Lattice Sentry QSPI Monitor IP Core for MachXO3D - Lattice Propel Builder

User Guide

FPGA-IPUG-02110-1.0

May 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

Figures

Tables

Acronyms in This Document

A list of acronyms used in this document.

Acronym	Definition
APB	Advanced Peripheral Bus
CPU	Central Processing Unit
EAR	Extended Address Register
QSPI	Quad Serial Peripheral Interface
PLD	Programmable Logic Device
SPI	Serial Peripheral Interface

1. Introduction

A Quad-Serial Peripheral Interface (QSPI) is a serial interface wherein four data lines are used to read, write, and erase flash chips. It is faster than the traditional Serial Peripheral Interface (SPI) and is specifically designed to communicate with flash chips that support this interface. Unlike the traditional SPI that uses separate data lines for input and output (MISO and MOSI), the QSPI interface configures the data lines on the fly to act as outputs to send some information to the flash memory and act as inputs to read some memory contents.

The Lattice Semiconductor Sentry™ QSPI Monitor for MachXO3D™ is a security module that can monitor SPI or QSPI buses. The design is implemented in Verilog HDL. It can be configured and generated using Lattice Propel™ Builder. It can be targeted to MachXO3D FPGA devices and implemented using the Latttice Diamond® software Place and Route tool integrated with the Synplify Pro® synthesis tool.

1.1. Features

The key features of the QSPI Monitor IP are:

- Supports up to five external SPI/QSPI buses to monitor illegal activity
- Enable/disable dynamically the flash initialization commands per monitor
- Flash commands (program, read, erase) are monitored based on address ranges
- Supports up to four dynamically configurable address ranges for filtering per monitor
- Supports both 24-bit and 32-bit flash addressing modes/commands
- AMBA 3 APB Protocol v1.0

1.2. Conventions

1.2.1. Nomenclature

The nomenclature used in this document is based on Verilog HDL.

1.2.2. Signal Names

Signal names that end with:

- *_n* are active low (asserted when value is logic 0)
- *_i* are input signals
- *_o* are output signals
- *_io* are bi-directional input/output signals

1.2.3. Host

The logic unit inside the FPGA interacts with the QSPI Monitor IP through APB.

1.2.4. Attribute Names

Attribute names in this document are formatted in title case and italicized (*Attribute Name*).

2. Functional Description

2.1. Overview

The QSPI Monitor is a configurable security module that can monitor up to five SPI or QSPI buses for unauthorized activity and prevent transactions from completing by controlling external quick switch devices. In addition to monitoring, the QSPI Monitor can connect external SPI/QSPI buses to internal SPI/QSPI masters and slaves through a programmable mux/demux block.

2.2. Block Diagram

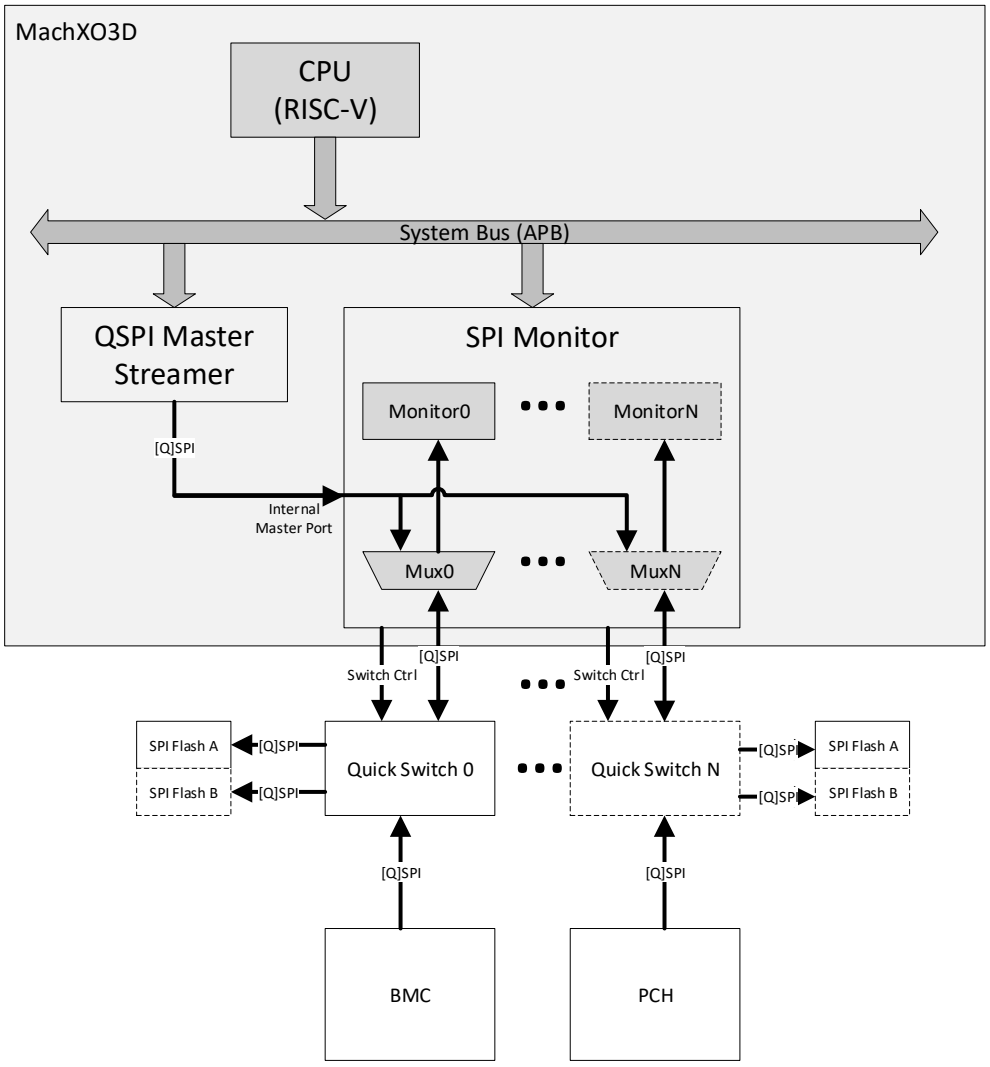

Figure 2.1. QSPI Monitor Block Diagram

2.3. Signal Description

Table 2.1. QSPI Monitor Signal Description

Port	Width	Direction	Description
System			
clk_i	1	Input	Master clock input
reset_i	1	Input	Asynchronous reset active high
int_o	1	Output	Interrupt request
APB			
apb_psel_i	In	1	Select signal. Indicates that the slave device is selected and a data transfer is required.
apb_paddr_i	In	32	Address signal.
apb_pwdata_i	In	32	Write data signal.
apb_pwrite_i	In	1	Direction signal. Write = 1, Read = 0
apb_penable_i	In	1	Enable signal. Indicates the second and subsequent cycles of an APB transfer.
apb_pready_o	Out	1	Ready signal. Indicates transfer completion. Slave uses this signal to extend an APB transfer.
apb_prdata_o	Out	32	Read data signal.
External QSPI Buses			
qpi_csn_pre_i	*No. of Bus Monitors*	Input	Chip select before quick switch
qpi_csn_o	*No. of Bus Monitors*	Output	Chip select
qpi_sck_io	*No. of Bus Monitors*	Input	SPI/QSPI clock
qpi_sio0	*No. of Bus Monitors*	Input	SPI: MOSI QSPI: serial data input and output
qpi_sio1	*No. of Bus Monitors*	Inpout	SPI: MISO QSPI: serial data input and output
qpi_sio2	*No. of Bus Monitors*	Input	SPI: unused QSPI: serial data input and output
qpi_sio3	*No. of Bus Monitors*	Input	SPI: unused QSPI: serial data input and output
External Quick Switch Control			
qs_out_en_o	*No. of Bus Monitors*	Output	Quick Switch Output Enable (0=disabled, 1=enabled)
qs_flasha_dis_o	*No. of Bus Monitors*	Output	Quick Switch Disable Flash A (0=enabled, 1=disabled)
qs_flashb_dis_o	*No. of Bus Monitors*	Output	Quick Switch Disable Flash B (0=enabled, 1=disabled)
SPI/QSPI Mux Master Port			
spi_mst_csn_i	1	Input	Chip select
spi_mst_sck_i	1	Input	SPI/QSPI clock
spi_mst_si_o	4	Output	SPI: spi_mst_si_o[1]=MISO, spi_mst_si_o[3:2]=unused, spi_mst_si_o[0]=unused QSPI: spi_mst_si_o[3:0] = serial data input
spi_mst_so_i	4	Input	SPI: spi_mst_so_i[0]=MOSI, spi_mst_so_i[3:1]=unused QSPI: spi_mst_so_i[3:0] = serial data output
spi_mst_oe_i	3	Input	spi_mst_oe_i[0]: direction control for qpi_sio0 (1=output, 0=input) spi_mst_oe_i[1]: direction control for qpi_sio1 (1=output, 0=input) spi_mst_oe_i[2]: direction control for qpi_sio2 and qpi_sio3 (1=output, 0=input)

2.4. Attribute Summary

The configurable attributes of the QSPI Monitor IP are as shown in Table 2.2 and are described in Table 2.3.

Table 2.2. Attributes Table

Attribute	Selectable Values	Default	Dependency on Other Attributes
General			
No. of Bus Monitors	1, 2, 3, 4, 5	1	—
Monitor N Settings (where N == *No. of Bus Monitors*)			
Monitor only	0, 1	0	*No. of Bus Monitors == N*
SPI Mode	0, 3	0	*No. of Bus Monitors == N*
Maximum Address	FFFF - FFFFFFFF	3FFFFFF	*No. of Bus Monitors == N*
Initialization Command 0	00 - FF, FFFF	01 (WRSR)	*No. of Bus Monitors == N*
Initialization Command 1	00 - FF, FFFF	04 (WRDI)	*No. of Bus Monitors == N*
Initialization Command 2	00 - FF, FFFF	05 (RDSR)	*No. of Bus Monitors == N*
Initialization Command 3	00 - FF, FFFF	06 (WREN)	*No. of Bus Monitors == N*
Initialization Command 4	00 - FF, FFFF	50 (WRSR_EN)	*No. of Bus Monitors == N*
Initialization Command 5	00 - FF, FFFF	9F (RDID)	*No. of Bus Monitors == N*
Initialization Command 6	00 - FF, FFFF	C7 (CHIP_ERASE)	*No. of Bus Monitors == N*
Initialization Command 7	00 - FF, FFFF	60 (CHIP_ERASE)	*No. of Bus Monitors == N*
Initialization Command 8	00 - FF, FFFF	FFFF	*No. of Bus Monitors == N*
Initialization Command 9	00 - FF, FFFF	FFFF	*No. of Bus Monitors == N*
Page Program Command	00 - FF, FFFF	02	*No. of Bus Monitors == N*
Page Program Quad Address Quad Data Command	00 - FF, FFFF	38	*No. of Bus Monitors == N*
Erase 4KB Command	00 - FF, FFFF	20	*No. of Bus Monitors == N*
Erase 32KB Command	00 - FF, FFFF	52	*No. of Bus Monitors == N*
Erase 64KB Command	00 - FF, FFFF	D8	*No. of Bus Monitors == N*
Read Command	00 - FF, FFFF	03	*No. of Bus Monitors == N*
Fast Read Command	00 - FF, FFFF	0B	*No. of Bus Monitors == N*
Read Quad Data Command	00 - FF, FFFF	6B	*No. of Bus Monitors == N*
Read Quad Address Quad Data Command	00 - FF, FFFF	EB	*No. of Bus Monitors == N*
Enable Quad SPI Mode	0, 1	0	*No. of Bus Monitors == N*
Quad SPI Mode Enter Command	00 - FF, FFFF	35	*No. of Bus Monitors == N* *Enable Quad SPI Mode == 1*
Quad SPI Mode Exit Command	00 - FF, FFFF	F5	*No. of Bus Monitors == N* *Enable Quad SPI Mode == 1*
Enable 4-byte Address	0, 1	0	*No. of Bus Monitors == N*
4-byte Mode Enter Command	00 - FF, FFFF	B7	*No. of Bus Monitors == N* *Enable 4-byte Address == 1*
4-byte Mode Exit Command	00 - FF, FFFF	E9	*No. of Bus Monitors == N* *Enable 4-byte Address == 1*
4-byte Read Extended Address Command	00 - FF, FFFF	C8	*No. of Bus Monitors == N* *Enable 4-byte Address == 1*
4-byte Write Extended Address Command	00 - FF, FFFF	C5	*No. of Bus Monitors == N* *Enable 4-byte Address == 1*
4-byte Page Program Command	00 - FF, FFFF	12	*No. of Bus Monitors == N* *Enable 4-byte Address == 1*
4-byte Page Program Quad Address Quad Data Command	00 - FF, FFFF	3E	*No. of Bus Monitors == N* *Enable 4-byte Address == 1*
4-byte Erase 4KB Command	00 - FF, FFFF	21	*No. of Bus Monitors == N* *Enable 4-byte Address == 1*

Attribute	Selectable Values	Default	Dependency on Other Attributes
4-byte Erase 32KB Command	00 - FF, FFFF	5C	*No. of Bus Monitors == N* *Enable 4-byte Address == 1*
4-byte Erase 64KB Command	00 - FF, FFFF	DC	*No. of Bus Monitors == N* *Enable 4-byte Address == 1*
4-byte Read Command	00 - FF, FFFF	13	*No. of Bus Monitors == N* *Enable 4-byte Address == 1*
4-byte Fast Read Command	00 - FF, FFFF	0C	*No. of Bus Monitors == N* *Enable 4-byte Address == 1*
4-byte Read Quad Data Command	00 - FF, FFFF	6C	*No. of Bus Monitors == N* *Enable 4-byte Address == 1*
4-byte Read Quad Address Quad Data Command	00 - FF, FFFF	EC	*No. of Bus Monitors == N* *Enable 4-byte Address == 1*

Table 2.3. Attribute Descriptions

Attribute	Description
General	
No. of Bus Monitors	Number of external SPI/QSPI buses to monitor
Monitor N Settings (where N == *No. of Bus Monitors*)	
Monitor only	Monitor N Monitor Only When this parameter is 1, illegal operations are detected and reported but are not blocked (operations are allowed to proceed).
SPI Mode	Monitor N SPI Mode (0 or 3)
Maximum Address	Monitor N Maximum Address SPI transaction starting addresses and incremental addresses are masked with this value before comparison with address space ranges.
Initialization Command 0	Monitor N Initialization Command 0
Initialization Command 1	Monitor N Initialization Command 1
Initialization Command 2	Monitor N Initialization Command 2
Initialization Command 3	Monitor N Initialization Command 3
Initialization Command 4	Monitor N Initialization Command 4
Initialization Command 5	Monitor N Initialization Command 5
Initialization Command 6	Monitor N Initialization Command 6
Initialization Command 7	Monitor N Initialization Command 7
Initialization Command 8	Monitor N Initialization Command 8
Initialization Command 9	Monitor N Initialization Command 9
Page Program Command	Monitor N Page Program Command Command/Address/Data widths are all 1-bit in SPI mode, 4-bit in QSPI mode.
Page Program Quad Address Quad Data Command	Monitor N Page Program Quad Address Quad Data Command Command width is 1-bit. Address and Data widths are 4-bit.
Erase 4KB Command	Monitor N Erase 4 KB Command
Erase 32KB Command	Monitor N Erase 32 KB Command
Erase 64KB Command	Monitor N Erase 64 KB Command
Read Command	Monitor N Read Command.
Fast Read Command	Monitor N Fast Read Command Command/Address/Data widths are all 1-bit in SPI mode, 4-bit in QSPI mode.
Read Quad Data Command	Monitor N Read Quad Data Command Command/Address widths are 1-bit in SPI mode, 4-bit in QSPI mode. Data width is 4-bit.

Attribute	Description
Read Quad Address Quad Data Command	Monitor N Read Quad Address Quad Data Command Command width is 1-bit in SPI mode, 4-bit in QSPI mode. Address and Data widths are 4-bit.
Enable Quad SPI Mode	Monitor N Enable Quad SPI Mode Support When this parameter is 1, the monitor watches for the specified SPI commands to enter and leave Quad SPI Mode and mirrors the SPI/QSPI status of the flash device. When this parameter is 0, these SPI commands are treated as illegal (blocked and logged) and the monitor does not change state.
Quad SPI Mode Enter Command	Monitor N Quad SPI Mode Enter Command
Quad SPI Mode Exit Command	Monitor N Quad SPI Mode Exit Command
Enable 4-byte Address	Monitor N Enable 4-Byte Address Support When this parameter is 1, the 4B_*_CMD parameters are valid and 4-byte addressing can be enabled/disabled dynamically by the allow_4byte_addr bit field. When this parameter is 0, all of the associated 4-byte address monitoring logic is removed, the 4B_*_CMD parameters are ignored, allow_4byte_addr is forced to 0, and all 4-byte address commands are treated as illegal.
4-byte Mode Enter Command	Monitor N 4-Byte Mode Enter Command
4-byte Mode Exit Command	Monitor N 4-Byte Mode Exit Command
4-byte Read Extended Address Command	Monitor N 4-Byte Read Extended Address Register Command
4-byte Write Extended Address Command	Monitor N 4-Byte Write Extended Address Register Command
4-byte Page Program Command	Monitor N 4-Byte Page Program Command
4-byte Page Program Quad Address Quad Data Command	Monitor N 4-Byte Page Program Quad Address Quad Data Command.
4-byte Erase 4KB Command	Monitor N 4-Byte Erase 4 KB Command
4-byte Erase 32KB Command	Monitor N 4-Byte Erase 32 KB Command
4-byte Erase 64KB Command	Monitor N 4-Byte Erase 64 KB Command
4-byte Read Command	Monitor N 4-Byte Read Command
4-byte Fast Read Command	Monitor N 4-Byte Fast Read Command Command/Address/Data widths are all 1-bit in SPI mode, 4-bit in QSPI mode.
4-byte Read Quad Data Command	Monitor N 4-Byte Read Quad Data Command Command/Address widths are 1-bit in SPI mode, 4-bit in QSPI mode. Data width is 4-bit.
4-byte Read Quad Address Quad Data Command	Monitor N 4-Byte Read Quad Address Quad Data Command Command width is 1-bit in SPI mode, 4-bit in QSPI mode. Address and Data widths are 4-bit.

2.5. Register Description

Global registers are mapped to offsets 0x000–0x0FC and per-monitor registers are mapped to 0xN00–0xNFF, where *N* corresponds to the monitor number, in the range of 1 to NUM_BUS_MONITORS. For example, registers of the first monitor are at offsets 0x100–0x1FC and registers of the second monitor are at 0x200–0x2FC.

Table 2.4. Summary of QSPI Monitor IP Core Registers

Offset	Register Name	Access	Default Value	Description
0x000	MONITOR_CFG	RO	(depends on the *No. of Bus Monitors* attribute)	num_bus_monitors[3:0] – Number of bus monitors (NUM_BUS_MONITORS) reserved[31:4]
0x004	MONITOR_CTRL	RW	0	The number of valid bit fields in this register depends on NUM_BUS_MONITORS. monitor0_en[0] – Enable/disable Monitor0 monitor1_en[1] – Enable/disable Monitor1 monitor2_en[2] – Enable/disable Monitor2 monitor3_en[3] – Enable/disable Monitor3 monitor4_en[4] – Enable/disable Monitor4 reserved[31:5] **Note:** Any unused enable bits are considered reserved.
0x010	INT_STATUS	RW	0	Interrupt Status The number of valid bit fields in this register depends on NUM_BUS_MONITORS. Interrupt status: illegal_op0_int[0] – Bus 0 Illegal Operation interrupt illegal_op0_overflow_int[1] – Bus 0 Illegal Operation Overflow interrupt reserved[3:2] illegal_op1_int[4] – Bus 1 Illegal Operation interrupt illegal_op1_overflow_int[5] – Bus 1 Illegal Operation Overflow interrupt reserved[7:6] illegal_op2_int[8] – Bus 2 Illegal Operation interrupt illegal_op2_overflow_int[9] – Bus 2 Illegal Operation Overflow interrupt reserved[11:10] illegal_op3_int[12] – Bus 3 Illegal Operation interrupt illegal_op3_overflow_int[13] – Bus 3 Illegal Operation Overflow interrupt reserved[15:14] illegal_op4_int[16] – Bus 4 Illegal Operation interrupt illegal_op4_overflow_int[17] – Bus 4 Illegal Operation Overflow interrupt reserved[31:18] Writing 1 to a bit clears that interrupt.

Offset	Register Name	Access	Default Value	Description
0x014	INT_ENABLE	RW	0	Interrupt Enable The number of valid bit fields in this register depends on NUM_BUS_MONITORS. Interrupt enable: illegal_op0_en[0] – Enable Bus 0 Illegal Operation interrupt illegal_ op0_overflow_en[1] – Enable Bus 0 Illegal Operation Overflow interrupt reserved[3:2] illegal_op1_en[4] – Enable Bus 1 Illegal Operation interrupt illegal_op1_overflow_en[5] – Enable Bus 1 Illegal Operation Overflow interrupt reserved[7:6] illegal_op2_en[8] – Enable Bus 2 Illegal Operation interrupt illegal_op2_overflow_en[9] – Enable Bus 2 Illegal Operation Overflow interrupt reserved[11:10] illegal_op3_en[12] – Enable Bus 3 Illegal Operation interrupt illegal_op3_overflow_en[13] – Enable Bus 3 Illegal Operation Overflow interrupt reserved[15:14] illegal_op4_en[16] – Enable Bus 4 Illegal Operation interrupt illegal_op4_overflow_en[17] – Enable Bus 4 Illegal Operation Overflow interrupt reserved[31:18]
0x018	INT_SET	RW	0	Interrupt Set The number of valid bit fields in this register depends on NUM_BUS_MONITORS. Interrupt set: illegal_op0_set[0] – Set Bus 0 Illegal Operation interrupt illegal_op0_overflow_set[1] – Set Bus 0 Illegal Operation Overflow interrupt reserved[3:2] illegal_op1_set[4] – Set Bus 1 Illegal Operation interrupt illegal_op1_overflow_set[5] – Set Bus 1 Illegal Operation Overflow interrupt reserved[7:6] illegal_op2_set[8] – Set Bus 2 Illegal Operation interrupt illegal_op2_overflow_set[9] – Set Bus 2 Illegal Operation Overflow interrupt reserved[11:10] illegal_op3_set[12] – Set Bus 3 Illegal Operation interrupt illegal_op3_overflow_set[13] – Set Bus 3 Illegal Operation Overflow interrupt reserved[15:14] illegal_op4_set[16] – Set Bus 4 Illegal Operation interrupt illegal_op4_overflow_set[17] – Set Bus 4 Illegal Operation Overflow interrupt reserved[31:18] Writing 1 to a bit sets that interrupt

Offset	Register Name	Access	Default Value	Description
0x*N*00	CONTROL	RW	0x00	mux_sel[3:0] – Select which internal client is connected to the external SPI/QSPI pins 0: SPI/QSPI Monitor 1: Internal master interface 0 2-7: reserved flash_a_en[4] – Flash A is disabled (0) or enabled (1) flash_b_en[5] – Flash B is disabled (0) or enabled (1) reserved[7:6] init_cmd_filter[8] – Block initialization commands allow_4byte_addr[9] – Allow 4-byte addressing commands reserved[31:10]
0x*N*04	SPACE_EN	RW	0x00	Space monitoring enable bits space0_en[0] – Disable (0) or enable (1) monitoring of space 0 space1_en[1] – Disable (0) or enable (1) monitoring of space 1 space2_en[2] – Disable (0) or enable (1) monitoring of space 2 space3_en[3] – Disable (0) or enable (1) monitoring of space 3 reserved[31:4]
0x*N*08	READ_DUMMY_NUM	RW	0x8	Number of dummy cycles in an SPI flash read The minimum allowed value is 1. See the flash device data sheet for details. num_dummy_cycles[4:0] reserved[31:5]
0x*N*20	SPACE0_FILTER_CTRL	RW	0x03	prg_cmd_allow[0] – Allow (whitelist) program commands in space 0 erase_cmd_allow[1] – Allow (whitelist) erase commands in space 0 read_cmd_block[2] – Block (blacklist) read commands in space 0 reserved[31:3]
0x*N*24	SPACE0_START_ADDR	RW	0x00000000	page_start_addr[31:8] – Start address for space 0, aligned to 256-byte page boundary reserved[7:0] – Writes are ignored; Reads return 0
0x*N*28	SPACE0_END_ADDR	RW	0x000000FF	page_end_addr[31:8] – End address for space 0, aligned to 256-byte page boundary reserved_ff[7:0] – Writes are ignored; Reads return 0xFF.
0x*N*40	SPACE1_FILTER_CTRL	RW	0x03	prg_cmd_allow[0] – Allow (whitelist) program commands in space 1 erase_cmd_allow[1] – Allow (whitelist) erase commands in space 1 read_cmd_block[2] – Block (blacklist) read commands in space 1 reserved[31:3]
0x*N*44	SPACE1_START_ADDR	RW	0x00000000	page_start_addr[31:8] – Start address for space 1, aligned to 256-byte page boundary reserved[7:0] – Writes are ignored; Reads return 0.
0x*N*48	SPACE1_END_ADDR	RW	0x000000FF	page_end_addr[31:8] – End address for space 1, aligned to 256-byte page boundary reserved_ff[7:0] – Writes are ignored; Reads return 0xFF.

Offset	Register Name	Access	Default Value	Description
0x*N*60	SPACE2_FILTER_CTRL	RW	0x03	prg_cmd_allow[0] – Allow (whitelist) program commands in space 2 erase_cmd_allow[1] – Allow (whitelist) erase commands in space 2 read_cmd_block[2] – Block (blacklist) read commands in space 2 reserved[31:3]
0x*N*64	SPACE2_START_ADDR	RW	0x00000000	page_start_addr[31:8] – Start address for space 2, aligned to 256-byte page boundary. reserved[7:0] – Writes are ignored; Reads return 0.
0x*N*68	SPACE_END_ADDR	RW	0x000000FF	page_end_addr[31:8] – End address for space 2, aligned to 256-byte page boundary. reserved_ff[7:0] – Writes are ignored; Reads return 0xFF.
0x*N*80	SPACE3_CMD_CTRL	RW	0x03	prg_cmd_allow[0] – Allow (whitelist) program commands in space 3 erase_cmd_allow[1] – Allow (whitelist) erase commands in space 3 read_cmd_block[2] – Block (blacklist) read commands in space 3 reserved[31:3]
0x*N*84	SPACE3_START_ADDR	RW	0x00000000	page_start_addr[31:8] – Start address for space 3, aligned to 256-byte page boundary reserved[7:0] – Writes are ignored; Reads return 0.
0x*N*88	SPACE3_END_ADDR	RW	0x000000FF	page_end_addr[31:8] – End address for space 3, aligned to 256-byte page boundary reserved_ff[7:0] – Writes are ignored; Reads return 0xFF.
0x*N*F0	ILLEGAL_CMD	RO	0x00	illegal_cmd[7:0]: Illegal operation command reserved[31:8]
0x*N*F4	ILLEGAL_ADDR	RO	0x00000000	Illegal operation address

The behavior of registers to write and read access is defined by its access type, which is defined in Table 2.5.

Table 2.5. Access Type Definition

Access Type	Behavior on Read Access	Behavior on Write Access
RO	Returns register value	Ignores write access
WO	Returns 0	Updates register value
RW	Returns register value	Updates register value
RW1C	Returns register value	Writing 1’b1 on register bit clears the bit to 1’b0. Writing 1’b0 on register bit is ignored.
RSVD	Returns 0	Ignores write access

2.6. Initialization Command Filtering

When initialization command filtering is enabled, the QSPI Monitor watches for all of the commands defined in the *Initialization Command x* attribute (where x is the command number). If one of these commands is detected, the transaction is terminated immediately, the command is recorded in the illegal_cmd register, illegal_addr is set to 0, and an illegal operation interrupt is sent.

By default, filtering for initialization commands is disabled. In a typical use case, initialization commands are allowed for a certain period of time (such as during boot up) and then filtering can be enabled through the register interface.

2.7. Address Filtering

The QSPI Monitor can filter program, erase, and read commands based on address ranges. Up to four address ranges (also called spaces) can be monitored, and filtering can be enabled independently for program, erase, and read commands for each space. Each space consists of a start address, end address, and whitelist/blacklist indicators for each type of command. Address spaces are aligned on 256-byte page boundaries. The default setting for all spaces is to allow (whitelist) program, erase, and read operations in that space. The settings for each space can be modified to block (blacklist) program, erase, or read operations. Each type of operation (program, erase, or read) has a separate whitelist/blacklist setting.

Program/erase operations are considered illegal for all addresses except spaces that have been whitelisted.

- If a program operation starts from a page address that is not inside a whitelisted address space, it is considered illegal.
- If an erase operation starts from an address that is not inside a whitelisted address space, or starts from an address inside a whitelisted address space but the address range goes outside the whitelisted address space, it is considered illegal.

Read operations are allowed for all addresses except spaces that have been blacklisted.

- If a read operation starts from an address that is inside a blacklisted address space, or starts from an address outside a blacklisted address space and the incremental address crosses into a blacklisted address space, it is considered illegal.

When an illegal operation is detected, the transaction is terminated immediately, the command and address are saved in the illegal_cmd and illegal_addr registers, and an illegal operation interrupt is generated.

Because program/erase operations are blacklisted by default and read operations are whitelisted by default, the recommended usage model is to only define whitelist areas for program/erase operations and blacklist areas for read operations as address spaces.

Overlapping program/erase whitelist and read blacklist address spaces should be avoided because it can lead to unintended consequences, such as an address range being writable but not readable. This would prevent common use cases, such as the host verifying data written to flash by reading it back.

2.7.1. 24/32-Bit Addressing

Flash devices larger than 128 Mb (16 MB) provide three separate mechanisms for addressing beyond the traditional 24-bit address space:

- Commands to enter/exit 4-byte mode (EN4B/EX4B)
  When the flash is in 4-byte mode, commands which normally take a 3-byte address (read, erase, program, and others) expect 4-byte addresses instead of 3-byte addresses. The default is 3-byte mode.
- Extended Address Register (EAR)
  The EAR is an 8-bit register in the flash, which can be read and written using special commands (RDEAR/WREAR). When the flash is in 3-byte mode, the EAR is used to select which 128 Mbit segment is addressed by the 3-byte address. In other words, the value in EAR is used as the upper 8 bits of the 32-bit flash address (flash_addr[31:0] = {EAR, addr[23:16], addr[15:8], addr[7:0]}). The EAR default value is 0.
- 4-Byte Address Commands
  The 4-Byte commands, such as READ4B, FAST_READ4B, are separate commands from the standard 3-byte commands, such as READ, FAST_READ. The 4-Byte commands always take 4-byte addresses, regardless of whether the flash is in 4-byte or 3-byte mode, and do not use the EAR.

When the monitor is configured to allow 32-bit addressing, the monitor internally tracks the addressing status of the flash (3-byte/4-byte mode, EAR) based on commands observed on the SPI/QSPI bus and uses this information to filter addresses observed on the bus. When the flash is in 4-byte mode or a 4-byte command is detected, the monitor compares the 32-bit address on the bus with the configured address spaces to determine if the operation is illegal or allowed. When the flash is in 3-byte mode, the monitor compares the 32-bit value comprised of EAR and the 24-bit address on the bus with the configured address spaces to determine if the operation is illegal or allowed.

All address comparisons are performed with the full 32-bits to prevent aliasing between 24-bit and 32-bit addresses which could result in security holes or false illegal operation detection.

When the monitor is configured to not allow 32-bit addressing (allow_4byte_addr = 0), the monitor is set to 3-byte mode, EAR is set to 0, and all of the 4-byte commands defined in the *4-byte * Command* attribute (see Table 2.2) are considered illegal operations. If one of these commands is detected, the transaction is terminated immediately, the command and address are recorded in the illegal_cmd and illegal_addr registers, and an illegal operation interrupt is sent.

2.8. Unrecognized Command Filtering

If a command is detected that does not match any of the commands defined in the attributes table (see Table 2.2), the transaction is terminated immediately, the command is recorded in the illegal_cmd register, illegal_addr is set to 0, and an illegal operation interrupt is sent.

2.9. Timing Sequence

2.9.1. Illegal Command Blocking

If one of illegal command is detected (Figure 2.2), the transaction is terminated immediately by extending chip select and adding a clock pulse to confuse the SPI flash.

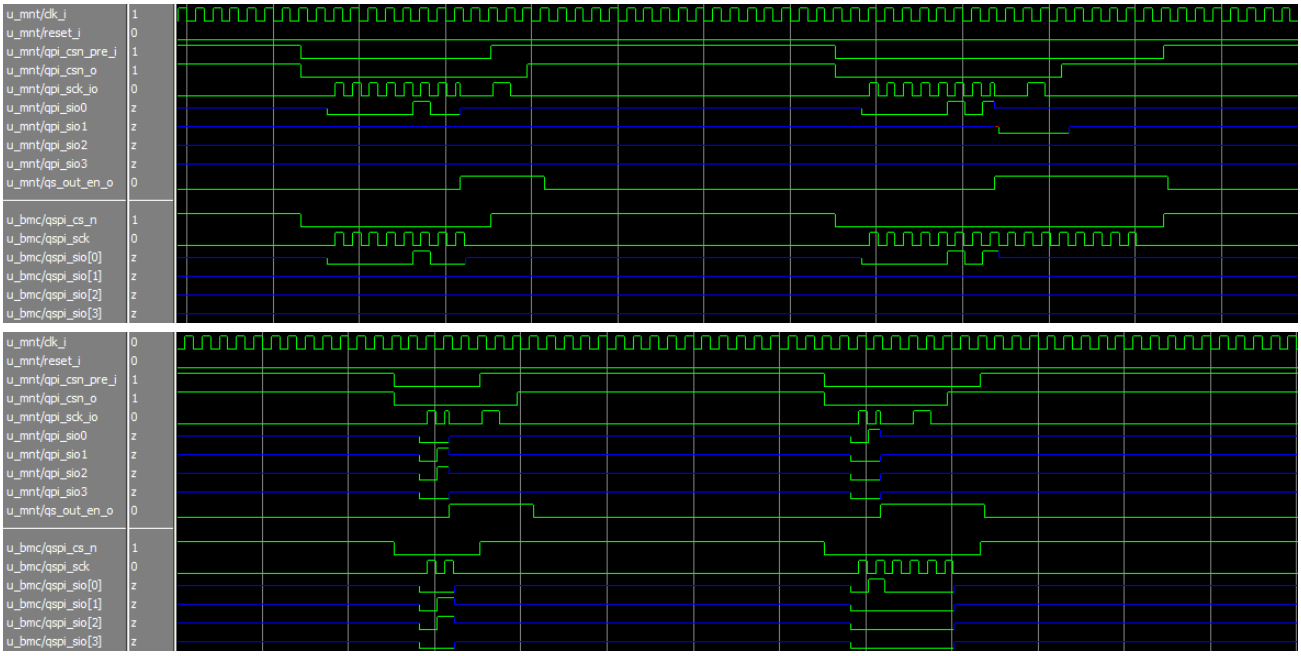

Figure 2.2. One Illegal Command

2.9.2. Illegal Erase Command Breaking (3-Byte Address)

If an illegal erase command is detected (Figure 2.3), the transaction is terminated immediately by driving chip select high.

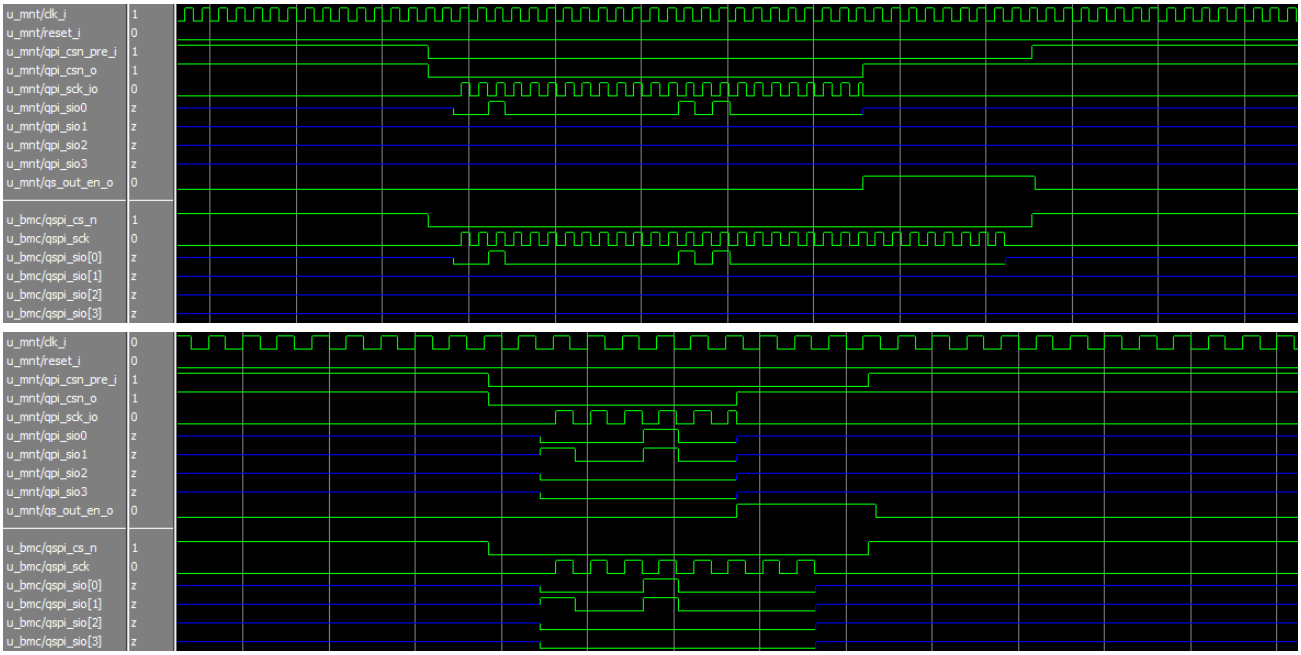

Figure 2.3. Illegal Erase Command

2.9.3. Illegal Program Command Breaking (3-Byte Address, Illegal Start Address)

If an illegal program command is detected (Figure 2.4), the transaction is terminated immediately by driving chip select high.

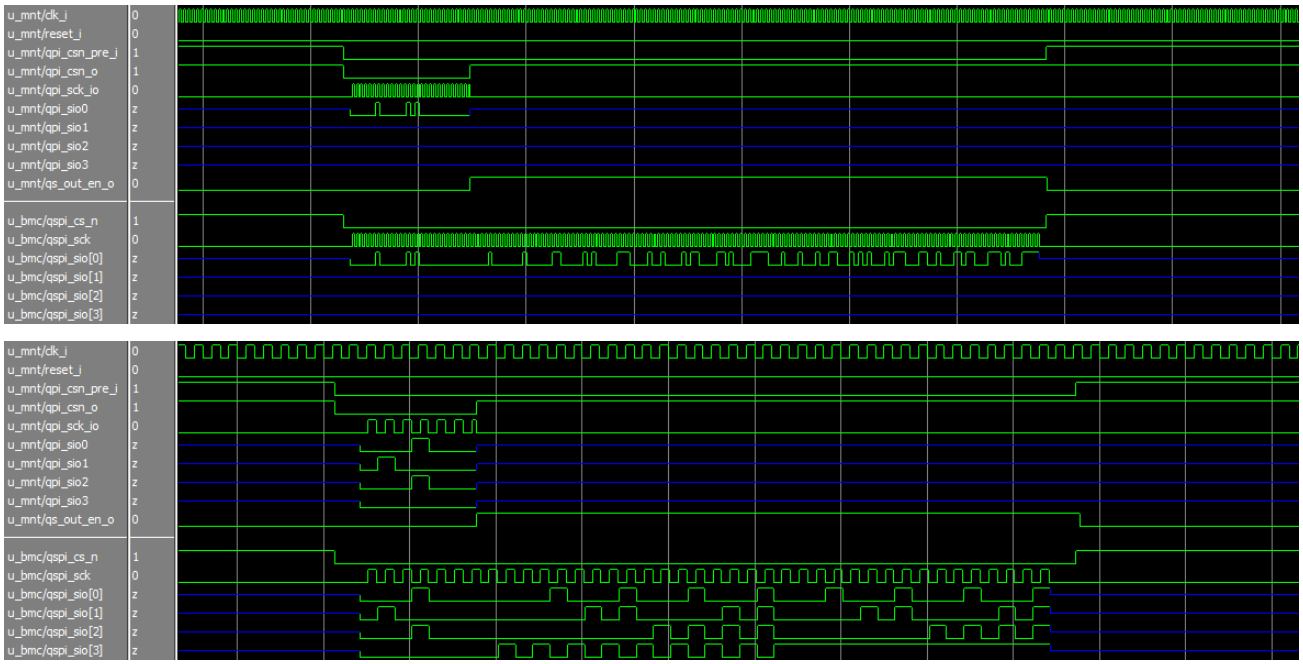

Figure 2.4. Illegal Program Command (3-byte Address, Illegal Start Address)

2.9.4. Illegal Read Command Breaking (3-Byte Address, Illegal Start Address)

If an illegal read command is detected (Figure 2.5), the transaction is terminated immediately by driving chip select high.

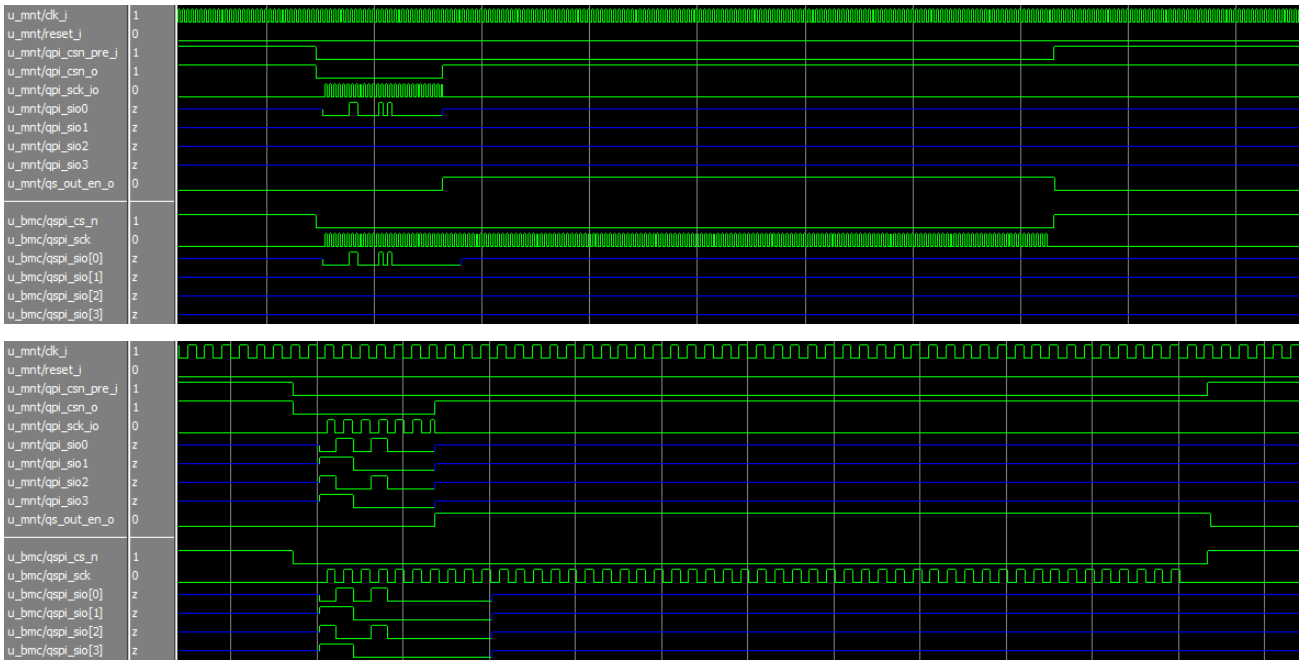

Figure 2.5. Illegal Read Command (3-byte Address, Illegal Start Address)

2.9.5. Illegal Read Command Breaking (3-byte address, incremental address overflow)

If a read command incremental address overflow is detected (Figure 2.6), the transaction is terminated immediately by driving chip select high.

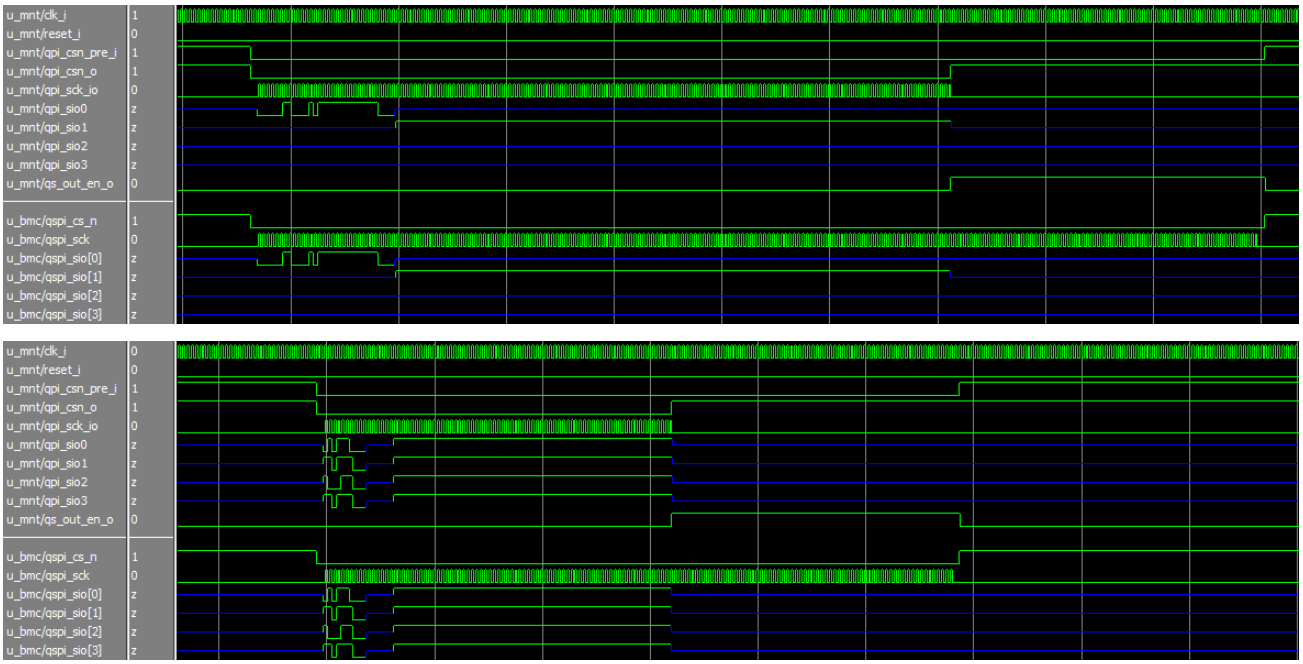

Figure 2.6. Illegal Read Command (3-Byte Address, Incremental Address Overflow)

2.9.6. Illegal 4-Byte Command Breaking

If a 4-byte command is disabled and a 4-byte command is detected (Figure 2.7), the transaction is terminated immediately by driving chip select high.

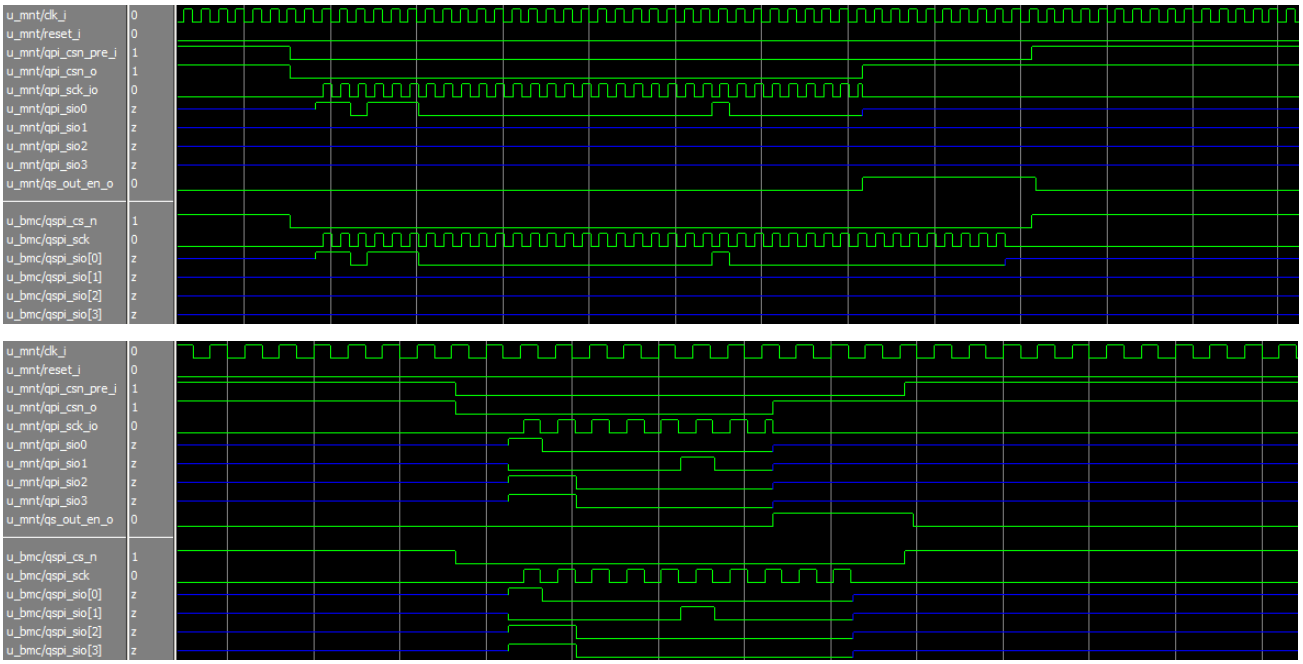

Figure 2.7. Illegal 4-Byte Command Breaking

2.10. Mux/Demux Functionality

Each external SPI/QSPI bus can be connected either to its corresponding monitor, or to an internal SPI/QSPI master through a mux/demux block. This allows the internal master to disable the monitor and access the external flash.

Each bus/monitor/mux combination is independent of the others. It is the responsibility of the firmware to manage the muxes appropriately to prevent the internal SPI/QSPI master from being connected to more than one external bus at a time.

3. Ordering Part Number

The Ordering Part Number (OPN) for the QSPI Monitor IP Core targeting MachXO3D FPGA devices are the following:

- QSPIMON-M3D-U – Project License
- QSPIMON-M3D-UT – Site License

Appendix A. Resource Utilization

Table A.1. Resource Utilization

NUM_BUS_MONITORS	Registers	LUTs	EBRs	Target Device	Synthesis Tools
1	550	885	0	MachXO3D	Synopsys® Synplify Pro N-2018.03L-SP1-1

References

- MachXO3D FPGA Web Page in latticesemi.com
- Lattice Propel 1.0 User Guide
- Lattice Diamond Software 3.11 User Guide

Technical Support Assistance

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

Revision History

Revision 1.0, May 2020

Section	Change Summary
All	Initial release.

www.latticesemi.com