



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	Active
Number of LABs/CLBs	-
Number of Logic Elements/Cells	-
Total RAM Bits	147456
Number of I/O	177
Number of Gates	1000000
Voltage - Supply	1.14V ~ 1.575V
Mounting Type	Surface Mount
Operating Temperature	-40°C ~ 100°C (TJ)
Package / Case	256-LBGA
Supplier Device Package	256-FPBGA (17x17)
Purchase URL	https://www.e-xfl.com/product-detail/microchip-technology/a3p1000l-fgg256i

Table of Contents

Introduction	7
Contents	7
Revision History	7
Related Information	7
1 FPGA Array Architecture in Low Power Flash Devices	9
Device Architecture	9
FPGA Array Architecture Support	10
Device Overview	11
Related Documents	20
List of Changes	20
2 Flash*Freeze Technology and Low Power Modes	21
Flash*Freeze Technology and Low Power Modes	21
Flash Families Support the Flash*Freeze Feature	22
Low Power Modes Overview	23
Static (Idle) Mode	23
Flash*Freeze Mode	24
Sleep and Shutdown Modes	32
Flash*Freeze Design Guide	34
Conclusion	42
Related Documents	42
List of Changes	42
3 Global Resources in Low Power Flash Devices	47
Introduction	47
Global Architecture	47
Global Resource Support in Flash-Based Devices	48
VersaNet Global Network Distribution	49
Chip and Quadrant Global I/Os	51
Spine Architecture	57
Using Clock Aggregation	60
Design Recommendations	62
Conclusion	74
Related Documents	74
List of Changes	75
4 Clock Conditioning Circuits in Low Power Flash Devices and Mixed Signal FPGAs	77
Introduction	77
Overview of Clock Conditioning Circuitry	77
CCC Support in Microsemi's Flash Devices	79
Global Buffers with No Programmable Delays	80
Global Buffer with Programmable Delay	80
Global Buffers with PLL Function	83
Global Input Selections	87

Introduction	213
Low Power Flash Device I/O Support	214
Pro I/Os—IGLOOe, ProASIC3EL, and ProASIC3E	215
I/O Architecture	220
I/O Standards	223
I/O Features	227
Simultaneously Switching Outputs (SSOs) and Printed Circuit Board Layout	241
I/O Software Support	242
User I/O Naming Convention	245
Board-Level Considerations	246
Conclusion	248
Related Documents	248
List of Changes	249
9 I/O Software Control in Low Power Flash Devices	251
Flash FPGAs I/O Support	252
Software-Controlled I/O Attributes	253
Implementing I/Os in Microsemi Software	254
Assigning Technologies and VREF to I/O Banks	264
Conclusion	269
Related Documents	269
List of Changes	270
10 DDR for Microsemi's Low Power Flash Devices	271
Introduction	271
Double Data Rate (DDR) Architecture	271
DDR Support in Flash-Based Devices	272
I/O Cell Architecture	273
Input Support for DDR	275
Output Support for DDR	275
Instantiating DDR Registers	276
Design Example	282
Conclusion	284
List of Changes	285
11 Programming Flash Devices	287
Introduction	287
Summary of Programming Support	287
Programming Support in Flash Devices	288
General Flash Programming Information	289
Important Programming Guidelines	295
Related Documents	297
List of Changes	298
12 Security in Low Power Flash Devices	301
Security in Programmable Logic	301
Security Support in Flash-Based Devices	302
Security Architecture	303
Security Features	304
Security in Action	308

FlashROM Security Use Models	311
Generating Programming Files	313
Conclusion	324
Glossary	324
References	324
Related Documents	325
List of Changes	325
13 In-System Programming (ISP) of Microsemi's Low Power Flash Devices Using FlashPro4/3/3X...	327
Introduction	327
ISP Architecture	327
ISP Support in Flash-Based Devices	328
Programming Voltage (VPUMP) and VJTAG	329
Nonvolatile Memory (NVM) Programming Voltage	329
IEEE 1532 (JTAG) Interface	330
Security	330
Security in ARM-Enabled Low Power Flash Devices	331
FlashROM and Programming Files	333
Programming Solution	334
ISP Programming Header Information	335
Board-Level Considerations	337
Conclusion	338
Related Documents	338
List of Changes	339
14 Core Voltage Switching Circuit for IGLOO and ProASIC3L In-System Programming	341
Introduction	341
Microsemi's Flash Families Support Voltage Switching Circuit	342
Circuit Description	343
Circuit Verification	344
DirectC	346
Conclusion	346
List of Changes	347
15 Microprocessor Programming of Microsemi's Low Power Flash Devices	349
Introduction	349
Microprocessor Programming Support in Flash Devices	350
Programming Algorithm	351
Implementation Overview	351
Hardware Requirement	354
Security	354
Conclusion	355
List of Changes	356
16 Boundary Scan in Low Power Flash Devices.	357
Boundary Scan	357
TAP Controller State Machine	357
Microsemi's Flash Devices Support the JTAG Feature	358
Boundary Scan Support in Low Power Devices	359
Boundary Scan Opcodes	359

Global Resource Support in Flash-Based Devices

The flash FPGAs listed in Table 3-1 support the global resources and the functions described in this document.

Table 3-1 • 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 PLUS	IGLOO FPGAs with enhanced I/O capabilities
	IGLOO nano	The industry's lowest-power, smallest-size solution
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 products as listed in Table 3-1. 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 3-1. 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*.

CCC Support in Microsemi's Flash Devices

The flash FPGAs listed in Table 4-1 support the CCC feature and the functions described in this document.

Table 4-1 • 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 PLUS	IGLOO FPGAs with enhanced I/O capabilities
	IGLOO nano	The industry's lowest-power, smallest-size solution
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 4-1. 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 4-1. 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*.

FlashROM Design Flow

The Microsemi Libero System-on-Chip (SoC) software has extensive FlashROM support, including FlashROM generation, instantiation, simulation, and programming. Figure 5-9 shows the user flow diagram. In the design flow, there are three main steps:

1. FlashROM generation and instantiation in the design
2. Simulation of FlashROM design
3. Programming file generation for FlashROM design

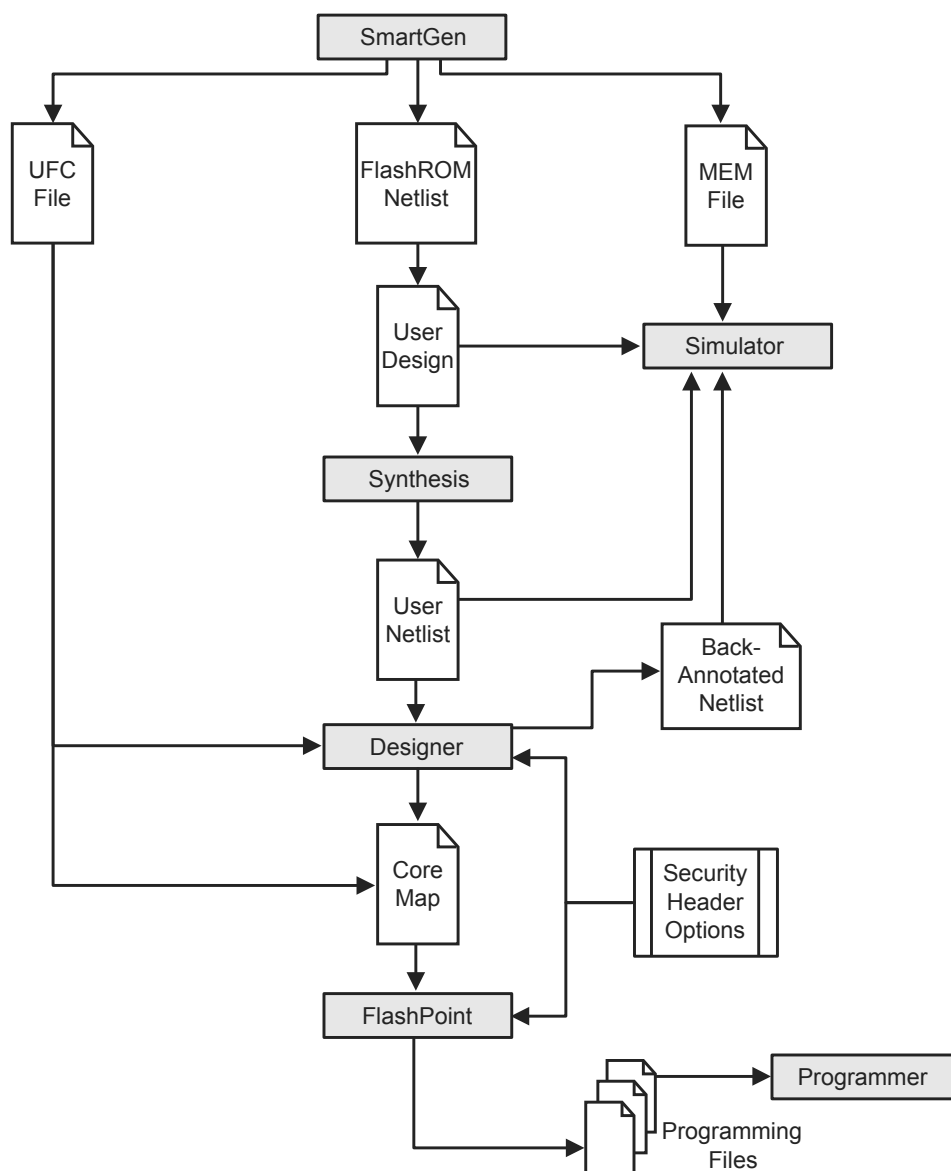


Figure 5-9 • FlashROM Design Flow

Figure 5-12 shows the programming file generator, which enables different STAPL file generation methods. When you select **Program FlashROM** and choose the UFC file, the FlashROM Settings window appears, as shown in Figure 5-13. In this window, you can select the FlashROM page you want to program and the data value for the configured regions. This enables you to use a different page for different programming files.

Figure 5-12 • Programming File Generator

Figure 5-13 • Setting FlashROM during Programming File Generation

The programming hardware and software can load the FlashROM with the appropriate STAPL file. Programming software handles the single STAPL file that contains multiple FlashROM contents for multiple devices, and programs the FlashROM in sequential order (e.g., for device serialization). This feature is supported in the programming software. After programming with the STAPL file, you can run DEVICE_INFO to check the FlashROM content.

without reprogramming the device. Dynamic flag settings are determined by register values and can be altered without reprogramming the device by reloading the register values either from the design or through the UJTAG interface described in the "Initializing the RAM/FIFO" section on page 164.

SmartGen can also configure the FIFO to continue counting after the FIFO is full. In this configuration, the FIFO write counter will wrap after the counter is full and continue to write data. With the FIFO configured to continue to read after the FIFO is empty, the read counter will also wrap and re-read data that was previously read. This mode can be used to continually read back repeating data patterns stored in the FIFO (Figure 6-15).

Figure 6-15 • SmartGen FIFO Configuration Interface

FIFOs configured using SmartGen can also make use of the port mapping feature to configure the names of the ports.

Limitations

Users should be aware of the following limitations when configuring SRAM blocks for low power flash devices:

- SmartGen does not track the target device in a family, so it cannot determine if a configured memory block will fit in the target device.
- Dual-port RAMs with different read and write aspect ratios are not supported.
- Cascaded memory blocks can only use a maximum of 64 blocks of RAM.
- The Full flag of the FIFO is sensitive to the maximum depth of the actual physical FIFO block, not the depth requested in the SmartGen interface.

Features Supported on Every I/O

Table 7-5 lists all features supported by transmitter/receiver for single-ended and differential I/Os. Table 7-6 on page 180 lists the performance of each I/O technology.

Table 7-5 • I/O Features

Feature	Description
All I/O	<ul style="list-style-type: none"> • High performance (Table 7-6 on page 180) • Electrostatic discharge (ESD) protection • I/O register combining option
Single-Ended Transmitter Features	<ul style="list-style-type: none"> • Hot-swap: <ul style="list-style-type: none"> – 30K gate devices: hot-swap in every mode – All other IGLOO and ProASIC3 devices: no hot-swap • Output slew rate: 2 slew rates (except 30K gate devices) • Weak pull-up and pull-down resistors • Output drive: 3 drive strengths • Programmable output loading • Skew between output buffer enable/disable time: 2 ns delay on rising edge and 0 ns delay on falling edge (see the "Selectable Skew between Output Buffer Enable and Disable Times" section on page 199 for more information) • LVTTTL/LVCMOS 3.3 V outputs compatible with 5 V TTL inputs
Single-Ended Receiver Features	<ul style="list-style-type: none"> • 5 V–input–tolerant receiver (Table 7-12 on page 193) • Separate ground plane for GNDQ pin and power plane for VMV pin are used for input buffer to reduce output-induced noise.
Differential Receiver Features—250K through 1M Gate Devices	<ul style="list-style-type: none"> • Separate ground plane for GNDQ pin and power plane for VMV pin are used for input buffer to reduce output-induced noise.
CMOS-Style LVDS, B-LVDS, M-LVDS, or LVPECL Transmitter	<ul style="list-style-type: none"> • Two I/Os and external resistors are used to provide a CMOS-style LVDS, DDR LVDS, B-LVDS, and M-LVDS/LVPECL transmitter solution. • High slew rate • Weak pull-up and pull-down resistors • Programmable output loading

5 V Input and Output Tolerance

IGLOO and ProASIC3 devices are both 5 V-input- and 5 V-output-tolerant if certain I/O standards are selected. Table 7-5 on page 179 shows the I/O standards that support 5 V input tolerance. Only 3.3 V LVTTTL/LVCMOS standards support 5 V output tolerance. Refer to the appropriate family datasheet for the detailed description and configuration information.

This feature is not shown in the I/O Attribute Editor.

5 V Input Tolerance

I/Os can support 5 V input tolerance when LVTTTL 3.3 V, LVCMOS 3.3 V, LVCMOS 2.5 V, and LVCMOS 2.5 V / 5.0 V configurations are used (see Table 7-12 on page 193). There are four recommended solutions for achieving 5 V receiver tolerance (see Figure 7-9 on page 195 to Figure 7-12 on page 197 for details of board and macro setups). All the solutions meet a common requirement of limiting the voltage at the input to 3.6 V or less. In fact, the I/O absolute maximum voltage rating is 3.6 V, and any voltage above 3.6 V may cause long-term gate oxide failures.

Solution 1

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

This scheme will also work for a 3.3 V PCI/PCI-X configuration, but the internal diode should not be used for clamping, and the voltage must be limited by the two external resistors as explained below. Relying on the diode clamping would create an excessive pad DC voltage of $3.3\text{ V} + 0.7\text{ V} = 4\text{ V}$.

This solution requires two board resistors, as demonstrated in Figure 7-9 on page 195. Here are some examples of possible resistor values (based on a simplified simulation model with no line effects and $10\ \Omega$ transmitter output resistance, where $R_{tx_out_high} = (V_{CCI} - V_{OH}) / I_{OH}$ and $R_{tx_out_low} = V_{OL} / I_{OL}$).

Example 1 (high speed, high current):

$$R_{tx_out_high} = R_{tx_out_low} = 10\ \Omega$$

$$R1 = 36\ \Omega (\pm 5\%), P(r1)_{min} = 0.069\ \Omega$$

$$R2 = 82\ \Omega (\pm 5\%), P(r2)_{min} = 0.158\ \Omega$$

$$I_{max_tx} = 5.5\text{ V} / (82 \times 0.95 + 36 \times 0.95 + 10) = 45.04\text{ mA}$$

$$t_{RISE} = t_{FALL} = 0.85\text{ ns at } C_{pad_load} = 10\text{ pF (includes up to 25\% safety margin)}$$

$$t_{RISE} = t_{FALL} = 4\text{ ns at } C_{pad_load} = 50\text{ pF (includes up to 25\% safety margin)}$$

Example 2 (low-medium speed, medium current):

$$R_{tx_out_high} = R_{tx_out_low} = 10\ \Omega$$

$$R1 = 220\ \Omega (\pm 5\%), P(r1)_{min} = 0.018\ \Omega$$

$$R2 = 390\ \Omega (\pm 5\%), P(r2)_{min} = 0.032\ \Omega$$

$$I_{max_tx} = 5.5\text{ V} / (220 \times 0.95 + 390 \times 0.95 + 10) = 9.17\text{ mA}$$

$$t_{RISE} = t_{FALL} = 4\text{ ns at } C_{pad_load} = 10\text{ pF (includes up to 25\% safety margin)}$$

$$t_{RISE} = t_{FALL} = 20\text{ ns at } C_{pad_load} = 50\text{ pF (includes up to 25\% safety margin)}$$

Other values of resistors are also allowed as long as the resistors are sized appropriately to limit the voltage at the receiving end to $2.5\text{ V} < V_{in}(rx) < 3.6\text{ V}$ when the transmitter sends a logic 1. This range of $V_{in_dc}(rx)$ must be assured for any combination of transmitter supply ($5\text{ V} \pm 0.5\text{ V}$), transmitter output resistance, and board resistor tolerances.

I/O Banks and I/O Standards Compatibility

I/Os are grouped into I/O voltage banks.

Each I/O voltage bank has dedicated I/O supply and ground voltages (VMV/GNDQ for input buffers and V_{CCI} /GND for output buffers). Because of these dedicated supplies, only I/Os with compatible standards can be assigned to the same I/O voltage bank. Table 8-3 on page 217 shows the required voltage compatibility values for each of these voltages.

There are eight I/O banks (two per side).

Every I/O bank is divided into minibanks. Any user I/O in a VREF minibank (a minibank is the region of scope of a VREF pin) can be configured as a VREF pin (Figure 8-2). Only one V_{REF} pin is needed to control the entire V_{REF} minibank. The location and scope of the V_{REF} minibanks can be determined by the I/O name. For details, see the user I/O naming conventions for "IGLOOe and ProASIC3E" on page 245. Table 8-5 on page 217 shows the I/O standards supported by IGLOOe and ProASIC3E devices, and the corresponding voltage levels.

I/O standards are compatible if they comply with the following:

- Their VCCI and VMV values are identical.
- Both of the standards need a VREF, and their VREF values are identical.
- All inputs and disabled outputs are voltage tolerant up to 3.3 V.

For more information about I/O and global assignments to I/O banks in a device, refer to the specific pin table for the device in the packaging section of the datasheet, and see the user I/O naming conventions for "IGLOOe and ProASIC3E" on page 245.

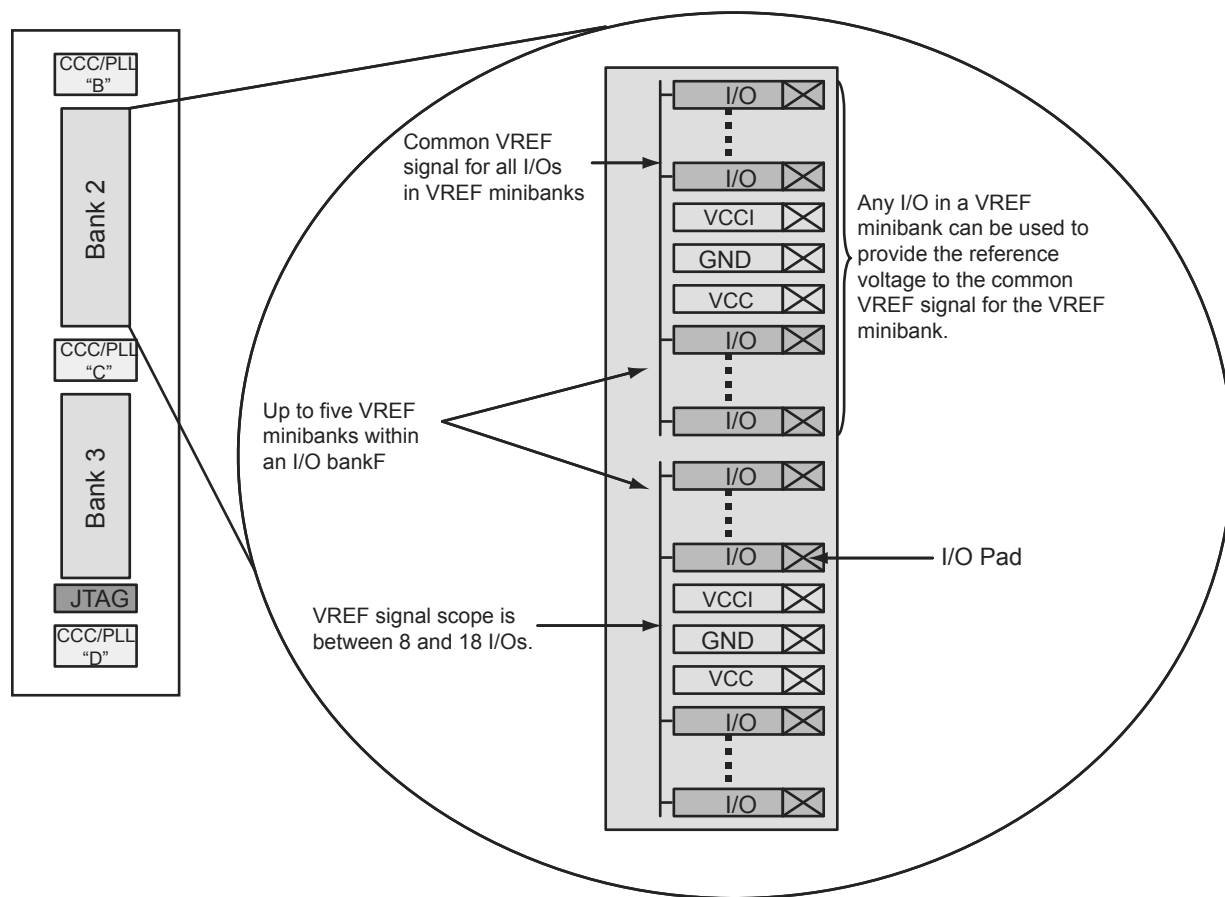


Figure 8-2 • Typical IGLOOe and ProASIC3E I/O Bank Detail Showing V_{REF} Minibanks

B-LVDS/M-LVDS

Bus LVDS (B-LVDS) refers to bus interface circuits based on LVDS technology. Multipoint LVDS (M-LVDS) specifications extend the LVDS standard to high-performance multipoint bus applications. Multidrop and multipoint bus configurations may contain any combination of drivers, receivers, and transceivers. Microsemi LVDS drivers provide the higher drive current required by B-LVDS and M-LVDS to accommodate the loading. The driver requires series terminations for better signal quality and to control voltage swing. Termination is also required at both ends of the bus, since the driver can be located anywhere on the bus. These configurations can be implemented using TRIBUF_LVDS and BIBUF_LVDS macros along with appropriate terminations. Multipoint designs using Microsemi LVDS macros can achieve up to 200 MHz with a maximum of 20 loads. A sample application is given in Figure 8-9. The input and output buffer delays are available in the LVDS sections in the datasheet.

Example: For a bus consisting of 20 equidistant loads, the terminations given in EQ 8-1 provide the required differential voltage, in worst case industrial operating conditions, at the farthest receiver:

$$R_S = 60 \, \Omega, R_T = 70 \, \Omega, \text{ given } Z_0 = 50 \, \Omega (2'') \text{ and } Z_{\text{stub}} = 50 \, \Omega (\sim 1.5'').$$

EQ 8-1

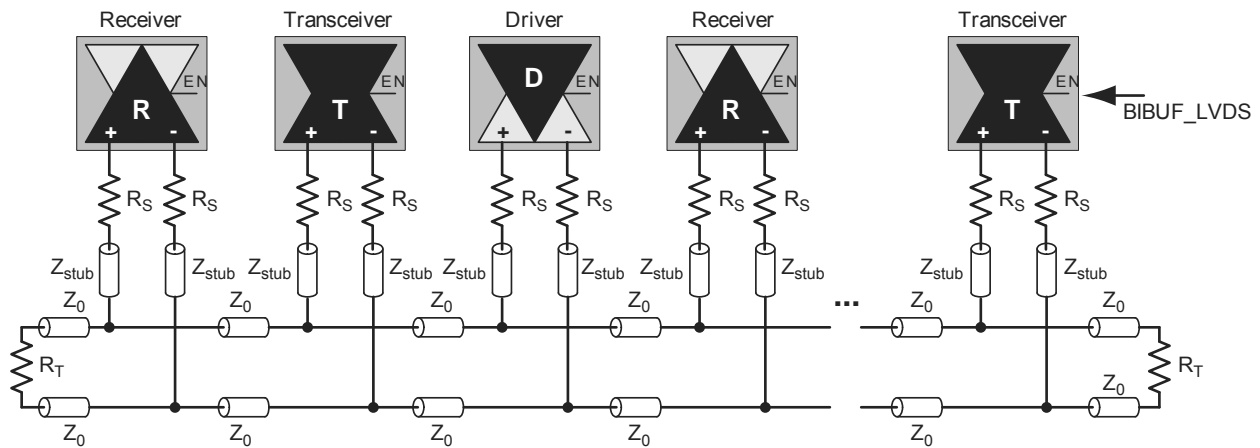


Figure 8-9 • A B-LVDS/M-LVDS Multipoint Application Using LVDS I/O Buffers

Instantiating DDR Registers

Using SmartGen is the simplest way to generate the appropriate RTL files for use in the design. Figure 10-4 shows an example of using SmartGen to generate a DDR SSTL2 Class I input register. SmartGen provides the capability to generate all of the DDR I/O cells as described. The user, through the graphical user interface, can select from among the many supported I/O standards. The output formats supported are Verilog, VHDL, and EDIF.

Figure 10-5 on page 277 through Figure 10-8 on page 280 show the I/O cell configured for DDR using SSTL2 Class I technology. For each I/O standard, the I/O pad is buffered by a special primitive that indicates the I/O standard type.

Figure 10-4 • Example of Using SmartGen to Generate a DDR SSTL2 Class I Input Register

```

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

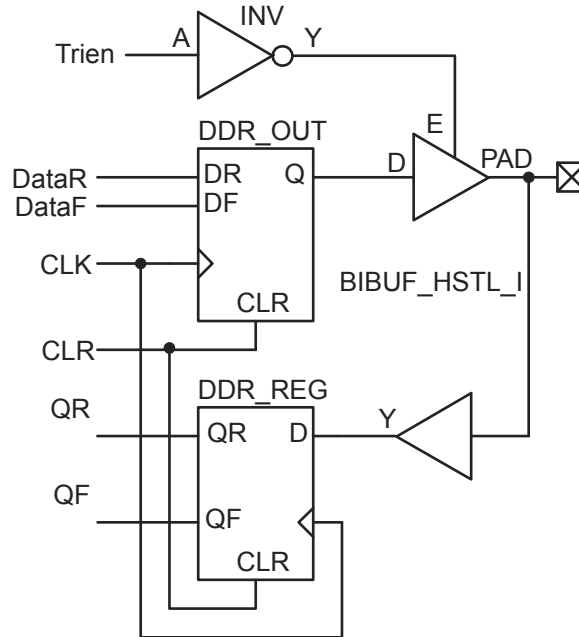


Figure 10-8 • DDR Bidirectional Buffer, LOW Output Enable (HSTL Class II)

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

```

General Flash Programming Information

Programming Basics

When choosing a programming solution, there are a number of options available. This section provides a brief overview of those options. The next sections provide more detail on those options as they apply to Microsemi FPGAs.

Reprogrammable or One-Time-Programmable (OTP)

Depending on the technology chosen, devices may be reprogrammable or one-time-programmable. As the name implies, a reprogrammable device can be programmed many times. Generally, the contents of such a device will be completely overwritten when it is reprogrammed. All Microsemi flash devices are reprogrammable.

An OTP device is programmable one time only. Once programmed, no more changes can be made to the contents. Microsemi flash devices provide the option of disabling the reprogrammability for security purposes. This combines the convenience of reprogrammability during design verification with the security of an OTP technology for highly sensitive designs.

Device Programmer or In-System Programming

There are two fundamental ways to program an FPGA: using a device programmer or, if the technology permits, using in-system programming. A device programmer is a piece of equipment in a lab or on the production floor that is used for programming FPGA devices. The devices are placed into a socket mounted in a programming adapter module, and the appropriate electrical interface is applied. The programmed device can then be placed on the board. A typical programmer, used during development, programs a single device at a time and is referred to as a single-site engineering programmer.

With ISP, the device is already mounted onto the system printed circuit board when programming occurs. Typically, ISP programming is performed via a JTAG interface on the FPGA. The JTAG pins can be controlled either by an on-board resource, such as a microprocessor, or by an off-board programmer through a header connection. Once mounted, it can be programmed repeatedly and erased. If the application requires it, the system can be designed to reprogram itself using a microprocessor, without the use of any external programmer.

If multiple devices need to be programmed with the same program, various multi-site programming hardware is available in order to program many devices in parallel. Microsemi In House Programming is also available for this purpose.

Programming Features for Microsemi Devices

Flash Devices

The flash devices supplied by Microsemi are reprogrammable by either a generic device programmer or ISP. Microsemi supports ISP using JTAG, which is supported by the FlashPro4 and FlashPro3, FlashPro Lite, Silicon Sculptor 3, and Silicon Sculptor II programmers.

Levels of ISP support vary depending on the device chosen:

- All SmartFusion, Fusion, IGLOO, and ProASIC3 devices support ISP.
- IGLOO, IGLOOe, IGLOO nano V5, and IGLOO PLUS 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.

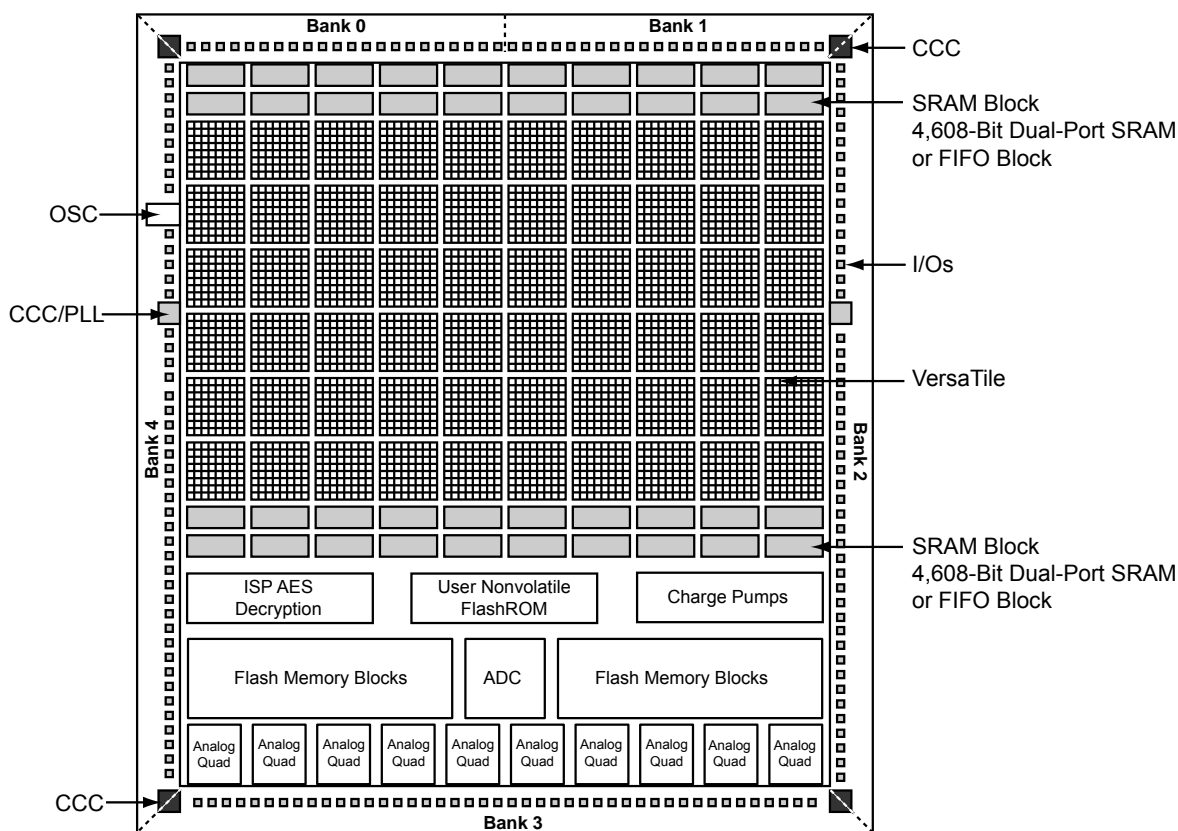


Figure 12-3 • Block Representation of the AES Decryption Core in a Fusion AFS600 FPGA

Security Features

IGLOO and ProASIC3 devices have two entities inside: FlashROM and the FPGA core fabric. Fusion devices contain three entities: FlashROM, FBs, and the FPGA core fabric. The parts can be programmed or updated independently with a STAPL programming file. The programming files can be AES-encrypted or plaintext. This allows maximum flexibility in providing security to the entire device. Refer to the "Programming Flash Devices" section on page 287 for information on the FlashROM structure.

Unlike SRAM-based FPGA devices, which require a separate boot PROM to store programming data, low power flash devices are nonvolatile, and the secured configuration data is stored in on-chip flash cells that are part of the FPGA fabric. Once programmed, this data is an inherent part of the FPGA array and does not need to be loaded at system power-up. SRAM-based FPGAs load the configuration bitstream upon power-up; therefore, the configuration is exposed and can be read easily.

The built-in FPGA core, FBs, and FlashROM support programming files encrypted with the 128-bit AES (FIPS-192) block ciphers. The AES key is stored in dedicated, on-chip flash memory and can be programmed before the device is shipped to other parties (allowing secure remote field updates).

Security in ARM-Enabled Low Power Flash Devices

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

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

Figure 13-2 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.

Microsemi low power flash devices also provide the unique Microsemi 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. Microsemi does 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 Microsemi Designer software. Refer to the "Security in Low Power Flash Devices" section on page 301 for more information.

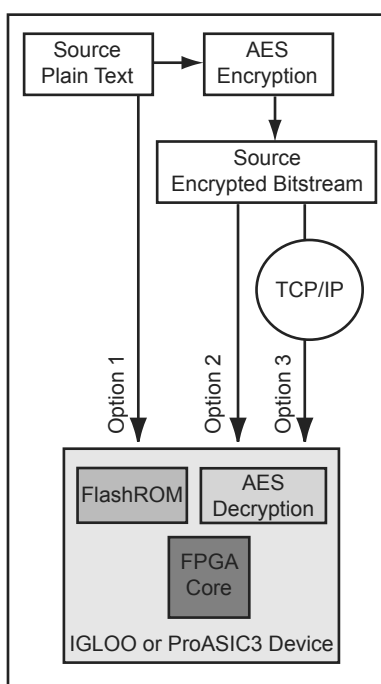


Figure 13-2 • Different ISP Use Models

ISP Programming Header Information

The FlashPro4/3/3X 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 Microsemi SoC Products Group (FP3-10PIN-ADAPTER-KIT).

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 also use FP3-10PIN-ADAPTER-KIT.

Table 13-3 • 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.
Microsemi	FP3-10PIN-ADAPTER-KIT	Transition adapter kit to allow FP3 to be connected to a micro 10-pin header (50 mil pitch). Includes a 6 inch Samtec FFSD-05-D-06.00-01-N cable in the kit. The transition adapter board was previously offered as FP3-26PIN-ADAPTER and includes a 26-pin adapter for design transitions from ProASIC ^{PLUS} based boards to ProASIC3 based boards.

TCK	1	2	GND
TDO	3	4	NC (FlashPro3/3X); Prog_Mode* (FlashPro4)
TMS	5	6	VJTAG
VPUMP	7	8	TRST
TDI	9	10	GND

*Note: *Prog_Mode on FlashPro4 is an output signal that goes High during device programming and returns to Low when programming is complete. This signal can be used to drive a system to provide a 1.5 V programming signal to IGLOO nano, ProASIC3L, and RT ProASIC3 devices that can run with 1.2 V core voltage but require 1.5 V for programming. IGLOO nano V2 devices can be programmed at 1.2 V core voltage (when using FlashPro4 only), but IGLOO nano V5 devices are programmed with a VCC core voltage of 1.5 V.*

Figure 13-5 • Programming Header (top view)

Microsemi's Flash Families Support Voltage Switching Circuit

The flash FPGAs listed in Table 14-1 support the voltage switching circuit feature and the functions described in this document.

Table 14-1 • Flash-Based FPGAs Supporting Voltage Switching Circuit

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	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

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 14-1. 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 14-1. 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*.

Circuit Verification

The power switching circuit recommended above is implemented on Microsemi's Icicle board (Figure 14-2). On the Icicle board, VJTAGENB is used to control the N-Channel Digital FET; however, this circuit was modified to use TRST instead of VJTAGENB in this application. There are three important aspects of this circuit that were verified:

1. The rise on VCC from 1.2 V to 1.5 V when TRST is HIGH
2. VCC rises to 1.5 V before programming begins.
3. VCC switches from 1.5 V to 1.2 V when TRST is LOW.

Verification Steps

1. The rise on VCC from 1.2 V to 1.5 V when TRST is HIGH.
-

Figure 14-2 • Core Voltage on the IGLOO AGL125-QNG132 Device

In the oscilloscope plots (Figure 14-2), the TRST from FlashPro3 and the VCC core voltage of the IGLOO device are labeled. This plot shows the rise characteristic of the TRST signal from FlashPro3. Once the TRST signal is asserted HIGH, the LTC3025 shown in Figure 14-1 on page 343 senses the increase in voltage and changes the output from 1.2 V to 1.5 V. It takes the circuit approximately 100 μ s to respond to TRST and change the voltage to 1.5 V on the VCC core.