PRODUCT PREVIEW

DALLAS SEMICONDUCTOR

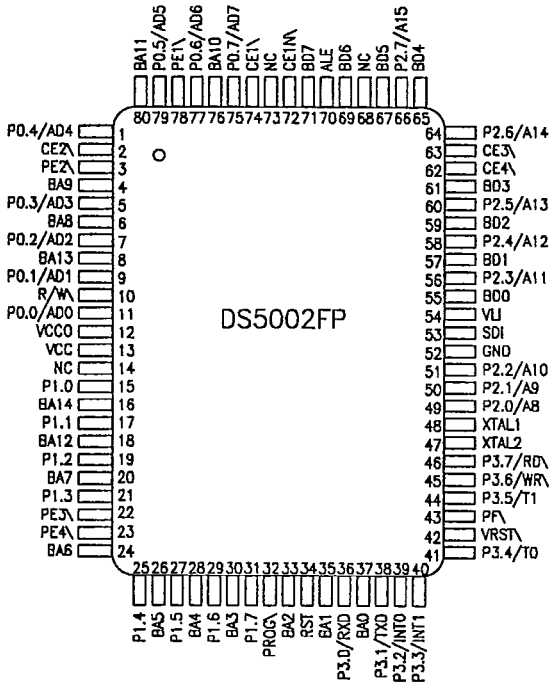
DS5002FP
Secure Micro Chip

T-49-19-08

FEATURES

- Enhanced security features:
  - Stronger address/data encryptor
  - 64-bit encryption key word
  - Automatic true random key generation
  - SDI (Self-Destruct Input)
  - Top coating defeats microprobe attack
- Customer-specific encryption versions available
- Incorporates enhanced memory and I/O features of DS5001FP 128K Micro Chip.
- 100% compatible with 8051 instruction set
- 80-pin Quad Flat Pack (QFP) surface-mount package

PACKAGE OUTLINE



DESCRIPTION

The DS5002FP Secure Micro Chip is a secure version of the DS5001FP 128K Micro Chip. In addition to the memory and I/O enhancements of the DS5001FP, the Secure Micro Chip incorporates the most sophisticated security features available in any microcontroller. The security features of the DS5002FP include an array of mechanisms which are designed to resist all levels of threat, including observation, analysis, and physical attack. As a result, a massive effort would be required to obtain any information about memory contents. Furthermore, the soft nature of the DS5002FP allows frequent modification of the secure information, thereby minimizing the value of any secure information obtained at any given time by such a massive effort.

The DS5002FP implements a security system that is an improved version of its predecessor, the DS5000 Soft Microcontroller. Like the DS5000, the DS5002FP loads and executes application software in encrypted form in up to 128K x 8 bytes of standard SRAM on its byte-wide bus. This RAM is converted by the DS5002FP into lithium-backed nonvolatile storage for programs and data. As a result, the contents of the RAM and the execution of the

software appear unintelligible to the outside observer. The encryption algorithm uses an internally stored and protected key. Any attempt to discover the key value results in its erasure, rendering the encrypted contents of the RAM useless.

The Secure Micro Chip offers a number of major enhancements to the software security implemented in the previous generation of the DS5000 Soft Microcontroller. First, the DS5002FP provides a stronger software encryption algorithm which incorporates elements of DES encryption. Second, the encryption is based on a 64-bit key word, as compared to the DS5000's 40-bit key. Third, the key can only be loaded from an on-chip true random number generator. As a result, the true key value is never known by the user. Fourth, a Self-Destruct Input pin (SDI) is provided to interface to external tamper detection circuitry. With or without the presence of V_{CC}, activation of the SDI pin has the same effect as resetting the security lock: immediate erasure of the key word and the 48-byte vector RAM area. Fifth, a special top-coating of the die prevents access of information using microprobing techniques. Finally, customer-specific versions of the DS5002FP are available that incorporate a one-of-a-kind encryption algorithm.

When implemented as a part of a secure system design, the DS5002FP can typically provide a level of security which requires more time and resources to defeat than it is worth to unauthorized individuals who have reason to try.

FOR FURTHER INFORMATION

A complete data sheet for the DS5002FP is available on request to customers who have a signed non-disclosure agreement on file with Dallas Semiconductor.

ORDERING INFORMATION

The following versions of the DS5002FP are available as standard products from Dallas Semiconductor.

PART #	CLOCK	PACKAGE
DS5002FP -08	8 MHz	80-pin QFP
DS5002FP -12	12 MHz	80-pin QFP
DS5002FP -16	16 MHz	80-pin QFP

Please contact Dallas Semiconductor for ordering information on customer-specific versions of the DS5002FP.