In-System Programming (ISP) in ProASIC3/E Using FlashPro3

Introduction

The ProASIC3/E Flash FPGA devices offer enhanced performance over the ProASIC PLUS® family. ProASIC3/E devices offer a single-chip, live-at-power-up solution with the ASIC advantages of security, low power, and low unit cost through nonvolatile Flash technology. ProASIC3/E devices are the first FPGAs with 1 kbit of on-chip, user-accessible, nonvolatile FlashROM (FROM). The FROM can be used in diverse system applications such as Internet Protocol (IP) addressing, user system preference storage, device serialization, or subscription-based business models. ProASIC3/E devices offer the best single-voltage in-system programming (ISP) solution, FlashLock™ security features, and AES-decryption-based ISP.

This application note describes the general requirements for programming a device and specific requirements for the FlashPro3 programmer.

Programming Voltage (V_{PUMP}) and V_{JTAG}

ProASIC3/E devices support on-chip programming of charge pumps, and only a single 3.3 V programming voltage is required for the V_{PUMP} pin during programming. When the device is not being programmed, the V_{PUMP} pin can be left floating or can be tied (pulled up) to any voltage between 0 V and 3.6 V. During programming, the target board or the FlashPro3 programmer can provide V_{PUMP}. FlashPro3 is capable of supplying V_{PUMP} to a single device. If more than one device is to be programmed using FlashPro3 on a given board, then FlashPro3 should not be relied on to supply the V_{PUMP} voltage.

ProASIC3/E device I/Os support a bank-based, voltage-supply architecture that simultaneously supports multiple I/O voltage standards (Table 1). By isolating the JTAG power supply in a separate bank from the user I/Os, ProASIC3/E devices provide greater flexibility with supply selection and simplify power supply and printed circuit board (PCB) design. The JTAG pins can be run at any voltage from 1.5 V to 3.3 V (nominal). Actel recommends that TCK be tied to GND or V_{JTAG} when not used. This prevents a possible totempole current on the input buffer stage. For TDI, TMS, and TRST pins, ProASIC3/E devices provide an internal nominal 10 kΩ pull-up resistor. During programming, all I/O pins, except for JTAG interface pins, are tristated and weakly pulled up to V_{CCI}. This isolates the part and prevents the signals from floating.

Table 1 • **Power Supplies**

Power Supply	Normal Operation	Programming Mode	Current During Programming
V_{CC}	1.5 V	1.5 V	< 70 mA
V_{CCI}	1.5 V / 1.8 V / 2.5 V / 3.3 V (Bank Selectable)	1.5 V / 1.8 V / 2.5 V / 3.3 V (Bank Selectable)	I/Os are weakly pulled up
V_{JTAG}	1.5 V / 1.8 V / V2.5 V / 3.3 V	1.5 V / 1.8 V / 2.5 V / 3.3 V	< 20 mA
V_{PUMP}	0 V to 3.3 V (nominal) or floating	3.0 V to 3.6 V	< 80 mA

IEEE1532 (JTAG) Interface

The supported industry-standard IEEE1532 programming interface builds on the IEEE1149.1 (JTAG) standard. IEEE1532 defines the standardized process and methodology for ISP. Both silicon and software issues are addressed in IEEE1532 to create a simplified ISP environment. Any IEEE1532-compliant programmer can be used to program ProASIC3/E devices. However, only limited security and FROM features are supported using the IEEE1532 standard. The Actel FlashPro3 programmer was developed exclusively for ProASIC3/E devices and will support all the security and device serialization features. Refer to the standard for detailed information about IEEE1532.

Security

Unlike SRAM-based FPGAs that require loading at power-up from an external source such as a microcontroller or boot PROM, Actel nonvolatile ProASIC3/E devices are live at power-up, and there is no bitstream required to load the device when power is applied. The unique Flash-based architecture prevents reverse engineering of the programmed code on the device, because the programmed data is stored in nonvolatile memory cells. Each nonvolatile memory cell is made up of small capacitors and any physical deconstruction of the device will disrupt stored electrical charges.

The ProASIC3/E device has a built-in 128-bit Advanced Encryption Standard (AES) decryption core, except for the A3P030 device. Any FPGA core or FROM content loaded into the device can optionally be sent as encrypted bitstream and decrypted as it is loaded. This is particularly suitable for applications where device updates must be transmitted over an unsecured network such as the Internet. The embedded AES decryption core can prevent sensitive data from being intercepted (Figure 1). A single 128-bit AES Key (32 HEX characters) is used to encrypt FPGA core programming data and/or FROM programming data in the Actel tools. The ProASIC3/E devices also decrypt with a single 128-bit AES Key. In addition, ProASIC3/E devices support a Message Authentication Code (MAC) for authentication of the encrypted bitstream on-chip. This allows the encrypted bitstream to be authenticated and prevents erroneous data from being programmed into the device. The ProASIC3/E FPGA core and FROM content of ProASIC3/E devices can be updated independently using a programming file which is AES-encrypted (cipher text) or uses plain text.

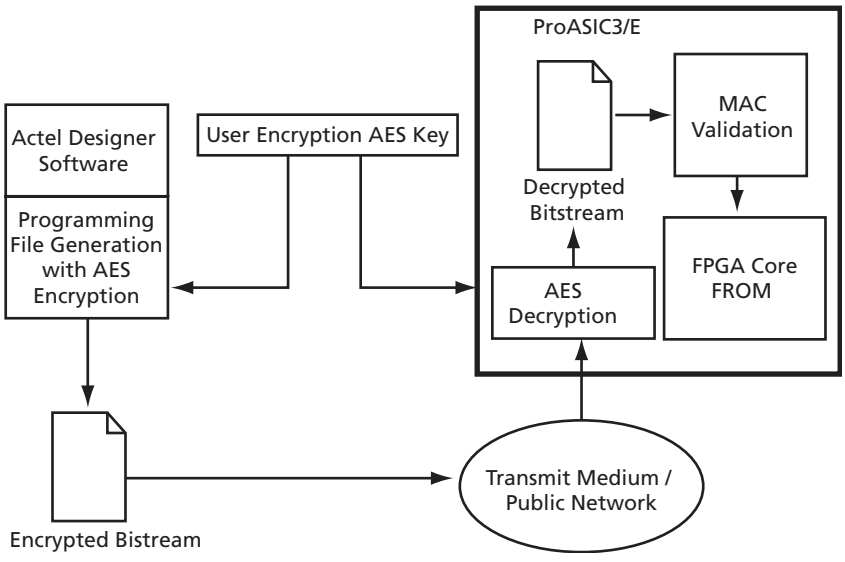

Figure 1 • **AES-128 Security Features in ProASIC3/E Devices**

Figure 2 shows different applications for ISP programming.

1. In a trusted programming environment, you can program the device using the unencrypted (plain text) programming file.
2. You can program the AES Key in a trusted programming environment and finish the final programming in an untrusted environment using the AES encrypted (cipher text) programming file.
3. For the remote ISP updating/reprogramming, the AES Key stored in the device enables the encrypted programming bitstream to be transmitted through the untrusted network connection.

Actel ProASIC3/E devices also provide the unique Actel FlashLock feature, which protects the Pass Key and AES Key. Unless the original FlashLock Pass Key is used to unlock the device, security settings cannot be modified. ProASIC3/E devices do not support read back of FPGA core-programmed data; however, the FROM contents can selectively be read back (or disabled) via the JTAG port based on the security settings established by the Actel Designer software. Refer to the *ProASIC3/E Security* application note for more information.

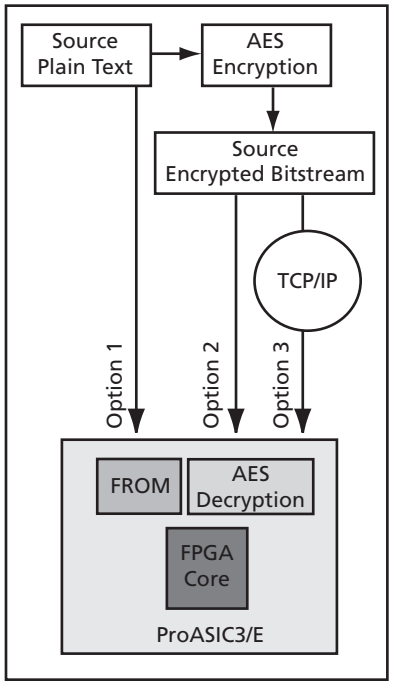

Figure 2 • **Different ISP Use Models**

FlashROM (FROM) and Programming Files

Each ProASIC3/E device has 1 kbit of on-chip, nonvolatile Flash memory that can be accessed from the FPGA core. This nonvolatile FROM is arranged in 8 pages of 128 bits (Figure 3). Each page can be programmed independently with or without 128-bit AES encryption. The FROM can only be programmed via the IEEE1532 JTAG port and cannot be programmed from the FPGA core. In addition, during programming of the FROM, the FPGA core is powered down automatically by the on-chip programming control logic.

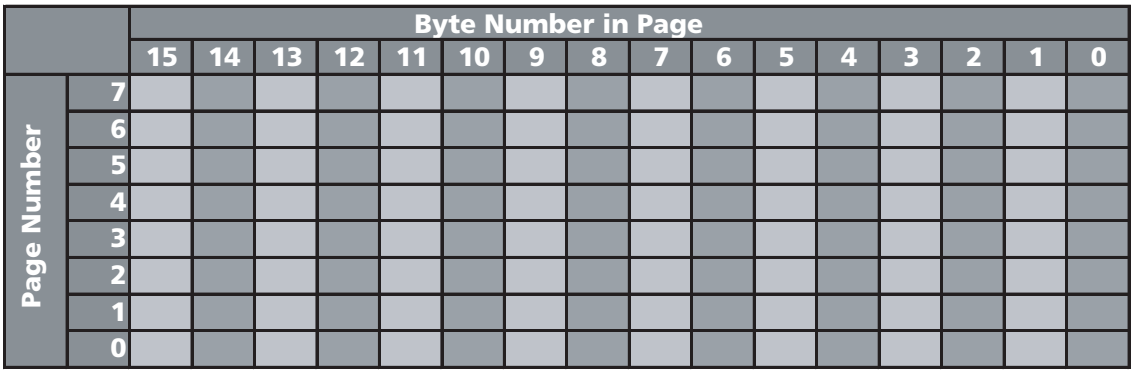

Figure 3 • **FROM Architecture**

Using FROM combined with AES, many subscription-based applications or device serialization applications are possible. ACTgen supports easy management of the FROM contents even over large numbers of devices. ACTgen can support FROM contents that contain the following:

- Static values
- Random numbers
- Values read from a file
- Independent updates of each page

In addition, auto-incrementing of fields is possible. In applications where the FROM content is different for each device, you have the option to generate a single STAPL file for all the devices or individual serialization files for each device. For more information on how to generate the FROM content for device serialization, refer to the *ProASIC3/E FlashROM (FROM)* application note.

Actel Libero® Integrated Designed Environment (IDE) software suite includes a unique tool to support the generation and management of FROM and FPGA programming files. This tool is called FlashPoint.

Depending on the applications, designers can use the FlashPoint software to generate a STAPL file with different contents. In each case, optional AES encryption and/or different security settings can be set.

In Designer, when you click on the Programming File icon, FlashPoint launches, and you can generate STAPL file(s) with four different cases (Figure 4 on page 5). When the serialization feature is used during the configuration of FROM in ACTgen, you can generate a single STAPL file that will program all the devices or an individual STAPL file for each device.

The following cases present the FPGA core and FROM programming file combinations that can be used for different applications. In each case, you can set the optional security settings (FlashLock Pass Key and/or AES Key) depending on the application.

1. A single STAPL file or multiple STAPL files with multiple FROM contents and the FPGA core content. A single STAPL file will be generated if the device serialization feature is not used. You can program the whole FROM or selectively program individual pages.
2. A single STAPL file for the FPGA core content
3. A single STAPL file or multiple STAPL files with multiple FROM contents. A single STAPL file will be generated if the device serialization feature is not used. You can program the whole FROM or selectively program individual pages.
4. A single STAPL file to configure the security settings for the device, such as the AES Key and/or Pass Key.

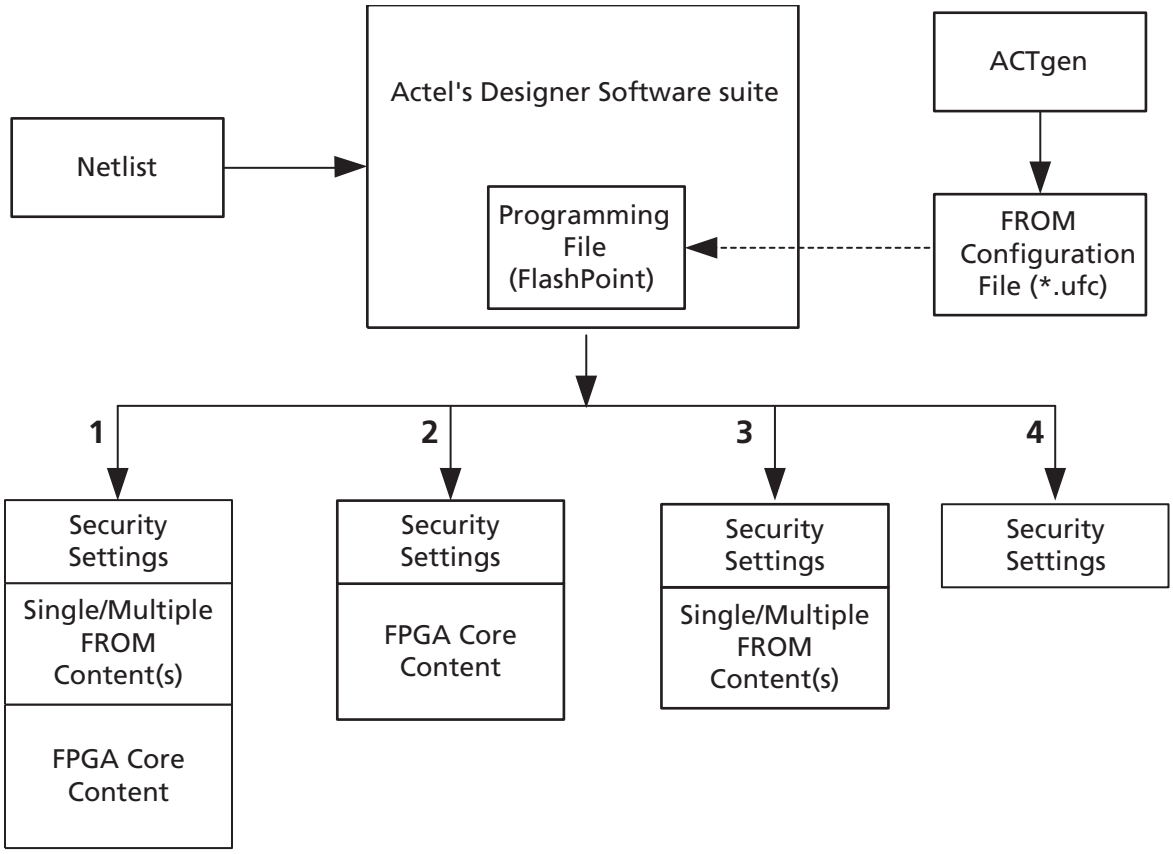

Figure 4 • **Flexible Programming File Generation for Different Applications**

Programming Solution

For device programming, any IEEE1532-compliant programmer can be used; however, the FlashPro3 programmer must be used to control the ProASIC3/E device's rich security features and FROM programming options. The FlashPro3 programmer is a low-cost portable programmer for the Actel ProASIC3/E families. It can also be used with a powered USB hub for parallel programming. General specifications for the FlashPro3 programmer are as follows:

- Programming Clock – TCK is used with a maximum frequency of 20 MHz and the default frequency is 4 MHz.
- Programming File – STAPL
- Daisy Chain – supported. You can use the ChainBuilder software to build the programming file for the chain.
- Parallel programming – supported. Multiple FlashPro3 programmers can be connected together using a powered USB hub or through the multiple USB ports on the PC.
- Power Supply – the target board must provide the V_{CC}, V_{CCI}, V_{PUMP}, and V_{JTAG} during programming. However, if there is only one ProASIC3/E device on the target board, the FlashPro3 can generate the required V_{PUMP} voltage from the USB port.

ISP Programming Header Information

The FlashPro3 programming cable connector can be connected with a 10-pin 0.1" pitch programming header. The recommended programming headers are manufactured by AMP (103310-1) and 3M (2510-6002UB). If you have limited board space, you can use a compact programming header manufactured by Samtec (FTSH-105-01-L-D-K). Using this compact programming header, you are required to order an additional header adapter manufactured by Actel (FP3-26PIN-ADAPTER).

Existing ProASIC^{PLUS} family customers, who are using Samtec Small Programming Header (FTSH-113-01-L-D-K) and are planning to migrate to ProASIC3/E devices, can order a separate adapter from Actel (FP3-26PIN-ADAPTER).

Table 2 • **Programming Header Ordering Code**

Manufacturer	Part Number	Description
AMP	103310-1	10-pin 0.1" pitch cable header (right angle PCB mount angle)
3M	2510-6002UB	10-pin 0.1" pitch cable header (straight PCB mount angle)
Samtec	FTSH-113-01-L-D-K	Small programming header supported by FlashPro and Silicon Sculptor
Samtec	FTSH-105-01-L-D-K	Compact programming header
Actel	FP3-26PIN-ADAPTER	Migration and compact header adapter

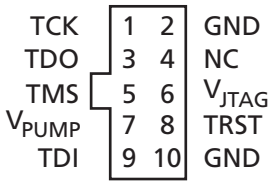

Figure 5 • **Programming Header (top view)**

Table 3 • **Programming Header Pin Numbers and Description**

Pin	Signal	Source	Description
1	TCK	Programmer	JTAG Clock
2	GND[1]	–	Signal Reference
3	TDO	Target Board	Test Data Output
4	NC	–	No Connect
5	TMS	Programmer	Test Mode Select
6	V_{JTAG}	Target Board	JTAG Supply Voltage
7	V_{PUMP}[2]	Programmer/Target Board	Programming Supply Voltage
8	nTRST	Programmer	JTAG Test Reset (Hi-Z with 10 kΩ pull-down, High, Low, or Toggling)
9	TDI	Programmer	Test Data Input
10	GND[1]	–	Signal Reference

Notes:

1. *Both GND pins must be connected.*
2. *FlashPro3 can provide V_{PUMP} if there is only one device on the target board.*

Board-Level Considerations

A bypass capacitor is required from V_{PUMP} to GND for all ProASIC3/E devices during programming. This bypass capacitor protects the ProASIC3/E devices from voltage spikes that may occur on the V_{PUMP} supplies during the erase and programming cycles. This bypass capacitor should have a voltage rating greater than 5.0 V with a minimum value of 0.1 µF. An example of this bypass capacitor would be a low-cost 16 V, 0.1 µF, ±10% surface-mount, multi-layer ceramic chip capacitor manufactured by BC Components (part number 0603B104K160BT). The bypass capacitor must be placed within 2.5 cm of the device pins.

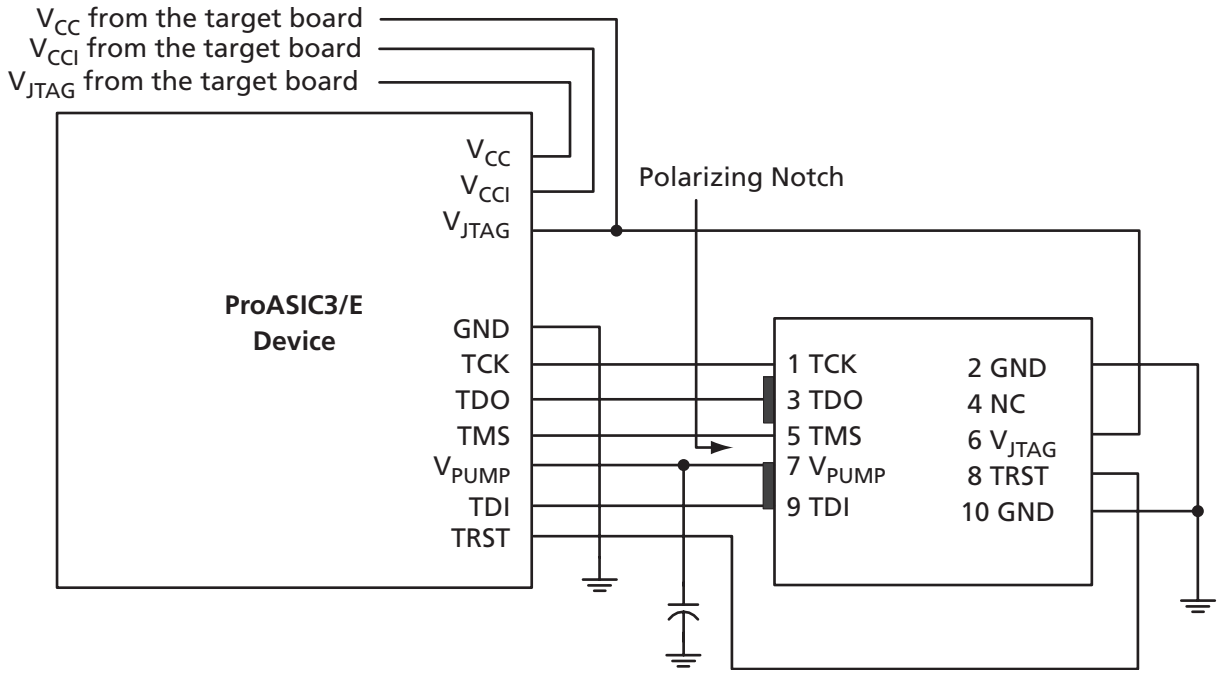

Figure 6 • **ProASIC3/E ISP Board Layout and Programming Header Top View**

Conclusion

ProASIC3/E devices offer a low-cost, single-chip solution that is live at power-up through nonvolatile Flash technology. The FlashLock Pass Key and 128-bit AES Key security features enable secure ISP programming in an untrusted environment. On-chip FROM enables a host of new applications, including device serialization, subscription-based applications, and IP addressing. Additionally, as the FROM is nonvolatile, all of these services can be provided without battery back-up. These advanced features are available in a single ProASIC3/E chip.

Related Documents

Application Notes

ProASIC3/E Security

http://www.actel.com/documents/PA3_E_Security_AN.pdf

ProASIC3/E FlashROM (FROM)

http://www.actel.com/documents/PA3_E_FROM_AN.pdf

User’s Guides

FlashPro User's Guide

http://www.actel.com/documents/flashproUG.pdf

Appendix – Troubleshooting

Signal Integrity

Symptoms of a Signal Integrity Problem

A signal integrity problem can manifest itself in many ways. The problem may show up as extra or dropped bits during serial communication, changing the meaning of the communication. There is a normal variation of threshold voltage and frequency response between parts even from the same lot. Because of this, the effects of signal integrity may not always affect different devices on the same board in the same way. Sometimes replacing a device appears to make signal integrity problems go away, but this is just masking the problem. Different parts on identical boards will exhibit the same problem sooner or later. It is important to fix signal integrity problems early. Unless the signal integrity problems are severe enough to completely block all communication between the device and the programmer, they may show up as subtle problems. Some of the FlashPro3 exit codes that are caused by signal integrity problems are listed below. Signal integrity problems are not the only possible cause of these errors, but this list is intended to show where problems can occur. FlashPro3 allows TCK to be lowered from 24 MHz down to 1 MHz to allow you to address some signal integrity problems that may occur with impedance mismatching at higher frequencies.

Chain Integrity Test Error or Analyze Chain Failure

Normally, the FlashPro3 Analyze Chain command expects to see 0x2 on the TDO pin. If the command reports reading 0x0 or 0x3, it is seeing the TDO pin stuck at 0 or 1. The only time the TDO pin comes out of tristate is when the JTAG TAP State Machine is in the Shift-IR or Shift-DR states. If noise or reflections on the TCK or TMS lines have disrupted the correct state transitions, the device's TAP State Controller might not be in one of these two states when the programmer tries to read the device. When this happens, the output is floating when it is read and does not match the expected data value. This can also be caused by a broken TDO net. Only a small amount of data is read from the device during the Analyze Chain command, so marginal problems may not always show up during this command.

Exit 11

This error occurs during the verify stage of programming a device. After programming the design into the ProASIC3/E device, the device is verified to ensure it is programmed correctly. The verification is done by shifting the programming data into the device. An internal comparison is performed within the device to verify that all switches are programmed correctly. Noise induced by poor signal integrity can disrupt the writes and reads or the verification process and produce a verification error. While technically a verification error, the root cause is often related to signal integrity.

Refer to the *FlashPro User's Guide* for other error messages and solutions. For the most up-to-date known issues and solutions, please refer to http://www.actel.com/support.

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

Suite 2114, Two Pacific Place
88 Queensway, Admiralty
Hong Kong
Phone +852 2185 6460
Fax +852 2185 6488

51900055-1/01.05