Programming ProASIC3/E Using a Microprocessor

Introduction

The ProASIC3/E families of Flash FPGAs offer enhanced performance, density, and features beyond those of the Actel ProASIC^{PLUS} family. The nonvolatile Flash technology gives the ProASIC3/E families the advantage of a secure, low-power, live-at-power-up, and single-chip solution. ProASIC3/E devices are reprogrammable and offer time-to-market benefits at an ASIC-level unit cost. These features enable engineers to create high-density systems using existing ASIC or FPGA design flows and tools.

Because the ProASIC3/E families are Flash-based, the configuration information is stored in on-chip Flash cells. Once programmed, the configuration data is an inherent part of the FPGA fabric and no external configuration data needs to be loaded at system power-up (unlike SRAM-based FPGAs). In addition, Flash-based ProASIC3/E FPGAs do not require system components, such as configuration serial nonvolatile memory (EEPROM) or a microcontroller and/or Flash memory to load the device configuration data at every system power-on. This reduces bill of materials costs, printed circuit board (PCB) area, and increases system reliability.

Programming Algorithm

JTAG Interface

The ProASIC3/E families are fully compliant with the IEEE1149.1 (JTAG) standard. They support all the mandatory boundary-scan instructions (EXTEST, SAMPLE/PRELOAD, and BYPASS) as well as six optional public instructions (USERCODE, IDCODE, HIGHZ, and CLAMP).

IEEE1532

The ProASIC3/E families are also fully compliant with the IEEE1532 programming standard. The IEEE1532 standard adds programming instructions and associated data registers to devices that comply with the IEEE1149.1 standard (JTAG). These instructions and registers extend the capabilities of the IEEE1149.1 standard such that the Test Access Port (TAP) may be used for configuration activities. The IEEE1532 standard greatly simplifies the programming algorithm, reducing the amount of time needed to implement microprocessor in-system programming (ISP).

Implementation Overview

To implement device programming with a microprocessor, the user should first download the C-based STAPL player or DirectC code from the Actel website. (See the Actel website for future updates regarding the STAPL player and DirectC code). Using the easy-to-follow Actel User's Guide, create the low-level Application Programming Interface (API) to provide the necessary basic functions. These API functions act as the interface between the programming software and the actual hardware (Figure 1 on page 2).

The API is then linked with the STAPL player or DirectC and compiled using the microprocessor's compiler. Once the entire code is compiled, the user must download the resulting binary into the MCU system's program memory (such as ROM, EEPROM, or Flash). The system is now ready for programming.

To program a design into the FPGA, the user creates a bitstream or STAPL file using the Actel Designer software, downloads it into the MCU system's volatile memory, and activates the stored programming binary file (Figure 2 on page 2). Once the programming is completed, the bitstream or STAPL file can be removed from the system as the configuration profile is stored in the Flash FPGA fabric and does not need to be reloaded at every system power-on.

© 2005 Actel Corporation

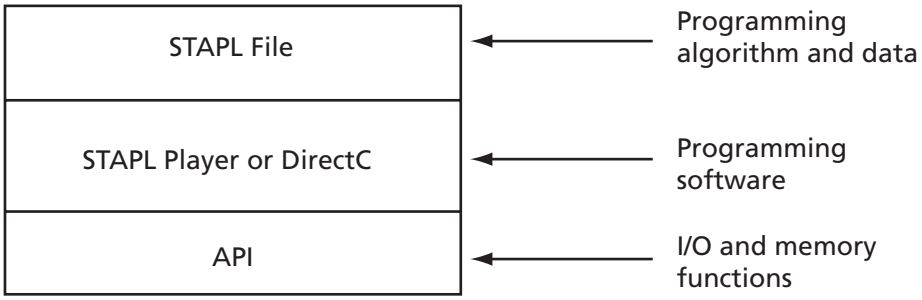

Figure 1 • **Device Programming Code Relationship**

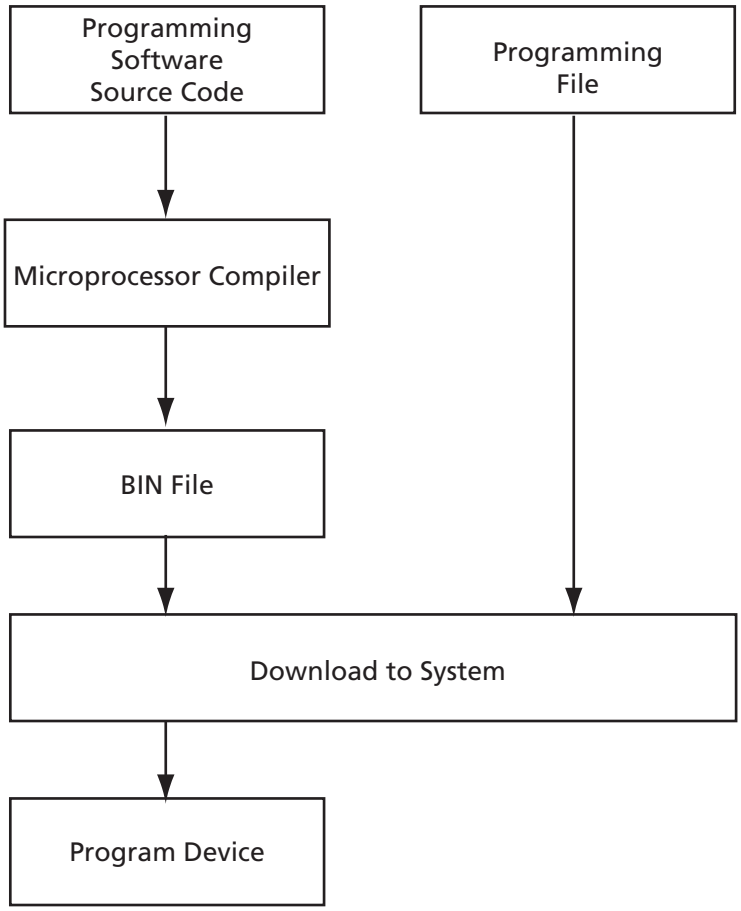

Figure 2 • **MCU FPGA Programming Model**

FlashROM (FROM)

Actel ProASIC3/E devices have 1 kbit of user-accessible, nonvolatile, FlashROM (FROM) on-chip. This nonvolatile FROM can be programmed along with the core or on its own, using the standard IEEE1532 JTAG programming interface.

The FROM is architected as eight pages of 128 bits. Each page can be individually programmed (erased and written). Additionally, on-chip AES security decryption can be used selectively to load data securely into the FROM (e.g., over public or private networks, such as the Internet). Refer to the *ProASIC3/E FlashROM (FROM)* for more information.

STAPL vs. DirectC

Programming the ProASIC3/E devices is performed using DirectC or STAPL. Both tools use the STAPL file as an input. DirectC is a compiled language, while STAPL is an interpreted language. Microprocessors will be able to load the DirectC much more quickly than STAPL. This speed advantage becomes more apparent when lower clock speeds of 8- or 16-bit microprocessors are used. DirectC also requires less memory than STAPL. STAPL does have one advantage over DirectC—the ability to upgrade. When a new programming algorithm is required, the STAPL user simply needs to regenerate a STAPL file using the latest version of the Designer software and download it to the system. The DirectC user must download the latest version of DirectC from Actel, compile everything, and download the result into the system (Figure 3).

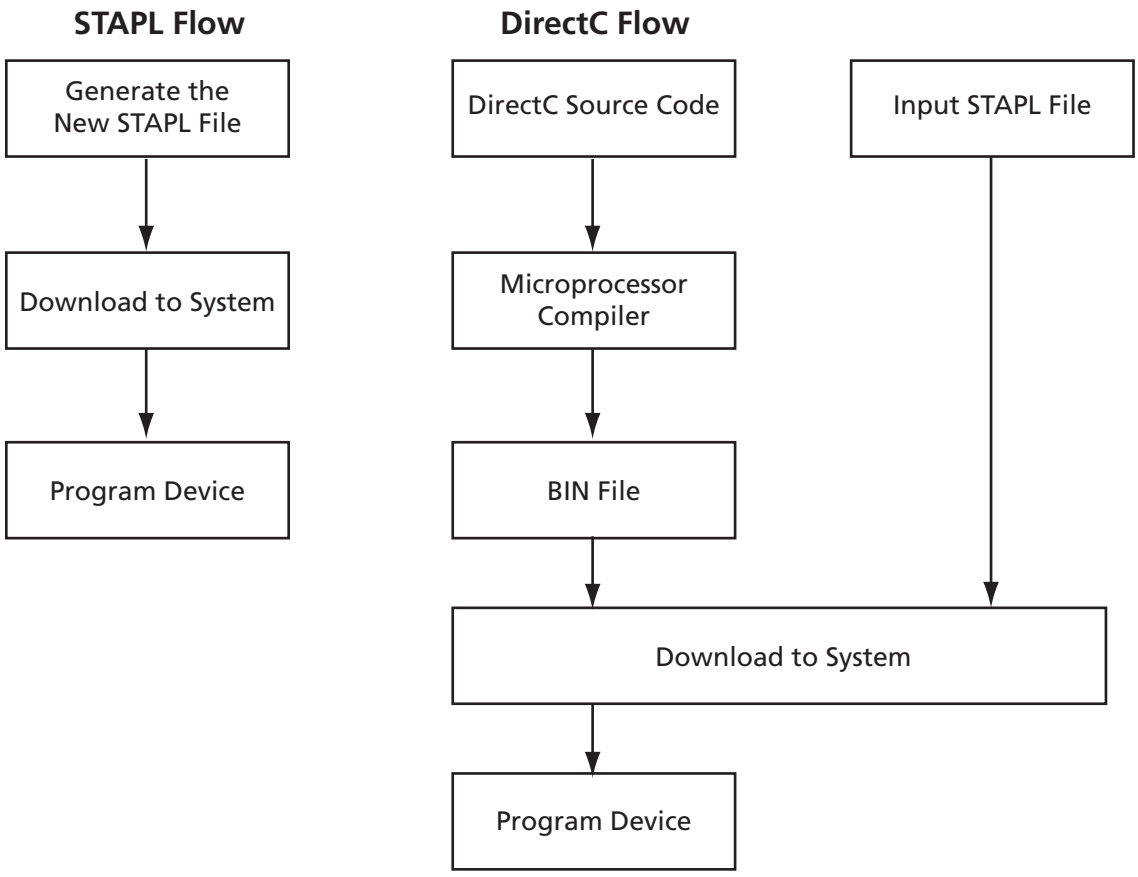

Figure 3 • **STAPL vs. DirectC**

Remote Upgrade via TCP/IP

Transmission Control Protocol (TCP) provides a reliable bitstream transfer service between two endpoints on a network. TCP depends on Internet Protocol (IP) to move packets around the network on its behalf. TCP protects against data loss, data corruption, packet reordering, and data duplication by adding checksums and sequence numbers to transmitted data and, on the receiving side, sending back packets and acknowledging the receipt of data.

The system containing the ProASIC3/E device FPGA can be assigned an IP address when deployed in the field. When the ProASIC3/E device requires an update (core or FROM), the programming instructions along with the new programming data (AES-encrypted cipher text) can be sent over the Internet to the target system via the TCP/IP protocol. Once the MCU receives the instruction and data, it can proceed with the FPGA update. ProASIC3/E devices support message authentication code (MAC), which can be used to validate data for the specific ProASIC3/E device. More details are given in the "Message Authentication Code (MAC) Validation/Authentication" section on page 5.

Hardware Requirement

To facilitate the programming of the ProASIC3/E families, the system must have a microprocessor (with access to the ProASIC3/E JTAG pins) to process the programming algorithm, memory to store the programming algorithm, programming data, and the necessary programming voltage (Table 1).

Table 1 • **Voltage Requirement**

Voltage Supply	Requirement	Description
V_{CC}	1.5V± 5%	Core voltage
V_{CCI}	1.5/1.8/2.5/3.3V ± 5%	I/O voltage
V_{JTAG}	1.5/1.8/2.5/3.3V ± 5%	JTAG voltage
V_{PUMP}*	3.3V ± 10% during programming 0-3.6V during normal operation	Charge pump voltage

Note: **V_{PUMP} must be 3.3V ± 10% during programming. During normal operation, this voltage can be left floating or be connected to up to 3.6V.*

Security

Read-Back Prevention

The ProASIC3/E devices are designed with security in mind. Even without any security measures (such as FlashLock with AES), it is not possible to read back the programming data from a programmed device. Upon programming completion, the programming algorithm will reload the programming data into the device. The device will then use built-in circuitry to determine if it was programmed correctly.

As an additional security measure, the ProASIC3/E devices are equipped with AES decryption. AES works in two steps. The first step is to program a key into the devices in a secure or trusted programming center (such as Actel in-house programming (IHP) center). The second step is to encrypt any programming files with the same encryption key. The encrypted programming file will only work with the devices that have the same key. The AES used in the ProASIC3/E families is the 128-bit AES decryption engine (Rijndael algorithm).

Message Authentication Code (MAC) Validation/Authentication

The ProASIC3/E families are equipped with a MAC validation/authentication system. MAC is an authentication tag, also called a checksum, derived by applying an on-chip authentication scheme to a STAPL file as it is loaded into the ProASIC3/E FPGA. MACs are computed and verified with the same key so that they can only be verified by the intended recipient. When the MCU system receives the AES encrypted programming data (cipher text), it can validate the data by loading it into the FPGA and performing a MAC verification prior to loading the data, via a second programming pass, into the FPGA core cells. This prevents erroneous or corrupt data from getting into the FPGA.

The ProASIC3/E families with AES and MAC are superior to devices with only DES or 3DES encryption. Because the MAC verifies the correctness of the data, the ProASIC3/E is protected from erroneous loading of invalid programming data that could damage a device (Figure 4).

The AES with MAC enables field updates over public networks without fear of having the design stolen. An encrypted programming file can only work on devices with the correct key, rendering any stolen files useless to the thief. To learn more about ProASIC3/E security features, please refer to the *ProASIC3E Security* application note.

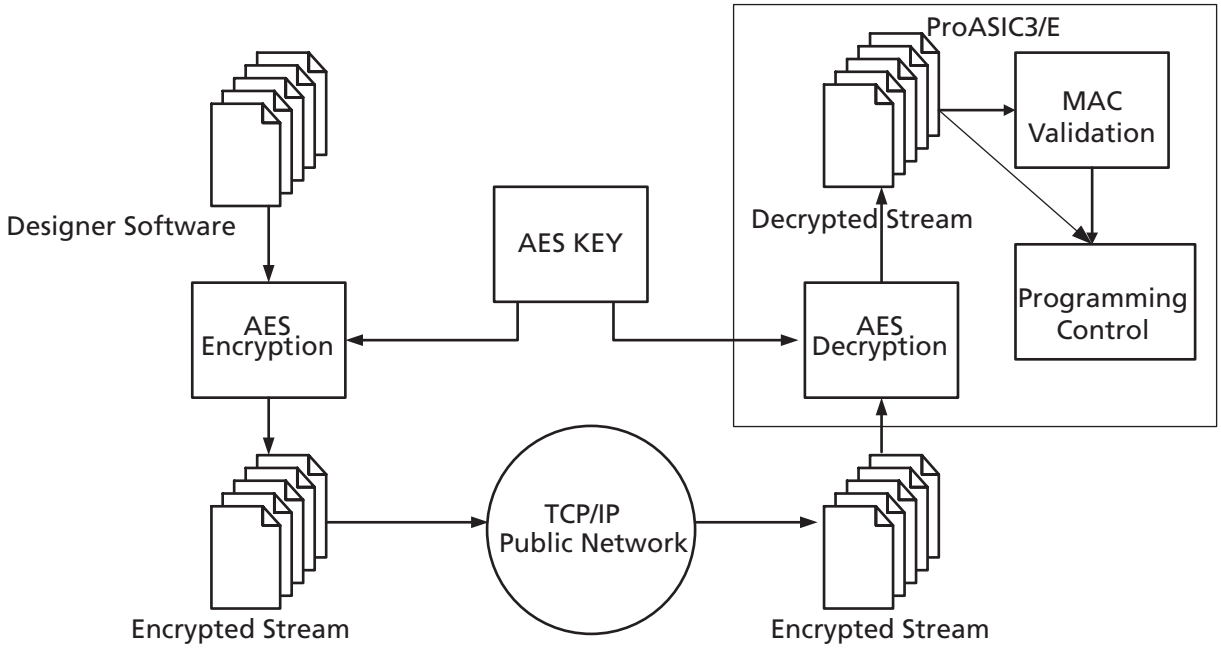

Figure 4 • **Encryption Flow**

Conclusion

The Actel ProASIC3/E families of Flash FPGAs are ideal for applications that require field upgrades. The single-chip ProASIC3/E solution saves board space by eliminating the need for EEPROM. The built-in AES with MAC enables transmission of programming data over any network without fear of design theft. ProASIC3/E is IEEE1532-compliant and supports STAPL, making the target programming software easy to implement.

Related Documents

Application Notes

ProASIC3/E FlashROM (FROM)
http://www.actel.com/documents/PA3_E_FROM_AN.pdf
ProASIC3/E Security
http://www.actel.com/documents/PA3_E_Security_AN.pdf

Actel and the Actel logo are registered trademarks of Actel Corporation.
All other trademarks are the property of their owners.

http://www.actel.com

Actel Corporation

2061 Stierlin Court
Mountain View, CA
94043-4655 USA
Phone 650.318.4200
Fax 650.318.4600

Actel Europe Ltd.

Dunlop House, Riverside Way
Camberley, Surrey GU15 3YL
United Kingdom
Phone +44 (0) 1276 401 450
Fax +44 (0) 1276 401 490

Actel Japan
www.jp.actel.com

EXOS Ebisu Bldg. 4F
1-24-14 Ebisu Shibuya-ku
Tokyo 150 Japan
Phone +81.03.3445.7671
Fax +81.03.3445.7668

Actel Hong Kong
www.actel.com.cn

Two Pacific Place
88 Queensway, Admiralty
Hong Kong
Phone +852.2185 6460
Fax +852.2185 6488

51900054-0/1.05