统宕机问题，若CPU0和CPU1中的任意一个添加了PCI桥及PCI设备的AER错误信息识别功能则将继续导致宕机问题的存在，无论物理是单路服务器还是双路服务器都需要对CPU0和CPU1的PCI链路桥及PCI设备添加AER错误信息识别功能才行。故本申请实施例在ATF固件部分将CPU的PCI链路及PCI设备的扫描层级增多至多级，最少3层级及以上，同时，将CPU0和CPU1的PCI链路桥及PCI设备添加AER错误信息识别功能方可解决系统下重启PCI设备或者系统重启时的宕机问题。

接下来，结合硬件架构对配置流程进行如下详细描述。

参照图11，示出了本申请实施例提供的一种硬件架构的示意图。如图11所示，本实施例的硬件架构可以包括：ARM服务器以及OS（Operating System）操作系统，以及ARM服务器下的BIOS，BIOS下的UTF固件和UEFI固件。

在具体流程中，可以先启动ARM服务器，ARM服务器启动之后，可以加载BIOS镜像。进而，可以加载ATF镜像固件。在ATF固件启动过程可以进行安全启动校验，完成之后，对进行内存初始化。

在内存初始化完成之后，可以对PCI链路桥及PCI设备初始化，此时，可以进行PCI链路桥以及PCI设备多层级扫描，并配置PCI配置空间。

根据扫描结果，确定PCI链路桥下是否存在多层级PCI设备。若PCI链路桥下不存在多层级PCI设备则预留PCI设备配置空间寄存器的空间，即寄存器配置空间。若PCI链路桥下存在多层级PCI设备，则可以对多层级PCI设备配置空间寄存器。

然后，可以选择是否对CPU0和CPU1的PCI链路桥的多层级PCI设备添加AER错误识别信息。若选择对CPU0和CPU1的PCI链路桥的多层级PCI设备添加AER错误识别信息，则初始化AER表格将PCI链路及多层级的PCI设备的AER信息进行设置。

在ATF固件初始化完成之后，可以加载UEFI固件，并启动加载DPU虚拟云盘系统。

通过系统下PCI命令重启如PCI设备T4卡未出现重启宕机问题，或者，通过系统命令重启DPU虚拟云盘操作系统也未出现重启宕机问题，故重启PCI设备宕机问题彻底解决。

本申请实施例针对ARM架构服务器的固件划分及ARM服务器的具体实际应用情况，针对DPU虚拟云盘重启或者虚拟云盘下重启PCI设备时出现的宕机问题，在ATF中将PCI链路桥及PCI设备进行多层级扫描并配置管理寄存器，同时，将CPU0和CPU1的每个PCI链路桥及PCI设备添加AER错误信息识别功能，倘若不添加则出现重启时的二次宕机出现，故采用此方案可解决系统下重启和PCI设备重启时出现的两次宕机问题，所以，本实施例通过增加PCI链路桥及PCI设备在ATF固件中的扫描层级并配置寄存器设置，同时，无论是单路还是双路服务器都需要在ATF中增加PU0和CPU1的每个PCI链路桥及PCI设备添加AER错误信息识别功能即可，能彻底解决DPU虚拟云盘系统下重启或者DPU虚拟云盘系统下重启PCI设备宕机的问题。

本申请实施例提供的应用于ARM服务器的ARM安全固件配置方法，通过调用ARM服务

器的ARM安全固件，对PCI链路桥和PCI链路桥下N个层级的PCI设备配置空间寄存器，ARM安全固件为ARM服务器的处理器固件，N为大于等于3的正整数。在ARM安全固件内，添加ARM服务器的所有CPU的AER错误识别信息。本申请实施例通过增加PCI链路桥及PCI设备在ATF固件中的扫描层级并配置寄存器设置，同时，无论是单路还是双路服务器都需要在ATF中增加所有CPU的每个PCI链路桥及PCI设备添加AER错误信息识别功能，可以有效解决DPU虚拟云盘系统下重启或者DPU虚拟云盘系统下重启PCI设备宕机的问题。

参照图12，示出了本申请实施例提供的一种应用于ARM服务器的ARM安全固件配置装置的结构示意图。如图12所示，该应用于ARM服务器的ARM安全固件配置装置1200可以包括以下模块：

寄存器配置模块1210，用于调用ARM服务器的ARM安全固件，对PCI链路桥和PCI链路桥下N个层级的PCI设备配置空间寄存器，ARM安全固件为ARM服务器的处理器固件，N为大于等于3的正整数；

AER信息添加模块1220，用于在ARM安全固件内，添加ARM服务器的所有CPU的AER错误识别信息。

在一些实施例中，寄存器配置模块包括：

扫描结果获取单元，用于在ARM安全固件加载启动过程中，调用ARM安全固件，对所有CPU进行PCI链路桥及N个层级的PCI设备扫描，得到扫描结果；

空间寄存器配置单元，用于在扫描结果指示PCI链路桥下存在N个层级的PCI设备的情况下，对PCI链路桥下N个层级的PCI设备配置空间寄存器。

在一些实施例中，空间寄存器配置单元包括：

PCI设备初始化子单元，用于对PCI链路桥下N个层级的PCI设备进行初始化；

空间寄存器配置子单元，用于对PCI链路桥下N个层级的PCI设备配置空间寄存器。

在一些实施例中，装置包括：

ARM安全固件加载模块，用于响应于ARM服务器启动且BIOS加载成功，加载ARM安全固件；

安全启动校验模块，用于对ARM安全固件进行安全启动校验；

内存初始化模块，用于响应于ARM安全固件安全启动校验成功，对ARM安全固件进行内存初始化。

在一些实施例中，扫描结果获取单元包括：

扫描结果获取子单元，用于响应于ARM安全固件内存初始化完成，调用ARM安全固件，对所有CPU进行PCI链路桥及N个层级的PCI设备扫描，得到扫描结果；

PCI配置空间配置子单元，用于在初始化的内存中配置PCI链路桥对应的PCI配置空间。

在一些实施例中，空间寄存器配置单元包括：

寄存器配置子单元，用于在PCI配置空间内，对PCI链路桥下N个层级的PCI设备分别配置空间寄存器。

在一些实施例中，装置还包括：

配置空间预留模块，用于在扫描结果指示PCI链路桥下的PCI设备的层级小于N的情况下，在PCI配置空间内预留PCI链路桥对应的寄存器配置空间。

在一些实施例中，AER信息添加模块包括：

PCI设备获取单元，用于获取ARM服务器的所有CPU下的链路桥，及所有CPU下的链路桥下的所有PCI设备；

AER信息添加单元，用于在ARM安全固件内，添加所有CPU下的链路桥下的所有PCI设备的AER错误识别信息。

在一些实施例中，AER信息添加单元包括：

配置信息获取子单元，用于获取所有CPU下的链路桥的AER配置信息；

AER信息添加子单元，用于在ARM安全固件内，基于AER配置信息，对所有CPU下的链路桥下的所有PCI设备进行初始化，以添加AER错误识别信息。

在一些实施例中，装置还包括：

配置完成检测模块，用于检测ARM安全固件下的所有PCI链路桥下的PCI设备是否均配置完成；

虚拟云盘系统加载模块，用于响应于所有PCI链路桥下的PCI设备均配置完成，启动ARM服务器的UEFI固件，并启动加载虚拟云盘系统。

在一些实施例中，装置还包括：

未配置设备获取模块，用于响应于所有PCI链路桥下的PCI设备存在未配置的PCI链路桥，获取未配置的PCI链路桥下的PCI设备；

PCI设备配置模块，用于依次对未配置的PCI链路桥和未配置的PCI链路桥下的PCI设备进行寄存器配置和AER错误识别信息的添加。

在一些实施例中，装置还包括：

宕机现象确定模块，用于在重启PCI设备和重启虚拟云盘系统的情况下，确定ARM服务器是否出现宕机现象；

配置成功确定模块，用于响应于ARM服务器未出现宕机现象，确定ARM安全固件配置成功。

本申请实施例提供的应用于ARM服务器的ARM安全固件配置装置，通过调用ARM服务器的ARM安全固件，对PCI链路桥和PCI链路桥下N个层级的PCI设备配置空间寄存器，ARM安全固件为ARM服务器的处理器固件，N为大于等于3的正整数。在ARM安全固件内，添加ARM服务器的所有CPU的AER错误识别信息。本申请实施例通过增加PCI链路桥及PCI设备在ATF固件中的扫描层级并配置寄存器设置，同时，无论是单路还是双路服务器都需要在ATF中增加所有CPU的每个PCI链路桥及PCI设备添加AER错误信息识别功能，可以有效解决DPU虚拟云盘系统下重启或者DPU虚拟云盘系统下重启PCI设备宕机的问题。

另外地，本申请实施例还提供了一种电子设备，包括：存储器、处理器及存储在存储器上并可在处理器上运行的计算机程序，计算机程序被处理器执行时实现上述应用于ARM服务器的ARM安全固件配置方法。

图13示出了本申请实施例的一种电子设备1300的结构示意图。如图13所示，电子设备1300包括中央处理单元（CPU）1301，其可以根据存储在只读存储器（ROM）1302中的计算机程序指令或者从存储单元1308加载到随机访问存储器（RAM）1303中的计算机程序指令，来执行各种适当的动作和处理。在RAM1303中，还可存储电子设备1300操作所需的各种程序和数据。CPU1301、ROM1302以及RAM1303通过总线1304彼此相连。输入/输出（I/O）接口1305也连接至总线1304。

电子设备1300中的多个部件连接至I/O接口1305，包括：输入单元1306，例如键盘、鼠标、麦克风等；输出单元1307，例如各种类型的显示器、扬声器等；存储单元1308，例如磁盘、光盘等；以及通信单元1309，例如网卡、调制解调器、无线通信收发机等。通信单元1309允许电子设备1300通过诸如因特网的计算机网络和/或各种电信网络与其他设备交换信息/数据。

上文所描述的各个过程和处理，可由处理单元1301执行。例如，上述任一实施例的方法可被实现为计算机软件程序，其被有形地包含于计算机可读介质，例如存储单元1308。在一些实施例中，计算机程序的部分或者全部可以经由ROM1302和/或通信单元1309而被载入和/或安装到电子设备1300上。当计算机程序被加载到RAM1303并由CPU1301执行时，可以执行上文描述的方法中的一个或多个动作。

本申请实施例还提供了一种计算机非易失性可读存储介质，计算机非易失性可读存储介质上存储有计算机程序，计算机程序被处理器执行时实现上述应用于ARM服务器的ARM安全固件配置方法实施例的各个过程，且能达到相同的技术效果，为避免重复，这里不再赘述。其中，计算机非易失性可读存储介质，如只读存储器（Read-Only Memory，简称ROM）、随机存取存储器（Random Access Memory，简称RAM）、磁碟或者光盘等。

以上，仅为本申请的一些实施例，但本申请的保护范围并不局限于此，任何熟悉本技术领域的技术人员在本申请揭露的技术范围内，可轻易想到变化或替换，都应涵盖在本申请的保护范围之内。因此，本申请的保护范围应以权利要求的保护范围为准。

权 利 要 求 书

1. 一种应用于ARM服务器的ARM安全固件配置方法，其特征在于，所述方法包括：
调用所述ARM服务器的ARM安全固件，对PCI链路桥和所述PCI链路桥下N个层级的PCI设备配置空间寄存器，所述ARM安全固件为所述ARM服务器的处理器固件，N为大于等于3的正整数；

在所述ARM安全固件内，添加所述ARM服务器的所有CPU的AER错误识别信息。

2. 根据权利要求1所述的方法，其特征在于，所述调用所述ARM服务器的ARM安全固件，对PCI链路桥和所述PCI链路桥下N个层级的PCI设备配置空间寄存器，包括：

在所述ARM安全固件加载启动过程中，调用所述ARM安全固件，对所有CPU进行PCI链路桥及N个层级的PCI设备扫描，得到扫描结果；

在所述扫描结果指示所述PCI链路桥下存在N个层级的PCI设备的情况下，对所述PCI链路桥下N个层级的PCI设备配置所述空间寄存器。

3. 根据权利要求2所述的方法，其特征在于，所述对所述PCI链路桥下N个层级的PCI设备配置所述空间寄存器，包括：

对所述PCI链路桥下N个层级的PCI设备进行初始化；

对所述PCI链路桥下N个层级的PCI设备配置所述空间寄存器。

4. 根据权利要求2所述的方法，其特征在于，在所述调用所述ARM安全固件，对所有CPU进行PCI链路桥及N个层级的PCI设备扫描，得到扫描结果之前，包括：

响应于所述ARM服务器启动且BIOS加载成功，加载所述ARM安全固件；

对所述ARM安全固件进行安全启动校验；

响应于所述ARM安全固件安全启动校验成功，对所述ARM安全固件进行内存初始化。

5. 根据权利要求4所述的方法，其特征在于，所述调用所述ARM安全固件，对所有CPU进行PCI链路桥及N个层级的PCI设备扫描，得到扫描结果，包括：

响应于所述ARM安全固件内存初始化完成，调用所述ARM安全固件，对所有CPU进行PCI链路桥及N个层级的PCI设备扫描，得到扫描结果；

在初始化的内存中配置所述PCI链路桥对应的PCI配置空间。

6. 根据权利要求5所述的方法，其特征在于，所述调用所述ARM安全固件，对所有CPU进行PCI链路桥及N个层级的PCI设备扫描，还包括：

根据所述PCI链路桥的拆分情况对所述PCI链路桥及N个层级的PCI设备进行扫描。

7. 根据权利要求5所述的方法，其特征在于，所述对所述PCI链路桥下N个层级的PCI设备配置所述空间寄存器，包括：

在所述PCI配置空间内，对所述PCI链路桥下N个层级的PCI设备分别配置所述空间寄存器。

8. 根据权利要求5所述的方法，其特征在于，在所述调用所述ARM安全固件，对所有CPU进行PCI链路桥及N个层级的PCI设备扫描，得到扫描结果之后，还包括：

在所述扫描结果指示所述PCI链路桥下的PCI设备的层级小于N的情况下，在PCI配置空间内预留所述PCI链路桥对应的寄存器配置空间。

9. 根据权利要求8所述的方法，其特征在于，所述在PCI配置空间内预留所述PCI链路

桥对应的寄存器配置空间之后，还包括：

在预留的寄存器配置空间内对后续接入的N个层级的PCI设备配置所述空间寄存器。

10. 根据权利要求1所述的方法，其特征在于，所述在所述ARM安全固件内，添加所述ARM服务器的所有CPU的AER错误识别信息，包括：

获取所述ARM服务器的所有CPU下的链路桥，及所述所有CPU下的链路桥下的所有PCI设备；

在所述ARM安全固件内，添加所述所有CPU下的链路桥下的所有PCI设备的AER错误识别信息。

11. 根据权利要求10所述的方法，其特征在于，所述在所述ARM安全固件内，添加所述所有CPU下的链路桥下的所有PCI设备的AER错误识别信息，包括：

获取所述所有CPU下的链路桥的AER配置信息；

在所述ARM安全固件内，基于所述AER配置信息，对所述所有CPU下的链路桥下的所有PCI设备进行初始化，以添加所述AER错误识别信息。

12. 根据权利要求1所述的方法，其特征在于，在所述添加所述ARM服务器的所有CPU的AER错误识别信息之后，还包括：

检测所述ARM安全固件下的所有PCI链路桥下的PCI设备是否均配置完成；

响应于所述所有PCI链路桥下的PCI设备均配置完成，启动所述ARM服务器的UEFI固件，并启动加载虚拟云盘系统。

13. 根据权利要求12所述的方法，其特征在于，在所述检测所述ARM安全固件下的所有PCI链路桥下的PCI设备是否均配置完成之后，还包括：

响应于所述所有PCI链路桥下的PCI设备存在未配置的PCI链路桥，获取所述未配置的PCI链路桥下的PCI设备；

依次对所述未配置的PCI链路桥和所述未配置的PCI链路桥下的PCI设备进行寄存器配置和AER错误识别信息的添加。

14. 根据权利要求12所述的方法，其特征在于，在所述启动所述ARM服务器的UEFI固件，并启动加载虚拟云盘系统之后，还包括：

在重启PCI设备和重启所述虚拟云盘系统的情况下，确定所述ARM服务器是否出现宕机现象；

响应于所述ARM服务器未出现宕机现象，确定所述ARM安全固件配置成功。

15. 根据权利要求14所述的方法，其特征在于，所述在重启PCI设备和重启所述虚拟云盘系统的情况下，确定所述ARM服务器是否出现宕机现象，包括：

当所述PCI设备未出现重启宕机问题，以及所述虚拟云盘操作系统也未出现重启宕机问题，则确定所述ARM服务器未出现宕机现象。

16. 根据权利要求14所述的方法，其特征在于，在所述确定所述ARM服务器是否出现宕机现象之后，还包括：

响应于所述ARM服务器出现宕机现象，输出宕机报警信息。

17. 根据权利要求1所述的方法，其特征在于，所述ARM服务器至少包括一个CPU。

18. 一种应用于ARM服务器的ARM安全固件配置装置，其特征在于，所述装置包括：

寄存器配置模块，用于调用所述ARM服务器的ARM安全固件，对PCI链路桥和所述

PCI链路桥下N个层级的PCI设备配置空间寄存器，所述ARM安全固件为所述ARM服务器的处理器固件，N为大于等于3的正整数；

AER信息添加模块，用于在所述ARM安全固件内，添加所述ARM服务器的所有CPU的AER错误识别信息。

19. 一种电子设备，其特征在于，包括：

存储器、处理器及存储在所述存储器上并可在所述处理器上运行的计算机程序，所述计算机程序被所述处理器执行时实现如权利要求1至17中任一项所述的应用于ARM服务器的ARM安全固件配置方法。

20. 一种计算机非易失性可读存储介质，其特征在于，当所述计算机非易失性可读存储介质中的指令由电子设备的处理器执行时，使得电子设备能够执行权利要求1至17任一项所述的应用于ARM服务器的ARM安全固件配置方法。

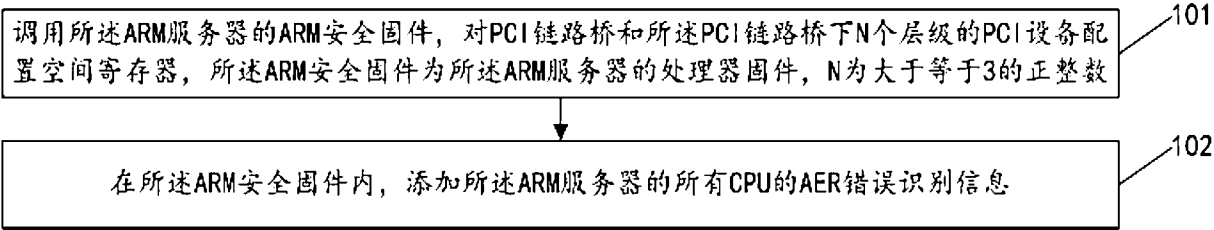


图 1

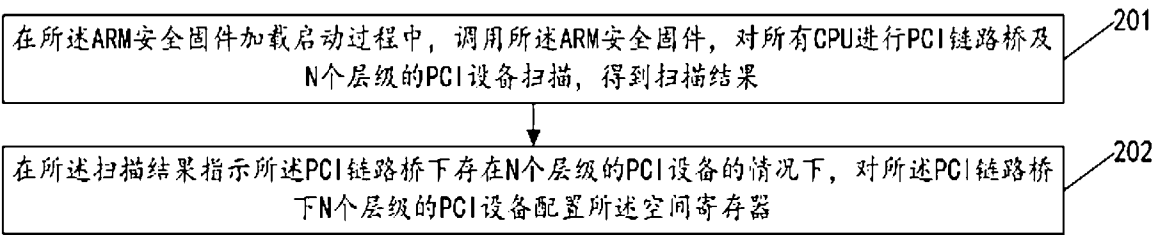


图 2

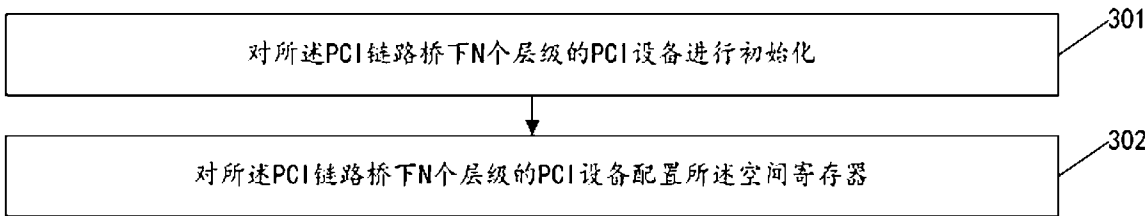


图 3

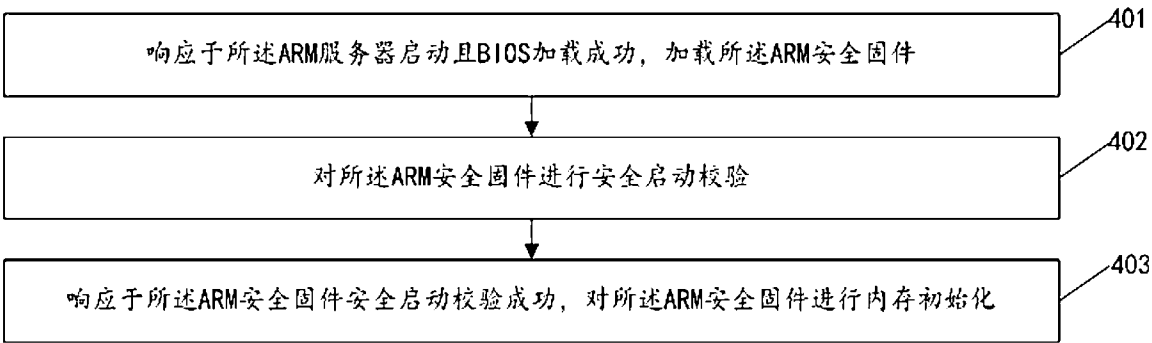


图 4

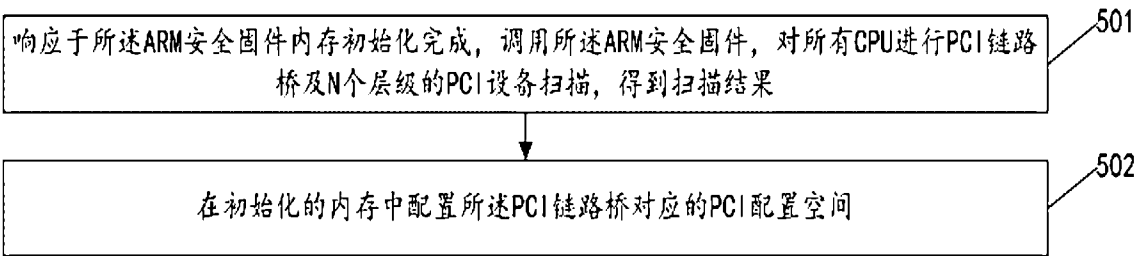


图 5

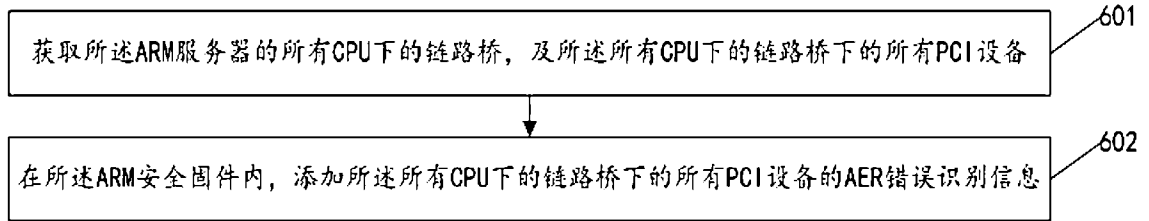


图 6

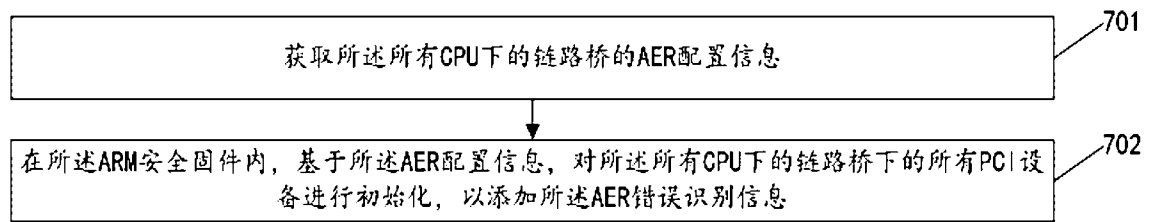


图 7

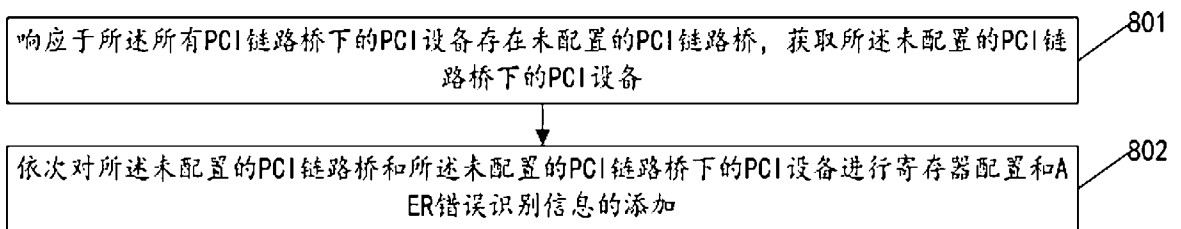


图 8

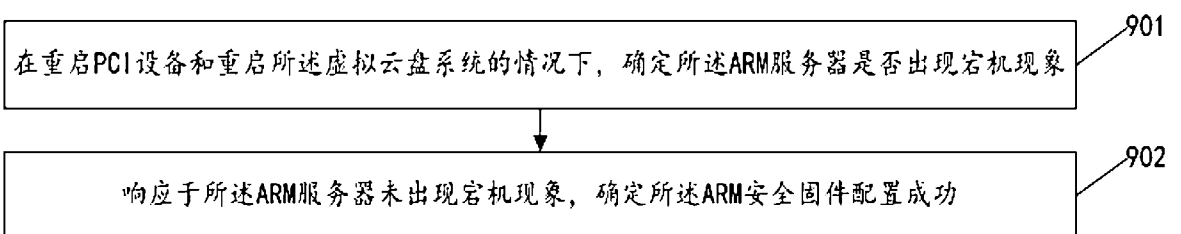


图 9

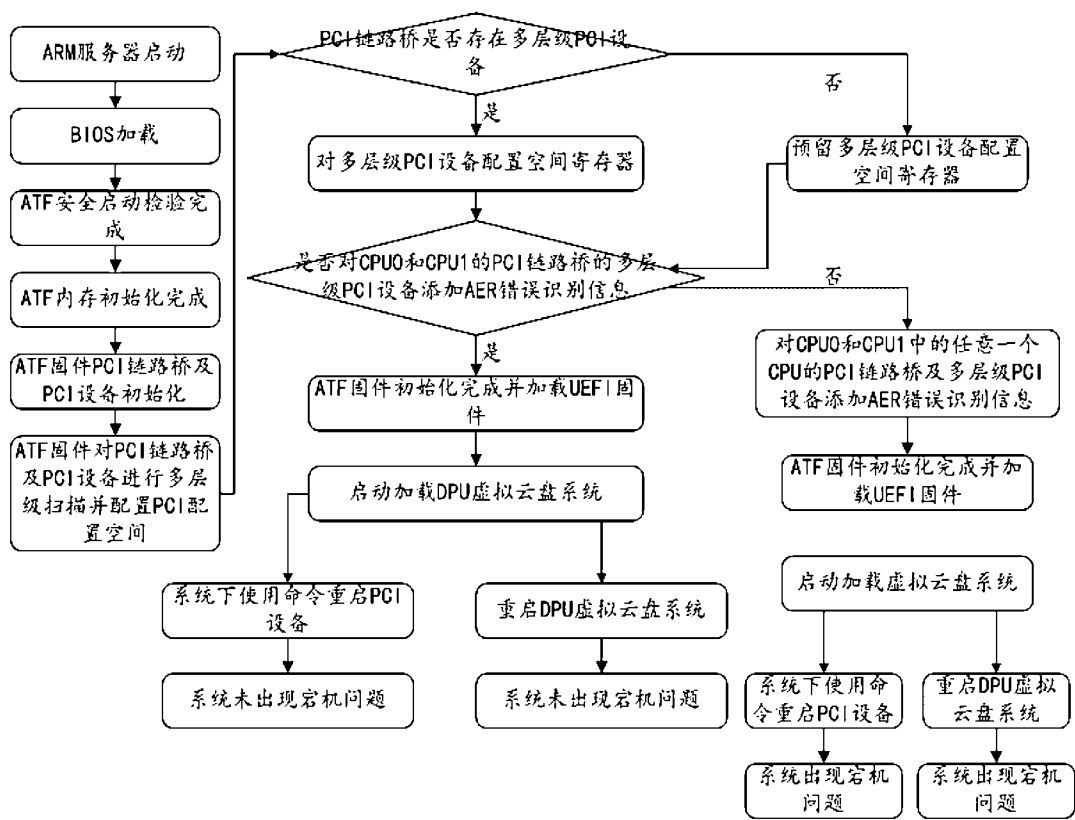


图 10

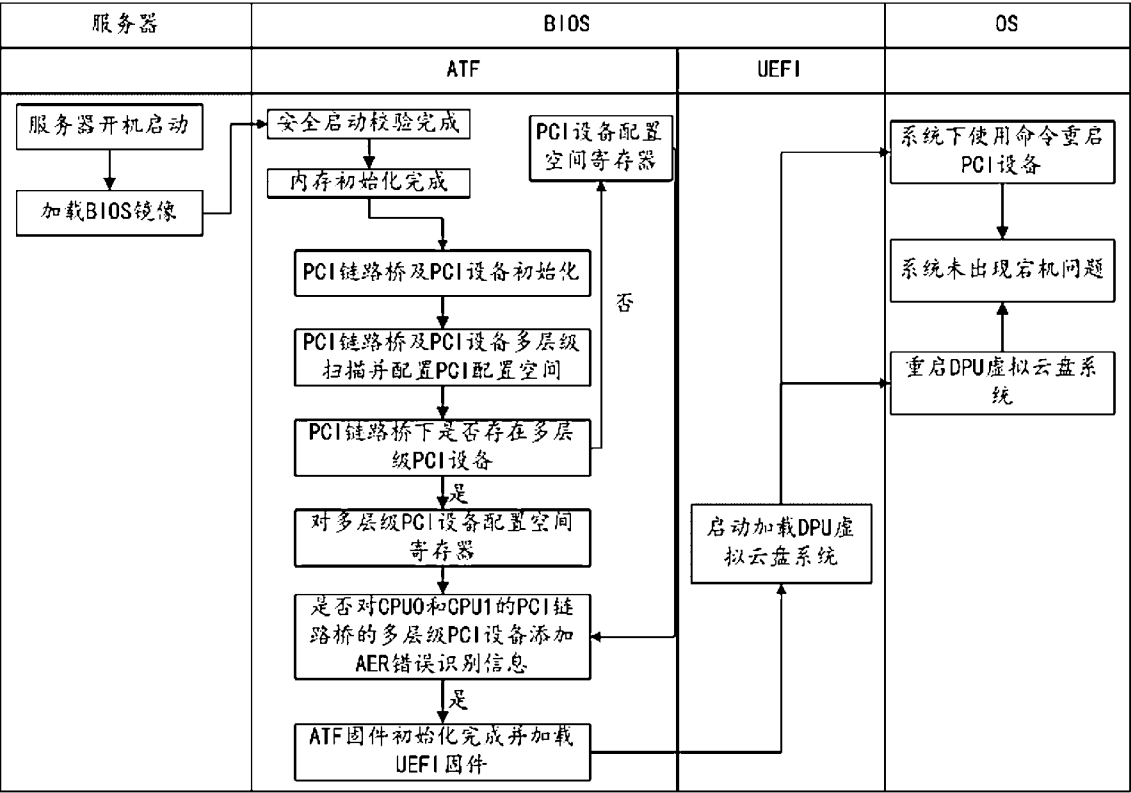


图 11

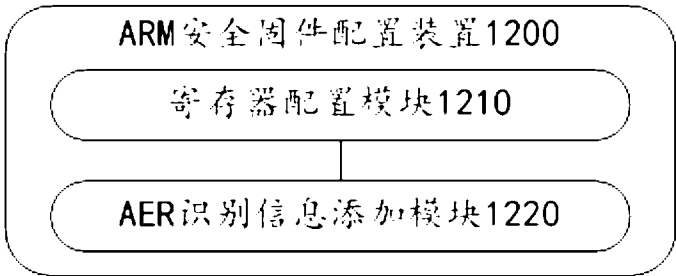


图 12

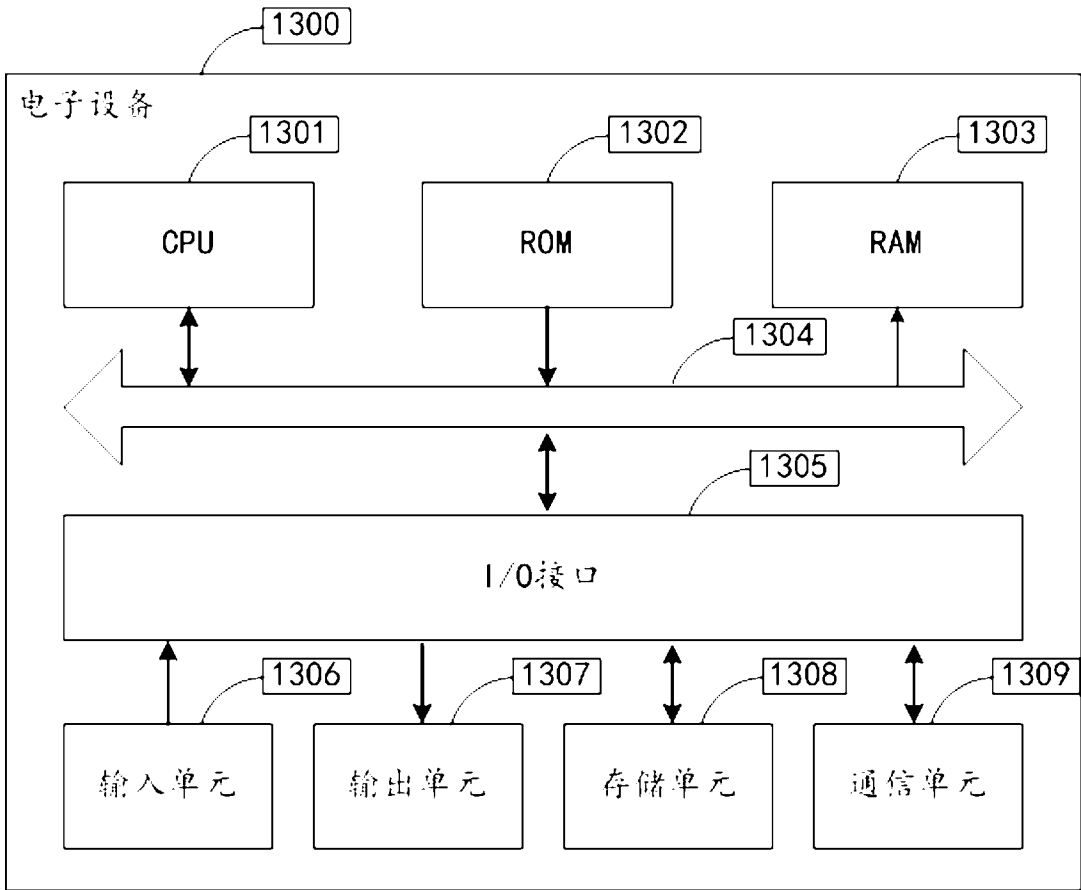


图 13

INTERNATIONAL SEARCH REPORT

International application No.

PCT/CN2024/099921

A. CLASSIFICATION OF SUBJECT MATTER

G06F11/00(2006.01)i; G06F9/4401(2018.01)i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC: G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

VEN, CNABS, CNTXT, WOTXT, EPTXT, USTXT, CNKI, IEEE: 服务器, 外设, 层级, 多级, 链路, 内存, 寄存器, 高级错误报告, 所有, 全部, 固件, 重启, 宕机, 虚拟, 云盘, ARM, server, advanced RISC machines, PCI, peripheral component interconnect, hierarchical, level, link, memory, register, AER, all, firmware, restart, down, virtual, cloud disk, CPU, ATF, arm trusted firmware

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
PX	CN 117331723 A (SUZHOU YUANNAO INTELLIGENT TECHNOLOGY CO., LTD.) 02 January 2024 (2024-01-02) description, paragraphs 0035-0144	1-20
A	CN 114201360 A (SUZHOU INSPUR INTELLIGENT TECHNOLOGY CO., LTD.) 18 March 2022 (2022-03-18) description, paragraphs 0052-0108	1-20
A	CN 109614259 A (ZHENGZHOU YUNHAI INFORMATION TECHNOLOGY CO., LTD.) 12 April 2019 (2019-04-12) entire document	1-20
A	CN 114185607 A (SUZHOU INSPUR INTELLIGENT TECHNOLOGY CO., LTD.) 15 March 2022 (2022-03-15) entire document	1-20
A	CN 116700821 A (SUZHOU INSPUR INTELLIGENT TECHNOLOGY CO., LTD.) 05 September 2023 (2023-09-05) entire document	1-20



Further documents are listed in the continuation of Box C.



See patent family annex.

* Special categories of cited documents:

“A” document defining the general state of the art which is not considered to be of particular relevance
“D” document cited by the applicant in the international application
“E” earlier application or patent but published on or after the international filing date
“L” document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
“O” document referring to an oral disclosure, use, exhibition or other means
“P” document published prior to the international filing date but later than the priority date claimed

“T” later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

“X” document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

“Y” document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

“&” document member of the same patent family

Date of the actual completion of the international search

28 August 2024

Date of mailing of the international search report

02 September 2024

Name and mailing address of the ISA/CN

China National Intellectual Property Administration (ISA/
CN)
China No. 6, Xitucheng Road, Jimenqiao, Haidian District,
Beijing 100088

Authorized officer

Telephone No.

INTERNATIONAL SEARCH REPORT

International application No.

PCT/CN2024/099921

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 2017068636 A1 (AVAGO TECHNOLOGIES GENERAL IP (SINGAPORE) PTE. LTD.) 09 March 2017 (2017-03-09) entire document	1-20

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2024/099921

Patent document cited in search report			Publication date (day/month/year)	Patent family member(s)			Publication date (day/month/year)
CN	117331723	A	02 January 2024	None			
CN	114201360	A	18 March 2022	None			
CN	109614259	A	12 April 2019	None			
CN	114185607	A	15 March 2022	WO	2023151287	A1	17 August 2023
CN	116700821	A	05 September 2023	None			
US	2017068636	A1	09 March 2017	None			

A. 主题的分类

G06F11/00(2006.01)i; G06F9/4401(2018.01)i

按照国际专利分类(IPC)或者同时按照国家分类和IPC两种分类

B. 检索领域

检索的最低限度文献(标明分类系统和分类号)

IPC: G06F

包含在检索领域中的除最低限度文献以外的检索文献

在国际检索时查阅的电子数据库(数据库的名称, 和使用的检索词(如使用))

VEN, CNABS, CNTXT, WOTXT, EPTXT, USTXT, CNKI, IEEE: 服务器, 外设, 层级, 多级, 链路, 内存, 寄存器, 高级错误报告, 所有, 全部, 固件, 重启, 宕机, 虚拟, 云盘, ARM, server, advanced RISC machines, PCI, peripheral component interconnect, hierarchical, level, link, memory, register, AER, all, firmware, restart, down, virtual, cloud disk, CPU, ATF, arm trusted firmware

C. 相关文件

类型*	引用文件, 必要时, 指明相关段落	相关的权利要求
PX	CN 117331723 A (苏州元脑智能科技有限公司) 2024年1月2日 (2024 - 01 - 02) 说明书第0035-0144段	1-20
A	CN 114201360 A (苏州浪潮智能科技有限公司) 2022年3月18日 (2022 - 03 - 18) 说明书第0052-0108段	1-20
A	CN 109614259 A (郑州云海信息技术有限公司) 2019年4月12日 (2019 - 04 - 12) 全文	1-20
A	CN 114185607 A (苏州浪潮智能科技有限公司) 2022年3月15日 (2022 - 03 - 15) 全文	1-20
A	CN 116700821 A (苏州浪潮智能科技有限公司) 2023年9月5日 (2023 - 09 - 05) 全文	1-20
A	US 2017068636 A1 (AVAGO TECHNOLOGIES GENERAL IP (SINGAPORE) PTE. LTD.) 2017年3月9日 (2017 - 03 - 09) 全文	1-20

☐ 其余文件在C栏的续页中列出。

☒ 见同族专利附件。

* 引用文件的具体类型:

“A” 认为不特别相关的表示了现有技术一般状态的文件

“D” 申请人在国际申请中引证的文件

“E” 在国际申请日的当天或之后公布的在先申请或专利

“L” 可能对优先权要求构成怀疑的文件, 或为确定另一篇引用文件的公布日而引用的或者因其他特殊理由而引用的文件(如具体说明的)

“O” 涉及口头公开、使用、展览或其他方式公开的文件

“p” 公布日先于国际申请日但迟于所要求的优先权日的文件

“T” 在申请日或优先权日之后公布, 与申请不相抵触, 但为了理解发明之理论或原理的在后文件

“X” 特别相关的文件, 单独考虑该文件, 认定要求保护的发明不是新颖的或不具有创造性

“Y” 特别相关的文件, 当该文件与另一篇或者多篇该类文件结合并且这种结合对于本领域技术人员为显而易见时, 要求保护的发明不具有创造性

“&” 同族专利的文件

国际检索实际完成的日期

2024年8月28日

国际检索报告邮寄日期

2024年9月2日

ISA/CN的名称和邮寄地址

中国国家知识产权局
中国北京市海淀区蓟门桥西土城路6号 100088

授权官员

韦佳黎

电话号码 (+86) 010-53961398

PCT/ISA/210 表(第2页) (2022年7月)

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2024/099921

检索报告引用的专利文件			公布日 (年/月/日)	同族专利	公布日 (年/月/日)
CN	117331723	A	2024年1月2日	无	
CN	114201360	A	2022年3月18日	无	
CN	109614259	A	2019年4月12日	无	
CN	114185607	A	2022年3月15日	WO 2023151287 A1	2023年8月17日
CN	116700821	A	2023年9月5日	无	
US	2017068636	A1	2017年3月9日	无	