引用格式:王宁,牛玥瑶,崔西宁. 基于QEMU仿真的ARM多核启动技术研究[J]. 航空计算技术,2023,53(5):96-99.
WANG Ning,NIU Yue-yao,CUI Xi-ning. Research on Technology of ARM Multi-core's Startup Based on QEMU[J]. Aeronautical Computing Technique,2023,53(5):96-99.

基于QEMU仿真的ARM多核启动技术研究

王 宁,牛玥瑶,崔西宁

(航空工业西安航空计算技术研究所,陕西 西安 710000)

摘 要:针对QEMU模拟仿真软件6.1.0版本下基于ARM内核的VIRT模拟器运行天脉操作系统时,不能正确启动处理器各个从核的问题,分析了VIRT模拟器针对ARM处理器从核的启动方式及流程,同时查阅了ARM体系结构手册中关于处理器从核启动的相关指令说明,进一步分析天脉操作系统中关于从核启动的相关代码,找出了天脉操作系统从核启动代码与VIRT模拟器从核启动流程之间的匹配差异。通过修改VIRT模拟器的从核启动代码,完成对天脉操作系统从核启动代码的匹配。在不改动天脉操作系统从核启动代码的情况下,顺利将模拟的ARM处理器各个从核启动成功。

关键词:QEMU仿真;SMC指令;SEV指令;多核启动

中图分类号:TP319 **文献标识码**:A **文章编号**:1671-654X(2023)05-0096-04

Research on Technology of ARM Multi-core's Startup Based on QEMU

WANG Ning,NIU Yue-yao,CUI Xi-ning

(*Xi'an Aeronautics Computing Technique Research Institute,AVIC,Xi'an* 710000,*China*)

Abstract:VIRT emulator in QEMU (version 6.1.0) is developed for hardware emulation of ARM architecture. But TianMai Operating System developed for ARM architecture cannot start every PE of emulated ARM CPU correctly every time when running on VIRT emulator. However,the same operating system can work correctly when running on real hardware environment. By analyzing the multi-core's startup manner and order of VIRT emulator,every related instructions' description in ARM architecture reference manual,and the source code about multi-cores' startup in TianMai operating system,the differences between VIRT emulator and TianMai operating system are found. Based on these new-found differences,by modifying the source code about multi-cores' startup in virt emulator,TianMai operting system is matched properly. Finally,each PE of ARM CPU in VIRT emulator is started correctly without changing any source code in TianMai operating system.

Key words:QEMU emulation;SMC instruction;SEV instruction;multi-core's startup

引言

QEMU模拟仿真软件是基于动态二进制翻译技术的快速模拟器(Quick Emulator),QEMU支持系统模拟和用户态模拟两种方式,在实际使用过程中,用户更多地使用了系统模拟方式。QEMU的所有软件代码都是开源的,这就方便用户根据自己的实际使用环境对QEMU软件进行适应性修改,以更好地匹配用户需求[1-3]。

在QEMU开源的工作模式下,全球各地的开源爱好者贡献了大量针对不同硬件环境的模拟器[4-6]。但是,这些模拟器大多都是模拟技术成熟、市场占有率高的商业硬件产品。对于一些专用领域(例如:航空航天领域)的硬件产品,这些已有的模拟器在细节上并不能很好地与之匹配。

天脉嵌入式实时操作系统是国内完全正向开发、拥有自主知识产权的系列化产品,可广泛应用于通用强实时、分区综合化以及多核高性能等多种嵌入式应用场景。天脉操作系统产品及开发环境已广泛应用于

收稿日期:2023-06-01
基金项目:航空科学基金项目资助(2022Z071031001)
作者简介:王 宁(1982-),男,陕西渭南人,高级工程师。

航空航天的各个领域,覆盖了综合处理、通信导航、数据采集、图形图像处理等多种应用场景[1]。

将基于 ARM 多核处理器的天脉操作系统运行在 QEMU5.1.0 版本下的 VIRT 模拟器上时,发现在真实硬件上能够成功运行的代码,并不一定能将 VIRT 模拟器模拟的 ARM 处理器的所有从核成功启动。这是因为 VIRT 模拟器与天脉操作系统所运行的真实硬件平台存在差异。

本文通过深入分析 VIRT 模拟器从核启动机制、ARM 体系架构说明文档、以及天脉操作系统的从核启动代码,找出了 VIRT 模拟器与天脉操作系统从核启动代码之间的匹配差异,进而通过修改 VIRT 模拟器的从核启动代码,完成对天脉操作系统的适配。最终,在不改动天脉操作系统从核启动代码的情况下,顺利将 VIRT 模拟器的各个从核启动成功。

修改后的 VIRT 模拟器可以很好地适配运行天脉操作系统。在一些暂时缺少真实硬件的场合,可以将 VIRT 模拟器先期提供给用户进行上层应用的开发调试,从而大大缩短当后期硬件环境具备以后所需的软硬件联试时间,对于实际工程项目的软件开发具有极大的推动作用。

1　ARM 处理器从核启动方式

本文所涉及的 ARM 处理器的从核启动方式有以下两种:

1)通过 SEV 指令启动从核运行[7];

2)通过 SMC 指令启动从核运行[8]。

在 VIRT 模拟器上运行不同版本的天脉操作系统时发现,当采用第一种从核启动方式时,VIRT 模拟器模拟的 ARM 处理器从核能够顺利启动运行;但是,当采用第二种从核启动方式时,VIRT 模拟器模拟的 ARM 处理器的从核不能够顺利启动。

下面首先分析 ARM 处理器体系架构手册中有关这两种从核启动方式的描述[4,9]。

1.1　通过 SEV 指令启动从核

通过 SEV 指令启动从核,需要从核执行 WFE 指令,将自己切入低功耗等待状态,然后等待主核通过执行 SEV 指令将自己唤醒。

ARM 体系结构手册中与通过 SEV 指令启动从核相关的描述如下:

ARM 处理器提供了一种事件等待机制(Wait For Event Mechanism),该机制允许多核处理器中的任何一个核心,通过 WFE 指令请求进入低功耗状态,直到发生以下事件将它再次唤醒。

1)其他 CPU 核通过 SEV 指令产生一个事件;

2)有外部中断产生;

3)有异常产生。

ARM 处理器核心执行 WFE 指令时,并不一定会进入低功耗状态,而是会先去判断事件寄存器(Event Register)是否为 1,如果事件寄存器为 1,处理器核心会将事件寄存器清零,然后继续执行下一条指令,并不会进入低功耗状态;只有当事件寄存器为 0 时,处理器核心才会进入低功耗状态,等待被事件唤醒。

事件寄存器(Event Register)是个一位寄存器(Single Bit Register),当事件寄存器为 1 时,表示自从上次事件寄存器被清零以后,又有新的事件发生。处理器核心将事件寄存器清零,表示已对新发生的事件进行了相应的处理。

ARM 处理器核心可以通过执行 SEV(Send Event)指令,将处理器所有核心的事件寄存器设置为 1,通知其他核心当前有新的事件需要处理。

总结:当采用 SEV 指令方式启动从核时,系统上电后会给 ARM 处理器的所有从核都进行供电,然后主核按照正常流程启动运行,而所有从核则会调用 WFE 指令进入低功耗状态,等待来自主核的 SEV 指令唤醒自己。

1.2　通过 SMC 指令启动从核

通过 SMC 指令启动从核需要依赖 ARM 处理器的电源管理 PSCI 接口,通过 PSCI 接口主核可以控制对从核进行上下电等操作。

ARM 体系结构手册中与通过 SMC 指令启动从核相关的描述如下:

SMC 是用于低运行级别向高运行级别请求服务的指令,SMC 可以陷入 EL3 最高安全的运行级别,高运行级别会根据 SMC 指令传递的参数来决定提供什么样的服务。

在 AARCH64 架构下的 ARM 处理器,每块 SOC 可以包含多个簇(cluster),每个簇又可以包含多个核。通过 ARM 处理器的 PSCI 接口,可以对每个簇或者每个核进行独立的上下电操作。

ARM 处理器实现了安全和非安全两种运行状态,以及 EL0 ~ EL3 共 4 个不同级别的异常等级。其中 EL3 为最高级别的异常等级,并且工作在安全状态下。为了调用 PSCI 接口对处理器的各个核进行上下电操作,ARM 处理器必须通过 SMC 指令进入最高安全状态下的 EL3 运行级别。

通过 SMC 指令调用 PSCI 接口时需要传递的参数信息包括:接口功能 ID 以及执行该功能所需的其他数据。启动从核运行时需要调用 PSCI 的 CPU_ON 接口,该接口对应的功能 ID 为 0xC4000003,同时还需要提

供目标核号以及入口地址。CPU_ON 接口执行完成之后,会将执行结果返回给调用 SMC 指令的主核,该返回值可以是启动成功或者启动失败的错误码。

总结:当采用 SMC 指令方式启动从核时,系统上电后只会给主核供电,所有从核都处于 POWER_OFF 状态。然后主核按照正常流程启动运行,而所有从核则会等待来自主核的 SMC 指令唤醒自己。

2 天脉操作系统的从核启动

基于 ARM 多核处理器的天脉操作系统不同版本,既有采用 SEV 指令启动从核的方式,也有采用 SMC 指令启动从核的方式。这两种启动方式对应的从核启动核心代码分述如下。

2.1 SEV 指令启动代码分析

天脉操作系统通过 SEV 指令启动从核的核心代码如图 1、图 2 所示。

从图 1 的启动代码可以看出,主核和从核上电后同时启动运行,然后在初始化阶段根据获取的 CPU 核号分别进入不同的分支流程。主核分支继续按正常流程执行,从核分支则通过执行 WFE 指令进入低功耗等待唤醒状态。当从核被唤醒以后,通过读取从核启动标志的值来判断是否是被主核的 SEV 指令唤醒,如果是则跳转进入从核启动地址继续执行;如果从核不是被主核的 SEV 指令唤醒,则会继续执行 WFE 重新进入低功耗等待唤醒状态。

```
    ....
    MRC     p15,0,r1,c0,c0,5     /* 获取当前的核号 */
    cmp     r1,#0                /* 判断是否为主核，0为主核号 */

    beq     master_cpu           /* 主核则跳转到主核分支继续执行 */

slave_cpu: /* 非主核则进入从核分支 */

    wfe     /* 执行WFE指令进入低功耗等待唤醒模式 */

    /* 从核被外部事件唤醒之后，继续执行以下代码 */
    ldr     r0, =(SLAVE_START_FLAG_ADDR)
    ldr     r1,[r0]       /* 首先读取从核启动标志 */

    /* 判断从核启动标志是否为0
     * 从核启动标志为0表示此次并非被主核SEV指令唤醒 */
    cmp     r1,#0

    beq     slave_cpu /* 非SEV指令唤醒则继续进入从核等待唤醒分支 */

    /* 被主核SEV指令唤醒则跳转进入从核启动地址 */
    ldr     r1,=__slave_start_addr
    mov     pc,r1

master_cpu:
    ....
```

图 1 主从核初始化阶段的代码

```
 ....

/* 设置从核启动标志为 1 */
*(UINT32 *)(SLAVE_START_FLAG_ADDR) = 1;

/* 执行 SEV 指令唤醒所有从核 */
__asm__ __volatile__("sev");

 ....
```

图 2 SEV 指令启动从核的代码

图 2 主核启动从核的代码则简单明了:首先设置从核启动标志值为 1,然后调用 SEV 指令唤醒所有从核。

2.2 SMC 指令启动代码分析

天脉操作系统通过 SMC 指令启动从核的核心代码如图 3 所示。

从图 3 的启动从核代码可以看出,主核在调用 SMC 指令启动从核之前,需要传入 3 个执行参数:

1)CPU_ON 命令的标识 0xC4000003;

2)从核的核号;

3)从核的启动地址。

与 SEV 指令一次唤醒所有从核不同,SMC 指令每次只能给一个从核执行上电操作。因此,主核需要多

次调用 StartSlaveCore 函数,每次传入不同的从核 ID(0x2、0x4、0x8)。

```
/* 启动指定的从核 */
void StartSlaveCore(UINT32 CoreId){
  UINT32 input[7]  = {0}; /* 输入参数 */
  UINT32 output[7] = {0}; /* 输出参数 */

  ....
  /* 执行CPU_ON的命令ID */
  input[0] = 0xC4000003;
  /* 指定需要上电的从核号 */
  input[1] = CoreId;
  /* 指定从核的启动地址 */
  input[2] = (UINT32)(slave_start_addr);

  /* 调用SMC指令请求给从核上电 */
  exeSmcCall(&input[0], &output[0]);
  ....
}

  ....
  /* 启动三个从核运行 */
  StartSlaveCore(0x2);
  StartSlaveCore(0x4);
  StartSlaveCore(0x8);
  ....
```

图 3　SMC 指令启动从核的代码

3　VIRT 模拟器的从核启动

通过分析 VIRT 模拟器的源码发现,VIRT 模拟器在默认情况下会将 ARM 处理器的所有核全部加电运行。此种情况与通过 SEV 指令启动从核的方式一致,但是并不适用于通过 SMC 指令启动从核的方式。

在 SMC 指令启动从核的方式下,主核只有在完成相关硬件初始化之后,才会执行 SMC 指令给从核上电。即:所有从核默认当自己上电运行时,已经由主核将相关硬件初始化完毕[2]。而在 VIRT 模拟器的实现代码中,主从核是同时上电运行,从核运行时主核并没有完成对相关硬件的初始化。

进一步分析 VIRT 模拟器的源码发现,VIRT 模拟器也是可以支持在启动阶段不给从核上电。该行为由 VIRT 模拟器的 PSCI 属性进行控制。VIRT 模拟器支持将自身的 PSCI 属性设置为以下 3 种值:

1)QEMU_PSCI_CONDUIT_DISABLED;

2)QEMU_PSCI_CONDUIT_ HVC;

3)QEMU_PSCI_CONDUIT_ SMC。

其中,QEMU_PSCI_CONDUIT_DISABLED 为默认值,表示不支持 PSCI,即启动后所有 ARM 处理器核心同时上电;QEMU_PSCI_CONDUIT_HVC 不在本文讨论范围之内;QEMU _PSCI _CONDUIT_ SMC 表示通过 SMC 指令支持 PSCI 功能。当通过 SMC 指令启动从核时,需要将 VIRT 模拟器的 PSCI 属性值设置为 QEMU_PSCI_CONDUIT_ SMC。

将 VIRT 模拟器的 PSCI 属性值设置为 QEMU_PSCI_CONDUIT_ SMC 之后,就可以通过执行 SMC 指令调用 PSCI 的各种接口功能,包括启动从核所需的 CPU_ON 功能。

继续分析 VIRT 模拟器 PSCI 的 CPU_ON 功能实现,发现在执行从核上电过程中,VIRT 模拟器将 ARM 处理器的所有核,从 0 开始采用自然递增的方式进行编号,即主核号为 0,从核号按顺序依次为:1,2,3,…。这样的从核编号方式与天脉操作系统所运行的真实硬件对从核的编号方式并不相同。天脉操作系统对从核采用了按位分配的编号方式,即主核号同样为 0,从核号则按顺序依次为:0x2、0x4、0x8、0x16…。

通过以上分析可知,为了让 VIRT 模拟器能够支持天脉操作系统以 SMC 方式启动从核,需要对 VIRT 模拟器做以下改动:

1)将 VIRT 模拟器对 PSCI 的支持方式设置为 QEMU_PSCI_CONDUIT_ SMC;

2)将 VIRT 模拟器对 ARM 处理器的从核编码方式修改为按位标识。

以上两点改动的相关代码如图 4、图 5 所示。

```
....
vms->psci_conduit = QEMU_PSCI_CONDUIT_SMC;

....
if (vms->psci_conduit != QEMU_PSCI_CONDUIT_DISABLED) {
    /* 设置所有从核初始状态为 powered-off */
    if (n > 0) {
        object_property_set_bool(cpuobj, "start-powered-off", true, NULL);
    }
}
....
```

图 4　设置 PSCI 属性及从核启动状态

(下转第 104 页)

到负载平衡,也可以提高专用 IO 设备的资源利用率。

4 结束语

本文分析了机载软件开发过程对效能监视的需求、研究了效能监视的范畴和效能监视工具的架构,并根据/针对嵌入式操作系统给出一组效能监视工具的设计与实现。对比国外先进厂商的监视产品,效能监视工具在运行模式、稳定性、数据图形化表达等方面仍存在不少差距,今后仍有较大的改进空间。

参考文献:

[1] 林卓,齐晓斌,田丹. 基于运行时嵌入式系统的动态升级技术研究[J]. 航空计算技术,2022,52(6):93 - 97.

[2] Luecke K. What is the Current State of Software Development for Multi- core Processors[R]. USA: Infotech@ Aerospace, 2011.

[3] Robert W M. The Aircraft's Place in the IOT Revolution[J]. Avionics Magazine,2016(6/7):16 - 19.

[4] Dyer M, Greenhill C. The Complexity of Counting Graph Homomorphisms[J]. Random Structures & Algorithms,2000,17(3 - 4):260 - 289.

[5] 陈贝,许庆国. 基于静态检测的 C ++ 内存泄漏分析[J]. 计算机工程与科学,2017,39(1):118 - 124.

[6] 李肖坚,钟达夫,夏冰,等. 缓冲区溢出原理及植入代码的分析研究[J]. 计算机应用研究,2007,24(1):164 - 166.

(上接第 99 页)

```
  ....
  /* 初始化处理器核号的映射关系 */
  g_arm_cpuid_map[0] = 0 ;
  g_arm_cpuid_map[1] = 0x2 ;
  g_arm_cpuid_map[2] = 0x4 ;
  g_arm_cpuid_map[3] = 0x8 ;
  ....

/* 给处理器核执行上电操作 */
int arm_set_cpu_on ( uint64_t cpuid, .... ){
  ....
  int i ;
  uint64_t qemu_cpu_id ;

  /* cpuid: 操作系统执行SMC指令时传入的核号
   * qemu_cpu_id: QEMU执行上电操作时使用的核号
   * 二者的映射关系记录在数组g_arm_cpuid_map中
   */

  /* 在处理器核号映射数组中查找cpuid */
  for ( i=0; i<ELEMENTS_OF(g_arm_cpuid_map); i++ ){
      if(g_arm_cpuid_map[i] == cpuid){
          qemu_cpu_id = i ; /* 设置qemu_cpu_id */
          break;
      }
  }

  if ( i >= ELEMENTS_OF(g_arm_cpuid_map) ){
      printf("UnMapped cpuid:%llx \n",cpuid);
      return -1 ;
  }

  ....
}
```

图 5 处理模拟器与真实硬件的核号映射关系

4 结束语

天脉操作系统对 ARM 处理器从核的启动方式完全遵守 ARM 体系架构说明文档中的描述。在 VIRT 模拟器上运行天脉操作系统时出现从核不能启动成功的问题,是因为 VIRT 模拟器与天脉操作系统使用的真实硬件在 CPUID 定义以及初始上电状态两方面存在差异。通过修改 VIRT 模拟器源码消除这些差异之后,天脉操作系统即可成功启动运行模拟的 ARM 处理器从核。

本文在 CPUID 的映射关系方面依然存在不足之处:每次映射关系改变之后,都需要修改 VIRT 模拟器源码。如何在不修改 VIRT 模拟器源码的情况下,适应真实硬件改变所带来的 CPUID 映射关系改变,是下一步需要研究的内容。

参考文献:

[1] 郝继峰,胡宁,任晓瑞,等. 嵌入式多核操作系统的形式化建模与验证[J]. 航空计算技术,2022,52(6):124 - 128.

[2] 陈思宇,王鹏德,孙嘉懿. FT - 2000A/2 处理器应用验证板卡设计 [J]. 航空计算技术,2023,53(1):77 - 81.

[3] The QEMU Project Developers. QEMU Documentation: Release 6.1.0[S/OL]. [2021 - 08 - 24]. www. qemu. org.

[4] 葛文博,柴小丽,张淡墨. 国产 ARM 架构芯片的多核启动方法研究[J]. 单片机与嵌入式系统应用,2022,22(12):12 - 15,27.

[5] 陈瑀,罗永红,李春雷. 基于 QEMU 的全数字仿真环境设计[J]. 环境技术,2016(8):46 - 49.

[6] 张东昕,段小虎,段宇博. 基于 FT - 2000/4 处理器的启动机制设计[J]. 信息技术与信息化,2023,(4):168 - 171.

[7] ARM. ARM Architecture Reference Manual: ARMv7 - A and ARMv7- R edition[S/OL]. [2012 - 07 - 24]. www. arm. com.

[8] ARM. ARM Architecture Reference Manual: ARMv8, for ARMv8 - A Architecture Profile[S/OL]. [2013 - 12 - 24]. www. arm. com.

[9] 李鑫志,戈志华,刘向明. 基于 ARM 平台 AMP 架构下从核重复加载设计与实现[J]. 计算机应用与软件,2017,34(1):218 - 221.