Technical Disclosure Commons

Defensive Publications Series

September 10, 2018

SELF-HEALING AND RECOVERING DEVICE FROM MASS STORAGE FILE SYSTEM CORRUPTION

Wenwei Weng

Ning Zhao

Guru Darshan Pollepalli Manohara

Ibrahim Mortada

SELF-HEALING AND RECOVERING DEVICE FROM MASS STORAGE FILE SYSTEM CORRUPTION

AUTHORS:
Wenwei Weng
Ning Zhao
Guru Darshan Pollepalli Manohara
Ibrahim Mortada

ABSTRACT

Techniques are provided for a device to become more robust using self-healing and recovering functionality in place when operating in harsh environment. This process is seamless and transparent, and improves customer satisfaction and reduces Return Merchandise Authorization (RMA) rate.

DETAILED DESCRIPTION

Traditional networking devices such as routers and switches are deployed by enterprises and service providers, which are operated by Information Technology (IT) professionals. They are deployed in well controlled and stable environments, and the file system corruption in mass storage devices is not often observed. With the arrival of the Internet of Things (IoT) era, networking devices are rapidly deployed in harsh and unstable environments. They are operated by Operational Technology (OT) professionals.

For example, many IoT routers are deployed in trains, buses, ambulances, etc., with volatile power supplies and strong mechanical vibrations. In this environment, the power supply is very unstable, resulting in frequent and sudden device reboot, which significantly increases the chances for mass storage file system corruption. Once mass storage file system corruption occurs, the device is no longer usable as the bootloader fails to find any bootable image on the mass storage. Most of the time OT professionals simply Return Merchandise Authorization (RMA) the devices.

There are also IoT routers deployed in very remote and rural areas, where there are no staff on site to manage the devices. Once the device becomes unusable due to mass storage file system corruption, a technician must be sent to the deployment site.

These bad consequences would be avoided if the device could be self-healed and automatically recovered from the mass storage file system corruption.

The mass storage is typically partitioned and formatted by the system to fully leverage its capacity. In order to implement self-healing and recovery, a certain amount of mass storage space is reserved, typically at the end of the space. The reserved space is determined by the size of the system image, system configuration, and any other user data which are critical and required for the system to function properly. The reserved space is utilized in the following manner.

First, it is formatted in a certain file system type when the first time the device is booted up during manufacture or immediately after upgrading the image with feature support.

Second, when the device is up and running, the reserved space is not mounted/accessed by the Operating System (OS) and/or applications, so this reserved space will not become corrupted even if the sudden power cycle causes a sudden reboot.

Third, the reserved space is mounted/accessed only during the window where the system image is being installed/upgraded. The new system image is copied into this reserved space, along with any critical operational user data. The space is then unmounted.

Fourth, during system boot up, if the bootloader finds the valid image on the mass storage file system, it boots the image as usual. Otherwise (e.g., file system corruption occurs, resulting in system image corruption or total loss), the bootloader mounts the reserved space and fetches the system image into Dynamic Random Access Memory (DRAM) to jump start the system.

Fifth, in the early stage of system boot, the software may inspect the mass storage file system. In this example, file system corruption is found. The system software may repartition and reformat the mass storage with knowledge of the existence of reserved space. After the mass storage repartition and reformat is completed, the reserved space is mounted. All the backed up data is restored from the reserved space to the normal area of mass storage. At this point, the device is considered fully healed and recovered.

The whole process may be transparent to the end user.

Figure 1 below illustrates backup of critical information into a reserved space.

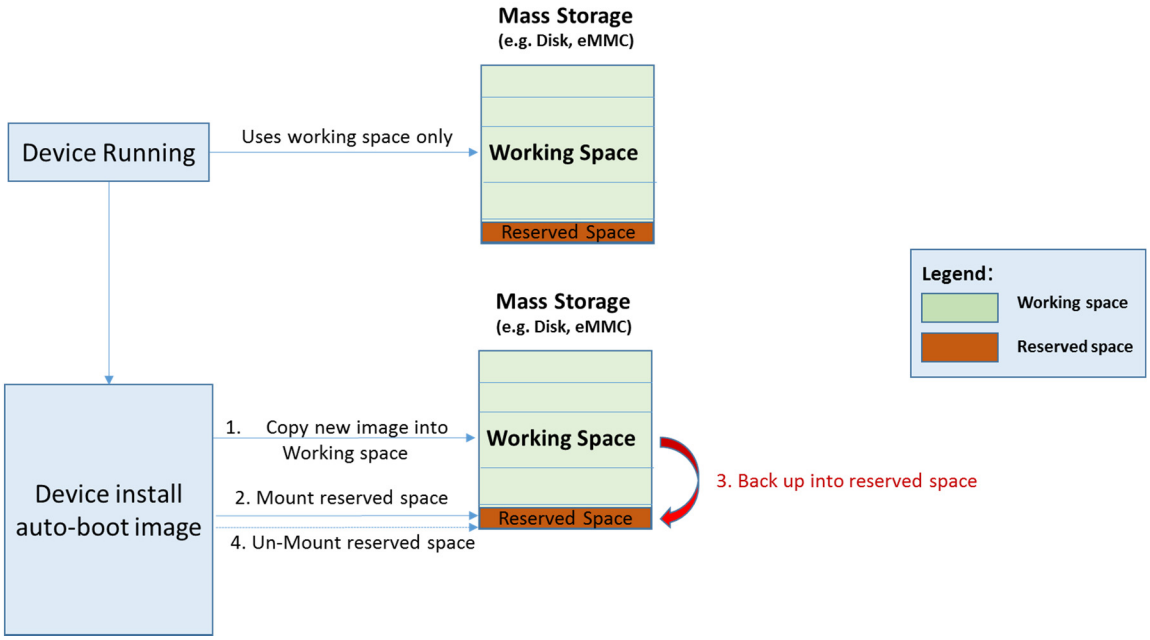

Figure 1

Figure 2 below illustrates device self-healing/recovery if there is corruption.

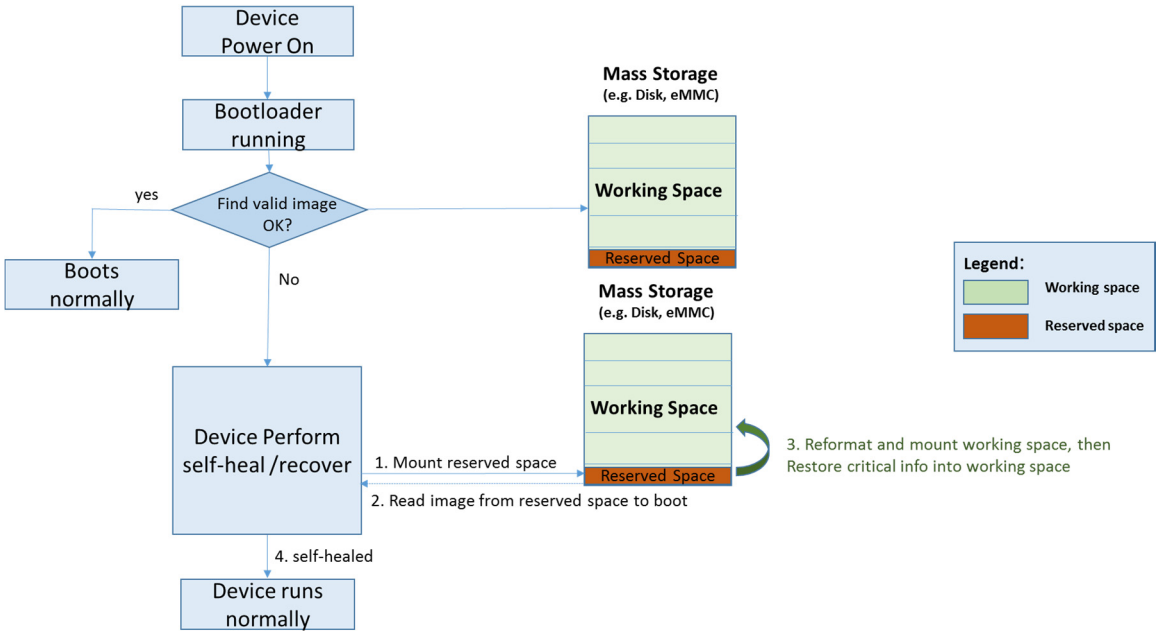

Figure 2

In summary, techniques are provided for a device to become more robust using self-healing and recovering functionality in place when operating in harsh environment. This process is seamless and transparent, and improves customer satisfaction and reduces RMA rate.