



# Secure Microcontroller AT90S04 Summary

## Features

### General

- High-performance, Low-power 8-/16-bit Enhanced RISC Architecture Microcontroller
- Low Power Idle and Power-Down Modes
- Internal Variable Frequency Oscillator up to 30 Mhz
- Bond Pad Locations Conforming to ISO 7816-2
- ESD Protection up to  $\pm 4000V$
- Operating Range: 2.7V to 5.5V
- Operating Temperature:  $-25^{\circ}C$  to  $+85^{\circ}C$
- Available in Wafers, Modules and standard ROHS packages:
  - 8-DFN (RoHS compliant) 5mm x 6mm
  - 8-SOIC (RoHS compliant) 5mm x 5mm

### Memory

- 96K Bytes of ROM Program Memory
- 4K Bytes of EEPROM, including 128 OTP Bytes and 384 Bit-addressable Bytes
  - 1 to 64-byte Program / Erase
  - 2 ms Program / 2 ms Erase
  - Typically 500,000 Write / Erase Cycles at a Temperature of  $25^{\circ}C$
  - 10 Years Data Retention
- 2K Bytes of RAM Memory

### Peripherals

- One ISO 7816 Controller
  - Up to 625 kbps at 5 MHz
  - Compliant with T = 0 and T = 1 Protocols

- High Speed Master / Slave SPI Serial Interface up to 20 Mbits/s
- Hardware Communication Interface Detection
- Four I/O Ports (two reserved for ISO 7816)
- Programmable Internal Oscillator (Up to 30 MHz)
- Two 16-bit Timers
- Random Number Generator (RNG)
- 2-level Interrupt Controller
- Hardware DES/TDES Engine DPA/DEMA Resistant
- Checksum Accelerator
- Code Signature Module
- CRC 16 & 32 Engine (Compliant with ISO / IEC 3309)

### Security

- Dedicated Hardware for Protection Against SPA/DPA/SEMA/DEMA Attacks
- Advanced Protection Against Physical Attack, including Active Shield, Enhanced Protection Object, CStack Checker, Slope Detector, Parity Errors
- Environmental Protection Systems (Voltage, Frequency, Temperature Monitors)
- Secure Memory Management/Access Protection (Supervisor Mode)

### Development Tools

- Voyager Emulation Platform (ATV4+) to Support Software Development
- IAR Embedded Workbench<sup>®</sup> V5.40 Debugger or Above
- Software Libraries and Application Notes

# Description

Targeted for low cost security applications, the AT90SO4 is a low-power, high-performance, 8-/16-bit microcontroller with ROM program memory, EEPROM memory, based on RISC architecture microcontroller.

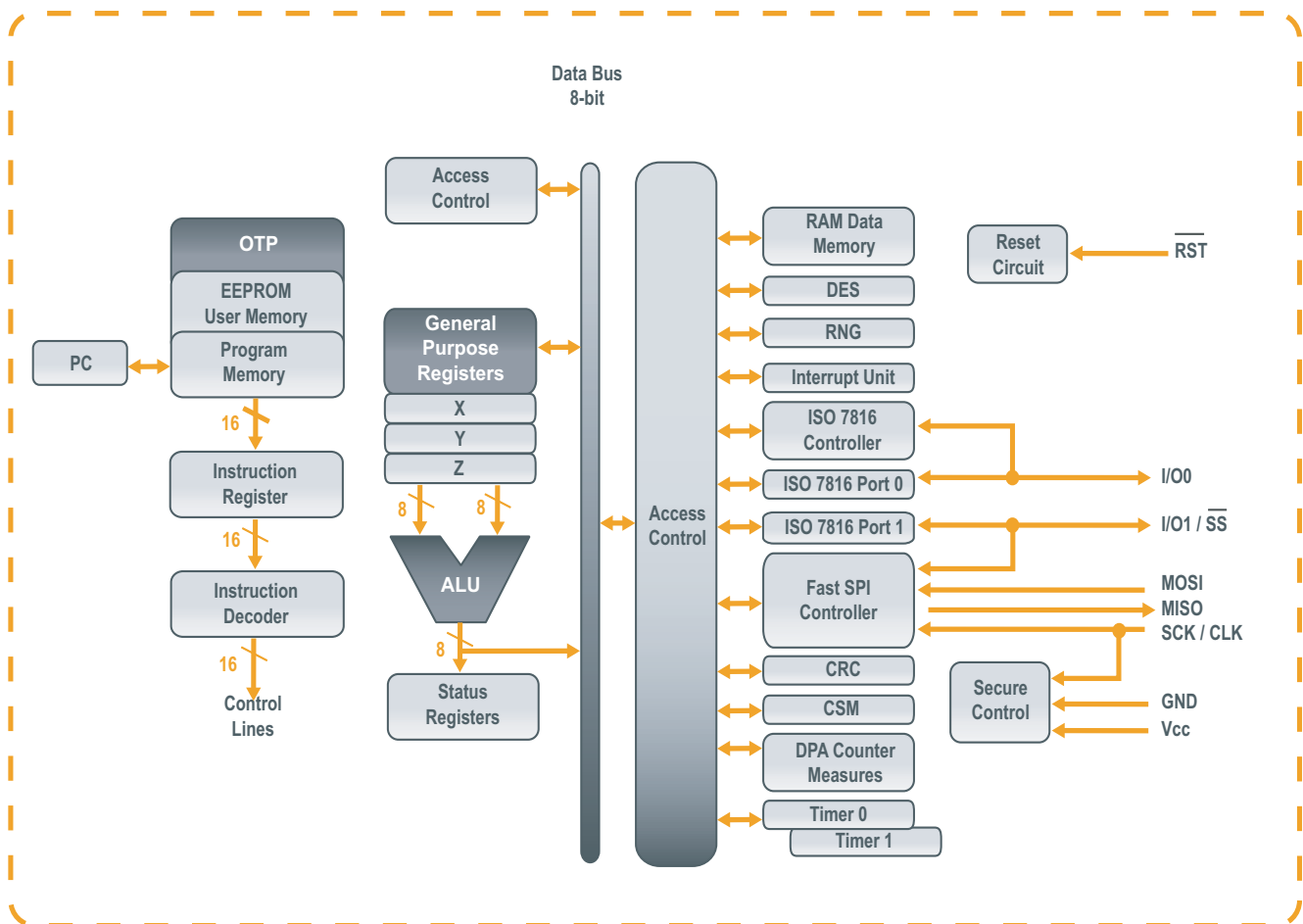
By executing powerful instructions in a single clock cycle, the AT90SO4 achieves throughputs close to 1 MIPS per MHz. Its Harvard architecture includes 32 general-purpose working registers directly connected to the ALU, allowing two independent registers to be accessed in one single instruction executed in one clock cycle.

In addition to the 96K Bytes of embedded ROM, the AT90SO4 includes 4K Bytes of high density EEPROM.

The ability to map the EEPROM in the code space allows parts of the program memory to be reprogrammed in-system. This technology combined with the versatile 8/16-bit CPU on a monolithic chip provides a highly flexible and cost-effective solution to many applications.

The High Speed SPI, when configured as a master, provides a clock up to 20MHz thanks to the dedicated internal VFO clock system. A specific DMA controller allows fast transfers between DPRAM banks to CPU RAM. The internal DPRAM memory provides 4 DPRAM buffers of 16 bytes each. The SPI controller features three sources of interrupt (Byte Transmitted, Time-out and Reception Overflow) and a programmable clock and inter-bytes (guardtime) delays.

Figure 1 AT90SO4 RISC CPU Core Architecture

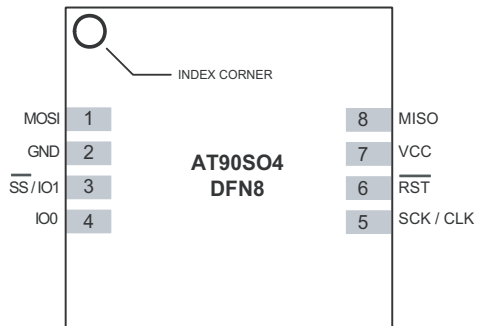


## Ordering information

| Reference            | Description   |
|----------------------|---|
| <b>AT90SO4-xxx-P</b> | <b>xxx</b> : Chip Personalization Number*<br><b>P</b> = 8Z : DFN8 Package<br><b>R</b> : SOIC8 Package |

\* For more details about the Chip Personalization Number, please contact your local INSIDE Secure sales office.

**Figure 2** AT90SO4 pinout - DFN8 package



**Figure 3** AT90SO4 pinout - SOIC8 package

