AC478
Application Note
PolarFire FPGAs for Safety-Critical Applications

Microsemi
a Microchip company

a Microchip company

Microsemi Headquarters
One Enterprise, Aliso Viejo,
CA 92656 USA
Within the USA: +1 (800) 713-4113
Outside the USA: +1 (949) 380-6100
Sales: +1 (949) 380-6136
Fax: +1 (949) 215-4996
Email: sales.support@microsemi.com
www.microsemi.com

About Microsemi

Microsemi, a wholly owned subsidiary of Microchip Technology Inc. (Nasdaq: MCHP), offers a comprehensive portfolio of semiconductor and system solutions for aerospace & defense, communications, data center and industrial markets. Products include high-performance and radiation-hardened analog mixed-signal integrated circuits, FPGAs, SoCs and ASICs; power management products; timing and synchronization devices and precise time solutions, setting the world's standard for time; voice processing devices; RF solutions; discrete components; enterprise storage and communication solutions, security technologies and scalable anti-tamper products; Ethernet solutions; Power-over-Ethernet ICs and midspans; as well as custom design capabilities and services. Learn more at www.microsemi.com.

51900478. 1.0 10/18

Contents

Tables

Figures

1 Revision History

The revision history describes the changes that were implemented in the document. The changes are listed by revision, starting with the current publication.

1.1 Revision 1.0

The first publication of this document.

2 PolarFire FPGA Safety-Critical Features

2.1 Introduction

Microsemi PolarFire® FPGAs are designed to address the high-reliability requirements of safety-critical systems in industrial, aviation, military, and communication applications with the following features:

- SEE immune FPGA configuration
- No external configuration device required
- On-chip memories with built-in error detection and correction capabilities
- Built-in self-test
- Passivation and monitoring of unused hard IP blocks

The following sections describe these features.

2.2 Reliability of FPGA Configuration Cell

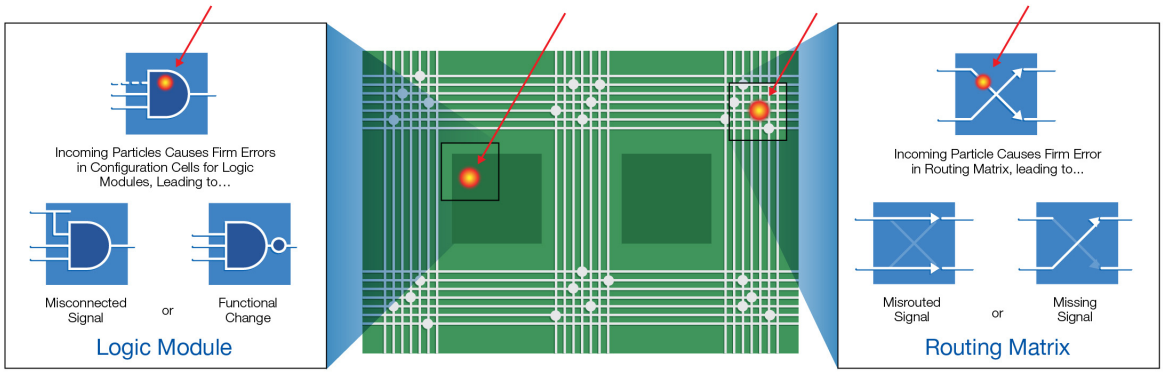
PolarFire FPGA family uses Silicon-Oxide-Nitride-Oxide-Silicon (SONOS) non-volatile (NV) technology to build the FPGA configuration cell. The SONOS NV technology uses a push-pull cell containing an N-channel and a P-channel NV device. For reliability test results of PolarFire FPGAs, see *Microsemi FPGA and SoC Products Reliability Report*.

2.3 Single Event Effects Immunity of FPGA Configuration Cell

Malfunctions in integrated circuits (ICs) due to radiation effects (single event effects) from high energy neutrons at ground level and high altitudes are a major concern for safety-critical applications.

Configuration upsets in FPGAs are problematic because the configuration memory must remain static and error free during all the operating hours of the device for correct operation. Any upset will be persistent until the device is powered-down or the cell is reprogrammed correctly. If an upset occurs in the erroneous state, the logic or routing of the FPGA fabric will be wrong, potentially causing not just a single wrong data value, but a string of wrong results until it is fixed. This may require a full system reboot.

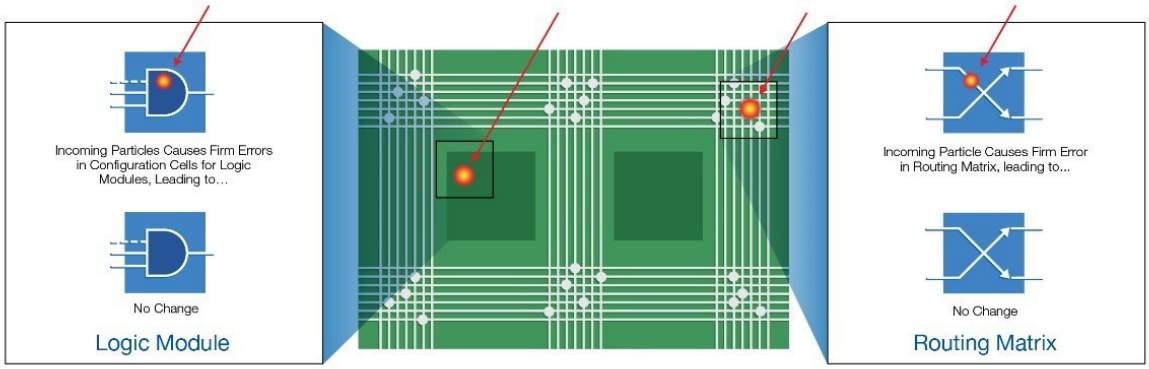
Figure 1 • **Configuration Upsets in SRAM FPGAs due to Single Event Effects**



Attempts to mitigate configuration upsets in SRAM FPGAs are extremely complex. Typically, they require dual-redundant FPGAs with an external controller, which periodically searches for configuration errors in each SRAM FPGA and initiates a failover from primary to secondary FPGA while reprogramming of the primary FPGA takes place. This presumes that the system will not be detrimentally affected by the bad data produced by the FPGA during the period that the configuration SEU is undetected. It also presumes that the system can tolerate the subsequent loss of processing while the failover from primary to secondary takes place.

The PolarFire FPGA configuration is SEE immune because of the non-volatile technology, unlike the configuration memory in SRAM-based FPGAs, which can flip state due to neutron hits. In the PolarFire FPGA family, the SONOS NV charge is stored in the nitride dielectric, which is not susceptible to charge loss from neutron hit, making it immune to Neutron induced configuration upsets.

Figure 2 • **SEE Immunity of PolarFire FPGA Configuration Cells**



The first phase of neutron testing is performed on PolarFire FPGA family. The main objective is to test the product for latch-up behavior and to get soft error data on the fabric. For test results, see *TR0043: PolarFire Neutron Test Results Test Report*.

For more information about radiation effects, see the following web page *https://www.microsemi.com/product-directory/reliability/4883-see#overview*.

2.4 The Live-at-Power-Up ("Instant On") and "Single-Chip" Features

An advantage of the NV technology is that there is no need to reload the FPGA bitstream at power-up because the FPGA configuration cell retains its state after power-down. Thus, there is no need for an external flash. This improves overall system reliability. In large systems, that use many FPGAs this can result in a significant increase in reliability. For example, in some large passenger airplanes, there can be over 1,000 FPGAs used throughout the system. Eliminating configuration devices brings a significant increase in reliability. Additionally, the use of internal NV memory for each configuration transistor means that these devices are live at power-up. This 'instant on' capability improves system robustness since the designer need not consider the various 'complexities' that occur during power-up if some devices are not working.

2.5 Error Correction and Detection Capabilities of Embedded Block RAMs

PolarFire devices include SRAM blocks as part of the hard IP blocks and FPGA fabric. Except for the uSRAM blocks, all other embedded RAM blocks (see Table 1) are implemented with error detection and correction (ECC) capabilities to protect them from SEU effects.

Table 1 • **ECC Support in Embedded Block RAMs**

Block	Component	ECC
FPGA Fabric	LSRAM	Yes[1]
FPGA Fabric	uSRAM	No
User Cryptoprocessor	Code and Data RAMs	Yes
PCIe	PCIe Tx Buffer	Yes
PCIe	PCIe Rx Buffer	Yes
PCIe	PCIe to AXI (P2A) Buffer	Yes
PCIe	AXI to PCIe (A2P) Buffer	Yes

1. For LSRAMs, the ECC operation is supported only in two-port mode with a data width of 33-bit. See *UG0680: PolarFire FPGA Fabric User Guide* for more information.

2.5.1 ECC Operation in LSRAMs

LSRAMs configured in two-port mode with 33-bit data width supports ECC with single-bit error correction and dual-bit error detection capabilities. The LSRAMs are designed with an interleave distance of 11.52 µm (center to center distance) to prevent multiple bit upsets within a single word. Also, in the memory array, latch-up (SEL) is prevented by including rows of tub ties spaced no more than 8.0 m.

The ECC logic in LSRAMs generates the following flags for the user logic to take necessary action:

- SB_CORRECT—gets asserted when a single-bit error is detected. If SB_CORRECT is set without the dual-bit error flag being asserted, the corrupted bit is corrected in read data output. The data scrubbing is not implemented in the ECC logic. The scrubbing must be implemented in the user logic if required.
- DB_DETECT—gets asserted when a dual-bit error is detected, but not corrected. Multi-bit errors (more than two bits) produce unknown results on the flags and data outputs. If DB_DETECT is set, correction is not performed on read data output.

For more information about LSRAM ECC operation, see *UG0680: PolarFire FPGA Fabric User Guide*.

2.5.2 ECC Operation in User Cryptoprocessor RAMs

The User Cryptoprocessor's built-in RAMs support ECC for single bit error correction and dual bit error detection. The User Cryptoprocessor can be used in the design by instantiating PF_CRYPTO macro in the design. In the event of a correctable error, the operation of the core will not be interrupted. Uncorrectable error detection causes an immediate halt of the current operation and automatic purge of the User Cryptoprocessor. The ALARM output signal of PF_CRYPTO gets set in the event of uncorrectable error detection. The purge operation zeroizes all the internal memories. An automatic soft reset is issued after completion of the purge operation. The COMPLETE output is asserted upon completion of the purge operation. All the cryptographic operations are performed through TeraFire cryptographic application library (CAL) functions and the CALPKTrfRes function is used to complete an operation. The CALPKTrfRes function returns an error code in the event of an alarm. For more information about CAL functions, see *Athena TeraFire Cryptographic Algorithm Library (CAL) Users Guide*.

2.5.3 ECC Operation in PCIe Data Buffers

The PCIe data buffers—PCIe Tx Buffer, PCIe Rx Buffer, PCIe to AXI (P2A) Buffer, and AXI to PCIe (A2P) Buffer—support single bit error correction and dual bit error detection. The single bit errors in the PCIe buffers get corrected automatically. The dual bit error detection is reported to the user logic using dedicated fabric ports and status registers. The following table summarizes the effect of dual bit error in the PCIe data buffers. For more information about ECC operation, see *UG0685: PolarFire FPGA PCI Express User Guide*.

Table 2 • **Summary of Dual-bit Error Effects in PCIe Data Buffers**

Dual Error in Buffer	Effect in TLP (PCIe IF)	Effect at Fabric IF
Rx	TLP is forwarded to AXI IF.	Application requires to poll SEC_ERROR_EVENT_CNT / DED_ERROR_EVENT_CNT status register to find out the error.
Tx	TLP is transmitted. Tx buffer memory error is ignored and cannot be recovered by PCIe protocol	Application requires to poll SEC_ERROR_EVENT_CNT /DED_ERROR_EVENT_CNT to find out the error.
PCIE to AXI	TLP forwarded to AXI IF.	The PCIE_#_M_WDERR and PCIE_#_S_RDERR signals to fabric IF are asserted
AXI to PCIE	If ECRC is enabled, PCIe interface marks this TLP as erroneous and an ECRC error is generated by PCIe controller. If ECRC is disabled, TLP is discarded. If this AXI to PCIE buffer error is during a read transaction, it results in a completion timeout.	If this AXI to PCIE buffer error is during a write transaction, write response PCIESS_AXI_#_S_BRESP [1:0] == 2'b10 is returned in AXI Write Response.

Note: ECRC is enabled when PCIE Specific Capabilities Settings Register PCIE_PEX_SPC Bit[31] is set to 1 to indicate Advanced Error Reporting (AER) is enabled. ECRC error generation and checking can further be individually disabled or enabled by register PCIE_PEX_SPC2 Bit[1] and Bit[2].

Note: Rx/Tx buffer reports either SEC or DED error, when TLP is forwarded to AXI interface. The ERROR_INT and ERROR_EVENT_CNT registers indicate the SEC or DED errors.

2.6 Built-in Self-Test

PolarFire devices have a built-in self-test mechanism that can be used (optionally) to check the reliability and security of a device automatically upon power-up, or on-demand. The contents of all the non-volatile configuration memory segments, including security keys, security settings, and the FPGA fabric configuration, plus any memory pages declared as ROM by the user (all the write-protected pages) are tested using digest check. This test provides assurance against both natural and maliciously induced failures.

Digests are used for protecting data integrity. In the factory and user security segment, each logical page contains an automatically generated digest calculated dynamically at the time of programming the data to be written. For the FPGA fabric, the digest includes an overall value covering the data to be programmed. In addition, digests are calculated and stored for the sNVM pages marked as ROM. The digests can be verified on-demand by the user, either internally using a system service, or externally using a programming instruction. In addition, the user can automatically run digest checks on each power-up. The following section describes the various options to run the digest check.

An endurance limit specifies how many times a digest of the FPGA fabric can be run. See the *DS0141: PolarFire FPGA Datasheet* for more information about the FPGA configuration memory endurance limits. Therefore, depending upon how the system is deployed and used (for example, how often it is powered-up), the on-demand digest check may be more appropriate for testing the integrity of the FPGA fabric.

2.6.1 Power-On Reset Digest Check

PolarFire FPGA device may be configured to perform automatic digest checks while powering up the user design (after power-on reset) to check the integrity of the selected non-volatile memories. The user can specify, which digest to check. If any of the selected digest checks fails, a tamper event is generated to fabric for user action. The power-on digest check can be enabled and monitored using PF_TAMPER macro.

If, for example, the first-stage boot code for a soft CPU is stored in the sNVM, then the power-on reset digest check could be used to automatically provide a high-level of assurance that the code had not been changed, either through a natural or malicious event, since the digest was stored.

2.6.2 On-Demand Digest Check

The on-demand digest check recalculates and compares digests of selected non-volatile memories with the stored digests. A failure of any digest results in the tamper event being triggered. The on-demand digest check is invoked by calling digest check design system service. Note that the LSRAMs does not retain the user data after performing digest check on FPGA fabric. The status of the fabric digest check must be monitored by a state machine (for example, CoreABC core) implemented in the fabric. After checking the status of the fabric digest check, the state machine needs to issue a design reset or device reset depending on the design requirements. For more information about system services, see System Services chapter of *UG0753: PolarFire FPGA Security User Guide*.

2.6.3 Exporting Digests

The stored digests can be exported via a design system service, or the JTAG or SPI-slave interface. Read Digests service returns the stored digests. For more information about running system services, see *UG0753: PolarFire FPGA Security User Guide*.

2.7 Passivation and Monitoring of Unused Hard IP Blocks

This section describes how to passivate and monitor unused hard IP blocks for design assurance purposes in the safety-critical applications.

Note: All unused user I/Os are tri-stated with internal weak pull-up resistors.

2.7.1 System Controller Suspend Mode

In PolarFire devices, the system controller manages device and memory initialization, programming operations, and handles the system service requests. After power-on-reset or device reset (DEVRST_N) events, the system controller performs the initialization sequence of the I/O banks, FPGA fabric, and hard IP blocks.

For high-reliability applications, such as avionics applications, the system controller must be held in suspend mode after the completion of device initialization to protect the device from unintended device programming or zeroization of the device due to SEUs.

The system controller suspend mode is designed to provide an SEU immune reset state for the system controller. The system controller reset generation circuitry is designed with a triple modular redundancy (TMR) self-refreshing latch to provide SEU immunity. In this mode, the system controller is held in reset while its output ports to the rest of the system are forced to known and well-determined states.

The following figure shows the system controller reset generation circuitry.

Figure 3 • **System Controller Suspend Mode**

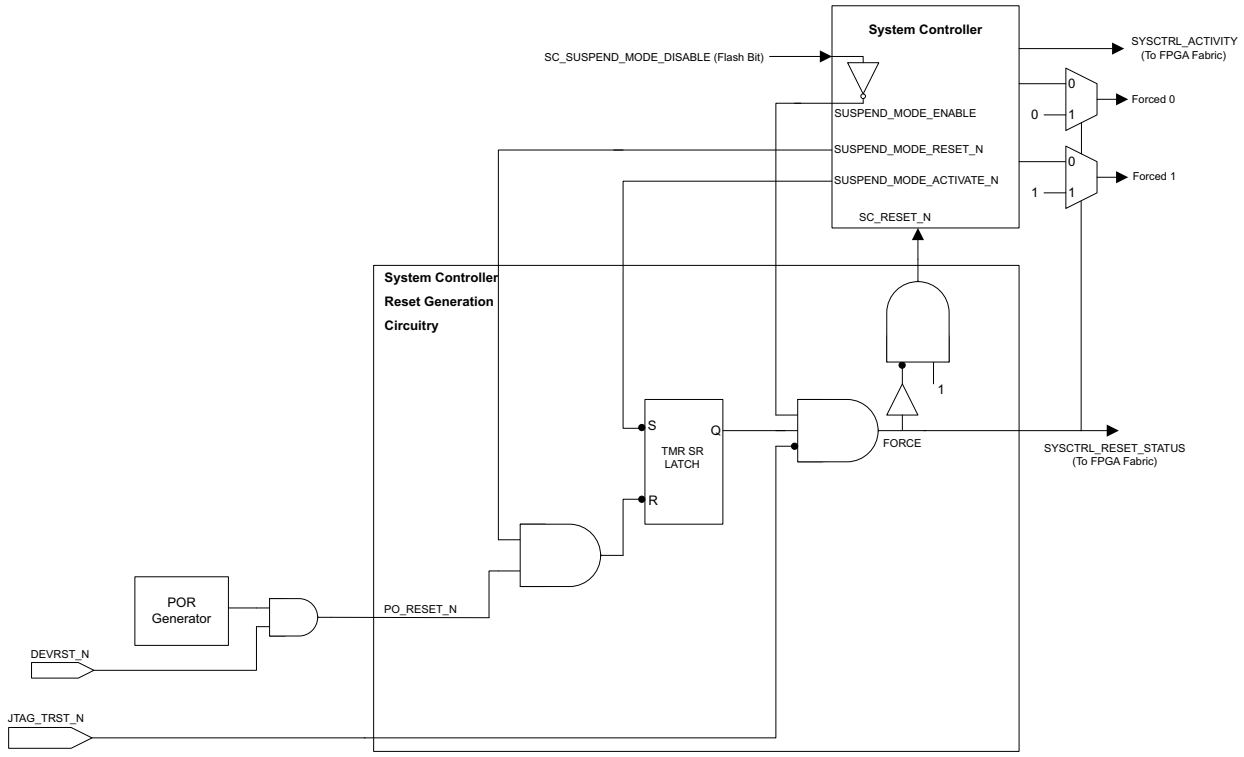


Table 3 • **System Controller Ports and Description**

Port	Direction	Description
SUSPEND_MODE_RESET_N	Output (Internal)	Active-low signal to reset the TMR SR Latch. Sourced from a system register.
SUSPEND_MODE_ACTIVATE_N	Output (Internal)	Active-low signal to set the TMR SR Latch. Sourced from a system register
SUSPEND_MODE_ENABLE	Output (Internal)	Enable signal for suspend mode. Sourced from device configuration flash bit.
SC_RESET_N	Input (Internal)	System controller reset signal. This is activated after the FORCE signal.
FORCE	Input (Internal)	Indicates that all the outputs should be switched to suspend mode.
SYSCTRL_RESET_STATUS	Output (To FPGA Fabric)	Direct connection of FORCE signal to the FPGA fabric indicating that FORCE is asserted and the system controller is in suspend mode. If SYSCTRL_RESET_STATUS = 1, the system controller suspend mode is enabled. If SYSCTRL_RESET_STATUS = 0, the system controller suspend mode is disabled.
SYSCTRL_ACTIVITY	Output (To FPGA Fabric)	Signal to FPGA fabric that is the logical OR of the System Controller HTRANS signals. This should always be low when the system controller is in suspend mode. When not in suspend mode, this signal is held high.

System controller suspend mode is controlled by a flash bit (SC_SUSPEND_MODE_DISABLE), which is set during device programming, and is not accessible either by external pin or from within the design. It is only accessed by the programming file loaded into the device, during programming. Since the SC_SUSPEND_MODE_DISABLE control bit is stored as a flash cell, it is immune to SEUs.

- If SC_SUSPEND_MODE_DISABLE = 1, the system controller suspend mode is disabled.
- If SC_SUSPEND_MODE_DISABLE = 0, the system controller suspend mode is enabled.

The suspend mode will be activated if enabled by the factory flash bit (SC_SUSPEND_MODE_DISABLE = 0) and the external JTAG reset is active. The system controller becomes active if the device is power-cycled or if a device reset (DEVRST_N) is applied, but it returns to suspend mode after the initialization sequence is completed. To restore normal operation, the device must be reprogrammed with the system controller suspend mode turned off (SC_SUSPEND_MODE_DISABLE = 1).

After the device has entered the suspend mode, the system controller is held in reset and cannot provide any system services and reprogramming services. To facilitate reprogramming of the device, the JTAG_TRST_N pin is used to gate the internal FORCE signal and releases the system controller from reset. In an avionics environment, JTAG_TRST_N must be held asserted to prevent JTAG circuitry from affecting the I/Os due to SEUs. Releasing JTAG_TRST_N puts the system controller out of reset and allows the device to be reprogrammed. When a programming mode instruction is loaded, the system controller sends a pulse on SUSPEND_MODE_RESET_N to clear the TMR latch so that the device can re-execute a normal boot sequence after programming is completed. Reprogramming via the system controller SPI (SC_SPI) interface is also possible. However, JTAG_TRST_N must be controlled by the external host.

The state of the system controller can be monitored by the FPGA fabric logic by reading the state of the SYSCTRL_RESET_STATUS signal and SYSCTRL_ACTIVITY signal. The future version of Libero software provides a macro (SC_STATUS) for system controller status monitoring from fabric logic.

2.7.2 User Cryptoprocessor

PolarFire "S" grade devices include a dedicated cryptoprocessor and NRBG (referred to as the User Cryptoprocessor) for data security applications. It provides complete support for Commercial National Security Algorithm (CNSA) suite and beyond, and includes side-channel analysis (SCA) resistant cryptographic countermeasures.

The User Cryptoprocessor in the "S" grade devices can be held in reset by tying its reset and other enable signals to zero. Here the reset and enable signals are directly driven from flash configuration cells which are immune to SEUs. Users can monitor AHB-slave and AHB-master interfaces, and BUSY signal for safety-critical design assurance purposes.

The User Cryptoprocessor is disabled using a SEU immune flash cell in the non "S" grade PolarFire devices. There is no way to read the status of that flash bit during runtime. If there is a requirement to monitor the status of User Cryptoprocessor at runtime then the only way to accomplish this is by using 'S' grade device and disable the User Cryptoprocessor by holding it in reset. In "S" grade devices the state of the User Cryptoprocessor can be monitored by monitoring AHB-slave and AHB-master interfaces, and BUSY signal using fabric logic.

The following table lists the PolarFire FPGA export classification using the MPF300T as an example. The MPF100T, MPF200T, and MPF500T device densities have identical classifications. This table is applicable to Extended commercial and Industrial temperature grade devices.

Table 4 • **PolarFire FPGA Export Classification**

Device Options	Data Security (S)	ECCN
MPF300T	No	3A991.d
MPF300TL	No	3A991.d
MPF300TS	Yes	5A002.a.1
MPF300TLS	Yes	5A002.a.1

2.7.3 PCIe Blocks

PolarFire devices include two PCIe controllers as hard IP blocks. The Libero software holds the unused PCIe hard IP blocks in reset using SEU immune flash bits. The status of these blocks can be monitored by reading the appropriate status registers using dynamic reconfiguration interface (DRI). Note that the hard IP blocks do not need to be instantiated in the design for reading the status registers using DRI.

The status of PCIe block reset can be monitored using "Soft Reset Logic Debug Information" register bits available in PCIE0_CTRL and PCIE1_CTRL address space.

See *PolarFire Device Register Map* for address map of PCIe control and status registers.

For information about how to use DRI for dynamic register configuration, see *AC475: PolarFire FPGA Dynamic Reconfiguration Interface Application Note*.

3 DO-254

Microsemi FPGA families have more than 20 years of proven performance across product deployments in hundreds of commercial aviation systems on Airbus, Boeing, and other aircraft.

These devices perform critical functions in design assurance level (DAL) A and B applications such as flight computers, braking systems, cockpit displays, engine controls, actuator systems, safety warning systems, cabin data management, and more.

Microsemi product families meet the stringent requirements of 10^6 device hours of operations, which are needed for the most safety-critical applications for DO-254 certification.

Microsemi product families offer dissimilar technologies (anti-fuse, flash, SONOS), which is ideal for safety-critical and redundant systems. Microsemi FPGAs address a critical high-reliability requirement for commercial aviation with zero Failure in Time (FIT) rate for FPGA configuration.

Microsemi provides validation artifacts to assist system level designers with DO-254 certification. For more questions about validation artifacts, contact aviation@microchip.com.

4 IEC 61508

Microsemi is offering an IEC61508 certified Functional Safety Data Package for the following families:

- ProASIC3, ProASIC3e, ProASIC3L
- IGLOO, IGLOOe, IGLOO nano, IGLOO PLUS
- SmartFusion

The functional safety packet is designed to assist with IEC 61508 certification and includes:

- Information on the relevant devices
- Libero SoC Design Suite v11.5 SP2 certified by TUV
- Libero SoC documentation
- Relevant IP cores and associated documentation
- IEC 61508 Safety Data Manual

The packet is available for purchase using the ordering code SAFETY-PKG-G3. For more information, see *www.microsemi.com/product-directory/reliability/4882-functional-safety#overview*.