

(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
2016 年 10 月 6 日 (06.10.2016)



(10) 国际公布号
WO 2016/155524 A1

- (51) 国际专利分类号:
G06F 21/57 (2013.01)
- (21) 国际申请号: PCT/CN2016/076830
- (22) 国际申请日: 2016 年 3 月 21 日 (21.03.2016)
- (25) 申请语言: 中文
- (26) 公布语言: 中文
- (30) 优先权:
201510142360.X 2015 年 3 月 27 日 (27.03.2015) CN
- (71) 申请人: 阿里巴巴集团控股有限公司 (ALIBABA GROUP HOLDING LIMITED) [—/CN]; 开曼群岛英属开曼群岛大开曼资本大厦一座四层 847 号邮箱, Grand Cayman (KY)。
- (72) 发明人: 罗金华 (LUO, Jinhua); 中国浙江省杭州市余杭区文一西路 969 号 3 号楼 5 楼阿里巴巴集团法务部, Zhejiang 311121 (CN)。于志斌 (YU, Zhibin); 中国浙江省杭州市余杭区文一西路 969 号 3 号楼 5 楼阿里巴巴集团法务部, Zhejiang 311121 (CN)。
- (74) 代理人: 北京三友知识产权代理有限公司 (BEIJING SANYOU INTELLECTUAL PROPERTY AGENCY LTD.); 中国北京市金融街 35 号国际企业大厦 A 座 16 层, Beijing 100033 (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, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, 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, GH, GM, KE, LR, LS, MW, MZ, NA, RW, 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, 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))。

(54) Title: METHOD AND APPARATUS FOR REALIZING SAFE UPGRADE OF SYSTEM

(54) 发明名称: 一种系统安全升级的方法和装置

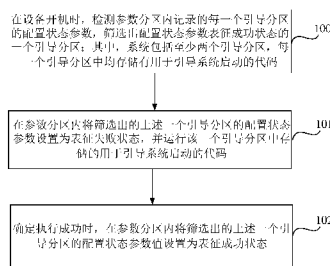


图 1

100 Detecting the configuration state parameter of each of boot partitions recorded in a parameter partition and sifting a single boot partition whose configuration state parameter represents a successful state when the device is started; wherein, the system includes at least two boot partitions and codes for booting up the system are stored in each of boot partitions

101 Setting the configuration state parameter of the above sifted boot partition to represent a failure state in the parameter partition, and executing codes for booting up the system stored in the boot partition

102 Setting the configuration state parameter of the above sifted boot partition to represent the successful state in the parameter partition when the execution is determined to be successful

(57) Abstract: A method and apparatus for realizing safe upgrade of a system are disclosed to solve the problem of high unavailability rate of a device due to the upgrade of the system. The method includes: detecting the configuration state parameter of each of boot partitions recorded in a parameter partition and sifting a single boot partition whose configuration state parameter represents a successful state when the device is started; setting the configuration state parameter of the above sifted boot partition to represent a failure state in the parameter partition, and executing codes for booting up the system stored in the boot partition; and setting the configuration state parameter value of the above sifted boot partition to represent the successful state in the parameter partition when the execution is determined to be successful. Thus, the probability that the device is unavailable due to the upgrade of the system can be reduced significantly, the reliability of the system is improved, the usability of the device is improved, and the system is ensured to be upgraded safely and reliably.

(57) 摘要: 本发明公开了一种系统安全升级的方法和装置, 以解决由于系统升级出现的设备不可用率高的情况。该方法为, 在设备开机时, 检测参数分区内记录的每一个引导分区的配置状态参数, 筛选出配置状态参数表征成功状态的一个引导分区; 在参数分区内将筛选出的上述一个引导分区的配置状态参数设置为表征失败状态, 并运行该引导分区中存储的用于引导系统启动的代码; 确定执行成功时, 在参数分区内将筛选出的上述一个引导分区的配置状态参数值设置为表征成功状态。这样, 能够大大降低由于系统升级导致设备不可用的概率, 提升系统的可靠性, 提高设备的可用性, 确保系统能够安全可靠地升级。



WO 2016/155524 A1

一种系统安全升级的方法和装置

本申请要求 2015 年 03 月 27 日递交的申请号为 201510142360.X、发明名称为“一种系统安全升级的方法和装置”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。

5

技术领域

本发明涉及计算机领域，尤其涉及一种系统安全升级的方法和装置。

背景技术

10 系统升级，通常包括引导分区（bootloader），OS，中间件，应用等组件的升级。在嵌入式产品，如智能电视机，各种盒子如交互式网络电视（Internet protocol TV，IPTV）盒子，过顶（Over The Top，OTT）盒子，数字视频广播（Digital Video Broadcasting，DVB）盒子，机顶盒等，其内置的存储器通常是计算机闪存设备（NAND）介质或者内嵌式存储器（Embedded Multi Media Card，eMMC）介质，NAND 和 eMMC 的特点是容
15 易出现坏块、导致其损坏。系统升级会加大对 NAND 或 eMMC 的读写，如果在升级过程中，突然断电，更会使存储介质损坏的可能性大大增加。常见的升级，例如：安卓系统的升级通常包括对 bootloader，操作系统内核（kernel），系统（system），恢复（recovery），缓存（cache）等分区的内容进行更新。系统在线升级的时候，往往更新其中部分分区或者全部分区的内容。

20 由此可知，系统升级包括全部升级和部分升级。通常的做法是依次更新 bootloader，kernel，system 等分区的内容，如果关键分区如 bootloader 分区由于断电导致破坏，整个系统将无法启动，设备无法正常运行，俗称导致设备变“砖”。

发明内容

25 本发明的目的是提供一种系统安全升级的方法和装置，以解决由于系统升级出现的设备不可用率高的情况。

本发明的目的是通过以下技术方案实现的：

一种系统安全升级的方法，包括：

30 在设备开机时，检测参数分区内记录的每一个引导分区的配置状态参数，筛选出配置状态参数表征成功状态的一个引导分区；其中，系统包括至少两个引导分区，每一个

引导分区中均存储有用于引导系统启动的代码；

在所述参数分区内将筛选出的所述一个引导分区的配置状态参数设置为表征失败状态，并运行所述一个引导分区中存储的用于引导系统启动的代码；

确定执行成功时，在所述参数分区内将筛选出的所述一个引导分区的配置状态参数
5 值设置为表征成功状态。

这样，能够大大降低由于系统升级时关键分区损坏导致设备不可用的概率，利用多个引导分区实现设备的快速恢复启动，不影响系统的正常运行时间，为用户提供了方便，进一步提升系统的可靠性，提高设备的可用性，确保系统能够安全可靠地升级。

较佳的，在设备首次开机之前，将参数分区内记录的每一个引导分区的配置状态参
10 数值均设置为表征成功状态。

较佳，系统包括的至少两个引导分区为相同的引导分区，所述系统为嵌入式系统。

可选的，在设备开机时，检测参数分区内记录的每一个引导分区的配置状态参数，筛选出配置状态参数表征成功状态的一个引导分区，具体包括：

在设备开机后，执行只读芯片 ROM 中保存的引导代码；

15 在引导代码执行完毕后，通过执行初始化分区中存储的代码，依次检测参数分区内记录的每一个引导分区的配置状态参数；其中，每读取一个引导分区的配置状态参数，判断是否表征成功状态，若是，则将所述一个引导分区标记为待操作引导分区，否则，将所述一个引导分区标记为待修复引导分区；

从已标记的待操作引导分区中筛选出一个引导分区。

20 可选的，确定执行成功时，在所述参数分区内将所述一个引导分区的配置状态参数值设置为表征成功状态之后，进一步包括：

将所述一个引导分区内存储的代码复制到每一个已标记的待修复引导分区中；

每确定所述一个引导分区内存储的代码成功复制到一个待修复引导分区后，在参数分区内将所述一个待修复引导分区的配置状态参数值设置为表征成功状态。

25 一种系统安全升级的装置，包括：

筛选单元，用于在该设备开机时，检测参数分区内记录的每一个引导分区的配置状态参数，筛选出配置状态参数表征成功状态的一个引导分区；其中，系统包括至少两个引导分区，每一个引导分区中均存储有用于引导系统启动的代码；

30 处理单元，用于在所述参数分区内将筛选出的所述一个引导分区的配置状态参数设置为表征失败状态，并运行所述一个引导分区中存储的用于引导系统启动的代码；

确定单元，用于确定执行成功时，在所述参数分区内将筛选出的所述一个引导分区的配置状态参数值设置为表征成功状态。

这样，能够大大降低由于系统升级时关键分区损坏导致设备不可用的概率，利用多个引导分区实现设备的快速恢复启动，不影响系统的正常运行时间，为用户提供了方便，

5 进一步提升系统的可靠性，提高设备的可用性，确保系统能够安全可靠地升级。

较佳的，所述筛选单元检测的系统包括的至少两个引导分区为相同的引导分区，所述系统为嵌入式系统。

较佳的，所述筛选单元进一步用于：

在设备首次开机之前，将参数分区内记录的每一个引导分区的配置状态参数值均设

10 置为表征成功状态。

较佳的，在设备开机时，检测参数分区内记录的每一个引导分区的配置状态参数，筛选出配置状态参数表征成功状态的一个引导分区时，所述筛选单元具体用于：

在设备开机后，执行只读芯片 ROM 中保存的引导代码；

在引导代码执行完毕后，通过执行初始化分区中存储的代码，依次检测参数分区内

15 记录的每一个引导分区的配置状态参数；其中，每读取一个引导分区的配置状态参数，判断是否表征成功状态，若是，则将所述一个引导分区标记为待操作引导分区，否则，将所述一个引导分区标记为待修复引导分区；

从已标记的待操作引导分区中筛选出一个引导分区。

较佳的，确定执行成功时，在所述参数分区内将筛选出的所述一个引导分区的配置

20 状态参数值设置为表征成功状态之后，所述确定单元进一步用于：

将筛选出的所述一个引导分区内存储的代码复制到每一个已标记的待修复引导分区中；

每确定筛选出的所述一个引导分区内存储的代码成功复制到一个待修复引导分区后，在参数分区内将所述一个待修复引导分区的配置状态参数值设置为表征成功状态。

25

附图说明

图 1 为本发明实施例中系统安全升级的方法流程示意图；

图 2 为本发明实施例中参数分区的示意图；

图 3 为本发明实施例中安卓设备的存储器分区示意图；

30 图 4 为本发明实施例中系统安全升级的装置结构示意图。

具体实施方式

下面将结合本发明实施例中的附图，对本发明实施例中的技术方案进行清楚、完整地描述，显然，所描述的实施例仅仅是本发明一部分实施例，并不是全部的实施例。基于本发明中的实施例，本领域普通技术人员在没有做出创造性劳动前提下所获得的所有其他实施例，都属于本发明保护的范围。

存储介质（如 NAND/eMMC）的分区管理与系统升级密切相关。通常系统升级时，执行完芯片上的引导代码（ROM code）后总是跳转到固定分区执行其相关代码，而不会根据分区是否损坏跳转到别的分区，如果升级过程中关键分区例如引导分区（bootloader）由于断电出现毁坏情况时，会导致系统升级无法正常进行，进一步导致设备不可用，影响用户的正常使用。和通常的做法不同，本发明实施例中设计了初始化（Init）分区，并对引导分区进行了多个分区的备份，用以大大提高系统升级的可靠性。

参阅图 1 所示，本发明实施例中，提供一种系统安全升级的方法，具体流程如下：

步骤 100：在设备开机时，检测参数分区内记录的每一个引导分区的配置状态参数，筛选出配置状态参数表征成功状态的一个引导分区；其中，系统包括至少两个引导分区，每一个引导分区中均记录有用于引导系统启动的代码。

具体的，系统包括的至少两个引导分区为相同的引导分区，可以互为备份，该系统为嵌入式系统。

进一步的，在设备次开机之前，将参数分区内记录的每一个引导分区的配置状态参数数值均设置为表征成功状态。

例如，参数（parameter）分区采用 key-value 方式存放一些启动过程必须的参数，包括表征引导分区的配置状态的参数，具体的，可参阅图 2 所示，用“SUCCESS”表征成功的配置状态，用“FAILED”表征失败的配置状态，在设备首次开机（即出厂）之前，将参数分区内记录的每一个引导分区的配置状态参数值均设置为“SUCCESS”状态。

具体的，在设备开机时，检测参数分区内记录的每一个引导分区的配置状态参数，筛选出配置状态参数表征成功状态的一个引导分区，具体过程为：在设备开机后，执行只读芯片 ROM 中保存的引导代码；在引导代码执行完毕后，通过执行初始化分区中存储的代码，依次检测参数分区内记录的每一个引导分区的配置状态参数；其中，每读取一个引导分区的配置状态参数，判断是否表征成功状态，若是，则将该一个引导分区标记为待操作引导分区，否则，将该一个引导分区标记为待修复引导分区；从已标记的待

操作引导分区中筛选出一个引导分区。

步骤 101：在参数分区内将筛选出的上述一个引导分区的配置状态参数设置为表征失败状态，并运行该一个引导分区中存储的用于引导系统启动的代码。

5 步骤 102：确定执行成功时，在参数分区内将筛选出的上述一个引导分区的配置状态参数值设置为表征成功状态。

需要说明的是，这里检测到一个配置状态为成功状态的引导分区后，执行该引导分区的代码时，将该引导分区的配置状态设置为失败状态，在成功执行完该引导分区的代码后，将该引导分区的配置状态设置为成功状态，这样做能够确保在执行完某一个引导分区的代码后，参数分区中保存的该分区的配置状态是正确的，如果不执行这样的操作，在执行引导分区的代码时若由于断电或电路板短路等原因导致升级失败时，将导致
10 参数分区内记录该引导分区的配置状态出现错误，再次升级时可能会出现升级失败的情形。

进一步的，确定执行成功时，在参数分区内将筛选出的上述一个引导分区的配置状态参数值设置为表征成功状态之后，将上述一个引导分区内存储的代码复制到每一个已
15 标记的待修复引导分区中；每确定上述一个引导分区内存储的代码成功复制到一个待修复引导分区后，在参数分区内将该一个待修复引导分区的配置状态参数值设置为表征成功状态。

例如，系统中存在两个引导分区，这两个引导分区互为备份，这里用 `bootloader0` 和 `bootloader1` 来表示这个互为备份的引导分区，检测到 `bootloader0` 的配置状态为
20 “SUCCESS” 状态，`bootloader1` 的配置状态为 “FAILED” 状态，设备开机后成功执行完 `bootloader0` 中存储的代码后，需要将 `bootloader0` 中存储的代码复制到 `bootloader1` 中，在确定 `bootloader0` 中存储的代码成功复制到 `bootloader1` 中后，将 `bootloader1` 的配置状态修改为 “SUCCESS” 状态，这样，能够实现对出现毁坏情况的引导分区恢复至正常情况。

进一步的，需要说明的是，初始化分区、引导分区以及设备的存储器的其他分区的
25 代码执行，都是先将分区的代码下载（load）到内存中（如 DDR 或 IRAM），CPU 从内存中读取对应分区的代码进行加载。

具体的，下面以一安卓（Android）设备的存储器分区为例针对上述系统安全升级的方法进行详细说明。

Android 设备的存储器即 eMMC/NAND 分区情况，参阅图 3 所示，包括：Parameter，
30 Init 区，Bootloader0，Bootloader1，…BootloaderN，Kernel，Android，recovery，cache，

其他（other）等分区。其中：

Parameter 分区采用简单的 key-value 方式存放一些启动过程中必须的参数，包括 bootloder0/bootloder1/...bootloderN 的配置（boot）状态。这里用“SUCCESS”表征成功的配置状态，用“FAILED”表征失败的配置状态，初始化时，这些引导分区的状态都是“SUCCESS”状态。

Init 分区存储有一段初始化代码，该初始化代码根据 parameter 分区的记录的引导分区的参数决定跳转到哪个引导分区，其中 BootLoader0, BootLoader1,...BootLoaderN 是同一个引导分区的多个备份。

每一个引导分区都存储有一段为启动操作系统做准备的代码，为启动操作系统做准备。

Kernel 分区是指操作系统的内核分区，通常存储有内核、驱动相关代码，如 Linux kernel；android 分区包括 android 相关的组件，通常存储有 android 相关的框架代码、虚拟机代码、用到的库等；recovery 分区是指 android 的 recovery 分区，该分区包含一个简单的 Linux 系统，用于升级；cache 分区用以保存系统升级下载的升级包；Other 分区是指其他分区，由各个产品自己定义。

当设备开机时，最先执行只读芯片“ROM”芯片里面的代码即引导代码（ROM code），该引导代码执行完毕之后，会跳转到 Init 分区的代码，Init 分区的代码会检查 parameter 分区的 Bootloder0_Boot_state 的值，如果是“SUCCESS”，则从该分区执行；如果是“FAILED”，记录 Bootloder_Boot_state = FAILED 的引导分区，进一步的继续检查 Bootloder1_Boot_state 的值...如此下去，直到找到一个配置状态为“SUCCESS”的引导分区执行该分区存储的代码。在执行一个引导分区存储的代码时，首先把该引导分区对应的 Bootloder_Boot_state 设置为“FAILED”，直到引导分区存储的代码成功执行完毕后才把其对应的 Bootloder_Boot_state 改为“SUCCESS”。如果该引导分区存储有损坏的代码，导致该引导分区存储的代码将不会被完全成功执行，从而该引导分区对应的 Bootloder_Boot_state 不会被改写为“SUCCESS”。在该引导分区存储的代码成功执行完毕之后，要负责恢复 Bootloder_Boot_state = FAILED 的引导分区，即把该引导分区存储的代码复制到损坏的备份引导分区中，在确定该引导分区存储的代码成功复制到损坏的备份引导分区中之后，将损坏的备份引导分区的配置状态修改为“SUCCESS”；最后把执行权交给 kernel 做后面的启动过程，此过程不做详细描述。

需要说明的是，通常情况下，设备开机时执行完 ROM code 后总是跳转到固定分

区执行，而不会根据分区是否损坏跳转到别的分区。本发明实施例中，设备开机时执行完 ROM code 后通过跳转到 Init 分区，Init 分区根据 parameter 分区中记录的引导分区的配置状态决定跳转到哪个引导分区中，由于 Init 分区的内容不会通过系统升级而改变，所以理论上该分区不会因为升级而损坏，而 bootloader 的多个备份机制保证了 bootloader 5 的可靠性。Kernel 等其他分区只有在恢复(recovery)模式下进行更新，如果更新失败（如断电），重启后，恢复(recovery)模式会继续更新 kernel 等分区的内容，从而保证了其他分区的可靠性，Recovery 模式特指 Android recovery 模式，其实质是更新升级包。

基于上述技术方案，参阅图 4 所示，本发明实施例中提供一种系统安全升级的装置，包括：筛选单元 40，处理单元 41 和确定单元 42，其中：

10 筛选单元 40，用于在设备开机时，检测参数分区内记录的每一个引导分区的配置状态参数，筛选出配置状态参数表征成功状态的一个引导分区；其中，系统包括至少两个引导分区，每一个引导分区中均存储有用于引导系统启动的代码；

处理单元 41，用于在参数分区内将筛选出的上述一个引导分区的配置状态参数设置为表征失败状态，并运行该引导分区中存储的用于引导系统启动的代码；

15 确定单元 42，用于确定执行成功时，在参数分区内将筛选出的上述一个引导分区的配置状态参数值设置为表征成功状态。

较佳的，所述筛选单元检测的系统包括的至少两个引导分区为相同的引导分区，该系统为嵌入式系统。

较佳的，筛选单元 40 进一步用于：

20 在设备首次开机之前，将参数分区内记录的每一个引导分区的配置状态参数值均设置为表征成功状态。

较佳的，在设备开机时，检测参数分区内记录的每一个引导分区的配置状态参数，筛选出配置状态参数表征成功状态的一个引导分区时，筛选单元 40 具体用于：

在设备开机后，执行只读芯片 ROM 中保存的引导代码；

25 在引导代码执行完毕后，通过执行初始化分区中存储的代码，依次检测参数分区内记录的每一个引导分区的配置状态参数；其中，每读取一个引导分区的配置状态参数，判断是否表征成功状态，若是，则将该引导分区标记为待操作引导分区，否则，将该引导分区标记为待修复引导分区；

从已标记的待操作引导分区中筛选出一个引导分区。

30 较佳的，确定执行成功时，在参数分区内将筛选出的上述一个引导分区的配置状态

参数值设置为表征成功状态之后，确定单元 42 进一步用于：

将筛选出的上述一个引导分区内存储的代码复制到每一个已标记的待修复引导分区中；

每确定筛选出的该一个引导分区内存储的代码成功复制到一个待修复引导分区后，

5 在参数分区内将该待修复引导分区的配置状态参数值设置为表征成功状态。

综上所述，本发明实施例中，在设备开机时，检测参数分区内记录的每一个引导分区的配置状态参数，筛选出配置状态参数表征成功状态的一个引导分区；在参数分区内将上述一个引导分区的配置状态参数设置为表征失败状态，并运行该一个引导分区中存储的用于引导系统启动的代码；确定执行成功时，在参数分区内将上述一个引导分区的配置状态参数值设置为表征成功状态。这样，能够大大降低由于系统升级导致设备不可用的概率，提升系统的可靠性，提高设备的可用性，确保系统能够安全可靠地升级。

本领域内的技术人员应明白，本发明的实施例可提供为方法、系统、或计算机程序产品。因此，本发明可采用完全硬件实施例、完全软件实施例、或结合软件和硬件方面的实施例的形式。而且，本发明可采用在一个或多个其中包含有计算机可用程序代码的计算机可用存储介质（包括但不限于磁盘存储器、CD-ROM、光学存储器等）上实施的计算机程序产品的形式。

本发明是参照根据本发明实施例的方法、设备（系统）、和计算机程序产品的流程图和 / 或方框图来描述的。应理解可由计算机程序指令实现流程图和 / 或方框图中的每一流程和 / 或方框、以及流程图和 / 或方框图中的流程和 / 或方框的结合。可提供这些计算机程序指令到通用计算机、专用计算机、嵌入式处理机或其他可编程数据处理设备的处理器以产生一个机器，使得通过计算机或其他可编程数据处理设备的处理器执行的指令产生用于实现在流程图一个流程或多个流程和 / 或方框图一个方框或多个方框中指定的功能的装置。

这些计算机程序指令也可存储在能引导计算机或其他可编程数据处理设备以特定方式工作的计算机可读存储器中，使得存储在该计算机可读存储器中的指令产生包括指令装置的制造品，该指令装置实现在流程图一个流程或多个流程和 / 或方框图一个方框或多个方框中指定的功能。

这些计算机程序指令也可装载到计算机或其他可编程数据处理设备上，使得在计算机或其他可编程设备上执行一系列操作步骤以产生计算机实现的处理，从而在计算机或其他可编程设备上执行的指令提供用于实现在流程图一个流程或多个流程和 / 或方框图

一个方框或多个方框中指定的功能的步骤。

尽管已描述了本发明的优选实施例，但本领域内的技术人员一旦得知了基本创造性概念，则可对这些实施例作出另外的变更和修改。所以，所附权利要求意欲解释为包括优选实施例以及落入本发明范围的所有变更和修改。

- 5 显然，本领域的技术人员可以对本发明实施例进行各种改动和变型而不脱离本发明实施例的精神和范围。这样，倘若本发明实施例的这些修改和变型属于本发明权利要求及其等同技术的范围之内，则本发明也意图包含这些改动和变型在内。

权 利 要 求 书

1、一种系统安全升级的方法，其特征在于，包括：

在设备开机时，检测参数分区内记录的每一个引导分区的配置状态参数，筛选出配置状态参数表征成功状态的一个引导分区；其中，系统包括至少两个引导分区，每一个引导分区中均存储有用于引导系统启动的代码；

在所述参数分区内将筛选出的所述一个引导分区的配置状态参数设置为表征失败状态，并运行所述一个引导分区中存储的用于引导系统启动的代码；

确定执行成功时，在所述参数分区内将筛选出的所述一个引导分区的配置状态参数值设置为表征成功状态。

2、如权利要求 1 所述的方法，其特征在于，进一步包括：

在设备首次开机之前，将参数分区内记录的每一个引导分区的配置状态参数值均设置为表征成功状态。

3、如权利要求 1 所述的方法，其特征在于，系统包括的至少两个引导分区为相同的引导分区，所述系统为嵌入式系统。

4、如权利要求 1、2 或 3 所述的方法，其特征在于，在设备开机时，检测参数分区内记录的每一个引导分区的配置状态参数，筛选出配置状态参数表征成功状态的一个引导分区，具体包括：

在设备开机后，执行只读芯片 ROM 中保存的引导代码；

在引导代码执行完毕后，通过执行初始化分区中存储的代码，依次检测参数分区内记录的每一个引导分区的配置状态参数；其中，每读取一个引导分区的配置状态参数，判断是否表征成功状态，若是，则将所述一个引导分区标记为待操作引导分区，否则，将所述一个引导分区标记为待修复引导分区；

从已标记的待操作引导分区中筛选出一个引导分区。

5、如权利要求 4 所述的方法，其特征在于，确定执行成功时，在所述参数分区内将筛选出的所述一个引导分区的配置状态参数值设置为表征成功状态之后，进一步包括：

将筛选出的所述一个引导分区内存储的代码复制到每一个已标记的待修复引导分区中；

每确定筛选出的所述一个引导分区内存储的代码成功复制到一个待修复引导分区后，在参数分区内将所述一个待修复引导分区的配置状态参数值设置为表征成功状态。

6、一种系统安全升级的装置，其特征在于，包括：

筛选单元，用于在该设备开机时，检测参数分区内记录的每一个引导分区的配置状态参数，筛选出配置状态参数表征成功状态的一个引导分区；其中，系统包括至少两个引导分区，每一个引导分区中均存储有用于引导系统启动的代码；

5 处理单元，用于在所述参数分区内将所述一个引导分区的配置状态参数设置为表征失败状态，并运行所述一个引导分区中存储的用于引导系统启动的代码；

确定单元，用于确定执行成功时，在所述参数分区内将筛选出的所述一个引导分区的配置状态参数值设置为表征成功状态。

7、如权利要求 6 所述的装置，其特征在于，所述筛选单元检测的系统包括的至少
10 两个引导分区为相同的引导分区，所述系统为嵌入式系统。

8、如权利要求 6 所述的装置，其特征在于，所述筛选单元进一步用于：

在设备首次开机之前，将参数分区内记录的每一个引导分区的配置状态参数值均设置为表征成功状态。

9、如权利要求 6、7、8 所述的装置，其特征在于，在设备开机时，检测参数分区
15 内记录的每一个引导分区的配置状态参数，筛选出配置状态参数表征成功状态的一个引导分区时，所述筛选单元具体用于：

在设备开机后，执行只读芯片 **ROM** 中保存的引导代码；

在引导代码执行完毕后，通过执行初始化分区中存储的代码，依次检测参数分区内记录的每一个引导分区的配置状态参数；其中，每读取一个引导分区的配置状态参数，
20 判断是否表征成功状态，若是，则将所述一个引导分区标记为待操作引导分区，否则，将所述一个引导分区标记为待修复引导分区；

从已标记的待操作引导分区中筛选出一个引导分区。

10、如权利要求 9 所述的装置，其特征在于，确定执行成功时，在所述参数分区内将筛选出的所述一个引导分区的配置状态参数值设置为表征成功状态之后，所述确定单
25 元进一步用于：

将筛选出的所述一个引导分区内存储的代码复制到每一个已标记的待修复引导分区中；

每确定筛选出的所述一个引导分区内存储的代码成功复制到一个待修复引导分区后，在参数分区内将所述一个待修复引导分区的配置状态参数值设置为表征成功状态。

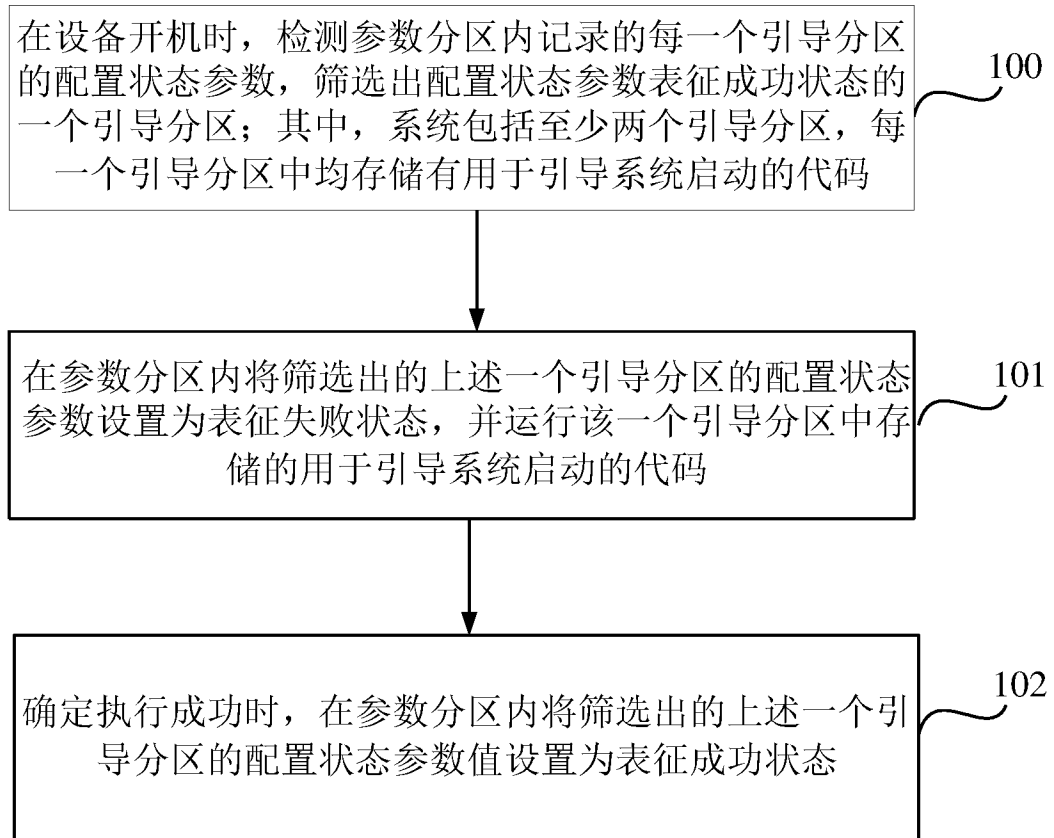


图 1

Parameter 分区

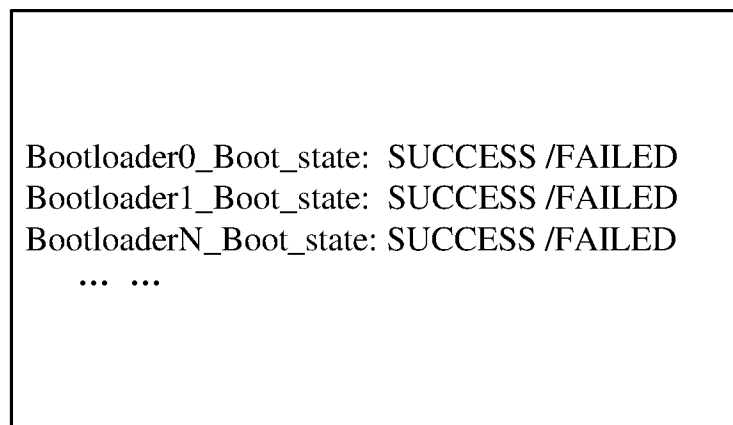


图 2

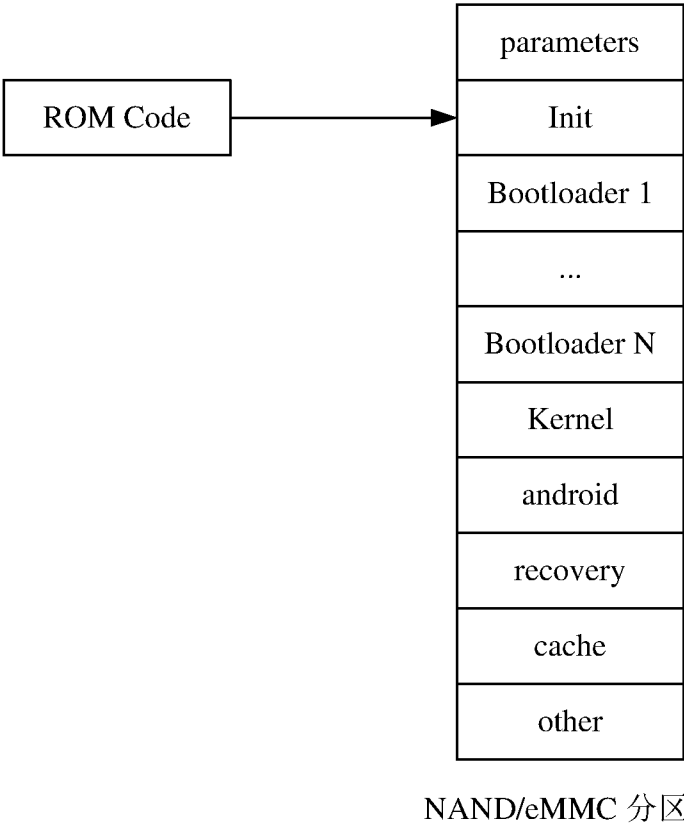


图 3

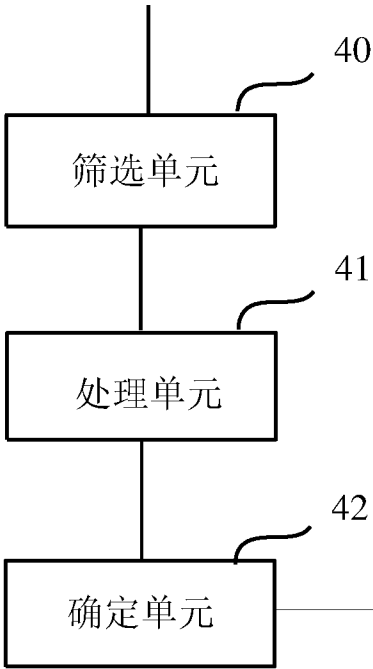


图 4

INTERNATIONAL SEARCH REPORT

International application No.

PCT/CN2016/076830

A. CLASSIFICATION OF SUBJECT MATTER

G06F 21/57 (2013.01) 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)

G06F 21/-

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)

CPRSABS; CNTXT; CNABS; DWPI; TWTXT: two, multiple, boot partition, status parameter, upgrade, update, section, multi-guide, system, parameter, status, startup, repair

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	CN 102289397 A (GOOSAT TECHNOLOGY (ZHUHAI) CO., LTD.), 21 December 2011 (21.12.2011), description, paragraphs [0006]-[0011]	1-10
A	CN 102104750 A (KONKA GROUP CO., LTD.), 22 June 2011 (22.06.2011), the whole document	1-10
A	CN 102508686 A (SUZHOU C2 MICROSYSTEMS CO., LTD.), 20 June 2012 (20.06.2012), the whole document	1-10

☐ Further documents are listed in the continuation of Box C.

☒ See patent family annex.

* Special categories of cited documents:	“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
“A” document defining the general state of the art which is not considered to be of particular relevance	“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
“E” earlier application or patent but published on or after the international filing date	“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
“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)	“&” document member of the same patent family
“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	

Date of the actual completion of the international search 20 May 2016 (20.05.2016)	Date of mailing of the international search report 30 May 2016 (30.05.2016)
Name and mailing address of the ISA/CN: State Intellectual Property Office of the P. R. China No. 6, Xitucheng Road, Jimenqiao Haidian District, Beijing 100088, China Facsimile No.: (86-10) 62019451	Authorized officer LI, Xiaoqing Telephone No.: (86-10) 62411891

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.

PCT/CN2016/076830

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
CN 102289397 A	21 December 2011	CN 102289397 B	13 February 2013
CN 102104750 A	22 June 2011	CN 102104750 B	11 February 2015
CN 102508686 A	20 June 2012	None	

A. 主题的分类 G06F 21/57 (2013. 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) G06F 21/- 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)) CPRSABS; CNTXT; CNABS; DWPI; TWTXT: 升级, 两个, 多个, 引导分区, 系统, 状态参数, 启动, 修复 upgrade, update, section, multi-guide, system, parameter, status, startup, repair		
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
X	CN 102289397 A (全星科技珠海有限公司) 2011年 12月 21日 (2011 - 12 - 21) 说明书第【0006】-【0011】段	1-10
A	CN 102104750 A (康佳集团股份有限公司) 2011年 6月 22日 (2011 - 06 - 22) 全文	1-10
A	CN 102508686 A (苏州希图视鼎微电子有限公司) 2012年 6月 20日 (2012 - 06 - 20) 全文	1-10
☐ 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 “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 2016年 5月 20日		国际检索报告邮寄日期 2016年 5月 30日
ISA/CN的名称和邮寄地址 中华人民共和国国家知识产权局 (ISA/CN) 中国北京市海淀区蓟门桥西土城路6号 100088 传真号 (86-10) 62019451		授权官员 李小青 电话号码 (86-10) 62411891

国际检索报告
关于同族专利的信息

国际申请号

PCT/CN2016/076830

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	102289397	A	2011年 12月 21日	CN 102289397 B	2013年 2月 13日
CN	102104750	A	2011年 6月 22日	CN 102104750 B	2015年 2月 11日
CN	102508686	A	2012年 6月 20日	无	