

SECTION 1: INTRODUCTION

The Secure Microcontroller family is a line of 8051-compatible devices that utilize nonvolatile RAM (NV RAM) rather than ROM for program storage. The use of NV RAM allows the design of a "soft" microcontroller which provides a number of unique features to embedded system designers. Foremost among these is the enhanced security features that are employed by the Secure Microcontroller Family to protect the user application software against piracy and tampering. These devices offer varying degrees of security, ranging from simple access prevention to a full encryption of program and data memory of the device. Attempts to gain access to protected information will result in the self-destruction of all data. The Secure Microcontroller family is the heart of a wide range of security-critical applications such as electronic banking, commercial transactions, and pay TV access control, or any situation which requires the protection of proprietary software and algorithms.

The Secure Microcontroller family is divided between chips and modules. The chips are monolithic microprocessors that connect to a standard SRAM and lithium battery. The modules combine the microprocessor with the SRAM and lithium battery in a preassembled, pretested module. Depending on the specific configuration, modules are available in either 40-pin encapsulated DIP or SIMM module format.

In addition to NV RAM, Dallas Semiconductor microcontrollers offer a number of peripherals that simplify and reduce the cost of embedded systems. Although the specific features of each chip or module vary, all devices offer the following basic feature set:

- 100% code-compatible with 8051
- Directly addresses 64KB program/64KB data memory
- Nonvolatile memory control circuitry
- 10-year data retention in the absence of power
- In-system reprogramming via serial port
- 128 bytes fast access scratchpad RAM
- Two 16-bit general purpose timer/counters
- One UART
- Five interrupts with two external

- Dedicated memory bus, preserving four 8-bit ports for general purpose I/O
- Power-Fail Reset
- Early Warning Power Fail Interrupt
- Watchdog Timer

SOFTWARE SECURITY

One of the most important features of the Secure Microcontroller family is firmware/memory security. The devices were specifically designed to offer an unprecedented level of protection to the user application software, preventing unauthorized copying of firmware and denying access to critical data values. The use of RAM rather than the traditional ROM or EPROM for program storage increases the security, since tampering with the system will result in the loss of the RAM contents. Additional features such as real-time high-speed memory encryption, generation of dummy addresses on the bus, and internal storage of vector RAM increases the security of a Secure Microcontroller/Microprocessor-based system.

The DS5002FP Secure Microprocessor Chip and DS2252T Secure Microcontroller Module offer the highest level of security, with permanently enabled memory encryption, a 64-bit random encryption key, and a self-destruct input for tamper protection. The DS5000FP Soft Microprocessor Chip and DS5000(T) and DS2250(T) Soft Microcontroller Modules offer lesser, but still substantial, protection with optional data encryption and a 48-bit encryption key.

SEPARATE ADDRESS/DATA BUS

Soft Microprocessor chips provide a non-multiplexed address/data bus that interfaces to memory without interfering with I/O ports. This Byte-wide bus connects directly to standard CMOS SRAM in 8K x 8, 32K x 8, or 128K x 8 densities with no glue logic. Note that this is in addition to the standard 8051 port 0 and 2 multiplexed bus. In module form, the Byte-wide bus is already connected directly to on-board SRAM, so the memory access becomes transparent and the I/O ports free for application use. The extra memory bus also allows for a time-of-day function to be included, and all Soft Microcontroller modules are available with built in real-time clocks. The same clock devices are individually available when building a system from chips. Battery backup and decoding are automatically handled by the microprocessor.

LARGE NONVOLATILE MEMORY

Soft Microprocessor chips provide nonvolatile memory control for standard CMOS SRAM. Modules combine the microprocessor chip with memory and lithium backup. This includes conditionally write protected chip enables and a power supply output that switches between +5V and battery backup. The chip enables are decoded automatically based on user selectable memory sizes and partitioning. Partitioning defines the portion of memory used for program and data segments. Areas that are designated program are always write protected and are treated as ROM. Data areas are write protected only when power is out of tolerance. A large nonvolatile memory is useful for data logging and as flexible program storage. Memory will be retained for over 10 years at room temperature in the absence of power by ultra low-leakage lithium backed circuits.

IN-SYSTEM LOADING

The in-system programming capability lets the user update program code at any time. This program loading is supervised by a built-in ROM-based bootstrap loader. The ROM loader becomes transparent once program loading is complete. All devices allow program loading via the serial port. Data memory can also be retrieved using this loader function. Selected versions provide

other parallel loading protocols as well. In-system loading allows a system to be configured during final system test. A user can load custom software, diagnostic routines, or calibration constants. If something changes or new features arise, the system can then be reprogrammed while in the field.

HIGH RELIABILITY OPERATION

Secure Microcontroller devices are designed for unsupervised operation in remote locations. Special features prevent a system from running out of control during transient events. These include a reset when power is out of tolerance; an early warning power-fail interrupt that allows software to save critical data; and a watchdog to reset the micro if it gets lost. Also, nonvolatile memory allows software to save the operating state so a task can be resumed when power returns to normal.

The Secure Microcontroller family consists of three chips and their associated modules. Differences stem from I/O, memory access, and security features. The DS5000FP is used in DS2250T and DS5000(T) modules. The DS5001FP is used in the DS2251T, and the DS5002FP is used in the DS2252T. A full selector guide with all memory and speed permutations is provided in the next section.

CHIP	DESCRIPTION	BYTE-WIDE BUS MEMORY ACCESS	SECURITY	PACKAGE
DS5000FP	Soft Microprocessor Chip	8, 32, 64*K bytes	Optional	80-pin QFP
DS5001FP	128K Microprocessor Chip	32, 64, 128K bytes	None	80-pin QFP
DS5002FP	Secure Microprocessor Chip	32, 64, 128K bytes	Maximum	80-pin QFP

MODULE	DESCRIPTION	ON-BOARD MEMORY	PACKAGE
DS2250(T)	DS5000FP on SIMM	8, 32, 64*K bytes	40-pin SIMM
DS5000(T)	DS5000FP in DIP Module	8, 32K bytes	40-pin DIP
DS2251T	DS5001FP on SIMM	32, 64, 128K bytes	72-pin SIMM
DS2252T	DS5002FP on SIMM	32, 64, 128K bytes	40-pin SIMM

*32K partitionable, 32K restricted to data memory only.

NOTES:

"T" specifies optional on-board real-time clock.

128K byte versions provide fixed 64K program, 64K data segments. Other versions are partitionable.

PRODUCT DESCRIPTION

All devices listed below have the standard 8051 family feature set listed once here for convenience, but not repeated for each device.

- 8051-compatible instruction set
- Addresses 64K program and 64K data memory
- Four 8-bit pseudo-bidirectional I/O ports
- 128 bytes scratchpad RAM
- Two 16-bit timer/counters
- One UART
- Five Interrupts with two external

DS5000FP Soft Microprocessor Chip

The DS5000FP is the original Soft Microprocessor chip. It adds the following features to the 8051 set :

- Non-multiplexed Byte-wide address/data bus for memory access.
- Nonvolatile Control for 8K x 8 or 32K x 8 SRAMs
- Partitions one SRAM into program and data areas, and write protects the program segment
- Decodes memory for up to two 32K x 8 SRAMs (#2 is data memory only)
- Power-fail Reset, and Interrupt
- Precision Watchdog Timer
- ROM based Serial Bootstrap Loader
- Optional security features
 - Memory encryption in real-time
 - 48-bit user selected encryption key
 - Security lock destroys memory if unlocked
 - Vector RAM hides 48 bytes on-chip
 - Dummy operations on the memory bus

DS5000(T) Soft Microcontroller Module

The DS5000 incorporates the DS5000FP chip in a 40-pin module with an 8051 footprint and pinout.

- Familiar 40-pin DIP package

- Built-in NV RAM of 8K x 8 or 32K x 8
- I/O ports not disturbed by on-board memory access
- 10-year data retention and clock operation in the absence of power
- Partitions memory into program and data areas, write protects the program segment
- Power-fail Reset and Interrupt
- Precision Watchdog Timer
- ROM based Serial Bootstrap Loader
- Optional memory security
- Optional built-in real time clock (battery backed)

DS2250(T) Soft Microcontroller Module

The DS2250(T) incorporates the DS5000FP chip on a 40-pin SIMM module. It has the identical feature set as the DS5000(T), but is in a different form-factor. This package change allows up to 64K bytes NV RAM instead of 32K bytes. Note that as mentioned above, the second 32K is restricted to data memory. Like the DS5000(T), this module guarantees better than 10-year data retention at room temperature.

DS5001FP 128K Soft Microprocessor Chip

The DS5001FP provides the base feature set of the DS5000FP with the following extras:

- Accesses up to 128K bytes on the Byte-wide bus.
- Decodes memory for 32K x 8 or 128K x 8 SRAMs.
- Four additional decoded peripheral chip enables
- CRC hardware for checking memory validity
- Optionally emulates an 8042 style slave interface
- Bandgap reference for more accurate power monitor

Note: The DS5001FP has no memory encryption feature.

DS2251T 128K Soft Microcontroller Module

The DS2251T is a SIMM based on the DS5001. It provides up to 128K bytes of on-board NV RAM and has the Byte-wide bus available at the connector. This is used with the decoded peripheral enables for memory mapped peripherals such as a UART or A/D converter. The real-time clock is a parallel access type with interrupt capability. Like the older versions, the DS2251T provides 10-year data retention, even in the largest memory configuration.

DS5002FP Secure Microprocessor Chip

The DS5002FP is a highly secure version of the DS5001FP. It provides the operating features of the DS5001FP, with the following enhancements to the DS5000 security features.

- Security is active at all times
- Improved memory encryption using a 64-bit encryption key
- Automatic random generation of encryption keys
- Self-destruct input for tamper protection
- Optional top-coating prevents microprobe (DS5002FPM)

DS2252T Secure Microcontroller Module

The DS2252T incorporates the DS5002FP on a 40-pin SIMM. This includes from 32K bytes to 128K bytes of secure memory with a real time clock. The memory is highly secure from tampering and from competitors. Like other products in the family, the D2252T has a data retention period of over 10 years at room temperature.