Implementation of Security in Microsemi Antifuse FPGAs

Table of Contents

Introduction

Design security is a growing concern for system designers in today's highly competitive technology marketplace. When faced with the question of how to best protect valuable designs and critical intellectual property from theft, many designers turn to Microsemi® antifuse field programmable gate arrays (FPGAs). Microsemi nonvolatile antifuse FPGAs do not require a start-up bitstream, eliminating the possibility of configuration data being intercepted or copied. This ability to lock in the user's design also prevents in-system errors and accidental data erasures that otherwise may occur during download. In addition to the FuseLock™ advantage, Microsemi FPGAs also offer the inherent security of the architecture itself. The antifuses which form the interconnections within Microsemi FPGA are extremely small and densely distributed throughout the device (over 53 million on the largest Microsemi device). Furthermore, the fuses do not leave an observable signature that can be electrically probed or visually inspected. With these safeguards, Microsemi devices are virtually immune to copying and reverse engineering.

Fuse Technology on Microsemi Antifuse FPGAs

Depending upon the architecture selected, Microsemi antifuse FPGAs utilize a number of different fuse elements. Table 1 provides an overview of the different fuses used for each antifuse family.

Table 1 • **Fuse Types of Microsemi Antifuse FPGAs**

Fuse Types for all Microsemi Devices (Except ACT 1 and 40MX)	Fuse Types for ACT 1 and 40MX Devices
Array	Array
Security	Program
	Probe

Described below are the differences between these fuse types:

- Array Fuse: Used to build the metal-to-metal interconnect that creates nonvolatile, low power, high performance paths in Microsemi antifuse architecture
- Security Fuse: Used to prevent unauthorized probing of Microsemi FPGA. Also prevents further programming of the device
- Program Fuse: Prevents additional data from being programmed into the device (ACT 1 and 40MX only)
- Probe Fuse: Used to prevent probing of Microsemi FPGA (ACT 1 and 40MX only)

Securing Microsemi Antifuse FPGAs

In order to secure a Microsemi antifuse device from unwanted probing, it is necessary to program the internal security fuse. The security fuse can be set on any Microsemi device once the unit is programmed. This revolutionary ability to program the security fuse after programming array fuses allows the user to verify a design with the Debugger or Silicon Explorer diagnostic tool prior to permanently locking the device. Extended verification can continue through multiple design iterations, with the assurance that once a given design has been verified, Microsemi proprietary security fuses can be programmed to secure the device from further probing.

The ACT 1 and 40MX families contain two security fuses unique to their architecture: a Probe and a Program function. Programming the Probe fuse disables the probe circuitry, which also disables the use of the Debugger and Silicon Explorer diagnostic tools. This effectively prevents unauthorized users or potential attackers from compromising a design. In addition, programming the Program fuse prevents further programming of the device. This ensures devices are not inadvertently programmed twice or deliberately overwritten for malicious reasons. Figure 1, Figure 2 on page 3, Figure 3 on page 3, and Figure 4 on page 4 show how to use Microsemi Silicon Sculptor programming software to secure the Microsemi antifuse FPGAs. Figure 5 on page 4 and Figure 6 on page 4 show the same feature for the activator 2/2S programming software.

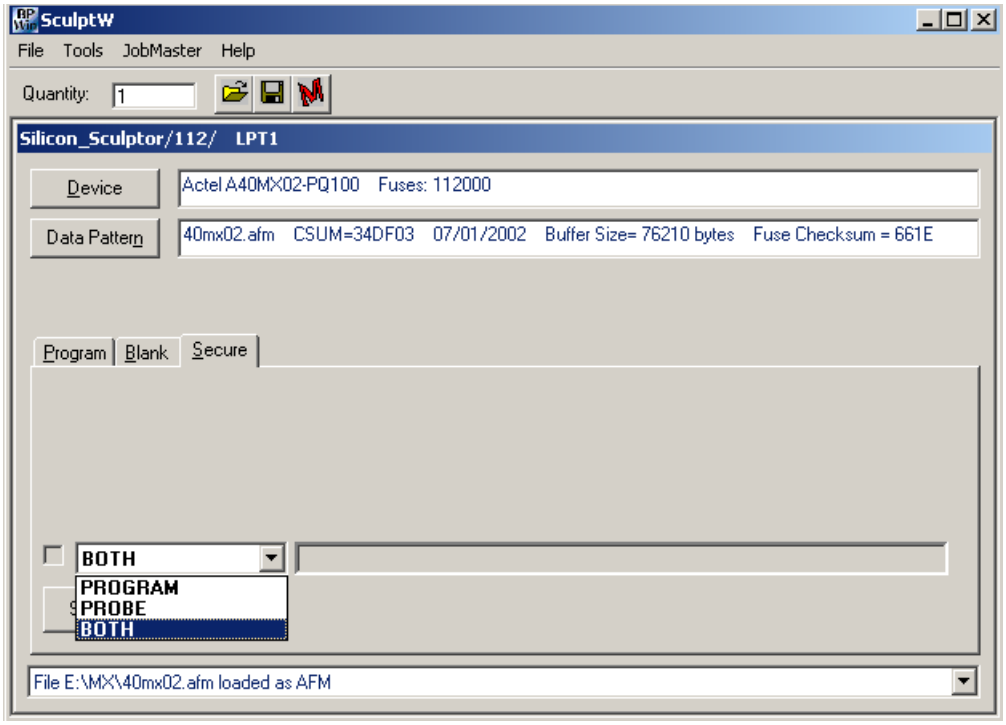

***Figure 1* • Programming Probe and Program Circuitry in Silicon Sculptor Software (Windows)**

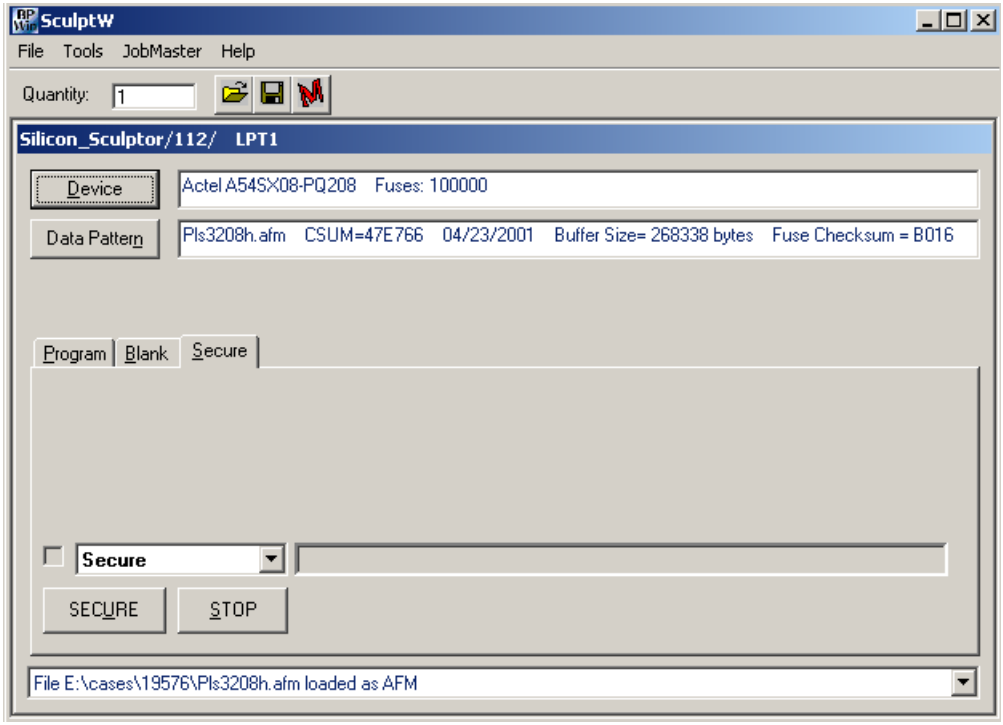

***Figure 2* • Programming Security Fuse in Silicon Sculptor Software (Windows)**

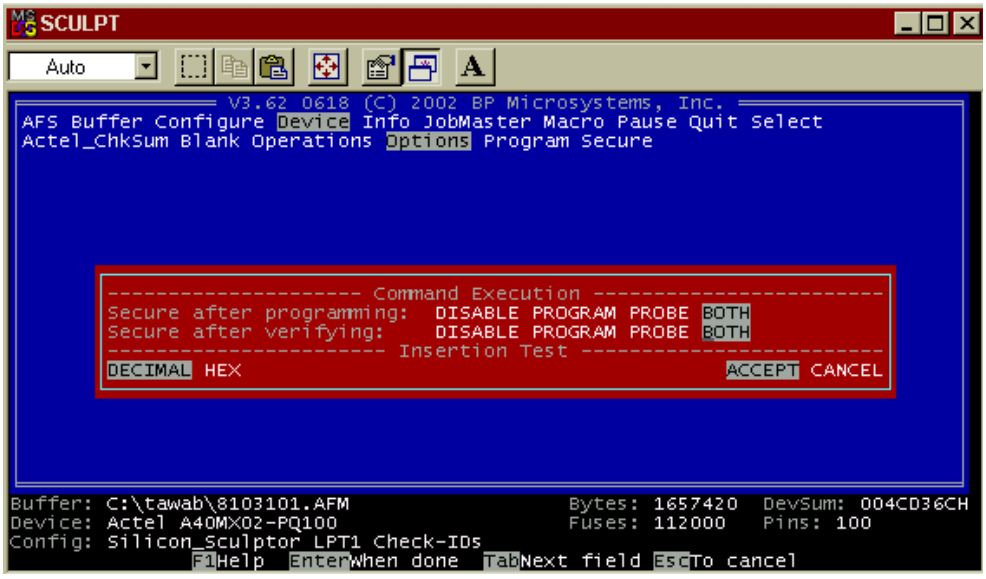

***Figure 3* • Programming Probe and Program Circuitry in Silicon Sculptor Software (Dos)**

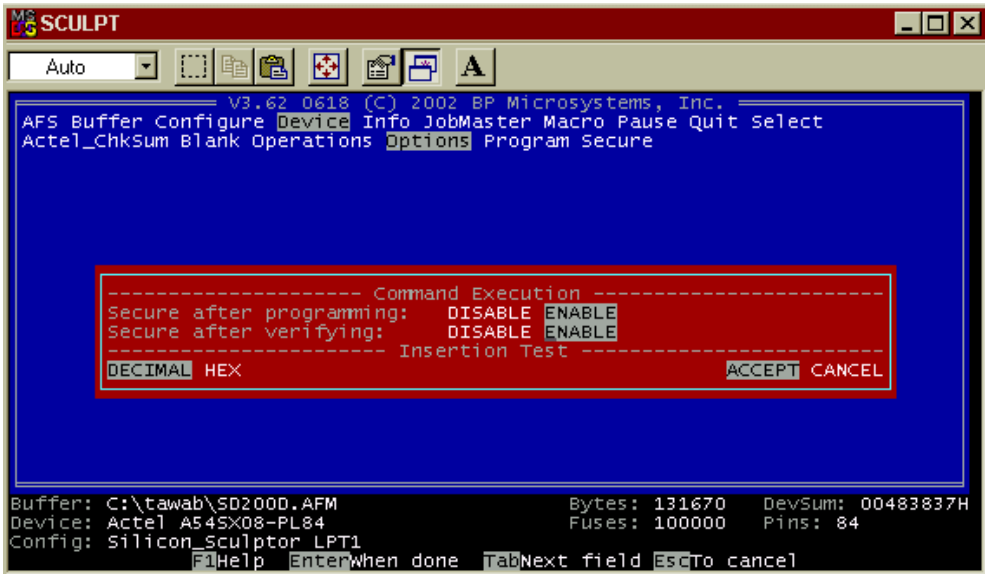

***Figure 4* • Programming Security Fuse in Silicon Sculptor Software (Dos)**

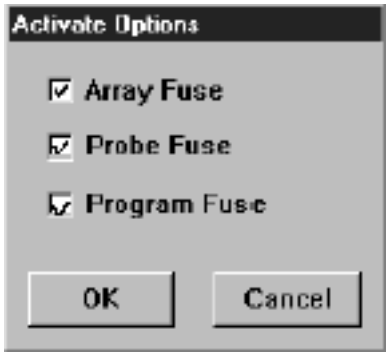

***Figure 5* • Activator Option to Program Probe and Program Fuses for ACT1 and 40MX FPGA**

***Figure 6* • Activator Option to Program Security Fuses for Other FPGAs**

Verifying the Status of the Security Fuse in Microsemi Antifuse FPGA

To verify the status of the security fuse in a Microsemi device, there are two unique flows depending upon the type of programmer and programming software used to program that device. The following description details the steps necessary to verify the state of the security fuse using both Silicon Sculptor with Sculptor software and Activator 2/2S with Windows programming software.

Silicon Sculptor and Sculptor Software

To verify the state of the security fuse using Silicon Sculptor, it is necessary to insert the programmed device in the appropriate Silicon Sculptor adapter module and to run the programming software. After selecting the device type, the correct Microsemi checksum test runs. The software returns a response similar to the one shown below identifying the state of the security fuse.

```
User ID: 0
Checksum: <device checksum>
The security fuse is programmed.
```

The line “The security fuse is programmed” will not be present if the security fuse is not programmed.

For ACT1 and 40MX devices, both the Program and Probe fuses should be programmed to enable security. When Microsemi checksum command is executed, the software responds with the following message:

```
User ID: 0
Checksum: <device checksum>
Both Probe and Program Fuses are programmed.
```

Activator 2/2S with Windows Programming Software

To check the status of the security fuse using Activator, a Blank check should be executed from the top line menu of the Windows Programming software. Table 2 describes the software feedback when the blank check is done.

Table 2 • **Software Response After Blank Check**

STATUS	SIGNATURE	CHECKSUM	SECURITY
Not blank	<silicon signature>	23F2	1*

Note: The “Security” heading indicates whether the security fuse is programmed (value =1) or not (value = 0).

Automatically Programming of the Security Fuse

To automatically program the security fuse, configure the .afm file in Microsemi antifuse devices using the Silicon Sculptor software. In order to program the security fuse as the default in Microsemi antifuse devices using the Silicon Sculptor software, the .afm file should be modified in the following way:

The header of the .afm file contains the following line:

```
|VAR PROGSECFUSE <NOT-SET>
```

This line should be replaced with:

```
|VAR PROGSECFUSE <S>
```

Conclusion

Microsemi has included security by design in all of our antifuse FPGAs. Designers can take advantage of Microsemi superior security with several easy steps using Microsemi Programmer and Programming software. These steps ensure a valuable design or critical intellectual property is best protected from unauthorized interference, possible corruption, or being illegally copied.

List of Changes

The following table lists critical changes that were made in the current version of the chapter.

Date	Changes	Page
Revision 1 (October 2012)	Added note in "Conclusion" section. (SAR 42214)	6

*Note: *The revision number is located in the part number after the hyphen. The part number is displayed at the bottom of the last page of the document. The digits following the slash indicate the month and year of publication.*

Microsemi Corporate Headquarters
One Enterprise, Aliso Viejo CA 92656 USA
Within the USA: +1 (949) 380-6100
Sales: +1 (949) 380-6136
Fax: +1 (949) 215-4996

Microsemi Corporation (NASDAQ: MSCC) offers a comprehensive portfolio of semiconductor solutions for: aerospace, defense and security; enterprise and communications; and industrial and alternative energy markets. Products include high-performance, high-reliability analog and RF devices, mixed signal and RF integrated circuits, customizable SoCs, FPGAs, and complete subsystems. Microsemi is headquartered in Aliso Viejo, Calif. Learn more at **www.microsemi.com**.

5192721-1/10.12