EVALUATION KIT AVAILABLE

Request Security User Guide and Developer Software ›

DS28E36

DeepCover Secure Authenticator

General Description

The DS28E36 is a DeepCover® secure authenticator that provides a core set of cryptographic tools derived from integrated asymmetric (ECC-P256) and symmetric (SHA-256) security functions. In addition to the security services provided by the hardware implemented crypto engines, the device integrates a FIPS/NIST true random number generator (RNG), 8Kb of secured EEPROM, a decrement-only counter, two pins of configurable GPIO, and a unique 64-bit ROM identification number (ROM ID). This unique ROM ID is used as a fundamental input parameter for cryptographic operations and also serves as an electronic serial number within the application. The DS28E36 communicates over the single-contact 1-Wire® bus at overdrive speed. The communication follows the 1-Wire protocol with the ROM ID acting as node address in the case of a multidevice 1-Wire network.

The ECC public/private key capabilities operate from the NIST defined P-256 curve and include FIPS 186 compliant ECDSA signature generation and verification to support a bidirectional asymmetric key authentication model. The SHA-256 secret-key capabilities are compliant with FIPS 180 and are flexibly used either in conjunction with ECDSA operations or independently for multiple HMAC functions.

Two GPIO pins can be independently operated under command control and include configurability supporting authenticated and nonauthenticated operation including an ECDSA-based crypto-robust mode to support secure-boot of a host processor.

DeepCover embedded security solutions cloak sensitive data under multiple layers of advanced security to provide the most secure key storage possible. To protect against device-level security attacks, invasive and noninvasive countermeasures are implemented including active die shield, encrypted storage of keys, and algorithmic methods.

Applications

- IoT Node Crypto-Protection
- Accessory and Peripheral Secure Authentication
- Secure Storage of Cryptographic Keys for a Host Controller
- Secure Boot or Download of Firmware and/or System Parameters

1-Wire and DeepCover are registered trademarks of Maxim Integrated Products, Inc.

Benefits and Features

- ECC-256 Compute Engine
  - FIPS 186 ECDSA P256 Signature and Verification
  - ECDH Key Exchange with Authentication Prevents Man-in-the-Middle Attacks
  - ECDSA Authenticated R/W of Configurable Memory
- SHA-256 Compute Engine
  - FIPS 180 MAC for Secure Download/Boot Operations
  - FIPS 198 HMAC for Bidirectional Authentication and Optional GPIO Control
- Two GPIO Pins with Optional Authentication Control
  - Open-Drain, 4mA/0.4V
  - Optional SHA-256 or ECDSA Authenticated On/Off and State Read
  - Optional Set On/Off after Multiblock Hash for Secure Boot/Download
- RNG with NIST SP 800-90B Compliant Entropy Source with Function to Read Out
- Optional Chip Generated Pr/Pu Key Pairs for ECC Operations
- 17-Bit One-Time Settable, Nonvolatile Decrement-Only Counter with Authenticated Read
- 8Kbits of EEPROM for User Data, Keys, and Certificates
- Unique and Unalterable Factory Programmed 64-Bit Identification Number (ROM ID)
  - Optional Input Data Component to Crypto and Key Operations
- Single-Contact 1-Wire Interface Communication with Host at 11.7kbps and 62.5kbps
- Operating Range: 3.3V ±10%, -40°C to +85°C
- 6-Pin TDFN-EP Package (3mm x 3mm)

***Ordering Information* and *Typical Application Circuit* appear at end of data sheet.**

19-100170; Rev 3; 3/20

maxim integrated™

Absolute Maximum Ratings

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

Package Information

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})	55ºC/W
Junction to Case (θ_{JC})	9ºC/W
Thermal Resistance, Four-Layer Board:	
Junction to Ambient (θ_{JA})	42ºC/W
Junction to Case (θ_{JC})	9ºC/W

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% production tested at T_A = +25°C and T_A = +85°C. Typical values are at T_A = +25°C. 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}	(Note 1)	2.97	3.3	3.63	V
1-Wire Pullup Resistance	R_{PUP}	(Notes 1, 2)	300		1000	Ω
Input Capacitance	C_{IO}	(Note 3)		0.1 + Cx		nF
Capacitor External	C_X	(Note 1)	399.5	470	540.5	nF
Input Load Current	I_L	IO pin at V_{PUP}		6	250	µA
Computation Current	I_{SPU}	During t_{RM}, t_{WM}, t_{CMP}, t_{VES}, t_{GKP} or t_{GES} (Note 20)			7.5	mA
Computation Voltage	V_{SPU}	Voltage at IO pin during t_{RM}, t_{WM}, t_{CMP}, t_{VES}, t_{GKP}, or t_{GES} (Note 20)	2.2			V
High-to-Low Switching Threshold	V_{TL}	(Notes 4, 5, 6)		0.65 x V_{PUP}		V
Input Low Voltage	V_{IL}	(Note 7)			0.10 x V_{PUP}	V

Electrical Characteristics (continued)

Limits are 100% production tested at T_A = +25°C and T_A = +85°C. Typical values are at T_A = +25°C. 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
Low-to-High Switching Threshold	V_{TH}	(Notes 4, 5, 8)		0.75 x V_{PUP}		V
Switching Hysteresis	V_{HY}	(Notes 4, 5, 9)		0.3		V
Output Low Voltage	V_{OL}	I_{OL} = 4mA (Note 10)			0.4	V
Recovery Time (Notes 1, 11, 12)	t_{REC}	Standard speed, R_{PUP} = 1000Ω	25			µs
		Overdrive speed, R_{PUP} = 1000Ω	10			
Rising-Edge Hold-off Time (Notes 4, 13)	t_{REH}	Applies to standard speed only		1		µs
Time Slot Duration (Notes 1, 14)	t_{SLOT}	Standard speed	85			µs
		Overdrive speed	16			
IO PIN: 1-Wire RESET, PRESENCE-DETECT CYCLE						
Reset Low Time (Note 1)	t_{RSTL}	Standard speed	480		640	µs
		Overdrive speed	48		80	
Reset High Time (Notes 1, 15)	t_{RSTH}	Standard speed	480			µs
		Overdrive speed	48			
Presence Detect Fall Time (Notes 4, 16)	t_{FPD}	Standard speed		1.25		µs
		Overdrive speed		0.15		
Presence-Detect Sample Time (Notes 1, 17)	t_{MSP}	Standard speed	65		75	µs
		Overdrive speed	7		10	
IO PIN: 1-Wire WRITE						
Write-Zero Low Time (Notes 1, 18)	t_{W0L}	Standard speed	60		120	µs
		Overdrive speed	6		16	
Write-One Low Time (Notes 1, 18)	t_{W1L}	Standard speed	0.25		15	µs
		Overdrive speed	0.25		2	
IO PIN: 1-Wire READ						
Read Low Time (Notes 1, 19)	t_{RL}	Standard speed	0.25		15 - δ	µs
		Overdrive speed	0.25		2 - δ	
Read Sample Time (Notes 1, 19)	t_{MSR}	Standard speed	t_{RL} + δ		15	µs
		Overdrive speed	t_{RL} + δ		2	
PIOA AND PIOB PINS						
Output Low	$PIOV_{OL}$	$PIOI_{OL}$ = 4mA (Note 10)			0.4	V
Input Low	$PIOV_{IL}$		-0.3		0.15 x V_{PUP}	V
Input High	$PIOV_{IH}$		0.7 x V_{PUP}		V_{PUP} + 0.3	V
Leakage Current	$PIOI_L$		-1		+1	µA

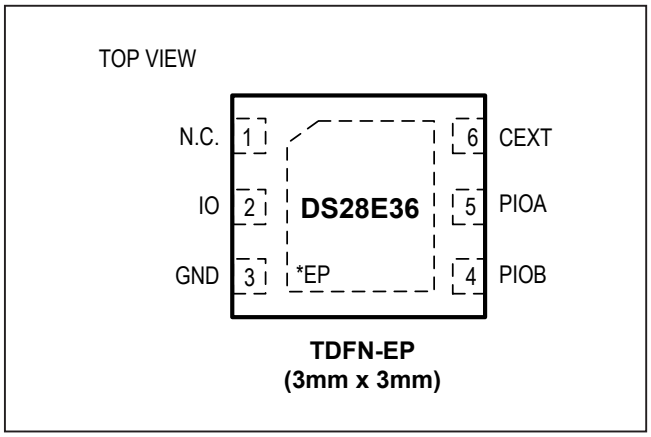
Electrical Characteristics (continued)

Limits are 100% production tested at T_A = +25°C and T_A = +85°C. Typical values are at T_A = +25°C. 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
STRONG PULLUP OPERATION						
Generate ECDSA Signature Time	t_{GES}	(Note 1)			50	ms
Generate ECC Key Pair	t_{GKP}	(Note 1)			100	ms
Verify ECDSA Signature or Compute ECDH Time	t_{VES}	(Note 1)			150	ms
Computation Time (HMAC or RNG)	t_{CMP}	(Note 1)			3	ms
EEPROM						
Read Memory Time	t_{RM}	(Note 1)			1	ms
Write Memory Time	t_{WM}	(Note 1)			15	ms
Write/Erase Cycles (Endurance)	N_{CY}	(Note 21)	100k			—
Data Retention	t_{DR}	T_A = +85°C (Note 22)	10			Years
POWER-UP						
Power-Up Time	t_{OSCWUP}	(Notes 1, 23)			2	ms

Note 1: System requirement.
Note 2: 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 3: Value represents the internal parasite capacitance when V_{PUP} is first applied. Once the parasite capacitance is charged, it does not affect normal communication. Typically, during normal communication, the internal parasite capacitance is effectively ~100pF.
Note 4: Guaranteed by design and/or characterization only. Not production tested.
Note 5: 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 6: Voltage below which, during a falling edge on IO, a logic-zero is detected.
Note 7: 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 8: Voltage above which, during a rising edge on IO, a logic-one is detected.
Note 9: 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 10: The I-V characteristic is linear for voltages less than 1V.
Note 11: Applies to a single device attached to a 1-Wire line.
Note 12: t_{REC} min covers operation at worst-case temperature V_{PUP}, R_{PUP}, C_X, t_{RSTL}, t_{WOL}, and t_{RL}. t_{RECMIN} can be significantly reduced under less extreme conditions. Contact the factory for more information.
Note 13: The earliest recognition of a negative edge is possible at t_{REH} after V_{TH} has been previously reached.
Note 14: Defines maximum possible bit rate. Equal to $1/(t_{W0LMIN} + t_{RECMIN})$.
Note 15: An additional reset of communication sequence sequence cannot begin until the reset high time has expired.
Note 16: Time from $V_{(IO)}$ = 80% of V_{PUP} and $V_{(IO)}$ = 20% of V_{PUP} at the negative edge on IO at the beginning of the Presence Detect pulse.
Note 17: Interval after t_{RSTL} during which a bus master can read a logic 0 on IO if there is a DS28E36 present.
Note 18: ε in Figure 6 represents the time required for the pullup circuitry to pull the voltage on IO up from V_{IL} to V_{TH}.
Note 19: δ in Figure 6 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.
Note 20: I_{SPU} is the current drawn from IO during a strong pullup (SPU) operation. The pullup circuit on IO during the SPU operation 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 21: Write-cycle endurance is tested in compliance with JESD47H.
Note 22: Data retention is tested in compliance with JESD47H.
Note 23: 1-Wire communication should not take place for at least t_{OSCWUP} after V_{PUP} reaches V_{PUP} min.

Pin Configuration



Pin Description

PIN	NAME	FUNCTION
1	N.C.	No Connection
2	IO	1-Wire IO
3	GND	Ground
4	PIOB	General-Purpose IO
5	PIOA	General-Purpose IO
6	CEXT	Input for External Capacitor
—	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.

Detailed Description

The DS28E36 is a secure authenticator that supports multiple asymmetric (ECC-P256) and symmetric (SHA-256) security functions. In addition to the security services provided by the hardware implemented ECC and SHA-256 engines, the device integrates a FIPS/NIST true random number generator (RNG), 8Kb of secured EEPROM, a decrement-only counter, two pins of configurable GPIO, and a unique 64-bit serial number. The ECC public/private key capabilities operate from the NIST defined P-256 curve and include FIPS 186 compliant ECDSA signature generation and verification for bidirectional asymmetric key authentication. Additionally, through FIPS/NIST 800-56B ECDH-based key agreement, the device supports secure storage and host communication of sensitive data, such as application-specific crypto keys that would be used independently by a host processor. The SHA-256 secret-key capabilities are compliant with FIPS 180 and are flexibly used either in conjunction with ECDSA operations or independently for multiple MAC and HMAC functions. Through the integrated RNG, the device further enhances system crypto functionality with the ability to supply FIPS-grade random numbers to a host processor along with internal-only functions including nonce values for ECDSA operation and optional generation of its ECC private keys. Two pins of GPIO can be independently operated under command control and include configurability supporting authenticated and nonauthenticated operation including an ECDSA-based crypto-robust mode to support secure-boot of a host processor.

The DS28E36 integrates an 8Kb secured EEPROM array to store keys, certificates, general-purpose data and control registers. Multiple user-programmable protection modes exist for the general-purpose memory space including open, ECDSA R/W authentication protection, SHA-256 HMAC R/W authentication protected, and SHA-256 one-time-pad (OTP) R/W encryption in conjunction with an ECDH established key. With these options, general-purpose memory can be flexibly configured to store end application data ranging from nonsensitive calibration constants to critically sensitive host-system crypto keys.

The DS28E36 also provides a dedicated 17-bit counter that operates in a decrement-only mode to support applications where limited use requirements exist and must be tracked. Once set and upon command, the device decrements the counter value by 1. After the counter reaches a value of 0, no additional changes are possible. To prevent reply attacks, a read of the counter is performed with user-selectable ECDSA or SHA-256 HMAC authentication.

The block diagram in Figure 1 shows the relationships between the circuit elements of the DS28E36.

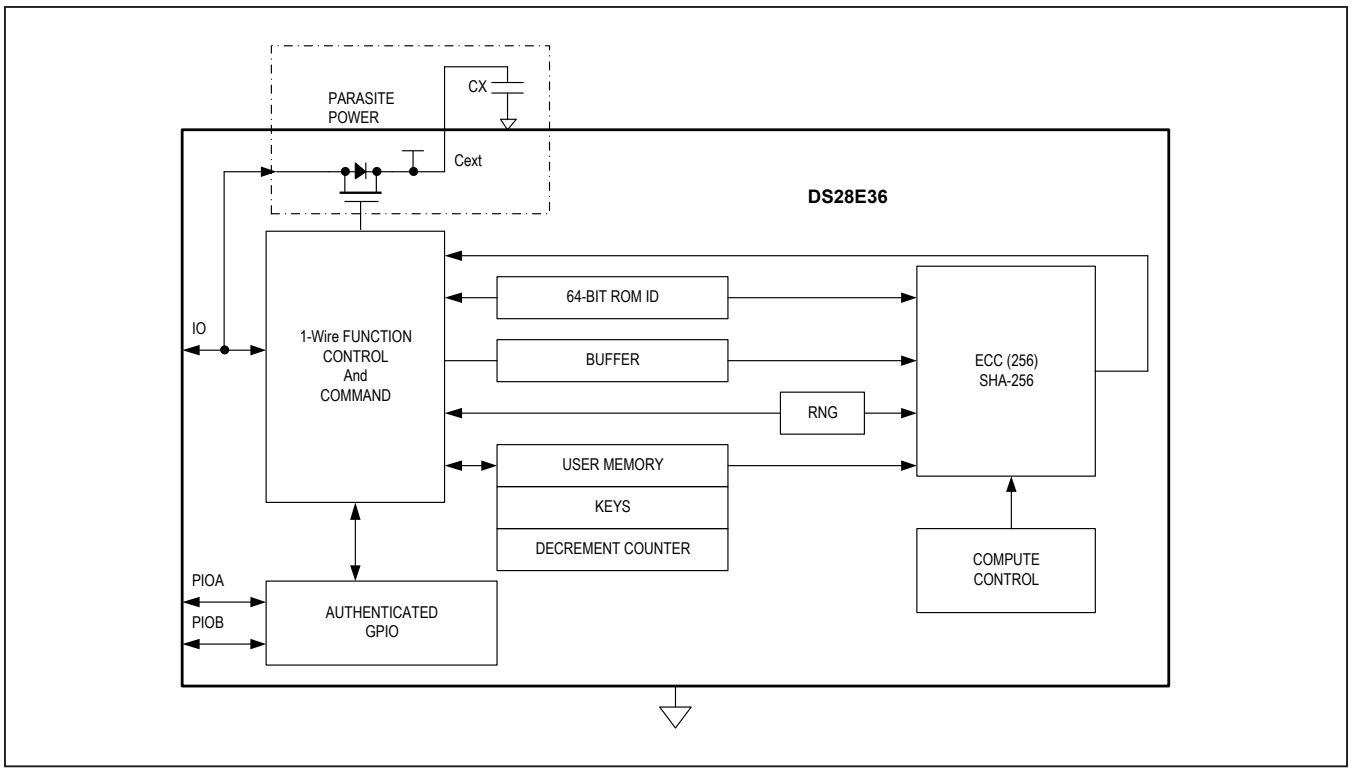


Figure 1. Simplified Block Diagram

Design Resource Overview

Operation of the DS28E36 involves use of device EEPROM and execution of device function commands. The following provides an overview including the decrement counter and GPIO pins. Refer to the *DS28E36 Security Guide* for full details.

Memory

A secured 8kbit EEPROM array is divided into two 4kbit regions. One 4kbit space for user-programmable and configurable memory, the other 4kbit space for registers including ECC and SHA-256 keys, the decrement-only counter, and programmable device control functions. Depending on the register function, there are either default or user-programmable protection modes.

Function Commands

After a 1-Wire Reset/Presence cycle and ROM function command sequence is successful, a device function command can be accepted. These commands, in general, follow the state flow diagrams of Figure 2 and Figure 3. Within these flow diagrams, the data transfer is verified when writing and reading by a CRC of 16-bit type (CRC-16). The CRC-16 is computed as described in Maxim's Application Note 27.

Decrement Counter

The 17-bit decrement only counter can be written/initialized one time. If unwritten, it reads as random data and cannot be authenticated with a read. 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.

GPIO Control

State setting and/or reads of the two open-drain GPIO pins is controlled in accordance with user-programmable protection settings. Multiple protection options exist based on ECDSA, ECDH key establishment, or SHA256-HMAC.

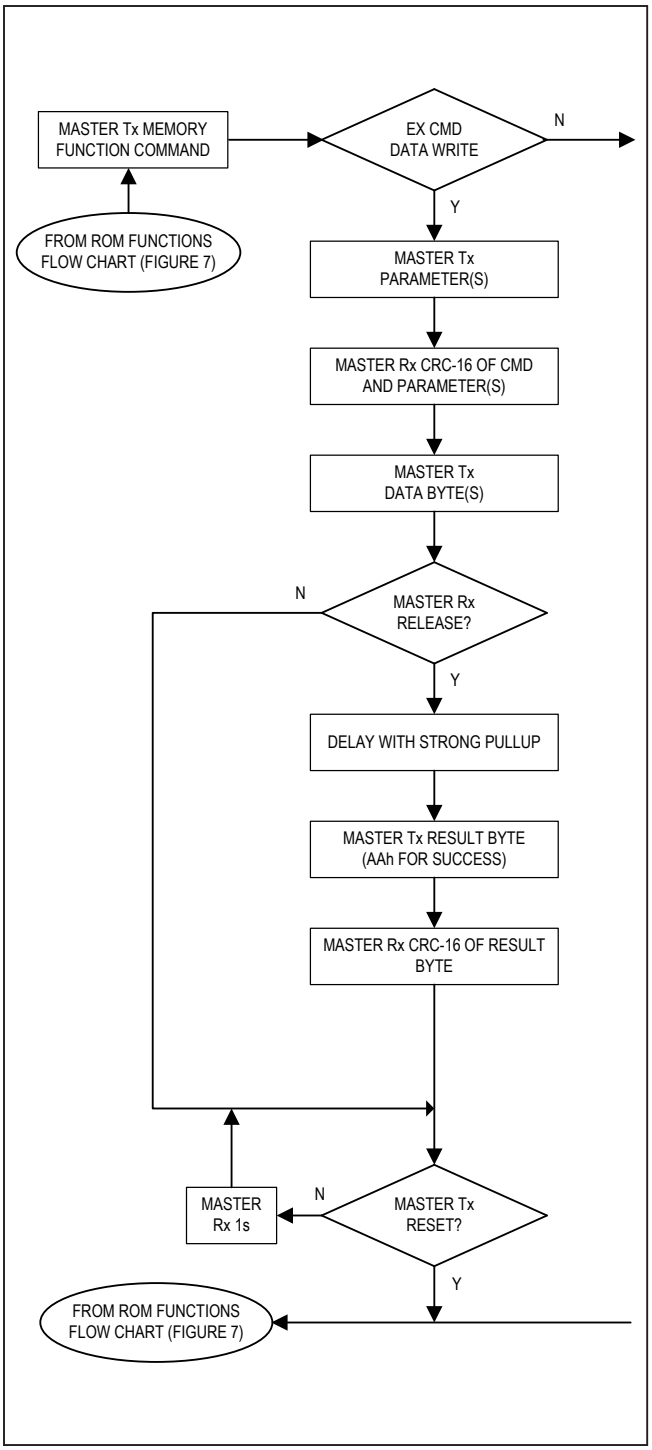


Figure 2. 1-Wire Device Execute Command or Data Write Flow Chart

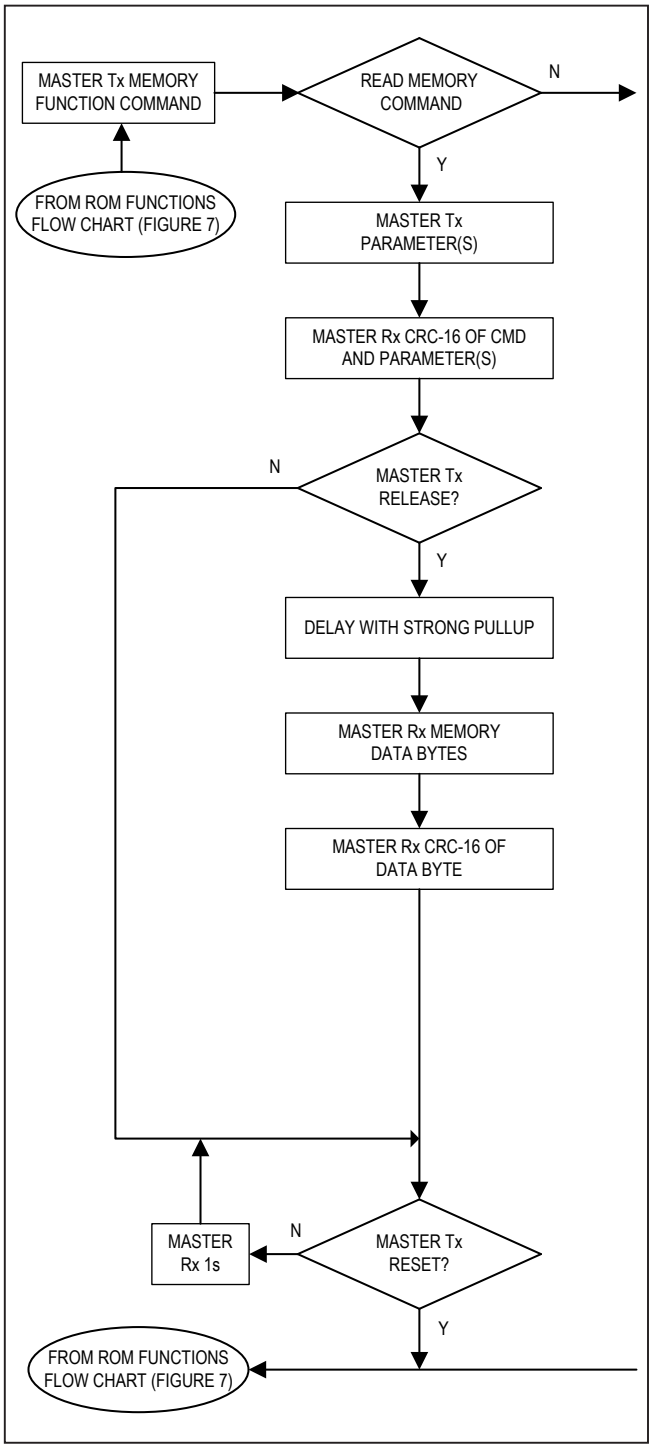


Figure 3. 1-Wire Device Data Read Flow Chart

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 DS28E36 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 DS28E36 is open drain with an internal circuit equivalent to that shown in Figure 4.

A multidrop bus consists of a 1-Wire bus with multiple slaves attached. The DS28E36 supports both a standard and overdrive communication speed of 11.7kbps (max) and 62.5kbps (max), respectively. The value of the pullup resistor primarily depends on the network size and load conditions. The DS28E36 requires a pullup resistor of 1kΩ (max) at any speed.

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 (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 DS28E36 through the 1-Wire port is as follows:

- Initialization
- ROM function command
- Memory 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 DS28E36 is on the bus and is ready to operate. For more details, see the *1-Wire Signaling and Timing* section.

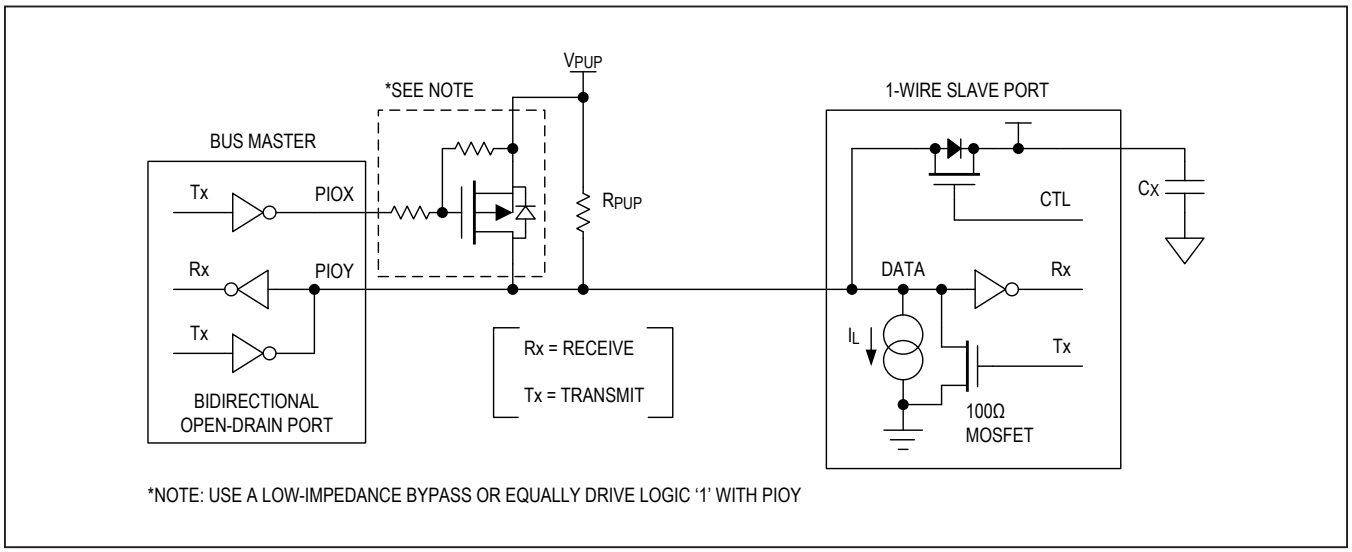


Figure 4. Hardware Configuration

1-Wire Signaling and Timing

The DS28E36 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 DS28E36 can communicate at two speeds: standard and overdrive. If not explicitly set into the overdrive mode, the DS28E36 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_{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 6 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 DS28E36 when determining a logical level, not triggering any events.

Figure 5 shows the initialization sequence required to begin any communication with the DS28E36. A reset pulse followed by a presence pulse indicates that the DS28E36 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 DS28E36 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 the case of a special driver chip, through the active circuitry. Now, the 1-Wire bus is pulled to V_{PUP} through the pullup resistor. When the threshold V_{TH} is crossed, the DS28E36 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 DS28E36 is ready for data communication. In a mixed population network, t_{RSTH} should be extended to a minimum 480µs at standard speed and a 48µs at overdrive speed to accommodate other 1-Wire devices.

Read/Write Time Slots

Data communication with the DS28E36 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 6 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 DS28E36 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.

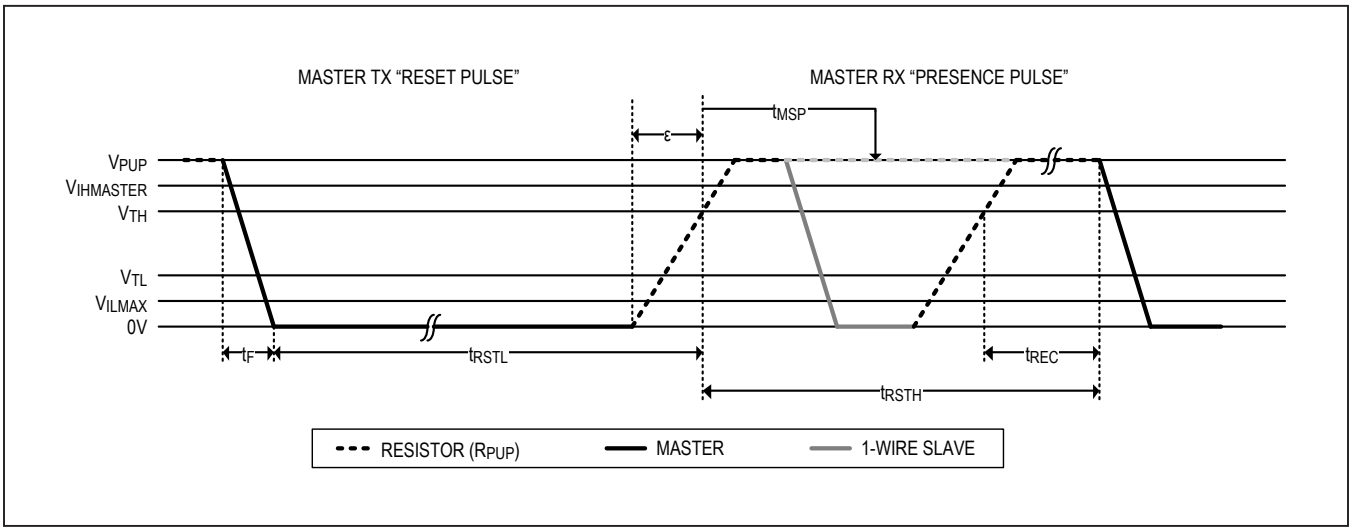


Figure 5. Initialization Procedure: Reset and Presence Pulse

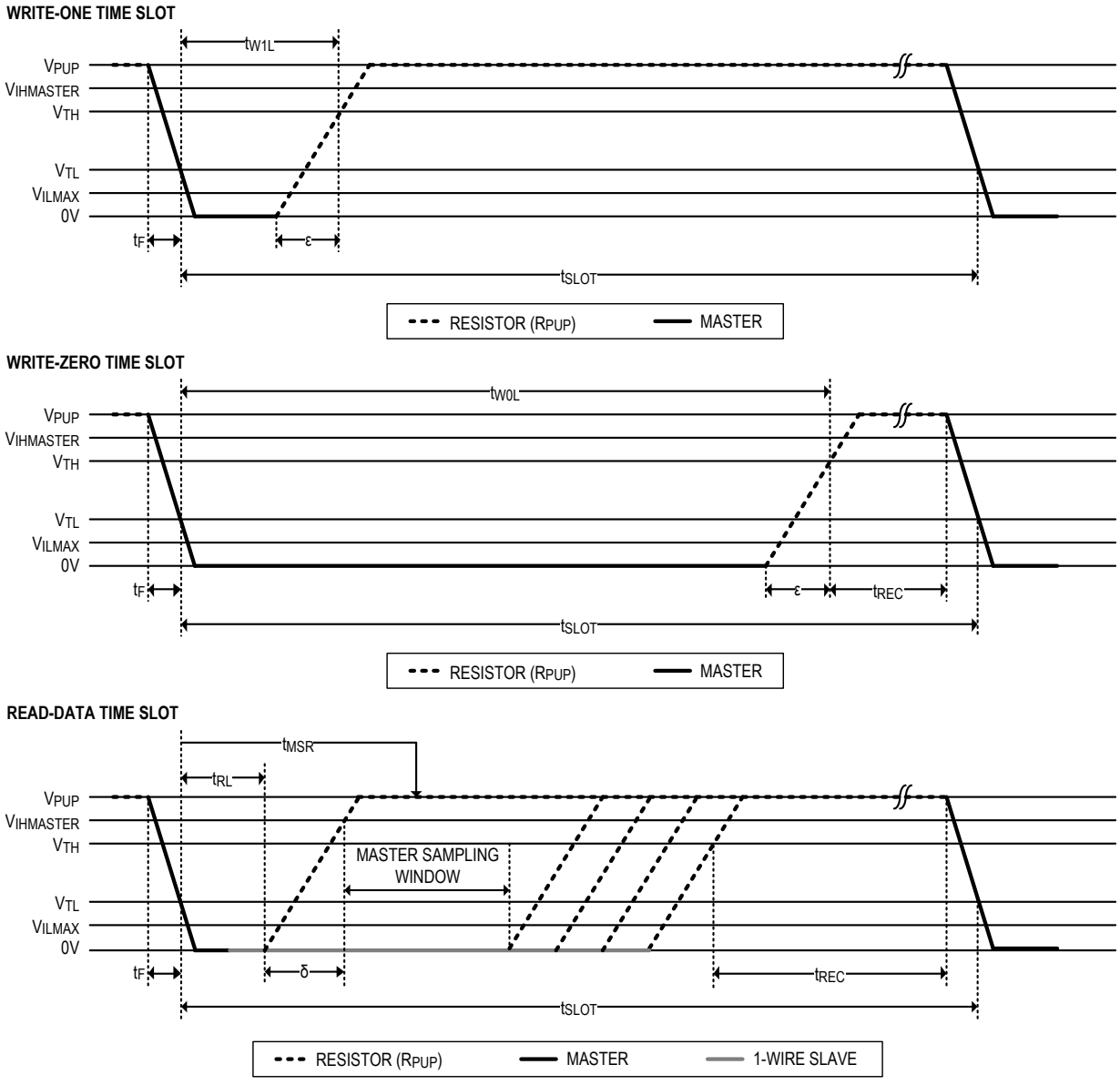


Figure 6. Read/Write Timing Diagrams

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 DS28E36 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 DS28E36 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 DS28E36 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 DS28E36 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 DS28E36 to get ready for the next time slot. Note that t_{REC} specified herein applies only to a single DS28E36 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 Function Commands

Once the bus master has detected a presence, it can issue one of the seven ROM function commands that the DS28E36 supports. All ROM function commands are 8 bits long. A list of these commands follows (see the flowchart in Figure 7-1 and Figure 7-2).

Read ROM [33h]

The Read ROM command allows the bus master to read the DS28E36'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 DS28E36 on a multidrop bus. Only the DS28E36 that exactly matches the 64-bit ROM sequence responds to the subsequent memory 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.

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.

Skip ROM [CCh]

This command can save time in a single-drop bus system by allowing the bus master to access the memory 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 memory function commands, similar to a Skip ROM command. The only way to set the RC bit is by 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 command sets the DS28E36 into 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 sequence transmitted at overdrive speed allows the bus master to address a specific DS28E36 on a multidrop bus and to simultaneously set it in overdrive mode. Only the DS28E36 that exactly matches the 64-bit ROM sequence responds to the subsequent memory 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 device or multiple devices on the bus.

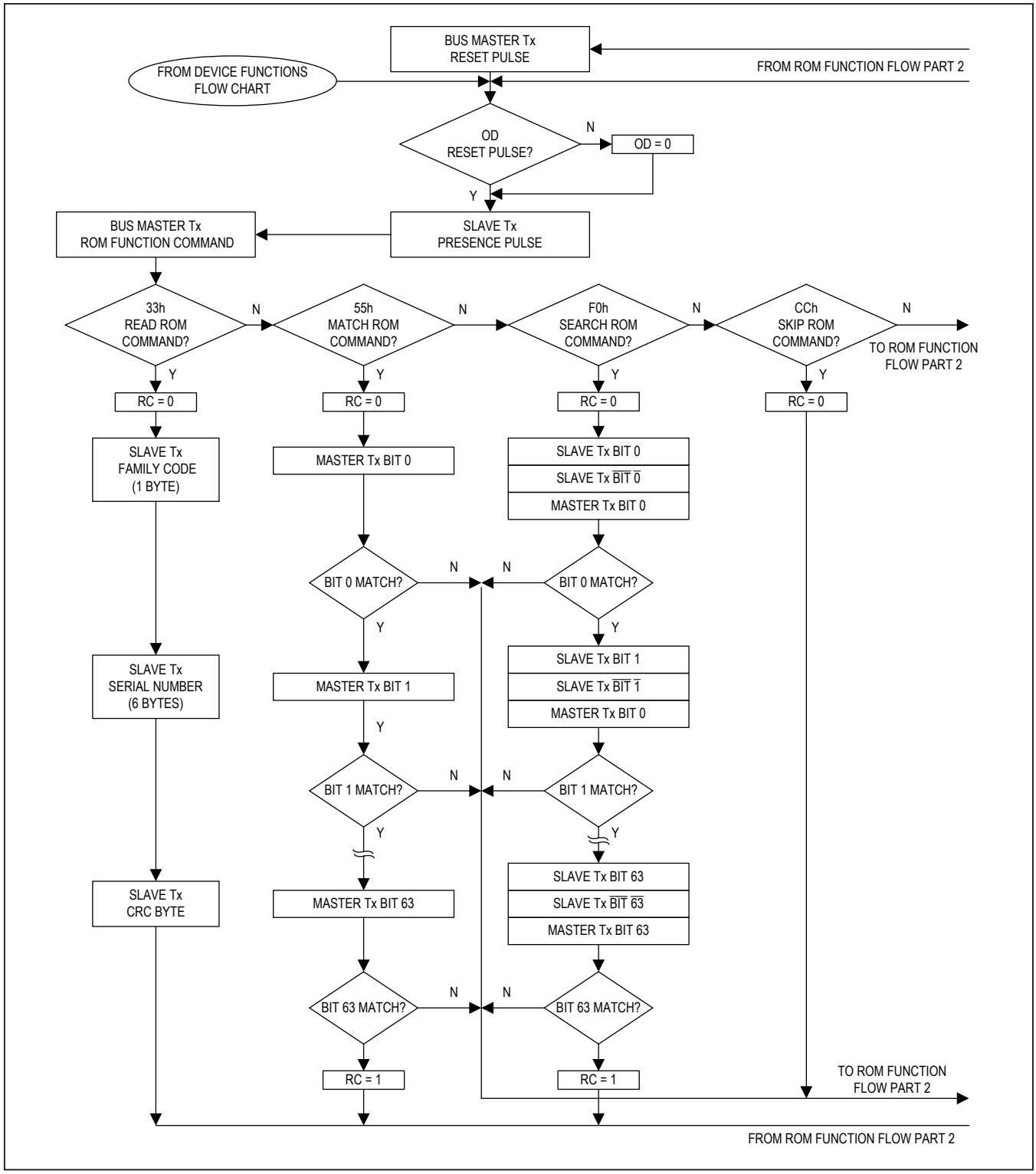


Figure 7-1. ROM Functions Flow Chart

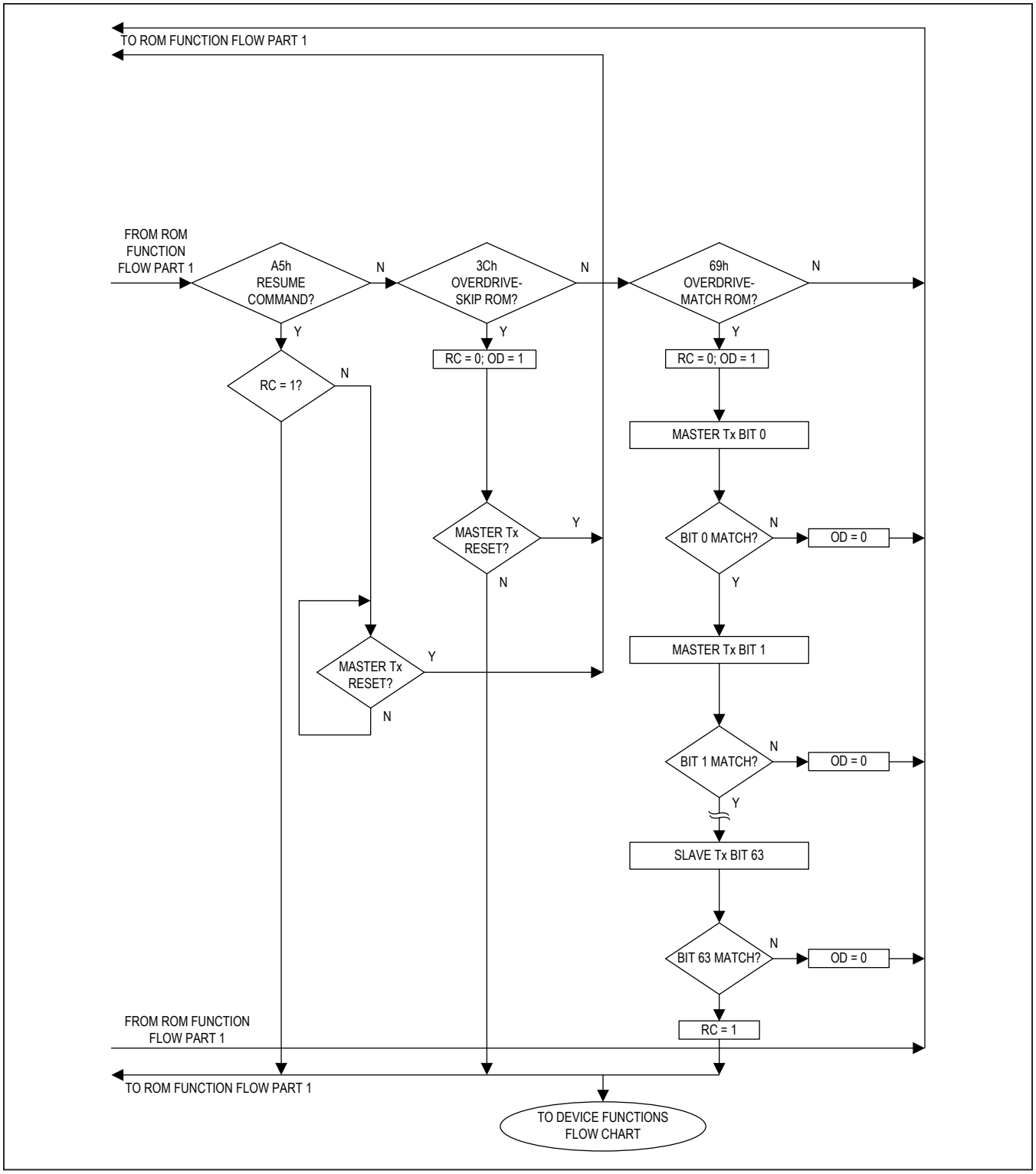


Figure 7-2. ROM Functions Flow Chart (continued)

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 Search ROM command coming to a dead end or cause a device-specific function command to abort. For better performance in network applications, the DS28E36 uses a 1-Wire front-end that is less sensitive to noise.

The DS28E36's 1-Wire front-end has the following features:

- The falling edge of the presence pulse has a controlled slew rate to reduce ringing. The slew rate control is specified by t_{FPD}.
- There is 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 8, Case A). The hysteresis is effective at any 1-Wire speed.
- 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 the V_{TH} - V_{HY} threshold (Figure 8, Case B, $t_{GL} < t_{REH}$). Deep voltage drops or glitches that appear late after crossing the V_{TH} threshold and extend beyond the t_{REH} window cannot be filtered out and are taken as the beginning of a new time slot (Figure 8, Case C, $t_{GL} \geq t_{REH}$).

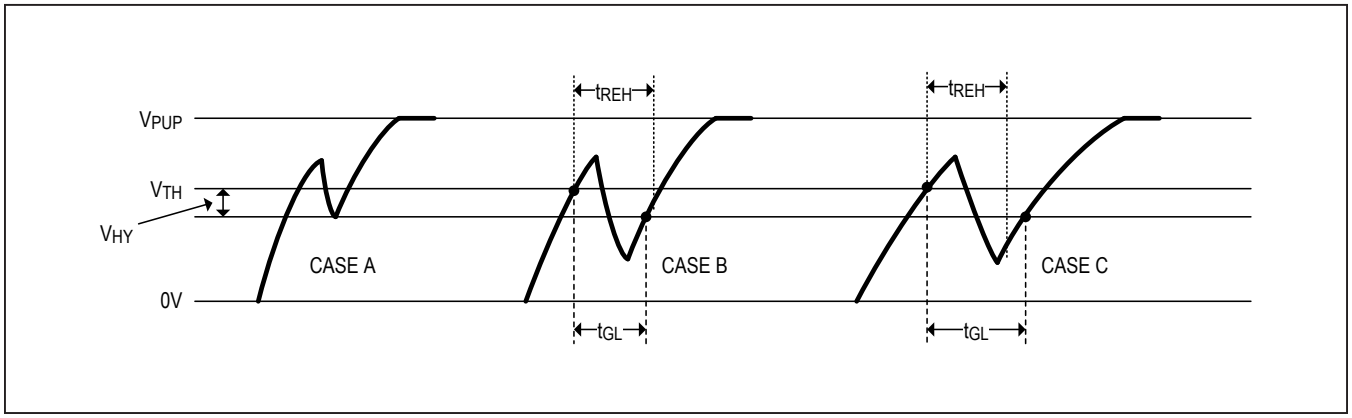
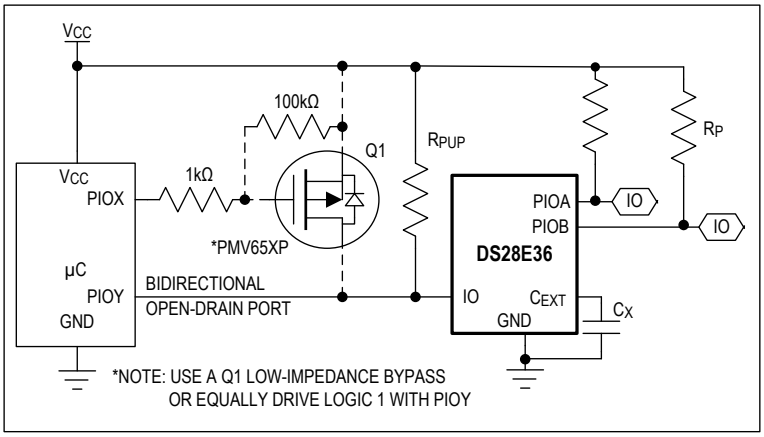


Figure 8. Noise Suppression Scheme

Typical Application Circuit



Ordering Information

PART	TEMP RANGE	PIN-PACKAGE
DS28E36Q+T†	-40°C to +85°C	6 TDFN-EP* (2.5k pcs)
DS28E36BQ+T	-40°C to +85°C	6 TDFN-EP* (2.5k pcs)

+Denotes a lead(Pb)-free/RoHS-compliant package.
T= Tape and reel.
**EP = Exposed pad.*
†Not recommended for new designs.

Package Information

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 statusonly. 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 TDFN-EP*	T633+2	21-0137	90-0058

Revision History

REVISION NUMBER	REVISION DATE	DESCRIPTION	PAGES CHANGED
0	10/17	Initial release	—
1	10/17	Updated *Package Information* section	2
2	11/18	Updated *Ordering Information* section	16
3	3/20	Updated *Typical Application Circuit*	16

X-ON Electronics

Largest Supplier of Electrical and Electronic Components

Click to view similar products for Security ICs / Authentication ICs ***category:***

Click to view products by Maxim ***manufacturer:***

Other Similar products are found below :

RJM8L151F6P6R AT97SC3204T-X2A1B-10 SLS32AIA020A4USON10XTMA2 AT97SC3205T-G3M4C-00 AT97SC3205T-H3M4C-20 AT97SC3204-U4A14-20 AT97SC3205T-H3M4C20B AT97SC3205-X3A12-10 AT97SC3204-U2MA-20 AT97SC3204-X2A1A-10 ATAES132-SH-EQ ATECC508A-MAHDA-S DS2401+ DS1990A-F3+ DS1990A-F5+ DS2401P+T&R DS2401Z+T&R DS2411P+ DS2411P+T&R ATSHA204-TH-CZ-T DS28CM00R-A00+T DS28C22Q+T ATTPM20P-G3MA1-10-B HCS515-IP HCS515P MCS3122-I/ST MIKROE-3047 ATECC508A-SSHDA-T ATSHA204A-SSHDA-B ATAES132A-SHEQ-B ATECC108A-SSHCZ-B ATSHA204A-SSHDA-T W74M32FVSSIQ IPL-CHP1.8V ATSHA204A-STUCZ-T DS2411R+T&R RJM8L151K8Q6Y CW3802 RJGT102WDP8 FM15160 508-03 RJGT102WDT6 RJMU401FHO ATECC108A-RBHCZ-T IPL-CHP 404726X AT88SC0808CA-Y6H-T AT88SA102S-SH-T MAX66240ESA+