Chipsmall Limited consists of a professional team with an average of over 10 year of expertise in the distribution of electronic components. Based in Hongkong, we have already established firm and mutual-benefit business relationships with customers from,Europe,America and south Asia,supplying obsolete and hard-to-find components to meet their specific needs.

With the principle of “Quality Parts,Customers Priority,Honest Operation,and Considerate Service”,our business mainly focus on the distribution of electronic components. Line cards we deal with include Microchip,ALPS,ROHM,Xilinx,Pulse,ON,Everlight and Freescale. Main products comprise IC,Modules,Potentiometer,IC Socket,Relay,Connector.Our parts cover such applications as commercial,industrial, and automotives areas.

We are looking forward to setting up business relationship with you and hope to provide you with the best service and solution. Let us make a better world for our industry!

Contact us

Tel: +86-755-8981 8866 Fax: +86-755-8427 6832
Email & Skype: info@chipsmall.com Web: www.chipsmall.com
Address: A1208, Overseas Decoration Building, #122 Zhenhua RD., Futian, Shenzhen, China

73S1217F

Bus-Powered 80515 System-on-Chip with USB, ISO 7816 / EMV, PINpad and More

Simplifying System Integration™

DATA SHEET

December 2008

GENERAL DESCRIPTION

The Teridian Semiconductor Corporation 73S1217F is a versatile and economical CMOS System-on-Chip device intended for smart card reader applications. The circuit features an ISO-7816 / EMV interface, an USB 2.0 interface (full-speed 12Mbps - slave) and a 5x6 PINpad interface. Additional features include 8 user I/Os, multiple interrupt options and an analog voltage input (for DC voltage monitoring such as battery level detection). Other built-in interfaces include an asynchronous serial and an I^2C interface.

The System-on-Chip is built around an 80515 high-performance core. Its feature and instruction set is compatible with the industry standard 8051, while offering one clock-cycle per instruction processing power (most instructions). With a CPU clock running up to 24MHz, it results in up to 20MIPS available that meets the requirements of various encryption needs such as AES, DES / 3-DES and even RSA (for PIN encryption for instance). The circuit requires a single 6 to 12 MHz crystal. An optional 32kHz crystal can be connected to a sub-system oscillator with a real-time-clock counter to enable stand-alone applications to access an RTC value.

The respective 73S1217F embedded memories are; 64KB Flash program memory, 2KB user XRAM memory, and 256B IRAM memory. On top of these memories are added independent FIFOs dedicated to the ISO7816 UART and to the USB interface.

The chip incorporates an inductor-based DC-DC converter that generates all the necessary voltages to the various 73S1217F function blocks (smart card interface, digital core, etc.) from any of two distinct power supply sources: The +5V USB bus (V_{BUS}, 4.4V to 6.5V), or a main battery (V_{BAT}, 4.0V to 6.5V). The chip automatically powers-up the DC-DC converter with V_{BUS} if it is present, or uses V_{BAT} as the supply input. Alternatively, the pin V_{PC} can support a wider power supply input range (2.7V to 6.5V), when using a single system supply source.

In addition, the circuit features an ON/OFF mode which operates directly with an ON/OFF system switch: Any activity on the ON/OFF button is debounced internally and controls the power generation circuit accordingly, under the supervision of the firmware (OFF request / OFF acknowledgement at firmware level). The OFF mode can be alternatively initiated from the controller (firmware action instead of ON/OFF switch).

In OFF mode, the circuit typically draws less than 1μA, which makes it ideal for applications where battery life must be maximized.

Wake-up of the controller upon USB cable insertion is supported.

Embedded Flash memory is in-system programmable and lockable by means of on-silicon fuses. This makes the Teridian 73S1217F suitable for both development and production phases.

Teridian Semiconductor Corporation offers with its 73S1217F a very comprehensive set of software libraries, including the smart card and USB protocol layers that are pre-approved against USB, Microsoft WHQL and EMV, as well as a CCID reference design. Refer to the Teridian Semiconductor Corporation *73S12xxF Software User's Guide* for a complete description of the Application Programming Interface (API Libraries) and related Software modules.

A complete array of development and programming tools, libraries and demonstration boards enable rapid development and certification of readers that meet most demanding smart card standards.

APPLICATIONS

- Hand-held PINpad smart card readers:
- With USB or serial connectivity
- Ideal for E-banking (MasterCard CAP, etc) and Digital Identification (Secure Login, Gov't ID...)
- Transparent USB card readers and USB keys
- General purpose smart card readers

ADVANTAGES

- Reduced BOM
- Larger built-in Flash / RAM than its competitors
- Higher performance CPU core (up to 24MIPS)
- On-chip DC-DC converter and CMOS switches for battery and USB power
- Sub-μA Power Down mode with ON/OFF switch
- Powerful In-Circuit Emulation and Programming
- A complete set of EMV4.1, USB and CCID libraries
- Overall, the ideal compromise cost / features for high volume, PINpad reader applications!

FEATURES

80515 Core:

- 1 clock cycle per instruction (most instructions)
- CPU clocked up to 24MHz
- 64kB Flash memory (lockable)
- 2kB XRAM (User Data Memory)
- 256 byte IRAM
- Hardware watchdog timer

Oscillators:

- Single low-cost 6MHz to 12MHz crystal
- Optional 32kHz crystal (with internal RTC)
- An Internal PLL provides all the necessary clocks to each block of the system

Interrupts:

- Standard 80C515 4-priority level structure
- 9 different sources of interrupt to the core

Power Down Modes:

- 2 standard 80C515 Power Down and IDLE modes
- Sub-µA OFF mode

ON/OFF Main System Power Switch:

- Input for an SPST momentary switch to ground

Timers:

- (2) Standard 80C52 timers T0 and T1
- (1) 16-bit timer that can generate RTC interrupts from the 32kHz clock

Built-in ISO-7816 Card Interface:

- LDO regulator produces VCC for the card
- (1.8V, 3V or 5V)
- Full compliance with EMV 4.1
- Activation/Deactivation sequencers
- Auxiliary I/O lines (C4-C8 signals)
- 7kV ESD protection on all interface pins

Communication with Smart Cards:

- ISO 7816 UART for T=0, T=1
- (2) 2-Byte FIFOs for transmit and receive
- Configured to drive multiple external Teridian 73S8010xx interfaces (for multi-SAM architectures)

Communication Interfaces:

- Full-duplex serial interface (1200 to 115kbps UART)
- USB 2.0 Full Speed 12Mbps Interface, PC/SC compliant with 4 Endpoints:
- Control (16B FIFO)
- Interrupt IN (32B FIFO)
- Bulk IN (128B FIFO)
- Bulk OUT (128B FIFO)
- I^2C Master Interface (400kbps)

Man-Machine Interface and I/Os:

- 6x5 Keyboard (hardware scanning, debouncing and scrambling)
- (8) User I/Os
- Single programmable current output (LED)

Voltage Detection:

- Analog Input (detection range: 1.0V to 1.5V)

Operating Voltage:

- Single supply 2.7V to 6.5V operation (VPC)
- USB supply (VBUS 4.4V to 5.5V) with or without battery back up operation (VBAT 4.0V to 6.5V).
- Automated detection of voltage presence - Priority on VBUS over VBAT

DC-DC Converter:

- Step-up converter
- Generates an intermediary voltage VP
- Requires a single 10µH Inductor
- 3.3V supply available for external circuits

Operating Temperature:

- -40°C to 85°C

Package:

- 68-pin QFN

Software:

- Two-level Application Programming Interface (ANSI C-language libraries)
- USB, T=0 / T=1 ISO and EMV compliant smart card protocol layers
- CCID reference design and Windows® driver

Table of Contents

Figures

Tables

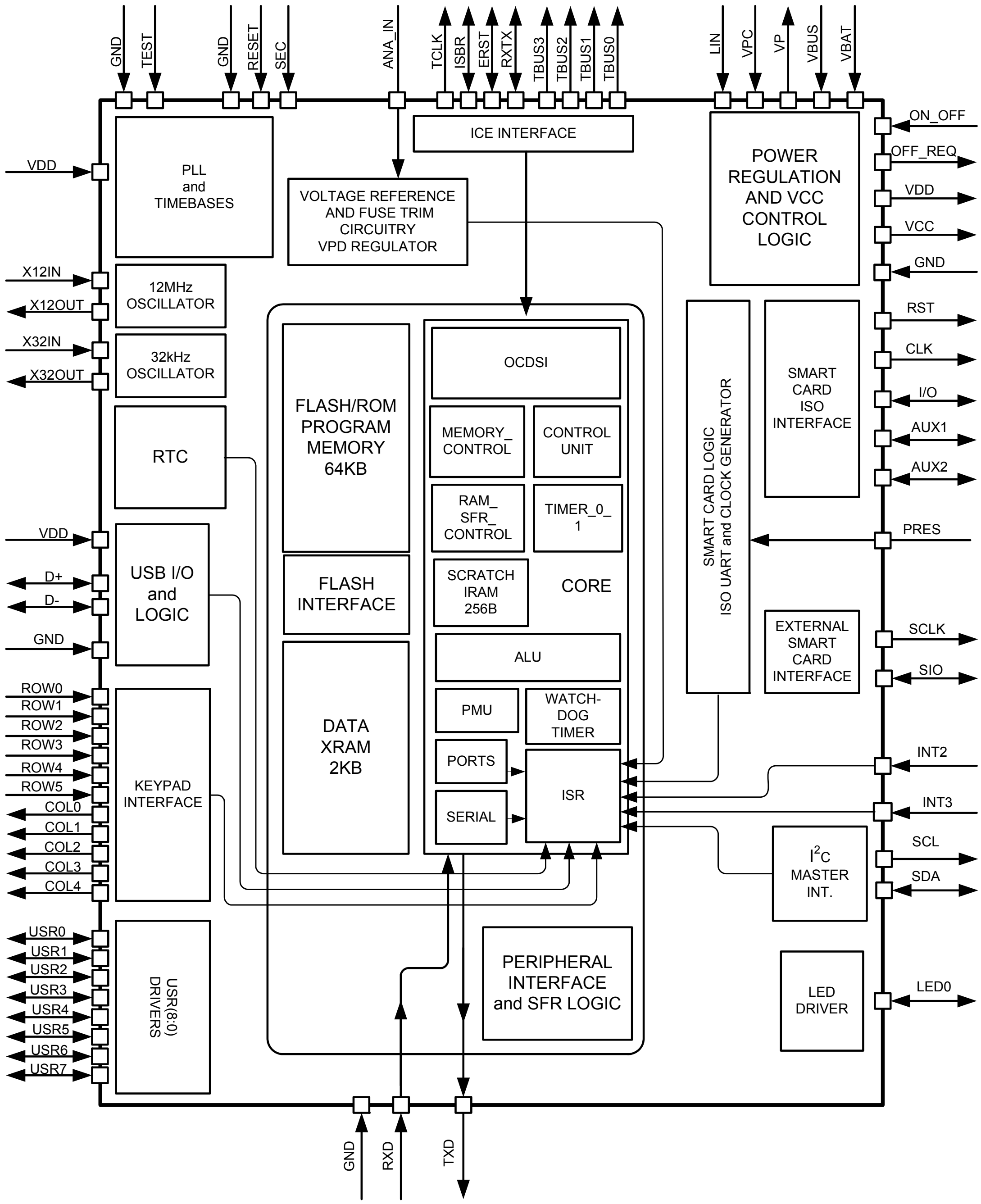


Figure 1: IC Functional Block Diagram

1 Hardware Description

1.1 Pin Description

Table 1: 73S1217 Pinout Description

Pin Name	Pin (68 QFN)	Type	Equivalent Circuit*	Description
X12IN	10	I	Figure 29	MPU/USB clock crystal oscillator input pin. A 12MHz crystal is required for USB operation. A 1MΩ resistor is required between pins X12IN and X12OUT.
X12OUT	11	O	Figure 29	MPU/USB clock crystal oscillator output pin.
X32IN	8	I	Figure 30	RTC clock crystal oscillator input pin. A 32768Hz crystal is required for low-power RTC operation.
X32OUT	7	O	Figure 30	RTC clock crystal oscillator output pin.
DP	26	IO	Figure 45	USB D+ IO pin, requires series 24Ω resistor.
DM	27	IO	Figure 45	USB D- IO pin, requires series 24Ω resistor.
ROW(5:0) 0 1 2 3 4 5	21 22 24 33 36 37	I	Figure 37	Keypad row input sense.
COL(4:0) 0 1 2 3 4	12 13 14 16 19	O	Figure 38	Keypad column output scan pins.
USR(7:0) 0 1 2 3 4 5 6 7	35 34 32 31 30 29 23 20	IO	Figure 33	General-purpose user pins, individually configurable as inputs or outputs or as external input interrupt ports.
SCL	5	O	Figure 32	I^2C (master mode) compatible Clock signal. Note: the pin is configured as an open drain output. When the I2C interface is being used, an external pull up resistor is required. A value of 3K is recommended.
SDA	6	IO	Figure 31	I^2C (master mode) compatible data I/O. Note: this pin is bi-directional. When the pin is configured as output, it is an open drain output. When the I2C interface is being used, an external pull up resistor is required. A value of 3K is recommended.
RXD	17	I	Figure 35	Serial UART Receive data pin.
TXD	18	O	Figure 32	Serial UART Transmit data pin.

Pin Name	Pin (68 QFN)	Type	Equivalent Circuit*	Description
INT3	48	I	Figure 35	General purpose interrupt input.
INT2	49	I	Figure 35	General purpose interrupt input.
SIO	47	IO	Figure 31	IO data signal for use with external Smart Card interface circuit such as 73S73S8010x.
SCLK	45	O	Figure 32	Clock signal for use with external Smart Card interface circuit.
PRES	53	I	Figure 44	Smart Card presence. Active high. Note: the pin has a very weak pull down resistor. In noisy environments, an external pull down may be desired to insure against a false card event.
CLK	55	O	Figure 42	Smart card clock signal.
RST	57	O	Figure 42	Smart card Reset signal.
IO	61	IO	Figure 43	Smart card Data IO signal.
AUX1	60	IO	Figure 43	Auxiliary Smart Card IO signal (C4).
AUX2	59	IO	Figure 43	Auxiliary Smart Card IO signal (C8).
VCC	58	PSO		Smart Card VCC supply voltage output. A 0.47μF capacitor is required and should be located at the smart card connector. The capacitor should be a ceramic type with low ESR.
GND	56	GND		Smart Card Ground.
VPC	65	PSI		Power supply source for main voltage converter circuit. A 10μF and a 0.1μF capacitor are required at the VPC input. The 10μF capacitor should be a ceramic type with low ESR.
VBUS	62	PSI		Alternate power source input from USB connector or hub.
VBAT	64	PSI		Alternate power source input, typically from two series cells, V > 4V.
VP	54	PSO		Intermediate output of main converter circuit. Requires an external 4.7μF low ESR filter capacitor to GND.
LIN	66	PSI		Connection to 10μH inductor for internal step up converter. Note: inductor must be rated for 400 mA maximum peak current.
ON_OFF	63	I	Figure 46	Power control pin. Connected to normally open SPST switch to ground. Closing switch for duration greater than de-bounce period will turn 73S1217F on. If 73S1217F is on, closing switch will flag the 73S1217F to go to the off state. Firmware will control when the power is shut down.

Pin Name	Pin (68 QFN)	Type	Equivalent Circuit*	Description
OFF_REQ	52	O	Figure 36	Digital output. If ON_OFF switch is closed (to ground) for de-bounce duration and circuit is "on," OFF_REQ will go high (Request to turn OFF). This output should be connected to an interrupt pin to signal the CPU core that a request to shut down power has been initiated. The firmware can then perform all of its shut down housekeeping duties before shutting down V_{DD}.
TBUS(3:0)0 1 2 3	50 46 44 41	IO		Trace bus signals for ICE.
RXTX	43	IO		ICE control.
ERST	38	IO		ICE control.
ISBR	3	IO		ICE control.
TCLK	39	I		ICE control.
ANA_IN	15	AI	Figure 41	Analog input pin. This signal goes to a programmable comparator and is used to sense the value of an external voltage.
LED0	4	IO	Figure 39	Special output driver, programmable pull-down current to drive LED. May also be used as an input.
SEC	2	I	Figure 40	Input pin for use in programming security fuse. It should be connected to ground when not in use.
TEST	51	DI	Figure 40	Test pin, should be connected to ground.
VDD	68 28 40	PSO		V_{DD} supply output pin. A 0.1μF capacitor is recommended at each VDD pin.
GND	9 25 42 67	GND		General ground supply pins for all IO and logic circuits.
RESET	1	I	Figure 35	Reset input, positive assertion. Resets logic and registers to default condition. Note: to insure proper reset operation after V_{DD} is turned on by application of V_{BUS} power or activation of the ON/OFF switch, external reset circuitry must generate a proper reset signal to the 73S1217F. This can be accomplished via a simple RC network.

* See the figures in the Equivalent Circuits section.

1.2 Hardware Overview

The 73S1217F single smart card controller integrates all primary functional blocks required to implement a smart card reader with host serial and / or USB interface. Included on chip are an 8051-compatible microprocessor (MPU) which executes up to one instruction per clock cycle (80515), a fully integrated IS0 7816 compliant smart card interface, expansion smart card interface, full speed USB 2.0 compatible interface, serial interface, I2C interface, 6 x 5 keypad interface, RAM, FLASH memory, a real time clock (RTC), and a variety of I/O pins.

Advanced power management features include a DC-DC converter and on-chip regulators that generate all the necessary voltages for the circuit: Primarily a smart card supply VCC, (selectable to 1.8V, 3V or 5V) and a 3.3V digital voltage output (VDD, pin #68) that must be connected to the power supply inputs of the digital core of the circuit, pins # 28 and 40 (these are not internally connected). Should external circuitry require a 3.3V digital power supply, the VDD output is capable of supplying additional current. The whole IC can be powered up either from a USB bus-power supply (VBUS +5V typical), or from a typical set of battery cells VBAT. Automated switching between these supply inputs give the priority to VBUS to save the battery life.

A functional block diagram of the 73S1217F is shown in Figure 1.

1.3 80515 MPU Core

1.3.1 80515 Overview

The 73S1217F includes an 80515 MPU (8-bit, 8051-compatible) that performs most instructions in one clock cycle. The 80515 architecture eliminates redundant bus states and implements parallel execution of fetch and execution phases. Normally a machine cycle is aligned with a memory fetch, therefore, most of the 1-byte instructions are performed in a single cycle. This leads to an 8x performance (average) improvement (in terms of MIPS) over the Intel 8051 device running at the same clock frequency.

Actual processor clocking speed can be adjusted to the total processing demand of the application (cryptographic calculations, key management, memory management, and I/O management) using the XRAM special function register MPUCKCtl.

Typical smart card, USB, serial, keyboard, I2C and RTC management functions are available for the MPU as part of the Teridian standard library. A standard ANSI “C” 80515-application programming interface library is available to help reduce design cycle. Refer to the *73S12xxF Software User’s Guide*.

1.3.2 Memory Organization

The 80515 MPU core incorporates the Harvard architecture with separate code and data spaces. Memory organization in the 80515 is similar to that of the industry standard 8051. There are three memory areas: Program memory (Flash), external data memory (XRAM), and internal data memory (IRAM). Data bus address space is allocated to on-chip memory as shown Table 2.

Table 2: MPU Data Memory Map

Address (hex)	Memory Technology	Memory Type	Typical Usage	Memory Size (bytes)
0000-FFFF	Flash Memory	Non-volatile	Program and non-volatile data	64KB
0000-07FF	Static RAM	Volatile	MPU data XRAM	2KB
FC00-FFFF	External SFR	Volatile	Peripheral control	1KB

Note: The IRAM is part of the core and is addressed differently.

Program Memory: The 80515 can address up to 64KB of program memory space from 0x0000 to 0xFFFF. Program memory is read when the MPU fetches instructions or performs a MOVC operation. After reset, the MPU starts program execution from location 0x0000. The lower part of the program memory includes reset and interrupt vectors. The interrupt vectors are spaced at 8-byte intervals, starting from 0x0003. Reset is located at 0x0000.

Flash Memory: The program memory consists of flash memory. The flash memory is intended to primarily contain MPU program code. Flash erasure is initiated by writing a specific data pattern to specific SFR registers in the proper sequence. These special pattern/sequence requirements prevent inadvertent erasure of the flash memory.

The mass erase sequence is:

1. Write 1 to the FLSH_MEEN bit in the FLSHCTL register (SFR address 0xB2[1]).
2. Write pattern 0xAA to ERASE (SFR address 0x94)

Note: The mass erase cycle can only be initiated when the ICE port is enabled.

The page erase sequence is:

1. Write the page address to PGADDR (SFR address 0xB7[7:1])
2. Write pattern 0x55 to ERASE (SFR address 0x94)

The PGADDR register denotes the page address for page erase. The page size is 512 (200h) bytes and there are 128 pages within the flash memory. The PGADDR denotes the upper seven bits of the flash memory address such that bit 7:1 of the PGADDR corresponds to bit 15:9 of the flash memory address. Bit 0 of the PGADDR is not used and is ignored. The MPU may write to the flash memory. This is one of the non-volatile storage options available to the user. The FLSHCTL SFR bit FLSH_PWE (flash program write enable) differentiates 80515 data store instructions (MOVX@DPTR,A) between Flash and XRAM writes. Before setting FLSH_PWE, all interrupts need to be disabled by setting EAL = 1. Table 3 shows the location and description of the 73S1217F flash-specific SFRs.

✓ Any flash modifications must set the CPUCLK to operate at 3.6923 MHz (MPUCLKCtl = 0x0C) before any flash memory operations are executed to insure the proper timing when modifying the flash memory.

Table 3: Flash Special Function Registers

Register	SFR Address	R/W	Description
ERASE	0x94	W	This register is used to initiate either the Flash Mass Erase cycle or the Flash Page Erase cycle. Specific patterns are expected for ERASE in order to initiate the appropriate Erase cycle (default = 0x00). 0x55 – Initiate Flash Page Erase cycle. Must be proceeded by a write to PGADDR @ SFR 0xB7. 0xAA – Initiate Flash Mass Erase cycle. Must be proceeded by a write to FLSH_MEEN @ SFR 0xB2 and the debug port must be enabled. Any other pattern written to ERASE will have no effect.
PGADDR	0xB7	R/W	Flash Page Erase Address register containing the flash memory page address (page 0 through 127) that will be erased during the Page Erase cycle (default = 0x00). Note: the page address is shifted left by one bit (see detailed description above). Must be re-written for each new Page Erase cycle.
FLSHCTL	0xB2	R/W	Bit 0 (FLSH_PWE): Program Write Enable: 0 – MOVX commands refer to XRAM Space, normal operation (default). 1 – MOVX @DPTR,A moves A to Program Space (Flash) @ DPTR. This bit is automatically reset after each byte written to flash. Writes to this bit are inhibited when interrupts are enabled.
		W	Bit 1 (FLSH_MEEN): Mass Erase Enable: 0 – Mass Erase disabled (default). 1 – Mass Erase enabled. Must be re-written for each new Mass Erase cycle.
		R/W	Bit 6 (SECURE): Enables security provisions that prevent external reading of flash memory and CE program RAM. This bit is reset on chip reset and may only be set. Attempts to write zero are ignored.

Internal Data Memory: The internal data memory provides 256 bytes (0x00 to 0xFF) of data memory. The internal data memory address is always one byte wide and can be accessed by either direct or indirect addressing. The Special Function Registers occupy the upper 128 bytes**. This SFR area is available only by direct addressing. Indirect addressing accesses the upper 128 bytes of Internal RAM.**

The lower 128 bytes contain working registers and bit-addressable memory. The lower 32 bytes form four banks of eight registers (R0-R7). Two bits on the program memory status word (PSW) select which bank is in use. The next 16 bytes form a block of bit-addressable memory space at bit addresses 0x00-0x7F. All of the bytes in the lower 128 bytes are accessible through direct or indirect addressing. Table 4 shows the internal data memory map.

Table 4: Internal Data Memory Map

Addres s	Direct Addressing	Indirect Addressing
0xFF	Special Function Registers (SFRs)	RAM
0x80		
0x7F	Byte-addressable area	
0x30		
0x2F	Byte or bit-addressable area	
0x20		
0x1F	Register banks R0…R7 (x4)	
0x00		

External Data Memory: While the 80515 can address up to 64KB of external data memory in the space from 0x0000 to 0xFFFF, only the memory ranges shown in Figure 2 contain physical memory. The 80515 writes into external data memory when the MPU executes a MOVX @Ri,A or MOVX @DPTR,A instruction. The MPU reads external data memory by executing a MOVX A,@Ri or MOVX A,@DPTR instruction.

There are two types of instructions, differing in whether they provide an eight-bit or sixteen-bit indirect address to the external data RAM.

In the first type (MOVX A,@Ri), the contents of R0 or R1, in the current register bank, provide the eight lower-ordered bits of address. This method allows the user access to the first 256 bytes of the 2KB of external data RAM. In the second type of MOVX instruction (MOVX A,@DPTR), the data pointer generates a sixteen-bit address.

Program Memory

Address	Use
0xFFFF	Flash Program Memory 64K Bytes
0x0000	

External Data Memory

Address	Use
0xFFFF	Peripheral Control Registers (128b)
0XFF80	
0xFF7F	Smart Card Control (384b)
0XFE00	
0xFDFF	USB Registers (512b)
0XFC00	
0xFBFF	–
0x0800	
0x07FF	XRAM
0x0000	

Internal Data Memory

Address	Use: Indirect Access	Use: Direct Access
0xFF	Byte RAM	SFRs
0x80		
0x7F	Byte RAM	
0x48		
0x47	Bit/Byte RAM	
0x20		
0x1F	Register bank 3	
0x18		
0x17	Register bank 2	
0x10		
0x0F	Register bank 1	
0x08		
0x07	Register bank 0	
0x00		

Figure 2: Memory Map

Dual Data Pointer: The Dual Data Pointer accelerates the block moves of data. The standard DPTR is a 16-bit register that is used to address external memory. In the 80515 core, the standard data pointer is called DPTR, the second data pointer is called DPTR1. The data pointer select bit chooses the active pointer. The data pointer select bit is located at the LSB of the DPS IRAM special function register (DPS.0). DPTR is selected when DPS.0 = 0 and DPTR1 is selected when DPS.0 = 1.

The user switches between pointers by toggling the LSB of the DPS register. All DPTR-related instructions use the currently selected DPTR for any activity.

Note: The second data pointer may not be supported by certain compilers.

1.4 Program Security

Two levels of program and data security are available. Each level requires a specific fuse to be blown in order to enable or set the specific security mode. Mode 0 security is enabled by setting the SECURE bit (bit 6 of SFR register FLSHCTL 0xB2). Mode 0 limits the ICE interface to only allow bulk erase of the flash program memory. All other ICE operations are blocked. This guarantees the security of the user's MPU program code. Security (Mode 0) is enabled by MPU code that sets the SECURE bit. The MPU code must execute the setting of the SECURE bit immediately after a reset to properly enable Mode 0. This should be the first instruction after the reset vector jump has been executed. If the "startup.a51" assembly file is used in an application, then it must be modified to set the SECURE bit after the reset vector jump. If not using "startup.a51", then this should be the first instruction in main(). Once security Mode 0 is enabled, the only way to disable it is to perform a global erase of the flash followed by a full circuit reset. Once the flash has been erased and the reset has been executed, security Mode 0 is disabled and the ICE has full control of the core. The flash can be reprogrammed after the bulk erase operation is completed. Global erase of the flash will also clear the data XRAM memory.

The security enable bit (SECURE) is reset whenever the MPU is reset. Hardware associated with the bit only allows it to be set. As a result, the code may set the SECURE bit to enable the security Mode 0 feature but may not reset it. Once the SECURE bit is set, the code is protected and no external read of program code in flash or data (in XRAM) is possible. In order to invoke the security Mode 0, the SECSET0 (bit 1 of XRAM SFR register SECReg 0xFFD7) fuse must be blown beforehand or the security mode 0 will not be enabled. The SECSET0 and SECSET1 fuses once blown, cannot be overridden.

Specifically, when SECURE is set:

- The ICE is limited to bulk flash erase only.
- Page zero of flash memory may not be page-erased by either MPU or ICE. Page zero may only be erased with global flash erase. Note that global flash erase erases XRAM whether the SECURE bit is set or not.
- Writes to page zero, whether by MPU or ICE, are inhibited.

Security mode 1 is in effect when the SECSET1 fuse has been programmed (blown open). In security mode 1, the ICE is completely and permanently disabled. The Flash program memory and the MPU are not available for alteration, observation, nor control. As soon as the fuse has been blown, the ICE is disabled. The testing of the SECSET1 fuse will occur during the reset and before the start of pre-boot and boot cycles. This mode is not reversible, nor recoverable. In order to blow the SECSET1 fuse, the SEC pin must be held high for the fuse burning sequence to be executed properly. The firmware can check to see if this pin is held high by reading the SECPIN bit (bit 5 of XRAM SFR register SECReg 0xFFD7). If this bit is set and the firmware desires, it can blow the SECSET1 fuse. The burning of the SECSET0 does not require the SEC pin to be held high.

In order to blow the fuse for SECSET1 and SECSET0, a particular set of register writes in a specific order need to be followed. There are two additional registers that need to have a specific value written to them in order for the desired fuse to be blown. These registers are FUSECtl (0xFFD2) and TRIMPCtl (0xFFD1). The sequence for blowing the fuse is as follows:

1. Write 0x54H to FUSECtl.
2. Write 0x81H for security mode 0 Note: only program one security mode at a time.
3. Write 0x82H for security mode 1 Note: SEC pin must be high for security mode 1.
4. Write 0xA6 to TRIMPCtl.
5. Delay about 500 us
6. Write 0x00 to TRIMPCtl and FUSECtl.

Table 5: Program Security Registers

Register	SFR Address	R/W	Description
FLSHCTL	0xB2	R/W	Bit 0 (FLSH_PWE): Program Write Enable: 0 – MOVX commands refer to XRAM Space, normal operation (default). 1 – MOVX @DPTR,A moves A to Program Space (Flash) @ DPTR. This bit is automatically reset after each byte written to flash. Writes to this bit are inhibited when interrupts are enabled.
		W	Bit 1 (FLSH_MEEN): Mass Erase Enable: 0 – Mass Erase disabled (default). 1 – Mass Erase enabled. Must be re-written for each new Mass Erase cycle.
		R/W	Bit 6 (SECURE): Enables security provisions that prevent external reading of flash memory and CE program RAM. This bit is reset on chip reset and may only be set. Attempts to write zero are ignored.
TRIMPCtl	0xFFD1	W	0xA6 value will cause the selected fuse to be blown. All other values will stop the burning process.
FUSECtl	0xFFD2	W	0x54 value will set up for security fuse control. All other values are reserved and should not be used.
SECReg	0xFFD7	W	Bit 7 (PARAMSEC): 0 – Normal operation. 1 – Enable permanent programming of the security fuses.
		R	Bit 5 (SECPIN): Indicates the state of the SEC pin. The SEC pin is held low by a pull-down resistor. The user can force this pin high during boot sequence time to indicate to firmware that sec mode 1 is desired.
		R/W	Bit 1 (SECSET1): See the Program Security section.
		R/W	Bit 0 (SECSET0): See the Program Security section.

1.5 Special Function Registers (SFRs)

The 1217 utilizes numerous SFRs to communicate with the many 1217 peripherals. This results in the need for more SFR locations outside the direct address IRAM space (0x80 to 0xFF). While some peripherals are mapped to unused IRAM SFR locations, additional SFRs for the USB, smart card and other peripheral functions are mapped to the top of the XRAM data space (0xFC00 to 0xFFFF).

1.5.1 Internal Data Special Function Registers (SFRs)

The Special Function Registers map is shown in Table 6.

Table 6: IRAM Special Function Registers Locations

Hex\Bin	X000	X001	X010	X011	X100	X101	X110	X111	Bin/ Hex
F8									FF
F0	B								F7
E8									EF
E0	A								E7
D8	BRCON								DF
D0	PSW	**KCOL**	**KROW**	**KSCAN**	**KSTAT**	**KSIZE**	**KORDERL**	**KORDERH**	D7
C8	T2CON								CF
C0	IRCON								C7
B8	IEN1	IP1	S0RELH	S1RELH					BF
B0			**FLSHCTL**					**PGADDR**	B7
A8	IEN0	IP0	S0RELL						AF
A0									A7
98	S0CON	S0BUF	IEN2	S1CON	S1BUF	S1RELL			9F
90	**USR70**	**UDIR70**	DPS		**ERASE**				97
88	TCON	TMOD	TL0	TL1	TH0	TH1		**MCLKCtl**	8F
80		SP	DPL	DPH	DPL1	DPH1	WDTREL	PCON	87

Only a few addresses are used, the others are not implemented. SFRs specific to the 73S1217F are shown in **bold** print (gray background). Any read access to unimplemented addresses will return undefined data, while most write access will have no effect. However, a few locations are reserved and not user configurable in the 73S1217F. **Writes to the unused SFR locations can affect the operation of the core and therefore must not be written to. This applies to all the SFR areas in both the IRAM and XRAM spaces. In addition, all unused bit locations within valid SFR registers must be left in their default (power on default) states.**

1.5.2 IRAM Special Function Registers (Generic 80515 SFRs)

Table 7 shows the location of the SFRs and the value they assume at reset or power-up.

Table 7: IRAM Special Function Registers Reset Values

Name	Location	Reset Value	Description
SP	0x81	0x07	Stack Pointer
DPL	0x82	0x00	Data Pointer Low 0
DPH	0x83	0x00	Data Pointer High 0
DPL1	0x84	0x00	Data Pointer Low 1
DPH1	0x85	0x00	Data Pointer High 1
WDTREL	0x86	0x00	Watchdog Timer Reload register
PCON	0x87	0x00	Power Control
TCON	0x88	0x00	Timer/Counter Control
TMOD	0x89	0x00	Timer Mode Control
TL0	0x8A	0x00	Timer 0, low byte
TL1	0x8B	0x00	Timer 1, high byte
TH0	0x8C	0x00	Timer 0, low byte
TH1	0x8D	0x00	Timer 1, high byte
MCLKCtl	0x8F	0x0A	Master Clock Control
USR70	0x90	0xFF	User Port Data (7:0)
UDIR70	0x91	0xFF	User Port Direction (7:0)
DPS	0x92	0x00	Data Pointer Select Register
ERASE	0x94	0x00	Flash Erase
S0CON	0x98	0x00	Serial Port 0, Control Register
S0BUF	0x99	0x00	Serial Port 0, Data Buffer
IEN2	0x9A	0x00	Interrupt Enable Register 2
S1CON	0x9B	0x00	Serial Port 1, Control Register
S1BUF	0x9C	0x00	Serial Port 1, Data Buffer
S1RELL	0x9D	0x00	Serial Port 1, Reload Register, low byte
IEN0	0xA8	0x00	Interrupt Enable Register 0
IP0	0xA9	0x00	Interrupt Priority Register 0
S0RELL	0xAA	0xD9	Serial Port 0, Reload Register, low byte
FLSHCTL	0xB2	0x00	Flash Control
PGADDR	0xB7	0x00	Flash Page Address
IEN1	0xB8	0x00	Interrupt Enable Register 1
IP1	0xB9	0x00	Interrupt Priority Register 1
S0RELH	0xBA	0x03	Serial Port 0, Reload Register, high byte
S1RELH	0xBB	0x03	Serial Port 1, Reload Register, high byte
IRCON	0xC0	0x00	Interrupt Request Control Register
T2CON	0xC8	0x00	Timer 2 Control
PSW	0xD0	0x00	Program Status Word
KCOL	0XD1	0x1F	Keypad Column

Name	Location	Reset Value	Description
KROW	0XD2	0x3F	Keypad Row
KSCAN	0XD3	0x00	Keypad Scan Time
KSTAT	0XD4	0x00	Keypad Control/Status
KSIZE	0XD5	0x00	Keypad Size
KORDERL	0XD6	0x00	Keypad Column LS Scan Order
KORDERH	0XD7	0x00	Keypad Column MS Scan Order
BRCON	0xD8	0x00	Baud Rate Control Register (only BRCON.7 bit used)
A	0xE0	0x00	Accumulator
B	0xF0	0x00	B Register

1.5.3 External Data Special Function Registers (SFRs)

A map of the XRAM Special Function Registers is shown in Table 8. The smart card registers are listed separately in Table 114.

Table 8: XRAM Special Function Registers Reset Values

Name	Location	Reset Value	Description
DAR	0x FF80	0x00	Device Address Register (I^2C)
WDR	0x FF81	0x00	Write Data Register (I^2C)
SWDR	0x FF82	0x00	Secondary Write Data Register (I^2C)
RDR	0x FF83	0x00	Read Data Register (I^2C)
SRDR	0x FF84	0x00	Secondary Read Data Register (I^2C)
CSR	0x FF85	0x00	Control and Status Register (I^2C)
USRIntCtl1	0x FF90	0x00	External Interrupt Control 1
USRIntCtl2	0x FF91	0x00	External Interrupt Control 2
USRIntCtl3	0x FF92	0x00	External Interrupt Control 3
USRIntCtl4	0x FF93	0x00	External Interrupt Control 4
INT5Ctl	0x FF94	0x00	External Interrupt Control 5
INT6Ctl	0x FF95	0x00	External Interrupt Control 6
MPUCKCtl	0x FFA1	0x0C	MPU Clock Control
RTCCtl	0x FFB0	0x00	Real Time Clock Control
RTCCnt3	0x FFB1	0x00	RTC Count 3
RTCCnt2	0x FFB2	0x00	RTC Count 2
RTCCnt1	0x FFB3	0x00	RTC Count 1
RTCCnt0	0x FFB4	0x00	RTC Count 0
RTCACC2	0x FFB5	0x00	RTC Accumulator 2
RTCACC1	0x FFB6	0x00	RTC Accumulator 1
RTCACC0	0x FFB7	0x00	RTC Accumulator 0
RTCTrim2	0x FFB8	0x00	RTC TRIM 2
RTCTrim1	0x FFB9	0x00	RTC TRIM 1
RTCTrim0	0x FFBA	0x00	RTC TRIM 0
ACOMP	0x FFD0	0x00	Analog Compare Register
TRIMPCtl	0x FFD1	0x00	TRIM Pulse Control

Name	Location	Reset Value	Description
FUSECtl	0x FFD2	0x00	FUSE Control
VDDFCtl	0x FFD4	0x00	VDDFault Control
SECReg	0x FFD7	0x00	Security Register
MISCtl0	0x FFF1	0x00	Miscellaneous Control Register 0
MISCtl1	0x FFF2	0x10	Miscellaneous Control Register 1
LEDCtl	0x FFF3	0xFF	LED Control Register

Accumulator (ACC, A): ACC is the accumulator register. Most instructions use the accumulator to hold the operand. The mnemonics for accumulator-specific instructions refer to accumulator as “A”, not ACC.

B Register: The B register is used during multiply and divide instructions. It can also be used as a scratch-pad register to hold temporary data.

Program Status Word (PSW):

Table 9: PSW Register Flags

MSB LSB

CV	AC	F0	RS1	RS	OV	–	P

<table>
<tr><th>Bit</th><th>Symbol</th><th>Function</th></tr>
<tr><td>PSW.7</td><td>CV</td><td>Carry flag.</td></tr>
<tr><td>PSW.6</td><td>AC</td><td>Auxiliary Carry flag for BCD operations.</td></tr>
<tr><td>PSW.5</td><td>F0</td><td>General purpose Flag 0 available for user.</td></tr>
<tr><td>PSW.4</td><td>RS1</td><td rowspan="2">Register bank select control bits. The contents of RS1 and RS0 select the working register bank:
<table>
<tr><th>RS1/RS0</th><th>Bank Selected</th><th>Location</th></tr>
<tr><td>00</td><td>Bank 0</td><td>(0x00 – 0x07)</td></tr>
<tr><td>01</td><td>Bank 1</td><td>(0x08 – 0x0F)</td></tr>
<tr><td>10</td><td>Bank 2</td><td>(0x10 – 0x17)</td></tr>
<tr><td>11</td><td>Bank 3</td><td>(0x18 – 0x1F)</td></tr>
</table></td></tr>
<tr><td>PSW.3</td><td>RS0</td></tr>
<tr><td>PSW.2</td><td>OV</td><td>Overflow flag.</td></tr>
<tr><td>PSW.1</td><td>F1</td><td>General purpose Flag 1 available for user.</td></tr>
<tr><td>PSW.0</td><td>P</td><td>Parity flag, affected by hardware to indicate odd / even number of “one” bits in the Accumulator, i.e. even parity.</td></tr>
</table>

Stack Pointer (SP): The stack pointer is a 1-byte register initialized to 0x07 after reset. This register is incremented before PUSH and CALL instructions, causing the stack to begin at location 0x08.

Data Pointer: The data pointer (DPTR) is 2 bytes wide. The lower part is DPL, and the highest is DPH. It can be loaded as a 2-byte register (MOV DPTR,#data16) or as two registers (e.g. MOV DPL,#data8). It is generally used to access external code or data space (e.g. MOVC A,@A+DPTR or MOVX A,@DPTR respectively).

Program Counter: The program counter (PC) is 2 bytes wide initialized to 0x0000 after reset. This register is incremented during the fetching operation code or when operating on data from program memory. Note: The program counter is not mapped to the SFR area.

Port Registers: The I/O ports are controlled by Special Function Register USR70. The contents of the SFR can be observed on corresponding pins on the chip. Writing a 1 to any of the ports (see Table 10) causes the corresponding pin to be at high level (3.3V), and writing a 0 causes the corresponding pin to be held at low level (GND). The data direction register UDIR70 define individual pins as input or output pins (see the User (USR) Ports section for details).

Table 10: Port Registers

Register	SFR Address	R/W	Description
USR70	0x90	R/W	Register for User port bits 7:0 read and write operations (pins USR0… USR7).
UDIR70	0x91	R/W	Data direction register for User port bits 0:7. Setting a bit to 0 means that the corresponding pin is an output.

All ports on the chip are bi-directional. Each consists of a Latch (SFR USR70), an output driver, and an input buffer, therefore the MPU can output or read data through any of these ports if they are not used for alternate purposes.

1.6 Instruction Set

All instructions of the generic 8051 microcontroller are supported. A complete list of the instruction set and of the associated op-codes is contained in the *73S12xxF Software User's Guide*.

1.7 Peripheral Descriptions

1.7.1 Oscillator and Clock Generation

The 73S1217F has two oscillator circuits; one for the main CPU clock and another for the RTC. The main oscillator circuit is designed to operate with various crystal or external clock frequencies. An internal divider working in conjunction with a PLL and VCO provides a 96MHz internal clock within the 73S1217F. 96 MHz is the required frequency for proper operation of specific peripheral blocks such as the USB, specific timers, ISO 7816 UART and interfaces, Step-up converter, and keypad. The clock generation and control circuits are shown in Figure 3.

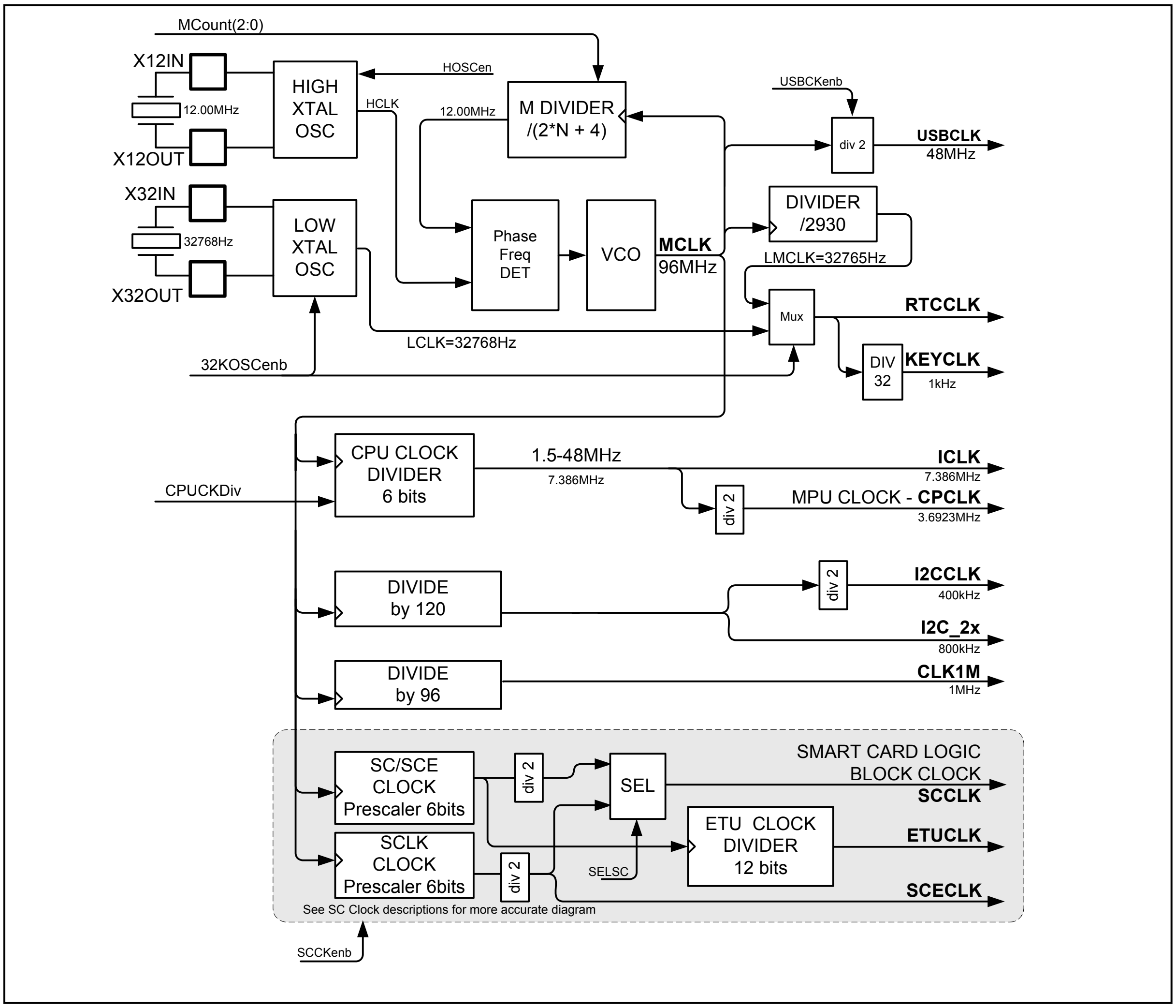


Figure 3: Clock Generation and Control Circuits

The master clock control register enables different sections of the clock circuitry and specifies the value of the VCO Mcount divider. The MCLK must be configured to operate at 96MHz to ensure proper operation of some of the peripheral blocks according to the following formula:

$$MCLK = (Mcount * 2 + 4) * F_{XTAL} = 96MHz$$

Mcount is configured in the MCLKCtl register must be bound between a value of 1 to 7. The possible crystal or external clock frequencies for getting MCLK = 96MHz are shown in Table 11.

Table 11: Frequencies and Mcount Values for MCLK = 96MHz

F_{XTAL} (MHz)	Mcount (N)
12.00	2
9.60	3
8.00	4
6.86	5
6.00	6

Master Clock Control Register (MCLKCtl): 0x8F ← 0x0A

Table 12: The MCLKCtl Register

MSB							LSB
HSOEN	KBEN	SCEN	USBEN	32KEN	MCT.2	MCT.1	MCT.0

Bit	Symbol	Function
MCLKCtl.7	HSOEN	High-speed oscillator disable. When set = 1, disables the high-speed crystal oscillator and VCO/PLL system. Do not set this bit = 1.
MCLKCtl.6	KBEN	1 = Disable the keypad logic clock.
MCLKCtl.5	SCEN	1 = Disable the smart card logic clock.
MCLKCtl.4	USBEN	1 = Disable the USB logic clock.
MCLKCtl.3	32KEN	1 = Disable the 32Khz oscillator. When the 32kHz oscillator is enabled, the RTC and other circuits such as debounce clocks are clocked using the 32kHz oscillator output. When disabled, the main oscillator provides the 32kHz clock for the RTC and other circuits. **Note: This bit must be set if there is no 32KHz crystal. Some internal clocks and circuits will not run if the oscillator is enabled and no crystal is connected.**
MCLKCtl.2	MCT.2	This value determines the ratio of the VCO frequency (MCLK) to the high-speed crystal oscillator frequency such that: $MCLK = (MCount*2 + 4)* F_{XTAL}$. The default value is MCount = 2h such that MCLK = (2*2 + 4)*12.00MHz = 96MHz.
MCLKCtl.1	MCT.1	
MCLKCtl.0	MCT.0	

The MPU clock that drives the CPU core defaults to 3.6923MHz after reset. The MPU clock is scalable by configuring the MPU Clock Control register (MPUCKCtl).

MPU Clock Control Register (MPUCKCtl): 0xFFA1 ← 0x0C

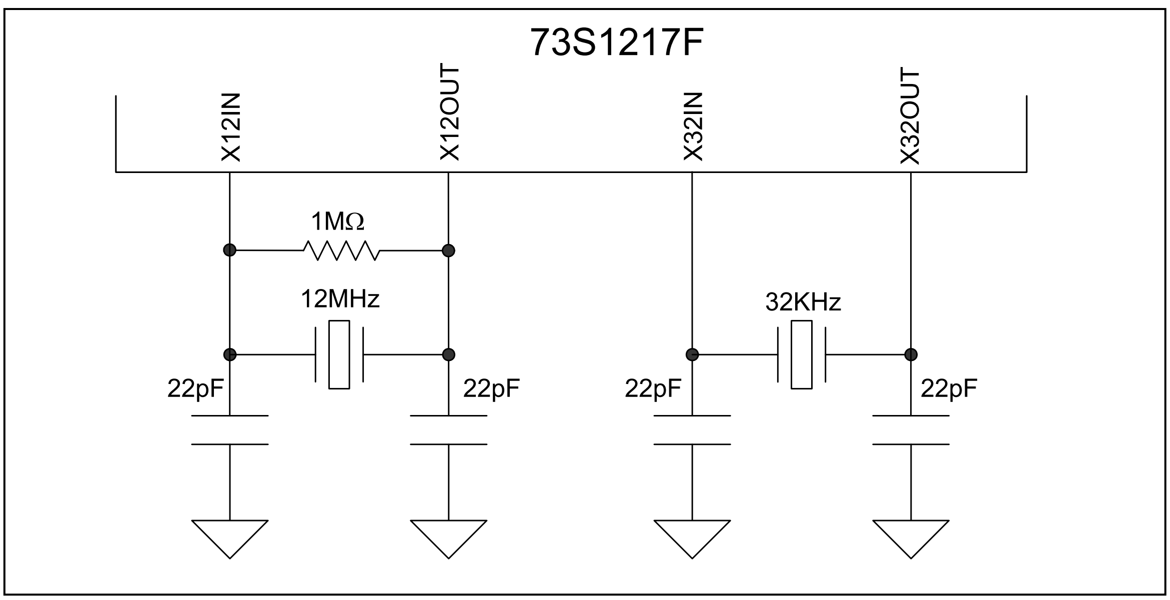
Table 13: The MPUCKCtl Register

MSB							LSB
–	–	MDIV.5	MDIV.4	MDIV.3	MDIV.2	MDIV.1	MDIV.0

Bit	Symbol	Function
MPUCKCtl.7	–	
MPUCKCtl.6	–	
MPUCKCtl.5	MDIV.5	This value determines the ratio of the MPU master clock frequency to the VCO frequency (MCLK) such that MPUClk = MCLK/(2 * (MPUCKDiv(5:0) + 1)). Do not use values of 0 or 1 for MPUCKDiv(n). Default is 0Ch to set CPCLK = 3.6923MHz.
MPUCKCtl.4	MDIV.4	
MPUCKCtl.3	MDIV.3	
MPUCKCtl.2	MDIV.2	
MPUCKCtl.1	MDIV.1	
MPUCKCtl.0	MDIV.0	

The oscillator circuits are designed to connect directly to standard parallel resonant crystal in a Pierce oscillator configuration. Each side of the crystal should include a 22pF capacitor to ground for both oscillator circuits and a 1MΩ resistor is required across the 12MHz crystal.

The CPU clock is available as an output on pin CPUCLK.



Note: The crystals should be placed as close as possible to the IC, and vias should be avoided.

Figure 4: Oscillator Circuit