Using Hardened Control Functions in MachXO3D Devices Reference Guide Supplement

Technical Note

FPGA-TN-02241-1.0

September 2020

Disclaimers

Lattice makes no warranty, representation, or guarantee regarding the accuracy of information contained in this document or the suitability of its products for any particular purpose. All information herein is provided AS IS and with all faults, and all risk associated with such information is entirely with Buyer. Buyer shall not rely on any data and performance specifications or parameters provided herein. Products sold by Lattice have been subject to limited testing and it is the Buyer's responsibility to independently determine the suitability of any products and to test and verify the same. No Lattice products should be used in conjunction with mission- or safety-critical or any other application in which the failure of Lattice's product could create a situation where personal injury, death, severe property or environmental damage may occur. The information provided in this document is proprietary to Lattice Semiconductor, and Lattice reserves the right to make any changes to the information in this document or to any products at any time without notice.

Contents

Acronyms in This Document 4
1. Introduction 5
2. Command Summary by Application 5
2.1.1. Read Status Register 1 (0x3D) 6
2.1.2. Reset Flash Address (0x46) 6
2.1.3. Reset UFM Address (0x47) 7
2.1.4. Set Address (0xB4) 7
2.1.5. Program UFM Security Settings (0x56) 7
2.1.6. Read UFM Security Settings (0x57) 8
2.1.7. Program Centralized Security Setting (0x54) 9
2.1.8. Read Centralized Security Setting (0x55) 12
2.1.9. Program Authentication Mode (0xC4) 15
2.1.10. Read Authentication Mode (0xC5) 15
2.1.11. Authentication DONE (0xCC) 16
2.1.12. Program FEABITs (0xF8) 16
2.1.13. Read FEABITs (0xF8) 17
Technical Support Assistance 18
Revision History 19

Tables

Table 2.1. Flash Commands 5
Table 2.2. Read Status Register 1 (0x3D) 6
Table 2.3. Reset Flash Address (0x46) 6
Table 2.4. Reset UFM Address (0x47) 7
Table 2.5. Set Address (0xB4) 7
Table 2.6. Program USEC (0x56) 7
Table 2.7. Read USEC (0x57) 8
Table 2.8. Program CSEC (0x54) 9
Table 2.9. Read CSEC (0x55) 12
Table 2.10. Program Authentication Mode (0xC4) 15
Table 2.11. Program Authentication Mode (0xC4) 15
Table 2.12. Authentication DONE (0xCC) 16
Table 2.13. Program FEABITs (0xF8) 16
Table 2.14. Read FEABITs (0xF8) 17

Acronyms in This Document

A list of acronyms used in this document.

Acronym	Definition
I^2C	Inter-Integrated Circuit
SPI	Serial Peripheral Interface
UFM	User Flash Memory

1. Introduction

This reference guide supplements Using Hardened Control Functions in Using Hardened Control Functions in MachXO3D Devices Reference Guide (FPGA-TN-02119), which explains the command sequences and register map. This document describes the central and UFM security settings and authentication commands.

2. Command Summary by Application

- Centralized and User Flash Security Settings (Hard and Soft Lock bits)
- Authentication commands

Table 2.1. Flash Commands

Command Name	Command MSB LSB	SVF Command Name	CFG	UFM	Feature, Security Policy	Security Keys	Description
Read Status Register 1	0x3D	LSC_READ_STATUS1	Y	Y	Y	Y	Read the 4-byte Configuration Status Register 1.
Reset Configuration Flash Address	0x46	LSC_INIT_ADDRESS	Y	Y	Y	Y	Reset the address to point to Sector 0, page 0 of the active Flash sector.
Reset UFM Address	0x47	LSC_INIT_ADDR_UFM	—	Y	—	—	Reset the address to point to sector 1, page 0 of the UFM.
Set Address	0xB4	LSC_WRITE_ADDRESS	Y	Y	Y	Y	Set the 14-bit Address to flash sector
Program USEC	0x56	LSC_PROG_USEC	—	—	Y	—	Program UFM security setting USEC)
Read USEC	0x57	LSC_READ_USEC	—	—	Y	—	Read UFM security setting USEC)
Program CSEC	0x54	LSC_PROG_CSEC	—	—	Y	—	Program centralized security setting for configuration, feature and security keys settings (CSEC).
Read CSEC	0x55	LSC_READ_CSEC	—	—	Y	—	Read centralized security setting for configuration, feature and security keys settings (CSEC).
Program Authentication Mode	0xC4	LSC_PROG_AUTH_MODE	—	—	Y	—	Program authentication mode bits to enable HMAC and ECDSA features.
Read Authentication Mode	0xC5	LSC_READ_AUTH_MODE	—	—	Y	—	Read authentication mode bits to enable HMAC and ECDSA features.
Program Authentication Done	0xCC	LSC_PROG_AUTH_DONE	—	—	Y	—	Program authentication done bit for faster booting applications.
Read FEABITS	0xFB	LSC_READ_FEABITS	—	—	Y	—	Read FEA bits.
Program FEABITS	0xF8	LSC_PROG_FEABITS	—	—	Y	—	Program FEA bits.

2.1.1. Read Status Register 1 (0x3D)

This command is used to read the Status Register 1. This register provides information about the flash sector selection, security, and lock settings. CSEC and USEC flash sectors information is described below for details about the other flash sectors, refer to Using Hardened Control Functions in MachXO3D Devices Reference Guide (FPGA-TN-02119).

Table 2.2. Read Status Register 1 (0x3D)

ISC Enable	CMD (Hex)	Operands (Hex)	Data Mode	Data Size	Data Format
N	3D	00 00 00	R	4B	xxxx xxxx xRGM BBBV YZFD CUAA LRPE SSSS

Data Format: SSSS bits[3:0]: Flash sector selection
0111: CSEC
1101: USEC
(all other bits reserved)

Usage: The BUSY bit should be checked following all Enable, Erase, or Program operations.

Note: Wait at least 1 µs after power-up or asserting wb_rst_i before accessing the EFB.

Example: 0x3D 00 00 00 Read four-byte Status Register. Return value example, 0x00 00 00 07 (CSEC flash sector is selected).

2.1.2. Reset Flash Address (0x46)

This command is used to reset the address counter to point to the first page of the various flash sectors. The flash sector is selected using operands. CSEC and USEC addresses are described below; for details about the other flash sectors, refer to Using Hardened Control Functions in MachXO3D Devices Reference Guide (FPGA-TN-02119).

Table 2.3. Reset Flash Address (0x46)

ISC Enable	CMD (Hex)	Operands (3 Bytes) (Hex)	Data Mode	Data Size	Data Format
Y	46	See Below	—	—	—

Operand: 0000 0fap ucwx yzpq 0000 0000(binary)

where: u: Reset address to User Security sector - USEC (Security Setting for UFM0,1,2 & 3).
0: No action
1: Reset Address
c: Reset address to Centralized security sector - CSEC (Security setting for CFG0, CFG1, Feature row, AESKEY and Public Key sectors).
0: No action
1: Reset Address

Examples: 0x46 00 80 00 Address is reset to point to USEC sector.

2.1.3. Reset UFM Address (0x47)

This command is used to reset the address counter to point to the first page of the various user flash sectors (UFMs). The user flash sector is selected using operands. USEC address is described below; for details about the other UFM flash sectors, refer to Using Hardened Control Functions in MachXO3D Devices Reference Guide (FPGA-TN-02119).

Table 2.4. Reset UFM Address (0x47)

ISC Enable	CMD (Hex)	Operands (Hex)	Data Mode	Data Size	Data Format
Y	47	See below	—	—	—

Operand: 0000 0000 u0wx yz00 0000 0000(binary)

where:
- u: Reset address to User Security sector - USEC (Security Setting for UFM0,1,2 & 3).
  - 0: No action
  - 1: Erase

Examples: 0x47 00 80 00 Address is reset to point to USEC sector.

2.1.4. Set Address (0xB4)

This command is used to set the address register for various flash sectors. CSEC and USEC addresses are described below; for details about the other flash sectors, refer to Using Hardened Control Functions in MachXO3D Devices Reference Guide (FPGA-TN-02119).

Table 2.5. Set Address (0xB4)

ISC Enable	CMD (Hex)	Operands (Hex)	Data Mode	Data Size	Data Format (Binary)
Y	B4	00 00 00	W	4B	0000 0000 0000 000ss ssaa aaaa aaaa aaaa

Data Format:
- ssss: Select Flash Sector
  - 0111: CSEC
  - 1011: USEC
- aa..aa: address 14-bit page address

Example: 0xB4 00 00 00 00 01 30 0A Set Address register to CSEC sector, page 10 decimal

2.1.5. Program UFM Security Settings (0x56)

This command is used to program the UFM security settings page.

Table 2.6. Program USEC (0x56)

ISC Enable	CMD (Hex)	Operands (Hex)	Data Mode	Data Size	Data Format (Binary)
Y	56	00 00 00	W	2B	0000 abcd efgh ijkl

Data Format: Most significant byte of this register is received first, LSB last.
- xxxx Reserved (default = 0)
- a Hard Lock enable for UFM3 sector (0 = Disabled (default), 1 = Enable)
- b Read protection enable for UFM3 sector (0 = Read possible, 1 = Read disable)
- c Erase protection enable for UFM3 sector (0 = Erase possible, 1 = Erase disable)
- d Hard Lock enable for UFM2 sector (0 = Disabled (default), 1 = Enable)
- e Read protection enable for UFM2 sector (0 = Read possible, 1 = Read disable)

f Erase protection enable for UFM2 sector (0 = Erase possible, 1 = Erase disable)

g Hard Lock enable for UFM1 sector (0 = Disabled (default), 1 = Enable)

h Read protection enable for UFM1 sector (0 = Read possible, 1 = Read disable)

i Erase protection enable for UFM1 sector (0 = Erase possible, 1 = Erase disable)

j Hard Lock enable for UFM0 sector (0 = Disabled (default), 1 = Enable)

k Read protection enable for UFM0 sector (0 = Read possible, 1 = Read disable)

l Erase protection enable for UFM0 sector (0 = Erase possible, 1 = Erase disable)

Example: 0x56 00 00 00 00 02

Lock the UFM0 flash sector to prohibit reading of that flash sector.

Note: Poll the BUSY bit (or wait 200us) after issuing this command for programming to complete before issuing a subsequent command other than Read Status or Check Busy.

2.1.6. Read UFM Security Settings (0x57)

This command is used to read the UFM security settings page.

Table 2.7. Read USEC (0x57)

ISC Enable	CMD (Hex)	Operands (Hex)	Data Mode	Data Size	Data Format (Binary)
Y	57	00 00 00	R	2B	xxxx abcd efgh ijkl

Data Format: Most significant byte of this register is received first, LSB last.

xxxx Reserved (default = 0)

a Hard Lock enable for UFM3 sector (0 = Disabled (default), 1 = Enable)

b Read protection enable for UFM3 sector (0 = Read possible, 1 = Read disable)

c Erase protection enable for UFM3 sector (0 = Erase possible, 1 = Erase disable)

d Hard Lock enable for UFM2 sector (0 = Disabled (default), 1 = Enable)

e Read protection enable for UFM2 sector (0 = Read possible, 1 = Read disable)

f Erase protection enable for UFM2 sector (0 = Erase possible, 1 = Erase disable)

g Hard Lock enable for UFM1 sector (0 = Disabled (default), 1 = Enable)

h Read protection enable for UFM1 sector (0 = Read possible, 1 = Read disable)

i Erase protection enable for UFM1 sector (0 = Erase possible, 1 = Erase disable)

j Hard Lock enable for UFM0 sector (0 = Disabled (default), 1 = Enable)

k Read protection enable for UFM0 sector (0 = Read possible, 1 = Read disable)

l Erase protection enable for UFM0 sector (0 = Erase possible, 1 = Erase disable)

Example: 0x57 00 00 00 00 02

Read the UFM Security settings sector.

UFM0 flash sector is prohibited from reading

2.1.7. Program Centralized Security Setting (0x54)

This command is used to program the centralized security settings for all other Flash sectors except UFM. For example: CFG, feature, and security keys settings, and others.

Table 2.8. Program CSEC (0x54)

ISC Enable	CMD (Hex)	Operands (Hex)	Data Mode	Data Size	Data Format (Binary)
Y	54	00 00 00	W	4B	0bcd ehii fssl jjag kmno pqrt uvwy zαβξ

Data Format:

0: reserved

b: Hard Lock enable for I^2C Bridge (0 = Disabled (default), 1 = Enable)

c: I^2C Bridge locked (0 = Disabled (default), 1 = Enable)

I^2C bridge commands are disabled once this bit is set

d: Hard Lock enable for JTAG to SPI Bridge (0 = Disabled (default), 1 = Enable)

e: JTAG to SPI Bridge is locked (0 = Disabled (default), 1 = Enable)

JTAG to SPI bridge commands are disabled once this bit is set

h: Hard Lock enable for Slave I^2C Port (0 = Disabled (default), 1 = Enable)

ii: Slave I^2C Port lock modes

Mode: Slave I^2C Port

Mode	Slave I^2C Port
00	Unlocked
01	Locked
10	Partially Locked*
11	Locked

*Only certain commands are allowed to execute in partial lock mode

f: Hard Lock enable for Slave SPI Port (0 = Disabled (default), 1 = Enable)

ss: Slave SPI Port lock modes

Mode: Slave SPI Port

Mode	Slave SPI Port
00	Unlocked
01	Locked
10	Partially Locked*
11	Locked

*Only certain commands are allowed to execute in partial lock mode

l: Hard Lock enable for JTAG Port (0 = Disabled (default), 1 = Enable)

jj: JTAG Port lock modes

Mode: JTAG Port

Mode	JTAG Port
00	Unlocked
01	Partially Locked*
10	Partially Locked**
11	Locked

*Only certain 1149 commands are allowed to execute in partial lock mode

**Only certain 1532 and some 1149 commands are allowed to execute in partial lock mode

a g k: SRAM lock settings

SRAM Lock Settings			
a	Hard Lock enable	0	Disable (default)
		1	Enable
g	Read Protection enable	0	Read possible (default)
		1	Read disable
k	Erase Protection enable	0	Erase possible (default)
		1	Erase disable

m n o: AESKEY Lock Settings

AESKEY Lock Settings			
m	Hard Lock Enable	0	Disabled (default)
		1	Enable
n	Read Protection Enable	0	Read possible (default)
		1	Read disable
o	Erase Protection Enable	0	Erase possible (default)
		1	Erase disable

p q r: Public Key Lock Settings

Public Key Lock Settings			
p	Hard Lock Enable	0	Disabled (default)
		1	Enable
q	Read Protection Enable	0	Read possible (default)
		1	Read disable
r	Erase Protection Enable	0	Erase possible (default)
		1	Erase disable

t u v: Feature Row Lock Settings

Feature Row Lock Settings			
t	Hard Lock Enable	0	Disabled (default)
		1	Enable
u	Read Protection Enable	0	Read possible (default)
		1	Read disable
v	Erase Protection Enable	0	Erase possible (default)
		1	Erase disable

w y z: CFG1 Sector Lock Settings

CFG1 Lock Settings			
w	Hard Lock Enable	0	Disabled (default)
		1	Enable
y	Read Protection Enable	0	Read possible (default)
		1	Read disable
z	Erase Protection Enable	0	Erase possible (default)
		1	Erase disable

α β ξ: CFG0 Sector Lock Settings

CFG0 Lock Settings			
α	Hard Lock Enable	0	Disabled (default)
		1	Enable
β	Read Protection Enable	0	Read possible (default)
		1	Read disable
ξ	Erase Protection Enable	0	Erase possible (default)
		1	Erase disable

Example: 0x54 00 00 00 0D 20 Program centralized security settings

2.1.8. Read Centralized Security Setting (0x55)

This command is used to read the centralized security settings for all other Flash sectors except UFM. For example: CFG, feature, and security keys settings.

Table 2.9. Read CSEC (0x55)

ISC Enable	CMD (Hex)	Operands (Hex)	Data Mode	Data Size	Data Format (Binary)
Y	55	00 00 00	W	4B	xbcd ehii fssl jjag kmno pqrt uvwy zαβξ

Data Format:

x: reserved

b: Hard Lock enable for I^2C Bridge (0 = Disabled (default), 1 = Enable)

c: I^2C Bridge locked (0 = Disabled (default), 1 = Enable)

I^2C bridge commands are disabled once this bit is set

d: Hard Lock enable for JTAG to SPI Bridge (0 = Disabled (default), 1 = Enable)

e: JTAG to SPI Bridge is locked (0 = Disabled (default), 1 = Enable)

JTAG to SPI bridge commands are disabled once this bit is set

h: Hard Lock enable for Slave I^2C Port (0 = Disabled (default), 1 = Enable)

ii: Slave I^2C Port lock modes

Mode: Slave I^2C Port

Mode	Slave I^2C Port
00	Unlocked
01	Locked
10	Partially Locked*
11	Locked

*Only certain commands are allowed to execute in partial lock mode

f: Hard Lock enable for Slave SPI Port (0 = Disabled (default), 1 = Enable)

ss: Slave SPI Port lock modes

Mode: Slave SPI Port

Mode	Slave SPI Port
00	Unlocked
01	Locked
10	Partially Locked*
11	Locked

*Only certain commands are allowed to execute in partial lock mode

l: Hard Lock enable for JTAG Port (0 = Disabled (default), 1 = Enable)

jj: JTAG Port lock modes

Mode: JTAG Port

Mode	JTAG Port
00	Unlocked
01	Partially Locked*
10	Partially Locked**
11	Locked

*Only certain 1149 commands are allowed to execute in partial lock mode

**Only certain 1532 and some 1149 commands are allowed to execute in partial lock mode

a g k: SRAM lock settings

SRAM Lock Settings			
a	Hard Lock enable	0	Disable (default)
		1	Enable
g	Read Protection enable	0	Read possible (default)
		1	Read disable
k	Erase Protection enable	0	Erase possible (default)
		1	Erase disable

m n o: AESKEY Lock Settings

AESKEY Lock Settings			
m	Hard Lock Enable	0	Disabled (default)
		1	Enable
n	Read Protection Enable	0	Read possible (default)
		1	Read disable
o	Erase Protection Enable	0	Erase possible (default)
		1	Erase disable

p q r: Public Key Lock Settings

Public Key Lock Settings			
p	Hard Lock Enable	0	Disabled (default)
		1	Enable
q	Read Protection Enable	0	Read possible (default)
		1	Read disable
r	Erase Protection Enable	0	Erase possible (default)
		1	Erase disable

t u v: Feature Row Lock Settings

Feature Row Lock Settings			
t	Hard Lock Enable	0	Disabled (default)
		1	Enable
u	Read Protection Enable	0	Read possible (default)
		1	Read disable
v	Erase Protection Enable	0	Erase possible (default)
		1	Erase disable

w y z: CFG1 Sector Lock Settings

CFG1 Lock Settings			
w	Hard Lock Enable	0	Disabled (default)
		1	Enable
y	Read Protection Enable	0	Read possible (default)
		1	Read disable
z	Erase Protection Enable	0	Erase possible (default)
		1	Erase disable

α β ξ: CFG0 Sector Lock Settings

CFG0 Lock Settings			
α	Hard Lock Enable	0	Disabled (default)
		1	Enable
β	Read Protection Enable	0	Read possible (default)
		1	Read disable
ξ	Erase Protection Enable	0	Erase possible (default)
		1	Erase disable

Example: 0x55 00 00 00 Read centralized security settings

2.1.9. Program Authentication Mode (0xC4)

This command is used to program the authentication mode bits.

Table 2.10. Program Authentication Mode (0xC4)

ISC Enable	CMD (Hex)	Operands (Hex)	Data Mode	Data Size	Data Format (Binary)
Y	C4	00 00 00	W	1B	xxxx xxaa

Data Format: xxxx xx: Reserved

aa: Authentication Mode

aa	Authentication Mode
00	Authentication disabled
01	Authentication disabled
10	HMAC authentication enabled
11	ECDSA signature verification enabled

Example: 0xC4 00 00 00 03 ECDSA Signature verification is enabled.

2.1.10. Read Authentication Mode (0xC5)

This command is used to read the authentication mode bits.

Table 2.11. Program Authentication Mode (0xC4)

ISC Enable	CMD (Hex)	Operands (Hex)	Data Mode	Data Size	Data Format (Binary)
Y	C5	00 00 00	W	1B	xxxx xxaa

Data Format: xxxx xx: Reserved

aa: Authentication Mode

aa	Authentication Mode
00	Authentication disabled
01	Authentication disabled
10	HMAC authentication enabled
11	ECDSA signature verification enabled

Example: 0xC4 00 00 00 00 03 Read the authentication mode. ECDSA Signature verification is enabled.

2.1.11. Authentication DONE (0xCC)

This command is used to program the authentication done bit.

Table 2.12. Authentication DONE (0xCC)

ISC Enable	CMD (Hex)	Operands (Hex)	Data Mode	Data Size	Data Format
Y	CC	00 00 00	—	—	—

Example: 0xCC 00 00 00

Set the Authentication DONE bit.

Note: Poll the BUSY bit (or wait 200 µs) after issuing this command for programming to complete before issuing a subsequent command other than Read Status or Check Busy.

2.1.12. Program FEABITs (0xF8)

This command is used to program the feature bits such as booting sequence selection, password settings, and others. CSEC and USEC flash sectors information is described below; for details about the other flash sectors, refer to Using Hardened Control Functions in MachXO3D Devices Reference Guide (FPGA-TN-02119).

Table 2.13. Program FEABITs (0xF8)

ISC Enable	CMD (Hex)	Operands (Hex)	Data Mode	Data Size	Data Format (Binary)
Y	F8	00 00 00	W	4B	0000 0000 0000 000e cbbb misj dnpa wvug

Data Format:

w	v	u	Flash Protection Sector Selection
0	0	0	No protection to any Flash sector
0	0	1	All UFMs
0	1	0	Feature, Security Keys, CSEC
0	1	1	Feature, Security Keys, CSEC, USEC, and all UFMs
1	0	0	CFG0 and CFG1
1	0	1	CFG0, CFG1, CSEC, all UFMs, and USEC
1	1	0	Feature, Security Keys, CSEC, CFG0, and CFG1
1	1	1	Feature, Security Keys, CSEC, CFG0, CFG1, USEC, and all UFMs

Example: 0xF8 00 00 00 0D 20 Programs the FEABITs

2.1.13. Read FEABITs (0xF8)

This command is used to read the feature bits such as booting sequence selection, password settings, and others. CSEC and USEC flash sectors information is described below for details about the other flash sector, refer to Using Hardened Control Functions in MachXO3D Devices Reference Guide (FPGA-TN-02119).

Table 2.14. Read FEABITs (0xF8)

ISC Enable	CMD (Hex)	Operands (Hex)	Data Mode	Data Size	Data Format (Binary)
Y	FB	00 00 00	R	4B	xxxx xxxx xxxx xxxe cbbb misj dnpa wvug

Data Format:

w	v	u	Flash Protection Sector Selection
0	0	0	No protection to any Flash sector
0	0	1	All UFMs
0	1	0	Feature, Security Keys, CSEC
0	1	1	Feature, Security Keys, CSEC, USEC, and all UFMs
1	0	0	CFG0 and CFG1
1	0	1	CFG0, CFG1, CSEC, all UFMs, and USEC
1	1	0	Feature, Security Keys, CSEC, CFG0, and CFG1
1	1	1	Feature, Security Keys, CSEC, CFG0, CFG1, USEC, and all UFMs

Example: 0xF8 00 00 00 Read the FEABITs

Technical Support Assistance

Submit a technical support case through www.latticesemi.com/techsupport.

Revision History

Revision 1.0, September 2020

Section	Change Summary
All	Initial release.

www.latticesemi.com