

Sanitize Frozen State Reset Transition Change

To: T13 Technical Committee
From: John Geldman
Lexar Media, Inc.
Phone: 510-580-8715
Email: jgeldman@lexar.com
Date: August 18, 2009

Background/Overview

ACS-2r2 integrated the Sanitize Proposal (e08197). Reviewing the balloted document made it clear that we had implemented a bad behavior. This proposal addresses a letter ballot comment.

The Sanitize Frozen state was defined to transition to the Sanitize Idle state on hardware resets. Unfortunately, this means that a COMRESET, which the host may not be aware of, would transition the device to an unfrozen state. This was unintentional.

Editor's Note 2 refers to this issue with a suggestion of adding Sanitize to be added to SSP. This proposal ~~offers a different solution~~ implements this.

Scope

Resolution of ACS-2 letter ballot comment

Proposed changes in ACS-2, Revision 2, T13 document #D2015r2.

Changes to 4.22 introduction

~~This~~ Sanitize Device operations shall use one of the methods defined in this subclause to make all previously written content in the user data area of the device ~~unretrievable~~ unable to be read.

~~Sanitize Device operations and~~ shall only affect the following:

- a) user data areas;
- b) user data areas that are not currently allocated (e.g., previously allocated areas and physical sectors that have become inaccessible); and
- e) ~~—~~user data caches.

Sanitize Device operations should not return an error if physical sectors that have become inaccessible were not successfully sanitized.

Sanitize Device operations shall not affect non-user data areas (e.g., logs (see Annex A), and Device SMART data structure (see Table 66)).

Automatic sector reallocation is permitted during the operation of this function. After completion of a Sanitize Device ~~command~~ operation, the device shall:

- a) return an error if physical sectors that are available to be allocated for user data (e.g. allocated; or unallocated physical sectors allowed by vendor-specific means to be usable for user data) were not successfully sanitized; or
- b) set the Sanitize Operation Complete Without Error bit if:
 - a. all physical sectors that are available to be allocated for user data have been successfully sanitized; and-
 - b. any physical areas that were not successfully sanitized were removed from use.

To perform a Sanitize Device operation the host should issue:

- a. CRYPTO SCRAMBLE EXT command (see 7.43.3);
- b. BLOCK ERASE EXT command (see 7.43.2); or
- c. OVERWRITE EXT command (see 7.43.4),

followed by a SANITIZE STATUS EXT command (see 7.43.6) to check for completion.

After a device has started processing a Sanitize Device operation, and until the device transitions to the Sanitize Idle state, the device shall abort all commands other than IDENTIFY DEVICE command, ~~DRIVE~~, REQUEST SENSE EXT command and SANITIZE STATUS EXT command. If a Sanitize Device operation is interrupted by a power cycle, the Sanitize Device operation shall continue to completion before reporting ready.

Change both Figure 15 Sanitize Device state machine, and the state documentation as follows:

Add SD3:SD1 transition on SANITIZE STATUS EXT with the Clear Failed State bit set to one.

Transition SD3:SD1: When the device is in the Sanitize Operation Failed state and:

- a) the Sanitize Operation was initiated by a Sanitize Device command with the Failure Mode bit set to one; and
- b) the SANITIZE STATUS EXT command has been successfully processed with the Clear Sanitize Operation Failed bit set to one.

The following two transitions are revised as follows:

Transition SD3b:SD3: When the device is in the Sanitize Operation Failed state, and it processes a SANITIZE STATUS EXT command with the Clear Sanitize Operation Failed bit cleared to zero, the device shall remain in the SD3 Sanitize Operation Failed state.

Transition SD3a:SD3: When the device is in the Sanitize Operation Failed state and it processes a hardware reset or power cycle, the device shall remain in the SD3 Sanitize Operation Failed state.

~~The SD1:SD0 transition should be only be triggered by power cycle (hardware reset would be removed from this transition).~~

~~The SD1:SD1 self transition (which processes a SANITIZE STATUS EXT command) should be relabeled as SD1a:SD1.~~

~~A new self transition SD1b:SD1 should be added which will transition on hard reset.~~

Changes to 4.25

Add to Table 16, Preserved Feature Sets and Settings (resolves Editor's Note 3)

SANITIZE FREEZE LOCK EXT: The Sanitize Frozen state established by the SANITIZE FREEZE LOCK EXT command (see 4.22).

Addition to Count field in 7.43.2 BLOCK ERASE EXT command, 7.43.3 Crypto Erase Ext command and 7.43.4 OVERWRITE EXT command:

<u>Bit</u>	<u>Description</u>
<u>X</u>	<u>Failure Mode</u>

Bit x: If the Failure Mode bit is set to one, then the device may exit the Sanitize Operation Failed state with successful processing of a SANITIZE STATUS EXT command. If the Failure Mode bit is cleared to zero, then the Sanitize Operation Failed state shall only allow additional Sanitize Operations.

Addition to Count field in 7.43.6, SANITIZE STATUS EXT Command

<u>Bit</u>	<u>Description</u>
<u>X</u>	<u>Clear Sanitize Operation Failed</u>

If in a Sanitize Operation

1) the Failure Mode bit was set to one in the Sanitize Device command that caused the Sanitize Operation;
2) the Sanitize Operation failed; and
3) the Clear Sanitize Operation Failed bit is set to one in the SANITIZE STATUS EXT command,
then the Sanitize state machine shall transition from the Sanitize Failed state to the Sanitize Idle state.

If Clear Sanitize Operation Failed bit is set to one in the SANITIZE STATUS EXT command, and the Failure Mode bit was set to zero in the Sanitize Device command that caused the Sanitize Operation, the SANITIZE STATUS EXT command shall return command aborted.

Changes to 9.2, Table 118, Sanitize Normal Output

Count Field

Bit Description

15 Sanitize operation complete without error

14 Sanitize operation in progress

13:0 Reserved