Rate This Document

# In-System Programming (ISP) of Actel's Low-Power Flash Devices Using FlashPro3

## Introduction

Actel's low-power flash devices are all in-system programmable. This document describes the general requirements for programming a device and specific requirements for the FlashPro3 programmer.

Fusion, IGLOO,® and ProASIC®3 devices offer a low-power, single-chip, live-at-power-up solution with the ASIC advantages of security and low unit cost through nonvolatile flash technology. Each device contains 1 kbit of on-chip, user-accessible, nonvolatile FlashROM. The FlashROM can be used in diverse system applications such as Internet Protocol (IP) addressing, user system preference storage, device serialization, or subscription-based business models. Fusion, IGLOO, and ProASIC3 devices offer the best in-system programming (ISP) solution, FlashLock® security features, and AES-decryption-based ISP.

## ISP Architecture

Low-power flash devices support ISP via JTAG and require a single $V_{PUMP}$ voltage of 3.3 V during programming. In addition, programming via a microcontroller in a target system is also supported.

Refer to *Microprocessor Programming of Actel's Low-Power Flash Devices*.

Family-specific support:

- Fusion, ProASIC3, and ProASIC3E devices support ISP.
- ProASIC3L devices operate using a 1.2 V core voltage and support ISP at 1.5 V only. Voltage switching is required in-system to switch from a 1.2 V core to 1.5 V core for programming.
- IGLOO and IGLOOe V5 devices can be programmed in-system when the device is using a 1.5 V supply voltage to the FPGA core.
- All IGLOO V2 and ProASIC3L devices can be operated at any voltage between 1.2 V and1.5 V. Designer software allows 50 mV increments in the voltage. Although devices can operate at 1.2 V core voltage, a device can only be reprogrammed when the core voltage is 1.5 V. Voltage switching is required in-system to switch from a 1.2 V supply ($V_{CC}$,$V_{CCI}$, and $V_{JTAG}$) to 1.5 V for programming.

IGLOO devices cannot be programmed in-system when the device is in Flash*Freeze mode. The device should exit Flash*Freeze mode and be in normal operation for programming to start. Programming operations in IGLOO devices can be achieved when the device is in normal operating mode and a 1.5 V core voltage is used.

### JTAG 1532

Fusion, IGLOO, and ProASIC3 devices support the JTAG-based IEEE 1532 standard for ISP. To start JTAG operations, the IGLOO device should exit Flash*Freeze mode and be in normal operation before starting to send JTAG commands to the device. As part of this support, when a device is in an unprogrammed state, all user I/O pins are disabled. This is achieved by keeping the global IO_EN signal deactivated, which also has the effect of disabling the input buffers. The SAMPLE/PRELOAD instruction captures the status of pads in parallel and shifts them out as new data is shifted in for loading into the Boundary Scan Register (BSR). When the device is in an unprogrammed state, the SAMPLE/PRELOAD instruction has no effect on I/O status; however, it will continue to shift in new data to be loaded into the BSR. Therefore, when SAMPLE/PRELOAD is used on an unprogrammed device, the BSR will be loaded with undefined data. For JTAG timing information on setup, hold, and fall times, refer to the *FlashPro User's Guide*.

# ISP Support in Flash-Based Devices

The flash FPGAs listed in Table 1 support the ISP feature and the functions described in this document.

***Table 1 •*** **Flash-Based FPGAs**

| Series | Family* | Description |
|---|---|---|
| IGLOO | IGLOO | Ultra-low-power 1.2 V to 1.5 V FPGAs with Flash*Freeze technology |
| | IGLOOe | Higher density IGLOO FPGAs with six PLLs and additional I/O standards |
| | IGLOO nano | The industry's lowest-power, smallest-size solution |
| | IGLOO PLUS | IGLOO FPGAs with enhanced I/O capabilities |
| ProASIC3 | ProASIC3 | Low-power, high-performance 1.5 V FPGAs |
| | ProASIC3E | Higher density ProASIC3 FPGAs with six PLLs and additional I/O standards |
| | ProASIC3 nano | Lowest-cost solution with enhanced I/O capabilities |
| | ProASIC3L | ProASIC3 FPGAs supporting 1.2 V to 1.5 V with Flash*Freeze technology |
| | RT ProASIC3 | Radiation-tolerant RT3PE600L and RT3PE3000L |
| | Military ProASIC3/EL | Military temperature A3PE600L, A3P1000, and A3PE3000L |
| | Automotive ProASIC3 | ProASIC3 FPGAs qualified for automotive applications |
| Fusion | Fusion | Mixed-signal FPGA integrating ProASIC3 FPGA fabric, programmable analog block, support for ARM® Cortex™-M1 soft processors, and flash memory into a monolithic device |

*Note: *The device names link to the appropriate datasheet, including product brief, DC and switching characteristics, and packaging information.*

## IGLOO Terminology

In documentation, the terms IGLOO series and IGLOO devices refer to all of the IGLOO devices as listed in Table 1. Where the information applies to only one product line or limited devices, these exclusions will be explicitly stated.

## ProASIC3 Terminology

In documentation, the terms ProASIC3 series and ProASIC3 devices refer to all of the ProASIC3 devices as listed in Table 1. Where the information applies to only one product line or limited devices, these exclusions will be explicitly stated.

To further understand the differences between the IGLOO and ProASIC3 devices, refer to the *Industry's Lowest Power FPGAs Portfolio*.

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

Low-power flash devices support on-chip charge pumps, and therefore require only a single 3.3 V programming voltage 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, FlashPro3 should not be relied on to supply the $V_{PUMP}$ voltage.

Low-power flash device I/Os support a bank-based, voltage-supply architecture that simultaneously supports multiple I/O voltage standards (Table 2 on page 3). By isolating the JTAG power supply in a separate bank from the user I/Os, low-power flash 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, the 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. The JTAG interface pins are driven by the FlashPro3 during programming, including the TRST pin, which is driven HIGH.

***Table 2 •*** **Power Supplies**

| Power Supply | Programming Mode | Current during Programming |
|---|---|---|
| $V_{CC}$ | 1.5 V | < 70 mA |
| $V_{CCI}$ | 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 / 2.5 V / 3.3 V | < 20 mA |
| $V_{PUMP}$ | 3.0 V to 3.6 V | < 80 mA |

*Note: All supply voltages should be at 1.5 V or higher, regardless of the setting during normal operation.*

# IEEE 1532 (JTAG) Interface

The supported industry-standard IEEE 1532 programming interface builds on the IEEE 1149.1 (JTAG) standard. IEEE 1532 defines the standardized process and methodology for ISP. Both silicon and software issues are addressed in IEEE 1532 to create a simplified ISP environment. Any IEEE 1532–compliant programmer can be used to program low-power flash devices. However, only limited security and FlashROM features are supported when using the IEEE 1532 standard. The Actel FlashPro3 programmer was developed exclusively for these devices and will support all the security and device serialization features. Refer to the standard for detailed information about IEEE 1532.

# Security

Unlike SRAM-based FPGAs that require loading at power-up from an external source such as a microcontroller or boot PROM, Actel nonvolatile 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.

Each low-power flash device has a built-in 128-bit Advanced Encryption Standard (AES) decryption core, except for the 30 k gate devices and smaller. Any FPGA core or FlashROM 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 on page 4). A single 128-bit AES Key (32 hex characters) is used to encrypt FPGA core programming data and/or FlashROM programming data in the Actel tools. The low-power flash devices also decrypt with a single 128-bit AES Key. In addition, low-power flash 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 FPGA core, FlashROM, and Flash Memory Blocks (FBs), in Fusion only, can be updated independently using a programming file that is AES-encrypted (cipher text) or uses plain text.

# Security in ARM-Enabled Low-Power Flash Devices

There are slight differences between the regular flash device and the ARM®-enabled flash devices, which have the M1 and M7 prefix.

The AES key is used by Actel and preprogrammed into the device to protect the ARM IP. As a result, the design will be encrypted along with the ARM IP, according to the details below.

## Cortex-M1 Device Security

Cortex-M1–enabled devices are shipped with the following security features:

- FPGA array enabled for AES-encrypted programming and verification
- FlashROM enabled for AES-encrypted write and verify
- Fusion Embedded Flash Memory enabled for AES encrypted write

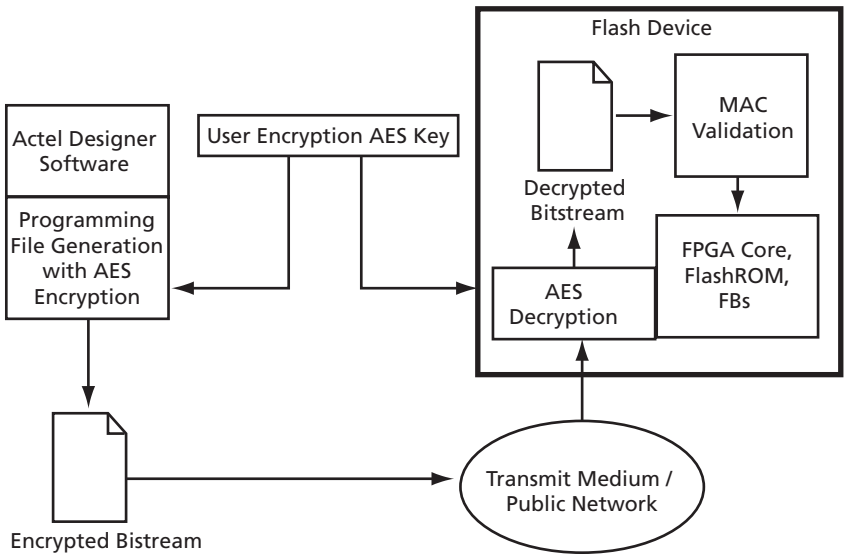


***Figure 1* • AES-128 Security Features**

Figure 2 shows different applications for ISP programming.

1. In a trusted programming environment, you can program the device using the unencrypted (plaintext) 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 low-power flash 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. Low-power flash devices do not support read-back of FPGA core-programmed data; however, the FlashROM 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 *Security in Low-Power Flash Devices* for more information.

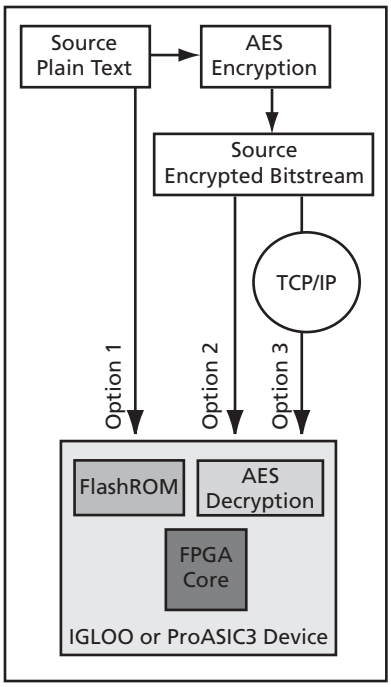


***Figure 2* • Different ISP Use Models**

# FlashROM and Programming Files

Each low-power flash device has 1 kbit of on-chip, nonvolatile flash memory that can be accessed from the FPGA core. This nonvolatile FlashROM is arranged in eight pages of 128 bits (Figure 3). Each page can be programmed independently, with or without the 128-bit AES encryption. The FlashROM can only be programmed via the IEEE 1532 JTAG port and cannot be programmed from the FPGA core. In addition, during programming of the FlashROM, the FPGA core is powered down automatically by the on-chip programming control logic.

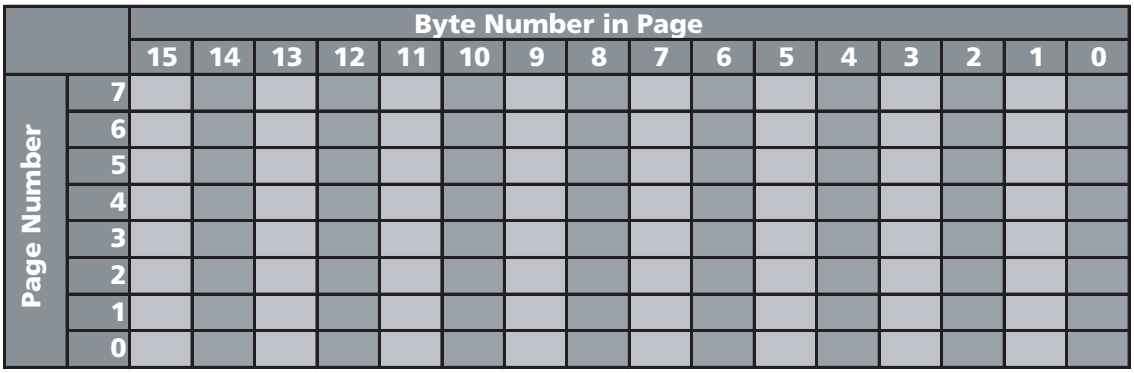


***Figure 3* • FlashROM Architecture**

Using FlashROM combined with AES, many subscription-based applications or device serialization applications are possible. SmartGen supports easy management of the FlashROM contents even over large numbers of devices. SmartGen can support FlashROM 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 FlashROM 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 FlashROM content for device serialization, refer to *FlashROM in Actel's Low-Power Flash Devices*.

Actel Libero® Integrated Designed Environment (IDE) includes a unique tool to support the generation and management of FlashROM 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 the Programming File icon, FlashPoint launches, and you can generate STAPL file(s) with four different cases (Figure 4 on page 7). When the serialization feature is used during the configuration of FlashROM in SmartGen, 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 FlashROM 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 FlashROM 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 FlashROM 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 FlashROM contents. A single STAPL file will be generated if the device serialization feature is not used. You can program the whole FlashROM 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.

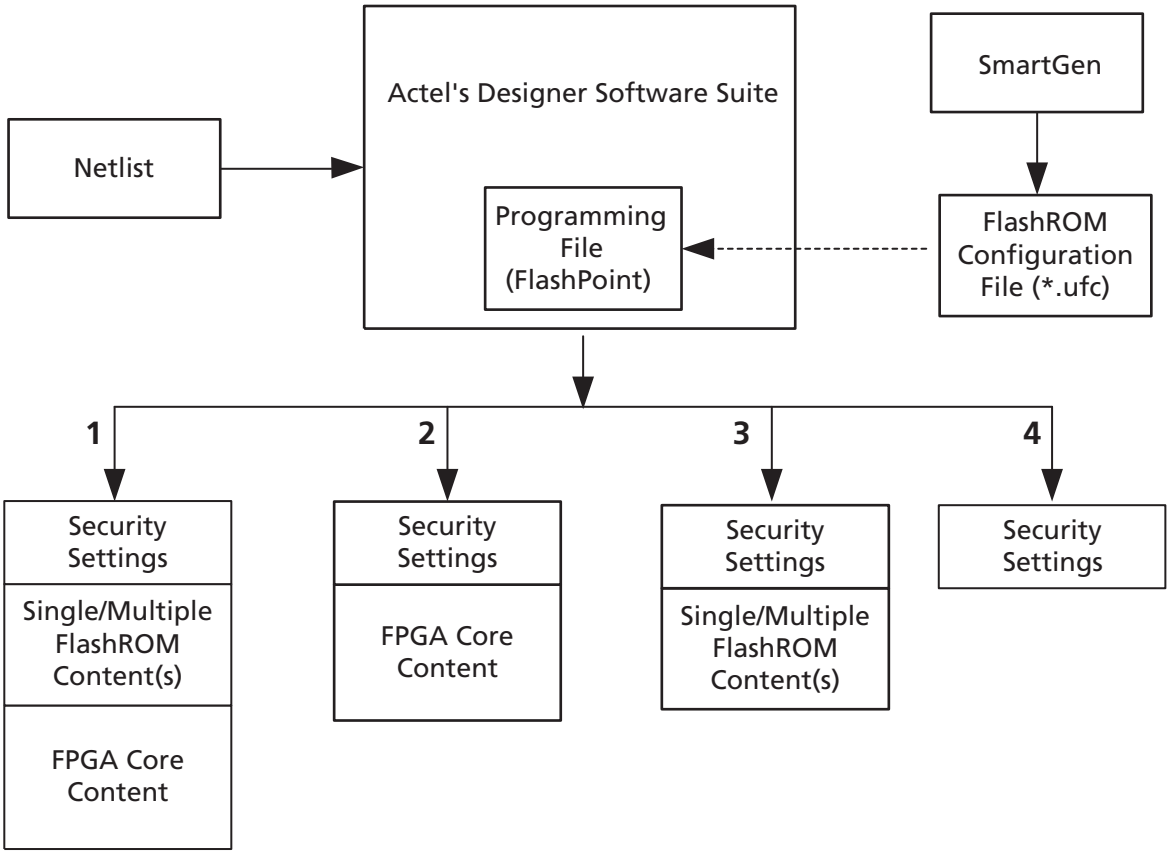


***Figure 4* • Flexible Programming File Generation for Different Applications**

# Programming Solution

For device programming, any IEEE 1532–compliant programmer can be used; however, the FlashPro3 programmer must be used to control the low-power flash device's rich security features and FlashROM programming options. The FlashPro3 programmer is a low-cost portable programmer for the Actel flash 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 $V_{CC}$, $V_{CCI}$, $V_{PUMP}$, and $V_{JTAG}$ during programming. However, if there is only one device on the target board, the FlashPro3 programmer 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 the Samtec Small Programming Header (FTSH-113-01-L-D-K) and are planning to migrate to IGLOO or ProASIC3 devices can order a separate adapter kit from Actel (FP3-10PIN-ADAPTER-KIT), which contains a compact 10-pin adapter kit as well as 26-pin migration capability.

***Table 3 •*** **Programming Header Ordering Codes**

| 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 |
| Samtec | FFSD-05-D-06.00-01-N | 10-pin cable with 50 mil pitch sockets; included in FP3-10PIN-ADAPTER-KIT. |
| Actel | FP3-10PIN-ADAPTER-KIT | Compact header and migration kit |

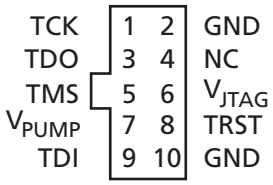


***Figure 5 •*** **Programming Header (top view)**

***Table 4 •*** **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 low-power flash devices during programming. This bypass capacitor protects the devices from voltage spikes that may occur on the $V_{PUMP}$ supplies during the erase and programming cycles. Refer to *Pin Descriptions* for specific recommendations. For proper programming, 0.01 µF and 0.33 µF capacitors (both rated at 16 V) are to be connected in parallel across $V_{PUMP}$ and GND, and positioned as close to the FPGA pins as possible. The bypass capacitor must be placed within 2.5 cm of the device pins.

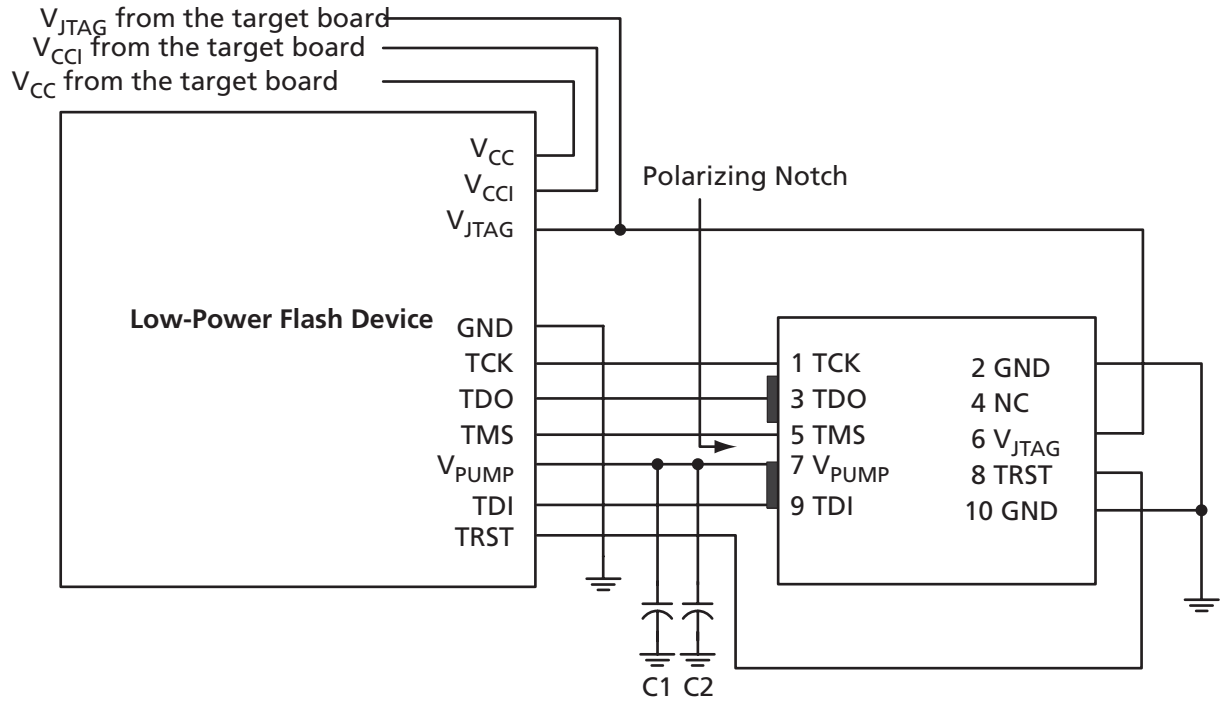


***Figure 6* • Board Layout and Programming Header Top View**

## 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 state. 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 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, refer to http://www.actel.com/support.

# Conclusion

Fusion, IGLOO, and ProASIC3 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 in an untrusted environment. On-chip FlashROM enables a host of new applications, including device serialization, subscription-based applications, and IP addressing. Additionally, as the FlashROM is nonvolatile, all of these services can be provided without battery backup.

# Related Documents

## Handbook Documents

*Microprocessor Programming of Actel's Low-Power Flash Devices*

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

*Security in Low-Power Flash Devices*

http://www.actel.com/LPD_Security_HBs.pdf

*FlashROM in Actel's Low-Power Flash Devices*

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

*Pin Descriptions*

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

## User's Guides

*FlashPro User's Guide*

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

# Part Number and Revision Date

This document was previously published as an application note describing features and functions of the device, and as such has now been incorporated into the device handbook format. No technical changes have been made to the content.

Part Number 51700094-015-5

Revised August 2009

# List of Changes

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

| Previous Version | Changes in Current Version (v1.5) | Page |
|---|---|---|
| v1.4 (December 2008) | The "CoreMP7 Device Security" section was removed from "Security in ARM-Enabled Low-Power Flash Devices", since M7-enabled devices are no longer supported. | 4 |
| v1.3 (October 2008) | The "ISP Architecture" section was revised to include information about core voltage for IGLOO V2 and ProASIC3L devices, as well as 50 mV increments allowable in Designer software. | 1 |
| | IGLOO nano and ProASIC3 nano devices were added to Table 1 · Flash-Based FPGAs. | 2 |
| | A second capacitor was added to Figure 6 · Board Layout and Programming Header Top View. | 9 |
| v1.2 (June 2008) | The "ISP Support in Flash-Based Devices" section was revised to include new families and make the information more concise. | 2 |
| v1.1 (March 2008) | The following changes were made to the family descriptions in Table 1 · Flash-Based FPGAs:<br>• ProASIC3L was updated to include 1.5 V.<br>• The number of PLLs for ProASIC3E was changed from five to six. | 2 |
| v1.0 (January 2008) | The "ISP Architecture" section was updated to included the IGLOO PLUS family in the discussion of family-specific support. The text, "When 1.2 V is used, the device can be reprogrammed in-system at 1.5 V only," was revised to state, "Although the device can operate at 1.2 V core voltage, the device can only be reprogrammed when all supplies ($V_{CC}$, $V_{CCI}$, and $V_{JTAG}$) are at 1.5 V." | 1 |
| | The "ISP Support in Flash-Based Devices" section and Table 1 · Flash-Based FPGAs were updated to include the IGLOO PLUS family. The "IGLOO Terminology" section and "ProASIC3 Terminology" section are new. | 2 |
| | The "Security" section was updated to mention that 15 k gate devices do not have a built-in 128-bit decryption core. | 3 |
| | Table 2 · Power Supplies was revised to remove the Normal Operation column and add a table note stating, "All supply voltages should be at 1.5 V or higher, regardless of the setting during normal operation." | 3 |
| | The "ISP Programming Header Information" section was revised to change FP3-26PIN-ADAPTER to FP3-10PIN-ADAPTER-KIT. Table 3 · Programming Header Ordering Codes was updated with the same change, as well as adding the part number FFSD-05-D-06.00-01-N, a 10-pin cable with 50-mil-pitch sockets. | 8 |
| | The "Board-Level Considerations" section was updated to describe connecting two capacitors in parallel across $V_{PUMP}$ and GND for proper programming. | 9 |

| Previous Version | Changes in Current Version (v1.5) | Page |
|---|---|---|
| 51900055-2/7.06 | Information was added to the "Programming Voltage (VPUMP) and VJTAG" section about the JTAG interface pin. | 3 |
| 51900055-1/1.05 | ACTgen was changed to SmartGen. | N/A |
| | In Figure 6 · Board Layout and Programming Header Top View, the order of the text was changed to:<br>$V_{JTAG}$ from the target board<br>$V_{CCI}$ from the target board<br>$V_{CC}$ from the target board | 9 |