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

SEC1110/SEC1210

Smart Card Bridge to USB and UART Interfaces

General Description

The SEC1110 and SEC1210 provide a single-chip solution for a Smart Card bridge to USB and UART interfaces. These bridges are controlled by an enhanced 8051 micro controller and all chip peripherals are accessed and controlled through the SFR or XDATA register space. TrustSpan™ Technology enables digital systems to securely communicate, process, move and store information on system boards, across networks and through the cloud.

Feature Highlights

- Smart Card
  - The SEC1110 provides one Smart Card interface and the SEC1210 provides two
  - Fully compliant with ISO/IEC 7816, EMV 4.2/4.3, ETSI TS 102 221 and PC/SC standards
  - Versatile ETU rate generation, supporting current and proposed rates (up to 826 Kbps)
  - Full support of both T=0 and T=1 protocols
  - Full-packet FIFO (261 bytes), for transmit and receive
  - Half-duplex operation (no software intervention required between transmit and receive phases of exchange)
  - Loose real-time response required of software (approximately 180 ms)
  - Dynamically programmable FIFO threshold with byte granularity
  - Time-out FIFO flush interrupt, independent of threshold
  - Programmable Smart Card clock frequency
  - UART-like register file structure
  - Supports Class A, Class B, Class C, or Class AB Smart Cards (1.8 V, 3.0 V and 5.0 V cards)
  - Automatic character repetition for T=0 protocol parity error recovery
  - Automatic card deactivation on card removal and on other system events, including persistent parity errors
  - Internal procedure byte filtering for T=0 protocol
  - Protocol timers (Guard, Timeout, and CWT) for EMV-defined timing parameters
    - –Detection of an unresponsive card
    - –Activation/deactivation sequences
    - –Cold/warm resets
    - –Monitoring for all EMV timing constraints
    - –16-bit general purpose down counter for software timing use
  - Fully compliant ESD protection on card pins
- USB
  - 12 Mbps USB operation compliant to the USB 2.0 Specification
  - Integrated USB 1.5 K pull-up resistor and Dp,Dm series termination resistors
  - Integrated USB devices controller with:
    - –8/16/32/64 byte control buffer
    - –Five 8/16/32/64 byte programmable (bulk/interrupt) endpoint buffers
- 8051 Processor
  - Reduced instruction cycle time (approximately 9 times 80C51)
  - 9.6 MHz max clock speed
  - Enhanced peripherals; three 16-bit timers, watchdog timer, interrupt controller, JTAG
  - OTP (One Time Programmable) ROM : 16 KB RAM : 1.5 KB
- Boot ROM : 16 KB UART (SEC1210 only)
  - — Standard PC baud rates supported
  - — 3 M baud high-speed rate (not PC standard)
- SPI (SEC1210 only)
  - Master capability with 12 MHz max performance
- General
  - 5.0 V tolerance on user accessible IO pins
  - Self-clocking internal oscillator, no external crystal required
  - 3.6 V - 5.5 V supply input
    - –Internal 4.8 V comparator disables Class A card support if the input voltage is too low
  - Available in commercial (0ºC to +70ºC) and industrial (-40ºC to +85ºC) temperature ranges

Applications

- USB Smart Card reader
- UART-based Smart Card reader
- Dual Smart Card reader

TO OUR VALUED CUSTOMERS

It is our intention to provide our valued customers with the best documentation possible to ensure successful use of your Microchip products. To this end, we will continue to improve our publications to better suit your needs. Our publications will be refined and enhanced as new volumes and updates are introduced.

If you have any questions or comments regarding this publication, please contact the Marketing Communications Department via E-mail at **docerrors@microchip.com**. We welcome your feedback.

Most Current Data Sheet

To obtain the most up-to-date version of this data sheet, please register at our Worldwide Web site at:

http://www.microchip.com

You can determine the version of a data sheet by examining its literature number found on the bottom outside corner of any page. The last character of the literature number is the version number, (e.g., DS30000000A is version A of document DS30000000).

Errata

An errata sheet, describing minor operational differences from the data sheet and recommended workarounds, may exist for current devices. As device/documentation issues become known to us, we will publish an errata sheet. The errata will specify the revision of silicon and revision of document to which it applies.

To determine if an errata sheet exists for a particular device, please check with one of the following:

- Microchip's Worldwide Web site; http://www.microchip.com
- Your local Microchip sales office (see last page)

When contacting a sales office, please specify which device, revision of silicon and data sheet (include -literature number) you are using.

Customer Notification System

Register on our web site at **www.microchip.com** to receive the most current information on all of our products.

Table of Contents

1.0 INTRODUCTION

The SEC1110 and SEC1210 provide a single-chip solution for a Smart Card bridge to USB and UART interfaces. These bridges are controlled by an enhanced 8051 micro controller and all chip peripherals are accessed and controlled through the SFR or XDATA register space.

1.1 Features

- Smart Card
  - Fully compliant with standards: ISO/IEC 7816, EMV 4.2/4.3, ETSI TS 102 221 and PC/SC
  - Versatile ETU rate generation, supporting current and proposed rates (to 826 Kbps and beyond)
  - Full support of both T=0 and T=1 protocols
  - Full-packet FIFO (261 bytes), for transmit and receive
  - Half-duplex operation, with no software intervention required between Transmit and Receive phases of an exchange
  - Very loose real-time response required of software: approximately 180 ms worst case
  - Dynamically programmable FIFO threshold, with byte granularity
  - Time-out FIFO flush interrupt, independent of threshold
  - Programmable Smart Card clock frequency
  - UART-like register file structure
  - Supports Class A, Class B, Class C, or Class AB Smart Cards (all 1.8 V, 3.0 V and 5.0 V cards)
  - Automatic character repetition for T=0 protocol parity error recovery
  - Automatic card deactivation on card removal and on other system events, including persistent parity errors
  - Internal procedure byte filtering for T=0 protocol
  - Protocol timers (guard, time-out and CWT) for EMV-defined timing parameters
    - Detection of an unresponsive card
    - Activation/deactivation sequences
    - Cold/warm resets
    - Monitoring for all EMV timing constraints
    - 16-bit general purpose down counter for software timing use
  - Fully compliant ESD protection on card pins per JESD22-A114D (March 2006) and JESD22-A115A “Machine Model” from AN1181
  - Fully EMV compliant, internal signal current limits
  - 3.3 V internal operation with 5.0 V tolerant buffers where required
  - Self-contained management of Smart Card power:
    - SC1_VCC and SC2_VCC, supply output
    - Regulator for 1.8 V, 3.0 V, and 5.0 V from supply input
    - Current limiter with over-current sense interrupt (short circuit detect)
    - Hardware-ensured, compliant deactivation sequence on card removal
    - Synchronous card support
- USB
  - 12 Mbps USB operation compliant with the *USB 2.0 Specification*
  - Integrated USB 1.5 K pull-up resistor
  - Integrated Series resistors on USB_DP, USB_DM
  - Integrated USB devices controller with:
    - 8/16/32/64 byte control endpoint 0 buffer
    - Five 8/16/32/64 byte programmable (bulk/interrupt) endpoint buffers
- 8051
  - Reduced instruction cycle time (approximately 9 times 80C51)
  - 9.6 MHz max clock speed
  - Enhanced peripherals: two 16-bit timers, watch dog timer, interrupt controller, JTAG
  - 16 KB One Time Programmable (OTP) ROM
  - 1.5 KB RAM
  - 4 KB (SEC1100/SEC1200)/ 16KB (SEC1110/SEC1210) ROM

- UART
  - Standard PC (9600, 19200, 38400 and 115200) baud rates supported
  - 3 M baud high-speed rate (non-PC standard)
- SPI
  - Master capability with 12 MHz max performance
- General
  - 5.0 V tolerance on user accessible IO pins
  - Self-clocking internal oscillator, no external crystal required
  - 3.6 V-5.5 V supply input
  - Internal 4.8 V comparator disables Class A card support if the input voltage is too low

1.2 Smart Card Subsystem

The SEC1110 and SEC1210 are fully compliant with the prevailing Smart Card standards: ISO7816, EMV, and PC/SC. It meets and exceeds all existing requirements for communication bit rate (ETU duration) and includes support for proposed bit rates up to 826 Kbps. Signal levels and current limits are also fully compliant.

The Smart Card power is regulated and switched internally, supporting all 5.0 V, 3.0 V, and 1.8 V Smart Cards (classes A, B, and C, respectively). Over-current protection is provided, and a detected over-current condition is available as an interrupt. The required standard activation and deactivation sequences are provided with software interaction. However, deactivation is handled in hardware as the card is being removed. This scenario ensures the required sequence regardless of software participation. If the system clock is inactive at the time, the card movement is detected asynchronously, and the Wake-On Event feature is used to re-start the system clock so that the de-activation sequence can continue.

Interface signals to the Smart Card are designed to meet both standard drive levels and current limitations internally, requiring no external series resistors. ESD protection on these signals meets the full standard requirements.

The device is a superset of the familiar 16450 UART architecture, with extensions in the form of a larger FIFO, specialized state machines for T=0 protocol parsing, automatic half-duplex turnaround at the completion of a transmitted message, and a specially-designed set of timers to enforce standards compliance in timing (as required of a terminal by the ISO7816 and EMV standards).

With the full-packet-depth FIFO on-chip, software is almost totally excluded from real-time requirements. It loads an outgoing message into the FIFO, triggers the transfer, and reads the returned data at any time after it becomes available. The reset sequence (cold or warm) is equally hands-off: software sets up the sequence and activates the reset, and is alerted when the ATR message has been received (via the FIFO Threshold Interrupt). The threshold is dynamically programmable with byte granularity, so that threshold interrupts can be received at various stages in the processing of a message of initially unknown length (such as ATR).

For detecting data time-outs, and for other mandatory timing tasks having to do with communication with a Smart Card, a set of three protocol timers is provided:

- Time-out timer, for monitoring the standard WWT, BWT and WTX time-out intervals
- CWT timer, for monitoring the T=1 CWT time-out interval
- Guard timer, for ensuring the BGT and EGT transmission intervals, with special usage during a Reset sequence.

A separate general purpose timer is provided for software driver use.

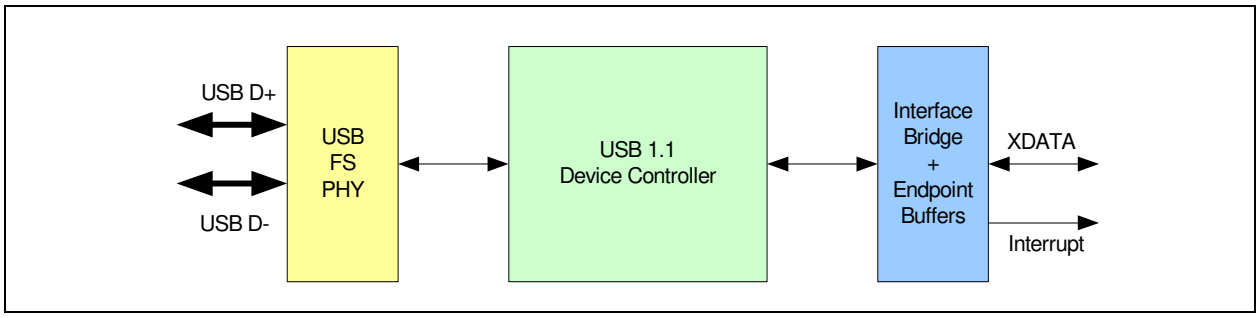
Synchronous card support using GPIOs controlled via registers in the Smart Card device.

1.3 USB Subsystem

The USB Subsystem is made up of the following 3 functional blocks

- FS USB PHY
- USB Device Controller (UDC)
- Interface Bridge with USB endpoint buffers

FIGURE 1-1: USB SUBSYSTEM BLOCK



1.3.1 FS USB PHY AND DEVICE CONTROLLER

The FS USB PHY contains the D+ pull-up resistor and handles the reception of USB data. The D+ and D- signals are passed through the differential receiver (which is external to the device controller core) to get a single-ended bit stream. The device controller has a digital phase-locked loop (DPLL) to extract the clock and data information. The clock and data are passed to the SIE (serial interface engine) block to identify the sync pattern and for NRZI-NRZ conversion. This NRZ data is then passed through a bit-stripper which strips off excessive inserted zeros. The data stream is passed through a PID decoder and checker to identify different PID's. The SIE block handles the protocol according to the type of PID and the endpoint to which the current transaction is addressed. If it is a data PID, the serial data is assembled into byte format and the received data is CRC is checked, then put into a one-byte buffer. The protocol layer takes the data from the buffer and forwards it to the Interface Bridge. On control transfers to endpoint 0, the protocol layer forwards the transfers to the endpoint block. If the application violates the data transfer protocol during the transfer of data from the buffer to the application bus, the protocol layer controls the SIE to recover from this error.

1.3.2 INTERFACE BRIDGE AND ENDPOINT BUFFERS

These act as the interface between the 8051 micro controller and the USB device controller. The USB endpoint buffers are memory mapped on the 8051 XDATA bus. A simple buffer scheme is employed, which assigns a single/ping-pong buffer to each USB endpoint for ease of software control. Each buffer must be cleared before the next data transfer can be started.

When USB OUT data is received, it is placed into the appropriate OUT endpoint buffer and the 8051 is signaled with an interrupt (polling is also available)

When an IN request is received, the 8051 is signaled with an interrupt and the 8051 will transfer data to the appropriate IN endpoint buffer and set a ready flag. The data will automatically be encoded for transfer over the USB bus.

1.4 Power Management Unit

The programmable clock divider supports division of the 48 MHz main clock. Additionally it enables power down under program or hardware control. Exit from power down is accomplished through a single input pin. The power management methods employed will enable a USB Suspend current of 200 μA typical (400 μA typical including Rpu current). In STOP Mode, 1 μA is the maximum current for a bare bones design.

2.0 BLOCK DIAGRAMS

FIGURE 2-1: SEC1110 BLOCK DIAGRAM

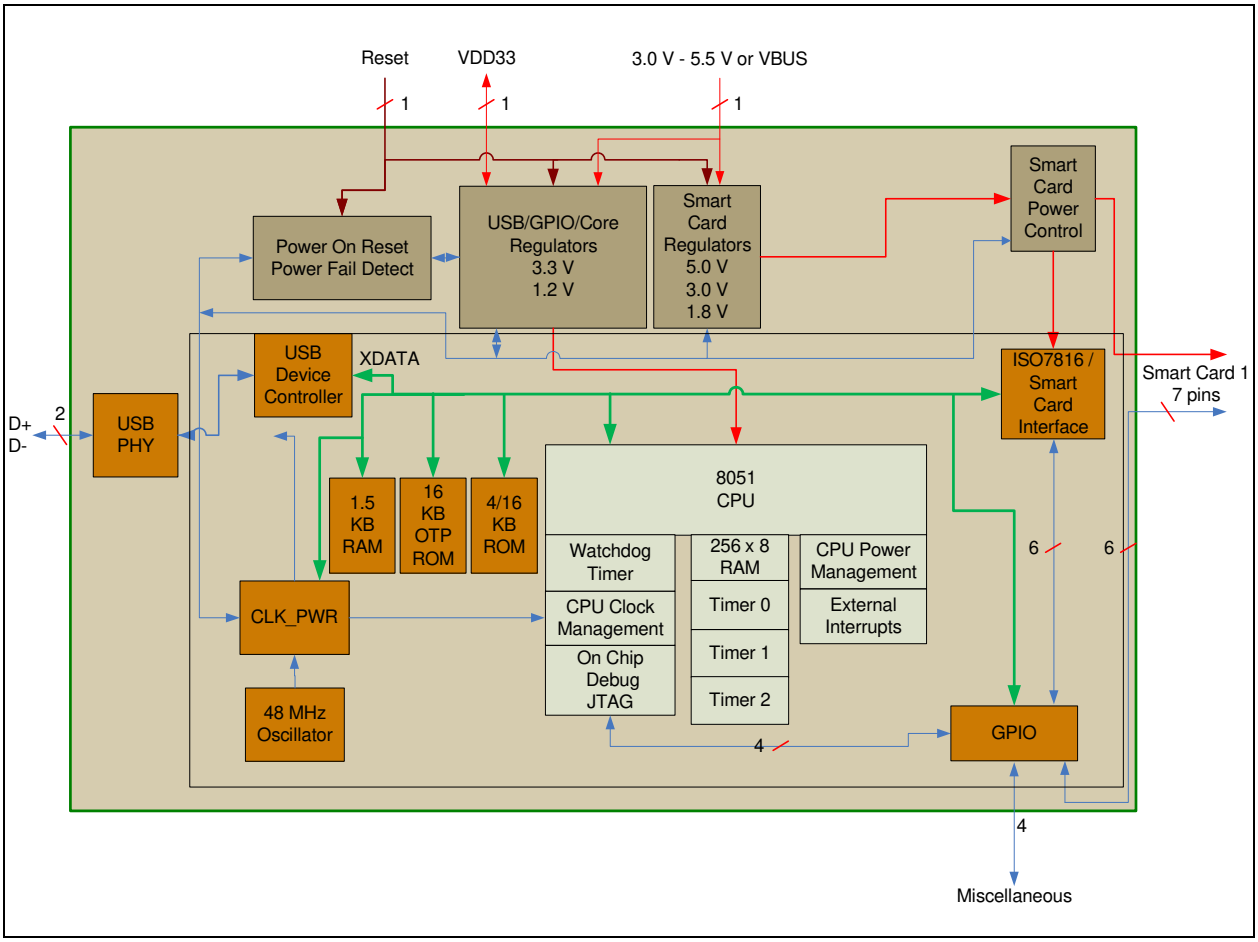
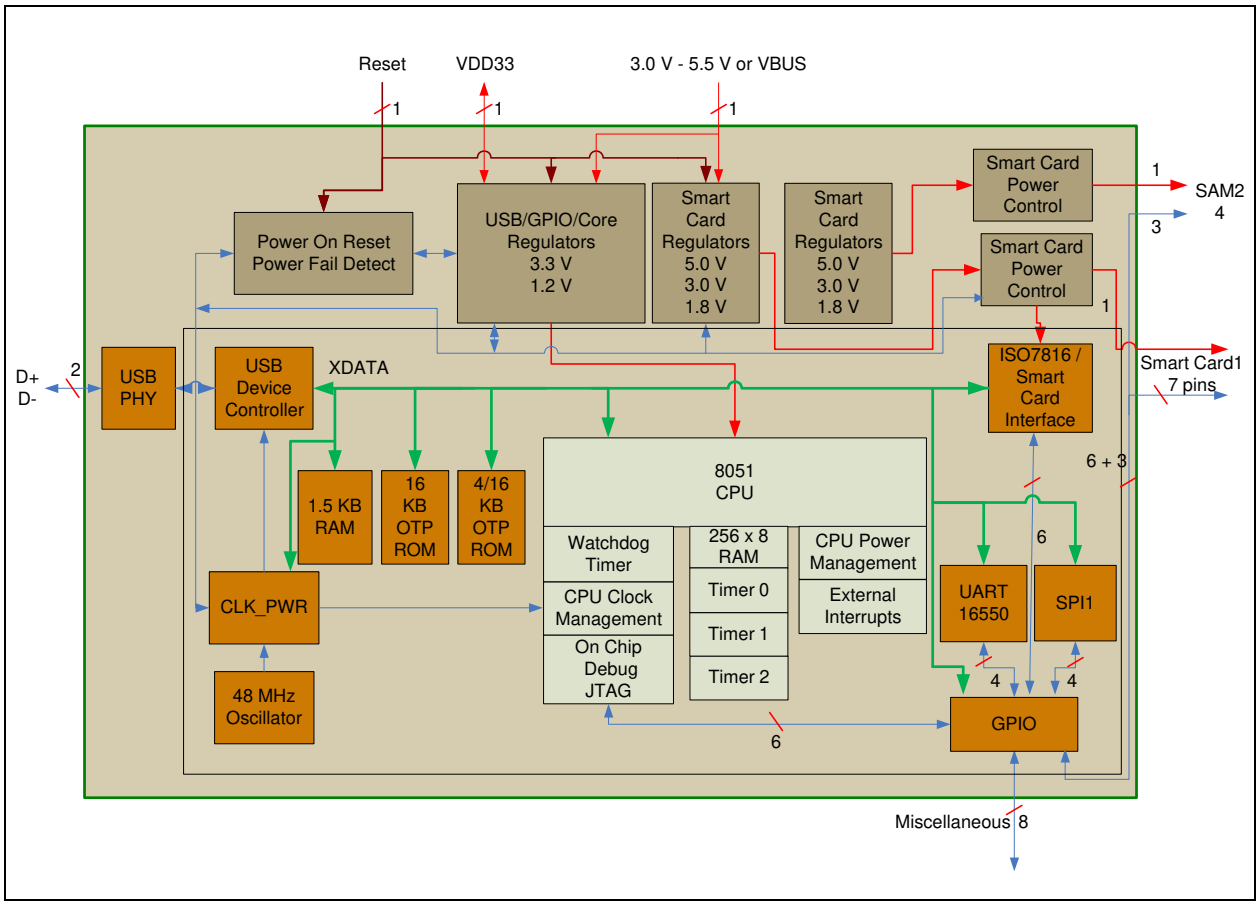


FIGURE 2-2: SEC1210 BLOCK DIAGRAM



3.0 PIN TABLE

3.1 SEC1110 16-Pin QFN

TABLE 3-1: SEC1110 16-PIN PACKAGE

SMART CARD (7 PINS)			
SC1_VCC	Sc1_rst_N	sc1_clk	sc1_io
SC1_C8	SC1_PRSNT_N/ JTAG_TMS	SC1_C4	
USB INTERFACE (2 PINS)			
USB_DP	usb_DM		
MISC (5 PINS)			
RESET_N	SC_LED_ACT_N/ JTAG_TDO	TEST	JTAG_CLK
JTAG_TDI			
DIGITAL, POWER (2 PINS)			
VDD33	VDD5		
TOTAL 16 (VSS - THERMAL SLUG)			

3.2 SEC1210 24-Pin QFN

TABLE 3-2: SEC1210 24-PIN PACKAGE

SMART CARD (7 PINS)			
SC1_VCC	Sc1_rst_N	sc1_clk	sc1_io
SC1_C8	SC1_PRSNT_N/ JTAG_TMS	SC1_C4	
SMART CARD 2/SECURITY AUTHENTICATION MODULE (5 PINS)			
SC2_VCC	Sc2_rst_N	sc2_clk	sc2_io
SC2_PRSNT_N/ JTAG_TDI			
USB INTERFACE (2 PINS)			
USB_DP	usb_DM		
SPI1/UART (4 PINS)			
SPI1_MISO/RXD	SPI1_MOSI/TXD	SPI1_CLK/CTS_OUT	SPI1_CE/RTS_IN
MISC (4 PINS)			

TABLE 3-2: SEC1210 24-PIN PACKAGE

RESET_N	SC_LED_ACT_N/ JTAG_TDO	TEST	JTAG_CLK
DIGITAL, POWER (2 PINS)			
VDD33	VDD5		
TOTAL 24 (VSS - THERMAL SLUG)			

Note: The NC pins are “No Connects”. There are no NC pads in the Known Good Die (KGD).

4.0 PIN CONFIGURATIONS

FIGURE 4-1: SEC1110 16-PIN QFN PACKAGE

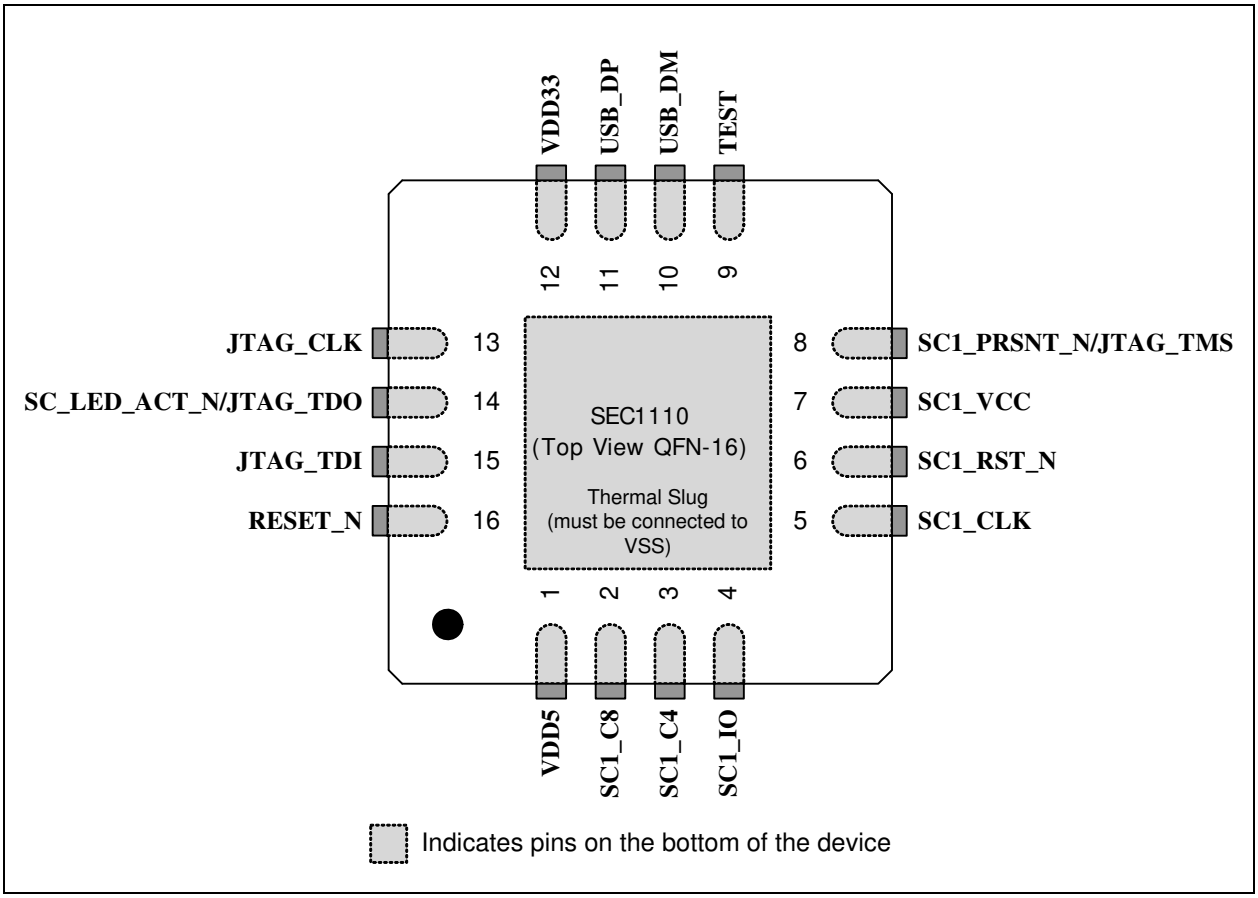
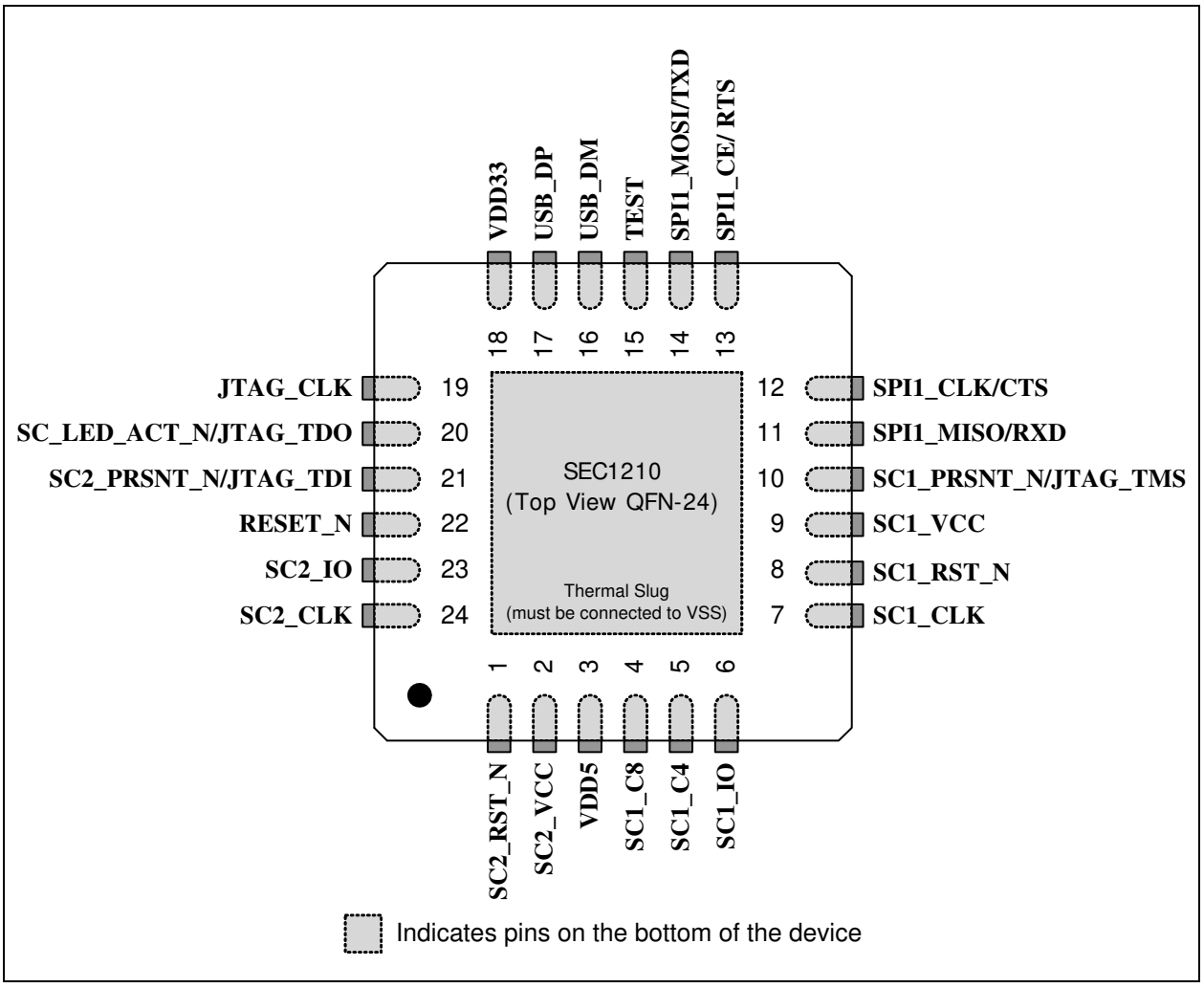


FIGURE 4-2: SEC1210 24-PIN QFN PACKAGE



5.0 PIN DESCRIPTIONS

This section provides a detailed description of each signal. The signals are arranged in functional groups according to their associated interface.

An *N* at the end of a signal name indicates that the active (asserted) state occurs when the signal is at a low voltage level. When the *N* is not present, the signal is asserted when it is at a high voltage level. The terms assertion and negation are used exclusively in order to avoid confusion when working with a mixture of active low and active high signals. The term assert, or assertion, indicates that a signal is active, independent of whether that level is represented by a high or low voltage. The term negate, or negation, indicates that a signal is inactive.

5.1 SEC1110 and SEC1210 Pin Descriptions

TABLE 5-1: SEC1110 AND SEC1210 PIN DESCRIPTIONS

Name	Symbol	Buffer Type	Description
SMART CARD INTERFACE			
SC Reset Output	SC1_RST_N/ GPIO2	Note 5-1	**SC1_RST_N**, **SC2_RST_N**: A low pulse resets the card and triggers an “answer to reset” (ATR) response message. This pin should be held low when the interface is not active.
	SC2_RST_N/ GPIO18		**GPIO2**, **GPIO18**: These pins may alternatively be configured as a general purpose I/O pins.
SC Clock Output	SC1_CLK/ GPIO1	Note 5-1	**SC1_CLK**, **SC2_CLK**: The clock reference for communication with the flash media card. This pin should be held low when the interface is not active.
	SC2_CLK/ GPIO17		**GPIO1**, **GPIO17**: These pins may alternatively be configured as general purpose I/O pins.
SC Data I/O	SC1_IO/ GPIO0	Note 5-1	**SC1_IO**, **SC2_IO**: The bidirectional serial data pin, which should be held low when the interface is not active.
	SC2_IO/ GPIO16		**GPIO0**, **GPIO16**: These pins may alternatively be configured as general purpose I/O pins.
SC Voltage for Card	SC1_VCC/ SC2_VCC		The voltage supply pin, where the output of the pin can be set to 1.8, 3.0, or 5.0 volts, depending on the type of Smart Card detected. These pins require an external1 µF capacitor. The same voltage must be applied to power **SCx_RST#**, **SCx_CLK**, **SCx_IO**, **SCx_C4**, and **SCx_C8** pins as digital inputs.
SC Standard or Proprietary Use Contact	SC1_C8 (SC1_SPU)/ GPIO4	Note 5-1	**SC1_C8**, **SC1_SPU**: These pins can be used for either standard or proprietary use as an input and/or output.
			This pin can alternatively be used as general purpose I/O pin.
SC Present	SC1_PRSNT_N/ JTAG_TMS/ TIMER0_IN/ GPIO6	I/O8PUD	**SC1_PRSNT_N**, **SC2_PRSNT_N**: Active-low signals used to detect the Smart Card device. These pins have an internal pull-up which can be activated by software to detect the Smart Card device.
	SC2_PRSNT_N/ JTAG_TDI/ GPIO19		**JTAG_TMS**, **JTAG_TDI**: These pins can alternatively be configured in debug mode by software.
			GPIO6, **GPIO19**: These pins can alternatively be used as general purpose I/O pins, or as the Timer 0 input pin.
SC1_FCB	SC1_C4 (SC1_FCB)/ GPIO3	Note 5-1	**SC1_C4**: This pin is to attach to C4 of the Smart Card for cards that support Function Code.
			GPIO3: This pin may alternatively be configured as a general purpose I/O pin.

TABLE 5-1: SEC1110 AND SEC1210 PIN DESCRIPTIONS (CONTINUED)

Name	Symbol	Buffer Type	Description
SC Active Indicator	SC_LED_ACT_N/	I/O8PUD	The driver for the active LED.
	JTAG_TDO/		This pin can alternatively be configured in debug mode by software.
	TIMER2_T2EX/ GPIO5		This pin may alternatively be used as general purpose I/O pin, or as the Timer 2 “t2ex” input pin.
USB INTERFACE			
USB Bus Data	USB_DM, USB_DP	I/O-U	These pins connect to the upstream USB bus data signals.
SPI1/UART INTERFACE (QFN24)			
SPI1 Chip Enable	SPI1_CE_N/	I/O8PUD	The active-low chip-enable output (Master mode). If the SPI1 interface is disabled, this pin must be driven high in idle state by software.
	RTS/		This pin can alternatively function as the UART RTS signal, when UART is used instead of SPI1.
	GPIO11		This pin may also be used as a general purpose I/O pin.
SPI1 Clock	SPI1_CLK/	I/O8PUD	The SPI1 clock output (Master mode).
	CTS/		This pin can alternatively function as the UART CTS signal, when UART is used instead of SPI1.
	GPIO10		This pin can alternatively be used as a general purpose I/O pin.
SPI1 Data In	SPI_MISO/	I/O8PUD	The Master data in to the controller. This pin must have a weak internal pull-down applied at all times to prevent floating.
	RXD/		This pin alternatively function as the UART RXD input signal, when UART is used instead of SPI1.
	GPIO8		This pin can alternatively be configured as a general purpose I/O pin.
SPI1 Data Out	SPI_MOSI/	I/O8PUD	This is the Master data output from the controller. This pin must have a weak internal pull-down applied when used as input to prevent floating.
	TXD/		This pin can alternatively function as the UART TXD output signal, when UART is used instead of SPI1.
	GPIO9		GPIO9: This pin can alternatively be used as a general purpose I/O pin.
MISC			
TEST	TEST	I/O8PUD	This signal is used for testing the chip. If the test function is not used, this pin must be tied low externally.
RESET input	RESET_N	IS	This active low signal is used by the system to reset the chip and enter STOP mode. The active low pulse should be at least 1 μs wide. This pin is an analog input signal with Vil=100 mV.
JTAG Clock	JTAG_CLK	I/O8PUD	This input pad is used for JTAG debugging and has a weak pull down. It can be left floating or grounded when not used. If the JTAG is connected, this signal will be detected high, and the software disables the pull-up after reset.
GPIO 28	GPIO28	I/O8PUD	General Purpose I/O pin.
GPIO 29	GPIO29	I/O8PUD	General Purpose I/O pin.
GPIO 30	GPIO30	I/O8PUD	General Purpose I/O pin.

TABLE 5-1: SEC1110 AND SEC1210 PIN DESCRIPTIONS (CONTINUED)

Name	Symbol	Buffer Type	Description
DIGITAL / POWER / GROUND			
VBUS 5V Power	VDD5		5.0 V (or VBUS) power input.
3.3V Analog Power Output	VDD33		3.3 V analog power output for decoupling capacitor. This pad requires an external 1 μF capacitor.
Ground	VSS		Ground reference

Note: All pins OTP_VPP_MON, OTP_VREF, OTP_VREFA, OTP_VREF_SA are NC's.

Note 5-1 This pin has a unique function, detailed in Section 18.0, "DC Parameters," on page 188.

5.2 Buffer Type Descriptions

TABLE 5-2: SEC1110 AND SEC1210 BUFFER TYPE DESCRIPTIONS

Buffer Type	Description
I	Input
IPU	Input with weak internal pull-up resistor
IS	Input with Schmitt trigger
I/O12	Input/output buffer with 12 mA sink and 12 mA source
I/O8PD	Input/output buffer with 8 mA sink and 8 mA source, with an internal weak pull-down resistor
I/O8PU	Input/output buffer with 8 mA sink and 8 mA source with an internal weak pull-up resistor
I/O8PUPD	Input/output buffer with 8 mA sink and 8 mA source, with a selectable pull-up and pull-down resistors
I/OD8PU	Input/open drain output buffer with a 8 mA sink
I/O12PD	Input/output buffer with 12 mA sink and 12 mA source, with an internal weak pull-down resistor
I/O12PU	Input/output buffer with 12 mA sink and 12 mA source with an internal weak pull-up resistor
I/O12PUPD	Input/output buffer with 12 mA sink and 12 mA source, with a selectable pull-up and pull-down resistors
I/OD12PU	Input/open drain output buffer with a 12 mA sink
O12	Output buffer with a 12 mA sink and a 12 mA source
O12PD	Output buffer with 12 mA sink and 12 mA source, with a pull-down resistor
O12PU	Output buffer with 12 mA sink and 12 mA source, with a pull-up resistor
ICLKx	XTAL clock input
OCLKx	XTAL clock output
I/O-U	Analog input/output defined in USB specification
I-R	RBIAS

6.0 PIN RESET STATES

TABLE 6-1: PIN RESET STATES

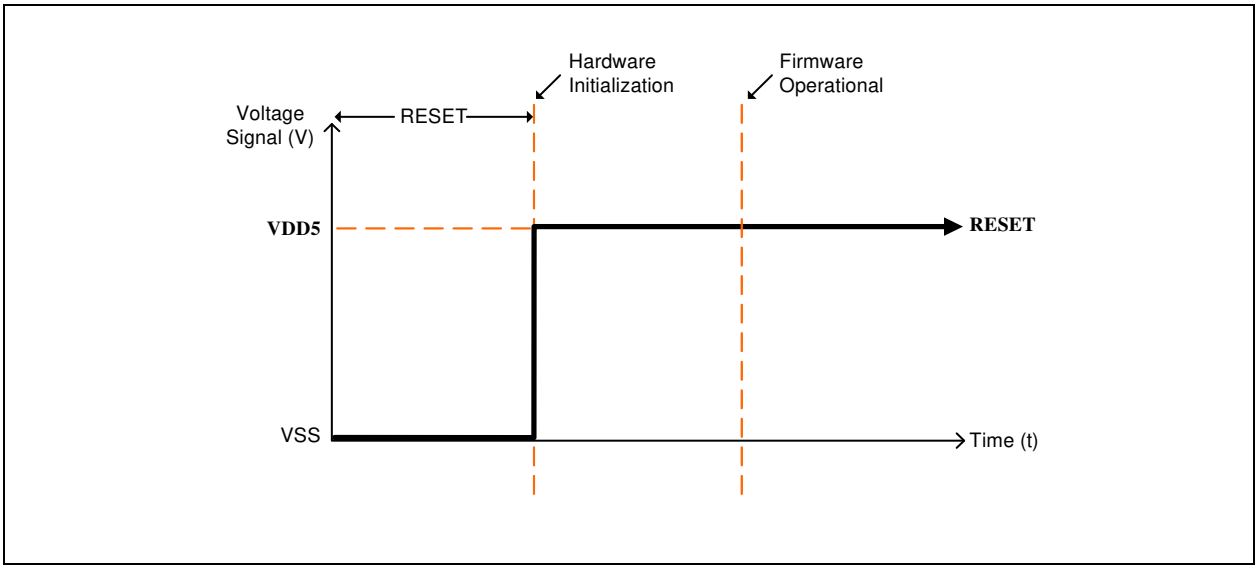


TABLE 6-2: LEGEND FOR PIN RESET STATES TABLE

Symbol	Description
Y	Hardware enables function
0	Output low
1	Output high
--	Hardware disables function
Z	Hardware disables output driver (high impedance)
PU	Hardware enables pull-up
PD	Hardware enables pull-down
HW	Hardware controls function, but state is protocol dependent
(FW)	Firmware controls function through registers
VDD	Hardware supplies power through pin, applicable only to CARD_PWR pins
none	Hardware disables pad

TABLE 6-3: SEC1110 QFN 16-PIN RESET STATES

		Reset State			
Pin	Pin Name	Function	Output	PU/PD	Input
1	VDD5	5.0 V supply			ANALOG
2	SC1_C8	Smart Card1 C8 pin	Z		
3	SC1_C4	Smart Card1 C4 pin	Z		
4	SC1_IO	Smart Card1 IO pin	Z		

TABLE 6-3: SEC1110 QFN 16-PIN RESET STATES

		Reset State			
Pin	**Pin Name**	**Function**	**Output**	**PU/PD**	**Input**
5	SC1_CLK	Smart Card1 CLK pin	Z		
6	SC1_RST_N	Smart Card1 RST_N pin	Z		
7	SC1_VCC	Smart Card1 Power supply output 5.0V/3.3V/1.8V	Note 6-1 Note 6-2		ANALOG
8	SC1_PRSNT_N/JTAG_TMS	GPIO input for Smart Card1 presence detect.	Z		
9	TEST	Test mode pin	Z	**PD** Note 6-8	Yes Note 6-6
10	USB_DM	USB D-	Z		
11	USB_DP	USB D+	Z		
12	VDD33	3.3 V power supply output	Note 6-3		ANALOG
13	JTAG_CLK	JTAG clock pin	Z	**PD** Note 6-4	Yes Note 6-6
14	SC_LED_ACT_N/JTAG_TDO	GPIO output for Smart Card1 LED	Z		
15	JTAG_TDI	JTAG data in pin	Z	**PD** Note 6-8	Yes Note 6-6
16	RESET_N	Reset input	Z		ANALOG Note 6-5
-	VSS	Package ground			ANALOG

TABLE 6-4: SEC1210 QFN 24-PIN RESET STATES

		Reset State			
Pin	**Pin Name**	**Function**	**Output**	**PU/PD**	**Input**
1	SC2_RST_N	Smart Card2 RST_N pin	Z		
2	SC2_VCC	Smart Card2 power supply output 5.0V/3.3V/1.8V	Note 6-1 Note 6-2		ANALOG
3	VDD5	5.0 V supply			ANALOG
4	SC1_C8	Smart Card1 C8 pin	Z		
5	SC1_C4	Smart Card1 C4 pin	Z		
6	SC1_IO	Smart Card1 IO pin	Z		
7	SC1_CLK	Smart Card1 CLK pin	Z		
8	SC1_RST_N	Smart Card1 RST_N pin	Z		
9	SC1_VCC	Smart Card1 Power supply output 5.0V/3.3V/1.8V	Note 6-1 Note 6-2		ANALOG
10	SC1_PRSNT_N/JTAG_TMS	GPIO input for Smart Card1 presence detect.	Z		
11	SPI1_MISO/RXD	GPIO pin for SPI1 data	Z		

TABLE 6-4: SEC1210 QFN 24-PIN RESET STATES

		Reset State			
Pin	**Pin Name**	**Function**	**Output**	**PU/PD**	**Input**
12	SPI1_CLK/CTS	GPIO pin for SPI1 clock	Z		
13	SPI1_CE/RTS	GPIO pin for SPI1 chip enable	Z		
14	SPI1_MOSI/TXD	GPIO pin for SPI1 data	Z		
15	TEST	Test mode pin	Z	**PD** Note 6-8	Yes Note 6-6
16	USB_DM	USB D-	Z		
17	USB_DP	USB D+	Z		
18	VDD33		Note 6-3		ANALOG
19	JTAG_CLK	JTAG clock pin	Z	**PD** Note 6-8	Yes Note 6-6
20	SC_LED_ACT_N/JTAG_TDO	GPIO output for Smart Card1 LED	Z		
21	SC2+PRSNT_N/JTAG_TDI	GPIO input for Smart Card1 presence detect.	Z	**PD** Note 6-8	Yes Note 6-6
22	RESET_N	Reset input	Z		ANALOG Note 6-5
23	SC2_IO	Smart Card2 IO pin	Z		
24	SC2_CLK	Smart Card2 CLK pin	Z		
-	VSS	Package ground			ANALOG

Note 6-1 The Smart Card1 and Smart Card2 power supply output is powered down at reset state.

Note 6-2 The Smart Card1 and Smart Card2 power supply output requires an external 1.0 μF capacitor.

Note 6-3 Internal voltage regulator output for USB, GPIO 3.3 V IO Supply. This pin requires an external 1.0 μF capacitor.

Note 6-4 A weak pull down is present on the **TEST**, **JTAG_CLK**, and **JTAG_TDI** pads. If JTAG is connected, and this pad is pulled high, then the reset state of the pins 8 (**JTAG_TMS**), 13(**JTAG_CLK**), 14(**JTAG_TDO**), and 15(**JTAG_TDI**) functions in JTAG Mode. The weak pull-down can be disabled after reset release by software.

Note 6-5 **RESET_N** is an analog input, which when low, powers down all internal voltage regulators and the pads are in high impedance state. The pads function as input, including pull-ups pull-downs functionality after internal 3.3V power (VDD33) is good.

Note 6-6 The **TEST**, **JTAG_CLK**, and **JTAG_TDI/GPIO[19]** values at internal power on reset release (after **RESET_N** release) is captured in the chip to enter various functional or test modes.

Note 6-7 Smart Card2 power supply output is powered down at reset state.

Note 6-8 A weak pull-down is present on **TEST**, **JTAG_CLK**, and **JTAG_TDI** pads if JTAG is connected, and this pad is pulled high. The reset state of the pins 10(**JTAG_TMS**), 19(**JTAG_CLK**), 20(**JTAG_TDO**), and 21(**JTAG_TDI**) function in JTAG Mode. The weak pull-down can be disabled after reset release by software.

Note 6-9 The LCD regulator LDO4 and Smart Card2 output is powered down at reset state.

7.0 8051 EMBEDDED CONTROLLER

The embedded controller used in the SEC1110 and SEC1210 is an R8051XC2 from Evatronix. The R8051XC2 is a high performance 8-bit embedded processor. The processor core is a low gate count core, with low-latency interrupt processing that features:

- Single clock per machine cycle: an average of 2.12 machine cycles per instruction
- Industry standard MCS51 instruction set
- Dual Data Pointers (2 x DPTR)

The R8051XC2's interrupt controller is closely integrated with the processor core to achieve low latency interrupt processing, incorporating the following features:

- 13 external interrupts
- 4 priority levels for each interrupt

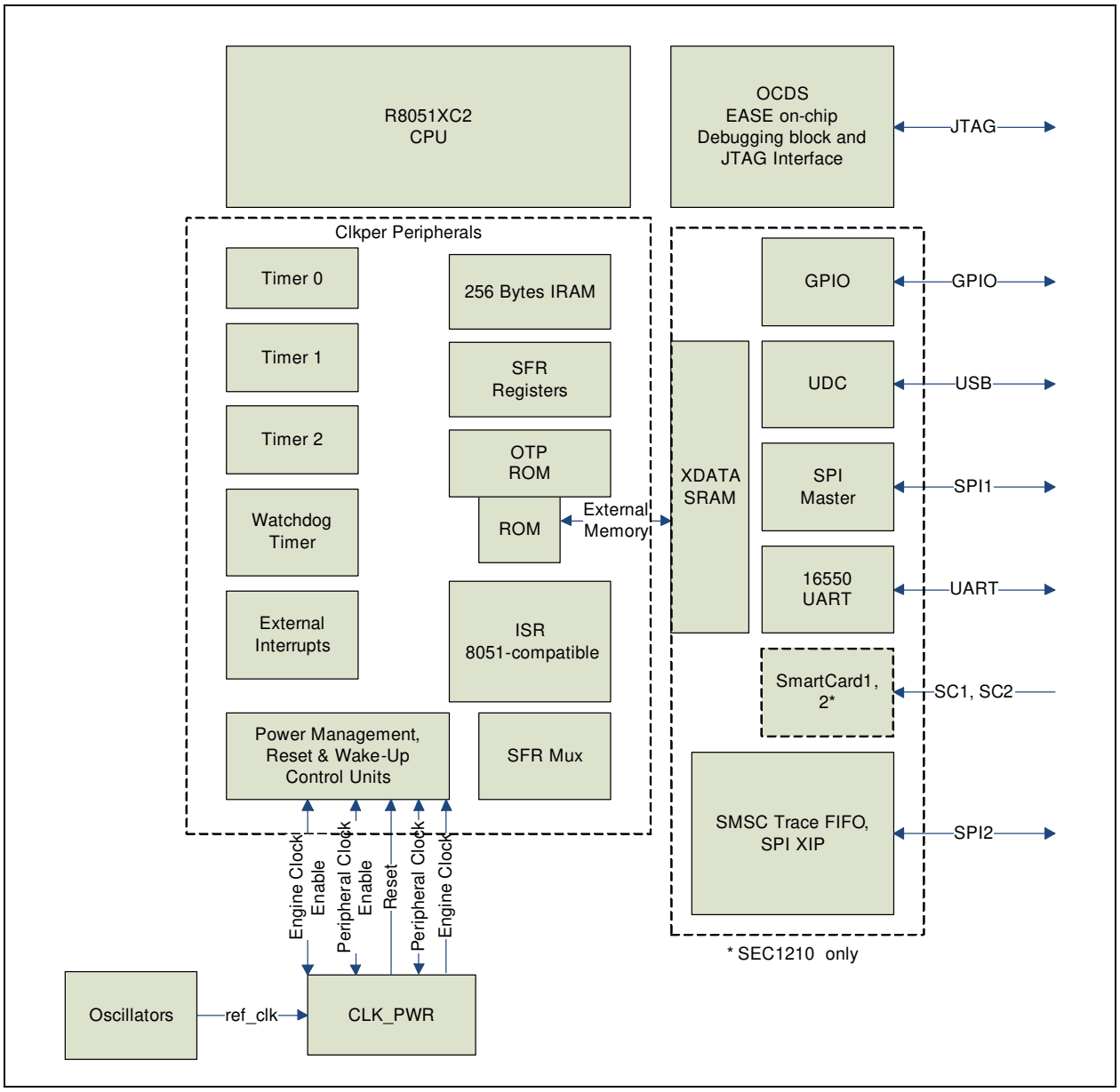
The embedded controller provides low-cost debug solutions, including:

- JTAG port for debugging using EASE OCDS debugging
- Software and 4 hardware breakpoints

The R8051XC2 bus interfaces include:

- 256 bytes internal data memory RAM
- Program Memory Write Mode
- Supports 128 KB program memory space with banking
- Supports 128 KB of external data memory space with banking

FIGURE 7-1: R8051XC2 Block Diagram



.

7.1 Sleep/Power Management

The R8051XC2 has a power management control unit that generates clock enable signals for the main CPU and for peripherals; serves Power Down Modes IDLE and STOP; and generates an internal synchronous reset signal (upon external reset, watchdog timer overflow, or software reset condition). The IDLE Mode leaves the clock of the internal peripherals running. Any interrupt will wake the CPU.

The STOP Mode turns off all internal clocks. The CPU will exit this state when an external interrupt (0 or 1)or reset occurs and internally generated interrupts are disabled since they require clock activity.

The Wake-up From Power-Down Mode control unit services two external interrupts during power-down modes. They can combinationally force the clock enable outputs back to active state so the clock generation can be resumed.

7.1.1 EC DATA MEMORY

The EC has 1.5 KB data memory that is accessed through the XDATA Bus which is implemented with static RAM and organized as 1.5 K x 8 bits. The base address of the memory is 8000h in the EC address space and extends to location 85FFh.

7.1.2 EC OTP INSTRUCTION MEMORY

The primary instruction memory for the EC is a 16 Kx 8 bit OTP ROM memory, located at locations 0000h through 3FFFh in the EC address space. There is also a 4 K x 8 bit ROM that is used to overlay the OTP memory when it has not been programmed. A bit in the OTP disables the ROM overlay. The OTP memory is also mapped into the XDATA space when the overlay is active so that the CPU can program the OTP from the USB bus.

7.2 EC Registers

TABLE 7-1: CODE EXECUTION TRUTH TABLE

OTP_CFG.FORCE_OTP_ROM	OTP_CFG.OTP_ROM_EN	EXT_SPI_EN/ BOND[2]	CODE EXECUTION
0	X	1	External SPI2
0	0	0	ROM
0	1	0	OTP
1	X	X	OTP

The truth table indicates which memory is mapped into the 8051 CODE space depending on the three signals ROM_EN, defined in the OTP_CFG Register. OTP_ROM_EN, and the EXT_SPI_EN (**BOND2** bond option).

7.3 EC Memory Map

TABLE 7-2: CODE SPACE

Name	Address Range
INTERNAL ROM (4 K) (SEC1110 and SEC1210) INTERNAL ROM (16 K) (later versions)	0000h-0FFFh C000h-CFFFh (alias address range) (deprecated) 18000h-18FFFh (alias address range) 1A000h-1DFFFh (alias address range) (later versions)
OTP ROM (16 K)	0000h-3FFFh
EXTERNAL SPI	0000-FFFFh
SRAM (1.5 K)	19000h-195FFh (alias address range)

TABLE 7-3: XDATA SPACE RANGES

Name	Address Range
OTP ROM (Note 7-1)	0000h-7FFFh
SRAM (1.5 K)	8000h-85FFh
Smart Card1,2	9000h-93FFh
UART	9500h-95FFh
USB DEVICE CONTROLLER	9600h-96FFh
SPI2 CODE MASTER	9A00h-9A18h
GPIO	9C00h-9DFFh
CLK_PWR	A000h-A3FFh
OTP_TEST	A400h-A7FFh
SPI2 CODE MASTER (TRACE FIFO)	BFFEh-BFFFh
INTERNAL ROM (4 K) (SEC1110 and SEC1210) INTERNAL ROM (16 K) (later versions)	C000h-CFFFh (alias address range) (deprecated) 18000h-18FFFh (alias address range) 1A000h-1DFFFh (alias address range) (later versions)

Note 7-1 OTP ROM is only visible in the XDATA space if the Internal ROM is enabled (see Table 7-1).

There is 128 KB of program space available. The lower 32 KB always is mapped to 0000-7FFFh. The higher ranges 32 KB to 128 KB are accessed through a window at 8000h-FFFFh using the pagesel registers.The ROM and SRAM are also mapped to address at 96 KB. This enables access to ROM code while executing from OTP_ROM. This also enables downloading code to SRAM and executing for test modes.

TABLE 7-4: CPU BOOT ADDRESS MAPPING

CPU CODE MAPPED ADDRESS[15:0]	CPU UNMAPPED ADDRESS[16:0]			COMMENT
	INTERNAL ROM BOOTING	**INTERNAL OTP_ROM BOOTING**	**EXTERNAL SPI BOOTING**	
	FORCE_OTP_ROM=0 OTP_ROM_EN=0	**(FORCE_OTP_ROM=1) | (EXT_SPI_EN=0 & OTP_ROM_EN=1)**	**FORCE_OTP_ROM=0 & EXT_SPI_EN=1**	
00000h-7FFFh	ROM= 00000h-00FFFh	OTP_ROM_16K= 00000h-03FFFh	EXT_SPI= 00000h-07FFFh	If size of internal ROM/ OTP_ROM/ External SPI is less than 32KB, then rest of the region is reserved. pagesel[2:0]=000 must not be used.
8000h-FFFFh		Reserved= (OTP_ROM_16K) 08000h-0FFFFh	EXT_SPI= 08000h-07FFFh	pagesel[1:0]=01 Upper 32K of ROM/OTP_ROM/EXT_ SPI code execution
8000h-FFFFh				pagesel[1:0]=10 32KB OTP_ROM code execution

TABLE 7-4: CPU BOOT ADDRESS MAPPING

CPU CODE MAPPED ADDRESS[15:0]	CPU UNMAPPED ADDRESS[16:0]			COMMENT
8000h-FFFFh	Reserved= 18000h-1FFFFh	ROM= 18000h-18FFFh	ROM= 18000h-18FFFh	pagesel[1:0]=11 SRAM code execution
	SRAM_1.5K= 19000h-195FFh	SRAM_1.5K= 19000h-195FFh	SRAM_1.5K= 19000h-195FFh	
	Reserved= (SRAM_1.5K) 19600h-19FFFh	Reserved= (SRAM_1.5K) 19600h-19FFFh	Reserved= (SRAM_1.5K) 19600h-19FFFh	
	In SEC1110/SEC1210 ROM= 1A000h-1DFFFh else Reserved= 1A000h-1FFFFh	In SEC1110/SEC1210 ROM= 1A000h-1DFFFh else Reserved= 1A000h-1FFFFh	In SEC1110/SEC1210 ROM= 1A000h-1DFFFh else Reserved= 1A000h-1FFFFh	

8.0 EC EXTERNAL INTERRUPTS

8.1 General Description

The R8051XC2 is 80515-compatible and will be configured to support thirteen external interrupt sources and four priority levels. In addition, there are individual internal interrupt sources for the R8051XC2 configured peripherals such as the timers and SPI1 interfaces. Each source has its own request flag(s). Each interrupt requested by the corresponding flag can be individually enabled or disabled by dedicated enable bits in the SFRs.

8.2 Interrupt Summary

TABLE 8-1: INTERRUPT VECTOR MAPPING

INTERRUPT INTPUT/ VECTOR	SOURCE	DESCRIPTION
int_vect_03	ie0	External Interrupt 0 - all interrupts ORed except GPIOs In SEC1110/SEC1210 version, the SPI1, Power Status interrupts will not cause an ie0 interrupt.
int_vect_0B	t0_f0	Timer 0 overflow
int_vect_13	ie1	External Interrupt 1 - GPIO Port 0,1,2 interrupts
int_vect_1B	tf1_gate	Timer 1 overflow
int_vect_23	uart_int	Serial Port 0 Interrupt
int_vect_2B	unused	Reserved
int_vect_43	iex7_gate	External Interrupt 7 - Reserved
int_vect_4B	iex2_gate	External Interrupt 2 - SPI1 Interrupt
int_vect_53	EP3INT	External Interrupt 3 - Endpoint 3 Interrupt. Also is active for Timer2 crc/cc0 comparator output.
int_vect_5B	EP4INT	External Interrupt 4 - Endpoint 4 Interrupt. Also is active for Timer2 cc1 comparator output.
int_vect_63	USB_INT_REG	External Interrupt 5 - USB Interrupt. Also is active for Timer2 cc2 comparator output. In SEC1110/SEC1210, the Timer2 cc2 comparator output will not cause an interrupt.
int_vect_6B	POWER_STS	External Interrupt 6 - Power status event. Also is active for Timer2 cc3 comparator output. In SEC1110/SEC1210, the Timer2 cc3 comparator output will not cause an interrupt.
int_vect_83	unused	External Interrupt -Reserved
int_vect_8B	EP1INT	External Interrupt 8 - Endpoint 1 Interrupt
int_vect_93	EP2INT	External Interrupt 9 - Endpoint 2 Interrupt
int_vect_9B	EP5INT	External Interrupt 10 - Endpoint 5 Interrupt
int_vect_A3	EP0INT	External Interrupt 11 - Endpoint 0 Interrupt
int_vect_AB	iex12	External Interrupt 12 - Smart Card1 and Smart Card2 Interrupt

Note: In SEC1110/SEC1210 version, External Interrupts 4, 5, and 6 are not active when TImer2 comparator outputs for cc1, cc2, and cc3 respectively are active. This *Anomaly 24* is fixed in later versions.

8.3 EC ISR

The Interrupt Service Routine (ISR) unit, is a subcomponent responsible for interrupt handling. It receives up to 19 interrupt requests. Each of the interrupt sources can be individually enabled or disabled by the corresponding enable flag in the ien0, ien1, ien2, and ien4 SFR registers. Additionally all interrupts can be globally enabled or disabled by the ea flag in the ien0 Special Function Register.

All interrupt sources are divided into 6 interrupts groups. The definition of each group is shown in Table 8-2.

TABLE 8-2: INTERRUPT PRIORITY GROUPS

	Highest Priority in Group						Lowest Priority in Group	
GROUP	INTERRUPT VECTOR	INTERRUPT ENABLE BIT NAME(BIT)	INTERRUPT VECTOR	INTERRUPT ENABLE BIT	INTERRUPT VECTOR	INTERRUPT ENABLE BIT	INTERRUPT VECTOR	INTERRUPT ENABLE BIT
Group0	int_vect_03 (External Interrupt 0 - all interrupts ORed except GPIOs)	ien0(0)	int_vect_83 (unused)	ien2(0)			int_vect_43 (External Interrupt 7 - reserved)	ien1(0)
Group1	int_vect_0B (Timer 0 Interrupt)	ien0(1)	int_vect_8B (External Interrupt 8 - Endpoint 1)	ien2(1)			int_vect_4B (External Interrupt 2 - SPI1 Interrupt)	ien1(1)
Group2	int_vect_13 (External Interrupt 1 - GPIO 0,1,2)	ien0(2)	int_vect_93 (External Interrupt 9 - Endpoint 2)	ien2(2)			int_vect_53 (External Interrupt 3- Endpoint 3)	ien1(2)
Group3	int_vect_1B (Timer 1 Interrupt)	ien0(3)	int_vect_9B (External Interrupt 10 - Endpoint 5)	ien2(3)			int_vect_5B (External Interrupt 4- Endpoint 4)	ien1(3)
Group4	int_vect_23 (16550 UART Interrupt)	ien0(4)	int_vect_A3 (External Interrupt 11 - Endpoint 0)	ien2(4)			int_vect_63 (External Interrupt 5- USB Interrupt)	ien1(4)
Group5	int_vect_2B (Timer 2 Interrupt)	ien0(5)	int_vect_AB (External Interrupt 12 - Smart Card 1/2)	ien2(5)	int_vect_EB (reserved)	ien4(5)	int_vect_6B (External Interrupt 6 - Power Status Event)	ien1(5)

Inside a group, hardware dictates the interrupt priority structure. Interrupt sources from the first column have the highest priority, sources from second column have middle priority, and sources from last column have the lowest priority. The interrupt priority inside the group cannot be changed, where there is also an interrupt priority structure between the groups. Group0 has the highest priority and Group5 has the lowest. The priority between groups can be programmed by changing priority level (priority level can be set from 0 to 3) that is assigned to each group. The priority level of an interrupt group is defined by flags of the ip0 and ip1 SFRs. When the priority levels for two groups are programmed to the same level, the priority among them is in the order, from high to low (Group0 down to Group5).

To determine which interrupt has the highest priority (which must be serviced in the first order) the following steps are completed:

1. From all groups, those with the highest priority level are chosen.
2. From those with the highest priority level, the one with the highest natural priority between the groups in chosen.
3. From the group with highest priority, the interrupt with the highest priority inside the group is chosen.

The currently running interrupt service subroutine can be interrupted only by interrupts with a higher priority level. No interrupt with the same or lower priority level can interrupt the currently running interrupt service subroutine. Therefore there can be a maximum of four interrupts in service at the same time.