Request DS28E16 Security User Guide

EVALUATION KIT AVAILABLE

Click here for production status of specific part numbers.

DS28E16

1-Wire Secure SHA-3 Authenticator

General Description

The DS28E16 secure authenticator combines FIPS202-compliant Secure Hash Algorithm (SHA-3) challenge and response authentication with secured EEPROM.

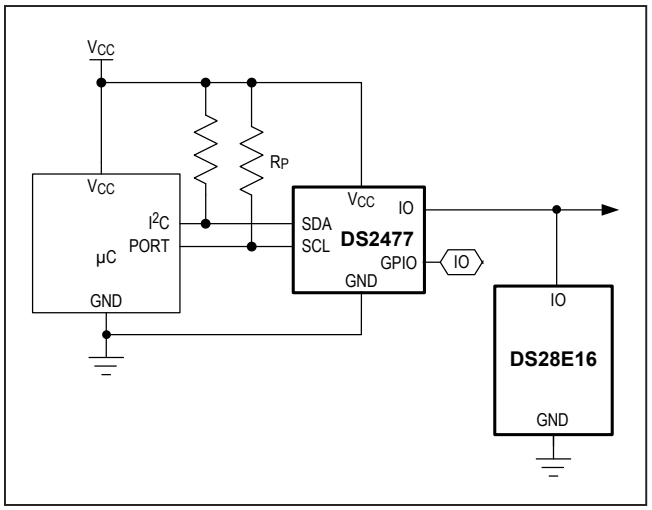
The device provides a core set of cryptographic tools derived from integrated blocks including a SHA-3 engine, 256 bits of secured user EEPROM, a decrement-only counter and a unique 64-bit ROM identification number (ROM ID). The unique ROM ID is used as a fundamental input parameter for cryptographic operations and serves as an electronic serial number within the application. The device communicates over the single-contact 1-Wire® bus. The communication follows the 1-Wire protocol with the ROM ID acting as node address in the case of a multidevice 1-Wire network.

Applications

- Medical Tools/Accessories Authentication and Calibration
- Accessory and Peripheral Secure Authentication
- Battery Authentication and Charge Cycle Tracking

1-Wire is a registered trademark of Maxim Integrated Products, Inc.

Typical Application Circuit



Benefits and Features

- Robust Countermeasures Protect Against Security Attacks
  - All Stored Data Cryptographically Protected from Discovery
- Efficient Secure Hash Algorithm Authenticates Peripherals
  - FIPS 202-Compliant SHA-3 Algorithm for Challenge/Response Authentication
  - FIPS 198-Compliant Keyed-Hash Message Authentication Code (HMAC)
- Supplemental Features Enable Easy Integration into End Applications
  - 17-Bit One-Time Settable, Nonvolatile Decrement-Only Counter with Authenticated Read
  - Secure Storage for Secrets
  - 256 Bits of Secure EEPROM for User Data
  - Unique and Unalterable Factory Programmed 64-Bit Identification Number (ROM ID)
  - Advanced 1-Wire Protocol Minimizes Interface to Single Contact
  - Full-Time Overdrive Communication Speed
  - Internal Parasite Power Capacitor
  - Operating Range: 1.71V–3.63V, -40°C to +85°C
  - WLP, TDFN-EP, and SFN Packages
  - ±8kV HBM ESD Protection (typ)
  - 3.5µA (typ) Input Load Current

***Ordering Information* appears at end of data sheet.**

19-100438; Rev 2; 1/20

maxim integrated™

Absolute Maximum Ratings

Voltage Range on Any Pin Relative to GND .....-0.5V to 4.0V
Maximum Current into Any Pin..... -20mA to 20mA
Operating Temperature Range..... -40°C to +85°C
Junction Temperature.....+150°C
Storage Temperature Range..... -40°C to +125°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.

Package Information

6 WLP

Package Code	Z60E1+1
Outline Number	**21-100327**
Land Pattern Number	Refer to **Application Note 1891**
Thermal Resistance, Four-Layer Board:	
Junction to Ambient (θ_{JA})	95.15°C/W
Junction to Case (θ_{JC})	N/A

6 TDFN-EP

Package Code	T633+2
Outline Number	**21-0137**
Land Pattern Number	**90-0058**
Thermal Resistance, Single-Layer Board:	
Junction to Ambient (θ_{JA})	55°C/W
Junction to Case (θ_{JC})	9°C/W
Thermal Resistance, Four-Layer Board:	
Junction to Ambient (θ_{JA})	42°C/W
Junction to Case (θ_{JC})	9°C/W

2 SFN (3.5mm x 5mm)

Package Code	S23A5N+1
Outline Number	**21-0661**
Land Pattern Number	**90-0398**

2 SFN (3.5mm x 6.5mm)

Package Code	T23A6N+1
Outline Number	**21-0575**
Land Pattern Number	**90-0431**

For the latest package outline information and land patterns (footprints), 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 thermal resistances were obtained using the method described in JEDEC specification JESD51-7, using a four-layer board. For detailed information on package thermal considerations, refer to **www.maximintegrated.com/thermal-tutorial**.

Electrical Characteristics

(Limits are 100% tested at T_A = +25ºC and T_A = +85ºC. Limits over the operating temperature range and relevant supply voltage range are guaranteed by design and characterization. Specifications marked GBD are guaranteed by design and not production tested. Specifications to the minimum operating temperature are guaranteed by design and are not production tested.)

PARAMETER	SYMBOL	CONDITIONS	MIN	TYP	MAX	UNITS
IO PIN: GENERAL DATA						
1-Wire Pullup Voltage	V_{PUP}	System requirement	1.71		3.63	V
1-Wire Pullup Resistance	R_{PUP}	(Note 1)	300		750	Ω
Input Capacitance	C_{IO}	(Notes 1, 2)		1700		pF
Input Load Current	I_L	IO pin at V_{PUP}		3.5	11	µA
High-to-Low Switching Threshold	V_{TL}	(Notes 3, 4)		0.65 x V_{PUP}		V
Input Low Voltage	V_{IL}	(Note 5)			0.18 x V_{PUP}	V
Low-to-High Switching Threshold	V_{TH}	(Notes 3, 6)		0.75 x V_{PUP}		V
Switching Hysteresis	V_{HY}	(Notes 3, 7)		0.3		V
Output Low Voltage	V_{OL}	I_{OL} = 4mA (Note 8)			0.4	V
IO PIN: 1-Wire INTERFACE						
Recovery Time	t_{REC}	(Note 9)	5			µs
Time Slot Duration	t_{SLOT}	(Note 10)	11			µs
IO PIN: 1-Wire RESET, PRESENCE-DETECT CYCLE						
Reset Low Time	t_{RSTL}	System requirement	48		60	µs
Reset High Time	t_{RSTH}	(Note 11)	48			µs
Presence-Detect Sample Time	t_{MSP}	(Note 12)	7		10	µs
IO PIN: 1-Wire WRITE						
Write-Zero Low Time	t_{W0L}	(Note 13)	6		16	µs
Write-One Low Time	t_{W1L}	(Note 13)	0.25		2	µs
IO PIN: 1-Wire READ						
Read Low Time	t_{RL}	(Note 14)	0.25		2 - δ	µs
Read Sample Time	t_{MSR}	(Note 14)	t_{RL} + δ		2	µs
STRONG PULLUP OPERATION						
Strong Pullup Current	I_{SPU}	(Note 15)			3	mA
Strong Pullup Voltage	V_{SPU}	(Note 15)	1.71			V
Read Memory Time	t_{RM}				5	ms
Write Memory Time	t_{WM}				60	ms
Short Write Memory Time	t_{WMS}				15	ms
Computation Time	t_{CMP}				15	ms

Electrical Characteristics (continued)

(Limits are 100% tested at T_A = +25ºC and T_A = +85ºC. Limits over the operating temperature range and relevant supply voltage range are guaranteed by design and characterization. Specifications marked GBD are guaranteed by design and not production tested. Specifications to the minimum operating temperature are guaranteed by design and are not production tested.)

PARAMETER	SYMBOL	CONDITIONS	MIN	TYP	MAX	UNITS
EEPROM						
Write/Erase Cycles (Endurance)	N_{CY}	(Note 16)	100K			
Data Retention	t_{DR}	T_A = +85°C (Note 17)	10			years
POWER-UP						
Power-Up Time	t_{OSCWUP}	System requirement (Note 18)			2	ms

Note 1: System requirement. Maximum allowable pullup resistance is a function of the number of 1-Wire devices in the system and 1-Wire recovery times. The specified value here applies to systems with only one device and with the minimum 1-Wire recovery times.

Note 2: Value represents the typical parasite capacitance when V_{PUP} is first applied. Once the parasite capacitance is charged, it does not affect normal communication.

Note 3: V_{TL}, V_{TH}, and V_{HY} are a function of the internal supply voltage, which is a function of V_{PUP}, R_{PUP}, 1-Wire timing, and capacitive loading on IO. Lower V_{PUP}, higher R_{PUP}, shorter t_{REC}, and heavier capacitive loading all lead to lower values of V_{TL}, V_{TH}, and V_{HY}.

Note 4: Voltage below which, during a falling edge on IO, a logic-zero is detected.

Note 5: The voltage on IO must be less than or equal to V_{ILMAX} at all times the master is driving IO to a logic-zero level.

Note 6: Voltage above which, during a rising edge on IO, a logic-one is detected.

Note 7: After V_{TH} is crossed during a rising edge on IO, the voltage on IO must drop by at least V_{HY} to be detected as logic-zero.

Note 8: The I-V characteristic is linear for voltages less than 1V.

Note 9: System requirement. Applies to a single device attached to a 1-Wire line.

Note 10: Defines maximum possible bit rate. Equal to $1/(t_{W0LMIN} + t_{RECMIN})$.

Note 11: An additional reset or communication sequence cannot begin until the reset high time has expired.

Note 12: System requirement. Interval after t_{RSTL} during which a bus master can read a logic 0 on IO if there is a device present. The power-up presence detect pulse can be outside this interval, but completes within 2ms after power-up.

Note 13: System requirement. ε in Figure 4 represents the time required for the pullup circuitry to pull the voltage on IO up from V_{IL} to V_{TH}. The actual maximum duration for the master to pull the line low is $t_{W1LMAX} + t_F - \varepsilon$ and $t_{W0LMAX} + t_F - \varepsilon$, respectively.

Note 14: System requirement. δ in Figure 4 represents the time required for the pullup circuitry to pull the voltage on IO up from V_{IL} to the input-high threshold of the bus master. The actual maximum duration for the master to pull the line low is $t_{RLMAX} + t_F$.

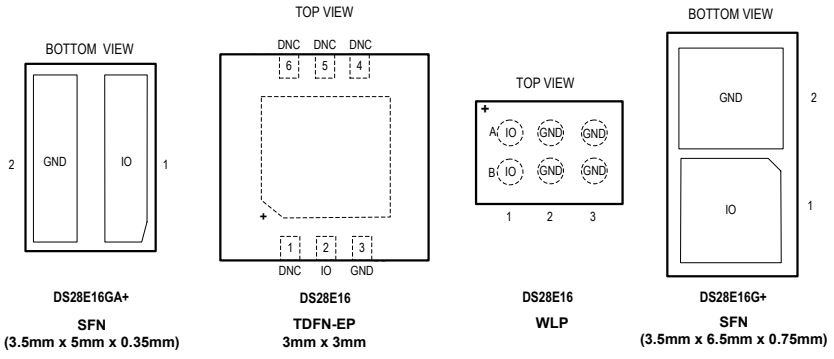
Note 15: Current drawn from IO during a SPU operation interval. The pullup circuit on IO during the SPU operation interval should be such that the voltage at IO is greater than or equal to V_{SPUMIN}. A low-impedance bypass of R_{PUP} activated during the SPU operation is the recommended way to meet this requirement.

Note 16: Write-cycle endurance is tested in compliance with JESD47H.

Note 17: Data retention is tested in compliance with JESD47H.

Note 18: 1-Wire communication should not take place for at least t_{OSCWUP} after V_{PUP} reaches V_{PUP} min.

Pin Configuration

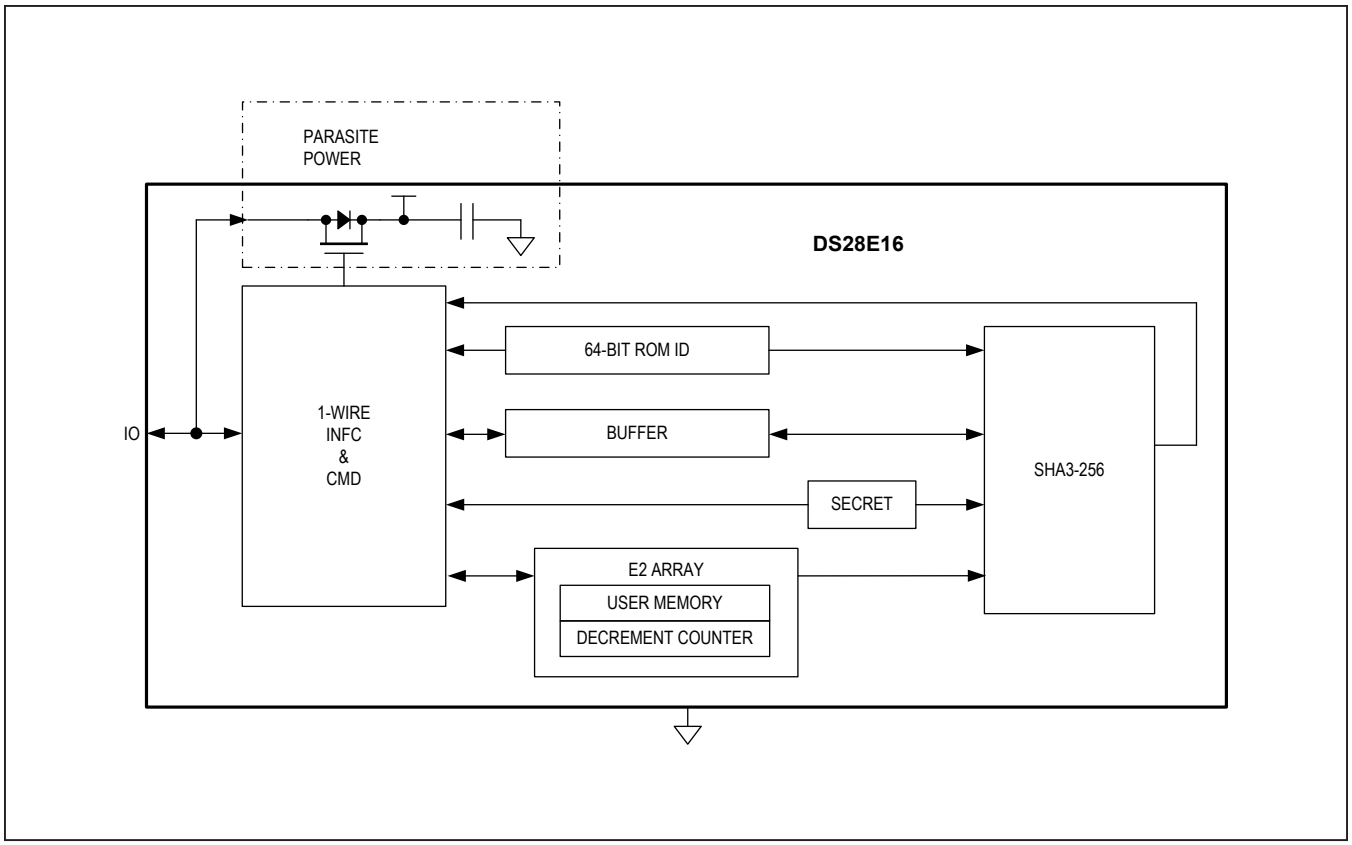


NOTE: THE SFN PACKAGE IS QUALIFIED FOR ELECTRO-MECHANICAL CONTACT USE CASES ONLY. NOT FOR SOLDERING.

Pin Description

PIN			NAME	FUNCTION
TDFN	WLP	SFN		
1, 4, 5, 6	—	—	DNC	Do Not Connect
2	A1, B1	1	IO	1-Wire IO
3	A2, A3, B2, B3	2	GND	Ground Reference. Connect all contacts to GND.
—	—	—	EP	Exposed Pad (TDFN Only). Solder evenly to the board's ground plane for proper operation. Refer to *Application Note 3273: Exposed Pads: A Brief Introduction for additional information*

Functional Diagram



Detailed Description

The DS28E16 integrates the Maxim DeepCover® capability to protect all device stored data from invasive discovery. In addition to the SHA-3 engine for signatures, 256-bit EEPROM for user memory, SHA-3 secret storage, 17-bit decrement counter, and control registers. The device operates from a 1-Wire interface with a parasitic supply by way of an internal capacitor.

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

Design Resource Overview

Operation of the DS28E16 involves use of device EEPROM and execution of device function commands. The following section provides an overview including the decrement counter. Refer to the *DS28E16 Security User Guide* for details.

Memory

A secured EEPROM array provides SHA-3 secret storage, along with a decrement counter, and/or general-purpose, user-programmable memory. Depending on the memory space, there are either default or user-programmable options to set protection modes.

Function Commands

After a 1-Wire reset/presence cycle and ROM function command sequence is successful, a command start can be accepted and then followed by a device function command. In general, these commands follow Figure 1. Within this diagram, the data transfer is verified when writing and reading by a 16-bit CRC (CRC-16). The CRC-16 is computed as described in Maxim's *Application Note 27*: Understanding and Using Cyclic Redundancy Checks with Maxim 1-Wire and iButton Products..

Decrement Counter

The optional 17-bit decrement counter can be written one time on a page of memory. A dedicated device function command is used to decrement the count value by one with each call. Once the count value reaches a value of 0, no additional decrements are possible.

1-Wire Bus System

The 1-Wire bus is a system that has a single bus master and one or more slaves. In all instances, the DS28E16 is a slave device. The bus master is typically a microcontroller or a coprocessor like the DS2477. 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 that are initiated on the falling edge of sync pulses from the bus master.

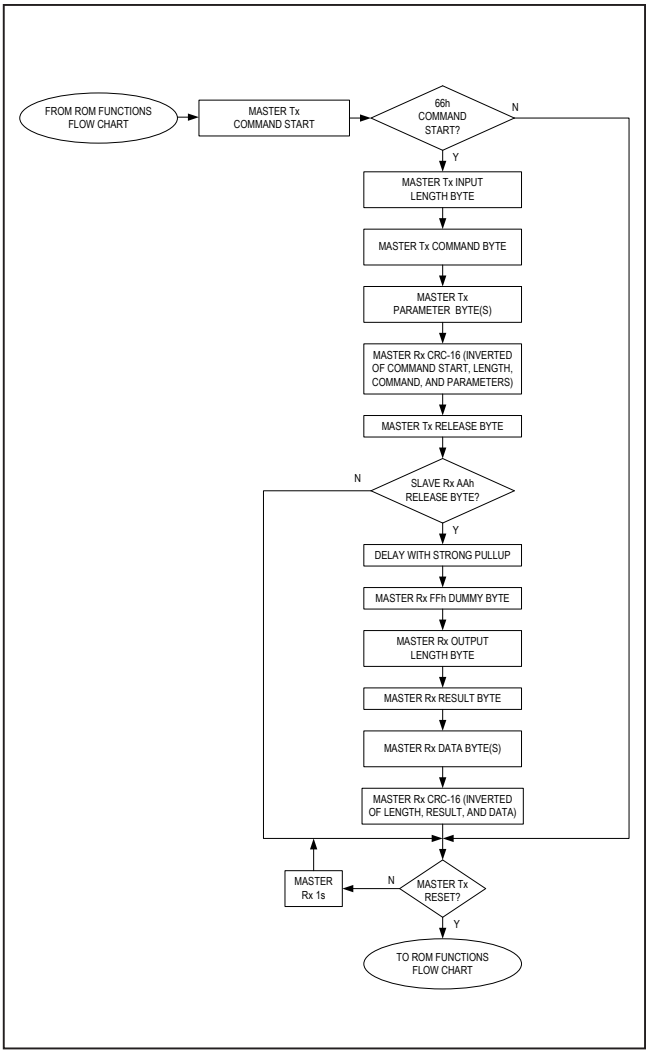


Figure 1. Device Function Flow Chart

Hardware Configuration

The 1-Wire bus has only a single line by definition; it is important that each device on the bus can drive it at the appropriate time. To facilitate this, each device attached to the 1-Wire bus must have open-drain or three-state outputs. The 1-Wire port of the DS28E16 is open drain with an internal circuit equivalent.

A multidrop bus consists of a 1-Wire bus with multiple slaves attached. The DS28E16 supports overdrive communication speed of 90.9kbps (max). The value of the pullup resistor primarily depends on the network size and load conditions. The DS28E16 requires a pullup resistor of 750Ω (max).

The idle state for the 1-Wire bus is high. If for any reason a transaction needs to be suspended, the bus must be left in the idle state if the transaction is to resume. If this does not occur and the bus is left low for more than 16µs one or more devices on the bus could be reset.

Transaction Sequence

The protocol for accessing the DS28E16 through the 1-Wire port is as follows:

- Initialization
- ROM Function command
- Device Function command
- Transaction/data

Initialization

All transactions on the 1-Wire bus begin with an initialization sequence. The initialization sequence consists of a reset pulse transmitted by the bus master followed by presence pulse(s) transmitted by the slave(s). The presence pulse lets the bus master know that the DS28E16 is on the bus and is ready to operate. For more details, see the *1-Wire Signaling and Timing* section.

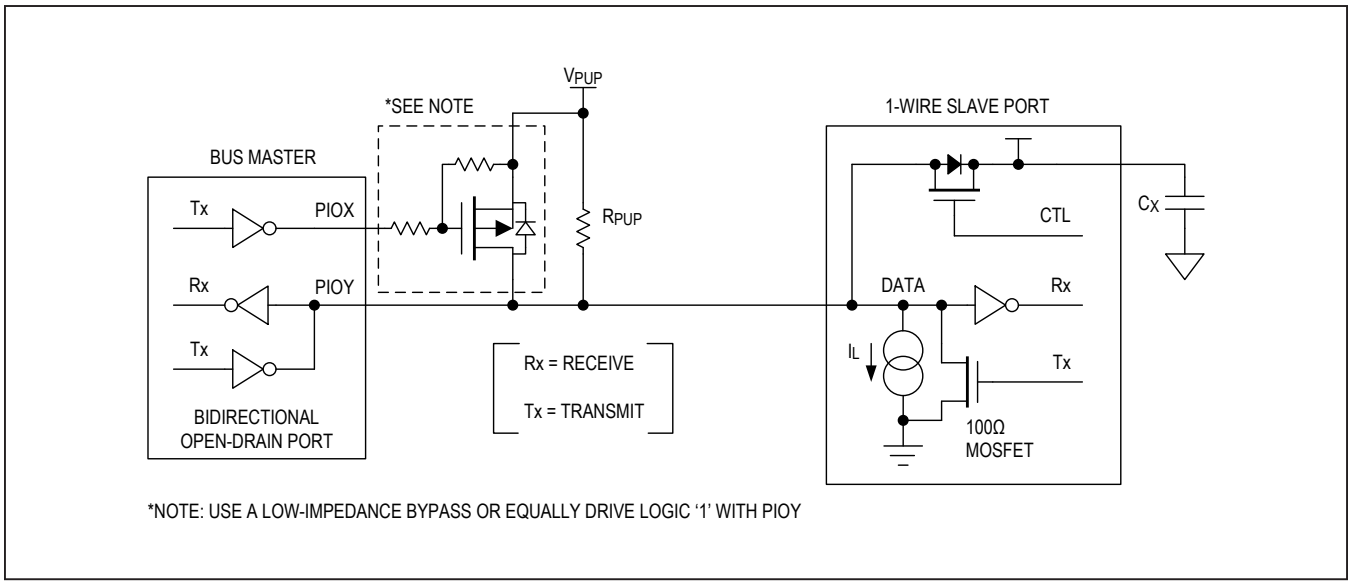


Figure 2. Hardware Configuration

1-Wire Signaling and Timing

The DS28E16 requires strict protocols to ensure data integrity. The protocol consists of four types of signaling on one line: reset sequence with reset pulse and presence pulse, write-zero, write-one, and read-data. Except for the presence pulse, the bus master initiates all falling edges.

To get from idle to active, the voltage on the 1-Wire line needs to fall from V_{PUP} below the threshold V_{TL}. To get from active to idle, the voltage needs to rise from V_{ILMAX} past the threshold V_{TH}. The time it takes for the voltage to make this rise is seen in Figure 3 as ε, and its duration depends on the pullup resistor (R_{PUP}) used and the capacitance of the 1-Wire network attached. The voltage V_{ILMAX} is relevant for the DS28E16 when determining a logical level, not triggering any events.

Figure 3 shows the initialization sequence required to begin any communication with the DS28E16. A reset pulse followed by a presence pulse indicates that the DS28E16 is ready to receive data, given the correct ROM and device function command. If the bus master uses slew-rate control on the falling edge, it must pull down the line for $t_{RSTL} + t_F$ to compensate for the edge.

After the bus master has released the line, it goes into receive mode. Now, the 1-Wire bus is pulled to V_{PUP} through the pullup resistor or, in the case of a special driver chip, through the active circuitry. When the threshold V_{TH} is crossed, the DS28E16 waits and then transmits a presence pulse by pulling the line low. To detect a presence pulse, the master must test the logical state of the 1-Wire line at t_{MSP}.

Immediately after t_{RSTH} has expired, the DS28E16 is ready for data communication.

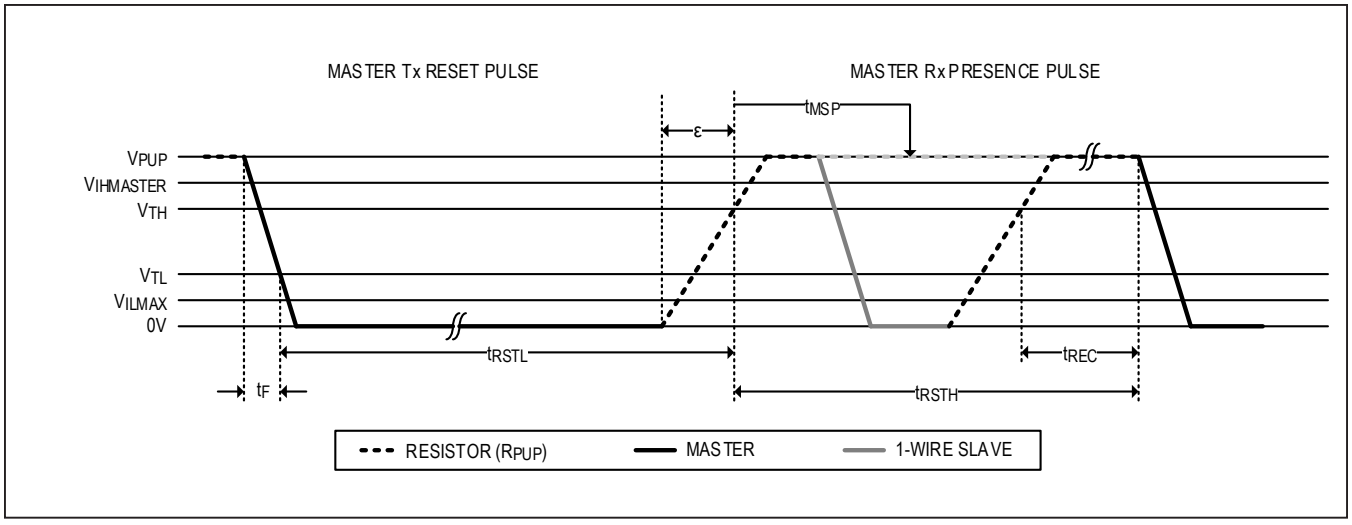


Figure 3. Initialization Procedure: Reset and Presence Pulse

Read/Write Time Slots

Data communication with the DS28E16 takes place in time slots that carry a single bit each. Write time slots transport data from bus master to slave. Read time slots transfer data from slave to master. Figure 4 illustrates the definitions of the write and read time slots.

All communication begins with the master pulling the data line low. As the voltage on the 1-Wire line falls below the threshold V_{TL}, the DS28E16 starts its internal timing generator that determines when the data line is sampled during a write time slot and how long data is valid during a read time slot.

Master to Slave

For a write-one time slot, the voltage on the data line must have crossed the V_{TH} threshold before the write-one low time t_{W1LMAX} is expired. For a write-zero time slot, the voltage on the data line must stay below the V_{TH} threshold until the write-zero low time t_{W0LMIN} is expired. For the most reliable communication, the voltage on the data line should not exceed V_{ILMAX} during the entire t_{W0L} or t_{W1L} window. After the V_{TH} threshold has been crossed, the DS28E16 needs a recovery time t_{REC} before it is ready for the next time slot.

Slave to Master

A read-data time slot begins like a write-one time slot. The voltage on the data line must remain below V_{TL} until the read low time t_{RL} is expired. During the t_{RL} window, when responding with a 0, the DS28E16 starts pulling the data line low; its internal timing generator determines when this pulldown ends and the voltage starts rising again. When responding with a 1, the DS28E16 does not hold the data line low at all, and the voltage starts rising as soon as t_{RL} is over.

The sum of t_{RL} + δ (rise time) on one side and the internal timing generator of the DS28E16 on the other side define the master sampling window (t_{MSRMIN} to t_{MSRMAX}), in which the master must perform a read from the data line. For the most reliable communication, t_{RL} should be as short as permissible, and the master should read close to, but no later than t_{MSRMAX}. After reading from the data line, the master must wait until t_{SLOT} is expired. This guarantees sufficient recovery time t_{REC} for the DS28E16 to get ready for the next time slot. Note that t_{REC} specified herein applies only to a single DS28E16 attached to a 1-Wire line. For multidevice configurations, t_{REC} must be extended to accommodate the additional 1-Wire device input capacitance. Alternatively, an interface that performs active pullup during the 1-Wire recovery time such as the special 1-Wire line drivers can be used.

1-Wire ROM Commands

Once the bus master has detected a presence, it can issue one of the five ROM function commands that the DS28E16 supports. All ROM function commands are 8 bits long. For operational details, see Figure 5. A descriptive list of these ROM function commands follows in the subsequent sections and the commands are summarized in Table 1.

Table 1. 1-Wire ROM Commands Summary

ROM FUNCTION COMMAND	CODE	DESCRIPTION
Search ROM	F0h	Search for a device
Read ROM	33h	Read ROM from device (single drop)
Match ROM	55h	Select a device by ROM number
Skip ROM	CCh	Select only device on 1-Wire
Resume	A5h	Selected device with RC bit set

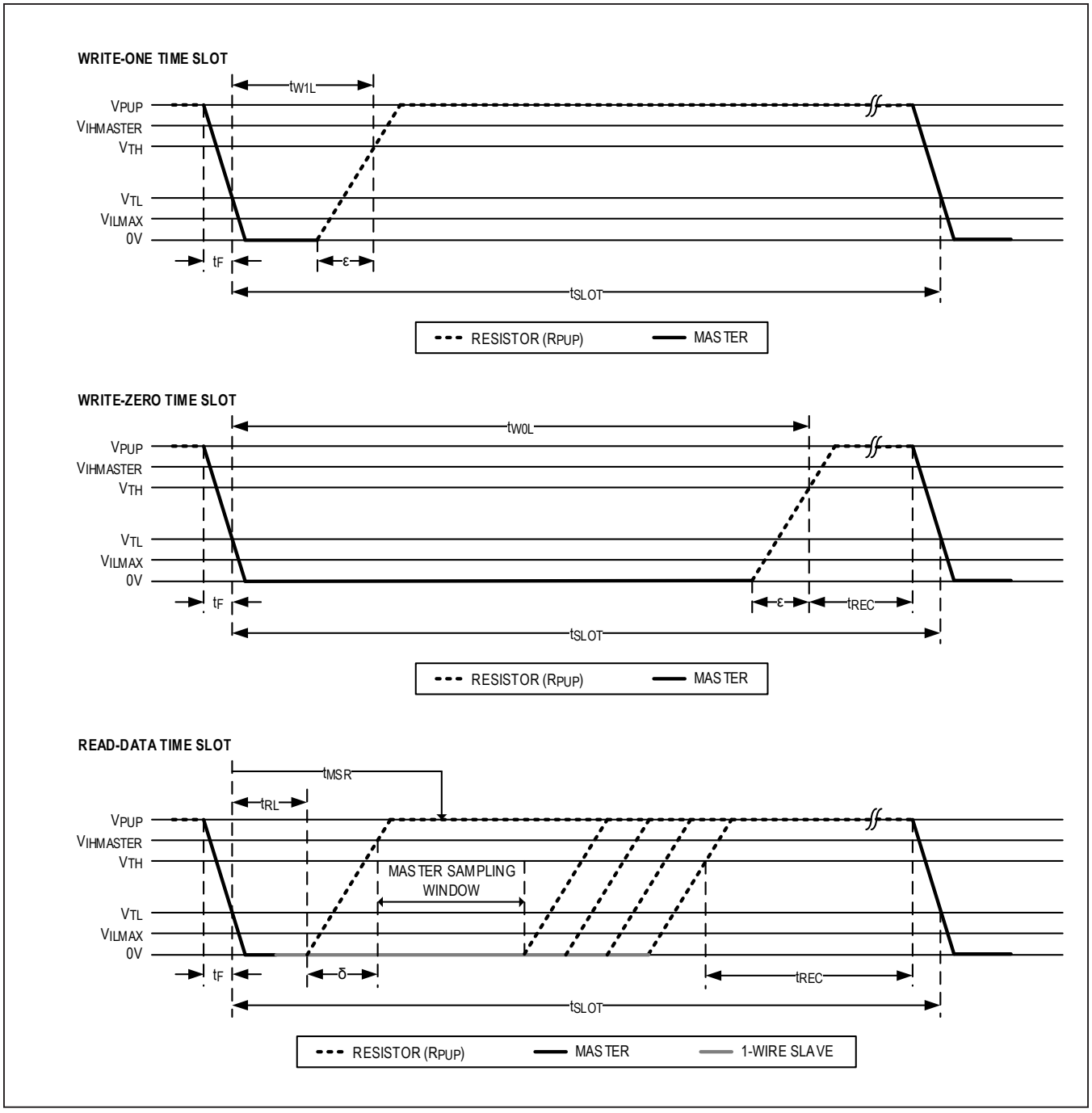


Figure 4. Read/Write Timing Diagrams

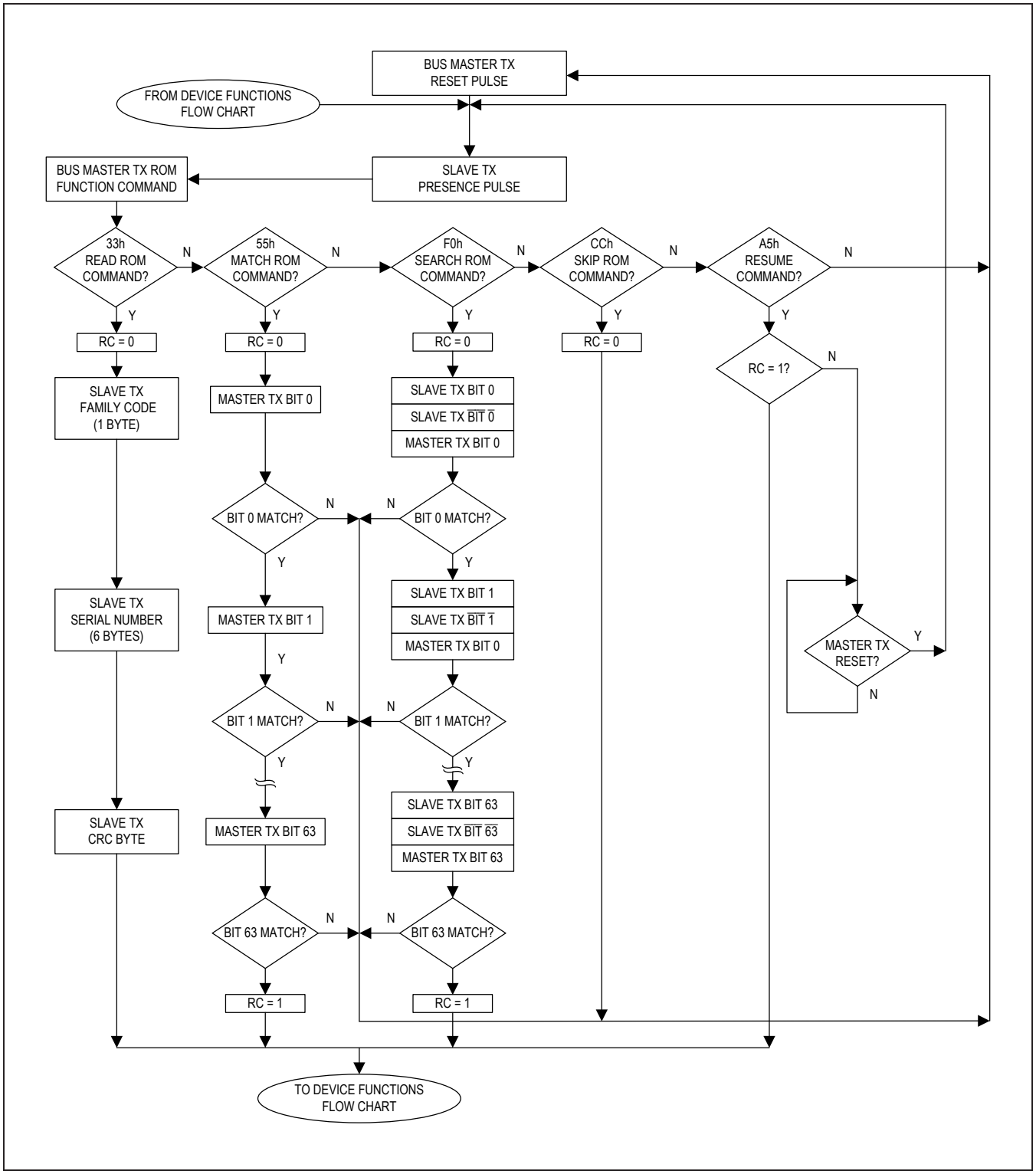


Figure 5. ROM Function Flow

Search ROM[F0h]

When a system is initially brought up, the bus master might not know the number of devices on the 1-Wire bus or their ROM ID numbers. By taking advantage of the wired-AND property of the bus, the master can use a process of elimination to identify the ID of all slave devices. For each bit in the ID number, starting with the least significant bit, the bus master issues a triplet of time slots. On the first slot, each slave device participating in the search outputs the true value of its ID number bit. On the second slot, each slave device participating in the search outputs the complemented value of its ID number bit. On the third slot, the master writes the true value of the bit to be selected. All slave devices that do not match the bit written by the master stop participating in the search. If both of the read bits are zero, the master knows that slave devices exist with both states of the bit. By choosing which state to write, the bus master branches in the search tree. After one complete pass, the bus master knows the ROM ID number of a single device. Additional passes identify the ID numbers of the remaining devices. Refer to *Application Note 187*: 1-Wire Search Algorithm for a detailed discussion, including an example.

Read ROM[33h]

The Read ROM command allows the bus master to read the DS28E16's 8-bit family code, unique 48-bit serial number, and 8-bit CRC. This command can only be used if there is a single slave on the bus. If more than one slave is present on the bus, a data collision occurs when all slaves try to transmit at the same time (open drain produces a wired-AND result). The resultant family code and 48-bit serial number result in a mismatch of the CRC.

Match ROM[55h]

The Match ROM command, followed by a 64-bit ROM sequence, allows the bus master to address a specific DS28E16 on a multidrop bus. Only the DS28E16 that exactly matches the 64-bit ROM sequence responds to the subsequent device function command. All other slaves wait for a reset pulse. This command can be used with a single device or multiple devices on the bus.

Skip ROM [CCh]

This command can save time in a single-drop bus system by allowing the bus master to access the device functions without providing the 64-bit ROM ID. If more than one slave is present on the bus and, for example, a read command is issued following the Skip ROM command, data collision occurs on the bus as multiple slaves transmit simultaneously (open-drain pulldowns produce a wired-AND result).

Resume [A5h]

To maximize the data throughput in a multidrop environment, the Resume command is available. This command checks the status of the RC bit and, if it is set, directly transfers control to the device function commands, similar to a Skip ROM command. The only way to set the RC bit is through successfully executing the Match ROM or Search ROM command. Once the RC bit is set, the device can repeatedly be accessed through the Resume command. Accessing another device on the bus clears the RC bit, preventing two or more devices from simultaneously responding to the Resume command.

Improved Network Behavior (Switch-Point Hysteresis)

In a 1-Wire environment, line termination is possible only during transients controlled by the bus master (1-Wire driver). 1-Wire networks, therefore, are susceptible to noise of various origins. Depending on the physical size and topology of the network, reflections from end points and branch points can add up or cancel each other to some extent. Such reflections are visible as glitches or ringing on the 1-Wire communication line. Noise coupled onto the 1-Wire line from external sources can also result in signal glitching. A glitch during the rising edge of a time slot can cause a slave device to lose synchronization with the master and, consequently, result in a Search ROM command coming to a dead end or cause a device-specific function command to abort. For better performance in network applications, the DS28E16 uses a 1-Wire front end with a hysteresis at the low-to-high switching threshold V_{TH}. If a negative glitch crosses V_{TH}, but does not go below V_{TH} - V_{HY}, it is not recognized (Figure 6).

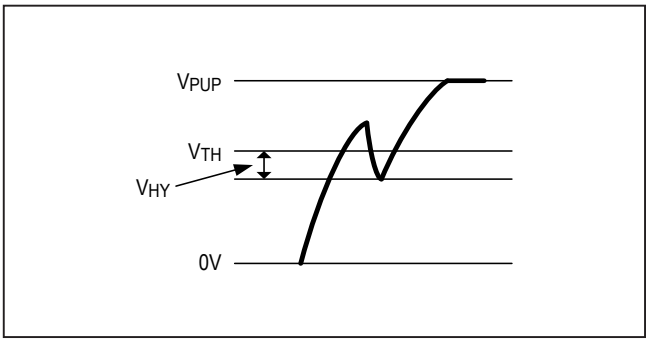


Figure 6. Noise Suppression Scheme

Ordering Information

PART	TEMP RANGE	PIN-PACKAGE
DS28E16X-S+T	-40°C to +85°C	6 WLP (2.5k pcs)
DS28E16Q+T	-40°C to +85°C	6 TDFN-EP (2.5k pcs)
DS28E16G+T	-40°C to +85°C	2 SFN (3.5mm x 6.5mm) (2.5k pcs)
DS28E16GA+T	-40°C to +85°C	2 SFN (3.5mm x 5mm) (2.5k pcs)

+Denotes a lead(Pb)-free/RoHS-compliant package.

T = Tape and reel.

EP = Exposed pad.

Revision History

REVISION NUMBER	REVISION DATE	DESCRIPTION	PAGES CHANGED
0	11/18	Initial release	—
1	3/19	Updated *Benefits and Features* section	1
2	1/20	Updated *Benefits and Features*, *Package Information*, *Pin Configuration*, *Pin Description*, and *Ordering Information*	1, 2, 5, 14

For pricing, delivery, and ordering information, please visit Maxim Integrated's online storefront at https://www.maximintegrated.com/en/storefront/storefront.html.

Maxim Integrated cannot assume responsibility for use of any circuitry other than circuitry entirely embodied in a Maxim Integrated product. No circuit patent licenses are implied. Maxim Integrated reserves the right to change the circuitry and specifications without notice at any time. The parametric values (min and max limits) shown in the Electrical Characteristics table are guaranteed. Other parametric values quoted in this data sheet are provided for guidance.

