(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 103095826 A
(43)申请公布日 2013.05.08

(21)申请号 201310009809.6

(22)申请日 2013.01.10

(71)申请人 上海斐讯数据通信技术有限公司
地址 201616 上海市松江区广富林路 4855 弄 20 号、90 号

(72)发明人 王海涛

(74)专利代理机构 上海申新律师事务所 31272
代理人 袁亚军

(51)Int.Cl.
H04L 29/08(2006.01)
H04L 12/28(2006.01)
G06F 9/445(2006.01)

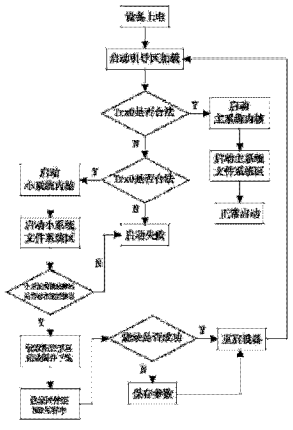
权利要求书2页 说明书7页 附图2页

(54)发明名称

一种网关设备升级保护的方法

(57)摘要

本发明涉及一种设备升级保护的方法，尤其涉及一种网关设备升级保护的方法，通过对 NOR 闪存进行合理的布局，以减小多次读写闪存造成的数据损失风险，并利用高度定制化、精简化的家庭网关小系统，在合理利用闪存存储空间的基础上，为后续固件的升级提供保证，进而实现在不影响家庭用户使用的状况下，为运营商远程固件升级提供一种可靠的、高效的机制，以便于运营商更好的满足用户需求，有针对性的提供高质量的网络服务。



CN 103095826 A

1. 一种网关设备升级保护的方法，应用在基于 Linux 系统开发的嵌入式设备上，所述网关设备采用 NOR 闪存作为存储器件，且该 NOR 闪存上设置有启动引导区、内核区、文件系统区和配置区，其特征在于：

所述 NOR 闪存还设置有小系统关键参数区；

所述文件系统区包括主系统文件系统区和小系统文件系统区，所述内核区包括主系统内核区和小系统内核区；

具体包括以下步骤：

步骤 S1：所述网关设备上电后，所述启动引导区进行加载；

步骤 S2：判断所述主系统内核区和 / 或所述主系统文件区是否合法；

若合法，则依次启动所述主系统的内核区和所述主系统的文件系统区，进行所述网关设备的正常启动；

若不合法，继续判断所述小系统内核区和 / 或所述小系统文件区是否合法；

步骤 S3：若所述小系统内核区和 / 或所述小系统文件区不合法，则启动失败；

若所述小系统内核区和所述小系统文件区合法，依次启动所述小系统的内核区和所述小系统的文件系统，并继续判断所述小系统关键参数区是否存在配置信息；

步骤 S4：若所述小系统关键参数区不存在配置信息，则启动失败；

若所述小系统关键参数区存在配置信息，则读取所述配置信息，完成固件下载，并烧录所述固件到所述 NOR 闪存中，并继续判断上述烧录是否成功；

步骤 S5：若所述烧录成功，则重启所述网关设备；

若所述烧录不成功，则保存参数，并重启所述网关设备。

2. 根据权利要求 1 所述的网关设备升级保护的方法，其特征在于，还包括：

当所述网关设备需要升级固件时，网络运营商通过广域网管协议告知家庭网关用户端；

所述家庭网关用户端获取并根据所述升级固件的网页地址、连接用户名和连接密码获取固件文件；

所述家庭网关用户端将所述固定文件烧录到所述 NOR 闪存中。

3. 根据权利要求 2 所述的网关设备升级保护的方法，其特征在于，还包括自动配置服务器；

所述家庭网关用户端将所述自动配置服务器下发的所述升级固件的网页地址、连接用户名和连接密码存入所述 NOR 闪存的关键信息区；

同时，所述家庭网关用户端还读取所述家庭网关的配置数据，获取并保存所述家庭网关所有广域网连接关系至所述 NOR 闪存的关键信息区；

所述家庭网关用户端通过 HTTP 协议获取并烧录所述固件文件至所述 NOR 闪存中；

重启所述家庭网关，完成固件升级操作。

4. 根据权利要求 1 所述的网关设备升级保护的方法，其特征在于，所述 NOR 闪存是基于块的可读写存储设备，且该 NOR 闪存每次进行读写操作时均基于一个块的操作。

5. 根据权利要求 4 所述的网关设备升级保护的方法，其特征在于，所述块的大小为 64k、128k 或 256k。

6. 根据权利要求 4 所述的网关设备升级保护的方法，其特征在于，所述启动引导区单

独占用一个块。

7. 根据权利要求 4 所述的网关设备升级保护的方法，其特征在于，所述启动引导区、主系统文件系统区、小系统文件系统区、所述主系统内核区、所述小系统内核区、所述配置区和所述小系统关键参数区的起始地址均为一个块的起始位置。

一种网关设备升级保护的方法

技术领域

[0001] 本发明涉及一种设备升级保护的方法，尤其涉及一种网关设备升级保护的方法。

背景技术

[0002] 目前，作为宽带接入设备的家庭网关设备，通过借助计算机网络，将家庭内部各种设备和家电与宽带网相连，即利用信息网络为人们提供各种丰富、多样化的信息服务，诸如上网冲浪、网络游戏、网络电话及网络安防等，相应的，作为信息服务的接入点，家庭网关设备在家庭的信息网络中扮演着至关重要的角色。

[0003] 现有的家庭网关设备一般是基于 Linux 系统的嵌入式设备，由于其具有接入方式灵活、性能稳定、可根据需求进行定制等特点，所以家庭网关设备一般是由网络运营商根据用户需求进行定制和管理，这样既能为网络运营商提供服务的可控性，又能为用户提供服务的选择性，进而减少用户必要的支出。

[0004] 由于家庭网关设备是在运营商和用户双向满足的基础上提供网络服务的，所以其需要随着技术的不断发展和用户需求的不断变化进行升级和定制，而在实际生活中，运营商会根据用户需求或者本身网络需求对家庭网关设备进行升级固件操作，这种操作一般是运营商通过网络进行远程实施。远程升级操作本身具有一定的风险，例如升级过程中如果断电，设备固件就回遭到破坏，进而导致设备无法正常运行，影响家庭用户网络的正常使用。如果出现此种状况，只能安排维修人员上门服务，造成了不必要的人力和物力的损失。

[0005] 具体的，由于家庭网关固件一般是按照网络运营商的需求进行定制，其升级功能主要包括本地固件升级和远程固件升级两种方式，而家庭网关固件则主要包括：

[0006] a. 启动引导区 (Boot Loader)

[0007] 在嵌入式操作系统中，Boot Loader 是系统上电启动的的初始程序，主要负责初始化硬件设备、设备内存空间、准备系统运行环境等，并在完成系统初始化任务之后，加载操作系统内核，并将系统交与内核接管。

[0008] b. 内核区 (Linux Kernel)

[0009] Linux Kernel 是嵌入式系统的核心部分，其主要是完成内存的初始化和管理，并负责进程管理和调度，及加载协议栈等核心功能。

[0010] c. 文件系统区 (File System)

[0011] File System 是操作系统对磁盘文件分区管理的可视化组织形式，主要负责用户文件的存入、读出、修改以及检索等，且 File System 还包含了操作系统所需要的基本目录结构和文件，用户层进程文件与配置等。

[0012] d. 配置区 (Configuration)

[0013] Configuration 是网关设备功能的配置文件的存储区，主要用于存放设备的基本配置文件和关键设备信息。

[0014] 其中，在固件升级过程中，一般只完成对内核区 (Linux Kernel) 和文件系统区 (File System) 的升级，仅在特殊情况下会升级配置区 (Configuration) 和启动引导区

(Boot Loader)。

[0015] 当前，家庭网关生产厂商为了满足运营商的需求一般会采用双 IMAGE 的做法，即在固件中包含两份文件系统区和内核区；图 1 是现有技术中双 IMAGE 模式的 Flash 布局示意图；如图 1 所示，家庭网关固件中的闪存 (FLASH) 中设置有启动引导区 (Boot Loader)、主系统内核区 (Kernel_1)、主系统文件系统区 (FS_1)、备份系统内核区 (Kernel_2)、备份系统文件系统区 (FS_2)、配置区 (Configuration) 和其他分区，即 FLASH 由两份系统文件系统区 (FS) 和两份内核区 (Kernel) 组成，其中，Kernel_1 和 FS_1 作为主系统分区，而 Kernel_2 和 FS_2 则作为备份系统分区，相应的在固件烧录时，一般会烧录到 Kernel_1 和 FS_1 分区，如果因为意外情况（例如突然断电）烧录出现问题，系统再次启动时，Boot Loader 会校验 Kernel_1 和 FS_1 的合法性与完整性，若出现问题，此时会启动 Kernle_2 和 FS_2 备份系统。

[0016] 虽然，双 IMAGE 模式能够保证系统升级突然中断造成主系统崩溃时，能启用备份系统，以保证系统正常运行；但是，由于备份系统要求和主系统使用具有相同功能的固件，因此会占用 Flash 较大空间。例如，通常家庭网关设备的 Flash 为 16M，其中 Boot Loader 与 Configure 区加起来最多 1M，而主系统和备份系统则分别占用的 Flash 空间大小最多为 7.5M，如果设备支持中间件等功能的话，每个系统的 Flash 可用空间就会更少，所以 Flash 空间的限制是制约家庭网关设备功能的重要因素，因此，合理利用 Flash 空间可以为用户和运营商在网关功能和服务上提供更多的选择性。

发明内容

[0017] 针对现有的嵌入式网关设备进行固件升级时存在的上述问题，现提供一种网关设备升级保护的方法，通过对 NOR 闪存进行合理的布局，以减小多次读写闪存造成的数据损失风险，并利用高度定制化、精简化的家庭网关小系统，在合理利用闪存存储空间的基础上，为后续固件的升级提供保证，进而实现在不影响家庭用户使用的状况下，为运营商远程固件升级提供一种可靠的、高效的机制，以便于运营商更好的满足用户需求，有针对性的提供高质量的网络服务。

[0018] 本发明的目的是通过下述技术方案实现的：

[0019] 一种网关设备升级保护的方法，应用在基于 Linux 系统开发的嵌入式设备上，所述网关设备采用 NOR 闪存作为存储器件，且该 NOR 闪存上设置有启动引导区、内核区、文件系统区和配置区，其中：

[0020] 所述 NOR 闪存还设置有小系统关键参数区；

[0021] 所述文件系统区包括主系统文件系统区和小系统文件系统区，所述内核区包括主系统内核区和小系统内核区；

[0022] 具体包括以下步骤：

[0023] 步骤 S1：所述网关设备上电后，所述启动引导区进行加载；

[0024] 步骤 S2：判断所述主系统内核区和 / 或所述主系统文件区是否合法；

[0025] 若合法，则依次启动所述主系统的内核区和所述主系统的文件系统区，进行所述网关设备的正常启动；

[0026] 若不合法，继续判断所述小系统内核区和 / 或所述小系统文件区是否合法；

[0027] 步骤 S3：若所述小系统内核区和 / 或所述小系统文件区不合法，则启动失败；

[0028] 若所述小系统内核区和所述小系统文件区合法，依次启动所述小系统的内核区和所述小系统的文件系统，并继续判断所述小系统关键参数区是否存在配置信息；

[0029] 步骤 S4：若所述小系统关键参数区不存在配置信息，则启动失败；

[0030] 若所述小系统关键参数区存在配置信息，则读取所述配置信息，完成固件下载，并烧录所述固件到所述 NOR 闪存中，并继续判断上述烧录是否成功；

[0031] 步骤 S5：若所述烧录成功，则重启所述网关设备；

[0032] 若所述烧录不成功，则保存参数，并重启所述网关设备。

[0033] 上述的网关设备升级保护的方法，其中，还包括：

[0034] 当所述网关设备需要升级固件时，网络运营商通过广域网管协议告知家庭网关用户端；

[0035] 所述家庭网关用户端获取并根据所述升级固件的网页地址、连接用户名和连接密码获取固件文件；

[0036] 所述家庭网关用户端将所述固定文件烧录到所述 NOR 闪存中。

[0037] 上述的网关设备升级保护的方法，其中，还包括自动配置服务器；

[0038] 所述家庭网关用户端将所述自动配置服务器下发的所述升级固件的网页地址、连接用户名和连接密码存入所述 NOR 闪存的关键信息区；

[0039] 同时，所述家庭网关用户端还读取所述家庭网关的配置数据，获取并保存所述家庭网关所有广域网连接关系至所述 NOR 闪存的关键信息区；

[0040] 所述家庭网关用户端通过 HTTP 协议获取并烧录所述固件文件至所述 NOR 闪存中；

[0041] 重启所述家庭网关，完成固件升级操作。

[0042] 上述的网关设备升级保护的方法，其中，所述 NOR 闪存是基于块的可读写存储设备，且该 NOR 闪存每次进行读写操作时均基于一个块的操作。

[0043] 上述的网关设备升级保护的方法，其中，所述块的大小为 64k、128k 或 256k。

[0044] 上述的网关设备升级保护的方法，其中，所述启动引导区单独占用一个块。

[0045] 上述的网关设备升级保护的方法，其中，所述启动引导区、主系统文件系统区、小系统文件系统区、所述主系统内核区、所述小系统内核区、所述配置区和所述小系统关键参数区的起始地址均为一个块的起始位置。

[0046] 综上所述，本发明一种网关设备升级保护的方法，通过对 NOR 闪存进行合理的布局，以减小多次读写闪存造成的数据损失风险，并利用高度定制化、精简化的家庭网关小系统，在合理利用闪存存储空间的基础上，为后续固件的升级提供保证，进而实现在不影响家庭用户使用的状况下，为运营商远程固件升级提供一种可靠的、高效的机制，以便于运营商更好的满足用户需求，有针对性的提供高质量的网络服务。

附图说明

[0047] 图 1 是现有技术中双 IMAGE 模式的 Flash 布局示意图；

[0048] 图 2 为本发明实施例中 NOR 闪存布局示意图；

[0049] 图 3 为本发明实施例中网关设备升级保护的方法的逻辑框图。

具体实施方式

[0050] 下面结合附图对本发明的具体实施方式作进一步的说明：

[0051] 本申请一种网关设备升级保护的方法，主要是应用在基于 Linux 系统开发的嵌入式设备如家庭网关上，且该家庭网关是采用 NOR 闪存 (flash) 作为其存储器件；而由于 flash 的布局会影响到家庭网关性能的优劣，所以通过合理的安排 flash 布局，能够增加网关主系统的内在功能，进而提高网关系统在家庭网络中的作用。

[0052] 图 2 为本发明实施例中 NOR 闪存布局示意图，如图 2 所示，在家庭网关设备的固件升级过程中，其整体的闪存布局 (flash layout) 参考图 2 设计，即包括启动引导区 (boot loader)、主系统内核区 (kernel_1)、主系统文件系统区 (FS_1)、小系统内核区 (kernel_2)、小系统文件系统区 (FS_2)、小系统关键参数区、其他分区和配置区 (configure)。

[0053] 同时，由于上述的 NOR flash 是一种基于块 (block) 的可读写存储设备，所以其每次读写操作都是基于一个块的操作，而每个块值的大小可以参考该 NOR flash 的数据手册 (datasheet) 和 / 或参考指南 (reference guide) 设置，如将块值大小设置为 64k、128k 或 256k 等。

[0054] 其中，由于合理的 flash 部件能够减小多次读写 flash 造成的数据损失的风险，且为了后去固件审计提供保证，当使用 NOR flash 作为家庭网关设备的主要存储器件时，启动引导区应当单独占用一个 block，如设置该启动引导区占用 NOR flash 的 #1block，且系统中的各个主要的分区如启动引导区、主系统内核区、主系统文件系统区、小系统内核区、小系统文件系统区、小系统关键参数区和配置区等的起始位置都应当是 flash 的某一个 block 的起始位置，而对于一些敏感的存储信息也应当单独的占用一个 block，且该 block 绝对不允许共用，对于普通的存储信息则可共用一个 block。

[0055] 下面以基于 Broadcom535X 芯片的家庭网关设备 (16M NOR Flash) 为例，对本申请网关设备升级保护的方法进行具体阐述现机制：

[0056] 由于，网络运营商一般使用广域网管理协议 (TR069) 对家庭网关实行远程升级，所以当家庭网关需要升级固件时，运营商就通过 TR069 协议告知家庭网关用户端设备 (Customer Premises Equipment，简称 CPE) 获取最新固件的网页地址 (Uniform Resource Locator，简称 URL)、连接用户名 (username) 和连接密码 (passwd) 等信息，而 CPE 则会根据获得的信息获取固件文件，并将该固件文件烧录到 Flash 中。

[0057] 其中，在 CPE 烧录固件的整个过程，主要包括以下几个步骤：首先，CPE 将自动配置服务器 (Auto-Configuration Server，简称 ACS) 下发的 URL、username 和 passwd 存入关键信息区 (NVRAM)，同时读取家庭网关的配置信息，以获取该家庭网关所有广域网 (Wide Area Network，简称 WAN) 连接信息，并将其保存到 NVRAM 中；其次，CPE 通过 HTTP 协议，获取最新固件文件并存储到 RAM 中；之后，CPE 将上述的固件文件烧录到 NOR Flash 中；最后，重启家庭网关设备，完成升级操作。

[0058] 进一步的，在本申请中设置的家庭网关小系统是高度定制化、精简化的网关系统，它是现有网关主系统的精简版，仅包含系统启动的必要进程、模块和服务，具体包括主进程 Master、Httpd，以用于完成网关固件的下载和升级；相应的该家庭网关小系统的自动化工作流程如下：

[0059] 首先，读取关键信息区存储的获取固件的 url、username、passwd 和所有 WAN 连接信息；其次，根据获得的信息，建立相应 WAN 连接，并通过 HTTP 协议获取固件，并将该固件保存到 RAM 中；最后，通过调用 FLASH 的 API 将获得的固件烧录到主系统区。

[0060] 进一步的，在本实施例中网关设备固件升级前需要对 Boot Loader 内部 Flash 布局进行定义，具体如下：

```
#define FALSH_BLOCK_TOTAL   256
#define ONEK                1024        /* 1K */
#define FLASH_BLOCK_SIZE    (64*ONEK)   /* 64K */
#define BOOT_BLOCK_NUM      2

#ifdef CFE_SUPPORT_AUXFS
#define AUXFS_BLOCK_NUM     32
#else
#define AUXFS_BLOCK_NUM     0
#endif

#define USER_BLOCK_NUM      5
/*NVARM+PSI+SYSLOG/sp+FACTORYDATA*/
#define SMALL_FS_SIZE_MAX   0x300000    /* 3M ,48 BLOCK*/


    uint32 free_blk_num = FALSH_BLOCK_TOTAL –
BOOT_BLOCK_NUM - AUXFS_BLOCK_NUM –
USER_BLOCK_NUM ;/* 186 = 48(small)+138(big) */
    uint32 big_fs_size_max = (free_blk_num –
SMALL_FS_SIZE_MAX/FLASH_BLOCK_SIZE)*FLASH_BLOCK_S
IZE;/* 8.5625M */

    /* Because CFE can only flash an entire partition */
    fprobe.flash_nparts = 6;
    fprobe.flash_parts[0].fp_size = bootsz;
    fprobe.flash_parts[0].fp_name = "boot"; /*启动区*/
    fprobe.flash_parts[1].fp_size = sizeof(struct trx_header);
    fprobe.flash_parts[1].fp_name = "trx0";/*主系统 Kernel*/
    fprobe.flash_parts[2].fp_size = big_fs_size_max - sizeof(struct
trx_header);
    fprobe.flash_parts[2].fp_name = "os0";/*主系统 FS*/
    fprobe.flash_parts[3].fp_size = sizeof(struct trx_header);
    fprobe.flash_parts[3].fp_name = "trx1";/*小系统 Kernel*/
    fprobe.flash_parts[4].fp_size = 0;
    fprobe.flash_parts[4].fp_name = "os1";/*小系统 FS*/
    fprobe.flash_parts[5].fp_size = NVRAM_SPACE;
    fprobe.flash_parts[5].fp_name = "nvram";
    cfe_add_device(drv, 0, 0, &fprobe);
```

图 3 为本发明实施例设备中网关升级保护的逻辑方法的框图；如图 3 所示：

[0061] 首先，网关设备上电后，启动引导区进行加载，以判断主系统内核区和/或主系统文件区是否合法，及判断是否合法（合法性和完整性等）；Trx0 若合法，则依次启动主系统的内核区（Kernel_1）和主系统的文件系统区（FS_1），进行网关设备的正常启动；

[0062] 而若 Trx1 不合法，继续判断小系统内核区和/或小系统文件区是否合法（合法性和完整性等），即判断 Trx2 是否合法。

[0063] 其次，若 Trx2 不合法，则启动失败；

[0065] 若Trx2合法，依次启动小系统的内核区(Kernel_2)和小系统的文件系统(FS_1)，并继续判断小系统关键参数区是否存在配置信息。

[0066] 之后，若小系统关键参数区不存在配置信息，则启动失败；

[0067] 若小系统关键参数区存在配置信息，则读取配置信息，完成固件下载，并烧录固件到NOR闪存中，并继续判断上述烧录是否成功。

[0068] 最后，若烧录成功，则重启网关设备，进而完成固件升级；

[0069] 若烧录不成功，则保存参数，并重启网关设备，继续启动引导区的加载。

[0070] 综上所述，本发明一种网关设备升级保护的方法，通过对NOR闪存进行合理的布局，以减小多次读写闪存造成的数据损失风险，并利用高度定制化、精简化的家庭网关小系统，在合理利用闪存存储空间的基础上，为后续固件的升级提供保证，进而实现在不影响家庭用户使用的状况下，为运营商远程固件升级提供一种可靠的、高效的机制，以便于运营商更好的满足用户需求，有针对性的提供高质量的网络服务。

[0071] 通过说明和附图，给出了具体实施方式的特定结构的典型实施例，基于本发明精神，还可作其他的转换。尽管上述发明提出了现有的较佳实施例，然而，这些内容并不作为局限。

[0072] 对于本领域的技术人员而言，阅读上述说明后，各种变化和修正无疑将显而易见。因此，所附的权利要求书应看作是涵盖本发明的真实意图和范围的全部变化和修正。在权利要求书范围内任何和所有等价的范围与内容，都应认为仍属本发明的意图和范围内。

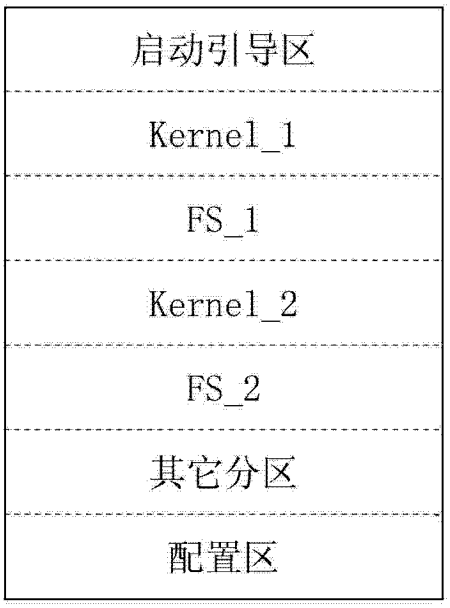

启动引导区
Kernel_1
FS_1
Kernel_2
FS_2
其它分区
配置区

图 1


启动引导区
主系统内核区
主系统文件系统区
小系统内核区
小系统文件系统区
小系统关键参数区
其它分区
配置区

图 2

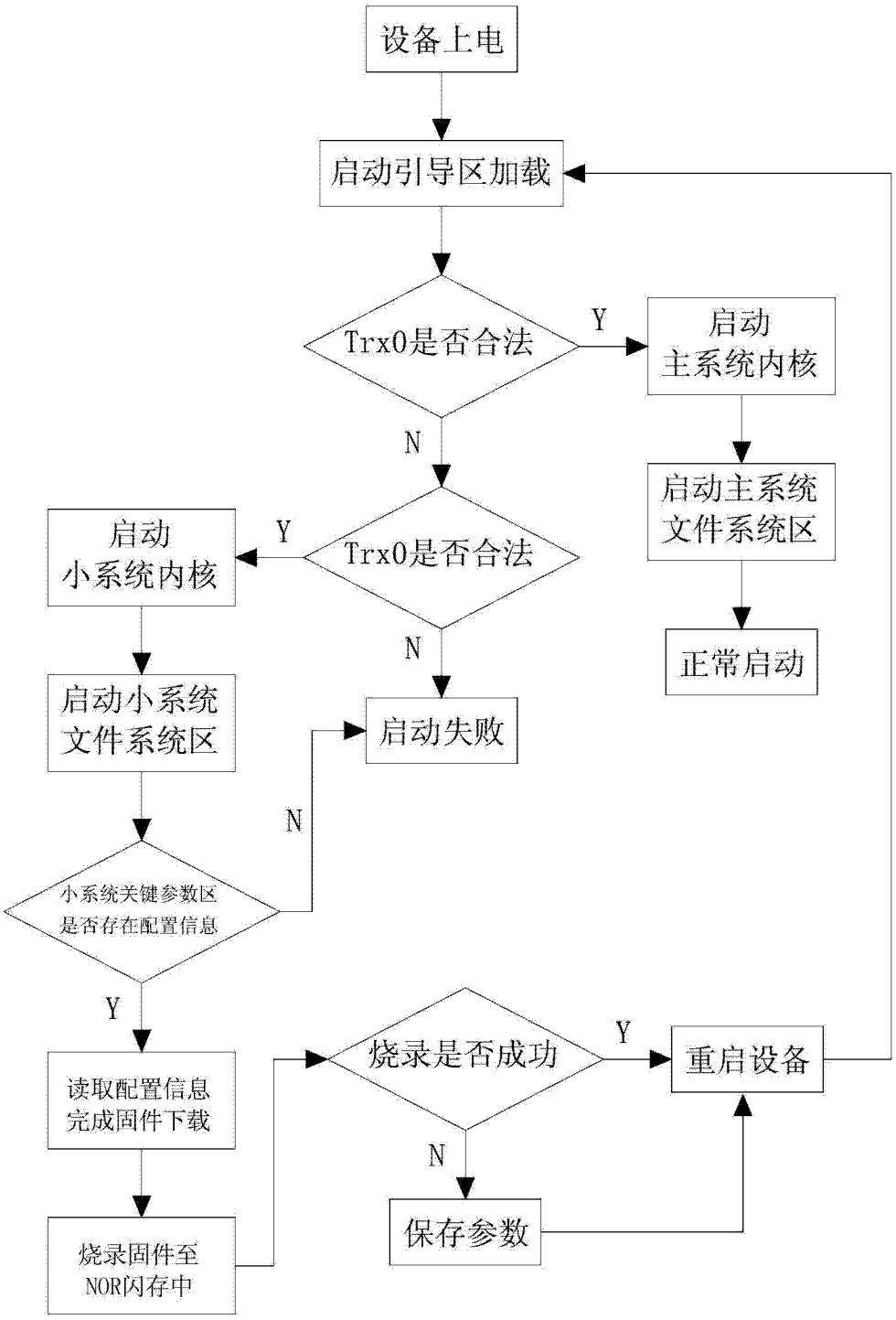

设备上电
启动引导区加载
Trx0是否合法
Y
启动
主系统内核
N
启动主系统
文件系统区
正常启动
启动
小系统内核
Y
Trx0是否合法
N
启动小系统
文件系统区
启动失败
N
小系统关键参数区
是否存在配置信息
Y
读取配置信息
完成固件下载
烧录固件至
NOR闪存中
烧录是否成功
Y
重启设备
N
保存参数

图 3