Features

General

- High-performance, Low-power secureAVR® Enhanced RISC Architecture
  - 135 Powerful Instructions (Most Executed in a Single Clock Cycle)
- 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 QFN44

Memory

- 288K bytes of ROM Program Memory including 32K bytes of ROM with specific access
- 128K bytes of EEPROM including 128 OTP bytes and 384 bytes of Bit-addressable Area
  - 1 to 128-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
- 12K bytes of RAM Memory (10K bytes of secureAVR RAM, 2K bytes of AdvX™ RAM, shared with the secureAVR core)

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
- USB 2.0 Full Speed Interface
  - Universal Serial Bus Specification Rev 2.0 compliant
  - Supports data transfer rates up to 12 Mbit/s
  - 8 Programmable Endpoints with IN or OUT Directions for Bulk, Interrupt or Isochronous Transfers (4 endpoints with double buffering of 64x2 bytes)
  - Endpoint 0 for Control Transfers : up to 64-bytes
  - DMA Controller for fast transfers between internal DPRAM to RAM
  - 48 MHz clock for Full-speed Bus Operation
  - USB Bus Disconnection on firmware request
- Hardware Communication Interface Detection
- Ten I/O Ports
  - I/O 0 and I/O 1 reserved for ISO 7816, SPI and I²C communication
  - 8 General Purpose I/Os
- Programmable Internal Oscillator (Up to 30 MHz for CPU and Crypto Accelerator)
- Low Power Real Time Clock (RTC)
- Two 16-bit Timers
- Random Number Generator (RNG)
- 2-level Interrupt Controller
- Hardware DES and Triple DES Engine DPA/DEMA Resistant
- Hardware AES 128/192/256 Engine DPA/DEMA Resistant
- Checksum Accelerator
- CRC 16 & 32 Engine (Compliant with ISO/IEC 3309)
- 32-bit AdvX™ Cryptographic Accelerator for Public Key Operations with full featured cryptography library (RSA, ECC, Key Generation)

Secure Microcontroller for Security Modules

AT90S0128

Preliminary Summary

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

Security

- **Dedicated Hardware for Protection Against SPA/DPA/SEMA/DEMA Attacks**
- **Advanced Protection Against Physical Attack, Including Active Shield**
- **Environmental Protection Systems**
- **Voltage Monitor**
- **Frequency Monitor**
- **Light Protection**
- **Temperature Monitor**
- **Secure Memory Management/Access Protection (Supervisor Mode)**

Development Tools

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

Certification targets

- **CC EAL4+**
- **USB 2.0**

Part Number

AT90SO128-xxx-P

AT: Atmel
90 : AVR Core
SO : Smart Object
128 : EEPROM Size
xxx : Chip Personalization Number*
P = Z : QFN44 Package
R : SOIC8 Package

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

Description

The AT90SO128 is a low-power, high-performance, 8/16-bit microcontroller with ROM program memory, EEPROM data memory, cryptographic accelerator based on the secureAVR enhanced RISC architecture. By executing powerful instructions in a single clock cycle, the AT90SO128 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 AT90SO128 uses a new AVR® architecture, the secureAVR 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.

The cryptographic accelerator featured in this product is the AdvX, a 32-bit accelerator dedicated to performing fast encryption and authentication functions. It is combined with a 32K byte-ROM for a high-performance and secure crypto firmware.

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 smart card 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 AT90SO128 is shown in Figure 1 hereafter.

USB Controller

The AT90SO128 features a USB V2.0 Full Speed controller which requires a 48 MHz external crystal for the data transfer. The USB interface consists of a Serial Interface Engine (SIE) and a Universal Function Interface (UFI). The SIE performs clock/data separation, NRZI encoding and decoding, bit stuffing, CRC generation and checking and serial-parallel data conversion.

The UFI connects the USB interface to the AVR. It consists of a protocol engine and provides eight configurable data transfer endpoints, each with its own DPRAM in the memory area. The data transfer type for each endpoint is configured by software.

A DMA controller allows a fast communication rate between the RAM of the CPU and the DPRAM.

The USB controller provides a dynamic pull-up attachment and detachment and a host detection mechanism.

Real Time Clock

The AT90SO128 offers a Real-time Clock peripheral designed for very low power consumption. The RTC is a standalone block powered by an external Lithium battery. The reference clock is an external 32.768 kHz crystal.

The RTC provides a full binary-coded decimal (BCD) clock that includes century (19/20), year (with leap years), month, date, day, hours, minutes and seconds. The valid year range is 1900 to 2099, a two-hundred-year Gregorian calendar achieving full Y2K compliance. The RTC can operate in 24-hour mode or in 12-hour mode with an AM/PM indicator. Updating time and calendar fields is performed by a parallel capture on the data bus. An entry control is performed to avoid loading registers with incompatible BCD format data or with an incompatible date according to the current month/year/century.

High-Speed SPI Controller

The AT90SO128 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.

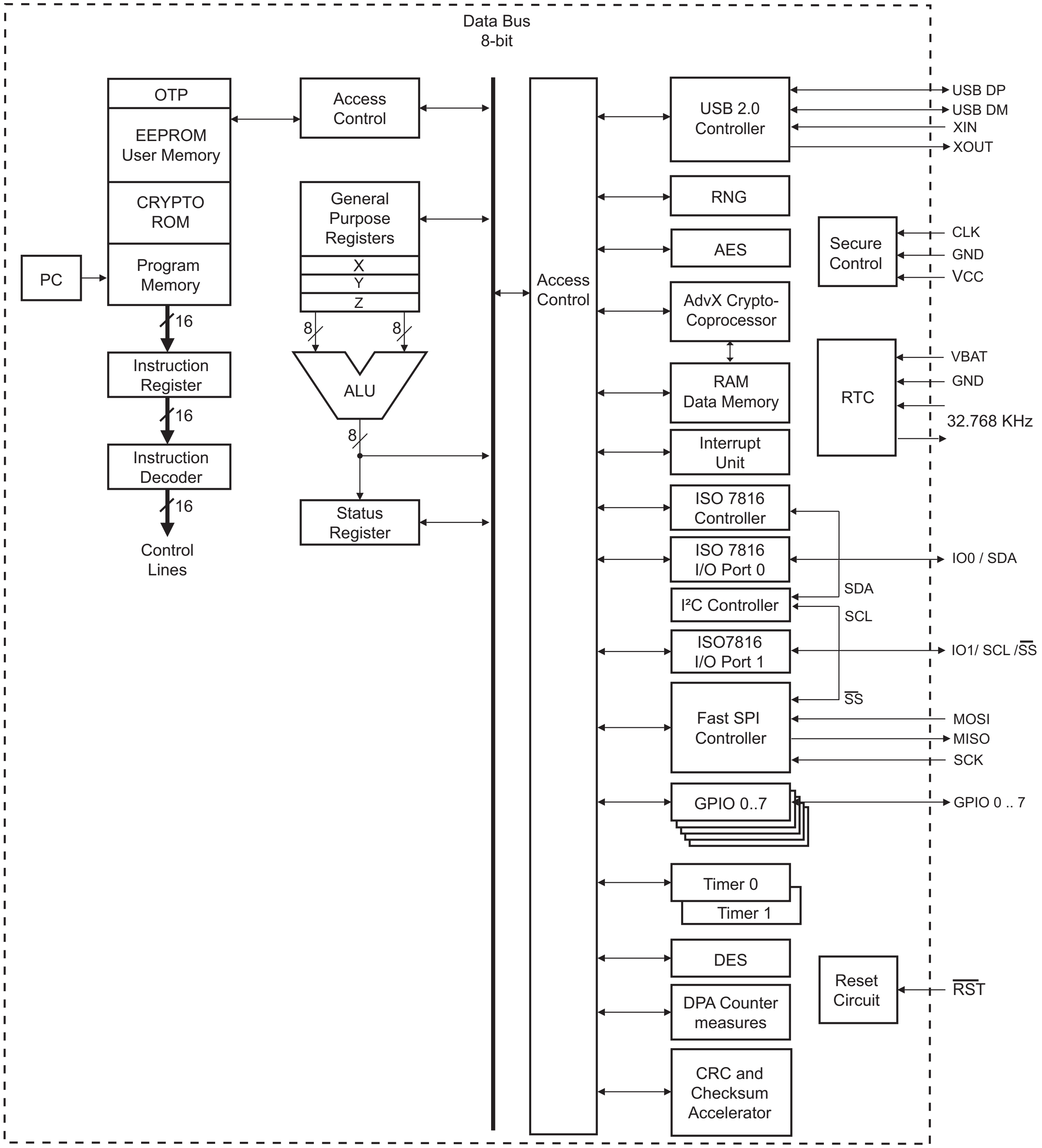
The SPI controller features three sources of interrupt (Byte Transmitted, Time-out and Reception Overflow) and a programmable clock and inter-bytes (guardtime) delays.

I²C Controller

The I²C interface interconnects components on a unique two-wire bus, made up of one clock line and one data line with speeds of up to 400 Kbits per second, based on a byte-oriented transfer format. It can be used with any Atmel two-wire bus product. The I²C is programmable as a master or a slave with sequential or single-byte access. Multiple master capability is supported. Arbitration of the bus is performed internally and puts the I²C in slave mode automatically if the bus arbitration is lsot.

A configurable baud rate generator permits the output data rate to be adapted to a wide range of core clock frequencies.

Figure 1. AT90SO128 secureAVR Enhanced RISC Architecture



Pinout and Package Information

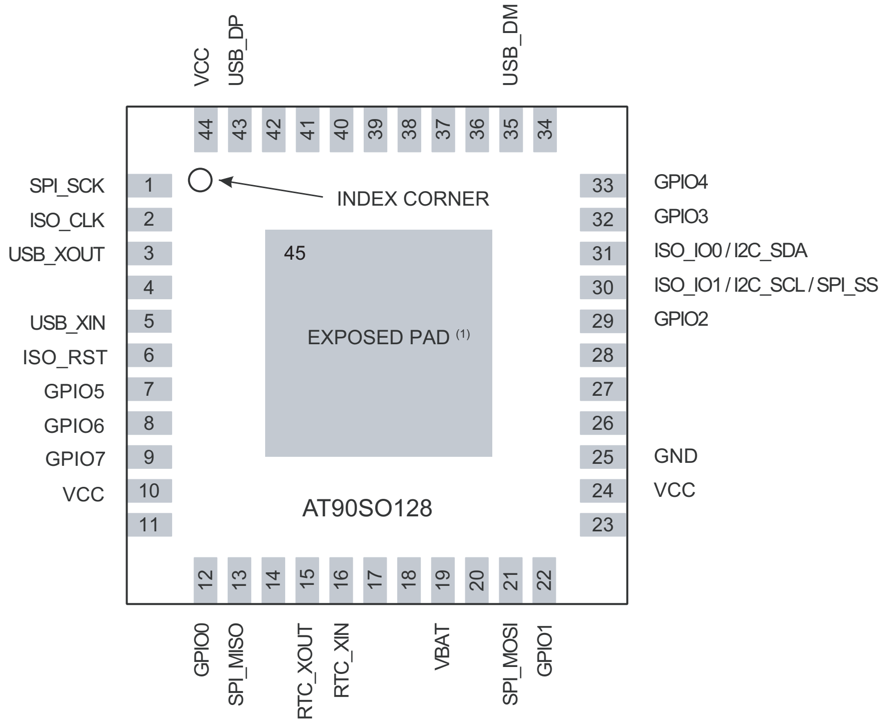


Figure 2. Pinout AT90SO128 - Package QFN44

Note: [1]The exposed pad is internally connected to the ground. It must be connected to GND.

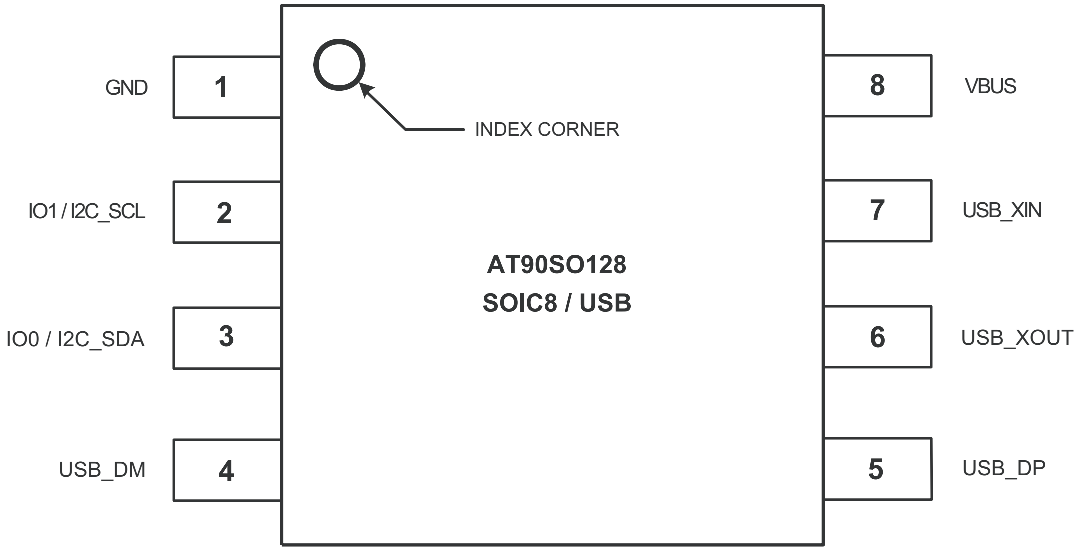


Figure 3. Pinout AT90SO128 - Package SOIC8 - USB Configuration

Figure 4. Pinout AT90SO128 - Package SOIC8 - SPI Configuration

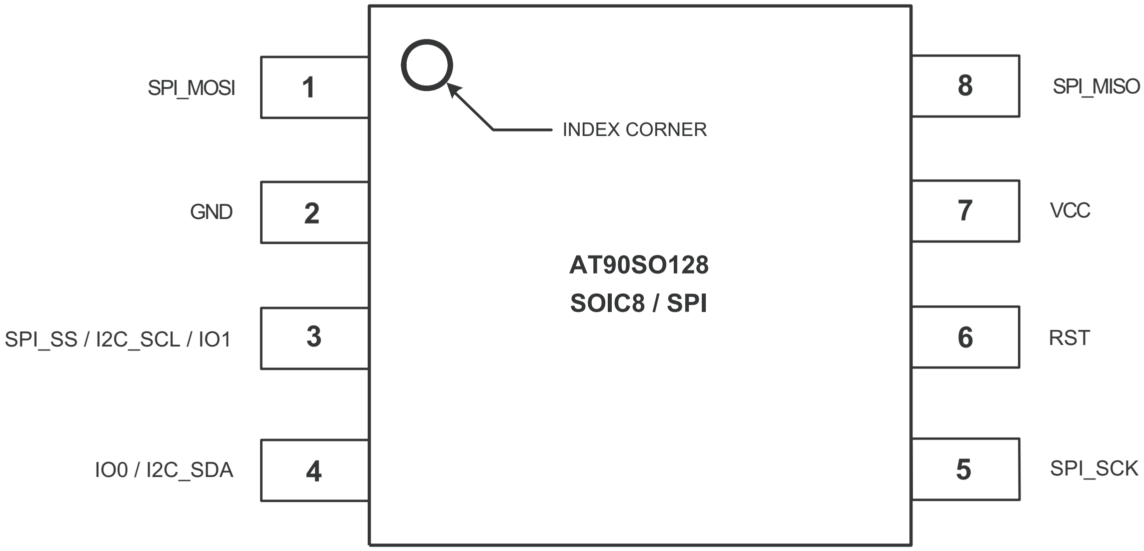


Figure 5. Pinout AT90SO128 - Package SOIC8 - ISO7816 Configuration

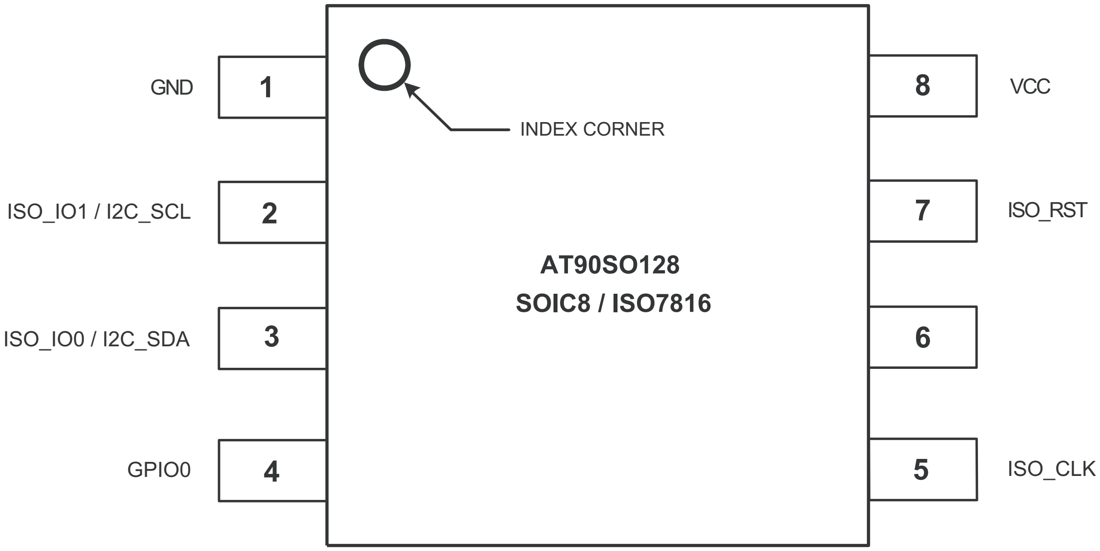
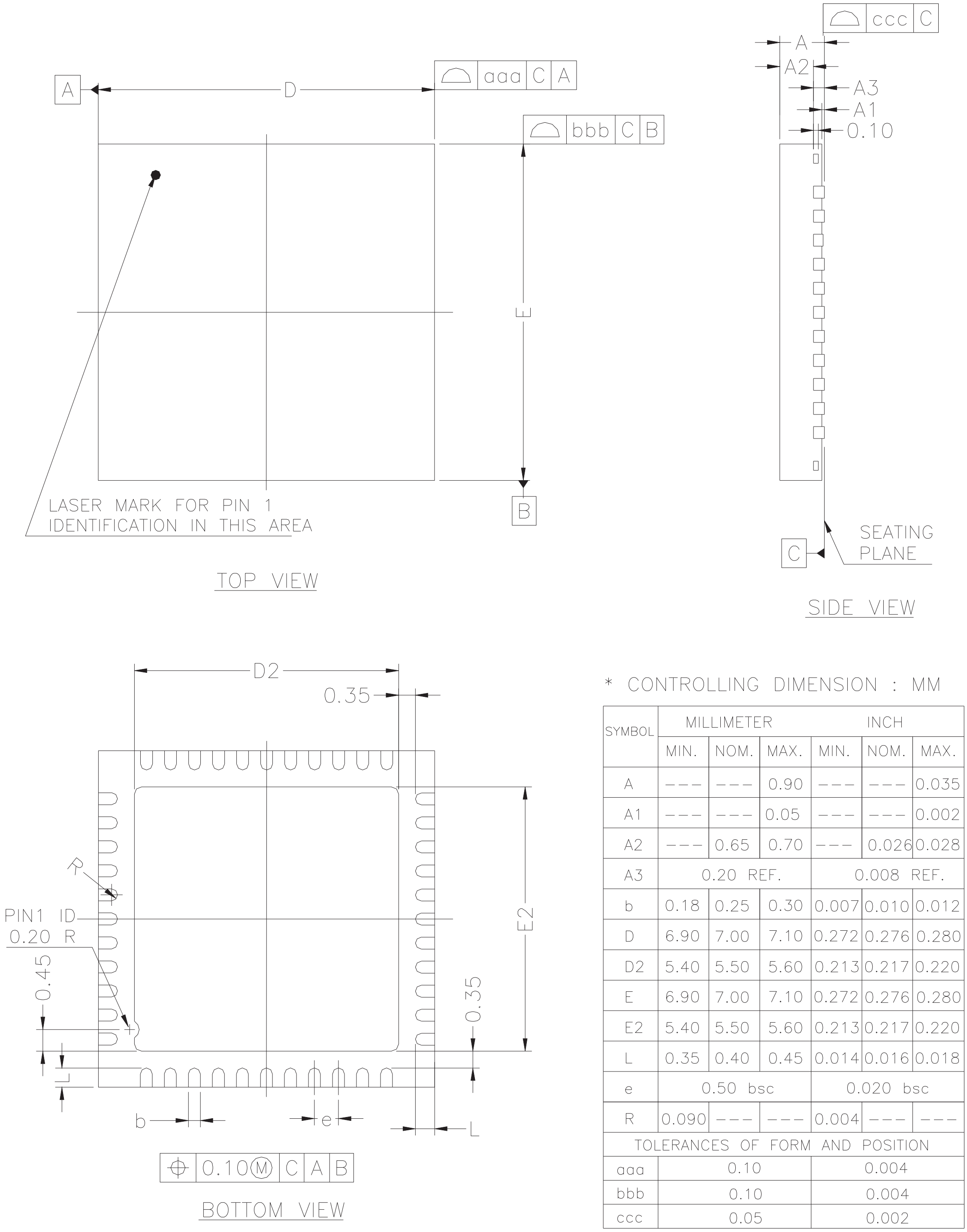


Figure 6. Quad Flat No Lead Package, 44 Leads



* CONTROLLING DIMENSION : MM

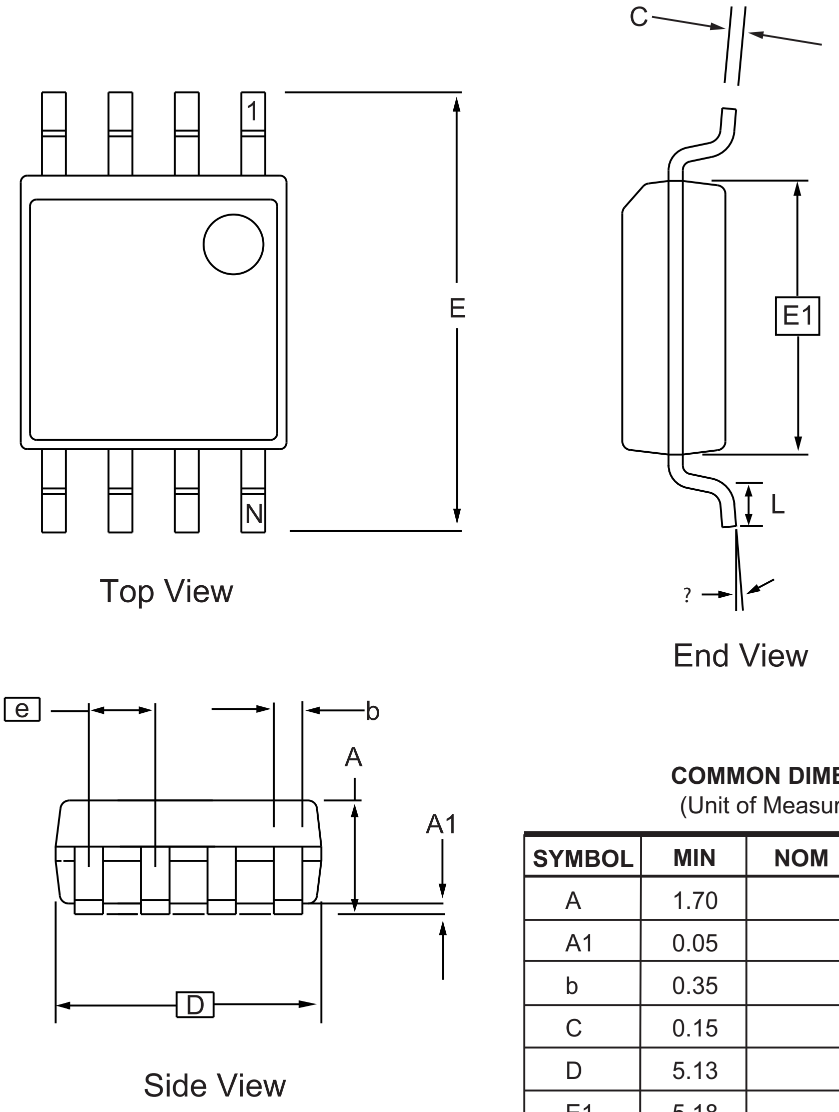
SYMBOL	MILLIMETER			INCH		
	MIN.	NOM.	MAX.	MIN.	NOM.	MAX.
A	---	---	0.90	---	---	0.035
A1	---	---	0.05	---	---	0.002
A2	---	0.65	0.70	---	0.026	0.028
A3	0.20 REF.			0.008 REF.		
b	0.18	0.25	0.30	0.007	0.010	0.012
D	6.90	7.00	7.10	0.272	0.276	0.280
D2	5.40	5.50	5.60	0.213	0.217	0.220
E	6.90	7.00	7.10	0.272	0.276	0.280
E2	5.40	5.50	5.60	0.213	0.217	0.220
L	0.35	0.40	0.45	0.014	0.016	0.018
e	0.50 bsc			0.020 bsc		
R	0.090	---	---	0.004	---	---
TOLERANCES OF FORM AND POSITION						
aaa	0.10			0.004		
bbb	0.10			0.004		
ccc	0.05			0.002		

NOTES :

1.ALL DIMENSIONS ARE IN MILLIMETERS.

2.PACKAGE WARPAGE MAX 0.08 mm.

Figure 7. Plastic Small Outline Package - 8-lead - 0.209” Body



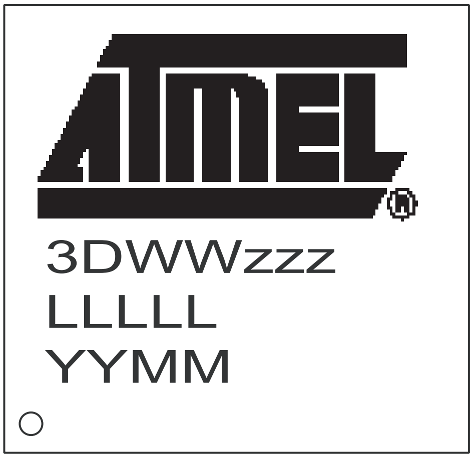
COMMON DIMENSIONS
(Unit of Measure = mm)

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.

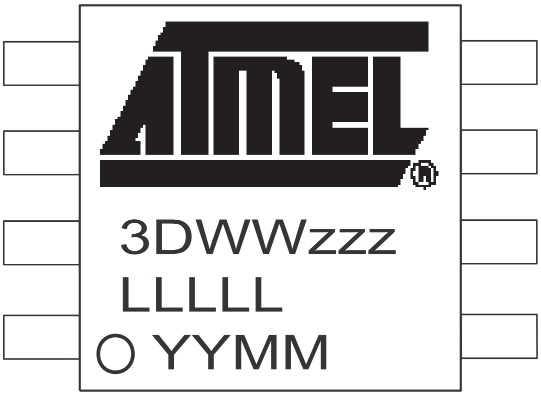
Product Marking

Figure 8. Package QFN44



3D: Chip Identification Number
WW: ROM Code
zzz: Chip Personalization Number
LLLLL : Lot Number
YYMM : Date Code

Figure 9. Package SOIC8



3D: 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

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

Symbol	Parameter	Condition	Min.	Typ.	Max.	Units
V_{CC}	Supply Voltage		2.7		5.5	V
V_{BAT}	RTC Supply Voltage		2.2		3.5	V
V_{IH}	Input High Voltage - I/O Input High Voltage - CLK Input High Voltage - RST		0.7*V_{CC} 0.7*V_{CC} 0.7*V_{CC}		V_{CC}+0.3 V_{CC}+0.3 V_{CC}+0.3	V
V_{IL}	Input Low Voltage - I/O Input Low Voltage - CLK Input Low Voltage - RST		-0.3 -0.3 -0.3		0.2*V_{CC} 0.2*V_{CC} 0.2*V_{CC}	V
I_{IH}	Leakage High Current - I/O Leakage High Current - CLK Leakage High Current - RST	$V_{IN} = V_{IH}$ $V_{IN} = V_{IH}$ $V_{IN} = V_{IH}$	-10 -10 -10		10 10 10	µA
I_{IL}	Leakage Low Current - I/O Leakage Low Current - CLK Leakage Low Current - RST	$V_{IN} = V_{IL}$ $V_{IN} = V_{IL}$ $V_{IN} = V_{IL}$	-40 -10 -40		10 10 10	µA
V_{OL}	Output Low Voltage - I/O	V_{CC} = 5V, I_{OL} = 1mA V_{CC} = 3V, I_{OL} = 1mA	-0.3 -0.3		0.08*V_{CC} 0.15*V_{CC}	V
V_{OH}	Output High Voltage - I/O	V_{CC} = 5V, I_{OL} = 1mA V_{CC} = 3V, I_{OL} = 1mA	0.7*Vcc 0.7*Vcc		Vcc+0.3 Vcc+0.3	V

Table 2. DC Characteristics (2.7V - 5.50V range; T= -25°C to +85°C) [1]

Symbol	Parameter	Condition	Min.	Typ.	Max.	Units
I_O	Output current - I/O Output current - I/O Output current - GPIO	V_{CC} = 5V V_{CC} = 3V V_{CC} = 5V			28.8 10.6 8	mA mA mA
R_{IO}	RST, IOx, SCK, MISO, MOSI pins pullup			220		kΩ
R_{GPIO}	GPIOx pins pullup			15		kΩ

1. This table only gives expected values. Real and accurate values will be available after characterization of the chip.

Table 3. AC Characteristics (2.7V - 5.50V range; T= -25°C to +85°C) [1]

Symbol	Parameter	Condition	Min.	Typ.	Max.	Units
f_{CLK}	External Clock Frequency		1		5	MHz
f_{VFO}	Variable Frequency Oscillator [2]	Expected value at 25°C Clock Jitter **not enabled**	25	30	35	MHz
f_{VFO} Average	Average Variable Frequency Oscillator[2]	Expected value at 25°C Clock Jitter **enabled**		25		MHz
t_{EEPROM}	EEPROM Write Time (erase+write)				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. This table only gives expected values. Real and accurate values will be available after characterization of the chip.
2. 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) [1]

Symbol	Parameter	Condition	Min.	Typ.	Max.	Units
V_{MAX}	Voltage Monitor: High Level Detection		5.5			V
V_{MIN}	Voltage Monitor: Low Level Detection				2.7	V
f_{MAX}	External Frequency Monitor: High Level Detection	Duty cycle = 40% to 60%	5			MHz

Table 4. Security Characteristics (2.7V - 5.50V range; T= -25°C to +85°C) [(1)]

Symbol	Parameter	Condition	Min.	Typ.	Max.	Units
f_{MIN}	External Frequency Monitor: Low Level Detection	Duty cycle = 40% to 60% Running on External Clock			1	MHz
T_{MON} Min	Temperature Monitor: Low Level Detection				-25	°C
T_{MON} Max	Temperature Monitor: High Level Detection	Class A, B	85			°C

1. This table only gives expected values. Real and accurate values will be available after characterization of the chip.

Table 5. Icc Characteristics (2.7V - 5.50V range; T= -25°C to +85°C) [(1)]

Symbol	Parameter	Condition	Min.	Typ.	Max.	Units
$I_{cc\ Run\ Mode}$	Supply Current in Run Mode f_{CLK}=5MHz	From ROM			TBD	mA
$I_{cc\ Run\ Mode}$	Supply Current in Run Mode f_{CLK}=5MHz	From EEPROM			TBD	mA
$I_{cc\ Run\ Mode}$	Supply Current in Run Mode f_{VFO}=26MHz	From ROM			20	mA
$I_{cc\ Run\ Mode}$	Supply Current in Run Mode f_{VFO}=26MHz	From EEPROM			TBD	mA
$I_{cc\ DES}$	Supply Current add-on when DES is running f_{CLK}=5MHz				4	mA
$I_{cc\ DES}$	Supply Current add-on when DES is running f_{VFO}=26MHz				10	mA
$I_{cc\ IDLE}$	Supply Current in IDLE Mode Clock :5MHz	V_{CC} = 5V V_{CC} = 3V			TBD TBD	mA
$I_{cc\ POWER\text{-}DOWN}$	Supply Current in POWER-DOWN Mode Clock : 1MHz	V_{CC} = 5V V_{CC} = 3V			TBD TBD	µA
$I_{cc\ POWER\text{-}DOWN}$	Supply Current in POWER-DOWN Mode No Clock Running	V_{CC} = 5V V_{CC} = 3V			TBD TBD	µA
$I_{cc\ BAT}$	RTC Supply Current				4	µA

1. This table only gives expected values. Real and accurate values will be available after characterization of the chip.

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

Disclaimer: The information in this document is provided in connection with Atmel products. No license, express or implied, by estoppel or otherwise, to any intellectual property right is granted by this document or in connection with the sale of Atmel products. **EXCEPT AS SET FORTH IN ATMEL'S TERMS AND CONDITIONS OF SALE LOCATED ON ATMEL'S WEB SITE, ATMEL ASSUMES NO LIABILITY WHATSOEVER AND DISCLAIMS ANY EXPRESS, IMPLIED OR STATUTORY WARRANTY RELATING TO ITS PRODUCTS INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. IN NO EVENT SHALL ATMEL BE LIABLE FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL, PUNITIVE, SPECIAL OR INCIDENTAL DAMAGES (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, BUSINESS INTERRUPTION, OR LOSS OF INFORMATION) ARISING OUT OF THE USE OR INABILITY TO USE THIS DOCUMENT, EVEN IF ATMEL HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.** Atmel makes no representations or warranties with respect to the accuracy or completeness of the contents of this document and reserves the right to make changes to specifications and product descriptions at any time without notice. Atmel does not make any commitment to update the information contained herein. Atmel's products are not intended, authorized, or warranted for use as components in applications intended to support or sustain life.