SECTION 3: SECURE MICROCONTROLLER ARCHITECTURE

Introduction

The Secure Microcontroller family is based on an 8051 compatible core with a memory interface and I/O logic build around it. Many functions are identical to standard 8051s and are documented here for completeness. In general, most architecture features apply to all members of the Secure Microcontroller family. When there is a difference between versions, this will be mentioned. A block diagram of the microcontroller core is shown in Figure 3–1 below.

Bus Organization

There are four major busses in the Secure Microprocessor: the Internal Data Bus, the Internal Address Bus, the Byte–wide Memory Bus, and the Expanded Bus. All addresses and data which are transferred during program execution are passed on the Internal Address and Data Busses. User Program and Data Memory is always accessed from either the byte–wide Program/Data RAM or from external memory located on the Expanded Bus.

The Byte–wide Memory Bus is used for access to Program/Data RAM in the same fashion as an 8051 Family device would access internal ROM or EPROM memory. This bus can be used in place of the Expanded Bus, freeing Port 2 and Port 0 pins for general I/O use.

CPU Registers

All of the CPU registers are mapped as Special Function Registers (SFR's) and are identical in number and function to those present within the 8051. These registers are described briefly below:

Accumulator

The Accumulator (A) is used as either a source or destination register in all arithmetic instructions. It may also be used in most other types of instructions.

Stack Pointer

The Stack Pointer (SP) is an 8–bit register which is used to mark the location of the last byte of data stored in the stack. The stack itself may be located anywhere in the on–chip 128–byte Scratchpad register area. The Stack Pointer pre-increments during a stack push and post-decrements during a stack pop.

B Register

The major function of the B register is as a source and destination register during multiply and divide instructions. It may also be used as a scratchpad register.

Program Status Word

The Program Status Word (PSW) contains status flags that are set according to the results of a previously executed instruction. In addition, the PSW contains register bank select bits.

Data Pointer

The Data Pointer (DPTR) is used to access Data Memory that may be mapped into Byte–wide Data RAM or onto external memory devices on the Expanded Bus. It is accessed by the user's program as either two 8–bit Special Function registers or as a 16–bit register with certain instructions.

Scratchpad Registers

Scratchpad registers are 128 registers where data may be stored directly. They are addressed from 00H to 7FH and may be accessed by a MOV instruction. Included in the scratchpad area are four 8–byte banks of working registers. These registers are not part of the data memory map.

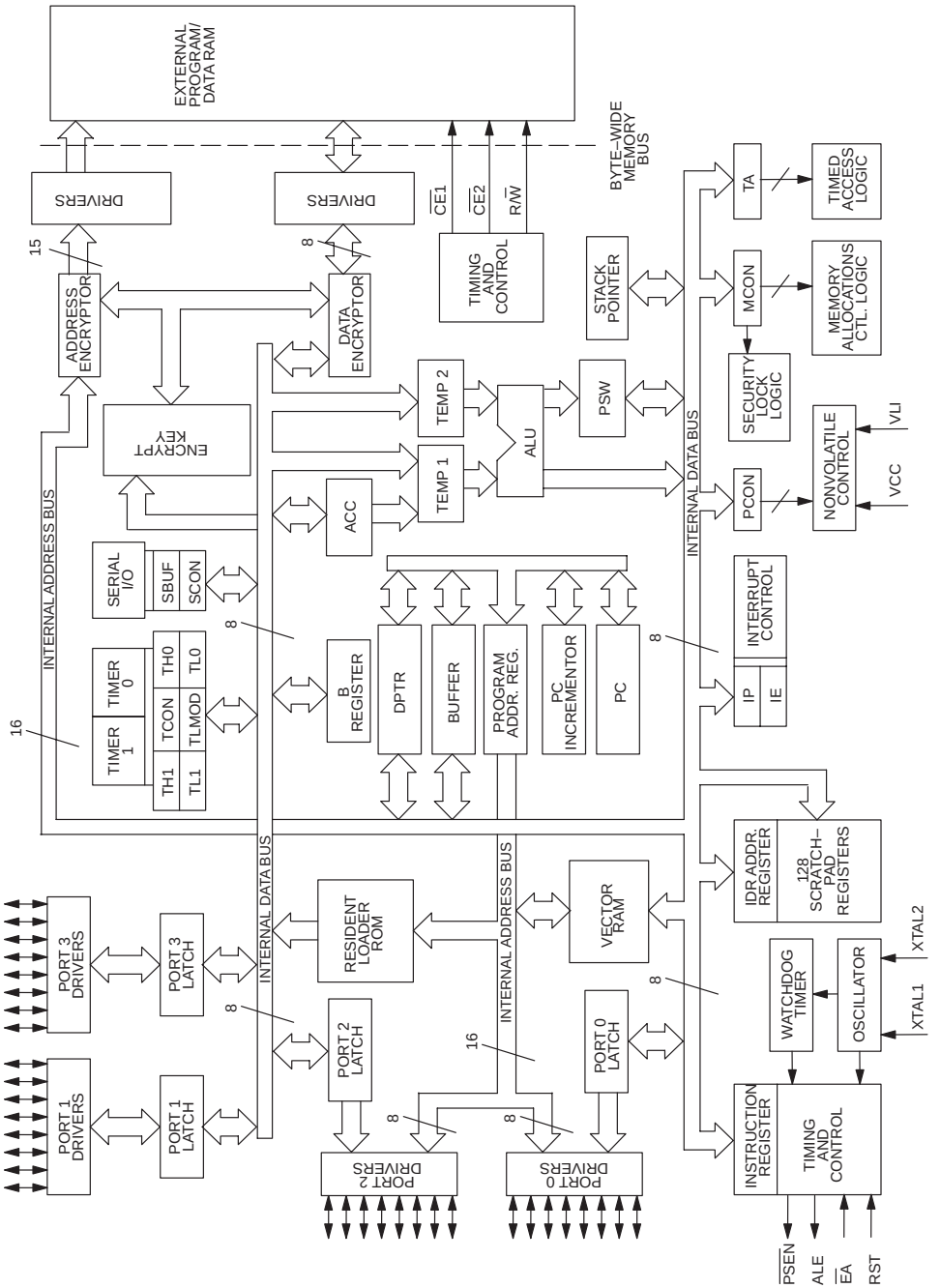
Serial I/O

The on–chip serial I/O port is comprised of a receive data buffer, a transmit data buffer, and a control register. Both the receive data buffer and the transmit data buffer are accessed in a single location (SBUF) in the Special Function Register map. The control register (SCON) is accessed in an separate location. When the serial I/O function is enabled, two external I/O pins (P3.0, P3.1) are re–assigned in hardware to serve the transmit and receive data functions.

Programmable Timers

Two 16–bit programmable timers are included that can perform various timing and counting functions. A total of four registers (TH1, TL1, TH0, and TL0) access the upper and lower halves of each of the two timer/counters. A single control register (TCON) is used to select the various operating modes of the two timers. Two external I/O pins (P3.4, P3.5) may be programmed to serve as external counter inputs, one pin for each of the two timer/counters.

SECURE MICROCONTROLLER ARCHITECTURAL BLOCK DIAGRAM Figure 3–1



Parallel I/O

Four SFR's provide access for the four parallel I/O port latches. These I/O ports are denoted as P0, P1, P2, and P3. A total of 32 bits of parallel I/O is available through these I/O ports. However, up to 16 bits are sacrificed when the Expanded Bus mode is used to interface to external memory and up to six bits may be sacrificed if any external interrupt inputs, timer counter inputs, or serial I/O functions are used. When using the Byte–wide bus, ports are not affected.

Program/Data RAM Interface

Secure Microcontrollers provide a non–multiplexed Byte–wide bus that connects to external SRAM. They also make this RAM nonvolatile, decode memory access for it, and write–protect portions designated as program memory. The Byte–wide bus consists of up to 16 address lines (depending on the version), eight data lines, read/write control, and decoded chip enables. When accessing the SRAM via its Byte–wide bus, there is no activity on the ports. Thus if memory access is restricted to this bus, all ports are free for use by the application. In module form, the microprocessor is already connected to SRAM via the Byte–wide bus making program and data memory access appear internal.

Secure Microprocessors can also access memory using the multiplexed Expanded Bus consisting of Port 0 and 2, $\overline{WR}$ (P3.6) and $\overline{RD}$ (P3.7). This is usually undesirable since it consumes port pins that can be used for other activity. If Expanded bus access is desired, up to 64K ROM and 64K RAM can be accessed in the same manner as a traditional 8051. Each version has different provisions for using the Expanded bus, depending on memory map and user's configuration. These issues are discussed under the Programmer's Guide.

High–Reliability Circuitry

This feature ensures proper operation of the micro and maintains the contents of the Program/Data RAM in the absence of V_{CC} using a self–contained lithium energy source. The logic provided includes the Power Fail Warning Interrupt, Automatic Power Down and Power On Reset. As a result, the Program/Data RAM may be modified whenever necessary during execution of the user's software but will remain unchanged when V_{CC} is absent. The circuitry also maintains the Internal Scratchpad RAM and certain Special Function registers during a power down condition.

Software Encryption Logic

DS5000 and DS5002 series parts provide software security circuits that include the Address Encryptor, Data Encryptor, and the Encryption Key Word. When the device is operating in the Encryption mode and using the Program/Data RAM, the Address Encryptor is used to transform "logical" addresses on the Internal Address Bus into encrypted addresses which appear on the Byte–wide Memory Bus to the RAM. Similarly, the Data Encryptor transforms data on the Internal Data bus into encrypted data during write operations on the Byte–wide Memory bus. When data is read back, the Data Encryptor restores it to its true value. Although each encryptor uses its own algorithm for encrypting data, both depend on the Encryption Key Word stored on–chip.

Security Lock Logic

The Security Lock logic prevents a read or write to any Program/Data RAM location using the bootstrap loader. In addition, it inhibits the device from fetching code in the Expanded Bus Mode. By disabling access to key internal resources, this feature precludes unauthorized disassembly of application software contained in Program/Data RAM. In contrast with an EPROM security bit, clearing the Security Lock wipes the entire RAM area.

Vector RAM

The Vector RAM is used to contain the reset and interrupt vector code when the Soft Microcontroller is operating in the Encryption mode. This feature is included to insure the security of the application software. The operation of the Vector RAM as well as the reason for its inclusion in the architecture are discussed in the Software Security section.

Timed Access Logic

The Timed Access logic is used to protect against inadvertent changes to configuration and to the Program RAM in the event of a loss of software control. The protected configuration parameters include the Partition Address bits in the MCON register, as well as the Enable Watchdog Timer bit, Stop Mode bit, and Power On Reset bit in the PCON register.

Watchdog Timer

When the user's software is being executed, the Watchdog Timer can be used to automatically restart the processor in the event that software control is lost. It is also used to generate an oscillator start–up delay to allow the clock frequency to stabilize. This occurs during reset cycles that follow a time in which the oscillator has been stopped (Stop Mode Reset and Power On Reset).

Resident Loader ROM

The Resident Loader ROM contains firmware that controls the initial loading of the nonvolatile Program/Data RAM. The firmware provides Serial Bootstrap Load operation via the on–chip serial port. The internal ROM is not accessible by the user and performs the loading function only when the device is strapped for operation in the Program mode. The ROM becomes transparent to the user once loading is complete and has no effect on the memory map.