swissbit®

X-500 Series Enhanced Erase

White Paper

BU: Flash Products
Date: April 30, 2013
Revision: 1.0
File: WhitePaper_X-500_Enhanced_Erase_Rev01_DRAFT.doc

made in germany

1 Overview

Swissbit X-500 products optionally include enhanced methods for secure and fast user data erase (data sanitizing / purge). All user data, and firmware and internal buffer blocks (used for garbage collection etc.) will be erased.

Enhanced erase can be triggered by a software command or a hardware input.

Currently available are the following algorithms according to the following standards:

- Basic erase (as fast as possible)
- DoD5220.22-M
- NSA (Manual 130-2)
- USA AirForce AFFSSI
- USA Army 380-19
- USA Navy NAVSO
- IREC (IRIG) 106-07
- NSA 9-12

More algorithms can be implemented by customer request.

2 Erase algorithm details

The following erase algorithms are implemented with the respective sequences:

Index	Method	Sequence
0	Basic Erase	Erase
1	DoD5220.22-M	Erase Program with repeated user parameter 1 Erase
2	NSA (Manual 130-2)	Erase ,Program with repeated randomly chosen value Erase, Program with repeated randomly chosen value Erase, Program with repeated user parameter 1
3	USA Air Force AFFSSI 5020	Erase, Program with repeated 0x00 Erase, Program with repeated 0xFF Erase, Program with repeated randomly chosen value
4	USA Army 380-19	Erase, Program with repeated randomly chosen value Erase, Program with repeated user parameter 1 Erase, Program with repeated user parameter 1
5	USA Navy NAVSO P-5239-26	Erase, Program with repeated user parameter 1 Erase, Program with repeated complement of parameter 1 Erase, Program with repeated randomly chosen value
6	IREC (IRIG) 106-07 Ch. 10	Erase, Program with repeated 0x55 Erase, Program with repeated 0xAA Erase, Program with repeated ASCII string “Secure Erase”
7	NSA 9-12	Erase, Program with repeated user parameter 1 Verify all data

3 Typical timings

The following table shows typical timings for the different devices densities and different algorithms:

Type / Density	16GB	32GB	64GB	128GB	256GB
Basic erase	00:08	00:08	00:15	00:17	00:30
DoD5220.22-M	01:21	02:12	04:25	08:13	15:58
NSA (Manual 130-2)	03:43	06:16	12:37	23:56	46:27
USA AirForce AFFSSI	03:45	06:18	12:41	23:59	46:33
USA Army 380-19	03:45	06:18	12:40	23:59	46:33
USA Navy NAVSO	03:45	06:18	12:40	23:59	46:33
IREC (IRIG) 106-07	03:45	06:18	12:41	23:59	46:33
NSA 9-12	01:14	02:05	04:12	08:00	16:04

Minutes : Seconds

4 Software Erase Trigger

Enhanced Erase can be triggered using the standard ATA commands from the Security Erase feature set.

The minimum commands that need to be implemented are:

- SECURITY SET PASSWORD (F1h)
- SECURITY ERASE PREPARE (F3h)
- SECURITY ERASE UNIT (F4h)

The standard SECURITY ERASE UNIT (F4h) command data structure is extended as follows:

Word	Content
0	Control word Bit 0 identifier (0 = user password, 1 = master password) Bit 1 erase mode (0 = normal erase, 1 = enhanced erase) Bits 15:2 reserved and must be zero
1-16	Password (32 bytes)
17	Index of erase algorithm to be used (little endian) See algorithm table
18	User parameter (little endian) if necessary
19-256	Reserved

If Word 0, Erase Mode is 0 (normal erase), the firmware will perform a "basic erase" (user area must be all zeroes).

If Word 0, Erase Mode is 1 (enhanced erase), the firmware shall perform the extended erase algorithm specified in Word 17, with user parameter (if needed) as specified in Word 18.

5 Hardware Erase Trigger

Enhanced erase can be trigger by a hardware input. A LED output is provided for erase status (blinking).

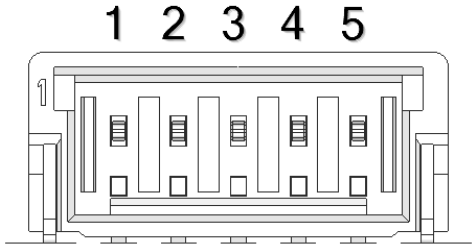
5.1 Feature connector

Figure 112: SSD connector side with power, SATA and feature connector

The X-500 SSD has a 5-circuit feature connector beside the SATA connector for the extra functions:

- write protect
- hardware erase as well as for operation signalization
- device activity
- erase activity

This feature connector mates e.g. with the Molex connector (part number 5013300500) with 5 wire to board terminals (part number 1513340000).



Feature connector at SSD

Pin	function	usage
1	-write protect input	write protection by low
2	ground	ground
3	device activity output	connect an LED to ground (serial resistor depending on color) LED is on at device activity (at each SATA command)
4	-erase input	enhanced erase starts if this pin is low for at least 0.8s
5	erase output	connect an LED to ground (serial resistor depending on color) LED blinks, if erase is in progress

Evaluation adapter cable for feature connector is available in sample quantities.

For more details please consult the X-500 datasheet.

5.2 Erase Algorithm

The erase algorithm (and parameter if necessary) used by the hardware input can be set byat Swissbit in mass production for customer specific products only.
It is possible to change these settings at the customer location using a vendor specific command.
Please consult Swissbit engineering for more details.

6 Document History

Table 1: Document Revision History

Date	Revision	Details
30-April-2013	1.0	First release