Features

General

- High-performance, Low-power secureAVR™ Enhanced RISC Architecture
- Low Power Idle and Power-Down Modes
- Bond Pad Locations Conforming to ISO 7816-2
- ESD Protection up to ± 4000V
- Operating Range: 2.7V to 5.5V
- Operating Temperature: -25°C to +85°C
- Internal Variable Frequency Oscillator up to 30 Mhz
- Available in Wafers, Modules and standard ROHS packages: SOIC8 or DFN8

Memory

- 96K bytes of ROM Program Memory
- 4K bytes of EEPROM including 128 OTP bytes and 384 bytes of Bit-addressable Area
  - 1 to 64-byte Program/Erase
  - 2 ms Program / 2 ms Erase
  - Typically More than 500,000 Write/Erase Cycles at a Temperature of 25°C
  - 10 Years Data Retention
- 2K bytes of RAM Memory

Peripherals

- 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
  - Supports clock up to 20MHz in Slave and Master Mode in typical conditions
  - Double Buffering for high performance (16x2 bytes DPRAM buffers)
  - DMA Controller for fast transfers between internal DPRAM to RAM
- Hardware Communication Interface Detection
- Two I/O Ports (supporting ISO 7816)
- Programmable Internal Oscillator (Up to 30 MHz for CPU)
- Two 16-bit Timers
- Random Number Generator (RNG)
- 2-level Interrupt Controller
- Hardware DES and Triple DES 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
- Environmental Protection Systems (Voltage, Frequency, Temperature, Light monitors...)
- Secure Memory Management/Access Protection (Supervisor Mode)

Development Tools

- Voyager Emulation Platform (ATV4 Plus) to Support Software Development
- IAR Systems EWAVR® V5.11B Debugger or Above
- Software Libraries and Application Notes

Secure Microcontroller for Security Modules

AT90SO4

Summary

6579A–SMS–29Jan10

Note: This is a summary document. A complete document will be available under NDA. For more information, please contact your local Atmel sales office.

Part Number

AT90SO4-xxx-P

AT: Atmel
90 : AVR Core
SO : Smart Object
4 : EEPROM Size
xxx : Chip Personalization Number*
P = Z : DFN8 Package
R : SOIC8 Package

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

Description

Targeted for low cost security applications, the AT90SO4 is based on the secureAVR architecture that allows the linear addressing of up to 8M bytes of code and up to 16M bytes of data as well as a number of new functional and security features. It is a low-power, high-performance, 8/16-bit microcontroller with ROM program memory, EEPROM data memory based on the secureAVR enhanced RISC architecture. 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.

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 embedded security applications.

Additional security features include power and frequency protection logic, logical scrambling on program data and addresses, Power Analysis countermeasures and memory accesses controlled by a supervisor mode. A block diagram of the AT90SO4 is shown in Figure 1 hereafter.

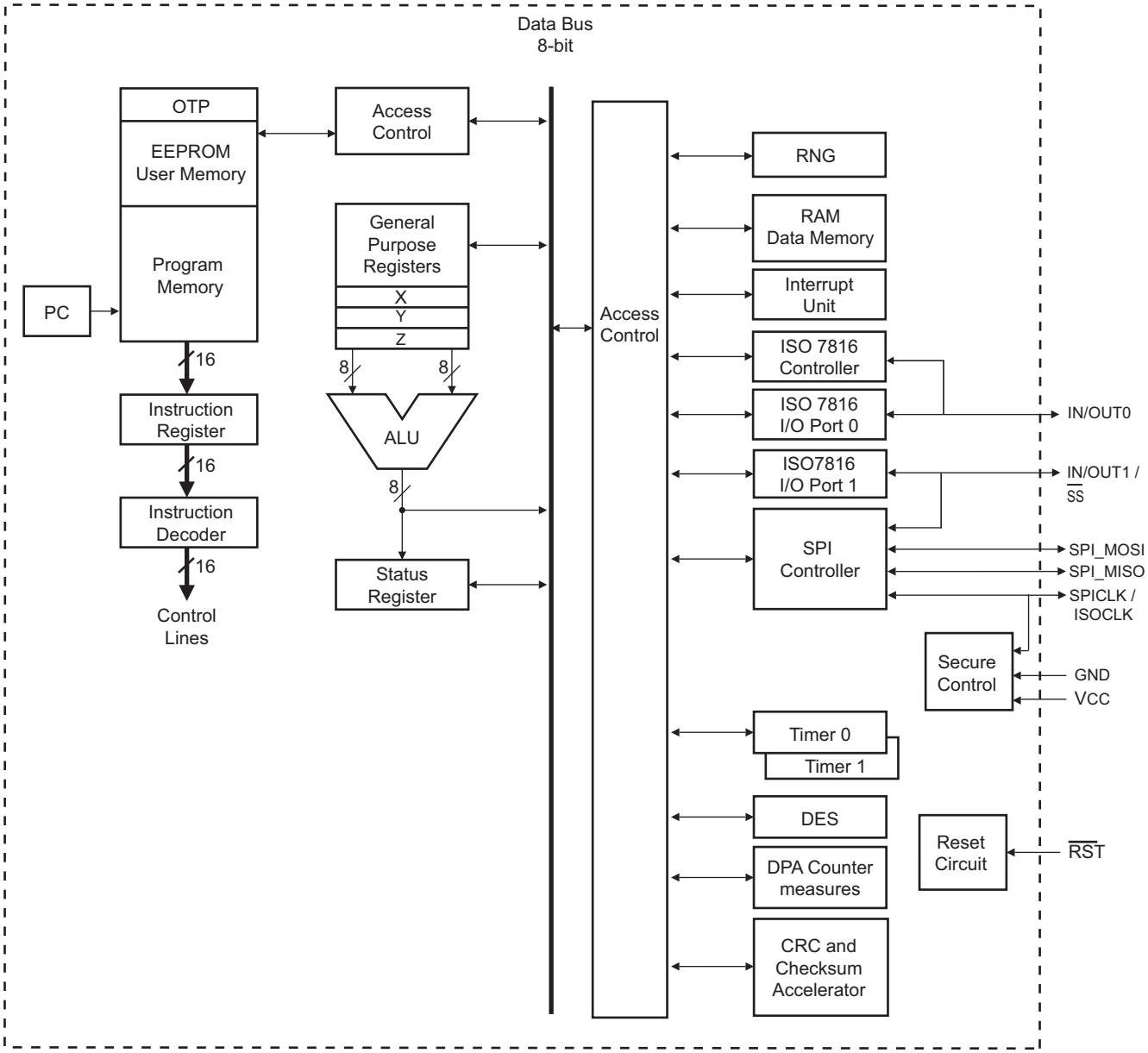
High-Speed SPI Controller

The AT90SO4 hosts a High Speed SPI interface for full-duplex and synchronous data transfer. When configured as a master, the controller provides clock up to 20MHz thanks to the dedicated internal VFO clock system.

A specific DMA contoller allows fast tranfers between DPRAM banks to CPU RAM. The internal DPRAM memory provides 4 DPRAM buffers of 16 bytes each: 2 for Reception and 2 for Transmission.

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 secureAVR Enhanced RISC Architecture



Pinout and Package Information

Figure 2. Pinout AT90SO4 - Package DFN8

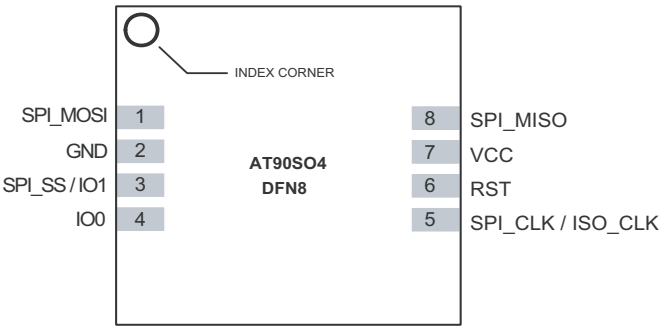


Figure 3. Pinout AT90SO4 - Package SOIC8

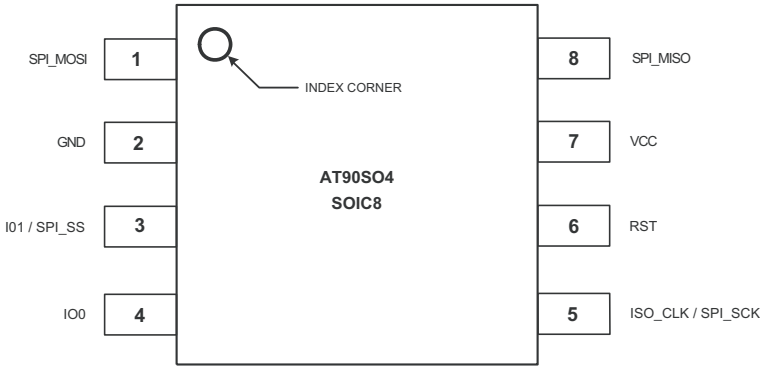
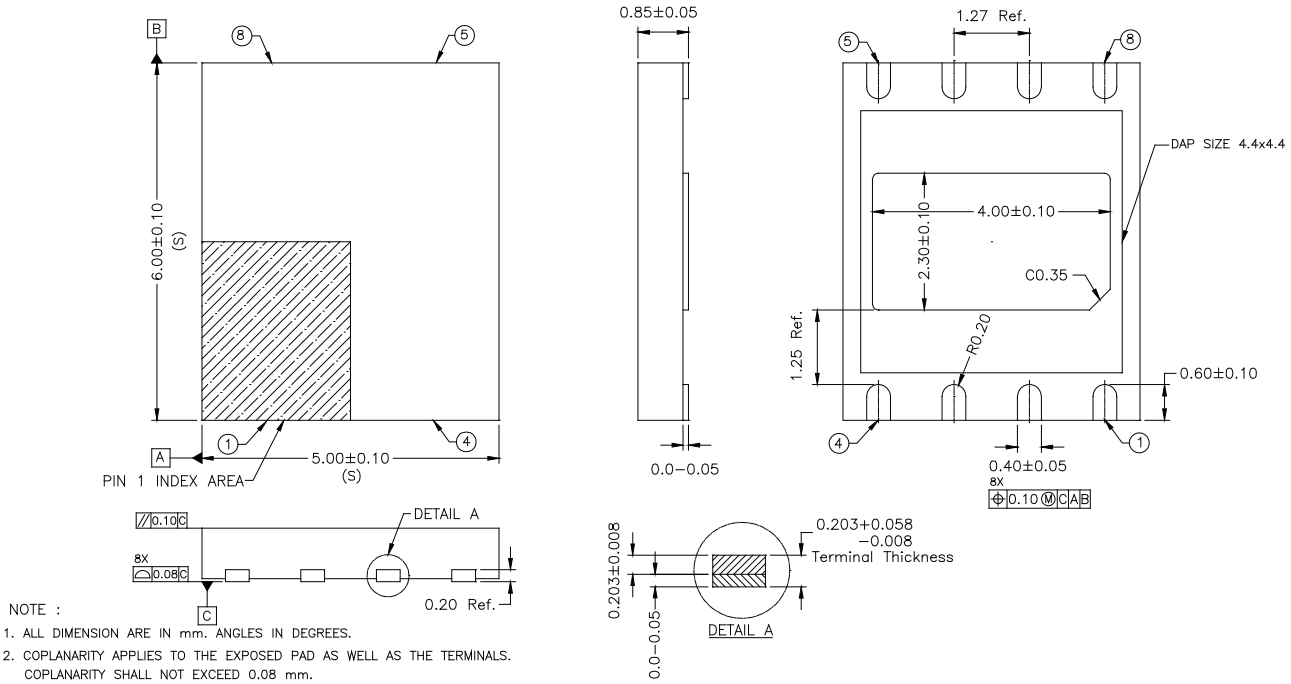


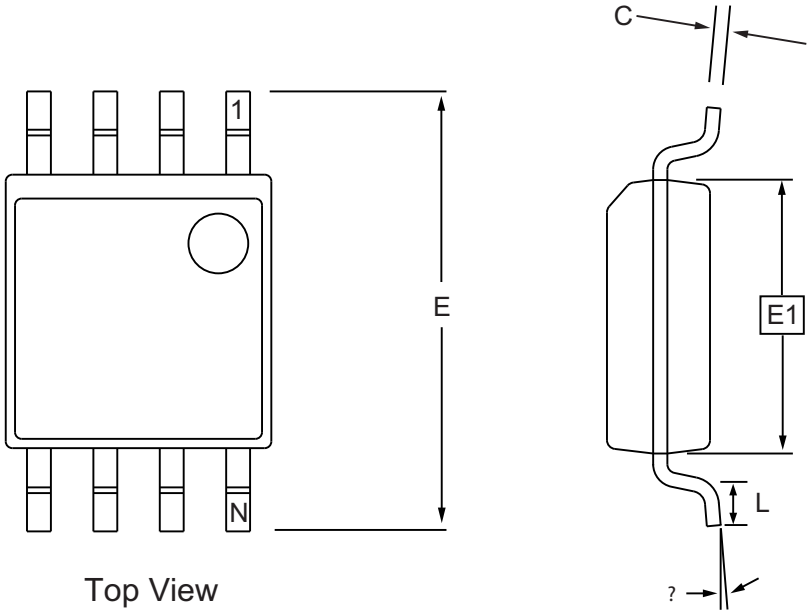
Figure 4. Dual Fleat No Lead Package, 8 leads

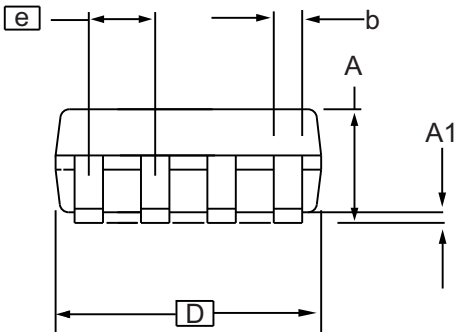


NOTE :

1. ALL DIMENSION ARE IN mm. ANGLES IN DEGREES.
2. COPLANARITY APPLIES TO THE EXPOSED PAD AS WELL AS THE TERMINALS. COPLANARITY SHALL NOT EXCEED 0.08 mm.
3. WARPAGE SHALL NOT EXCEED 0.10 mm.
4. PACKAGE LENGTH / PACKAGE WIDTH ARE CONSIDERED AS SPECIAL CHARACTERISTIC.(S)
5. REFER JEDEC MO−229.
6. FRAME STOCK# FL0106 (Ag Ring Plate), UTL PKG CODE ND56G008A OR ND−500X600G008A OR ND−500T600G008A OR ND−500L600G008A OR ND−500U600G008A
7. L/F STOCK# FR0221 (Ag Ring), UTL PKG CODE ND−500E600G008A OR ND−500S600G008A OR ND−500M600G008A OR ND−500D600G008A

Figure 5. Plastic Small Outline Package - 8-lead - 0.209” Body





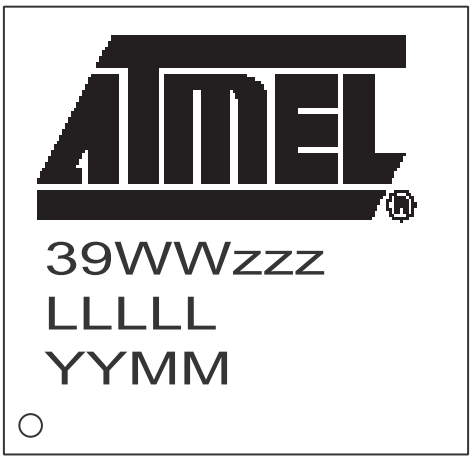
COMMON DIMENSIONS
(Unit of Measure = mm)

SYMBOL	MIN	NOM	MAX	NOTE
A	1.70		2.16	
A1	0.05		0.25	
b	0.35		0.48	5
C	0.15		0.35	5
D	5.13		5.35	
E1	5.18		5.40	2, 3
E	7.70		8.26	
L	0.51		0.85	
?	0˚		8˚	
e	1.27 BSC			4

Notes: 1. This drawing is for general information only; refer to EIAJ Drawing EDR-7320 for additional information.
2. Mismatch of the upper and lower dies and resin burrs are not included.
3. It is recommended that upper and lower cavities be equal. If they are different, the larger dimension shall be regarded.
4. Determines the true geometric position.
5. Values b and C apply to pb/Sn solder plated terminal.
The standard thickness of the solder layer shall be 0.010 +0.010/-0.005 mm.

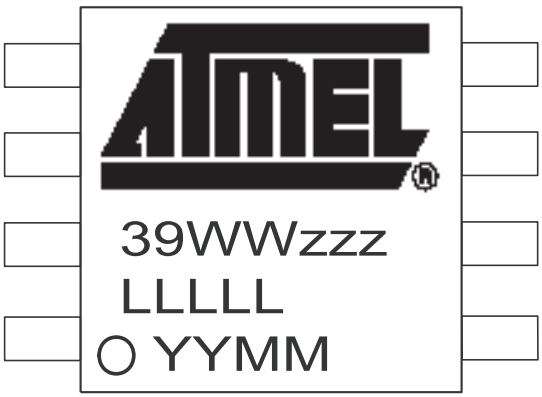
Product Marking

Figure 1. Package DFN8



39: Chip Identification Number
WW: ROM Code
zzz: Chip Personalization Number
LLLLL : Lot Number
YYMM : Date Code

Figure 1. Package SOIC8



39: Chip Identification Number
WW: ROM Code
zzz: Chip Personalization Number
LLLLL : Lot Number
YYMM : Date Code

Product Characteristics

Maximum Ratings

Table 1. Absolute Maximum Ratings

Symbol	Parameter	Min.	Max.	Unit
V_{CC}	Supply Voltage	-0.3	7.5	V
V_{IN}	Input Voltage	V_{SS}-0.3	V_{CC}+0.3	V
T_A	Operating Temperature	-25	+85	°C
E_{EEPROM}	EEPROM Endurance for write/erase cycles		500 000 (1)	cycles
$V_{DataRetention}$	EEPROM Data Retention Virgin		10	Years
ESD	Electrostatic Discharge (HBM)		4	kV
L_{up}	Latch-up		+/- 200	mA

1. Depends on conditions. Please refer to “EEPROM Reliability & Qualification Specification” (PE/SPEC/032).

AC/DC Characteristics (2.7V - 5.50V range; T= -25°C to +85°C)

Table 2. DC Characteristics (2.7V - 5.50V range; T= -25°C to +85°C)

Symbol	Parameter	Condition	Min.	Typ.	Max.	Units
V_{CC}	Supply Voltage		2.7		5.50	V
V_{CC}	Supply Voltage Supply Voltage	5.0V (+/- 10%) 3.0V (+/- 10%)	4.5 2.7	5.0 3.0	5.5 3.3	V
V_{IH}	Input High Voltage - I/O 0..1 Input High Voltage - ISOCLK Input High Voltage - RST Input High Voltage - MISO, MOSI	5V, 3V	0.7*V_{CC} 0.7*V_{CC} 0.7*V_{CC} 0.7*Vcc		V_{CC}+0.3 V_{CC}+0.3 V_{CC}+0.3 V_{CC}+0.3	V
V_{IL}	Input Low Voltage - I/O 0..1 Input Low Voltage - ISOCLK Input Low Voltage - RST Input Low Voltage - MISO, MOSI	5V, 3V	-0.3 -0.3 -0.3 -0.3		0.2*V_{CC} 0.2*V_{CC} 0.2*V_{CC} 0.2*V_{CC}	V
I_{IH}	Leakage High Current- I/O 0..1 Leakage High Current - ISOCLK Leakage High Current - RST Leakage High Current - MISO, MOSI	5V, 3V, V_{IN} = V_{IH}	-10 -10 -10 -10		10 10 10 10	µA
I_{IL}	Leakage Low Current - I/O 0..1 Leakage Low Current - ISOCLK Leakage Low Current - RST Leakage Low Current - MISO, MOSI	5V, 3V, V_{IN} = V_{IL}	-40 -10 -40 -40		10 10 10 10	µA

Table 2. DC Characteristics (2.7V - 5.50V range; T= -25°C to +85°C)

Symbol	Parameter	Condition	Min.	Typ.	Max.	Units
V_{OL}	Output Low Voltage - I/O 0..1 Output Low Voltage - MISO, MOSI	5V, I_{OL} = 1mA 3V, I_{OL} = 1mA	0 0		0.08*V_{CC} 0.15*V_{CC}	V
V_{OH}	Output High Voltage - I/O 0..1 Output High Voltage - MISO, MOSI	5V, 3V, I_{OH} = 1mA	0.7*Vcc 0.7*Vcc		Vcc Vcc	V
$R_{I/O}$	Pin Pull-up I/O0, RST, I/O1, MISO, MOSI			220		KOhm

Table 3. AC Characteristics (2.7V - 5.50V range; T= -25°C to +85°C)

Symbol	Parameter	Condition	Min.	Typ.	Max.	Units
f_{CLK}	External Clock Frequency		1		5	MHz
f_{VFO}	Variable Frequency Oscillator (1)	Expected value at 25°C Clock Jitter **not enabled** 5V, 3V	28	31	34	MHz
f_{VFO} Average	Average Variable Frequency Oscillator(2)	Expected value at 25°C Clock Jitter **enabled** 5V, 3V		28		MHz
t_{EEPROM}	EEPROM Write Time (erase+write)		1.6	2	2.4	ms
T_r	I/O Output Rise Time (HRD Mode)	C_{out}=30pF R_{pullup}=20kOhm			100	ns
T_f	I/O Output Fall Time	C_{out}=30pF R_{pullup}=20kOhm			100	ns

1. Please refer to Application Note “How to estimate a performance of a running code “ TPR0231X for the dependence on temperature, clock jitter and clock dividers.

Table 4. Security Characteristics (2.7V - 5.50V range; T= -25°C to +85°C)

Symbol	Parameter	Condition	Min.	Typ.	Max.	Units
V_{MAX}	Voltage Monitor: High Level Detection		5.5			V
V_{MIN}	Voltage Monitor: Low Level Detection	Chip trimmed to operate at 5V, 3V			2.7	V
f_{MAX}	External Frequency Monitor: High Level Detection	Duty cycle = 40% to 60% Running on External Clock	5			MHz
f_{MIN}	External Frequency Monitor: Low Level Detection	Duty cycle = 40% to 60% Running on External Clock			1	MHz
T_{MON} Max	Temperature Monitor: High Level Detection		85			°C
T_{MON} Min	Temperature Monitor: Low Level Detection				-25	°C

Table 5. Icc Characteristics (2.7V - 5.50V range; T= -25°C to +85°C)

Symbol	Parameter	Condition	Min.	Typ.	Max.	Units
$I_{cc\ Run\ Mode}$	Supply Current in Run Mode f_{CLK}=5MHz	5V, 3V From ROM			6	mA
$I_{cc\ Run\ Mode}$	Supply Current in Run Mode f_{VFO}=30MHz	5V, 3V From ROM			10	mA
$I_{cc\ DES}$	Supply Current add-on when DES is running f_{CLK}=5MHz	5V, 3V			4	mA
$I_{cc\ DES}$	Supply Current add-on when DES is running f_{VFO}=30MHz	5V, 3V			10	mA
$I_{cc\ IDLE}$	Supply Current in IDLE Mode Clock :5MHz	5V, 3V			2	mA
$I_{cc\ POWER\text{-}DOWN}$	Supply Current in POWER-DOWN Mode Clock : 1MHz	5V, 3V			200	µA
$I_{cc\ POWER\text{-}DOWN}$	Supply Current in POWER-DOWN Mode No Clock Running	5V, 3V			200	µA

Table 6. High Speed SPI characteristics in Master Mode (2.7V - 5.50V range; T= -25°C to +85°C)

Symbol	Parameter	Condition	Min.	Typ.	Max.	Units
$t_{MISOsetup}$	MISO Setup time before SCK rises	C_{OUT}=10pF C_{OUT}=20pF	10			ns
$t_{MISOhold}$	MISO Hold time after SCK rises	C_{OUT}=10pF C_{OUT}=20pF	10			ns
$t_{SCKrising}$	SCK rising to MOSI Delay	C_{OUT}=10pF C_{OUT}=20pF			10	ns
$t'_{MISOsetup}$	MISO Setup time before SCK falls	C_{OUT}=10pF C_{OUT}=20pF	10			ns
$t'_{MISOhold}$	MISO Hold time after SCK falls	C_{OUT}=10pF C_{OUT}=20pF	10			ns
$t_{SCKfalling}$	SCK falling to MOSI Delay	C_{OUT}=10pF C_{OUT}=20pF			10	ns
SCK	Host frequency	C_{OUT}=10pF C_{OUT}=20pF			20	MHz

Table 7. High Speed SPI characteristics in Slave Mode (2.7V - 5.50V range; T= -25°C to +85°C)

Symbol	Parameter	Condition	Min.	Typ.	Max.	Units
$t_{SCKfalling}$	SCK falling to MISO Delay	C_{OUT}=10pF C_{OUT}=20pF			13	ns
$t_{SCKrising}$	SCK rising to MISO Delay	C_{OUT}=10pF C_{OUT}=20pF			13	ns
$t_{MOSIsetup}$	MOSI Setup time before SCK rises	C_{OUT}=10pF C_{OUT}=20pF	10			ns
$t_{MOSIhold}$	MOSI Hold time after SCK rises	C_{OUT}=10pF C_{OUT}=20pF	10			ns
$t'_{MOSIsetup}$	MOSI Setup time before SCK falls	C_{OUT}=10pF C_{OUT}=20pF	10			ns
$t'_{MOSIhold}$	MOSI Hold time after SCK falls	C_{OUT}=10pF C_{OUT}=20pF	10			ns
$t_{SSsetup}$	SS Setup time	C_{OUT}=10pF C_{OUT}=20pF	10			ns
$t_{dat->dat}$	Interbyte delay	C_{OUT}=10pF C_{OUT}=20pF	10			ns
SCK	Slave frequency	C_{OUT}=10pF C_{OUT}=20pF			20	MHz

Atmel Corporation

2325 Orchard Parkway
San Jose, CA 95131, USA
Tel: 1(408) 441-0311
Fax: 1(408) 487-2600

Regional Headquarters

Europe
Atmel Sarl
Route des Arsenaux 41
Case Postale 80
CH-1705 Fribourg
Switzerland
Tel: (41) 26-426-5555
Fax: (41) 26-426-5500

Asia
Room 1219
Chinachem Golden Plaza
77 Mody Road Tsimshatsui
East Kowloon
Hong Kong
Tel: (852) 2721-9778
Fax: (852) 2722-1369

Japan
9F, Tonetsu Shinkawa Bldg.
1-24-8 Shinkawa
Chuo-ku, Tokyo 104-0033
Japan
Tel: (81) 3-3523-3551
Fax: (81) 3-3523-7581

Atmel Operations

Memory
2325 Orchard Parkway
San Jose, CA 95131, USA
Tel: 1(408) 441-0311
Fax: 1(408) 436-4314

Microcontrollers
2325 Orchard Parkway
San Jose, CA 95131, USA
Tel: 1(408) 441-0311
Fax: 1(408) 436-4314

La Chantrerie
BP 70602
44306 Nantes Cedex 3, France
Tel: (33) 2-40-18-18-18
Fax: (33) 2-40-18-19-60

ASIC/ASSP/Secure Microcontroller Solutions
Zone Industrielle
13106 Rousset Cedex, France
Tel: (33) 4-42-53-60-00
Fax: (33) 4-42-53-60-01

1150 East Cheyenne Mtn. Blvd.
Colorado Springs, CO 80906, USA
Tel: 1(719) 576-3300
Fax: 1(719) 540-1759

Scottish Enterprise Technology Park
Maxwell Building
East Kilbride G75 0QR, Scotland
Tel: (44) 1355-803-000
Fax: (44) 1355-242-743

RF/Automotive
Theresienstrasse 2
Postfach 3535
74025 Heilbronn, Germany
Tel: (49) 71-31-67-0
Fax: (49) 71-31-67-2340

1150 East Cheyenne Mtn. Blvd.
Colorado Springs, CO 80906, USA
Tel: 1(719) 576-3300
Fax: 1(719) 540-1759

Biometrics/Imaging/Hi-Rel MPU/
High Speed Converters/RF Datacom
Avenue de Rochepleine
BP 123
38521 Saint-Egreve Cedex, France
Tel: (33) 4-76-58-30-00
Fax: (33) 4-76-58-34-80

Literature Requests
www.atmel.com/literature