

SmartFusion2 SoC FPGA Data Security Devices Product Brief

Microsemi's SmartFusion² SoC FPGAs integrate fourth generation flash-based FPGA fabric, an ARM[®] Cortex[™]-M3 processor, and high-performance communications interfaces on a single chip. The SmartFusion2 family is the industry's lowest power, most reliable and highest security programmable logic solution. SmartFusion2 FPGAs offer up to 3.6X the gate density, up to 2X the performance of previous flash-based FPGA families, and includes multiple memory blocks and multiply accumulate blocks for DSP processing. The 166 MHz ARM Cortex-M3 processor is enhanced with an embedded trace macrocell (ETM), memory protection unit (MPU), 8 kbyte instruction cache, and additional peripherals, including controller area network (CAN), Gigabit Ethernet, and high speed universal serial bus (USB). High speed serial interfaces include PCI EXPRESS[®] (PCIe[®]), 10 Gbps attachment unit interface (XAUI) / XGMII extended sublayer (XGXS) plus native serialization/deserialization (SERDES) communication, while double data rate 2 (DDR2/DDR3) memory controllers provide high speed memory interfaces.

SmartFusion2 Family

Reliability

- Single Event Upset (SEU) Immune
 - Zero FIT FPGA Configuration Cells
- Junction Temperature: 125°C – Military Temperature, 100°C – Industrial Temperature, 85°C – Commercial Temperature
- Single Error Correct Double Error Detect (SECEDED) Protection on the Following:
 - Ethernet Buffers
 - CAN Message Buffers
 - Cortex-M3 Embedded Scratch Pad Memory (eSRAMs)
 - USB Buffers
 - PCIe Buffer
 - DDR Memory Controllers with Optional SECEDED Modes
- Buffers Implemented with SEU Resistant Latches on the Following:
 - DDR Bridges (MSS, MDDR, FDDR)
 - Instruction Cache
 - MMUART FIFOs
 - SPI FIFOs
- NVM Integrity Check at Power-Up and On-Demand
- No External Configuration Memory Required—Instant-On, Retains Configuration When Powered Off

Security

- Design Security Features (available on all devices)
 - Intellectual Property (IP) Protection Through Unique Security Features and Use Models New to the PLD Industry
 - Encrypted User Key and Bitstream Loading, Enabling Programming in Less-Trusted Locations

- Supply-Chain Assurance Device Certificate
- Enhanced Anti-Tamper Features
- Zeroization
- Data Security Features (available on premium devices)
 - Non-Deterministic Random Bit Generator (NRBG)
 - User Cryptographic Services (AES-256, SHA-256, Elliptical Curve Cryptographic (ECC) Engine)
 - User Physically Unclonable Function Enrollment and Regeneration
 - CRI Pass-Through DPA Patent Portfolio License
 - Hardware Firewalls Protecting Microcontroller Subsystem (MSS) Memories



Low Power

- Low Static and Dynamic Power
 - Flash*Freeze Mode for Fabric
- Power as low as 13 mW/Gbps per lane for SERDES devices
- Up to 50% lower total power than competing SoC devices

High-Performance FPGA

- Efficient 4-Input LUTs with Carry Chains for High-Performance and Low Power
- Up to 236 Blocks of Dual-Port 18 Kbit SRAM (Large SRAM) with 400 MHz Synchronous Performance (512 x 36, 512 x 32, 1 kbit x 18, 1 kbit x 16, 2 kbit x 9, 2 kbit x 8, 4 kbit x 4, 8 kbit x 2, or 16 kbit x 1)
- Up to 240 Blocks of Three-Port 1 Kbit SRAM with 2 Read Ports and 1 Write Port (micro SRAM)
- High-Performance DSP Signal Processing
 - Up to 240 Fast Mathblocks with 18 x 18 Signed Multiplication, 17 x 17 Unsigned Multiplication and 44-Bit Accumulator

Microcontroller Subsystem (MSS)

- Hard 166 MHz 32-Bit ARM Cortex-M3 Processor
 - 1.25 DMIPS/MHz
 - 8 Kbyte Instruction Cache
 - Embedded Trace Macrocell (ETM)
 - Memory Protection Unit (MPU)
 - Single Cycle Multiplication, Hardware Divide
 - JTAG Debug (4 wires), Serial Wire Debug (SWD, 2 Wires), and Serial Wire Viewer (SWV) Interfaces
- 64 KB Embedded SRAM (eSRAM)
- Up to 512 KB Embedded Nonvolatile Memory (eNVM)
- Triple Speed Ethernet (TSE) 10/100/1000 Mbps MAC
- USB 2.0 High Speed On-The-Go (OTG) Controller with ULPI Interface
- CAN Controller, 2.0B Compliant, Conforms to ISO11898-1, 32 Transmit and 32 Receive Buffers
- Two Each: SPI, I²C, Multi-Mode UARTs (MMUART) Peripherals
- Hardware Based Watchdog Timer
- 1 General Purpose 64-Bit (or two 32-bit) Timer(s)
- Real-Time Calendar/Counter (RTC)
- DDR Bridge (4 Port Data R/W Buffering Bridge to DDR Memory) with 64-Bit AXI Interface
- Non-Blocking, Multi-Layer AHB Bus Matrix Allowing Multi-Master Scheme Supporting 10 Masters and 7 Slaves
- Two AHB-Lite/APB3 Interfaces to FPGA Fabric (Master/Slave Capable)
- Two DMA Controllers to Offload Data Transactions from the Cortex-M3 Processor
 - 8-Channel Peripheral DMA (PDMA) for Data Transfer Between MSS Peripherals and Memory
 - High-Performance DMA (HPDMA) for Data Transfer Between eSRAM and DDR Memories

Clocking Resources

- Clock Sources
 - Up to Two High Precision 32 KHz to 20 MHz Main Crystal Oscillator
 - 1 MHz Embedded RC Oscillator
 - 50 MHz Embedded RC Oscillator
- Up to 8 Clock Conditioning Circuits (CCCs) with Up to 8 Integrated Analog PLLs
 - Output Clock with 8 Output Phases and 45° Phase Difference (Multiply/Divide, and Delay Capabilities)
 - Frequency: Input 1 MHz to 200 MHz, Output 20 MHz to 400 MHz

High Speed Serial Interfaces

- Up to 16 SERDES Lanes, Each Supporting:
 - XGXS/XAUI Extension (To Implement a 10 Gbps (XGMII) Ethernet PHY Interface)
 - Native SERDES Interface Facilitates Implementation of Serial RapidIO in Fabric or an SGMII Interface to the Ethernet MAC in MSS
 - PCI Express (PCIe) Endpoint Controller
 - x1, x2, x4 Lane PCI Express Core
 - Up to 2 Kbytes Maximum Payload Size
 - 64-Bit/32-Bit AXI and 64-Bit/32-Bit AHB Master and Slave Interfaces to the Application Layer

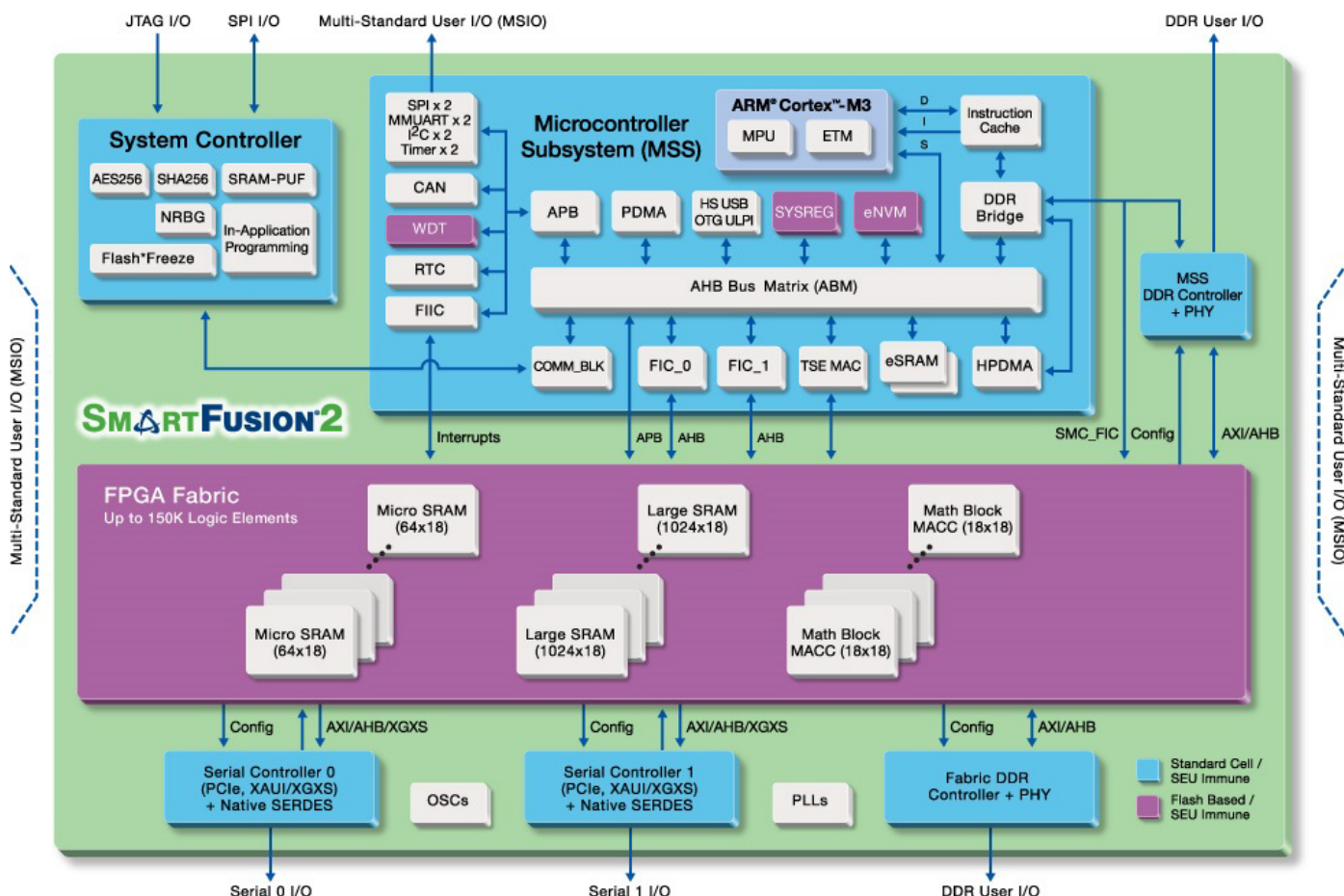
High Speed Memory Interfaces

- Up to 2 High Speed DDRx Memory Controllers
 - MSS DDR (MDDR) and Fabric DDR (FDDR) Controllers
 - Supports LPDDR/DDR2/DDR3
 - Maximum 333 MHz DDR Clock Rate
 - SECEDED Enable/Disable Feature
 - Supports Various DRAM Bus Width Modes, x8, x9, x16, x18, x32, x36
 - Supports Command Reordering to Optimize Memory Efficiency
 - Supports Data Reordering, Returning Critical Word First for Each Command
- SDRAM Support through the SMC_FIC and Additional Soft SDRAM Memory Controller

Operating Voltage and I/Os

- 1.2 V Core Voltage
- Multi-Standard User I/Os (MSIO/MSIOD)
 - LVTTTL/LVCMOS 3.3 V (MSIO Only)
 - LVCMOS 1.2 V, 1.5 V, 1.8 V, 2.5 V
 - DDR (SSTL2_1, SSTL2_2)
 - LVDS, MLVDS, Mini-LVDS, RSDS Differential Standards
 - PCI
 - LVPECL (Receiver Only)
- DDR I/Os (DDRIO)
 - DDR2, DDR3, LPDDR, SSTL2, SSTL18, HSTL
 - LVCMOS 1.2 V, 1.5 V, 1.8 V, 2.5 V
- Market Leading Number of User I/Os with 5G SERDES

SmartFusion2 SoC FPGA Block Diagram



Acronyms

AES	Advanced Encryption Standard	MMUART	Multi-Mode UART
AHB	Advanced High-Performance Bus	MPU	Memory Protection Unit
APB	Advanced Peripheral Bus	MSIO	Multi-Standard I/O
AXI	Advanced eXtensible Interface	MSS	Microcontroller Subsystem
COMM_BLK	Communication Block	PUF	Physically Unclonable Function
DDR	Double Data Rate	SECDED	Single Error Correct Double Error Detect
DPA	Differential Power Analysis	SEU	Single Event Upset
ECC	Elliptic Curve Cryptography	SHA	Secure Hashing Algorithm
EDAC	Error Detection And Correction	SMC_FIC	Soft Memory Controller
ETM	Embedded Trace Macrocell	TSE	Triple Speed Ethernet (10/100/1000 Mbps)
FDDR	DDR2/3 Controller in FPGA Fabric	ULPI	UTMI + Low Pin Interface
FIC	Fabric Interface Controller	UTMI	USB 2.0 Transceiver Macrocell Interface
FIIC	Fabric Interface Interrupt Controller	WDT	Watchdog Timer
HS USB OTG	High Speed USB 2.0 On-The-Go	XAUI	10 Gbps Attachment Unit Interface
IAP	In-Application Programming	XGMII	10 Gigabit Media Independent Interface
MACC	Multiply-Accumulate	XGXS	XGMII Extended Sublayer
MDDR	DDR2/3 Controller in MSS		

Table 1 • SmartFusion2 SoC FPGA Product Family

Features		M2S005S	M2S010 (T/TS)	M2S025 (T/TS)	M2S050 (T/TS)	M2S090 (T/TS)	M2S100 (T/TS)	M2S150 (T/TS)
Logic/DSP	Maximum Logic Elements (4LUT + DFF)*	6,060	12,084	27,696	56,340	86,316	99,512	146,124
	Mathblocks (18 x18)	11	22	34	72	84	160	240
	Fabric Interface Controllers (FICs)	1			2	1	2	
	PLLs and CCCs	2		6			8	
	Security	AES256, SHA256, RNG				AES256, SHA256, RNG, ECC, PUF		
MSS	Cortex-M3 + Instruction cache	Yes						
	eNVM (kbytes)	128	256			512		
	eSRAM (kbytes)	64						
	eSRAM (kbytes) Non SECCDED	80						
	CAN, 10/100/1000 Ethernet, HS USB	1 each						
	Multi-Mode UART, SPI, I ² C, Timer	2 each						
Fabric Memory	LSRAM 18K Blocks	10	21	31	69	109	160	236
	uSRAM1K Blocks	11	22	34	72	112	160	240
	Total RAM (kbits)	191	400	592	1314	2074	3040	4488
High Speed	DDR Controllers (Count x Width)	1x18			2x36	1x18	2x36	
	SERDES Lanes (T)	0	4		8	4	8	16
	PCIe Endpoints	0	1		2			4
User I/Os	MSIO (3.3 V)	115	123	157	139	309	292	292
	MSIOD (2.5 V)	28	40	40	62	40	106	106
	DDRIO (2.5 V)	66	70	70	176	76	176	176
	Total User I/O	209	233	267	377	425	574	574
Grades	Commercial(C), Industrial(I), Military(M)	C,I	C,I,M					

Note: * Total logic may vary based on utilization of DSP and memories in your design. Refer to the [SmartFusion2 Fabric UG](#) for details.

*Feature availability is package dependent, refer to [Table 3](#).

I/Os Per Package

Table 2 • I/Os per Package and Package Options

Package Options																				
Type	FCS325		VF256		FCS536		VF400		FCV484		VQ144		FG484		FG676		FG896		FC1152	
Pitch (mm)	0.5		0.8		0.5		0.8		0.8		0.5		1.0		1.0		1.0		1.0	
Length x Width (mm)	11x11		14x14		16x16		17x17		19x19		20x20		23x23		27x27		31x31		35x35	
Device	I/O	Lanes	I/O	Lanes	I/O	Lanes	I/O	Lanes	I/O	Lanes	I/O	Lanes	I/O	Lanes	I/O	Lanes	I/O	Lanes	I/O	Lanes
M2S005S			161	–			171	–			84	–	209	–						
M2S010 (T/TS) ³			138	2			195	4			84	–	233	4						
M2S025 (T/TS) ³	180	2	138	2			207	4					267	4						
M2S050 (T/TS) ³	200	2					207	4					267	4			377	8		
M2S090 (T/TS) ^{2,3}	180	4											267	4	425	4				
M2S100 (T/TS) ⁴																			574	8
M2S150 (T/TS) ⁴					293	4			273 ¹	4 ¹									574	16

Notes:

- Preliminary
 - 090 FCS325 is 11x13.5 package dimension
 - Mil Temp 010/025/050/090 devices are only available in the FG484 package
 - Mil Temp 100/150 devices are only available in the FC1152 package
- Pin compatible to other devices in the same package

Features per Device and Package Combination

Table 3 • Features per Device Package Combination

Features											
Package	Devices	MDDR	FDDR	Crystal Oscillators	5G ⁶ SERDES Lanes	PCIe Endpoints	USB	MSIO (3.3 V Max)	MSIOD (2.5 V Max)	DDRIO (2.5 V Max)	Total User I/O
VQ144 ⁵	M2S005S	—	—	2	—	—	1	52	9	23	84
	M2S010S	—	—	2	—	—	1	50	11	23	84
VF256	M2S005S	—	—	2	—	—	1	119	12	30	161
	M2S010 (T/TS)	x18 ¹	—	2	2	1	1	66	8	64	138
	M2S025 (T/TS)	x18 ¹	—	2	2	1	1	66	8	64	138
FCS325	M2S025 (T/TS)	x18 ¹	—	2	2	1	1	94	22	64	180
	M2S050 (T/TS)	x18 ²	—	1	2	1	0	90	22	88	200
	M2S090 (T/TS)	x18 ¹	—	2	4	2	1	104	12	64	180
VF400	M2S005S	x18 ¹	—	2	—	—	1	79	28	64	171
	M2S010 (T/TS)	x18 ¹	—	2	4	1	1	99	32	64	195
	M2S025 (T/TS)	x18 ¹	—	2	4	1	1	111	32	64	207
	M2S050 (T/TS)	x18 ²	—	1	4	1	0	87	32	88	207
FCV484 ⁵	M2S150 (T/TS)	x18 ¹	x18 ¹	2	4	4	1	TBD	TBD	TBD	273
FG484	M2S005S	x18 ¹	—	2	—	—	1	115	28	66	209
	M2S010 (T/TS)	x18 ¹	—	2	4	1	1	123	40	70	233
	M2S025 (T/TS)	x18 ¹	—	2	4	1	1	157	40	70	267
	M2S050 (T/TS)	x18 ²	—	1	4	1	0	105	40	122	267
	M2S090 (T/TS)	x18 ¹	—	2	4	2	1	157	40	70	267
FCS536	M2S150 (T/TS)	x18 ¹	x18 ¹	2	4	4	1	151	16	126	293
FG676	M2S090 (T/TS)	x18 ¹	—	2	4	2	1	309	40	76	425
FG896	M2S050 (T/TS)	x36 ⁴	x36 ⁴	1	8	2	1	139	62	176	377

Table 3 • Features per Device Package Combination (continued)

Package	Devices	MDDR	FDDR	Crystal Oscillators	5G ⁶ SERDES Lanes	PCIe Endpoints	USB	MSIO (3.3 V Max)	MSIOD (2.5 V Max)	DDRIO (2.5 V Max)	Total User I/O
FC1152	M2S100 (T/TS)	x36 ³	x36 ³	2	8	2	1	292	106	176	574
	M2S150 (T/TS)	x36 ³	x36 ³	2	16	4	1	292	106	176	574

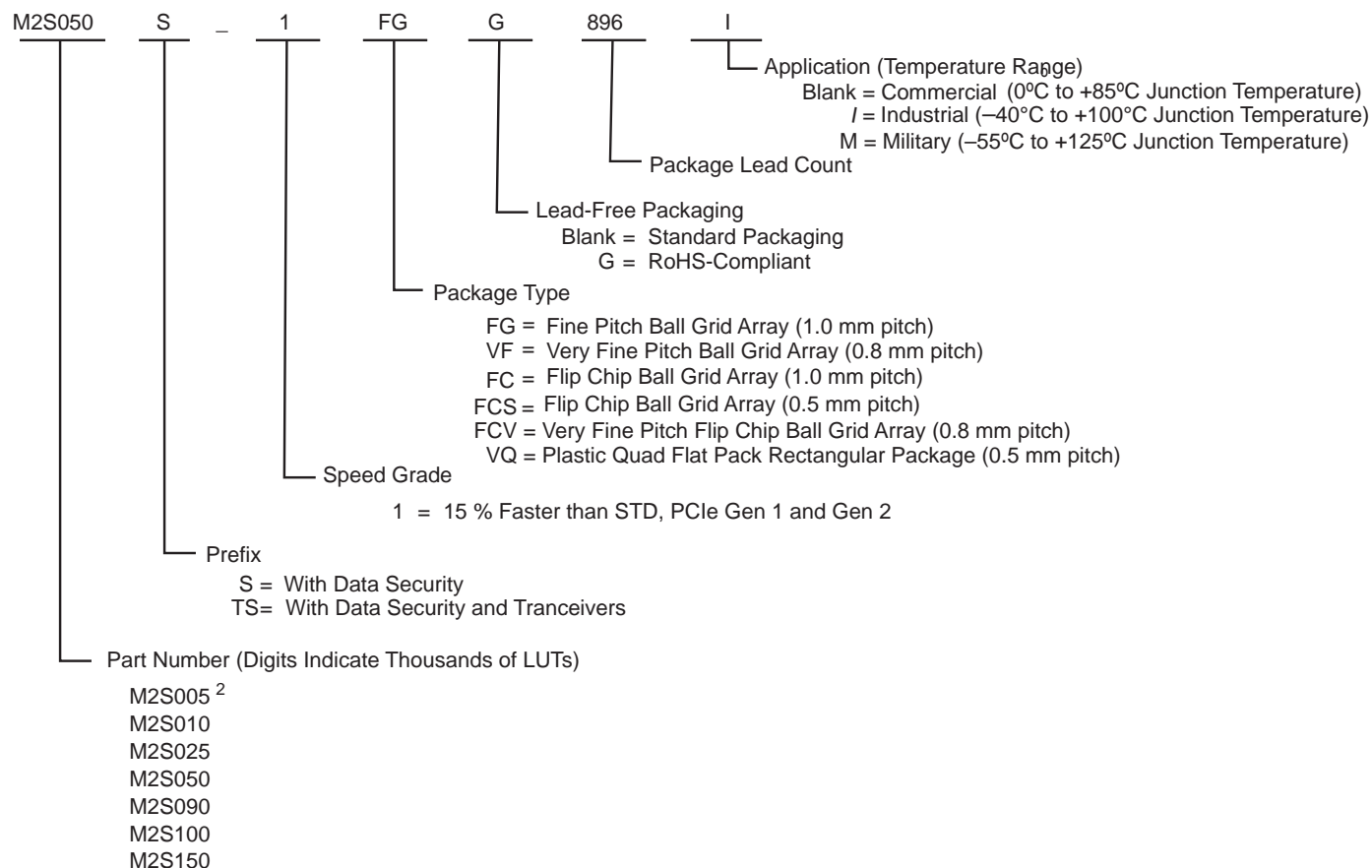
Notes:

1. DDR supports x18, x16, x9, and x8 modes
2. DDR supports x18 and x16 modes
3. DDR supports x36, x32, x18, x16, x9, and x8 modes
4. DDR supports x36, x32, x18, and x16 modes
5. Preliminary
6. Maximum SERDES rate for Mil temp devices is 3.125 Gbps

Table 4 • Programming Interfaces Available

Package	Devices	JTAG	SPI_0	Flash_GOLDEN_N	System Controller SPI Port
VQ144	M2S005S	Yes	Yes	No	No
	M2S010S	Yes	Yes	No	No
VF256	M2S005S	Yes	Yes	Yes	Yes
	M2S010 (T/TS)	Yes	Yes	Yes	No
	M2S025 (T/TS)	Yes	Yes	Yes	No
FCS325	M2S025 (T/TS)	Yes	Yes	No	No
	M2S050 (T/TS)	Yes	Yes	No	No
	M2S090 (T/TS)	Yes	Yes	No	No
VF400	M2S005S	Yes	Yes	Yes	Yes
	M2S010 (T/TS)	Yes	Yes	Yes	Yes
	M2S025 (T/TS)	Yes	Yes	Yes	Yes
	M2S050 (T/TS)	Yes	No	Yes	Yes
FCV484	M2S150 (T/TS)	Yes	Yes	Yes	Yes
FG484	M2S005S	Yes	Yes	Yes	Yes
	M2S010 (T/TS)	Yes	Yes	Yes	Yes
	M2S025 (T/TS)	Yes	Yes	Yes	Yes
	M2S050 (T/TS)	Yes	No	Yes	Yes
	M2S090 (T/TS)	Yes	Yes	Yes	Yes
FCS536	M2S150 (T/TS)	Yes	Yes	Yes	Yes
FG676	M2S090 (T/TS)	Yes	Yes	Yes	Yes
FG896	M2S050 (T/TS)	Yes	No	Yes	Yes
FC1152	M2S100 (T/TS)	Yes	Yes	Yes	Yes
	M2S150 (T/TS)	Yes	Yes	Yes	Yes

SmartFusion2 Ordering Information



Note: M2S005S devices are not available with Transceivers or in the Military temperature grade

SmartFusion2 Military Temperature Device Offering

Table 5 • SmartFusion2 Military Temperature Device Offering

M2S010TS-1FG484M	M2S010TS-1FGG484M
M2S025TS-1FG484M	M2S025TS-1FGG484M
M2S050TS-1FG484M	M2S050TS-1FGG484M
M2S090TS-1FG484M	M2S090TS-1FGG484M
M2S100TS-1FC1152M	M2S100TS-1FCG1152M
M2S150TS-1FC1152M	M2S150TS-1FCG1152M

Note: Gold Wire bonds are available for the FG484 package by appending X399 to the part number when ordering. For example: M2S090TS-1FG484MX399.

SmartFusion2 Device Status

Refer to the [SmartFusion2 Datasheet](#) for device status.

SmartFusion2 Datasheet and Pin Descriptions

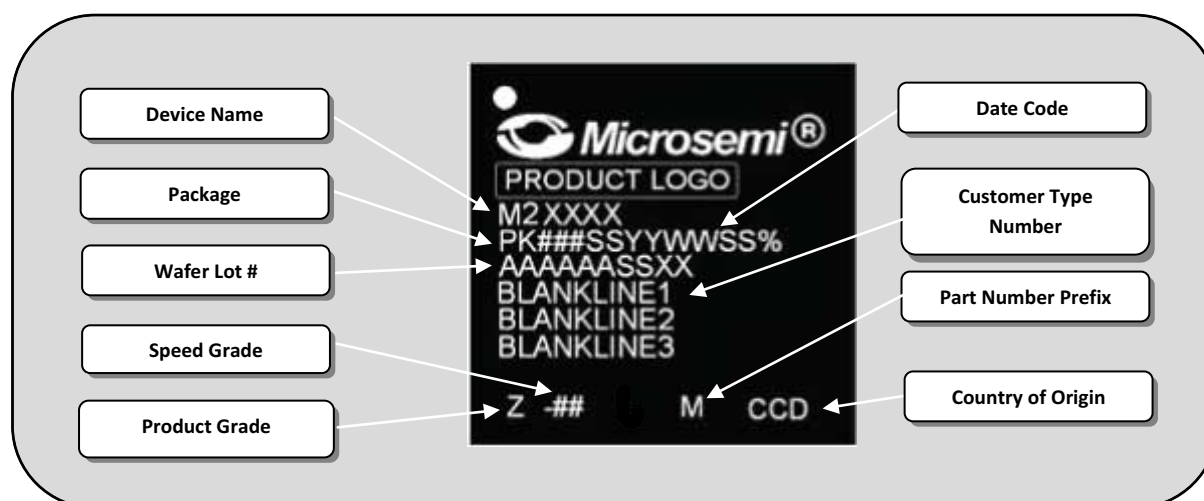
The datasheet and pin descriptions are published separately:

[SmartFusion2 Datasheet](#)

[SmartFusion2 Pin Descriptions](#)

Marking Specification Details

Microsemi normally topside marks the full ordering part number on each device. The figure below provides the details for each character code present on Microsemi's SmartFusion2 SoC FPGA devices.



Description:

- Device Name (M2XXXX): M2S for SmartFusion2 Devices
Example: M2S050
- Package (PK###): Available Package as below
 PK: Package code:
 FG(G): Fine Pitch BGA, 1.00 mm pitch
 FC(G): Flip Chip Fine Pitch BGA with Metal LID on top, 1.00 mm pitch
 FCV(G): Flip Chip Very Fine Pitch BGA with Metal LID on top, 0.8 mm pitch
 FCS(G): Flip Chip Ultra Fine Pitch BGA with Metal LID on top, 0.5 mm pitch
 VF(G): Very Fine Pitch BGA, 0.8 mm pitch
 VQ(G): Ultra Fine Pitch Thin Quad Flat Pack, 0.5 mm pitch
 ###: Number of Pins: Can be three or four digits. For example, 144, 256, or 1152
- Wafer Lot (AAAAAAXX): Microsemi Wafer lot #
 AAAAAA: Wafer lot number
 XX: One or two characters revision code
- Speed Grade (-##): Speed Binning Number
 Blank: Standard speed grade
 -1: -1 Speed grade

- Product grade (Z): Product Grade; assigned as follows
 - C: Commercial
 - ES: Engineering Samples
 - I: Industrial
 - M: Military Temperature
 - PP: Pre Production
- Date Code (YYWW): Assembly Date Code
 - YY: Last two digits for seal year
 - WW: Work week the part was sealed
 - SS: Two blank spaces
 - %: Can be digital number or character for new product
- Customer Type Number: As specified on lot traveler
 - GW: Gold Wire bond
- Part number Prefix: Part number prefix, assigned as below
 - S: Advanced Security
 - TS: Transceivers and Advanced Security
- Country of Origin (CCD): Assembly house country Location
 - Country name: Country Code
 - China: CHN
 - Hong Kong: HKG
 - Japan: JPN
 - Korea, South: KOR
 - Philippines: PHL
 - Taiwan: TWN
 - Singapore: SGP
 - United States: USA
 - Malaysia: MYS

1 – SmartFusion2 Device Family Overview

Microsemi's SmartFusion2 SoC FPGAs integrate fourth generation flash-based FPGA fabric, an ARM Cortex-M3 processor, and high-performance communications interfaces on a single chip. The SmartFusion2 FPGA is the industry's lowest power, the most secure, and has the highest reliability of any programmable logic solution. SmartFusion2 FPGAs offer up to 3.6X the gate density and up to 2X the performance of previous flash-based FPGA families and includes multiple memory blocks and multiply accumulate blocks for DSP processing. The 166 MHz ARM Cortex-M3 processor is enhanced with ETM and 8 kbyte instruction cache, and additional peripherals including CAN, Gigabit Ethernet, and high speed USB. High speed serial interfaces enable PCIe, XAUI / XGXS plus native SERDES communication while DDR2/DDR3 memory controllers provide high speed memory interfaces.

SmartFusion2 Chip Layout

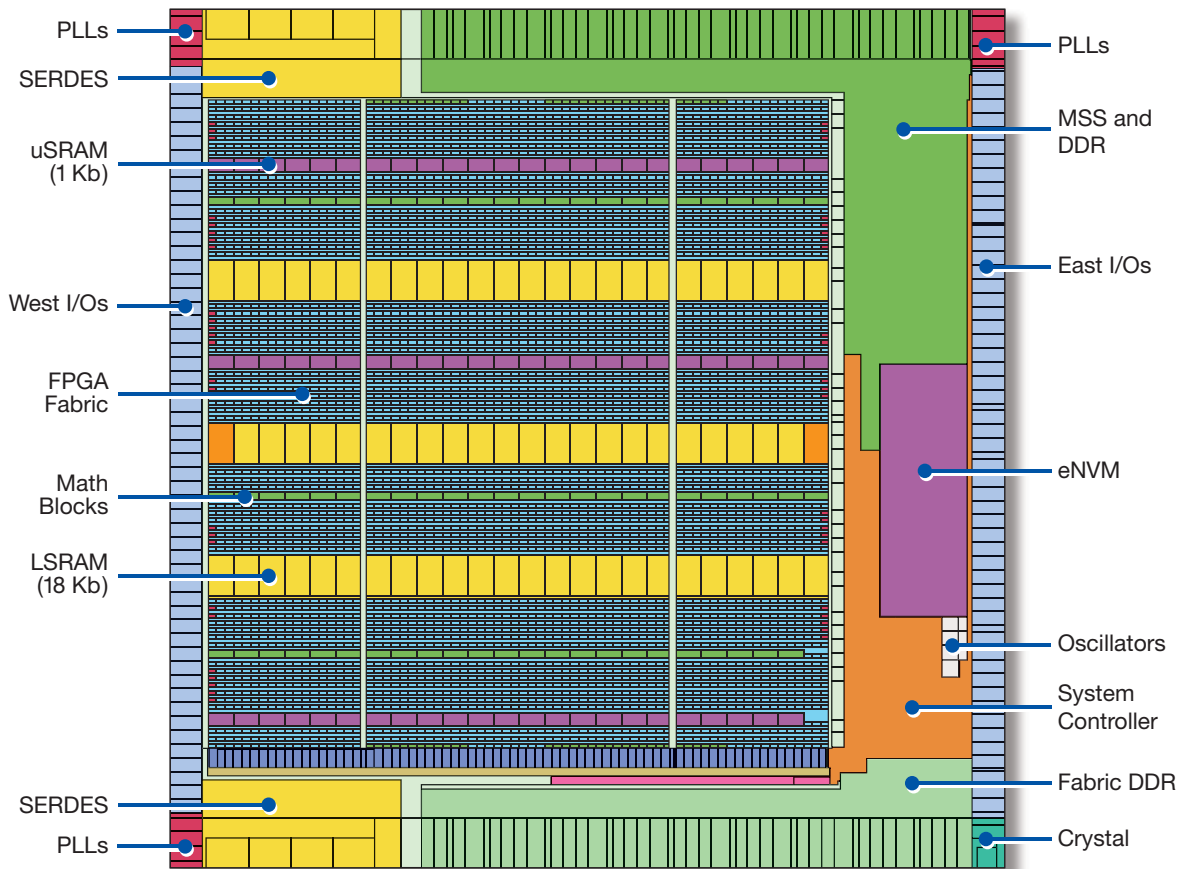


Figure 1-1 • SmartFusion2 Chip Layout

Reliability

SmartFusion2 flash-based fabric has zero FIT configuration rate due to its single event upset (SEU) immunity, which is critical in reliability applications. The flash fabric also has the advantage that no external configuration memory is required, making the device instant-on; it retains configuration when powered off. To complement this unique FPGA capability, SmartFusion2 devices add reliability to many other aspects of the device. Single Error Correct Double Error Detect (SECEDED) protection is implemented on the Cortex-M3 embedded scratch pad memory, Ethernet, CAN and USB buffers, and is optional on the DDR memory controllers. This means that if a one-bit error is detected, it will be corrected. Errors of more than one bit are detected only and not corrected. SECEDED error signals are brought to the FPGA fabric to allow the user to monitor the status of these protected internal memories. Other areas of the architecture are implemented with latches, which are more resistant to SEUs. Therefore, no correction is needed in these locations: DDR bridges (MSS, MDDR, FDDR), instruction cache and MMUART, SPI, and PCIe FIFOs.

Highest Security Devices

Building further on the intrinsic security benefits of flash nonvolatile memory technology, the SmartFusion2 family incorporates essentially all the legacy security features that made the original SmartFusion[®], Fusion[®], IGLOO[®], and ProASIC[®]3 third-generation flash FPGAs and cSoCs the gold standard for secure devices in the PLD industry. In addition, the fourth-generation flash-based SmartFusion2 SoC FPGAs add many unique design and data security features and use models new to the PLD industry.

Design Security vs. Data Security

When classifying security attributes of programmable logic devices (PLDs), a useful distinction is made between design security and data security.

Design Security

Design security is protecting the intent of the owner of the design, such as keeping the design and associated bitstream keys confidential, preventing design changes (insertion of Trojan Horses, for example), and controlling the number of copies made throughout the device life cycle. Design security may also be known as intellectual property (IP) protection. It is one aspect of anti-tamper (AT) protection. Design security applies to the device from initial production, includes any updates such as in-the-field upgrades, and can include decommissioning of the device at the end of its life, if desired. Good design security is a prerequisite for good data security.

The following are the main design security features supported:

Table 1-1 • Design Security Features

Features	M2S005	M2S090
	M2S010	M2S100
	M2S025	M2S150
	M2S050	
Software Memory Protection Unit (MPU)	x	x
FlashLock™ Passcode Security (256-bit)	x	x
Flexible security settings using flash lock-bits	x	x
Encrypted/Authenticated Design Key Loading	x	x
Symmetric Key Design Security (256-bit)	x	x
Design Key Verification Protocol	x	x
Encrypted/Authenticated Configuration Loading	x	x
Certificate-of-Conformance (C-of-C)	x	x
Back-Tracking Prevention (also known as, Versioning)	x	x
Device Certificate(s) (Anti-Counterfeiting)	x	x
Support for Configuration Variations	x	x
Fabric NVM and eNVM Integrity Tests	x	x
Information Services (S/N, Cert., USERCODE, and others)	x	x
Tamper Detection	x	x
Tamper Response (includes Zeroization)	x	x
ECC Public Key Design Security (384-bit)		x
Hardware Intrinsic Design Key (SRAM-PUF)		x

Data Security

Data security is protecting the information the FPGA is storing, processing, or communicating in its role in the end application. If, for example, the configured design is implementing the key management and encryption portion of a secure military radio, data security could entail encrypting and authenticating the radio traffic, and protecting the associated application-level cryptographic keys. Data security is closely related to the terms information assurance (IA) and information security.

All SmartFusion2 devices incorporate enhanced design security, making them the most secure programmable logic devices ever made. Select SmartFusion2 models also include an advanced set of on-chip data security features that make designing secure information assurance applications easier and better than ever before.

The following are the main data security features supported:

Table 1-2 • Data Security Features

Additional "S" Device Features	M2S005S	M2S090S/TS
	M2S010S/TS	M2S100S/TS
	M2S025S/TS	M2S150S/TS
	M2S050S/TS	
CRI Pass-through DPA Patent License	x	x
Hardware Firewalls protecting access to memories	x	x
Non-Deterministic Random Bit Generator Service	x	x
AES-128/256 Service (ECB, OFB, CTR, CBC modes)	x	x
SHA-256 Service	x	x
HMAC-SHA-256 Service	x	x
Key Tree Service	x	x
PUF Emulation (Pseudo-PUF)	x	
PUF Emulation (SRAM-PUF)		x
ECC Point-Multiplication Service		x
ECC Point-Addition Service		x
User SRAM-PUF Enrollment Service		x
User SRAM-PUF Activation Code Export Service		x
SRAM-PUF Intrinsic Key Generation and Enrollment Service		x
SRAM-PUF Key Import and Enrollment Service		x
SRAM-PUF Key Regeneration Service		x

Low Power

Microsemi's flash-based FPGA fabric results in extremely low power design implementation with static power on the as low as 7 mW. Flash*Freeze (F*F) technology provides an ultra-low power static mode (Flash*Freeze mode) for SmartFusion2 devices, with power less than 7 mW for the largest device. F*F mode entry retains all the SRAM and register information and the exit from F*F mode achieves rapid recovery to active mode.

High-Performance FPGA Fabric

Built on 65 nm process technology, the SmartFusion2 FPGA fabric is composed of 4 building blocks: the logic module, the large SRAM, the micro SRAM and the mathblock. The logic module is the basic logic element and has advanced features:

- A fully permutable 4-input LUT (look-up table) optimized for lowest power
- A dedicated carry chain based on carry look-ahead technique
- A separate flip-flop which can be used independently from the LUT

The 4-input look-up table can be configured either to implement any 4-input combinatorial function or to implement an arithmetic function where the LUT output is XORed with carry input to generate the sum output.

Dual-Port Large SRAM (LSRAM)

Large SRAM (RAM1Kx18) is targeted for storing large memory for use with various operations. Each LSRAM block can store up to 18,432 bits. Each RAM1Kx18 block contains two independent data ports: Port A and Port B. The LSRAM is synchronous for both Read and Write operations. Operations are triggered on the rising edge of the clock. The data output ports of the LSRAM have pipeline registers which have control signals that are independent of the SRAM's control signals.

Three-Port Micro SRAM (uSRAM)

Micro SRAM (RAM64x18) is the second type of SRAM which is embedded in the fabric of SmartFusion2 devices. RAM64x18 uSRAM is a 3-port SRAM; it has two read ports (Port A and Port B) and one write port (Port C). The two read ports are independent of each other and can perform Read operations in both synchronous and asynchronous modes. The write port is always synchronous. The uSRAM block is approximately 1 KB (1,152 bits) in size. These uSRAM blocks are primarily targeted for building embedded FIFOs to be used by any embedded fabric masters.

Mathblocks for DSP Applications

The fundamental building block in any digital signal processing algorithm is the multiply-accumulate function. SmartFusion2 FPGAs implement a custom 18x18 Multiply-Accumulate (18x18 MACC) block for efficient implementation of complex DSP algorithms such as finite impulse response (FIR) filters, infinite impulse response (IIR) filters, and fast Fourier transform (FFT) for filtering and image processing applications.

Each mathblock has the following capabilities:

- Supports 18x18 signed multiplications natively ($A[17:0] \times B[17:0]$)
- Supports dot product; the multiplier computes:
$$(A[8:0] \times B[17:9] + A[17:9] \times B[8:0]) \times 2^9$$
- Built-in addition, subtraction, and accumulation units to combine multiplication results efficiently

In addition to the basic MACC function, DSP algorithms typically need small amounts of RAM for coefficients and larger RAMs for data storage. SmartFusion2 micro RAMs are ideally suited to serve the needs of coefficient storage while the large RAMs are used for data storage.

Microcontroller Subsystem (MSS)

The microcontroller subsystem (MSS) contains a high-performance integrated Cortex-M3 processor, running at up to 166 MHz. The MSS contains an 8 Kbyte instruction cache to provide low latency access to internal eNVM and external DDR memory. The MSS provides multiple interfacing options to the FPGA fabric in order to facilitate tight integration between the MSS and user logic in the fabric.

ARM Cortex-M3 Processor

The MSS uses the latest revision (r2p1) of the ARM Cortex-M3 processor. Microsemi's implementation includes the optional embedded trace macrocell (ETM) features for easier development and debug and the memory protection unit (MPU) for real-time operating system support.

Cache Controller

In order to minimize latency for instruction fetches when executing firmware out of off-chip DDR or on-chip eNVM, an 8 kbyte, 4-way set associative instruction cache is implemented. This provides zero wait state access for cache hits and is shared by both I and D code buses of the Cortex-M3 processor. In the event of cache misses, cache lines are filled, replacing existing cache entries based on a least recently used (LRU) algorithm.

There is a configurable option available to operate the cache in a locked mode, whereby a fixed segment of code from either the DDR or eNVM is copied into the cache and locked there, so that it is not replaced when cache misses occur. This would be used for performance-critical code.

It is also possible to disable the cache altogether, which is desirable in systems requiring very deterministic execution times.

The cache is implemented with SEU tolerant latches.

DDR Bridge

The DDR bridge is a data bridge between four AHB bus masters and a single AXI bus slave. The DDR bridge accumulates AHB writes into write combining buffers prior to bursting out to external DDR memory. The DDR bridge also includes read combining buffers, allowing AHB masters to efficiently read data from the external DDR memory from a local buffer. The DDR bridge optimizes reads and writes from multiple masters to a single external DDR memory. Data coherency rules between the four masters and the external DDR memory are implemented in hardware. The DDR bridge contains three write combining / read buffers and one read buffer. All buffers within the DDR bridge are implemented with SEU tolerant latches and are not subject to the single event upsets (SEUs) that SRAM exhibits. SmartFusion2 devices implement three DDR bridges in the MSS, FDDR, and MDDR subsystems.

AHB Bus Matrix (ABM)

The AHB bus matrix (ABM) is a non-blocking, AHB-Lite multi-layer switch, supporting 10 master interfaces and 7 slave interfaces. The switch decodes access attempts by masters to various slaves, according to the memory map and security configurations. When multiple masters are attempting to access a particular slave simultaneously, an arbiter associated with that slave decides which master gains access, according to a configurable set of arbitration rules. These rules can be configured by the user to provide different usage patterns to each slave. For example, a number of consecutive access opportunities to the slave can be allocated to one particular master, to increase the likelihood of same type accesses (all reads or all writes), which makes more efficient usage of the bandwidth to the slave.

System Registers

The MSS System registers are implemented as an AHB slave on the AHB bus matrix. This means the Cortex-M3 processor or a soft master in the FPGA fabric may access the registers and therefore control the MSS. The System registers can be initialized by user-defined flash configuration bits on power-up. Each register also has a flash bit to enable write protecting the contents of the registers. This allows the MSS system configuration to be reliably fixed for a given application.

Fabric Interface Controller (FIC)

The FIC block provides two separate interfaces between the MSS and the FPGA fabric: the MSS master (MM) and fabric master (FM). Each of these interfaces can be configured to operate as AHB-Lite or APB3. Depending on device density, there are up to two FIC blocks present in the MSS (FIC_0 and FIC_1).

Embedded SRAM (eSRAM)

The MSS contains two blocks of 32 KB eSRAM, giving a total of 64 KB. Having the eSRAM arranged as two separate blocks allows the user to take advantage of the Harvard architecture of the Cortex-M3 processor. For example, code could be located in one eSRAM, while data, such as the stack, could be located in the other.

The eSRAM is designed for Single Error Correct Double Error Detect (SECCDED) protection. When SECCDED is disabled, the SRAM usually used to store SECCDED data may be reused as an extra 16 KB of eSRAM.

Embedded NVM (eNVM)

The MSS contains up to 512 KB of eNVM (64 bits wide). Accesses to the eNVM from the Cortex-M3 processor are cacheable.

DMA Engines

Two DMA engines are present in the MSS: high-performance DMA and peripheral DMA.

High-Performance DMA (HPDMA)

The high-performance DMA (HPDMA) engine provides efficient memory to memory data transfers between an external DDR memory and internal eSRAM. This engine has two separate AHB-Lite interfaces—one to the MDDR bridge and the other to the AHB bus matrix. All transfers by the HPDMA are full word transfers.

Peripheral DMA (PDMA)

The peripheral DMA engine (PDMA) is tuned for offloading byte-intensive operations, involving MSS peripherals, to and from the internal eSRAMs. Data transfers can also be targeted to user logic/RAM in the FPGA fabric.

APB Configuration Bus

On every SmartFusion2 device, an APB configuration bus is present to allow the user to initialize the SERDES ASIC blocks, the fabric DDR memory controller, and user instantiated peripherals in the FPGA fabric.

Peripherals

A large number of communications and general purpose peripherals are implemented in the MSS.

USB Controller

The MSS contains a high speed USB 2.0 On-The-Go (OTG) controller with the following features:

- Operates either as the function controller of a high-speed / full-speed USB peripheral or as the host/peripheral in point-to-point or multi-point communications with other USB functions.
- Complies with the USB 2.0 standard for high-speed functions and with the *On-The-Go* supplement to the USB 2.0 specification.
- Supports OTG communications with one or more high-speed, full-speed, or low-speed devices.

TSE Ethernet MAC

The triple speed Ethernet (TSE) MAC supports IEEE 802.3 10/100/1000Mbps Ethernet operation. The following PHY interfaces are directly supported by the MAC:

- GMII
- MII
- TBI

The Ethernet MAC hardware implements the following functions:

- 4 KB internal transmit FIFO and 8 KB internal receive FIFO
- IEEE 802.3X full-duplex flow control
- DMA of Ethernet frames between internal FIFOs and system memory (such as eSRAM or DDR)
- Cut-through operation
- SECEDED protection on internal buffers

SGMII PHY Interface

SGMII mode is implemented by means of configuring the MAC for 10-bit interface (TBI) operation, allocating one of the high-speed serial channels to SGMII, and by implementing custom logic in the fabric.

10 Gbps Ethernet

Support for 10 Gbps Ethernet is achieved by programming the SERDES interface to XAUI mode. In this mode, a soft 10G EMAC with XGMII interface can be directly connected to the SERDES interface.

Communication Block (COMM_BLK)

The COMM block provides a UART-like communications channel between the MSS and the system controller. System services are initiated through the COMM block.

SPI

The serial peripheral interface controller is compliant with the Motorola SPI, Texas Instruments synchronous serial, and National Semiconductor MICROWIRE™ formats. In addition, the SPI supports interfacing to large SPI flash and EEPROM devices by way of the slave protocol engine. The SPI controller supports both Master and Slave modes of operation.

The SPI controller embeds two 4x32 (depth x width) FIFOs for receive and transmit. These FIFOs are accessible through Rx data and Tx data registers. Writing to the Tx data register causes the data to be written to the transmit FIFO. This is emptied by transmit logic. Similarly, reading from the Rx data register causes data to be read from the receive FIFO.

Multi-Mode UART (MMUART)

SmartFusion2 devices contain two identical multi-mode universal asynchronous/synchronous receiver/transmitter (MMUART) peripherals that provide software compatibility with the popular 16550 device. They perform serial-to-parallel conversion on data originating from modems or other serial devices, and perform parallel-to-serial conversion on data from the Cortex-M3 processor to these devices.

The following are the main features supported:

- Fractional baud rate capability
- Asynchronous and synchronous operation
- Full programmable serial interface characteristics
 - Data width is programmable to 5, 6, 7, or 8 bits
 - Even, odd, or no-parity bit generation/detection
 - 1, 1½, and 2 stop bit generation
- 9-bit address flag capability used for multidrop addressing topologies

I²C

SmartFusion2 devices contain two identical master/slave I²C peripherals that perform serial to-parallel conversion on data originating from serial devices, and perform parallel-to-serial conversion on data from the ARM Cortex-M3 processor, or any other bus master, to these devices. The following are the main features supported:

- I²C v2.1
 - 100 Kbps
 - 400 Kbps
- Dual-slave addressing
- SMBus v2.0
- PMBus v1.1

Clock Sources: On-Chip Oscillators, PLLs, and CCCs

SmartFusion2 devices have two on-chip RC oscillators—a 1 MHz RC oscillator and a 50 MHz RC oscillator—and up to two main crystal oscillators (32 KHz–20 MHz). These are available to the user for generating clocks to the on-chip resources and the logic built on the FPGA fabric array. The second crystal oscillator available on the SmartFusion2 devices is dedicated for RTC clocking. These oscillators (except the RTC crystal oscillator) can be used in conjunction with the integrated user phase-locked loops (PLLs) and fabric clock conditioning circuits (FAB_CCC) to generate clocks of varying frequency and phase. In addition to being available to the user, these oscillators are also used by the system controller, power-on reset circuitry, MSS during Flash*Freeze mode, and the RTC.

SmartFusion2 devices have up to eight fabric CCC (FAB_CCC) blocks and a dedicated PLL associated with each CCC to provide flexible clocking to the FPGA fabric portion of the device. The user has the freedom to use any of the eight PLLs and CCCs to generate the fabric clocks and the internal MSS clock from the base fabric clock (CLK_BASE). There is also a dedicated CCC block for the MSS (MSS_CCC) and an associated PLL (MPLL) for MSS clocking and de-skewing the CLK_BASE clock. The fabric alignment clock controller (FACC), part of the MSS CCC, is responsible for generating various aligned clocks required by the MSS for correct operation of the MSS blocks and synchronous communication with the user logic in the FPGA fabric.

High Speed Serial Interfaces

SERDES Interface

SmartFusion2 has up to four 5 Gbps SERDES transceivers, each supporting the following:

- 4 SERDES lanes
- The native SERDES interface facilitates implementation of Serial RapidIO (SRIO) in fabric or an SGMII interface for the Ethernet MAC in MSS

PCI Express (PCIe)

PCIe is a high speed, packet-based, point-to-point, low pin count, serial interconnect bus. The SmartFusion2 family has two hard high-speed serial interface blocks. Each SERDES block contains a PCIe system block. The PCIe system is connected to the SERDES block and following are the main features supported:

- Supports x1, x2, and x4 lane configuration
- Endpoint configuration only
- PCI Express Base Specification Revision 2.0
- 2.5 and 5.0 Gbps compliant
- Embedded receive (2 KB), transmit (1 KB) and retry (1 KB) buffer dual-port RAM implementation
- Up to 2 kbytes maximum payload size
- 64-bit AXI or 32-bit AHB-Lite Master and Slave interface to the application layer
- 32-bit APB interface to access configuration and status registers of PCIe system
- Up to 3 x 64 bit base address registers
- 1 virtual channel (VC)

XAUI/XGXS Extension

The XAUI/XGXS extension allows the user to implement a 10 Gbps (XGMII) Ethernet PHY interface by connecting the Ethernet MAC fabric interface through an appropriate soft IP block in the fabric.

High Speed Memory Interfaces: DDRx Memory Controllers

There are up to three DDR subsystems, MDDR (MSS DDR) and FDDR (fabric DDR) present in SmartFusion2 devices. Each subsystem consists of a DDR controller, PHY, and a wrapper. The MDDR has an interface from the MSS and fabric, and FDDR provides an interface from the fabric.

The following are the main features supported by the FDDR and MDDR:

- Support for LPDDR, DDR2, and DDR3 memories
- Simplified DDR command interface to standard AMBA AXI/AHB interface
- Up to 667 Mbps (333 MHz double data rate) performance
- Supports 1, 2, or 4 ranks of memory
- Supports different DRAM bus width modes: x8, x9, x16, x18, x32, and x36
- Supports DRAM burst length of 2, 4, or 8 in full bus-width mode; supports DRAM burst length of 2, 4, 8, or 16 in half bus-width mode
- Supports memory densities up to 4 GB
- Supports a maximum of 8 memory banks
- SECEDED enable/disable feature
- Embedded physical interface (PHY)
- Read and Write buffers in fully associative CAMs, configurable in powers of 2, up to 64 Reads plus 64 Writes
- Support for dynamically changing clock frequency while in self-refresh
- Supports command reordering to optimize memory efficiency
- Supports data reordering, returning critical word first for each command

MDDR Subsystem

The MDDR subsystem has two interfaces to the DDR. One is an AXI 64-bit bus from the DDR bridge within the MSS. The other is a multiplexed interface from the FPGA fabric, which can be configured as either a single AXI 64-bit bus or two 32-bit AHB-Lite buses. There is also a 16-bit APB configuration bus, which is used to initialize the majority of the internal registers within the MDDR subsystem after reset. This APB configuration bus can be mastered by the MSS directly or by a master in the FPGA fabric. Support for 3.3 V Single Data Rate DRAMs (SDRAM) can be obtained by using the SMC_FIC interface in the MDDR subsystem. Users would then instantiate a soft AHB or AXI SDRAM memory controller in the FPGA fabric and connect I/O ports to 3.3 V MSIO.

FDDR Subsystem

The FDDR subsystem has one interface to the DDR. This is a multiplexed interface from the FPGA fabric, which can be configured as either a single AXI 64-bit bus or two 32-bit AHB-Lite buses. There is also a 16-bit APB configuration bus, which is used to initialize the majority of the internal registers within the FDDR subsystem after reset. This APB configuration bus can be mastered by the MSS or a master in the FPGA fabric.

SmartFusion2 Development Tools

Design Software

System designers can leverage the easy-to-use Libero[®] system-on-chip (SoC) software toolset for designing SmartFusion2 devices. Libero SoC highlights include the following:



- System Builder for creation of system level architecture
- Synthesis, DSP and debug support from Synopsys
- Simulation from Mentor Graphics
- Push-button design flow with power analysis and timing analysis
- SmartDebug for access to non-invasive probes within SmartFusion2 devices
- Integrated firmware flows for SoftConsole (GNU/Eclipse), IAR[®], and Keil[™]
- Operating system support includes uClinux[™] from Emcraft Systems, FreeRTOS[™], SAFERTOS[®] and uc/OS-III[™] from Micrium.

For more information refer to [Libero SoC](#).

Design Hardware

SmartFusion2 hardware is now available in a starter kit and development kit format. The starter kit is recommended for initial evaluation and the development kit for full system design and prototyping.

Table 1-3 • SmartFusion2 Kits

<p>SmartFusion2 Starter Kit</p> <p>The SmartFusion2 Starter Kit provides a cost effective platform for evaluation and development of a SmartFusion2 SoC FPGA based solution. The kit utilizes a miniature mezzanine form factor system-on-module, which integrates the SmartFusion2 device with 64 MB LPDDR, 16 MB SPI flash, and Ethernet PHY. The baseboard provides easy to use benchtop access to the SmartFusion2 SoC and interfaces.</p>	
<p>SmartFusion2 Development Kit</p> <p>The SmartFusion2 full feature development kit provides access to all peripherals of the SmartFusion2 device, including use of the SERDES, DDR, CAN, USB, and other embedded peripherals.</p> <p>Application-specific daughtercards are also in development for use with this kit.</p>	
<p>The SmartFusion2 Motor Control Kit will support up to 6-axis motor control and is currently in development This is used in conjunction with the SmartFusion2 Development Kit.</p>	
<p>The SmartFusion2 Micro Power Manager (MPM) Daughtercard will be the next revision in MPM system management platforms. This is used in conjunction with the SmartFusion2 Development Kit.</p>	

IP Cores

SmartFusion2 SoC FPGAs contain an ARM Cortex-M3 processor and multiple peripherals hardcoded into the device. In addition to these, Microsemi offers many soft peripherals that can be placed in the FPGA fabric of the device. These include Core429, Core1553, CoreJESD204BRX/TX, CoreFRI, CoreFFT, and many other DirectCores. Refer to [IP Cores](#) for more information.

2 – Product Brief Information

List of Changes

The following table lists critical changes that were made in each revision of the SmartFusion2 Product Brief.

Revision	Changes	Page
Revision 4 (August 2014)	Updated Device Packages 005-VF256 and 150 FCS536 in Table 2–Table 4 .	1-V–1-VII
Revision 3 (June 2014)	Updated Table 2 , Table 3 and Table 4 .	1-V, 1-VI, 1-VII
Revision 2 (March 2014)	Table 1 to Table 3 and "SmartFusion2 Ordering Information" were updated with Military device data. Table 4 and Table 5 and the "Marking Specification Details" section were added.	1-IV-1-VI 1-VII, 1-VIII 1-IX
Revision 1 (Dec 2013)	Tables 3-6 were combined into Table 3 . Fabric Interface Controller features were added to the "SmartFusion2 SoC FPGA Product Family" table. Packages VQ144 and FCV484 were added to Table 2 and Table 3 .	1-VI,1-IV 1-V,1-VI
Revision 0 (Nov 2013)	Initial Release	N/A

Datasheet Categories

Categories

In order to provide the latest information to designers, some datasheet parameters are published before data has been fully characterized from silicon devices. The data provided for a given device, as highlighted in the "[SmartFusion2 Device Status](#)" table on page IX, is designated as either "Product Brief," "Advance," "Preliminary," or "Production." The definitions of these categories are as follows:

Product Brief

The product brief is a summarized version of a datasheet (advance or production) and contains general product information. This document gives an overview of specific device and family information.

Advance

This version contains initial estimated information based on simulation, other products, devices, or speed grades. This information can be used as estimates, but not for production. This label only applies to the DC and Switching Characteristics chapter of the datasheet and will only be used when the data has not been fully characterized.

Preliminary

The datasheet contains information based on simulation and/or initial characterization. The information is believed to be correct, but changes are possible.

Production

This version contains information that is considered to be final.

Export Administration Regulations (EAR)

The products described in this document are subject to the Export Administration Regulations (EAR). They could require an approved export license prior to export from the United States. An export includes release of product or disclosure of technology to a foreign national inside or outside the United States.

Safety Critical, Life Support, and High-Reliability Applications Policy

The products described in this advance status document may not have completed the Microsemi qualification process. Products may be amended or enhanced during the product introduction and qualification process, resulting in changes in device functionality or performance. It is the responsibility of each customer to ensure the fitness of any product (but especially a new product) for a particular purpose, including appropriateness for safety-critical, life-support, and other high-reliability applications. Consult the Microsemi SoC Products Group Terms and Conditions for specific liability exclusions relating to life-support applications. For more information covering all of the SoC Products Group's products refer to the [Reliability Report](#). Microsemi also offers a variety of enhanced qualification and lot acceptance screening procedures. Contact your local sales office for additional reliability information.

Microsemi Corporate Headquarters

One Enterprise, Aliso Viejo, CA 92656 USA. Within the USA: +1 (949) 380-6100
Sales: +1 (949) 380-6136
Fax: +1 (949) 215-4996
Sales.Support@Microsemi.com



Microsemi Corporate Headquarters
One Enterprise, Aliso Viejo CA 92656 USA
Within the USA: +1 (949) 380-6100
Sales: +1 (949) 380-6136
Fax: +1 (949) 215-4996

Microsemi Corporation (Nasdaq: MSCC) offers a comprehensive portfolio of semiconductor and system solutions for communications, defense & security, aerospace 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; security technologies and scalable anti-tamper products; Power-over-Ethernet ICs and midspans; as well as custom design capabilities and services. Microsemi is headquartered in Aliso Viejo, Calif., and has approximately 3,400 employees globally. Learn more at www.microsemi.com.

© 2014 Microsemi Corporation. All rights reserved. Microsemi and the Microsemi logo are trademarks of Microsemi Corporation. All other trademarks and service marks are the property of their respective owners.