MachXO4 Root of Trust Tamper Detection/Response

Technical Note

FPGA-TN-02434-1.0

September 2026

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, with all faults, and all associated risk is the responsibility entirely of the Buyer. The information provided herein is for informational purposes only and may contain technical inaccuracies or omissions, and may be otherwise rendered inaccurate for many reasons, and Lattice assumes no obligation to update or otherwise correct or revise this information. 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. LATTICE PRODUCTS AND SERVICES ARE NOT DESIGNED, MANUFACTURED, OR TESTED FOR USE IN LIFE OR SAFETY CRITICAL SYSTEMS, HAZARDOUS ENVIRONMENTS, OR ANY OTHER ENVIRONMENTS REQUIRING FAIL-SAFE PERFORMANCE, INCLUDING ANY APPLICATION IN WHICH THE FAILURE OF THE PRODUCT OR SERVICE COULD LEAD TO DEATH, PERSONAL INJURY, SEVERE PROPERTY DAMAGE OR ENVIRONMENTAL HARM (COLLECTIVELY, "HIGH-RISK USES"). FURTHER, BUYER MUST TAKE PRUDENT STEPS TO PROTECT AGAINST PRODUCT AND SERVICE FAILURES, INCLUDING PROVIDING APPROPRIATE REDUNDANCIES, FAIL-SAFE FEATURES, AND/OR SHUT-DOWN MECHANISMS. LATTICE EXPRESSLY DISCLAIMS ANY EXPRESS OR IMPLIED WARRANTY OF FITNESS OF THE PRODUCTS OR SERVICES FOR HIGH-RISK USES. 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.

Inclusive Language

This document was created consistent with Lattice Semiconductor’s inclusive language policy. In some cases, the language in underlying tools and other items may not yet have been updated. Please refer to Lattice’s inclusive language FAQ 6878 for a cross reference of terms. Note in some cases such as register names and state names it has been necessary to continue to utilize older terminology for compatibility.

Contents

Figures

Tables

Abbreviations in This Document

A list of abbreviations used in this document.

Abbreviation	Definition
EFB	Embedded Function Block
I2C	Inter-Integrated Circuit
JTAG	Joint Test Action Group
SPI	Serial Peripheral Interface
SRAM	Static Random Access Memory
SSPI	Target Serial Peripheral Interface
SI2C	Target Inter-Integrated Circuit
UFM	User Flash Memory
WB	WISHBONE

1. Introduction

The Lattice MachXO4™ RoT device family is the next generation of Lattice Semiconductor low-density PLDs including enhanced security features and on-chip dual-boot flash. One of the new and unique features of the MachXO4 RoT device is the Tamper Detection and Response. The Tamper Detection feature gives the MachXO4 RoT device the capability to monitor the configuration ports as well as memory access (Flash and SRAM). Using this feature, the MachXO4 RoT prevents any illegal device access.

Once Tamper Detection is enabled, the MachXO4 RoT monitors and informs you of any malicious activity on the configuration ports of the device. With this feature, you can detect a variety of threats from the configuration ports. These threats include any commands/instructions that are used to access a locked MachXO4 RoT device. The MachXO4 RoT device also classifies these attacks based on type and source.

2. Overview of Tamper Detection/Response

The Tamper Detection/Response feature works closely with user logic to indicate if there is any illegal device access. This illegal device access includes access using external configuration ports or access to locked flash sectors and SRAM. As shown in Figure 2.1, the Tamper Detection feature is enabled by configuring the Embedded Function Block (EFB) module to enable Tamper Detection/Response. Once enabled, this feature continuously monitors the activity on external configuration ports as well as memory access (Flash sector and SRAM). The EFB module is instantiated using the IP Catalog in the Lattice Radiant™ software. Refer to Enabling Tamper Detection Using Radiant Software section.

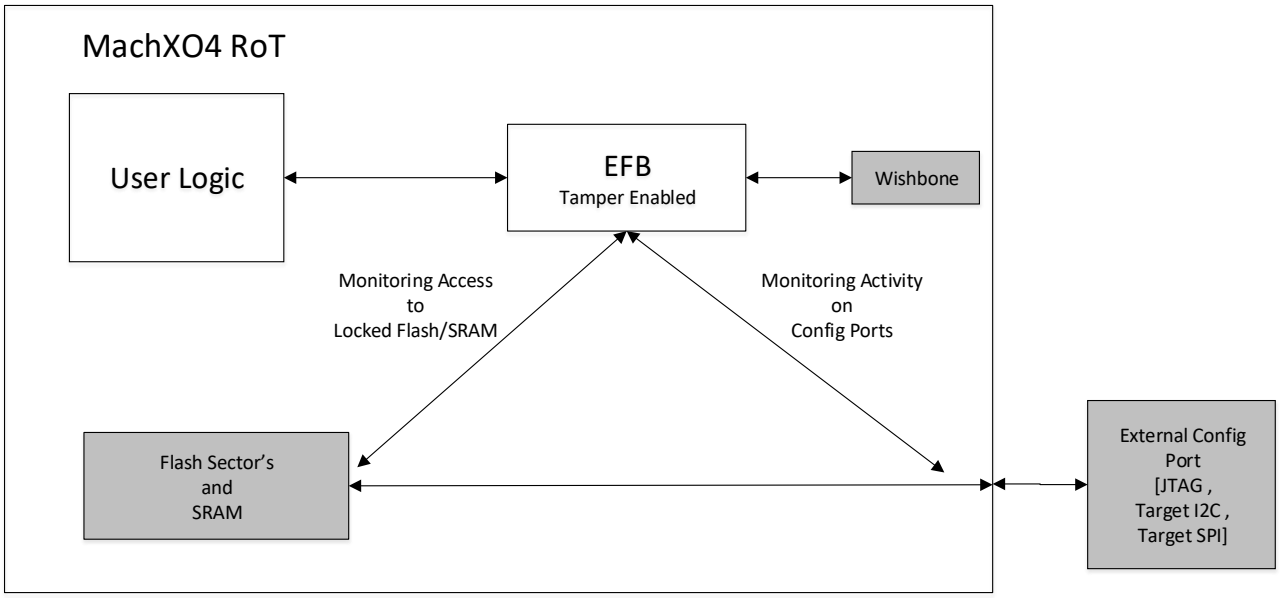

Figure 2.1. Tamper Detection Architecture in MachXO4 RoT Device Tamper Detection

This Tamper Detection feature in MachXO4 RoT devices not only identifies the tamper but also classifies the tamper based on the type of attack as well as the source of attack. This classification gives you the capability to take distinct action toward the attack and prevent any further device access.

2.1. Types of Tamper Detection

The MachXO4 RoT device not only detects the attack but also classifies the type of tamper based on the type of commands or instructions used to attack the device. These attacks are classified into three categories. You can enable or disable the type of attack using the Tamper Detection configuration options in the IP Catalog.

2.1.1. Password Tampering

Password Tampering refers to accessing a password-protected MachXO4 RoT device. In the Tamper Detection/Response user interface configuration, this tamper type is called Password Protection.

When the Password Protection feature is on, it informs you if an attacker is trying to access the device using an incorrect password or without entering the password if the device is password protected.

2.1.2. Memory (Flash/SRAM) Tampering

Memory Tampering refers to accessing a locked Flash sector or locked SRAM. In the Tamper Detection/Response user interface configuration, this tamper type is called Locked Flash/SRAM.

This type of tamper detects if you are accessing a locked Flash sector or locked SRAM. This tamper type informs you if an attacker is trying to issue any commands/instructions that are being used to access a locked MachXO4 RoT device.

2.1.3. Manufacturing Access Tampering

This type of tamper detects if you are trying to issue manufacturing mode commands. This tamper type is useful to identify tampering outside the usual norms. With this tamper type, some device features that are used for Lattice internal purposes are flagged if they are being used by the user.

2.2. Source of Tamper

The device can monitor and report which configuration interface is the source of tamper. The MachXO4 RoT device monitors the following configuration sources:

- Wishbone
- Target SPI
- Target I2C
- JTAG

2.3. Tamper Response

In response to a tamper event, you may choose to lock the configuration interfaces through user logic to prevent further tampering.

The Port Lock feature allows you to lock configuration ports. This Port Lock feature is useful after a tamper is detected on any configuration port. Refer to Tamper Detection User Configurable Options and the Tamper Detection/Response Timing section for more details on tamper configuration and response.

Once the *tamper_src_lock* signal is asserted, all monitored configuration ports are locked. Appropriate care should be exercised in determining which configuration ports to monitor, and when to lock those same MachXO4 RoT configuration ports.

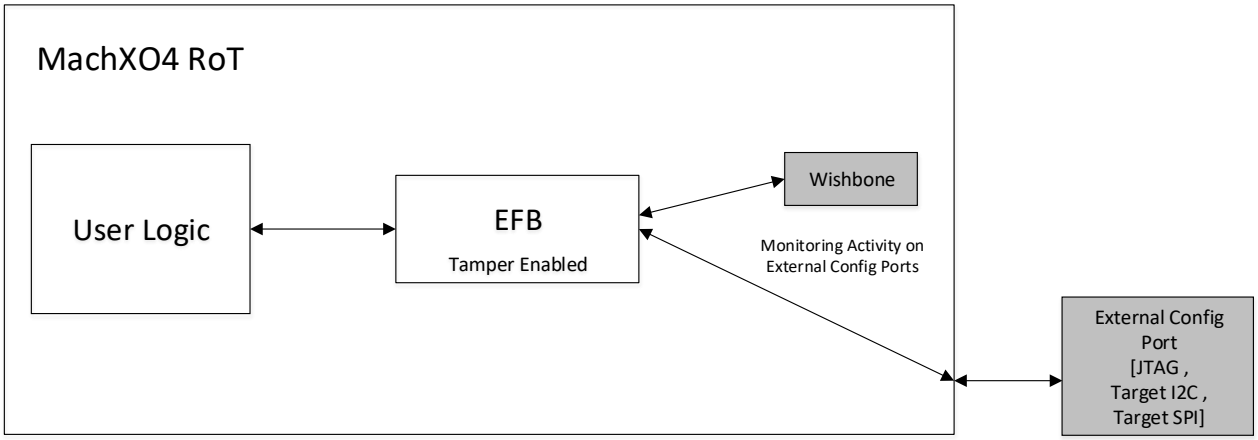

Figure 2.2. Tamper Response Block Diagram

3. Port Description of Tamper Detection/Response

Figure 3.1 shows the interface between user logic and the tamper section of the EFB module.

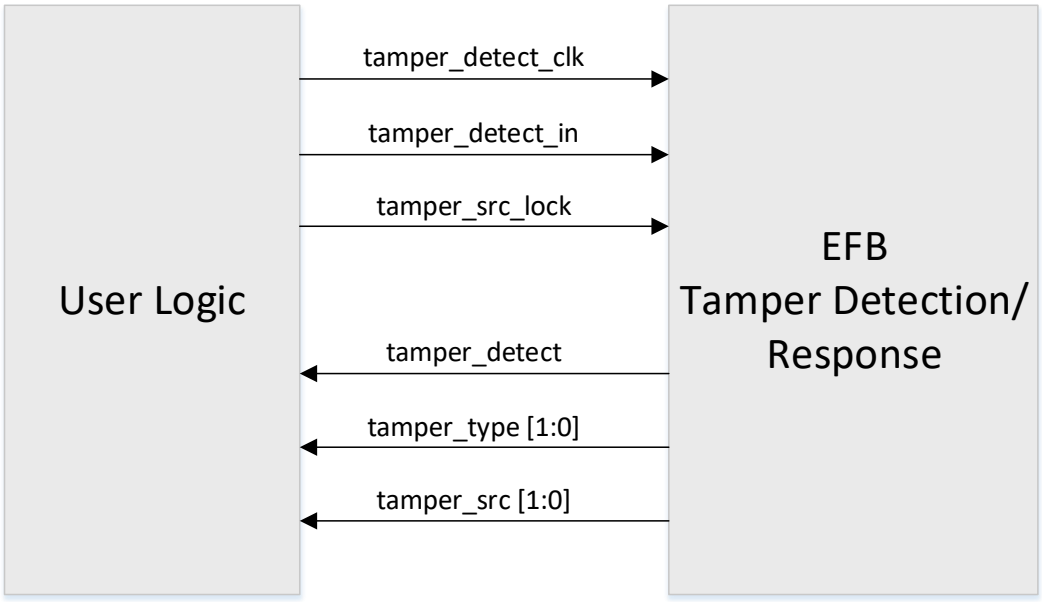

Figure 3.1. Tamper Detection Ports

Table 3.1. Ports for Tamper Detection/Response

Port Name	Input/Output	Default	Description
tamper_detect_clk	Input	—	Clock input to the Tamper Detection module.
tamper_detect_in	Input	—	Used to enable/disable Tamper Detection: 1 – Tamper Detection Enabled 0 – Tamper Detection Disabled
tamper_src_lock	Input	—	Used to lock all monitored configuration ports: 1 – Configuration Ports Locked 0 – Configuration Ports Unlocked
tamper_detect	Output	0	Used to indicate if tamper is detected on a monitored port: 1 – Tamper Detected 0 – Tamper Not Detected
tamper_type[1:0]	Output	00	Used to report the tamper type: 00 – Reserved 01 – Password Protection 10 – Locked Flash/SRAM 11 – Manufacture mode
tamper_src[1:0]	Output	00	Used to report the tamper source: 00 – Wishbone (WB) 01 – Target SPI (SSPI) 10 – Target I2C (SI2C) 11 – JTAG

3.1. Detailed Port Description

This section describes the ports of the Tamper Detection/Response module.

3.1.1. tamper_detect_clk

This signal provides the clock to the Tamper Detection module. The clock signal should be uninterrupted for this module to function at all times. All output signals are in this clock domain. Refer to the Tamper Detection/Response Timing section for the clock frequency requirements and detailed timing diagrams.

3.1.2. tamper_detect_in

This signal is used to enable/disable the Tamper Detection module. The user logic drives this signal high to enable the Tamper Detection module inside EFB. Once enabled, the Tamper Detection is active and continuously monitors the selected configuration ports and memory accesses:

- 1 – Tamper Detection Enabled
- 0 – Tamper Detection Disabled

Clearing (set to 0) the *tamper_detect_in* signal resets the tamper_detect output signal by pulling it low.

3.1.3. tamper_src_lock

This signal is used to lock configuration ports. Once tamper is detected, the user logic can choose to lock the configuration ports to prevent further device attack. To lock the pre-selected configuration ports, the user logic drives this signal high. Once the port is locked, any UFM, internal fabric, and device access, which includes reading, writing, and erasing, is blocked.

- 1 – Configuration ports locked
- 0 – Configuration ports unlocked

The configuration option *Port Lock* must be selected to enable the operation of *tamper_src_lock*. See Port Lock section for more details.

3.1.4. tamper_detect

This signal is used to indicate the detection of tamper. Once tamper is detected, the EFB module sends this signal to the user logic indicating Tamper Detection. Once the *tamper_detect* signal goes high, use the *tamper_detect_in* signal to reset the Tamper Detection logic. Refer to Tamper Clock Timing Specification section for the detailed timing diagram.

- 1 – Tamper Detected
- 0 – Tamper Not Detected

3.1.5. tamper_type[1:0]

This signal is used to report the type of tamper once tamper is detected. This signal gives you more information about the detected tamper as the EFB module classifies this tamper in the categories below.

Bits	Tamper Type
00	Reserved
01	Password Protection
10	Locked Flash/SRAM
11	Manufacture mode

3.1.6. tamper_src[1:0]

This signal is used to report the source of tamper once tamper is detected. This signal gives you information about the configuration interface that is used for the attack.

Bits	Tamper Source
00	Wishbone (WB)
01	Target SPI (SSPI)
10	Target I2C (SI2C)
11	JTAG

4. Enabling Tamper Detection Using Radiant Software

To enable the Tamper Detection feature in the MachXO4 RoT device, you must instantiate the EFB IP using the IP Catalog.

To enable this feature in the EFB IP, select the Tamper Detection/Response option in the IP Catalog as shown in Figure 4.1.

Note: The screenshots provided in this section are for reference only. Details may vary depending on the version of the IP or software being used. If there have been no significant changes to the GUI, a screenshot may reflect an earlier version of the IP.

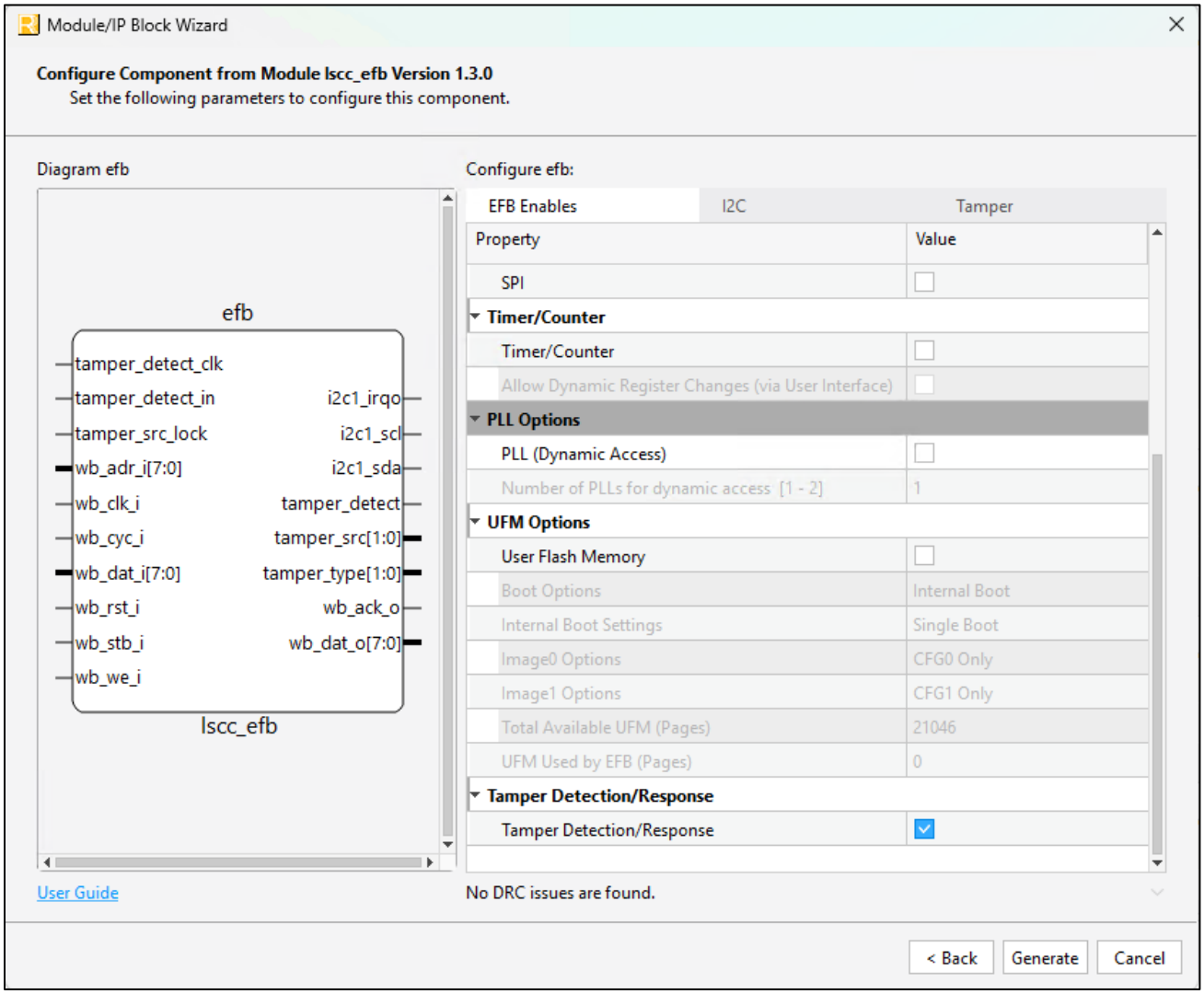

Figure 4.1. EFB Module with Tamper Detection/Response Enabled

4.1. Tamper Detection User Configurable Options

The Tamper Detection user interface gives you the option to select the type and source of tamper that needs monitoring. With this feature, you have the flexibility to enable or disable particular configuration ports based on their active usage.

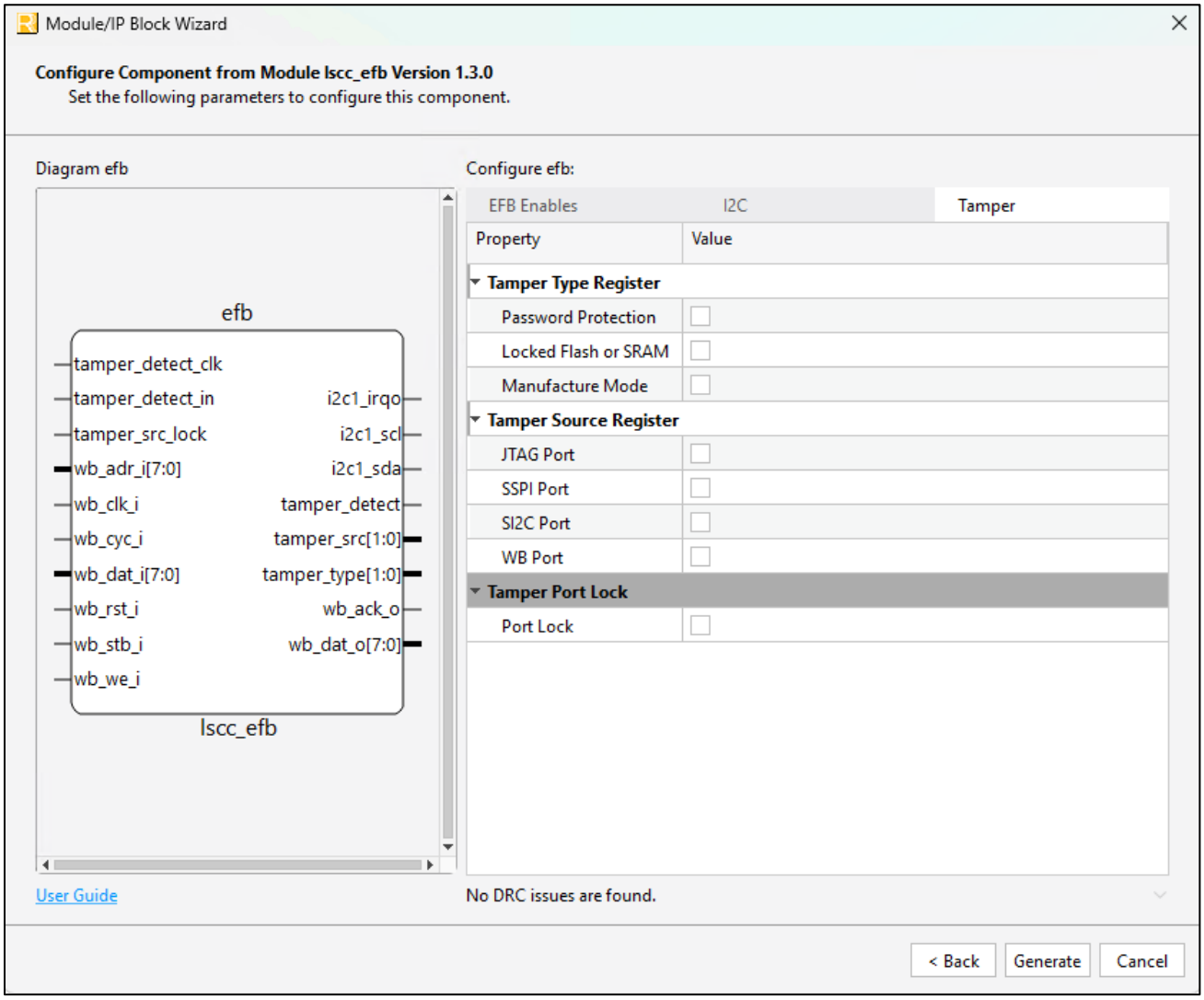

Figure 4.2. Tamper Configuration Options in EFB Module

4.1.1. Tamper Type Register

The Tamper Type Register is used to specify which types of Tamper Detection are active. There are three tamper types:

- Password Tampering – Password Protection
- Memory Tampering – Locked Flash or SRAM
- Manufacturing Access Tampering – Manufacture Mode

For more details on the tamper types, refer to the Types of Tamper Detection section.

4.1.2. Tamper Source Register

The Tamper Source Register is used to specify which ports are monitored. There are four tamper sources based on the ports used to interface with the MachXO4 RoT device:

- JTAG Port – Monitor JTAG configuration port

- SSPI Port – Monitor Target SPI configuration port
- SI2C Port – Monitor Target I2C configuration port
- WB Port – Monitor Wishbone configuration port

In Figure 4.2, for example, monitoring for malicious activity on JTAG and SI2C ports is enabled.

4.1.3. Port Lock

Checking *Port Lock* allows the *tamper_src_lock* input to lock the **Enabled Tamper Sources** when asserted. Unchecking *Port Lock* disables the *tamper_src_lock* input.

5. Tamper Detection/Response Timing

5.1. Tamper Clock Timing Specification

Table 5.1. Tamper Clock Timing Specification

Parameter	Min	Max	Units
tamper_detect_clk	0.00001	133*	MHz

***Note:** When running the clock at high speed, you must comply with the delay requirements of the Tamper Detection logic. Refer to Figure 5.2 for the detailed timing diagram.

5.2. Tamper Detection

The Tamper Detection logic runs on the *tamper_detect_clk* clock domain.

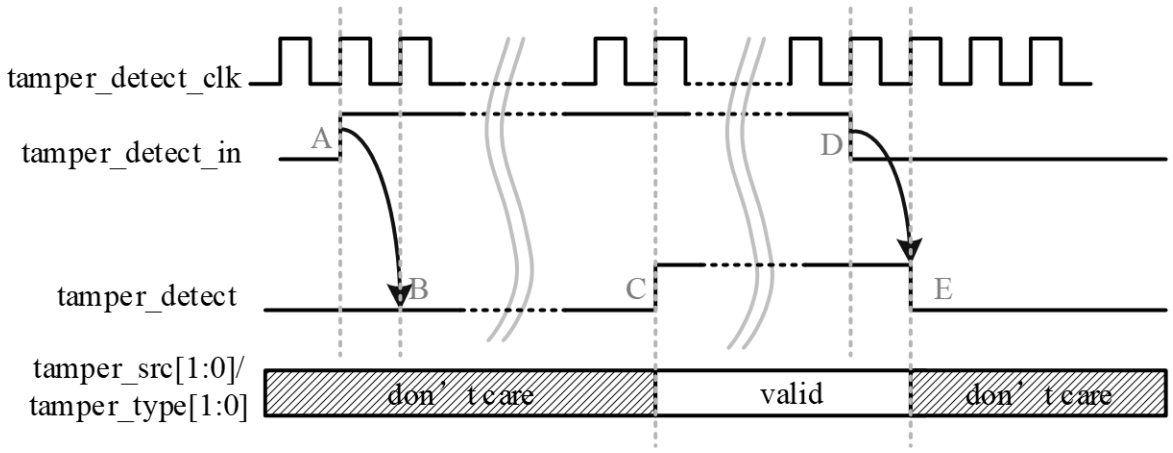

Figure 5.1. Tamper Detection Timing Diagram

5.2.1. Enable Tamper Detection

To enable the Tamper Detection, you must set the *tamper_detect_in* signal high (A).

The next rising edge of the *tamper_detect_clk* signal enables the detection logic (B), which enables the Tamper Detection.

5.2.2. Threat Detection

Once a threat is detected, the *tamper_detect* signal goes high (C).

Tamper Detection logic outputs the following information about the detected threat:

- *tamper_src* describes the source of the tamper
- *tamper_type* describes the tamper type

5.2.3. Reset Tamper Detection

To reset the Tamper Detection logic, pull the *tamper_detect_in* signal low (D).

On the next rising edge of the clock, the *tamper_detect* goes low and resets the Tamper Detection logic inside the EFB module (E).

Once the Tamper Detection module is reset, Tamper Detection is re-enabled by asserting *tamper_detect_in* signal high after a minimum of three *tamper_detect_clk* cycles.

5.3. Tamper Response

The tamper response logic also runs on the *tamper_detect_clk* clock domain.

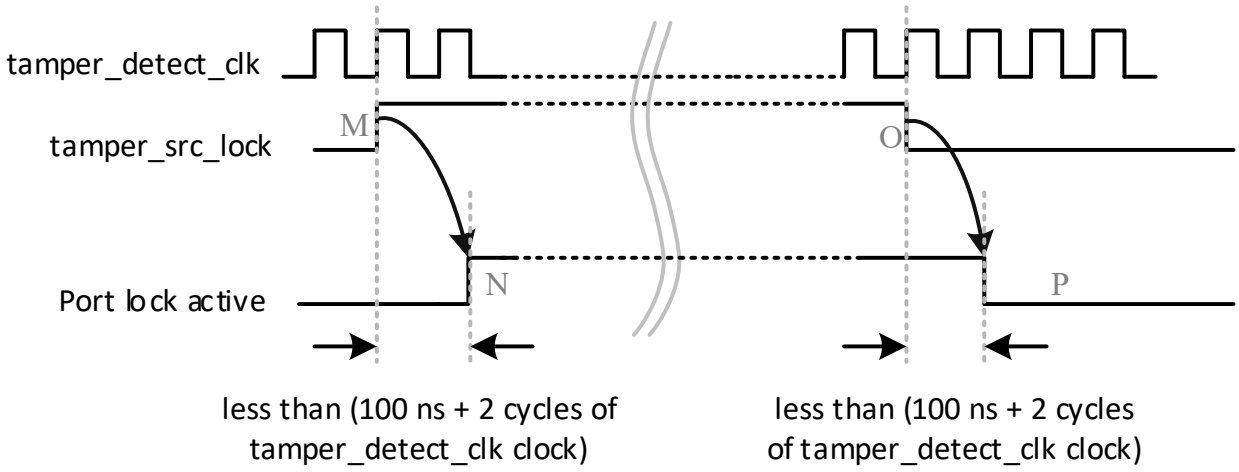

Figure 5.2. Tamper Response (Port Lock) Timing Diagram

5.3.1. Enable Port Lock

Once the threat is detected, you can choose to lock the pre-selected configuration ports to prevent any further attack on the device.

To enable the configuration port lock, enable the *tamper_src_lock* signal (M).

Once enabled, the configuration ports are locked after a certain delay (N) as shown in Figure 5.2.

5.3.2. Disable Port Lock

To unlock (re-enable) the configuration ports, drive the *tamper_src_lock* signal low (O).

Once this signal is driven low, the configuration ports are unlocked after a certain time delay (P).

References

- MachXO4 Family Root-of-Trust Devices Data Sheet (FPGA-DS-02126)
- MachXO4 web page
- Lattice Radiant FPGA design software
- Lattice Insights for Lattice Semiconductor training courses and learning plans

Technical Support Assistance

Submit a technical support case through www.latticesemi.com/techsupport. For frequently asked questions, refer to the Lattice Answer Database at www.latticesemi.com/Support/AnswerDatabase.

Revision History

Revision 1.0, September 2026

Section	Change Summary
All	Initial release.

www.latticesemi.com