maxim integrated™

MAXQ1004

DeepCover Secure Microcontroller with 1-Wire and SPI

General Description

DeepCover™ embedded security solutions cloak sensitive data under multiple layers of advanced physical security to provide the most secure key storage possible.

The low-power DeepCover Secure Microcontroller (MAXQ1004) integrates a 10-bit ADC, 1-Wire® slave interface, SPI, AES encryption, random-number generator (RNG), and temperature sensor with a 16-bit MAXQ® pipelined CPU. Performance bandwidth is sufficient to handle master or slave challenge-response authentication in portable devices.

The device incorporates 16KB of flash memory and 640B of RAM. Factory programming of a customer secret key is available upon request. The microcontroller runs within a wide 1.7V to 3.6V operating range.

For the ultimate in low-power performance, an ultra-low-power stop mode (300nA typ) is available. In this mode, only a minimum amount of circuitry is powered to support detection of the start of a 1-Wire transaction. When 1-Wire activity is detected, the microcontroller is turned on and the command is executed in an atomic fashion. This allows for stateless operation between commands, providing the highest reliability and lowest power consumption.

Applications

Portable Electronics

Battery Chargers

Battery Packs

Ordering Information

PART	TEMP RANGE	AES ENCRYPTION	PIN-PACKAGE
MAXQ1004-B01+	-40°C to +85°C	Yes	16 TQFN-EP*

+Denotes a lead(Pb)-free/RoHS-compliant package.
**EP = Exposed pad.*

DeepCover is a trademark and 1-Wire and MAXQ are registered trademarks of Maxim Integrated Products, Inc.

Features

- **High-Performance, Low-Power, 16-Bit MAXQ20 RISC Core**
- **6MHz Operation from an Internal Oscillator, Approaching 1MIPS per MHz**
- **1.7V to 3.6V Wide Operating Voltage**
- **Three Independent Data Pointers Accelerate Data Movement with Automatic Increment/Decrement**
- **Up to Eight General-Purpose I/O Pins**
- **16-Level Hardware Stack**
- **Optimized for C-Compiler (High-Speed/Density Code)**
- **Memory**
  - **16KB Flash Memory, In-Application Programmable**
  - **640B of Data RAM**
  - **4KB of ROM**
  - **JTAG/TAP Bootloader Mode for In-System Programming**
- **Peripheral Features**
  - **10-Bit Delta-Sigma ADC, Internal Reference**
  - **1-Wire Slave Interface**
  - **On-Chip Power-On Reset (POR)/Power-Fail Reset**
  - **Overvoltage Detection**
  - **Programmable Watchdog Timer**
  - **Built-In Temperature Sensor, ±6°C**
- **Secure Programming Interface**
  - **Flash Programming Through Secure ROM Loader**
  - **Secret Key Destruction on Mass Erase**
  - **Permanent Loader Lockout Option**
  - **Code and Secret Scrambling**
- **Unique 64-Bit Serial Number**
- **Low-Power Consumption**
  - **300nA (typ) in Stop Mode**
  - **3.75mA (typ) at 6MHz, 0.8mA (typ) at 1MHz**
  - **Low-Power Divide-by Modes (2, 4, 8, 256)**
  - **1-Wire/Interrupt Activity Detector**

For pricing, delivery, and ordering information, please contact Maxim Direct at 1-888-629-4642, or visit Maxim Integrated's website at www.maximintegrated.com.

19-5258; Rev 1; 1/13

TABLE OF CONTENTS

Absolute Maximum Ratings 4
Recommended DC Operating Conditions 4
10-Bit ADC Performance 5
SPI Electrical Characteristics 6
SPI Master Communications Timing 7
SPI Slave Communications Timing 7
Pin Configuration 8
Pin Description 8
Block Diagram 9
Detailed Description 10
MAXQ Core Architecture 10
Memory Organization 10
Utility ROM 10
Loading Flash Memory with the Bootstrap Loader 11
In-Application Flash Programming 11
Code Scrambling 11
ADC 11
Temperature Sensor 11
Nanopower Ring Wake-Up Timer 11
Serial Number/Device ID 11
Hardware AES Engine 12
Watchdog Timer 12
16-Bit Timer/Counter 13
Serial Peripherals 13
Serial Peripheral Interface (SPI) 13
1-Wire Bus System 13
Hardware Configuration 13
Slave Functionality 14
Operating Modes 14
In-Circuit Debug 15
Applications Information 15
Grounds and Bypassing 15
Design Guidelines for ESD Protection 15
Additional Documentation 16
Development and Technical Support 16
Typical Application Circuit 16
Package Information 17
Revision History 18

LIST OF FIGURES

Figure 1. ADC Block Diagram 12
Figure 2. In-Circuit Debugger 15
Figure 3. I/O Protection 16
Figure 4. Typical Application Circuit 17

LIST OF TABLES

Table 1. Watchdog Interrupt Timeout 13

ABSOLUTE MAXIMUM RATINGS

Voltage Range on All Pins (including V_{DD}), except DQ to GND ..... -0.5V to +3.6V
Voltage Range on DQ Relative to GND ..... -0.5V to +6.0V
Continuous Output Current
Any Single I/O Pin 35mA
All I/O Pins Combined 35mA

Continuous Power Dissipation (T_A = +70°C)
Single-Layer Board (derate 16.9mW/°C above +70°C) .. 1349.1mW
Multilayer Board (derate 25mW/°C above +70°C) 2000mW
Operating Temperature Range ..... -40°C to +85°C
Storage Temperature Range ..... -65°C to +150°C
Lead Temperature (soldering, 10s) ..... +300°C
Soldering Temperature (reflow) ..... +260°C

Stresses beyond those listed under "Absolute Maximum Ratings" may cause permanent damage to the device. These are stress ratings only, and functional operation of the device at these or any other conditions beyond those indicated in the operational sections of the specifications is not implied. Exposure to absolute maximum rating conditions for extended periods may affect device reliability.

RECOMMENDED DC OPERATING CONDITIONS

(V_{DD} = 1.7V to 3.6V, T_A = -40°C to +85°C, unless otherwise noted. Typical values are at T_A = +25°C and V_{DD} = 3.3V, unless otherwise noted.) (Note 1)

PARAMETER	SYMBOL	CONDITIONS		MIN	TYP	MAX	UNITS
Supply Voltage	V_{DD}			V_{RST}	3.3	3.6	V
1.8V Internal Regulator	V_{REG18}			1.62	1.8	1.98	V
Power-On Reset Voltage	V_{POR}			1.0		1.42	V
Power-Fail Reset Voltage	V_{RST}	(Note 2)		1.64		1.695	V
Power-Fail Warning Voltage	V_{PFW}	(Notes 3, 4)		1.75		1.85	V
Digital Overvoltage Detect	V_{HV}	Monitors V_{REG18}		2.4		2.8	V
Supply Current (Note 5)	I_{DD1}	Device is executing from flash	f_{SYS} = 6MHz			3.5	mA
	I_{DD2}		f_{SYS} = 1MHz		0.8		
Stop-Mode Current (Note 5)	I_{STOP1}	T_A = +25°C, CPU not backed up				5	µA
	I_{STOP2}	T_A = +85°C, CPU not backed up				7.5	
	I_{STOP3}	T_A = +25°C, CPU backed up				6.5	
	I_{STOP4}	T_A = +85°C, CPU backed up				9	
DIGITAL I/O							
Input High Voltage (P0, $\overline{RST}$)	V_{IH}			0.7 x V_{DD}		V_{DD}	V
Input Hysteresis	V_{IHYS}	(Note 6)			0.3		V
Input Low Voltage (P0, $\overline{RST}$)	V_{IL}			V_{GND}		0.3 x V_{DD}	V
Output Low Voltage (P0, $\overline{RST}$) (Note 7)	V_{OL}	V_{DD} = 3.6V, I_{OL} = 4mA (Note 6)				0.4	V
		V_{DD} = 1.85V, I_{OL} = 4mA				0.4	
Output High Voltage (P0, $\overline{RST}$)	V_{OH}	I_{OH} = -2mA		V_{DD} - 0.4		V_{DD}	V
Input Leakage Current	I_L	Internal pullup disabled		-100		+100	nA
Input/Output Pin Capacitance	C_{IO}	(Note 6)				15	pF
Input Low Current for All Pins	I_{IL}	V_{IN} = 0.4V, pullup enabled				-70	µA
$\overline{RST}$ Pullup Resistor	R_{RST}				65	±20%	kΩ

RECOMMENDED DC OPERATING CONDITIONS (continued)

(V_{DD} = 1.7V to 3.6V, T_A = -40°C to +85°C, unless otherwise noted. Typical values are at T_A = +25°C and V_{DD} = 3.3V, unless otherwise noted.) (Note 1)

PARAMETER	SYMBOL	CONDITIONS	MIN	TYP	MAX	UNITS
INTERNAL OSCILLATOR						
Oscillator Frequency	f_{OSC}		5	6	7	MHz
Oscillator Startup Time	t_{OSC_RDY}	V_{REG18} = 1.8V (Note 6)		350		µs
Oscillator Duty Cycle		(Note 6)	45		55	%
NANOPOWER RING OSCILLATOR						
Nanopower Ring Frequency	f_{NANO}	T_A = +25°C	3	11	22	kHz
Nanopower Ring Current	I_{NANO}	Typical at V_{DD} = 3.0V, active during wake-up (Note 6)		120	400	nA
Wakeup Timer Interval	t_{WAKEUP}	$1/f_{NANO}$	t_{NANO}		65,535 x t_{NANO}	s
FLASH MEMORY						
Flash Erase Time		Mass erase	20		40	ms
		Page erase	20		40	
Flash Programming Time per Word	t_{PROG}		20		40	µs
Write/Erase Cycles			1000			Cycles
Data Retention		T_A = +25°C	100			Years
Analog Supply Voltage	V_{AVDD}			V_{DD}		V

10-BIT ADC PERFORMANCE

(V_{DD} = 1.7V to 3.6V, V_{REF} = 1.845V, T_A = -40°C to +85°C, unless otherwise noted.)

PARAMETER	SYMBOL	CONDITIONS	MIN	TYP	MAX	UNITS
Resolution				10		Bits
ADC Clock Frequency	f_{ACLK}			f_{SYSCLK}		MHz
ADC Clock Period	t_{ACLK}			$1/f_{ACLK}$		µs
AN0 Input Voltage Range	V_{AN0}		V_{GND}		V_{AVDD}	V
Analog Input Capacitance	C_{AIN}			1		pF
Integral Nonlinearity	INL	(Note 6)			±2	LSB
Differential Nonlinearity	DNL	No missing codes over temperature			±1	LSB
Offset Error	V_{OS}				±2	LSB
ADC Active Current Consumption	I_{ADC}	f_{ACLK} = 6MHz, internal reference on, ADEN = 1 (Note 6)		100	150	µA
ADC Setup Time	t_{ADC_SETUP}			25		µs
ADC Output Latency	t_{ADC}			1025		t_{ACLK}
ADC Settling Time	t_{ADC_SETTLE}	Settling time due to channel, reference or scale change (not production tested)		10		µs
ADC Throughput				f_{ADC}/t_{ADC}		ksps
TEMPERATURE SENSOR						
Temperature Sensor Setup Time	t_{TSN_SETUP}			25		µs
Temperature Sensor Error	ΔT_{SN}				±6	°C

10-BIT ADC PERFORMANCE (continued)

(V_{DD} = 1.7V to 3.6V, V_{REF} = 1.845V, T_A = -40°C to +85°C, unless otherwise noted.)

PARAMETER	SYMBOL	CONDITIONS	MIN	TYP	MAX	UNITS
10-BIT ADC REFERENCE VOLTAGE						
Internal Reference Voltage	V_{IREF}			1.845	±5%	V

Note 1: Specifications to -40°C are guaranteed by design and are not production tested.

Note 2: The power-fail reset and POR detectors operate in tandem so one or both of these signals are active at all times when $V_{DD} < V_{RST}$, ensuring the device maintains the reset state until minimum operating voltage is achieved.

Note 3: The power-fail warning monitor and the power-fail reset monitor track each other with a typical delta between the two of 0.13V.

Note 4: Writes to flash memory must not be performed when the supply voltage drops below the power-fail warning levels, as there is uncertainty in the duration of continuous power supply. The user application should check the status of the power-fail warning flag before writing to flash to ensure valid write operations.

Note 5: Measured on the combined AVDD and V_{DD} pins and the part not in reset. All inputs are connected to GND or V_{DD}. Outputs do not source/sink any current.

Note 6: Guaranteed by design and not production tested.

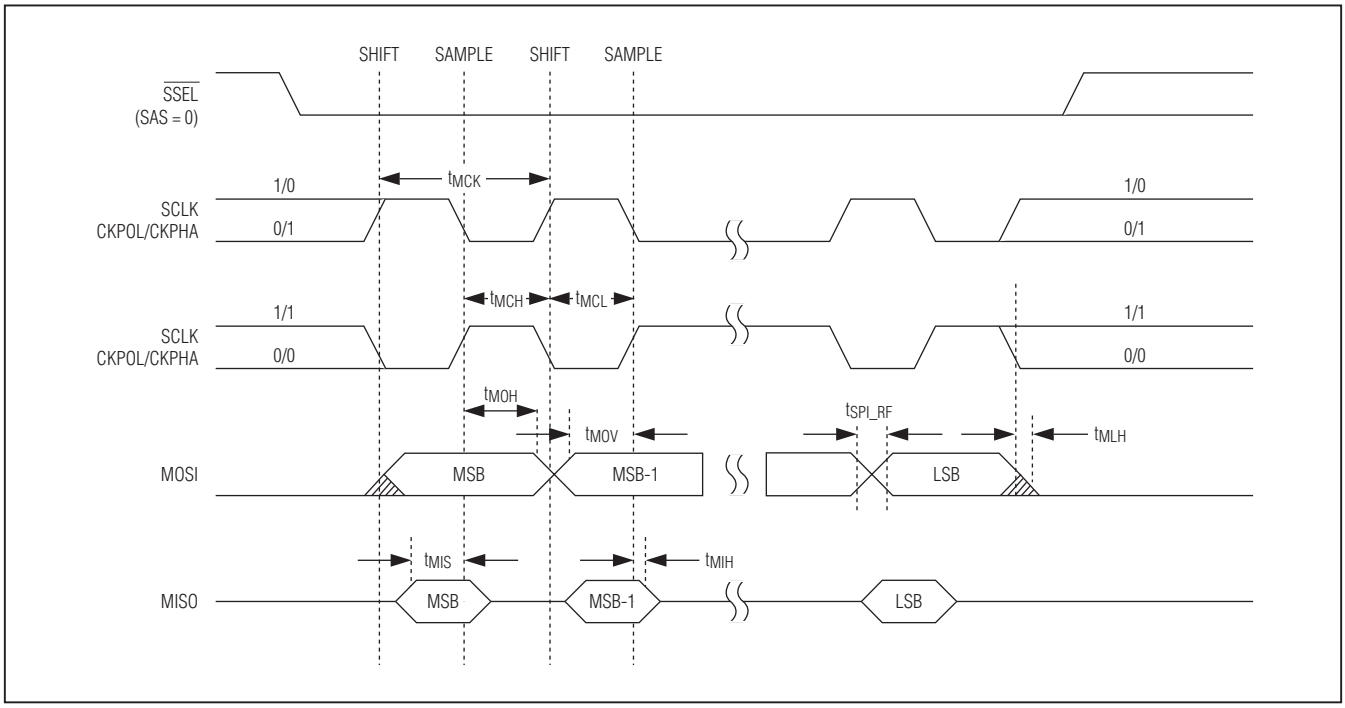
Note 7: The maximum total current, $I_{OH(MAX)}$ and $I_{OL(MAX)}$, for all outputs combined should not exceed 35mA to satisfy the maximum specified voltage drop.

SPI ELECTRICAL CHARACTERISTICS

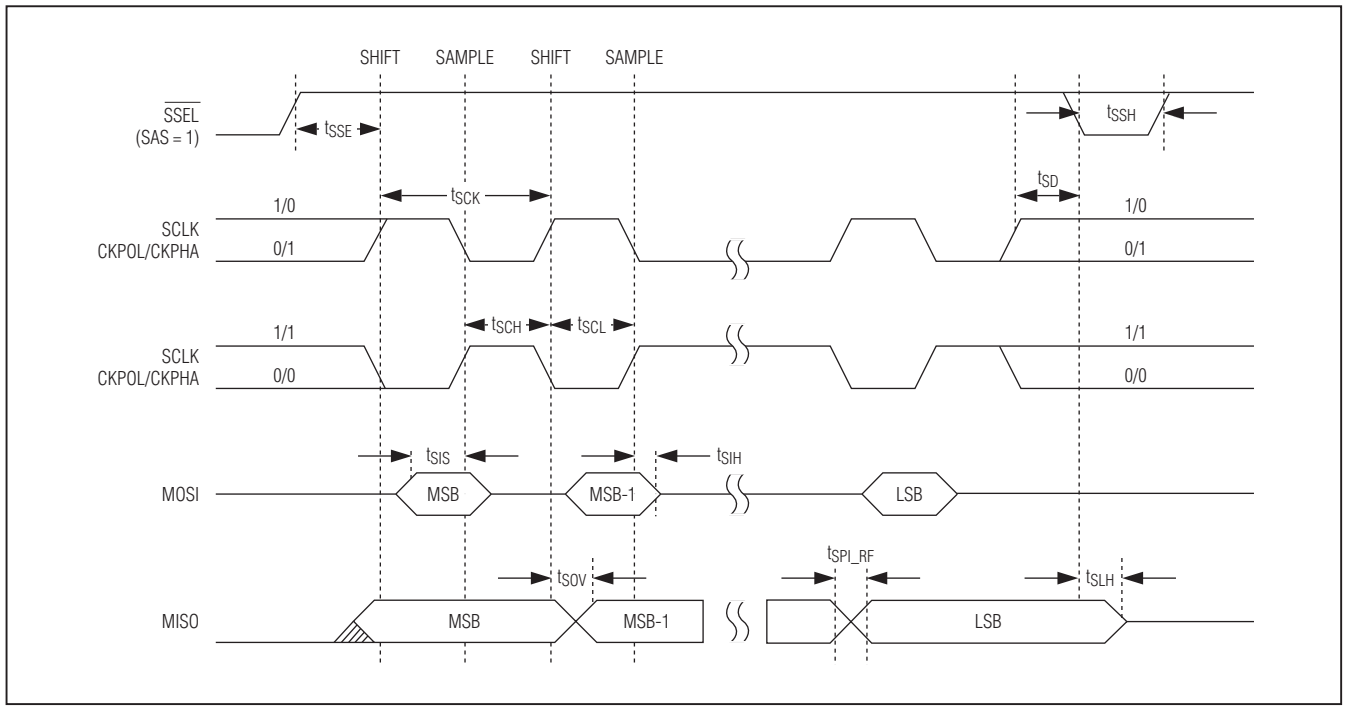
(V_{DD} = 1.7V to 3.6V, T_A = -40°C to +85°C, unless otherwise noted. AC electrical specifications are guaranteed by design and are not production tested.)

PARAMETER	SYMBOL	CONDITIONS	MIN	TYP	MAX	UNITS
SPI Master Operating Frequency	$1/t_{MCK}$				$f_{SYSCLK}/2$	MHz
SPI Slave Operating Frequency	$1/t_{SCK}$				$f_{SYSCLK}/4$	MHz
SPI I/O Rise/Fall Time	t_{SPI_RF}	C_L = 15pF, pullup = 560Ω	8.3		23.6	ns
SCLK Output Pulse-Width High/Low	t_{MCH}, t_{MCL}		$t_{MCK}/2 - t_{SPI\_RF}$			ns
MOSI Output Hold Time After SCLK Sample Edge	t_{MOH}		$t_{MCK}/2 - t_{SPI\_RF}$			ns
MOSI Output Valid to Sample Edge	t_{MOV}		$t_{MCK}/2 - t_{SPI\_RF}$			ns
MISO Input Valid to SCLK Sample Edge Rise/Fall Setup	t_{MIS}		25			ns
MISO Input to SCLK Sample Edge Rise/Fall Hold	t_{MIH}		0			ns
SCLK Inactive to MOSI Inactive	t_{MLH}		$t_{MCK}/2 - t_{SPI\_RF}$			ns
SCLK Input Pulse-Width High/Low	t_{SCH}, t_{SCL}			$t_{SCK}/2$		ns
$\overline{SSEL}$ Active to First Shift Edge	t_{SSE}		t_{SPI_RF}			ns
MOSI Input to SCLK Sample Edge Rise/Fall Setup	t_{SIS}		t_{SPI_RF}			ns
MOSI Input from SCLK Sample Edge Transition Hold	t_{SIH}		t_{SPI_RF}			ns
MISO Output Valid After SCLK Shift Edge Transition	t_{SOV}				$2t_{SPI\_RF}$	ns
$\overline{SSEL}$ Inactive	t_{SSH}		$t_{SCK} + t_{SPI\_RF}$			ns
SCLK Inactive to $\overline{SSEL}$ Rising	t_{SD}		t_{SPI_RF}			ns
MISO Output Disabled After $\overline{SSEL}$ Edge Rise	t_{SLH}				$2t_{SCK} + 2t_{SPI\_RF}$	ns

SPI Master Communications Timing

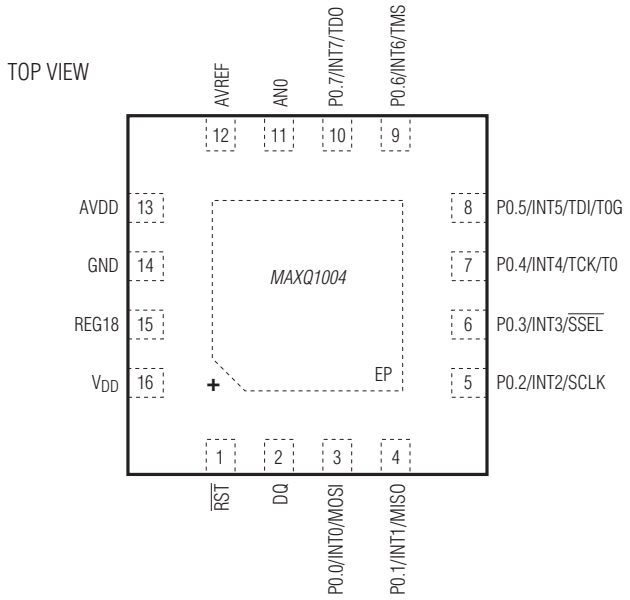


SPI Slave Communications Timing



DeepCover Secure Microcontroller with 1-Wire and SPI

Pin Configuration



TQFN
(4mm × 4mm)

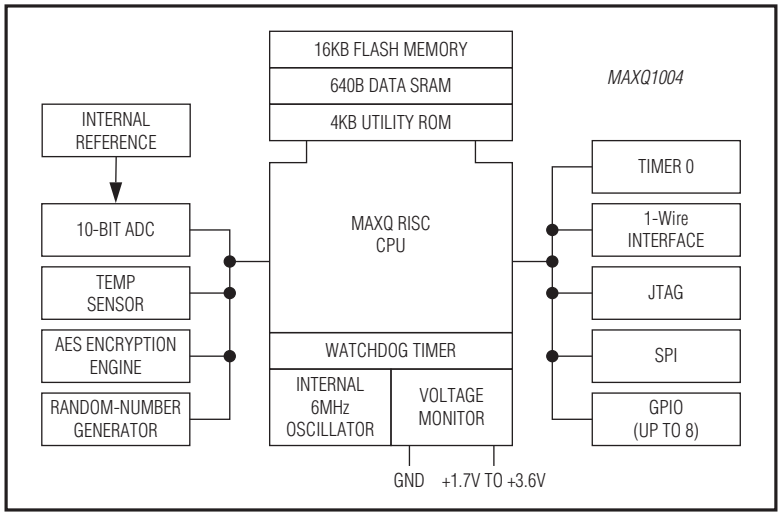
Pin Description

PIN	NAME	FUNCTION
		POWER PINS
11	AN0	Analog Input 0. This pin is the analog input to the ADC.
12	AVREF	Analog Voltage Reference. Do not connect anything external to this pin.
13	AVDD	Analog Supply Voltage. Directly connect AVDD to V_{DD}.
14	GND	Digital Ground
15	REG18	Regulator Capacitor. This pin must be connected to ground through an external 1µF low ESR (< 5Ω) capacitor.
16	V_{DD}	Digital Supply Voltage. +3.3V nominal supply voltage.
—	EP	Exposed Pad. Connect the EP to the ground plane.
		RESET AND STATUS PINS
1	$\overline{RST}$	Active-Low Reset. This bidirectional pin recognizes external active-low reset inputs and employs an internal pullup resistor to allow for a combination of wired-OR external reset sources. This pin also acts as an output when the source of the reset is internal to the device (e.g., watchdog timer, power-fail, etc.). In this case, the pin is low while the processor is in a reset state, and it returns high as the processor exits this state.

Pin Description (continued)

<table>
<tr><th>PIN</th><th>NAME</th><th>FUNCTION</th></tr>
<tr><td colspan="3">GENERAL-PURPOSE I/O PINS</td></tr>
<tr><td>3–10</td><td>P0.0–P0.7, INT0–INT7, MOSI, MISO, SCLK, SSEL, TCK, TDI, TMS, TDO</td><td>General-Purpose, Digital I/O, Type D Port/SPI Interface/JTAG Interface/External Edge-Selectable Interrupt. This port functions as 8-bit I/O and as an alternate interface to external interrupts. Each interrupt can be individually enabled and the active edge can be selected. The default reset condition of the pins is as a weak pullup input. To drive port 0 as output, the port direction register must be programmed to enable output. P0.7–P0.4 default to their JTAG function on any reset.
<table>
<tr><th>PIN</th><th>PORT</th><th>EXTERNAL INTERRUPT</th><th>SPECIAL FUNCTION</th></tr>
<tr><td>3</td><td>P0.0</td><td>INT0</td><td>MOSI: Master Out-Slave In (SPI)</td></tr>
<tr><td>4</td><td>P0.1</td><td>INT1</td><td>MISO: Master In-Slave Out (SPI)</td></tr>
<tr><td>5</td><td>P0.2</td><td>INT2</td><td>SCLK: Slave Clock (SPI)</td></tr>
<tr><td>6</td><td>P0.3</td><td>INT3</td><td>SSEL: Active-Low Slave Select (SPI)</td></tr>
<tr><td>7</td><td>P0.4</td><td>INT4</td><td>TCK: Test Clock (JTAG)/T0</td></tr>
<tr><td>8</td><td>P0.5</td><td>INT5</td><td>TDI: Test Data In (JTAG)/T0G</td></tr>
<tr><td>9</td><td>P0.6</td><td>INT6</td><td>TMS: Test Mode Select (JTAG)</td></tr>
<tr><td>10</td><td>P0.7</td><td>INT7</td><td>TDO: Test Data Out (JTAG)</td></tr>
</table></td></tr>
<tr><td>2</td><td>DQ</td><td>1-Wire Slave Interface, I/O. This 5V tolerant, open-drain I/O pin serves as both transmit and receive pin for the 1-Wire interface. The DQ pin requires an external pullup resistor, the value of which is determined by the speed mode.</td></tr>
</table>

Block Diagram



Detailed Description

The MAXQ1004 is a low-power, high-performance, 16-bit MAXQ microcontroller providing the high security and reliability demanded in today's portable electronics, battery chargers, and battery packs. An ISO/IEC 9797-1 standards-based authentication protocol is available as standard application code.

A 1-Wire communication interface minimizes battery-pack connections required to authenticate and monitor battery health. The 1-Wire I/O pin (DQ) can wake the device from low-power stop mode. In stop mode, power is supplied only to the circuitry required to wake up the slave microcontroller. During stop mode, 512 bytes of data memory are preserved, with an option to preserve the CPU state and the remaining 128 bytes of data memory.

MAXQ Core Architecture

The microcontroller is based on a low-power implementation of the 16-bit MAXQ family of RISC cores. The core supports the Harvard memory architecture with separate 16-bit program and data address buses. A fixed 16-bit instruction word is standard, but data can be arranged in 8 or 16 bits. The core is implemented as a pipelined processor with performance approaching 1MIPS per MHz. The 16-bit data path is implemented around register modules, and each register module contributes specific functions to the core. The accumulator module consists of sixteen 16-bit registers and is tightly coupled with the arithmetic logic unit (ALU).

Execution of instructions is triggered by data transfer between functional register modules or between a functional register module and memory. Because data movement involves only source and destination modules, circuit-switching activities are limited to active modules only. For power-conscious applications, this approach localizes power dissipation and minimizes switching noise. The modular architecture also provides a maximum of flexibility and reusability that is important for a microprocessor used in embedded applications.

The MAXQ instruction set is highly orthogonal. All arithmetical and logical operations can use any register in conjunction with the accumulator. Data movement is supported from any register to any other register. Memory is accessed through specific data-pointer registers with automatic increment/decrement support.

Memory Organization

There are three distinct memory areas: registers, program memory, and data memory. All registers are located on-chip. The device contains built-in program and data memory, including:

- 16KB flash memory, in-application programmable
- 640B of data RAM
- 4KB of ROM

Program flash memory is arranged in 1024-byte pages that can be individually erased and programmed through the use of utility ROM functions.

Utility ROM

The utility ROM is a block of internal ROM that defaults to a starting address of 8000h. The utility ROM consists of subroutines that can be called from application software. These include the following:

- In-system programming using a bootstrap loader
- Test routines (internal memory tests, memory loader, etc.)
- User-callable routines for in-application flash programming and fast table lookup

Following any reset, execution begins in the utility ROM. The ROM software determines whether the program execution should immediately jump to location 0000h, the start of application code, or to one of the special routines mentioned. Routines within the utility ROM are user-accessible and can be called as subroutines by the application software. More information on the utility ROM functions is contained in the *MAXQ1004 User's Guide*.

Some applications require protection against unauthorized viewing of program code memory. For these applications, access to in-system programming, in-application programming, or in-circuit debugging functions is prohibited until a password has been supplied. The password is defined as the 16 words of physical program memory at addresses 0010h–001Fh.

A single password lock (PWL) bit is implemented in the SC register. When the PWL is set to one (POR default) and the contents of the memory at addresses 0010h–001Fh are any value other than FFh or 00h, the password is required to access the utility ROM, including in-circuit debug and in-system programming routines that allow reading or writing of internal memory. When PWL is cleared to zero, these utilities are fully accessible without the password. The password is automatically set to all ones following a mass erase.

Loading Flash Memory with the Bootstrap Loader

An internal bootstrap loader allows the device to be reloaded over a simple JTAG interface. As a result, software can be upgraded in-system, eliminating the need for a costly hardware retrofit when updates are required. Remote software uploads are possible that enable physically inaccessible applications to be frequently updated. If in-system programmability is not required, a commercial gang programmer can be used for mass programming.

In-Application Flash Programming

From user-application code, internal flash memory can be programmed/erased by calling internal ROM utility functions from either C or assembly language. Memory protection is enforced by the ROM utility functions. The function declarations below show examples of some of the ROM utility functions provided for in-application flash memory programming.

```
/* Write one 16-bit word to code address 'dest'.
* Dest must be aligned to 16 bits.
* Returns 0 = failure, 1 = OK.
*/
int flash_write16(uint16_t dest, uint16_t data);
```

To erase, the following function would be used:

```
/* Erase the given Flash page
* addr: Flash offset (anywhere within page)
*/
int flash_erasepage(uint16_t addr);
```

Code Scrambling

Automated code scrambling protects user-code memory against attempts to determine the code contents. The proprietary scrambling algorithm is transparent to the user and still allows in-application programming. Address shuffling prevents well-known startup code from always being at the known location 0000h and interrupt vector code at known locations. This obfuscates confidential software and makes the application secure from hackers and copiers.

ADC

The 10-bit delta-sigma analog-to-digital converter (ADC) allows the application to measure external voltages, most commonly the voltage of the batteries driving V_{DD}. The analog input, AN0, can be optionally scaled by 50% for direct supply voltage measurement. The ADC value saturates (all data bits read 1) when the input voltage exceeds the maximum allowable ADC reference voltage. The internal temperature sensor is measured by the ADC when selected.

Each conversion can choose its own reference from AVDD or the internal reference. Data can be retrieved in either left-justified or right-justified format, giving the application direct control on data format.

A conversion takes 1025 ADCCLK cycles to complete. The ADCCLK is derived from the system clock with divide ratio defined by the ADC clock-divider bits (ADCCLK). Therefore, with 1025 ADCCLK to acquire one data, the fastest ADC rate = Sysclk/1025 (ADCCLK = 0h). See Figure 1.

Temperature Sensor

An integrated temperature sensor measures the internal temperature of the device with an error of ±6°C. The temperature sensor is connected to channel 1 of the ADC. To read the temperature sensor, select ADCH to 1.

Nanopower Ring Wake-Up Timer

A nanopower-ring oscillator can be used to drive a wake-up timer that causes the device to exit stop mode after a user-selectable time period. The wake-up timer is software programmable in 16-bit steps of the nanopower ring clock up to approximately 8 seconds.

Serial Number/Device ID

Each device has a factory-programmed, unique, 64-bit device identification number (ID). This ID ensures device traceability and serves as an input to the device's authentication protocol.

The first 8 bits of the device ID are a 1-Wire family code that is the same for all MAXQ1004 devices. The next 48 bits are a factory-programmed unique serial number. Even if multiple devices are used in a 1-Wire network, the unique, 48-bit serialization field prevents any address conflict, allowing communication with each device individually. The last 8 bits are a factory-programmed cyclic redundancy check (CRC) of the first 56 bits. The 1-Wire CRC is generated using a polynomial generator consisting of a shift register and XOR gates. The polynomial is $x^8 + x^5 + x^4 + 1$.

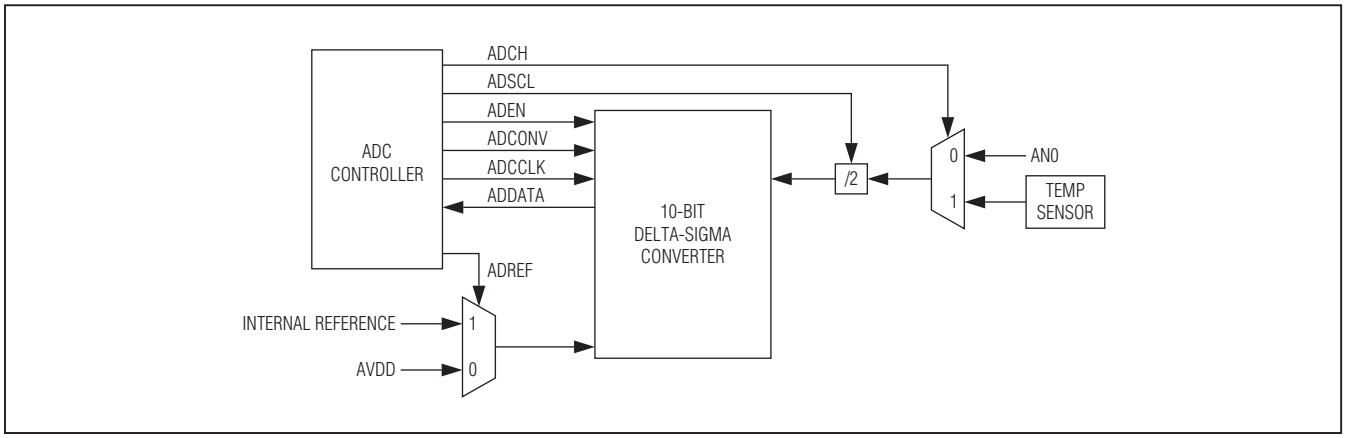


Figure 1. ADC Block Diagram

Hardware AES Engine

The AES engine is a bidirectional block cipher supporting encryption and decryption for all three key lengths recommended by the National Institute of Standards and Technology (NIST). Secret keys can be generated by an on-chip RNG and stored in a predetermined memory location. The AES engine operates independently of the processor, except for setting up an operation through the AES Control register (AESC). The AESC register provides AES engine operation status and option control.

The AES engine shares the cryptographic memory with the 1-Wire communications peripheral. Application software must ensure that the two peripherals do not access the cryptographic memory at the same time or data in the memory may be corrupted. Application software can interrogate activity bits to ensure that one peripheral does not interrupt the other. To perform an encryption or decryption, the keys and data are loaded into the cryptographic memory and the operation is started with the appropriate write to the AESC register. Completion of the operation can be detected by user firmware either by polling the AESC register or through the use of an interrupt.

The AES engine displays excellent performance. Based on key size, the following encryption throughputs are achieved:

- 128-bit key size—55 cycles (9.2µs at 6MHz)
- 192-bit key size—70 cycles (12.0µs at 6MHz)
- 256-bit key size—75 cycles (12.5µs at 6MHz)

An optional jitter injection feature reduces the effectiveness of differential power analysis (DPA) attacks against the device. Adding jitter causes random delays in both the start and ending times of the calculation, confounding attempts to determine the values in the AES operation by measuring minute power fluctuations. When active, the feature adds a variable random delay of 0 to 30 clock cycles to AES calculations. This is accomplished by randomly adding 0 to 15 clock cycles before the AES operation is started, and adding 0 to 15 clock cycles after the operation is complete.

Watchdog Timer

The watchdog timer functions as the source of both the timer timeout and the watchdog timer reset. The timeout period can be programmed in a range of 2^{12} to 2^{29} system clock cycles. An interrupt is generated when the timeout period expires, if the interrupt is enabled. All watchdog timer resets follow the programmed interrupt timeouts by 512 clock cycles. If the watchdog timer is not restarted for another full interval in this time period, a system reset occurs when the reset timeout expires. Table 1 shows values that demonstrate the various interrupt timeouts based on an internal clock frequency of 6MHz.

Table 1. Watchdog Interrupt Timeout

PMME	CD[1:0]	WATCHDOG INTERRUPT TIMEOUT (Sysclk = 6MHz)			
		WD[1:0] = 00	WD[1:0] = 01	WD[1:0] = 10	WD[1:0] = 11
0	00	2^{12} (683µs)	2^{15} (5.46ms)	2^{18} (43.7ms)	2^{21} (350ms)
0	01	2^{13} (1.36ms)	2^{16} (11ms)	2^{19} (87.4ms)	2^{22} (700ms)
0	10	2^{14} (2.73ms)	2^{17} (21.8ms)	2^{20} (175ms)	2^{23} (1.4s)
0	11	2^{15} (5.46ms)	2^{18} (43.7ms)	2^{21} (350ms)	2^{24} (2.8s)
1	xx	2^{20} (175ms)	2^{23} (1.4s)	2^{26} (11.2s)	2^{29} (89.5s)

16-Bit Timer/Counter

The microcontroller has one instance of the 16-bit Timer 0 timer/counter peripheral, which supports the following functions:

- 13-bit timer/counter
- 16-bit timer/counter
- 8-bit timer with autoreload
- 2 8-bit timer/counters

Serial Peripherals

Serial Peripheral Interface (SPI)

The integrated SPI is an independent serial communication channel that communicates synchronously with peripheral devices in a multiple-master or multiple-slave system. The interface allows access to a 4-wire, full-duplex serial bus and can be operated in either master mode or slave mode. Collision detection is provided when two or more masters attempt a data transfer at the same time.

The maximum SPI master transfer rate is Sysclk/2. When operating as an SPI slave, the device can support up to Sysclk/4 SPI transfer rate. Data is transferred as an 8-bit or 16-bit value, MSB first. In addition, the SPI module supports configuration of an active $\overline{SSEL}$ state through the slave active select.

1-Wire Bus System

The 1-Wire bus is a system that has a single bus master and one or more slaves. This microcontroller is always a slave device in any system. The bus master is typically another microcontroller. The discussion of this bus system is broken down into three topics: hardware configuration, transaction sequence, and 1-Wire signaling (signal types and timing). The 1-Wire protocol defines bus transactions in terms of the bus state during specific time slots, which are initiated on the falling edge of sync pulses from the bus master. Refer to Application Note 937: *Book of iButton® Standards* for a more detailed description the 1-Wire network and protocols.

The device permits the use of lower 1-Wire voltage levels (as low as 1.7V) to support the device's full operating voltage, but can still be connected to a regular 1-Wire bus of up to 6V.

Hardware Configuration

The 1-Wire bus has only a single data line (DQ); all devices on the bus must be able to drive it at the appropriate time. This means that each device attached to the 1-Wire bus must have open-drain or high-impedance outputs. The 1-Wire port is open drain.

Both the standard and overdrive communication speed of 15.4kbps (max) and 111kbps (max), respectively, are supported. The value of the pullup resistor primarily depends on the network size and load conditions. Recommended pullup resistor values can be found in Table 4-1 of Application Note 937: *Book of iButton® Standards*.

The idle state for the 1-Wire bus is high. If, for any reason, a transaction needs to be suspended, the bus must remain in the idle state if the transaction is to resume. If this does not occur and the bus is left low for more than 120µs (standard speed), one or more devices on the bus can be reset.

iButton is a registered trademark of Maxim Integrated Products, Inc.

Slave Functionality

The 1-Wire slave provides three functions. The first is that of a totally independent slave function, which can be externally accessed at any time to verify its identity. The 1-Wire front-end functions in an identical fashion to that of the DS1990 serial ID to verify the serial ID number. The bus master must provide one of the ROM function commands:

- Read ROM
- Match ROM
- Search ROM
- Skip ROM
- Overdrive-Skip ROM
- Overdrive-Match ROM
- Resume

The second function is that of a 1-Wire that includes full bidirectional data flow and data flow control. The 1-Wire functions that become accessible after a ROM function command is successfully executed initiate communications with the microcontroller through the use of specific 1-Wire commands:

- Read I/O Buffer
- Write I/O Buffer
- Read Command Buffer
- Write Command Buffer
- Read Command Buffer Extended
- Write Command Buffer Extended
- Status Register Read
- Status Register Write

The third function controls the operation of the 1-Wire interface:

- 1-Wire Micro Reset

And the remaining are 1-Wire run commands:

- Start Program
- Continue Program
- Write Command Buffer Extended and Start Program
- Write Command Buffer Extended and Continue Program

Operating Modes

The low-power mode of operation is stop mode. In this mode, CPU state and memories are preserved, but the CPU is not actively running. Wake-up sources include external I/O interrupts, the power-fail warning interrupt, a valid 1-Wire command received, or a power-fail reset. Any time the microcontroller is in a state where code does not need to be executed, the user software can enter stop mode.

An even lower stop mode is the data-retention mode, in which the CPU is not active. When the data-retention mode option is invoked (DRET = 1) and the regulator is disabled (REGEN = 0), only the first 512 bytes of data memory is retained (data memory word offset 0000h–00FFh). CPU status and 1-Wire/AES memory are powered down and contents are lost. A POR occurs when exiting stop mode from data-retention mode. This mode can be exited from any of the following enabled interrupt sources:

- Enabled external interrupts
- External reset
- Enabled PFW interrupt
- Valid 1-Wire command received
- Wake-up timer

The wake-up timer causes the device to exit stop mode after a user-selectable time period. The power-fail monitor is always on during normal operation. However, it can be selectively disabled during stop mode using the power-fail monitor disable (PFD) bit in the PWCN register. By default, the power-fail monitor function is enabled during stop mode. If power-fail monitoring is disabled (PFD = 1) during stop mode, the circuitry responsible for generating a power-fail warning or reset is shut down and neither condition is detected. Thus, the $V_{DD} < V_{RST}$ condition does not invoke a reset state. However, in the event that V_{DD} falls below the POR level, a POR is generated. The power-fail monitor is enabled prior to stop mode exit and before code execution begins. If a power-fail warning condition ($V_{DD} < V_{PFW}$) is then detected, the power-fail interrupt flag is set on stop mode exit. If a power-fail condition is detected ($V_{DD} < V_{RST}$), the CPU goes into reset.

The 1-Wire peripheral can operate in a special mode that draws minimal power, yet can serve as a wake-up source to bring the device out of stop mode. If the 1-Wire peripheral is required to run in stop mode, it can be enabled so a regular 1-Wire reset pulse briefly wakes up the 1-Wire controller. The 1-Wire controller then determines if it was addressed. If so, the 1-Wire controller wakes up the CPU from stop mode. If the microcontroller is not being addressed, then stop mode continues and the 1-Wire controller is powered down again, and the device returns to its lowest power state. The device does not respond to an overdrive reset pulse in stop mode.

In-Circuit Debug

Embedded debugging capability is available through the JTAG-compatible test access port (TAP). Embedded debug hardware and embedded ROM firmware provide in-circuit debugging capability to the user application, eliminating the need for an expensive in-circuit emulator. See Figure 2. The in-circuit debug features include the following:

- Hardware debug engine
- Set of debug service routines stored in the utility ROM

The embedded hardware debug engine is an independent hardware block in the microcontroller. The debug engine can monitor internal activities and interact with selected internal registers while the CPU is executing user code. Collectively, the hardware and software features allow two basic modes of in-circuit debugging:

- Background mode allows the host to configure and set up the in-circuit debugger while the CPU continues to execute the application software at full speed. Debug mode can be invoked from background mode.
- Debug mode allows the debug engine to take control of the CPU, providing read/write access to internal registers and memory and single-step trace operation.

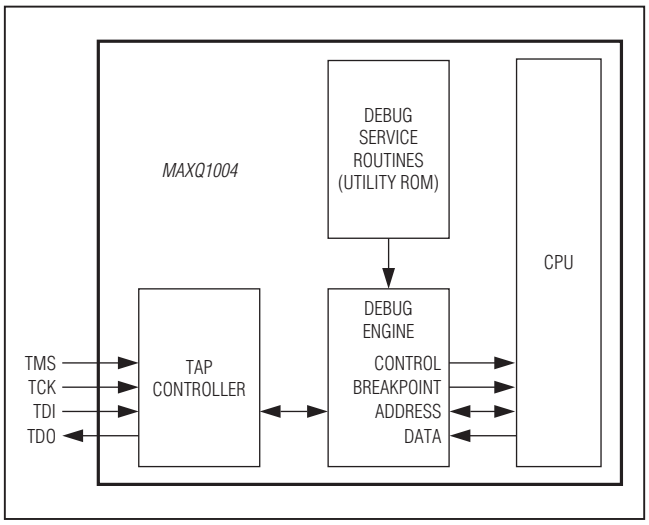


Figure 2. In-Circuit Debugger

Applications Information

Grounds and Bypassing

Careful PCB layout significantly minimizes crosstalk among the high-speed external address/data bus signals and with digital I/O that could cause improper operation. The use of multilayer boards is essential to allow the use of dedicated power planes. Bypass V_{DD} on each microcontroller with a 0.1µF capacitor located as close as possible to the pin.

Design Guidelines for ESD Protection

CMOS design guidelines for any semiconductor require that no pin be taken above V_{DD} or below ground. Violation of this guideline can result in a hard failure (damage to the silicon inside the device) or a soft failure (unintentional modification of memory contents). Voltage spikes above or below the device's absolute maximum ratings can cause a temporary brownout of the internal power rail, possibly corrupting memory.

Microcontrollers commonly experience negative voltage spikes through either their power pins or general-purpose I/O pins. Negative voltage spikes on power pins are especially problematic as they directly couple to the internal power buses. Devices such as keypads can conduct electrostatic discharges directly into the microcontroller and seriously damage the device. System designers must protect components against these transients that can corrupt system memory.

In a practical application, it is difficult to remove all voltages above V_{DD} or below ground. Undershoots of 0.3V can be tolerated by the microcontroller, and 5V tolerant pins can accept up to 5.5V. Figure 3 demonstrates a diode protection scheme that can be used to protect the I/O pins of a microcontroller. The scheme relies on the use of a Schottky diode and current limiting resistor to reduce the effect of current spikes on the device. When the voltage approaching the device pin exceeds V_{DD} or GND by more than 0.1V to 0.2V, the Schottky diodes become forward biased, conducting the excess voltage away from the device pins. The current limiting resistors also help dampen the effect of the voltage spike on the microcontroller.

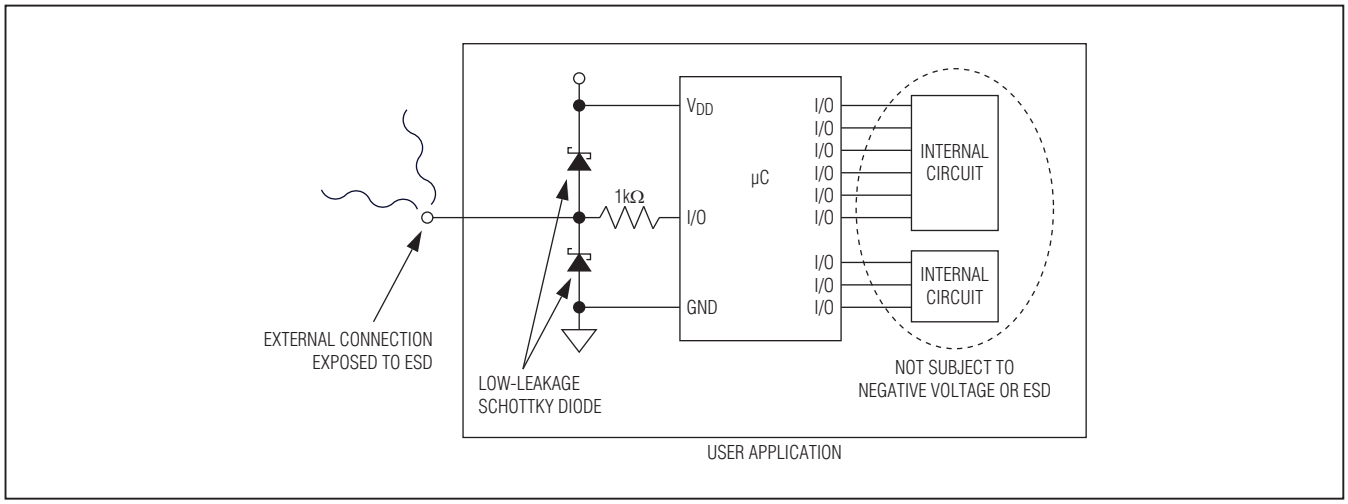


Figure 3. I/O Protection

Any Schottky diode used should have a leakage well below the maximum drive current of the sourcing device. Diodes with low reverse leakage currents are available from many vendors.

Additional Documentation

Designers must have the following documents to fully use all the features of this device. This data sheet contains pin descriptions, feature overviews, and electrical specifications. Errata sheets contain deviations from published specifications. The user's guides offer detailed information about device features and operation. The following documents can be downloaded from **www.maximintegrated.com/microcontrollers**.

- This MAXQ1004 data sheet, which contains electrical/timing specifications, pin descriptions, and package information.
- The MAXQ1004 revision-specific errata sheet (**www.maximintegrated.com/errata**).
- The *MAXQ1004 User's Guide*, which contains detailed information on core features and operation, including programming.

Development and Technical Support

Maxim and third-party suppliers provide a variety of highly versatile, affordably priced development tools for this microcontroller, including the following:

- Compilers
- In-circuit emulators
- Integrated Development Environments (IDEs)
- Serial-to-JTAG converters for programming and debugging.

A partial list of development tool vendors can be found at **www.maximintegrated.com/MAXQ_tools**.

For technical support, go to **https://support.maximintegrated.com/micro**.

Typical Application Circuit

The 1-Wire interface can be used to authenticate a 3-contact battery pack and also measure the battery voltage and temperature. See Figure 4 for a typical application circuit.

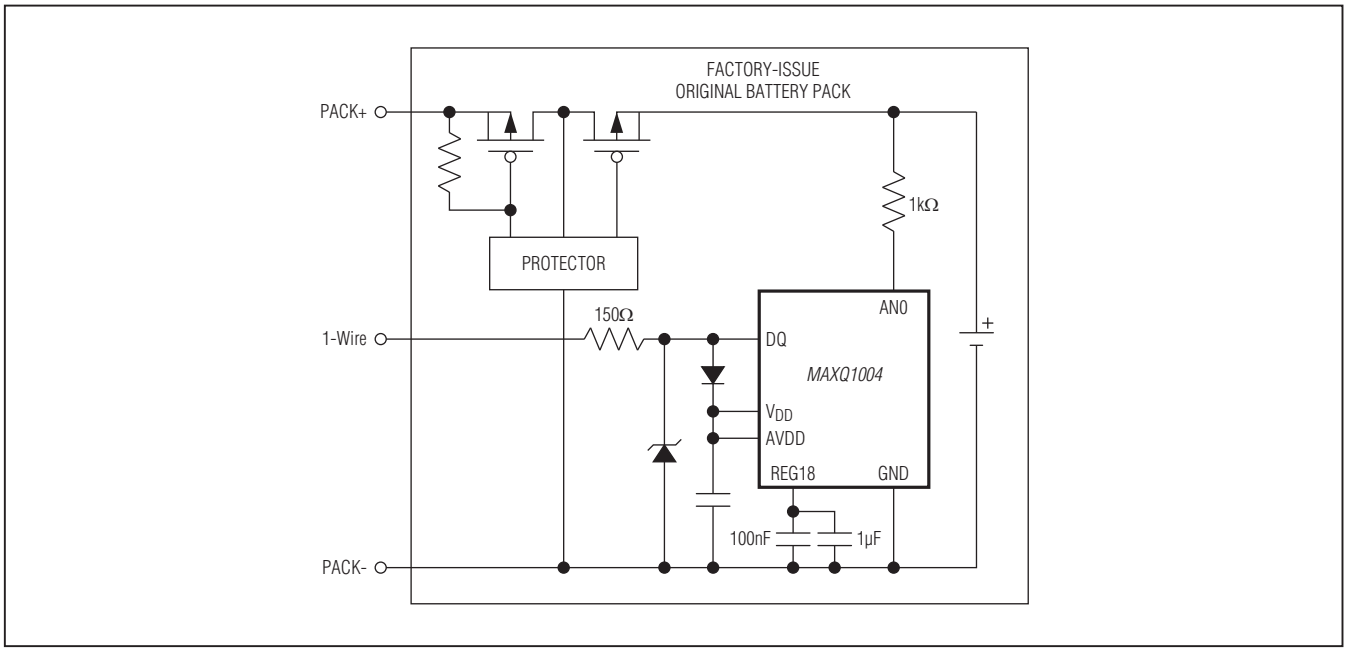


Figure 4. Typical Application Circuit

Package Information

For the latest package outline information and land patterns, go to **www.maximintegrated.com/packages.** Note that a "+", "#", or "-" in the package code indicates RoHS status only. Package drawings may show a different suffix character, but the drawing pertains to the package regardless of RoHS status.

PACKAGE TYPE	PACKAGE CODE	DOCUMENT NO.
16 TQFN-EP	T1644+4	21-0139

Revision History

REVISION NUMBER	REVISION DATE	DESCRIPTION	PAGES CHANGED
0	4/10	Initial release	—
1	1/13	Added DeepCover information	1