SMARTFUSION®2
The Fully Configurable Cortex-M3

Peter Trott
Snr FAE – Microsemi
Peter.trott@microsemi.com
Microsemi SoC Product Roadmap
Increasing system features on differentiated flash technology

SMARTFUSION®

SMARTFUSION™
- Up to 500K gate FPGA
- 100MHz ARM Cortex-M3
- 10/100Ethernet, SPI/UART/I2C
- Integrated analog w/ ADC, DAC, V/I/T monitors

SMARTFUSION®
- Most secure, highest reliability, lowest power customizable SoC
- Integrated DSP processing
- Peripheral-rich MCU with higher performance CPU
- Expanded connectivity via many high speed serial interfaces
- 3.6x fabric density
- 2x fabric performance

ProASIC®
- Up to 3M Gate FPGA
- High Performance
- High IO count

IGLOO
- Up to 3M Gate FPGA
- Power as low as 2uW
- Small packages

© 2013 Microsemi Corporation
Microsemi SmartFusion2 SoC FPGA

SmartFusion2 SoC FPGAs extend our leadership in **security, reliability** and **low power** into mainstream applications

- **Leadership in Low Power FPGAs**
  - 50X lower power in Flash Freeze Mode
  - 5X lower power in Standby

- **Leadership in Secure FPGAs**
  - State of the art security enables root-of-trust applications
  - Radically transforms the usefulness of FPGAs in security applications

- **Leadership in Reliable FPGAs**
  - Only SoC FPGA with SEU immune fabric and processor
  - Reliability designed for safety critical and mission critical systems

- **Leadership in Real-Time FPGAs**
  - ARM® Cortex™-M3 real-time microcontroller
  - Flash*Freeze real-time power management
  - Instant on real-time availability
SmartFusion2 - Flash SoC FPGA w/ ARM Cortex-M3
Most Secure, Highest Reliability, Lowest Power

- 166MHz ARM® Cortex™-M3 w/ on chip eSRAM & eNVM
  - Includes ETM and Instruction Cache
  - Extensive peripherals CAN, TSE, USB
- Most Secure FPGA
  - DPA Hardened, AES256, SHA256, Random Number Generator
- Most Reliable FPGA
  - SEU immune Zero FIT Flash FPGA Configuration
  - SEU Protected Memories: eSRAMs, DDR Bridges (MSS, MDDR, FDDR), Instruction Cache, Ethernet, CAN and USB Buffers, PCIe, MMUART and SPI FIFOs
  - Hard 667 mbps DDR2/3 controllers with SECDED (aka ECC or EDAC) protection
  - Power-Up and On-Demand NVM Data Integrity Check
- Lowest Power FPGA
  - 1mW in flash-freeze mode
  - 10mW static power during operation
- 2x Fabric performance
- 16x 5Gbps SERDES, PCIe, XAUI / XGXS+ Native SERDES
- Integrated DSP processing blocks
- 150k LUT, 5Mbit SRAM, 4Mbit eNVM

© 2013 Microsemi Corporation

Power Matters.
SmartFusion2 Architecture
# SmartFusion2 Family

<table>
<thead>
<tr>
<th>Features</th>
<th>M2S005</th>
<th>M2S010</th>
<th>M2S025</th>
<th>M2S050</th>
<th>M2S090</th>
<th>M2S100</th>
<th>M2S150</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Logic/DSP</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Maximum Logic Elements (4LUT + DFF)*</td>
<td>6,060</td>
<td>12,084</td>
<td>27,696</td>
<td>56,340</td>
<td>86,316</td>
<td>99,512</td>
<td>146,124</td>
</tr>
<tr>
<td>Math Blocks (18x18)</td>
<td>11</td>
<td>22</td>
<td>34</td>
<td>72</td>
<td>84</td>
<td>160</td>
<td>240</td>
</tr>
<tr>
<td>PLLs and CCCs</td>
<td>2</td>
<td>6</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Security</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>AES256, SHA256, RNG</td>
<td>1 each</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ECC, PUF</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>MSS</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cortex-M3 + Instruction cache</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>eNVM (K Bytes)</td>
<td>128</td>
<td>256</td>
<td>512</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>eSRAM (K Bytes)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>eSRAM (K Bytes) Non SECDED</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Fabric Memory</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>LSRAM 18K Blocks</td>
<td>10</td>
<td>21</td>
<td>31</td>
<td>69</td>
<td>109</td>
<td>160</td>
<td>236</td>
</tr>
<tr>
<td>uSRAM1K Blocks</td>
<td>11</td>
<td>22</td>
<td>34</td>
<td>72</td>
<td>112</td>
<td>160</td>
<td>240</td>
</tr>
<tr>
<td>Total RAM (K bits)</td>
<td>191</td>
<td>400</td>
<td>592</td>
<td>1314</td>
<td>2074</td>
<td>3040</td>
<td>4488</td>
</tr>
<tr>
<td><strong>High Speed</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DDR Controllers (Count x Width)</td>
<td>1x18</td>
<td>2x36</td>
<td>1x18</td>
<td>2x36</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SERDES Lanes</td>
<td>0</td>
<td>4</td>
<td>8</td>
<td>4</td>
<td>8</td>
<td>16</td>
<td></td>
</tr>
<tr>
<td>PCIe End Points</td>
<td>0</td>
<td>1</td>
<td></td>
<td>2</td>
<td></td>
<td></td>
<td>4</td>
</tr>
<tr>
<td><strong>User I/Os</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>MSIO (3.3V)</td>
<td>115</td>
<td>123</td>
<td>157</td>
<td>139</td>
<td>306</td>
<td>292</td>
<td>292</td>
</tr>
<tr>
<td>MSIOD (2.5V)</td>
<td>28</td>
<td>40</td>
<td>40</td>
<td>62</td>
<td>40</td>
<td>106</td>
<td>106</td>
</tr>
<tr>
<td>DDRIO (2.5V)</td>
<td>66</td>
<td>70</td>
<td>70</td>
<td>176</td>
<td>66</td>
<td>176</td>
<td>176</td>
</tr>
<tr>
<td>Total User I/O</td>
<td>209</td>
<td>233</td>
<td>267</td>
<td>377</td>
<td>412</td>
<td>574</td>
<td>574</td>
</tr>
</tbody>
</table>

*Total logic may vary based on utilization of DSP and memories in your design. Please see the SmartFusion2 Fabric UG for details.
# SmartFusion2 Packaging Options

<table>
<thead>
<tr>
<th>Type</th>
<th>VF400</th>
<th>FG484</th>
<th>FG676</th>
<th>FG896</th>
<th>FC1152</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pitch (mm)</td>
<td>0.8</td>
<td>1.0</td>
<td>1.0</td>
<td>1.0</td>
<td>1.0</td>
</tr>
<tr>
<td>Length x Width (mm)</td>
<td>17x17</td>
<td>23x23</td>
<td>27x27</td>
<td>31x31</td>
<td>35x35</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Device</th>
<th>I/O Lanes</th>
<th>I/O Lanes</th>
<th>I/O Lanes</th>
<th>I/O Lanes</th>
<th>I/O Lanes</th>
</tr>
</thead>
<tbody>
<tr>
<td>M2S005</td>
<td>169* -</td>
<td>209* -</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>M2S010(T)</td>
<td>195 4</td>
<td>233 4</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>M2S025(T)</td>
<td>195 4</td>
<td>267 4</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>M2S050(T)</td>
<td>207 4</td>
<td>267 4</td>
<td>377 8</td>
<td></td>
<td></td>
</tr>
<tr>
<td>M2S090(T)</td>
<td></td>
<td></td>
<td>267 4</td>
<td>412* 4*</td>
<td></td>
</tr>
<tr>
<td>M2S100(T)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>574 8</td>
</tr>
<tr>
<td>M2S150(T)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>574 16</td>
</tr>
</tbody>
</table>

* Preliminary
Most Secure, Highest Reliability, Lowest power
Security: Design Security vs. Data Security

- Design Security
  - Making sure that the *FPGA Design* is protected and the IP owner’s security intent is respected

- Data Security
  - The *Application* programmed into the device meets its security objectives (authenticity, confidentiality, integrity, etc.)
Security: Why is FPGA Design Security Important?

- **Design Security**
  - **Cloning**
    - Someone copies your design without even necessarily having to understand how it works
  - **Overbuilding**
    - Your contract manufacturer fills your order… then makes a few for himself. After all, he has all the data!
  - **Reverse engineering**
    - Someone figures out how your design works, then uses or improves on what he learned
  - **Counterfeiting**
    - Illegal use of your brand name on a work-alike or cloned product
  - **Tampering**
    - Changing the design for malicious intent

- **Data Security**
  - The data being managed by the device stays secure
  - Without design/device security, it is virtually impossible to provide good data security
Security: Programmable Design Security

- Built-in Design Security on all Devices
  - Protection against tampering, cloning, overbuilding, reverse engineering and counterfeiting
  - Virtually no design or manufacturing overhead to build secure devices
  - Supply-chain assurance with digital Device Certificate

- Design Protection
  - Anti-tamper detection with active zeroization
  - Bitstream is always encrypted with AES-256
  - Secure programming with SHA-256 bitstream authentication
  - On-demand or power-up integrity check for data in all non-volatile memories

- Security Key Protection
  - Cryptography Research Incorporated (CRI) DPA resistant technology
  - Intrinsic-ID physically unclonable function (PUF) for state of the art key protection
  - Non-deterministic random bit generator (NRBG) for key generation
  - Non-volatile key storage in encrypted form

*State of the art security enables root-of-trust applications*
Security: Breakthrough Data Security

- Security Processing Accelerators for Advanced Cryptographic Applications
  - Cryptographic services built into the device accessible to users
  - AES-128/256, SHA-256, HMAC services
  - 384 bit Elliptical Curve Cryptographic (ECC) Engine
  - Challenge-response services using Pseudo-PUF and SRAM-PUF
  - Non-Deterministic Random Bit Generator service
  - Key-tree protocol-level construct for DPA-safe designs
  - Hardware firewalls available in the ARM AHB bus matrix

- Protection of Application-level Cryptographic Keys
  - Cryptography Research Incorporated (CRI) DPA patent license
  - Intrinsic-ID’s SRAM physically unclonable function (SRAM-PUF) technology

Radically transforms the usefulness of FPGAs in security applications
Reliability: The Most Reliable FPGA In the Industry

- Flash FPGA Fabric
  - SEU immune Zero FIT rate configuration

- All SoC Memory SEU Tolerant
  - Through built in error detection and correction techniques
    - Cortex-M3 Embedded Scratch Pad Memory, Ethernet, CAN and USB Buffers, PCIe FIFOs
  - Or SEU tolerant implementation
    - DDR Bridges (MSS, MDDR, FDDR), Instruction Cache, MMUART and SPI FIFOs

Alpha / Neutron particles strike routing matrix

Flash FPGA No Error
SRAM FPGA Functional Failure

Reliability for safety critical or mission critical systems
Low Power: Flash FPGA Advantage

Typical Competitors SRAM Cell

- Substantial Leakage per Cell
- Millions of Configuration Cells
- High Static Current

Flash FPGA inherently lower power

- 1000x lower leakage per cell
- Ultra Low Static Current
Low Power: Competitive Comparison

- Conditions
  - Equivalent device size
  - Worst case
  - Industrial

Source: Online Power Estimators
Low Power: Lowest Power FPGA

- **Flash FPGAs**
  - Lowest power without sacrificing performance

- **Flash*Freeze Ultra Low Power Mode 10mW**
  - Simple command to initiate Flash*Freeze mode
  - Entry to Flash*Freeze 100 µs
    - Retains all register and SRAM state in Flash*Freeze mode
    - Set I/O state during Flash*Freeze mode
    - MSS can be operational during Flash*Freeze with low frequency clock
      - I/O’s associated with MSS peripherals can be operational
  - Exit Flash*Freeze mode in 100 µs

**Example**

- 500 usec on – 10msec period
- ~50K instructions
- ~50K FPGA cycles
- ~10M MACs

~1/20th Power
Asic Subsystems
Micro-Controller Subsystem

- 166 MHz Cortex M3 with Instruction Cache
- 4 Port DDR bridge for data caching
- HS USB OTG
- 10/100/1000 Triple Speed Ethernet
- CAN 2.0a/b with 32 transmit and receive message buffers
- All memories SEU tolerant or SECDED.

- Equivalent to >25K LE’s
Multi Protocol 5Gb/s SERDES

- **Physical Media Attachment (PMA) Features**
  - Up to 16 lanes at up to 5Gbps
  - Dual based reference clocks with single-lane rate granularity
    - Tx and Rx PLLs programmable for each lane
    - Reference clock is shared per groups of two lanes
  - **Transmitter Features**
    - Programmable Pre/Post-Emphasis
    - Programmable Impedance
    - Programmable Amplitude
  - **Receiver Features**
    - Programmable Termination
    - Programmable Linear Equalization
  - **Built-In System Debug Features**
    - PRBS Gen/Chk
    - Constant Patterns
    - Loopbacks

Igloo2 Eye Diagram
SERDES Rate Granularity

Dual based reference clocks with single-lane rate granularity
- Tx and Rx PLLs programmable for each channel
- Reference clock is shared per groups of two lanes

Example Scenario
- REFCLK0 at 100MHz
  - Lane0 at 5.0Gbps
  - Lane1 at 5.0Gbps
- REFCLK1 at 125MHz
  - Lane2 at 2.5Gbps
  - Lane3 at 3.125Gbps

- Special connectivity for x4 usage using single reference clock.
SERDES / Hard IP architecture

PMA - Multi-Protocol 5G transceiver
Organized in blocks of x4
4 blocks max for 16 lanes
Hard IP - SERDES-Based Protocol Features

- PCI Express Gen1/Gen2 Controller
  - Single-Function Endpoint Configuration
  - x1, x2, x4 Link Widths
    - Static Lane Reversal support
  - 256 Bytes Maximum Payload Size
  - 64/32-Bit AXI/AHB Master/Slave Interfaces to FPGA
  - APB Interface for control/status

- XAUI/XGXS Physical Layer
  - Full compliance with IEEE 802.3
  - 64-Bit XGMII to FPGA at 156.25MHz
  - MDIO Interface for status/control (802.3ae-clause 45)
Embedded DDR Memory Interfaces

- Up to 2 High Speed 667Mb/s DDRx Memory Controllers plus PHY
  - MSS DDR available on all devices
    - Connects to embedded AHB and HPDMA Controller
    - Connects directly to FPGA Fabric
  - Fabric DDR available on larger devices
    - Connects directly to FPGA Fabric
- Supports LPDDR/DDR2/DDR3
  - Burst lengths of 2, 4, 8, or 16
- AMBA AXI or AHB interface
- SECDED Supported
- Supports Command and Data Reordering
- Supports Dynamic changing clock frequency in Self-Refresh.
- External Memory Configurations
  - Memory densities up to 4 GB
  - Maximum of 8 memory banks
  - 1, 2, or 4 ranks of memory
  - Bus Width Modes of x16, x18, x32, x36
FPGA Math Block

- 11 to 240 math blocks
- Supports 18 x 18 signed, 17 x 17 unsigned
- Internal cascade signals (44-bit CDIN and CDOUt) to support larger accumulators/adders/subtracters without extra logic
- Loopback capability to support adaptive filtering
- Adder support: \((A \times B) + C\) or \((A \times B) + D\) or \((A \times B) + C + D\)
### High Speed Systolic Architecture

Resource utilization and max clock rates are shown below

<table>
<thead>
<tr>
<th>Filter Parameters</th>
<th>Results</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Taps</strong></td>
<td><strong>Bit width</strong></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Coef</strong></td>
</tr>
<tr>
<td>16</td>
<td>18</td>
</tr>
<tr>
<td>24</td>
<td>18</td>
</tr>
<tr>
<td>48</td>
<td>18</td>
</tr>
<tr>
<td>72</td>
<td>18</td>
</tr>
</tbody>
</table>

Commercial Temp
Resource Cautious Transposed Architecture

Resource utilization and max clock rates are shown below

<table>
<thead>
<tr>
<th>Filter Parameters</th>
<th>Results</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>MACC</td>
</tr>
<tr>
<td></td>
<td>Comb</td>
</tr>
<tr>
<td>Taps</td>
<td>Coef</td>
</tr>
<tr>
<td>24</td>
<td>18</td>
</tr>
<tr>
<td>32</td>
<td>18</td>
</tr>
<tr>
<td>48</td>
<td>18</td>
</tr>
<tr>
<td>72</td>
<td>18</td>
</tr>
</tbody>
</table>

Commercial Temp
Logic Element

- A fully permutable 4-input LUT
- A dedicated carry chain based on the carry look-ahead technique
- A separate flip-flop which can be used independently from the LUT
SmartFusion2 Ecosystem of Industry Leaders

ARM Connected Community

ARM

Compile/Debug

EDA

SAFE

RTOS®

ModelSim®

SYNOPSYS®

Synplify Pro®

Symphony Model Compiler

MathWorks®

MATLAB®

Simulink®

Keil®

IAR Systems

LaTourbach Development Tools

Micrium

uC/OS-III™

EmCraft Systems

Embedded Linux

SAFERTOS®

Trusted Ecosystem Partners accelerate design in time with IP and Ease of Use
SmartFusion2 System Builder

- System Builder Wizard
  - Asks the user basic questions on system architecture
  - Adds any additional peripherals in the fabric
  - Walks through configuration options for each selected feature
  - Builds complete base system and API – correct by design

Accelerates architecture design, so engineers can focus on their value add
SmartFusion2 IP & Solutions

- Leverage over 150 IP Cores in FPGA fabric
  - Peripherals: GPIO, I2C, SPI, Timers, UARTs, PWM
  - Cryptography: FIPS 140-2 compliant cores
  - Communications: MIL-STD-1553, ARINC 429, LPC, AXI, AXI to AHB
  - DSP: RS Encode/Decode, FIR and FFT using Math Blocks
  - SERDES & Protocols: JESD204, EPCS, RGMII

- Next Generation Solutions
  - Micro Power Manager (MPM)
  - Motor Control
Microsemi SmartFusion2 SoC FPGA

SmartFusion2 SoC FPGAs extend our leadership in **security, reliability** and **low power** into mainstream applications

- **Leadership in Low Power FPGAs**
  - 50X lower power in Flash Freeze Mode
  - 5X lower power in Standby

- **Leadership in Secure FPGAs**
  - State of the art security enables root-of-trust applications
  - Radically transforms the usefulness of FPGAs in security applications

- **Leadership in Reliable FPGAs**
  - Only SoC FPGA with SEU immune fabric and processor
  - Reliability designed for safety critical and mission critical systems

- **Leadership in Real-Time FPGAs**
  - ARM® Cortex™-M3 real-time microcontroller
  - Flash*Freeze real-time power management
  - Instant on real-time availability
SMARTFUSION® 2
Most Secure, Highest Reliability, Lowest Power