219-0009; Rev 2; 4/11

EVALUATION KIT AVAILABLE

1-Wire SHA-1 Authenticator

DS28E10

General Description

The DS28E10 combines secure challenge-and-response authentication functionality based on the FIPS 180-3 specified Secure Hash Algorithm (SHA-1) with 224 bits of one-time programmable user EPROM in a single chip. Once written, the memory is automatically write protected. Additionally, each device has its own guaranteed unique 64-bit ROM identification number (ROM ID) that is factory programmed into the chip. Memory writes are performed 4 bytes at a time. A secure and low-cost factory programming service is available to preprogram device data, including the SHA-1 security data components. The device communicates over the single-contact 1-Wire® bus. The communication follows the standard 1-Wire protocol with the ROM ID acting as node address in the case of a multidevice 1-Wire network.

Applications

Reference Design License Management

System Intellectual Property Protection

Sensor/Accessory Authentication and Calibration

Ordering Information

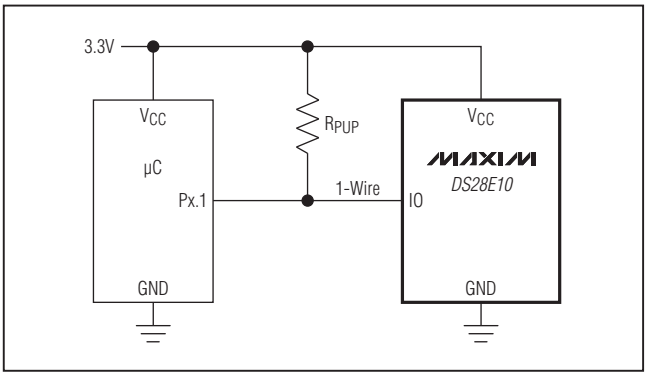
PART	TEMP RANGE	PIN-PACKAGE
DS28E10R+T	-40°C to +85°C	3 SOT23
DS28E10P+	-40°C to +85°C	6 TSOC
DS28E10P+T	-40°C to +85°C	6 TSOC

+Denotes a lead(Pb)-free/RoHS-compliant package.
T = Tape and reel.

Features

- **Dedicated Hardware-Accelerated SHA-1 Engine for Generating SHA-1 MACs**
- **One Page of 28 Bytes User OTP EPROM**
- **Irreversible Write Protection**
- **Unique, Factory-Programmed 64-Bit Identification Number**
- **1-Wire Interface for Standard and Overdrive Speed**
- **Communicates with Host at Up to 15.4kbps at Standard Speed or Up to 125kbps in Overdrive Mode**
- **Operating Range from 2.8V to 3.6V, -40°C to +85°C**
- **3-Lead SOT23, 6-Lead TSOC Package**
- **±6kV Human Body Model (HBM) ESD Protection (typ) on 1-Wire and V_{CC} Pin**

Typical Operating Circuit



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

1-Wire SHA-1 Authenticator

ABSOLUTE MAXIMUM RATINGS

IO Voltage to GND .....-0.5V, +7V
IO Sink Current.....20mA
V_{CC} Voltage to GND .....-0.5V, +7V
Operating Temperature Range..... -40°C to +85°C
Junction Temperature .....+150°C
Storage Temperature Range..... -55°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.

ELECTRICAL CHARACTERISTICS

(T_A = -40°C to +85°C, see Note 1.)

PARAMETER	SYMBOL	CONDITIONS	MIN	TYP	MAX	UNITS
V_{CC} PIN						
Supply Voltage	V_{CC}	During nonprogramming state (Note 2)	2.8		3.6	V
Standby Current	I_{CCS}	V_{CC} = 3.6V	0.5		4.0	µA
Operating Current	I_{CCO}	V_{CC} = 3.6V, reading (Note 3)			30	µA
IO PIN: GENERAL DATA						
1-Wire Pullup Voltage	V_{PUP}	(Note 4)	2.8		3.6	V
1-Wire Pullup Resistance	R_{PUP}	(Notes 4, 5)	0.3		2.2	kΩ
Input Capacitance	C_{IO}	(Note 3)		50		pF
Input Load Current	I_L	(IO pin at V_{PUP}) (Note 3)			2	µA
Input Low Voltage	V_{IL}	(Notes 4, 6, 7)			0.3 x V_{CC}	V
Input High Voltage	V_{IH}	(Notes 3, 8)	0.7 x V_{CC}			V
Switching Hysteresis	V_{HY}	(Notes 3, 9)	0.05 x V_{CC}			V
Output Low Voltage	V_{OL}	At 4mA load (Note 10)			0.3	V
Recovery Time (Notes 4, 11)	t_{REC}	Standard speed, R_{PUP} = 2.2kΩ	5			µs
		Overdrive speed, R_{PUP} = 2.2kΩ	2			
Rising-Edge Hold-Off Time (Notes 3, 12)	t_{REH}	Standard speed	0.5		5	µs
		Overdrive speed	Not applicable (0)			
Timeslot Duration (Notes 4, 13)	t_{SLOT}	Standard speed	65			µs
		Overdrive speed	8			
IO PIN: 1-Wire RESET, PRESENCE DETECT CYCLE						
Reset Low Time (Note 4)	t_{RSTL}	Standard speed	480		640	µs
		Overdrive speed	48		80	
Presence-Detect High Time	t_{PDH}	Standard speed	15		60	µs
		Overdrive speed	2		6	
Presence-Detect Low Time	t_{PDL}	Standard speed	60		240	µs
		Overdrive speed	8		24	
Presence-Detect Sample Time (Notes 4, 14)	t_{MSP}	Standard speed	60		75	µs
		Overdrive speed	6		10	
IO PIN: 1-Wire WRITE						
Write-Zero Low Time (Notes 4, 15)	t_{W0L}	Standard speed	60		120	µs
		Overdrive Speed	6		16	
Write-One Low Time (Notes 4, 15)	t_{W1L}	Standard speed	1		15	µs
		Overdrive speed	1		2	

ELECTRICAL CHARACTERISTICS (continued)

(T_A = -40°C to +85°C, see Note 1.)

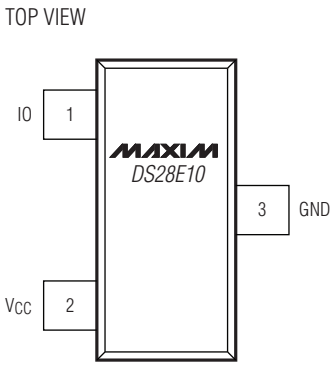
PARAMETER	SYMBOL	CONDITIONS	MIN	TYP	MAX	UNITS
IO PIN: 1-Wire READ						
Read Low Time (Notes 4, 16)	t_{RL}	Standard speed	5		15 - δ	µs
		Overdrive speed	1		2 - δ	
Read Sample Time (Notes 4, 16)	t_{MSR}	Standard speed	t_{RL} + δ		15	µs
		Overdrive speed	t_{RL} + δ		2	
EPROM						
Programming Current	I_{PROG}	$V_{PP} = V_{PP(MAX)}$ (Note 3)	**Refer to the full data sheet.**			mA
Programming Time	t_{PP}					ms
Programming Voltage	V_{PP}	(Note 2)				V
Data Retention	t_{DR}	At +85°C (Notes 17, 18)	10			Years
SHA-1 Engine						
SHA-1 Computation Current	I_{CCSHA}	V_{CC} = 3.6V	**Refer to the full data sheet.**			mA
SHA-1 Computation Time	t_{CSHA}	(Note 19)				ms

Note 1: Specifications at T_A = -40°C are guaranteed by design only and not production tested.
Note 2: **Refer to the full data sheet for this note.**

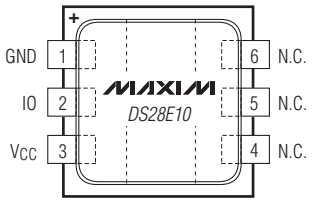
Note 3: Guaranteed by design, characterization, and/or simulation only. Not production tested.
Note 4: System requirement.
Note 5: Maximum allowable pullup resistance is a function of the number of 1-Wire devices in the system and 1-Wire recovery times. The specified value here applies to systems with only one device and with the minimum 1-Wire recovery times. For more heavily loaded systems, an active pullup such as that found in the DS2482-x00 might be required.
Note 6: Voltage below which, during a falling edge on IO, a logic 0 is detected.
Note 7: The voltage on IO needs to be less than or equal to V_{ILMAX} at all times while the master is driving IO to a logic 0 level.
Note 8: Voltage above which, during a rising edge on IO, a logic 1 is detected.
Note 9: After V_{IH} is crossed during a rising edge on IO, the voltage on IO has to drop by at least V_{HY} to be detected as logic 0.
Note 10: The I-V characteristic is linear for voltages less than 1V.
Note 11: Applies to a single DS28E10 attached to a 1-Wire line.
Note 12: The earliest recognition of a negative edge is possible at t_{REH} after V_{IH} has been reached on the preceding rising edge.
Note 13: Defines maximum possible bit rate. Equal to $1/(t_{W0LMIN} + t_{RECMIN})$.
Note 14: Interval after t_{RSTL} during which a bus master is guaranteed to sample a logic 0 on IO if there is a DS28E10 present. Minimum limit is t_{PDHMAX}; maximum limit is $t_{PDHMIN} + t_{PDLMIN}$.
Note 15: ε in Figure 10 represents the time required for the pullup circuitry to pull the voltage on IO up from V_{IL} to V_{IH}. The actual maximum duration for the master to pull the line low is $t_{W1LMAX} + t_F$ - ε and $t_{W0LMAX} + t_F$ - ε, respectively.
Note 16: δ in Figure 10 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 17: Data retention is degraded as T_A increases.
Note 18: Guaranteed by 100% production test at elevated temperature for a shorter time; equivalence of this production test to data sheet limit at operating temperature range is established by reliability testing.
Note 19: **Refer to the full data sheet for this note.**

1-Wire SHA-1 Authenticator

Pin Configurations



SOT23-3



TSOC

Pin Description

PIN		NAME	FUNCTION
SOT23	TSOC		
1	2	IO	1-Wire Bus Interface. Open drain; requires external pullup resistor.
2	3	V_{CC}	Supply Pin for Operating Power
3	1	GND	Ground Supply for the Device
—	4, 5, 6	N.C.	Not Connected

Detailed Description

The DS28E10 combines a 512-bit SHA-1 engine, security data, 224 bits of one-time programmable (OTP) EPROM, and a 64-bit ROM ID in a single chip. Data is transferred serially through the 1-Wire protocol, which requires only a single data lead and a ground return. In addition to its important use as a unique data value in cryptographic SHA-1 computations, the device's 64-bit ROM ID can be used to electronically identify the equipment in which the DS28E10 is used. The ROM ID also serves as node address in a multidrop 1-Wire network environment where multiple devices reside on a common 1-Wire bus and operate independently of each other.

Overview

The block diagram in Figure 1 shows the relationships between the major control and memory sections of the device. The device has six main data components: 64-bit ROM ID, security data, challenge buffer, 28 bytes of OTP user EPROM memory, special function registers, and a 512-bit SHA-1 engine. Figure 2 shows the hierarchical structure of the 1-Wire protocol. The bus master must first provide one of the seven ROM (network) function commands: 1) Read ROM, 2) Match ROM, 3) Search ROM, 4) Skip ROM, 5) Resume (communication), 6) Overdrive-Skip ROM or 7) Overdrive-Match ROM. Upon completion of an Overdrive-Skip ROM or Overdrive-Match ROM command executed at standard speed, the device enters overdrive mode where all subsequent communication occurs at a higher speed. The protocol required for these ROM function commands is described in Figure 8. After a ROM function command is successfully executed, the memory and SHA-1 functions become accessible and the master can provide any one of the six available function commands. The protocol for these commands is described in Figure 6. **All data is read and written least significant bit first.**

1-Wire SHA-1 Authenticator

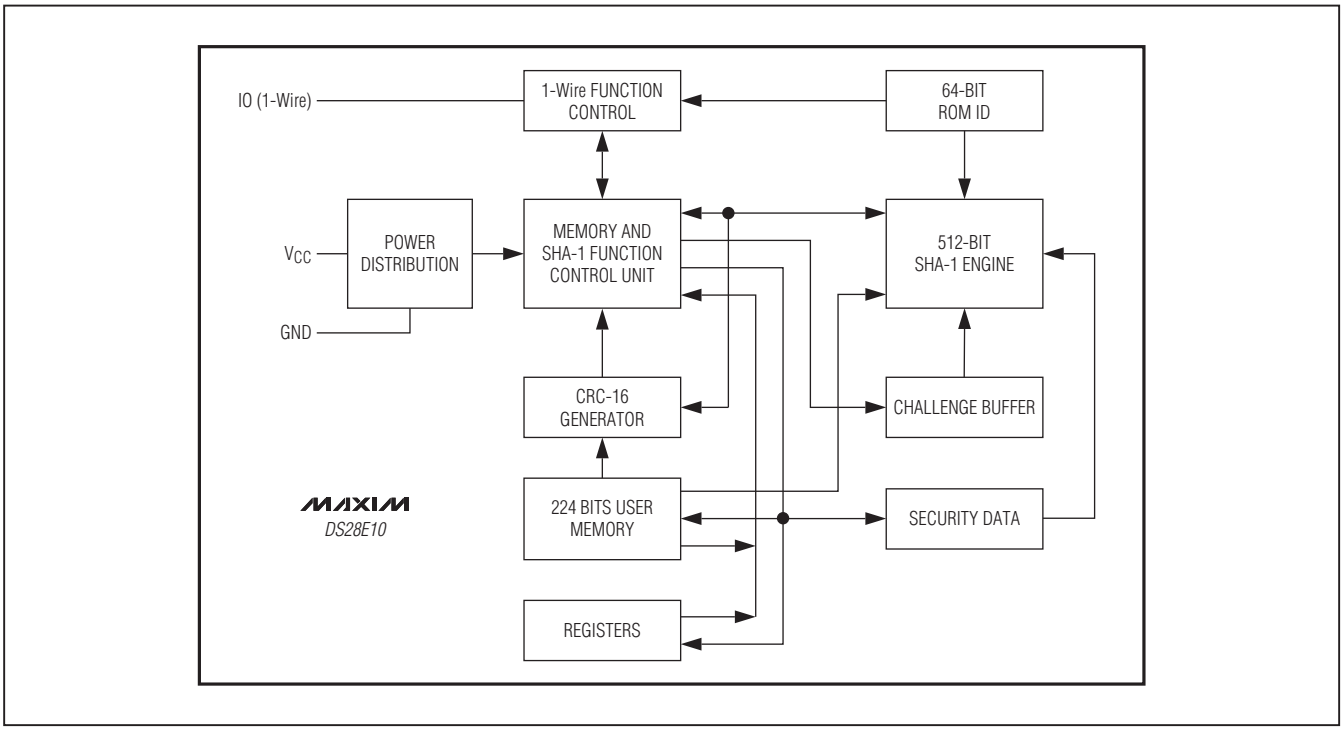


Figure 1. Block Diagram

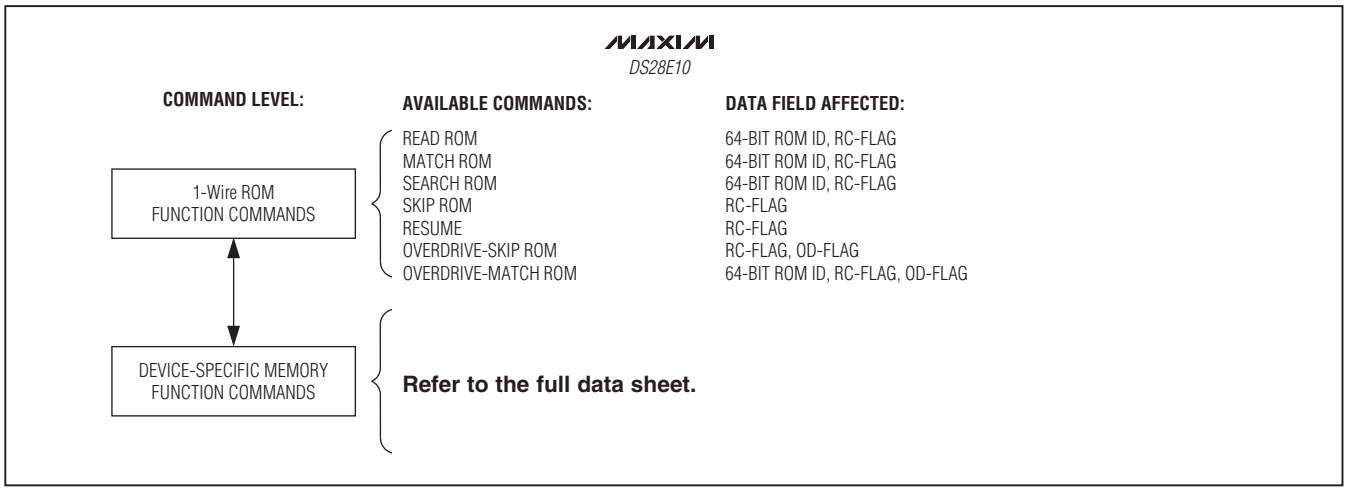


Figure 2. Hierarchical Structure for 1-Wire Protocol

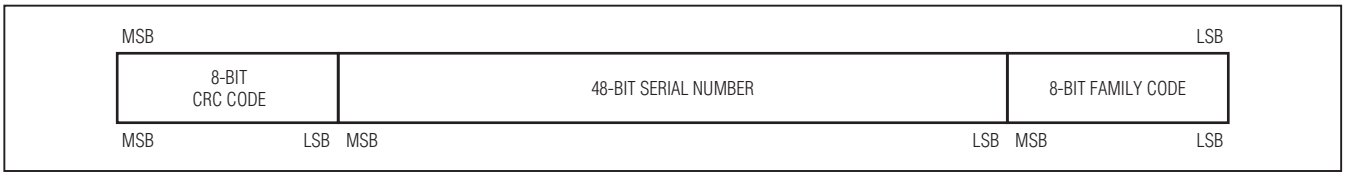


Figure 3. 64-Bit ROM ID

1-Wire SHA-1 Authenticator

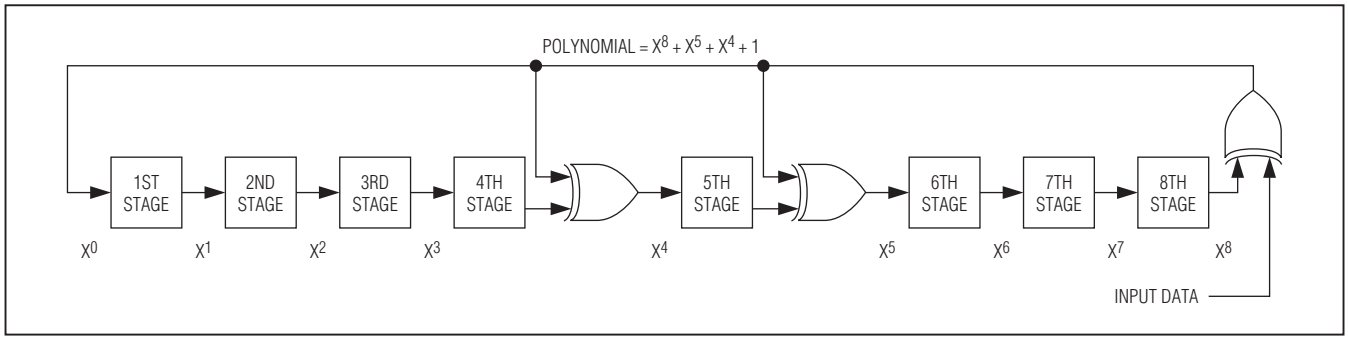


Figure 4. 1-Wire CRC Generator

64-Bit ROM ID

Each device contains a unique ROM ID that is 64 bits long. The first 8 bits are a 1-Wire family code. The next 48 bits are a unique serial number. The last 8 bits are a cyclic redundancy check (CRC) of the first 56 bits. See Figure 3 for details. The 1-Wire CRC is generated using a polynomial generator consisting of a shift register and XOR gates as shown in Figure 4. The polynomial is $X^8 + X^5 + X^4 + 1$. Additional information about the 1-Wire CRC is available in Application Note 27: *Understanding and Using Cyclic Redundancy Checks with Maxim iButton® Products*.

The shift register bits are initialized to 0. Then, starting with the least significant bit of the family code, one bit at a time is shifted in. After the 8th bit of the family code has been entered, the serial number is entered. After the last bit of the serial number has been entered, the shift register contains the CRC value. Shifting in the 8 bits of the CRC returns the shift register to all 0s.

Memory

The device has three memory areas: user memory, security data, and special function registers. User memory and special function registers are located in a linear address space, as shown in Figure 5. The user memory begins at address 0000h and ends at address 0017h. **Refer to the full data sheet for additional information.**

The user-writeable memory is implemented in EPROM technology. The factory-default state of the memory is 00h. During programming, bits of the target 4-byte block can be changed to a 1 or a 0. Once a block is written, the entire 4-byte block becomes automatically write protected. This means it is not possible to program a block multiple times, e.g., to change a few bits at a time.

Memory and SHA-1 Function Commands

This section describes the commands and flowcharts needed to use the memory and SHA-1 engine of the device. **Refer to the full data sheet for more information.**

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

1-Wire SHA-1 Authenticator

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 DS28E10 is a slave device. The bus master is typically a 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.

Hardware Configuration

The 1-Wire bus has only a single line by definition; it is important that each device on the bus be able to 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 DS28E10 is open drain with an internal circuit equivalent to that shown in Figure 7.

A multidrop bus consists of a 1-Wire bus with multiple slaves attached. The DS28E10 supports both a standard and overdrive communication speed of 15.4kbps (max) and 125kbps (max), respectively. The value of the pullup resistor primarily depends on the network size and load conditions. The DS28E10 requires a pullup resistor of 2.2kΩ (max) at any speed.

The idle state for the 1-Wire bus is high. If for any reason a transaction must 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 (overdrive speed) or more than 120µs (standard speed), one or more devices on the bus could be reset.

Transaction Sequence

The protocol for accessing the DS28E10 through the 1-Wire port is as follows:

- Initialization
- ROM Function Command
- Memory/SHA-1 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 a presence pulse(s) transmitted by the slave(s). The presence pulse lets the bus master know that the DS28E10 is on the bus and is ready to operate. For more details, see the *1-Wire Signaling* section.

1-Wire ROM Function Commands

Once the bus master has detected a presence, it can issue one of the seven ROM function commands that the DS28E10 supports. All ROM function commands are 8 bits long. A list of these commands follows (see the flowchart in Figure 8). Under certain conditions, the ROM function commands may not operate properly right after power-up. See the *Applications Information* section for a method to ensure proper operation.

Read ROM [33h]

The Read ROM command allows the bus master to read the DS28E10'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

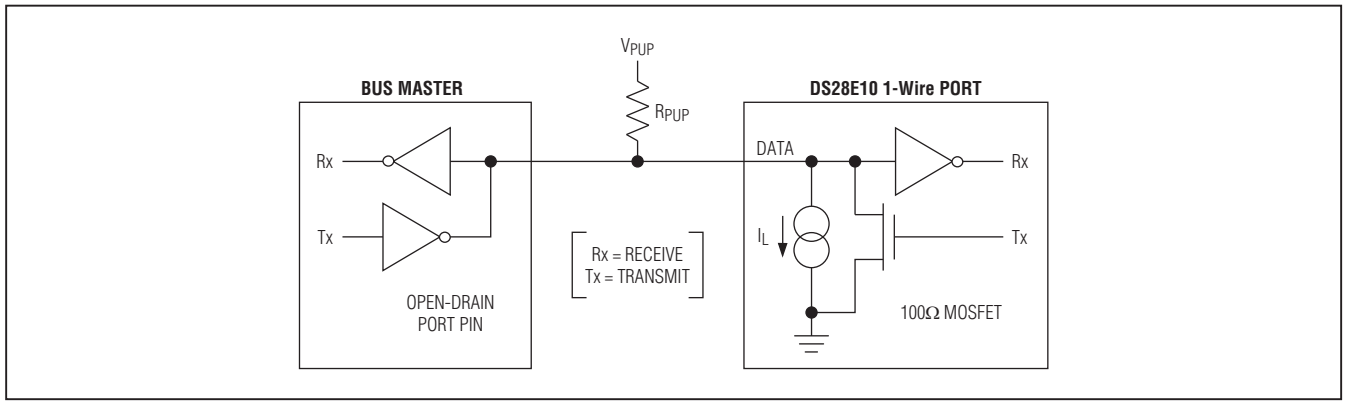


Figure 7. Hardware Configuration

1-Wire SHA-1 Authenticator

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 ID, allows the bus master to address a specific DS28E10 on a multidrop bus. Only the DS28E10 that exactly matches the 64-bit ROM ID responds to the following memory or SHA-1 function command. All other slaves wait for a reset pulse. This command can be used with a single or multiple devices on the bus.

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 of 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.

Skip ROM [CCh]

This command can save time in a single-drop bus system by allowing the bus master to access the memory or SHA-1 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 Command [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 memory and SHA-1 functions, similar to a Skip ROM command. The only way to set the RC bit is through successfully executing the Match ROM, Search ROM, or Overdrive-Match 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.

Overdrive-Skip ROM [3Ch]

On a single-drop bus this command can save time by allowing the bus master to access the memory functions without providing the 64-bit ROM ID. Unlike the normal Skip ROM command, the Overdrive-Skip ROM sets the DS28E10 in the overdrive mode (OD = 1). All communication following this command must occur at overdrive speed until a reset pulse of minimum 480µs duration resets all devices on the bus to standard speed (OD = 0).

When issued on a multidrop bus, this command sets all overdrive-supporting devices into overdrive mode. To subsequently address a specific overdrive-supporting device, a reset pulse at overdrive speed must be issued followed by a Match ROM or Search ROM command sequence. This speeds up the time for the search process. If more than one slave supporting overdrive is present on the bus and the Overdrive-Skip ROM command is followed by a read command, data collision occurs on the bus as multiple slaves transmit simultaneously (open-drain pulldowns produce a wired-AND result).

Overdrive-Match ROM [69h]

The Overdrive-Match ROM command followed by a 64-bit ROM ID transmitted at overdrive speed allows the bus master to address a specific DS28E10 on a multidrop bus and to simultaneously set it in overdrive mode. Only the DS28E10 that exactly matches the 64-bit number responds to the subsequent memory or SHA-1 function command. Slaves already in overdrive mode from a previous Overdrive-Skip ROM or successful Overdrive-Match ROM command remain in overdrive mode. All overdrive-capable slaves return to standard speed at the next reset pulse of minimum 480µs duration. The Overdrive-Match ROM command can be used with a single or multiple devices on the bus.

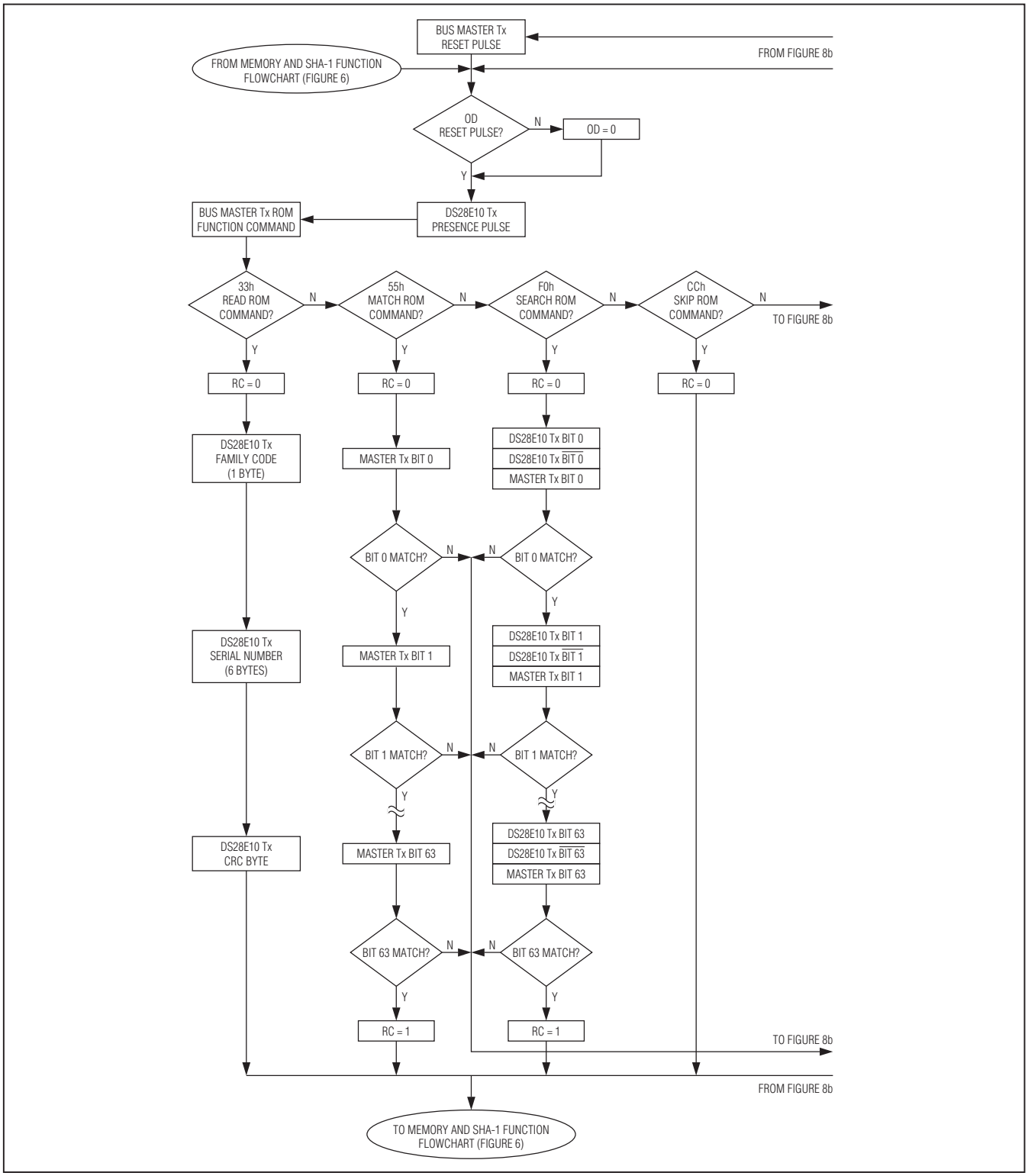
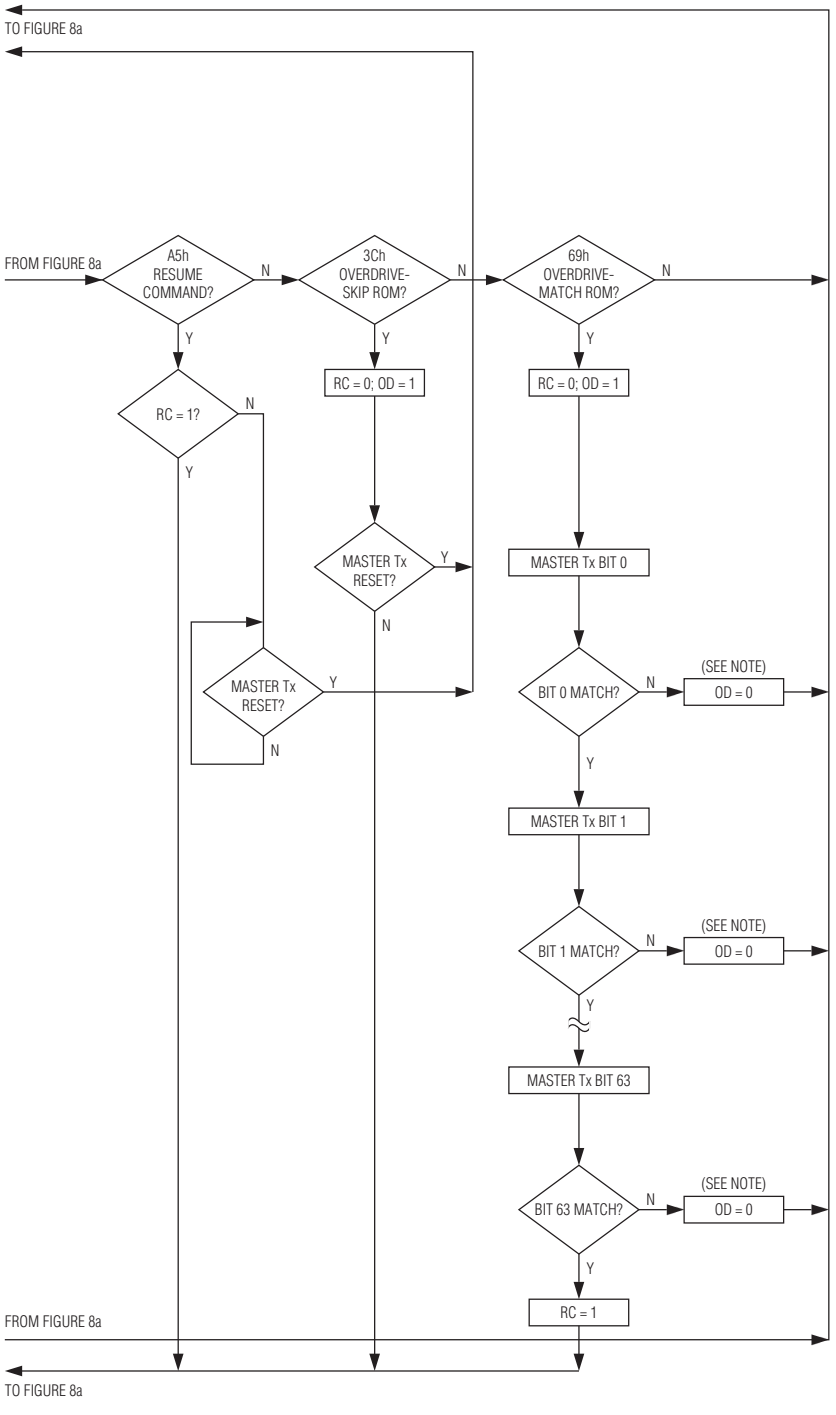


Figure 8a. ROM Functions Flowchart

1-Wire SHA-1 Authenticator



NOTE: THE OD FLAG REMAINS AT 1 IF THE DEVICE WAS ALREADY AT OVERDRIVE SPEED BEFORE THE OVERDRIVE-MATCH ROM COMMAND WAS ISSUED.

Figure 8b. ROM Functions Flowchart (continued)

1-Wire Signaling

The DS28E10 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. The DS28E10 can communicate at two different speeds: standard speed and overdrive speed. If not explicitly set into the overdrive mode, the DS28E10 communicates at standard speed. While in overdrive mode the fast timing applies to all waveforms.

To get from idle to active, the voltage on the 1-Wire line needs to fall from V_{PUP} below the threshold V_{IL}. To get from active to idle, the voltage needs to rise from 0V past the threshold V_{IH}. The time it takes for the voltage to make this rise is seen in Figure 9 as ε, and its duration depends on the pullup resistor (R_{PUP}) used and the capacitance of the 1-Wire network attached.

Figure 9 shows the initialization sequence required to begin any communication with the DS28E10. A reset pulse followed by a presence pulse indicates that the DS28E10 is ready to receive data, given the correct ROM and memory 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. A t_{RSTL} duration of 480µs or longer exits the overdrive mode, returning the device to standard speed. If the DS28E10 is in overdrive mode and t_{RSTL} is no longer than 80µs, the device remains in overdrive mode. If the device is in overdrive mode and t_{RSTL} is between 80µs and 480µs, the device resets, but the communication speed is undetermined.

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 case of a DS2482-x00 driver, by active circuitry. When the threshold V_{IH} is crossed, the DS28E10 waits for t_{PDH} and then transmits a presence pulse by pulling the line low for t_{PDL}. To detect a presence pulse, the master must test the logical state of the 1-Wire line at t_{MSP}.

The t_{RSTH} window must be at least the sum of t_{PDHMAX}, t_{PDLMAX}, and t_{RECMIN}. Immediately after t_{RSTH} is expired, the DS28E10 is ready for data communication. In a mixed population network, t_{RSTH} should be extended to minimum 480µs at standard speed and 48µs at overdrive speed to accommodate other 1-Wire devices.

Read/Write Time Slots

Data communication with the DS28E10 takes place in time slots, which 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 10 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_{IL}, the DS28E10 starts its internal timing generator that determines when the data line is sampled

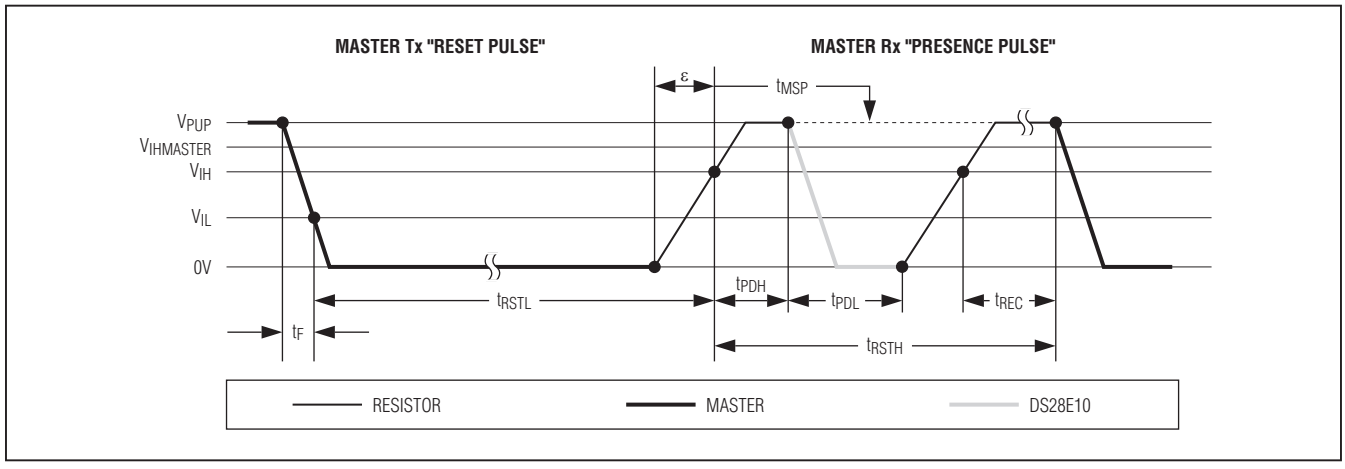


Figure 9. Initialization Procedure: Reset and Presence Pulse

1-Wire SHA-1 Authenticator

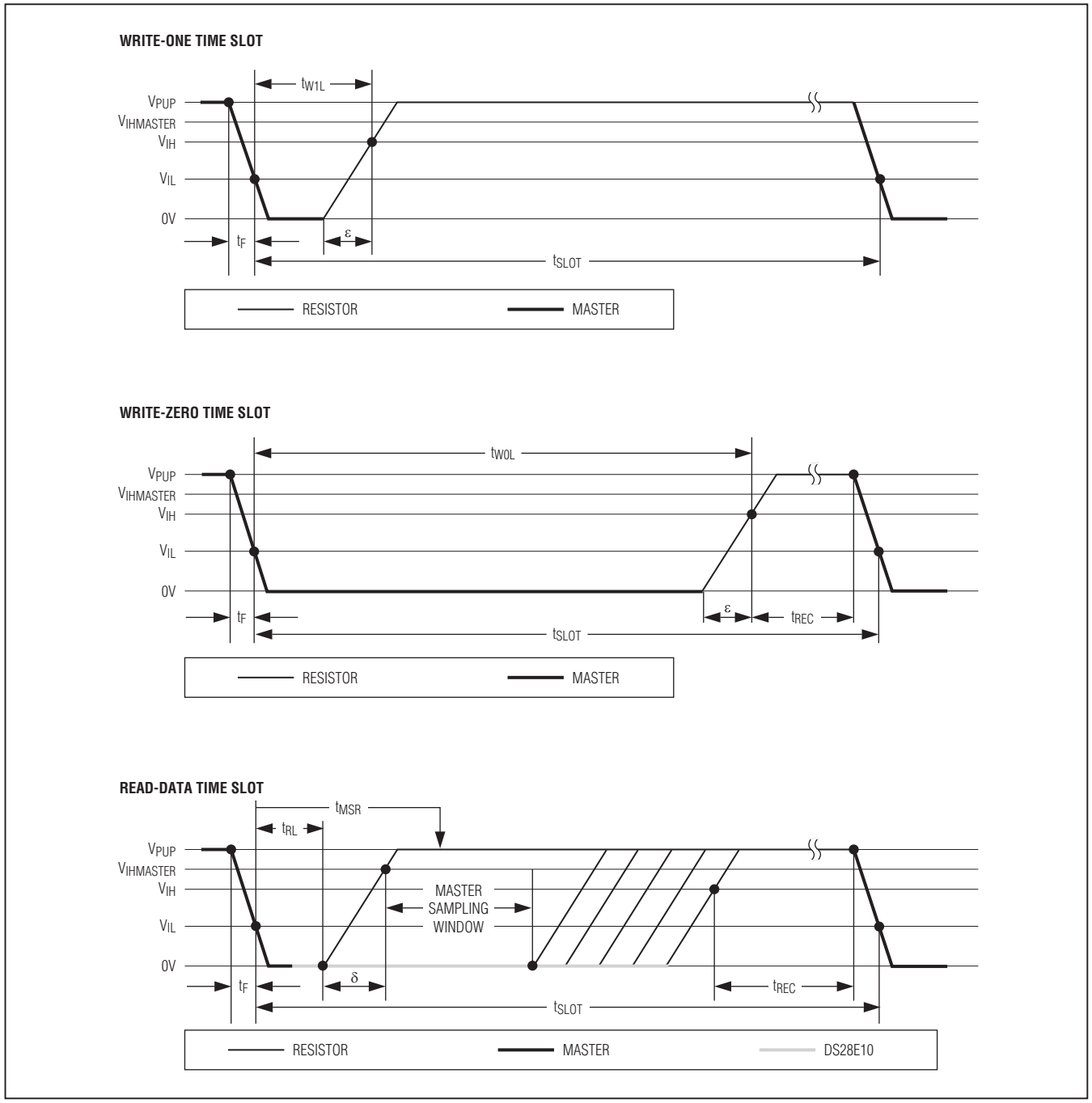


Figure 10. Read/Write Timing Diagrams

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_{IH} 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_{IH} 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_{IH} threshold has been crossed, the DS28E10 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_{IL} until the read low time t_{RL} is expired. During the t_{RL} window, when responding with a 0, the DS28E10 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 DS28E10 does not hold the data line low at all, and the voltage starts rising as soon as t_{RL} is over.

The sum of $t_{RL} + \delta$ (rise time) on one side and the internal timing generator of the DS28E10 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 DS28E10 to get ready for the next time slot. Note that t_{REC} specified herein applies only to a single DS28E10 attached to a 1-Wire line. For multidevice configurations, t_{REC} needs to 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 DS2482-x00 1-Wire line drivers, can be used.

Programming Pulse

Refer to the full data sheet for this information.

Improved Network Behavior (Switchpoint 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

Refer to the full data sheet for this information.

Figure 11. Programming Pulse Timing

1-Wire SHA-1 Authenticator

Refer to the full data sheet for this information.

Figure 12. Typical Circuit for EPROM Programming

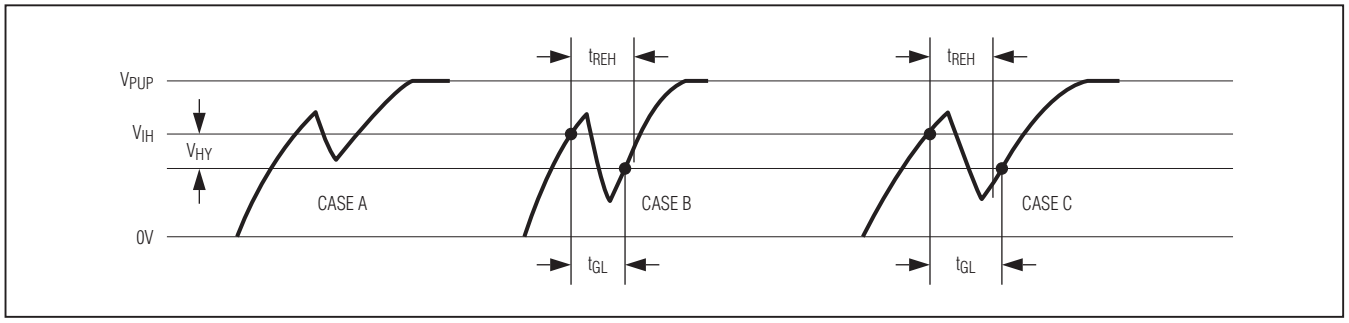


Figure 13. Noise Suppression Scheme

Search ROM command coming to a dead end or cause a device-specific function command to abort. For better performance there is a hysteresis at the low-to-high switching threshold V_{IH}. If a negative glitch crosses V_{IH} but does not go below V_{IH} - V_{HY}, it is not recognized (Figure 13, Case A). The hysteresis is effective at any 1-Wire speed.

For standard speed communication only, there is a time window specified by the rising-edge hold-off time t_{REH} during which glitches are ignored, even if they extend below V_{IH} - V_{HY} threshold (Figure 13, Case B, $t_{GL} < t_{REH}$). Deep voltage droops or glitches that appear late after crossing the V_{IH} threshold and extend beyond the t_{REH} window cannot be filtered out and are taken as the beginning of a new time slot (Figure 13, Case C, $t_{GL} \geq t_{REH}$). The rising-edge hold-off glitch filtering does not apply at overdrive speed.

CRC Generation

The DS28E10 uses two different types of CRCs. One CRC is an 8-bit type that is computed at the factory and is stored in the most significant byte of the 64-bit ROM ID number. The bus master can compute a CRC value from the first 56 bits of the 64-bit ROM ID and compare it to

the value read from the DS28E10 to determine if the ID has been received error-free. The equivalent polynomial function of this CRC is $X^8 + X^5 + X^4 + 1$. This 8-bit CRC is received in the true (noninverted) form.

The other CRC is a 16-bit type, which is used for error detection with memory and SHA-1 commands. **For details, refer to the full data sheet.**

Refer to the full data sheet for this information.

Figure 14. CRC-16 Hardware Description and Polynomial

1-Wire SHA-1 Authenticator

Applications Information

Power-Up Timing

The DS28E10 is sensitive to the power-on slew rate and can inadvertently power up with incomplete initialization. When this occurs, the Read ROM command does not deliver a valid ROM ID and the memory/SHA-1 functions do not work properly. Some production lots are more affected than others.

For most reliable operation, it is recommended to perform the following steps after the V_{CC} supply has reached its normal operating level:

1) Generate a reset/presence detect sequence (see Figure 9).
2) Issue the Skip ROM command.
3) Issue the Write Memory command (code 55h) with memory address 0000h.
4) Send 4 data bytes FFh.
5) Read the inverted CRC-16 and, without waiting for t_{PP}, send the 00h clocking byte. **Do not apply the programming pulse**; instead, leave V_{CC} at its normal level ($V_{CC} = V_{PUP}$).
6) Generate a reset/presence detect sequence.

These steps force an internal power-on reset with complete initialization. Now the device is ready to operate and delivers a valid ROM ID and correctly executes all ROM and memory/SHA-1 function commands. If there is more than one DS28E10 on the 1-Wire bus, this procedure initializes all of them at the same time.

Compatibility Considerations

The DS28E10 might not be the only device on the 1-Wire bus. Therefore, one should be aware of unintended consequences caused by issuing Skip ROM followed by command code 55h. As it turns out, 1-Wire memories understand command code 55h as Copy Scratchpad, a command that is executed only if preceded by a matching Write Scratchpad command; this precondition is not met here. Logger iButtons of the DS1922 series and the DS1923 understand command code 55h as Forced Conversion. This command would definitely be executed, but has no effect other than overwriting the Latest Conversion Readout register with new values; this occurs only if no mission is in progress.

Package Information

For the latest package outline information and land patterns, go to **www.maxim-ic.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	OUTLINE NO.	LAND PATTERN NO.
6 TSOC	D6+1	21-0382	90-0321
3 SOT23	U3+2	21-0051	90-0179

1-Wire SHA-1 Authenticator

Revision History

REVISION NUMBER	REVISION DATE	DESCRIPTION	PAGES CHANGED
0	6/10	Initial release	—
1	10/10	Changed ESD specification from 8kV to 6kV in the *Features* section and added land pattern information to the *Package Information* section	1, 23
2	4/11	Added the *Applications Information* section	24

Mouser Electronics

Authorized Distributor

Click to View Pricing, Inventory, Delivery & Lifecycle Information:

Maxim Integrated:

DS28E10P+ DS28E10R+T DS28E10P+T