Microsemi Corporation - M1A3P600L-1PQ208 Datasheet

Welcome to E-XFL.COM

Understanding Embedded - FPGAs (Field Programmable Gate Array)

Embedded - FPGAs, or Field Programmable Gate Arrays, are advanced integrated circuits that offer unparalleled flexibility and performance for digital systems. Unlike traditional fixed-function logic devices, FPGAs can be programmed and reprogrammed to execute a wide array of logical operations, enabling customized functionality tailored to specific applications. This reprogrammability allows developers to iterate designs quickly and implement complex functions without the need for custom hardware.

Applications of Embedded - FPGAs

The versatility of Embedded - FPGAs makes them indispensable in numerous fields. In telecommunications,

Details	
Product Status	Obsolete
Number of LABs/CLBs	-
Number of Logic Elements/Cells	-
Total RAM Bits	110592
Number of I/O	154
Number of Gates	600000
Voltage - Supply	1.14V ~ 1.575V
Mounting Type	Surface Mount
Operating Temperature	0°C ~ 85°C (TJ)
Package / Case	208-BFQFP
Supplier Device Package	208-PQFP (28x28)
Purchase URL	https://www.e-xfl.com/product-detail/microsemi/m1a3p600l-1pq208

Email: info@E-XFL.COM

Address: Room A, 16/F, Full Win Commercial Centre, 573 Nathan Road, Mongkok, Hong Kong

Using Sleep and Shutdown Modes in the System

Depending on the power supply and the components used in an application, there are many ways to power on or off the power supplies connected to the device. For example, Figure 2-6 shows how a microprocessor can be used to control a power FET. Microsemi recommends that power FETs with low resistance be used to perform the switching action.

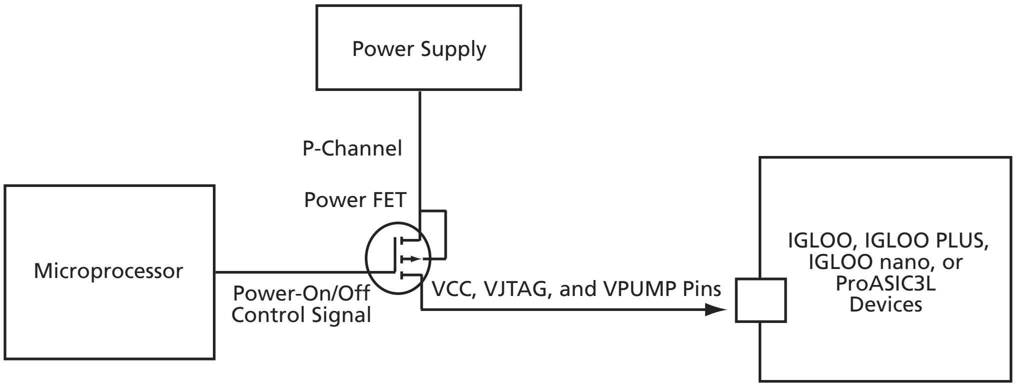

Figure 2-6 **• Controlling Power-On/-Off State Using Microprocessor and Power FET**

Figure 2-7 shows how a microprocessor can be used with a voltage regulator's shutdown pin to turn on or off the power supplies connected to the device.

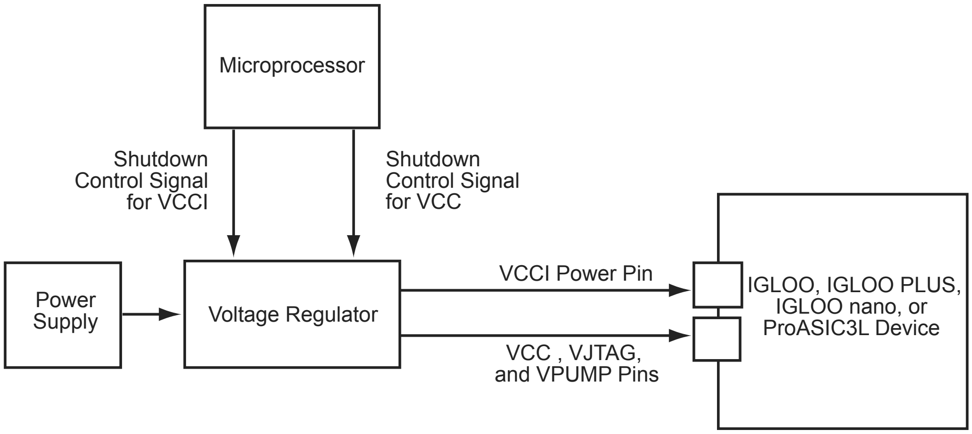

Figure 2-7 **• Controlling Power-On/-Off State Using Microprocessor and Voltage Regulator**

Power-Up/-Down Behavior

By design, all IGLOO, IGLOO nano, IGLOO PLUS, ProASIC3L, and RT ProASIC3 I/Os are in tristate mode before device power-up. The I/Os remain tristated until the last voltage supply (V_{CC} or V_{CCI}) is powered to its activation level. After the last supply reaches its functional level, the outputs exit the tristate mode and drive the logic at the input of the output buffer. The behavior of user I/Os is independent of the V_{CC} and V_{CCI} sequence or the state of other voltage supplies of the FPGA (V_{PUMP} and V_{JTAG}). During power-down, device I/Os become tristated once the first power supply (V_{CC} or V_{CCI}) drops below its deactivation voltage level. The I/O behavior during power-down is also independent of voltage supply sequencing.

Figure 2-8 on page 34 shows a timing diagram when the V_{CC} power supply crosses the activation and deactivation trip points in a typical application when the V_{CC} power supply ramp-rate is 100 µs (ramping from 0 V to 1.5 V in this example). This is the timing diagram for the FPGA entering and exiting Sleep mode, as this function is dependent on powering V_{CC} down or up. Depending on the ramp-rate of the

Clock Gating Block

Once DONE_HOUSEKEEPING is detected, the FSM will initiate the clock gating circuit by asserting ASSERT_GATE (active Low). ASSERT_GATE is named control_user_clock_net in the IP block. Upon assertion of the ASSERT_GATE signal, the clock will be gated in less than two cycles. The clock gating circuit is comprised of a flip-flop, latch, AND gate, and CLKINT, as shown in Figure 2-12. The clock gating block can support gating of up to 17 clocks.

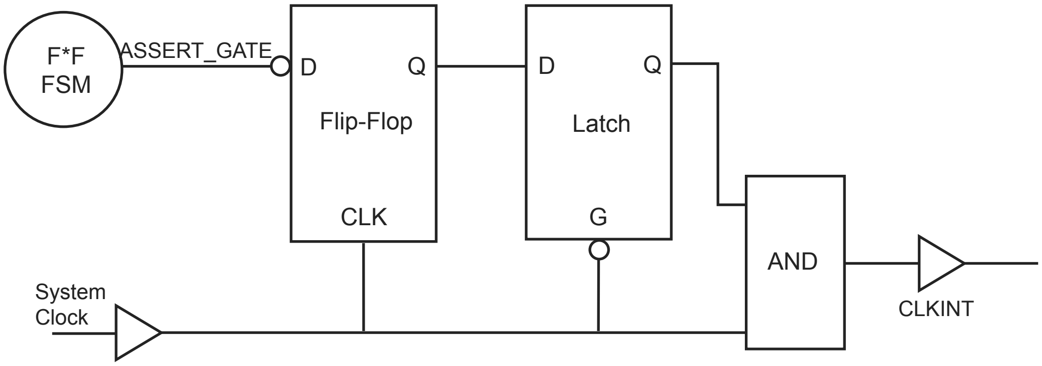

Figure 2-12 **• Clock Gating Circuit**

After initiating the clock gating circuit, the FSM will assert and hold the LSICC signal (active High), feeding the ULSICC macro. This will initiate the 1 µs entrance into Flash*Freeze mode.

Upon deassertion of the Flash*Freeze pin, the FSM will set ASSERT_GATE High. Once the I/O banks become active, the clock will enter the device and register the ASSERT_GATE signal, cleanly releasing the clock gate.

Design Flow[1]

Microsemi has developed a convenient and intuitive design flow for configuring and integrating Flash*Freeze technology into an FPGA design. Flash*Freeze type 1 is implemented by instantiating the INBUF_FF macro in the top level of a design. Flash*Freeze type 2 with management IP can be generated by the Libero core generator or SmartGen and instantiated as a single block in the user's design. This single block will include an INBUF_FF macro and the optional Flash*Freeze management IP, which includes the ULSICC macro. If designers do not wish to use this core generator, the INBUF_FF macro and the optional ULSICC macro may be instantiated in the design, and custom Flash*Freeze management IP can be developed by the user. The remainder of this section will cover configuration details of the INBUF_FF macro, the ULSICC macro, and the Flash*Freeze management IP.

Additional information on the tools discussed within this section may be found in the Libero online help.

INBUF_FF

The INBUF_FF macro is a special-purpose input buffer macro that is interpreted downstream in the design flow by Microsemi's Designer software. When this macro is used, the top-level port will be forced to the dedicated FF pin in the FPGA, and Flash*Freeze mode will be available for use in the device. The following are the design rules for INBUF_FF:

- If INBUF_FF is not used in the design, the device will not be configured to support Flash*Freeze mode.
- When the INBUF_FF macro is used, the FF pin will establish a hardwired connection to the Flash*Freeze technology circuit in the device, as shown in Figure 2-1 on page 25, Figure 2-3 on page 27, and Figure 2-10 on page 37, and described in the "Flash*Freeze Type 1: Control by Dedicated Flash*Freeze Pin" section on page 24.

---

[1] *This section applies to Libero / Designer software v8.3 and later. Microsemi recommends that designs created in earlier versions of the software be modified to accommodate this flow by instantiating the INBUF_FF macro or the Flash*Freeze management IP. Refer to the Libero / Designer software v8.3 release notes and the Libero online help for more information on migrating designs from older software versions.*

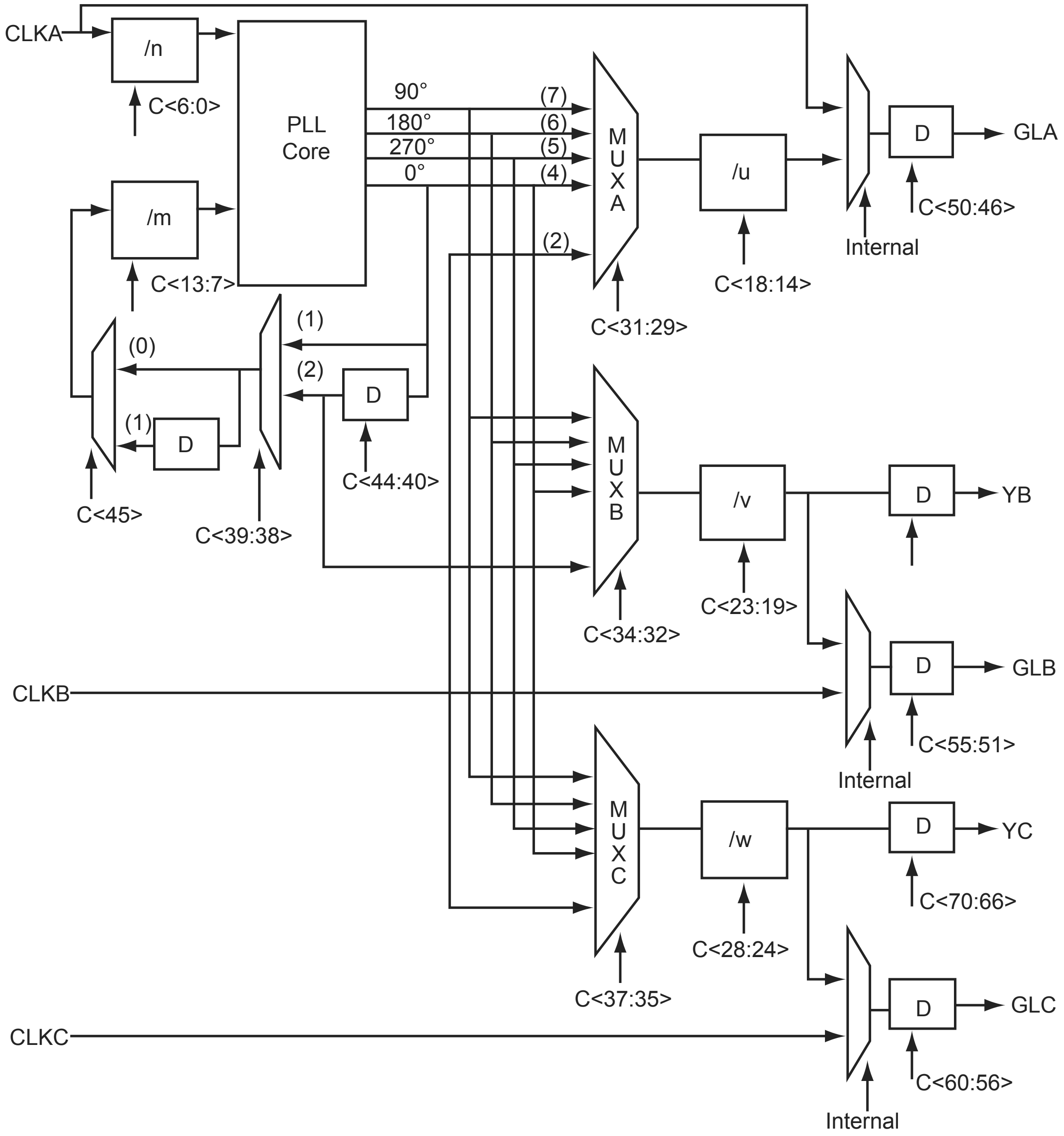

Figure 4-22 • **CCC Block Control Bits – Graphical Representation of Assignments**

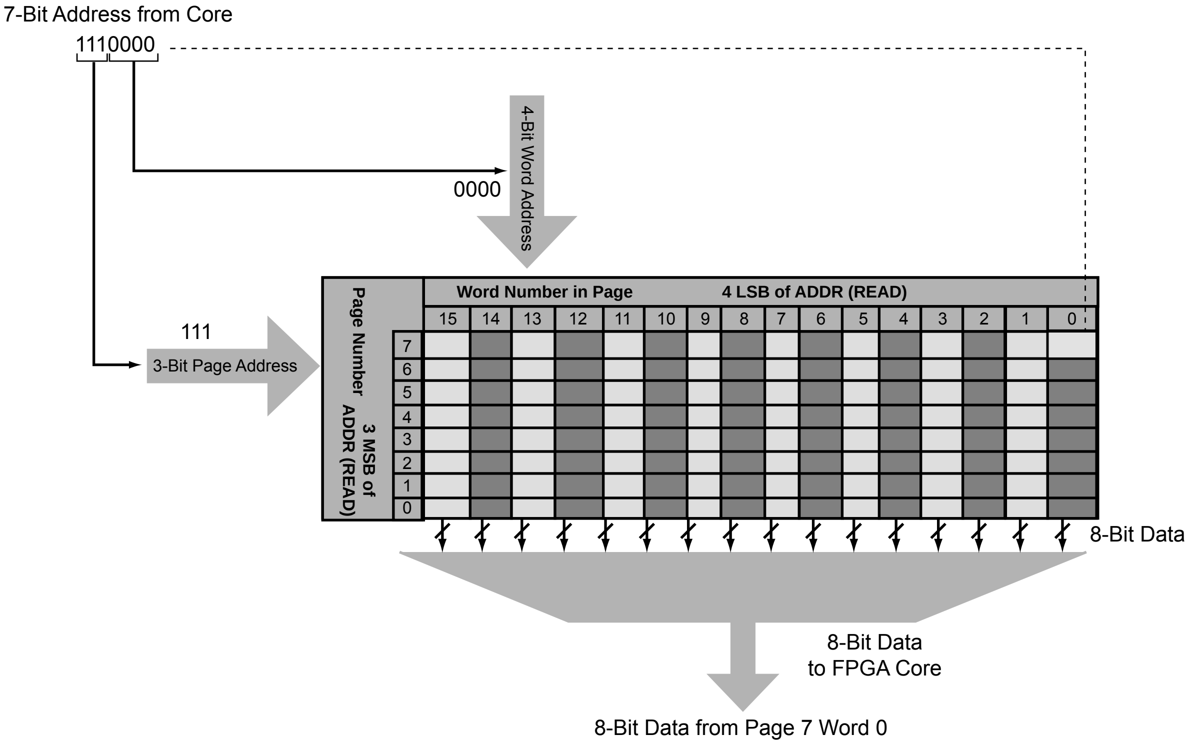

Figure 5-7 • **Accessing FlashROM Using FPGA Core**

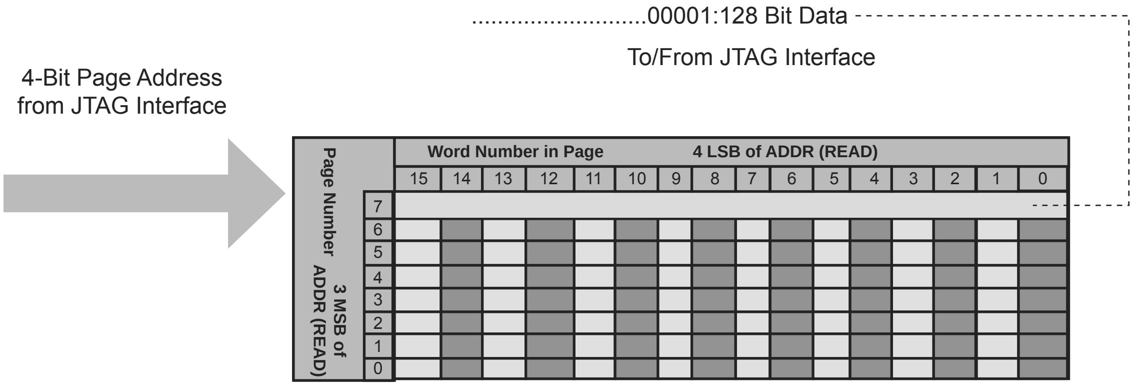

Figure 5-8 • **Accessing FlashROM Using JTAG Port**

SmartGen allows you to generate the FlashROM netlist in VHDL, Verilog, or EDIF format. After the FlashROM netlist is generated, the core can be instantiated in the main design like other SmartGen cores. Note that the macro library name for FlashROM is UFROM. The following is a sample FlashROM VHDL netlist that can be instantiated in the main design:

```
library ieee;
use ieee.std_logic_1164.all;
library fusion;

entity FROM_a is
  port( ADDR : in std_logic_vector(6 downto 0); DOUT : out std_logic_vector(7 downto 0));
end FROM_a;

architecture DEF_ARCH of  FROM_a is

  component UFROM
    generic (MEMORYFILE:string);
    port(DO0, DO1, DO2, DO3, DO4, DO5, DO6, DO7 : out std_logic;
      ADDR0, ADDR1, ADDR2, ADDR3, ADDR4, ADDR5, ADDR6 : in std_logic := 'U') ;
  end component;

  component GND
    port( Y : out std_logic);
  end component;

signal U_7_PIN2 : std_logic ;

begin

  GND_1_net : GND port map(Y => U_7_PIN2);
  UFROM0 : UFROM
  generic map(MEMORYFILE => "FROM_a.mem")
  port map(DO0 => DOUT(0), DO1 => DOUT(1), DO2 => DOUT(2), DO3 => DOUT(3), DO4 => DOUT(4),
    DO5 => DOUT(5), DO6 => DOUT(6), DO7 => DOUT(7), ADDR0 => ADDR(0), ADDR1 => ADDR(1),
    ADDR2 => ADDR(2), ADDR3 => ADDR(3), ADDR4 => ADDR(4), ADDR5 => ADDR(5),
    ADDR6 => ADDR(6));

end DEF_ARCH;
```

SmartGen generates the following files along with the netlist. These are located in the SmartGen folder for the Libero SoC project.

1. MEM (Memory Initialization) file
2. UFC (User Flash Configuration) file
3. Log file

The MEM file is used for simulation, as explained in the "Simulation of FlashROM Design" section on page 143. The UFC file, generated by SmartGen, has the FlashROM configuration for single or multiple devices and is used during STAPL generation. It contains the region properties and simulation values. Note that any changes in the MEM file will not be reflected in the UFC file. Do not modify the UFC to change FlashROM content. Instead, use the SmartGen GUI to modify the FlashROM content. See the "Programming File Generation for FlashROM Design" section on page 143 for a description of how the UFC file is used during the programming file generation. The log file has information regarding the file type and file location.

I/O Standards

Single-Ended Standards

These I/O standards use a push-pull CMOS output stage with a voltage referenced to system ground to designate logical states. The input buffer configuration, output drive, and I/O supply voltage (VCCI) vary among the I/O standards (Figure 7-5).

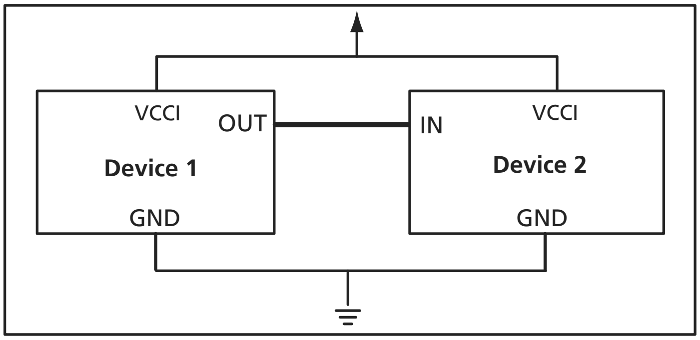

Figure 7-5 **• Single-Ended I/O Standard Topology**

The advantage of these standards is that a common ground can be used for multiple I/Os. This simplifies board layout and reduces system cost. Their low-edge-rate (*dv*/*dt*) data transmission causes less electromagnetic interference (EMI) on the board. However, they are not suitable for high-frequency (>200 MHz) switching due to noise impact and higher power consumption.

LVTTL (Low-Voltage TTL)

This is a general-purpose standard (EIA/JESD8-B) for 3.3 V applications. It uses an LVTTL input buffer and a push-pull output buffer. The LVTTL output buffer can have up to six different programmable drive strengths. The default drive strength is 12 mA. VCCI is 3.3 V. Refer to "I/O Programmable Features" on page 188 for details.

LVCMOS (Low-Voltage CMOS)

The low power flash devices provide four different kinds of LVCMOS: LVCMOS 3.3 V, LVCMOS 2.5 V, LVCMOS 1.8 V, and LVCMOS 1.5 V. LVCMOS 3.3 V is an extension of the LVCMOS standard (JESD8-B–compliant) used for general-purpose 3.3 V applications.

LVCMOS 2.5 V is an extension of the LVCMOS standard (JESD8-5–compliant) used for general-purpose 2.5 V applications.

There is yet another standard supported by IGLOO and ProASIC3 devices (except A3P030): LVCMOS 2.5/5.0 V. This standard is similar to LVCMOS 2.5 V, with the exception that it can support up to 3.3 V on the input side (2.5 V output drive).

LVCMOS 1.8 V is an extension of the LVCMOS standard (JESD8-7–compliant) used for general-purpose 1.8 V applications. LVCMOS 1.5 V is an extension of the LVCMOS standard (JESD8-11–compliant) used for general-purpose 1.5 V applications.

The VCCI values for these standards are 3.3 V, 2.5 V, 1.8 V, and 1.5 V, respectively. Like LVTTL, the output buffer has up to seven different programmable drive strengths (2, 4, 6, 8, 12, 16, and 24 mA). Refer to "I/O Programmable Features" on page 188 for details.

3.3 V PCI (Peripheral Component Interface)

This standard specifies support for both 33 MHz and 66 MHz PCI bus applications. It uses an LVTTL input buffer and a push-pull output buffer. With the aid of an external resistor, this I/O standard can be 5 V–compliant for low power flash devices. It does not have programmable drive strength.

3.3 V PCI-X (Peripheral Component Interface Extended)

An enhanced version of the PCI specification, 3.3 V PCI-X can support higher average bandwidths; it increases the speed that data can move within a computer from 66 MHz to 133 MHz. It is backward-

Table 7-12 **• I/O Hot-Swap and 5 V Input Tolerance Capabilities in IGLOO and ProASIC3 Devices**

	Clamp Diode [1]		Hot Insertion		5 V Input Tolerance [2]		
I/O Assignment	**AGL030 and A3P030**	**Other IGLOO and ProASIC3 Devices**	**AGL015 and AGL030**	**Other IGLOO Devices and All ProASIC3**	**AGL030 and A3P030**	**Other IGLOO and ProASIC3 Devices**	**Input and Output Buffer**
3.3 V LVTTL/LVCMOS	No	Yes	Yes	No	Yes [2]	Yes [2]	Enabled/Disabled
3.3 V PCI, 3.3 V PCI-X	N/A	Yes	N/A	No	N/A	Yes [2]	Enabled/Disabled
LVCMOS 2.5 V [5]	No	Yes	Yes	No	Yes [2]	Yes [4]	Enabled/Disabled
LVCMOS 2.5 V/5.0 V [6]	N/A	Yes	N/A	No	N/A	Yes [4]	Enabled/Disabled
LVCMOS 1.8 V	No	Yes	Yes	No	No	No	Enabled/Disabled
LVCMOS 1.5 V	No	Yes	Yes	No	No	No	Enabled/Disabled
Differential, LVDS/ B-LVDS/M-LVDS/LVPECL	N/A	Yes	N/A	No	N/A	No	Enabled/Disabled

Notes:

1. *The clamp diode is always off for the AGL030 and A3P030 device and always active for other IGLOO and ProASIC3 devices.*
2. *Can be implemented with an external IDT bus switch, resistor divider, or Zener with resistor.*
3. *Refer to Table 7-8 on page 189 to Table 7-11 on page 190 for device-compliant information.*
4. *Can be implemented with an external resistor and an internal clamp diode.*
5. *The LVCMOS 2.5 V I/O standard is supported by the 30 k gate devices only; select the LVCMOS25 macro.*
6. *The LVCMOS 2.5 V / 5.0 V I/O standard is supported by all IGLOO and ProASIC3 devices except 30K gate devices; select the LVCMOS5 macro.*

I/O Bank Structure

Low power flash device I/Os are divided into multiple technology banks. The number of banks is device-dependent. The IGLOOe, ProASIC3EL, and ProASIC3E devices have eight banks (two per side); and IGLOO, ProASIC3L, and ProASIC3 devices have two to four banks. Each bank has its own V_{CCI} power supply pin. Multiple I/O standards can co-exist within a single I/O bank.

In IGLOOe, ProASIC3EL, and ProASIC3E devices, each I/O bank is subdivided into V_{REF} minibanks. These are used by voltage-referenced I/Os. VREF minibanks contain 8 to 18 I/Os. All I/Os in a given minibank share a common VREF line (only one VREF pin is needed per VREF minibank). Therefore, if an I/O in a VREF minibank is configured as a VREF pin, the remaining I/Os in that minibank will be able to use the voltage assigned to that pin. If the location of the VREF pin is selected manually in the software, the user must satisfy VREF rules (refer to the "I/O Software Control in Low Power Flash Devices" section on page 251). If the user does not pick the VREF pin manually, the software automatically assigns it.

Figure 8-4 is a snapshot of a section of the I/O ring, showing the basic elements of an I/O tile, as viewed from the Designer place-and-route tool's MultiView Navigator (MVN).

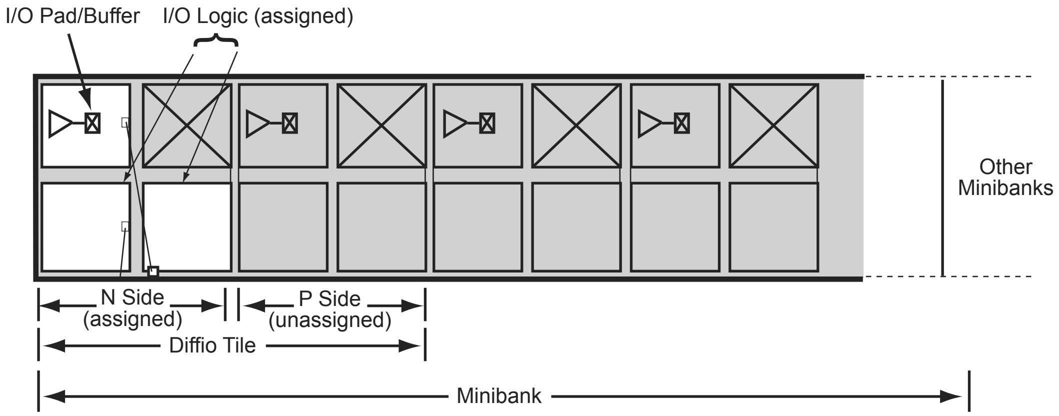

Figure 8-4 **• Snapshot of an I/O Tile**

Low power flash device I/Os are implemented using two tile types: I/O and differential I/O (diffio).

The diffio tile is built up using two I/O tiles, which form an I/O pair (P side and N side). These I/O pairs are used according to differential I/O standards. Both the P and N sides of the diffio tile include an I/O buffer and two I/O logic blocks (auxiliary and main logic).

Every minibank (E devices only) is built up from multiple diffio tiles. The number of the minibank depends on the different-size dies. Refer to the "Pro I/Os—IGLOOe, ProASIC3EL, and ProASIC3E" section on page 215 for an illustration of the minibank structure.

Figure 8-5 on page 222 shows a simplified diagram of the I/O buffer circuitry. The Output Enable signal (OE) enables the output buffer to pass the signal from the core logic to the pin. The output buffer contains ESD protection circuitry, an n-channel transistor that shunts all ESD surges (up to the limit of the device ESD specification) to GND. This transistor also serves as an output pull-down resistor.

Each output buffer also contains programmable slew rate, drive strength, programmable power-up state (pull-up/-down resistor), hot-swap, 5 V tolerance, and clamp diode control circuitry. Multiple flash switches (not shown in Figure 8-5 on page 222) are programmed by user selections in the software to activate different I/O features.

compatible, which means devices can operate at conventional PCI frequencies (33 MHz and 66 MHz). PCI-X is more fault-tolerant than PCI. It also does not have programmable drive strength.

Voltage-Referenced Standards

I/Os using these standards are referenced to an external reference voltage (VREF) and are supported on E devices only.

HSTL Class I and II (High-Speed Transceiver Logic)

These are general-purpose, high-speed 1.5 V bus standards (EIA/JESD 8-6) for signaling between integrated circuits. The signaling range is 0 V to 1.5 V, and signals can be either single-ended or differential. HSTL requires a differential amplifier input buffer and a push-pull output buffer. The reference voltage (VREF) is 0.75 V. These standards are used in the memory bus interface with data switching capability of up to 400 MHz. The other advantages of these standards are low power and fewer EMI concerns.

HSTL has four classes, of which low power flash devices support Class I and II. These classes are defined by standard EIA/JESD 8-6 from the Electronic Industries Alliance (EIA):

- Class I – Unterminated or symmetrically parallel-terminated
- Class II – Series-terminated
- Class III – Asymmetrically parallel-terminated
- Class IV – Asymmetrically double-parallel-terminated

SSTL2 Class I and II (Stub Series Terminated Logic 2.5 V)

These are general-purpose 2.5 V memory bus standards (JESD 8-9) for driving transmission lines, designed specifically for driving the DDR SDRAM modules used in computer memory. SSTL2 requires a differential amplifier input buffer and a push-pull output buffer. The reference voltage (VREF) is 1.25 V.

SSTL3 Class I and II (Stub Series Terminated Logic 3.3 V)

These are general-purpose 3.3 V memory bus standards (JESD 8-8) for driving transmission lines. SSTL3 requires a differential amplifier input buffer and a push-pull output buffer. The reference voltage (VREF) is 1.5 V.

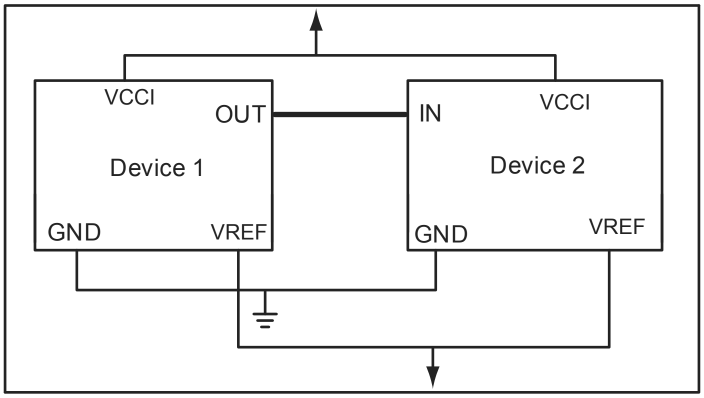

Figure 8-7 • **SSTL and HSTL Topology**

Solution 4

The board-level design must ensure that the reflected waveform at the pad does not exceed the voltage overshoot/undershoot limits provided in the datasheet. This is a requirement to ensure long-term reliability.

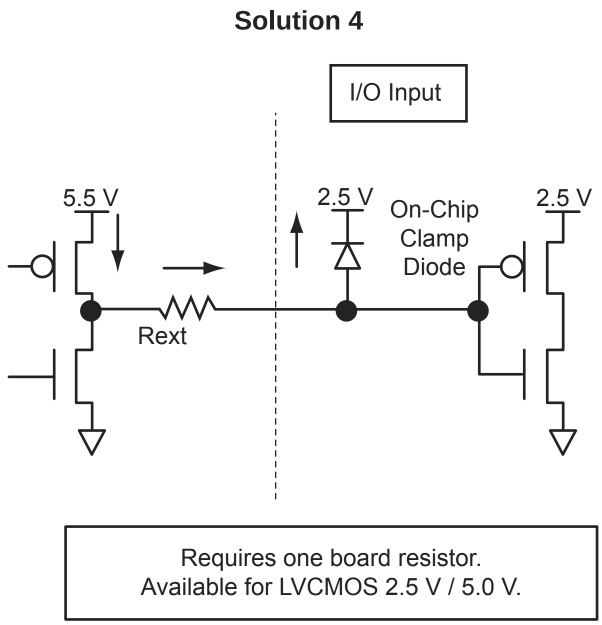

Figure 8-13 • **Solution 4**

Table 8-14 • **Comparison Table for 5 V–Compliant Receiver Solutions**

Solution	Board Components	Speed	Current Limitations
1	Two resistors	Low to High^1	Limited by transmitter's drive strength
2	Resistor and Zener 3.3 V	Medium	Limited by transmitter's drive strength
3	Bus switch	High	N/A
4	Minimum resistor value^{2,3,4,5} R = 47 Ω at T_J = 70°C R = 150 Ω at T_J = 85°C R = 420 Ω at T_J = 100°C	Medium	Maximum diode current at 100% duty cycle, signal constantly at 1 52.7 mA at T_J = 70°C / 10-year lifetime 16.5 mA at T_J = 85°C / 10-year lifetime 5.9 mA at T_J = 100°C / 10-year lifetime For duty cycles other than 100%, the currents can be increased by a factor of 1 / (duty cycle). Example: 20% duty cycle at 70°C Maximum current = (1 / 0.2) × 52.7 mA = 5 × 52.7 mA = 263.5 mA

Notes:

1. *Speed and current consumption increase as the board resistance values decrease.*
2. *Resistor values ensure I/O diode long-term reliability.*
3. *At 70°C, customers could still use 420 Ω on every I/O.*
4. *At 85°C, a 5 V solution on every other I/O is permitted, since the resistance is lower (150 Ω) and the current is higher. Also, the designer can still use 420 Ω and use the solution on every I/O.*
5. *At 100°C, the 5 V solution on every I/O is permitted, since 420 Ω are used to limit the current to 5.9 mA.*

Date	Changes	Page
v1.3 (October 2008)	The "Low Power Flash Device I/O Support" section was revised to include new families and make the information more concise.	214
v1.2 (June 2008)	The following changes were made to the family descriptions in Table 8-1 · Flash-Based FPGAs: • ProASIC3L was updated to include 1.5 V. • The number of PLLs for ProASIC3E was changed from five to six.	214
v1.1 (March 2008)	This document was previously part of *I/O Structures in IGLOO and ProASIC3 Devices*. To provide information specific to IGLOOe, ProASIC3E, and ProASIC3EL, the content was separated and made into a new document. For information on other low power flash family I/O structures, refer to the following documents: *I/O Structures in IGLOO and ProASIC3 Devices* contains information specific to IGLOO, ProASIC3, and ProASIC3L I/O features. *I/O Structures in IGLOO PLUS Devices* contains information specific to IGLOO PLUS I/O features.	N/A

4. Right-click and then choose **Highlight VREF range**. All the pins covered by that VREF pin will be highlighted (Figure 9-14).

Figure 9-14 • **VREF Range**

Using PinEditor or ChipPlanner, VREF pins can also be assigned (Figure 9-15).

Figure 9-15 • **Assigning VREF from PinEditor**

To unassign a VREF pin:

1. Select the pin to unassign.
2. Right-click and choose **Use Pin for VREF.** The check mark next to the command disappears. The VREF pin is now a regular pin.

Resetting the pin may result in unassigning I/O cores, even if they are locked. In this case, a warning message appears so you can cancel the operation.

After you assign the VREF pins, right-click a VREF pin and choose **Highlight VREF Range** to see how many I/Os are covered by that pin. To unhighlight the range, choose **Unhighlight All** from the **Edit** menu.

```
  DDR_OUT_0_inst : DDR_OUT
  port map(DR => DataR, DF => DataF, CLK => CLK, CLR => CLR, Q => Q);
  TRIBUFF_F_8U_0_inst : TRIBUFF_F_8U
  port map(D => Q, E => TrienAux, PAD => PAD);

end DEF_ARCH;
```

DDR Bidirectional Buffer

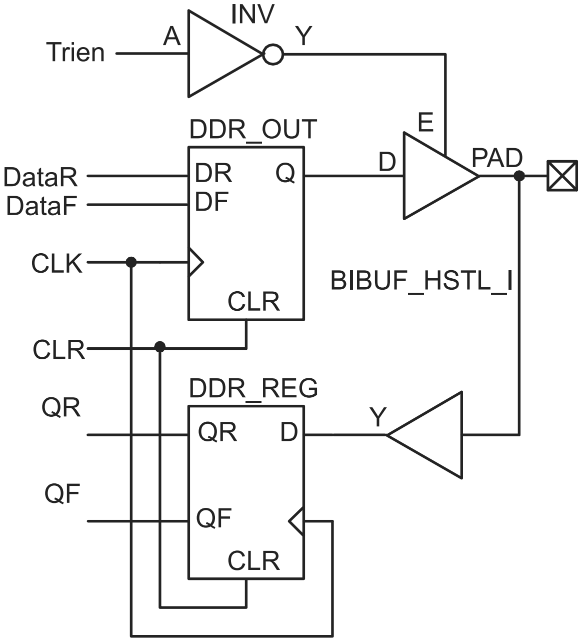

Figure 10-8 • **DDR Bidirectional Buffer, LOW Output Enable (HSTL Class II)**

Verilog

```
module DDR_BiDir_HSTL_I_LowEnb(DataR,DataF,CLR,CLK,Trien,QR,QF,PAD);

input   DataR, DataF, CLR, CLK, Trien;
output  QR, QF;
inout   PAD;

wire TrienAux, D, Q;

  INV Inv_Tri(.A(Trien), .Y(TrienAux));
  DDR_OUT DDR_OUT_0_inst(.DR(DataR),.DF(DataF),.CLK(CLK),.CLR(CLR),.Q(Q));
  DDR_REG DDR_REG_0_inst(.D(D),.CLK(CLK),.CLR(CLR),.QR(QR),.QF(QF));
  BIBUF_HSTL_I BIBUF_HSTL_I_0_inst(.PAD(PAD),.D(Q),.E(TrienAux),.Y(D));

endmodule
```

Programming Support in Flash Devices

The flash FPGAs listed in Table 11-1 support flash in-system programming and the functions described in this document.

***Table 11-1* • 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, supporting 1.2 V to 1.5 V core voltage with Flash*Freeze technology
	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 core voltage 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
SmartFusion	SmartFusion	Mixed-signal FPGA integrating FPGA fabric, programmable microcontroller subsystem (MSS), including programmable analog and ARM® Cortex™-M3 hard processor and flash memory in a monolithic device
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
ProASIC	ProASIC	First generation ProASIC devices
	ProASIC<u>PLUS</u>	Second generation ProASIC devices

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 11-1. 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 11-1. 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*.

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

AES Encryption of Programming Files

Low power flash devices employ AES as part of the security mechanism that prevents invasive and noninvasive attacks. The mechanism entails encrypting the programming file with AES encryption and then passing the programming file through the AES decryption core, which is embedded in the device. The file is decrypted there, and the device is successfully programmed. The AES master key is stored in on-chip nonvolatile memory (flash). The AES master key can be preloaded into parts in a secure programming environment (such as the Microsemi In-House Programming center), and then "blank" parts can be shipped to an untrusted programming or manufacturing center for final personalization with an AES-encrypted bitstream. Late-stage product changes or personalization can be implemented easily and securely by simply sending a STAPL file with AES-encrypted data. Secure remote field updates over public networks (such as the Internet) are possible by sending and programming a STAPL file with AES-encrypted data.

The AES key protects the programming data for file transfer into the device with 128-bit AES encryption. If AES encryption is used, the AES key is stored or preprogrammed into the device. To program, you must use an AES-encrypted file, and the encryption used on the file must match the encryption key already in the device.

The AES key is protected by a FlashLock security Pass Key that is also implemented in each device. The AES key is always protected by the FlashLock Key, and the AES-encrypted file does NOT contain the FlashLock Key. This FlashLock Pass Key technology is exclusive to the Microsemi flash-based device families. FlashLock Pass Key technology can also be implemented without the AES encryption option, providing a choice of different security levels.

In essence, security features can be categorized into the following three options:

- AES encryption with FlashLock Pass Key protection
- FlashLock protection only (no AES encryption)
- No protection

Each of the above options is explained in more detail in the following sections with application examples and software implementation options.

Advanced Encryption Standard

The 128-bit AES standard (FIPS-192) block cipher is the NIST (National Institute of Standards and Technology) replacement for DES (Data Encryption Standard FIPS46-2). AES has been designed to protect sensitive government information well into the 21st century. It replaces the aging DES, which NIST adopted in 1977 as a Federal Information Processing Standard used by federal agencies to protect sensitive, unclassified information. The 128-bit AES standard has 3.4×10^{38} possible 128-bit key variants, and it has been estimated that it would take 1,000 trillion years to crack 128-bit AES cipher text using exhaustive techniques. Keys are stored (securely) in low power flash devices in nonvolatile flash memory. All programming files sent to the device can be authenticated by the part prior to programming to ensure that bad programming data is not loaded into the part that may possibly damage it. All programming verification is performed on-chip, ensuring that the contents of low power flash devices remain secure.

Microsemi has implemented the 128-bit AES (Rijndael) algorithm in low power flash devices. With this key size, there are approximately 3.4×10^{38} possible 128-bit keys. DES has a 56-bit key size, which provides approximately 7.2×10^{16} possible keys. In their AES fact sheet, the National Institute of Standards and Technology uses the following hypothetical example to illustrate the theoretical security provided by AES. If one were to assume that a computing system existed that could recover a DES key in a second, it would take that same machine approximately 149 trillion years to crack a 128-bit AES key. NIST continues to make their point by stating the universe is believed to be less than 20 billion years old.[1]

13 – In-System Programming (ISP) of Microsemi's Low Power Flash Devices Using FlashPro4/3/3X

Introduction

Microsemi'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 FlashPro4/3/3X programmers[1].

IGLOO, ProASIC3, SmartFusion, and Fusion 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. IGLOO, ProASIC3, SmartFusion, and Fusion 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 VPUMP voltage of 3.3 V during programming. In addition, programming via a microcontroller in a target system is also supported.

Refer to the "Microprocessor Programming of Microsemi's Low Power Flash Devices" chapter of an appropriate FPGA fabric user's guide.

Family-specific support:

- ProASIC3, ProASIC3E, SmartFusion, and Fusion devices support ISP.
- ProASIC3L devices operate using a 1.2 V core voltage; however, programming can be done only at 1.5 V. 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.
- IGLOO nano V2 devices can be programmed at 1.2 V core voltage (when using FlashPro4 only) or 1.5 V. IGLOO nano V5 devices are programmed with a VCC core voltage of 1.5 V. Voltage switching is required in-system to switch from a 1.2 V supply (VCC,VCCI, and VJTAG) to 1.5 V for programming. The exception is that V2 devices can be programmed at 1.2 V VCC with FlashPro4.

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

IGLOO, ProASIC3, SmartFusion, and Fusion devices support the JTAG-based IEEE 1532 standard for ISP. To start JTAG operations, the IGLOO device must 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

---

[1] *FlashPro4 replaced FlashPro3/3X in 2010 and is backward compatible with FlashPro3/3X as long as there is no connection to pin 4 on the JTAG header on the board. On FlashPro3/3X, there is no connection to pin 4 on the JTAG header; however, pin 4 is used for programming mode (Prog_Mode) on FlashPro4. When converting from FlashPro3/3X to FlashPro4, users should make sure that JTAG connectors on system boards do not have any connection to pin 4. FlashPro3X supports discrete TCK toggling that is needed to support non-JTAG compliant devices in the chain. This feature is included in FlashPro4.*

Programming Voltage (VPUMP) and VJTAG

Low-power flash devices support on-chip charge pumps, and therefore require only a single 3.3 V programming voltage for the VPUMP pin during programming. When the device is not being programmed, the VPUMP pin can be left floating or can be tied (pulled up) to any voltage between 0 V and 3.6 V[2]. During programming, the target board or the FlashPro4/3/3X programmer can provide VPUMP. FlashPro4/3/3X is capable of supplying VPUMP to a single device. If more than one device is to be programmed using FlashPro4/3/3X on a given board, FlashPro4/3/3X should not be relied on to supply the VPUMP voltage. A FlashPro4/3/3X programmer is not capable of providing reliable VJTAG voltage. The board must supply VJTAG voltage to the device and the VJTAG pin of the programmer header must be connected to the device VJTAG pin. Microsemi recommends that VPUMP[3] and VJTAG power supplies be kept separate with independent filtering capacitors rather than supplying them from a common rail. Refer to the "Board-Level Considerations" section on page 337 for capacitor requirements.

Low power flash device I/Os support a bank-based, voltage-supply architecture that simultaneously supports multiple I/O voltage standards (Table 13-2). 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). Microsemi recommends that TCK be tied to GND through a 200 ohm to 1 Kohm resistor. This prevents a possible totempole current on the input buffer stage. For TDI, TMS, and TRST pins, the devices provide an internal nominal 10 Kohm pull-up resistor. During programming, all I/O pins, except for JTAG interface pins, are tristated and weakly pulled up to VCCI. This isolates the part and prevents the signals from floating. The JTAG interface pins are driven by the FlashPro4/3/3X during programming, including the TRST pin, which is driven HIGH.

Table 13-2 **• Power Supplies**

Power Supply	Programming Mode	Current during Programming
VCC	1.2 V / 1.5 V	< 70 mA
VCCI	1.2 V / 1.5 V / 1.8 V / 2.5 V / 3.3 V (bank-selectable)	I/Os are weakly pulled up.
VJTAG	1.2 V / 1.5 V / 1.8 V / 2.5 V / 3.3 V	< 20 mA
VPUMP	3.15 V to 3.45 V	< 80 mA

Note: All supply voltages should be at 1.5 V or higher, regardless of the setting during normal operation, except for IGLOO nano, where 1.2 V VCC and VJTAG programming is allowed.

Nonvolatile Memory (NVM) Programming Voltage

SmartFusion and Fusion devices need stable VCCNVM/VCCENVM[3] (1.5 V power supply to the embedded nonvolatile memory blocks) and VCCOSC/VCCROSC[4] (3.3 V power supply to the integrated RC oscillator). The tolerance of VCCNVM/VCCENVM is ± 5% and VCCOSC/VCCROSC is ± 5%.

Unstable supply voltage on these pins can cause an NVM programming failure due to NVM page corruption. The NVM page can also be corrupted if the NVM reset pin has noise. This signal must be tied off properly.

Microsemi recommends installing the following capacitors[5] on the VCCNVM/VCCENVM and VCCOSC/VCCROSC pins:

- Add one bypass capacitor of 10 µF for each power supply plane followed by an array of decoupling capacitors of 0.1 µF.
- Add one 0.1 µF capacitor near each pin.

---

[2] *During sleep mode in IGLOO devices connect VPUMP to GND.*

[3] *VPUMP has to be quiet for successful programming. Therefore VPUMP must be separate and required capacitors must be installed close to the FPGA VPUMP pin.*

[4] *VCCROSC is for SmartFusion.*

[5] *The capacitors cannot guarantee reliable operation of the device if the board layout is not done properly.*

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. Device serialization is not supported when using the IEEE1532 standard. 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, Microsemi 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 13-1 on page 331). A single 128-bit AES Key (32 hex characters) is used to encrypt FPGA core programming data and/or FlashROM programming data in the Microsemi 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.