1-Wire SHA3-256 Secure Authenticator with DS2431/DS28E07 Compatibility

DS28E54

Product Highlights

The DS28E54 secure authenticator combines FIPS 202-compliant secure hash algorithm (SHA-3) challenge and response authentication with secured electrically erasable programmable read-only memory (EEPROM).

The device provides a core set of cryptographic tools derived from integrated blocks, including an SHA-3 engine, 2.25Kbit of secured user EEPROM, a decrement-only counter, and a unique 64-bit ROM identification number (ROM ID), all while remaining reverse compatible to the DS2431/DS28E07.

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 the node address in the case of a multidevice 1-Wire network.

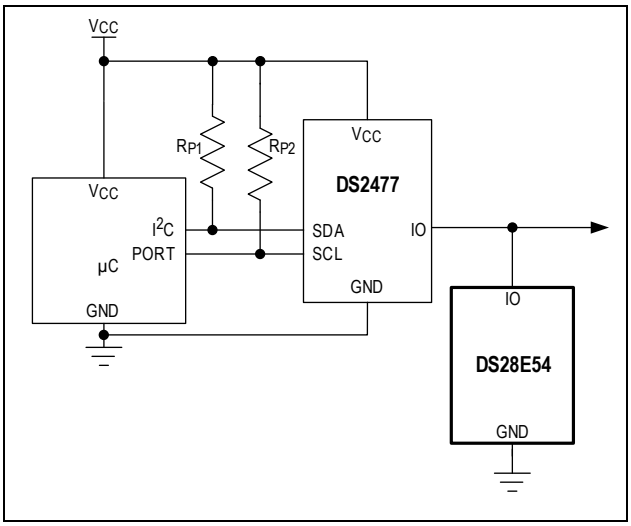
Key Applications

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

Benefits and Features

- DS2431/DS28E07 Reverse Compatibility
  - 2.25Kbits of EEPROM Memory Partitioned into 11 User Pages of 256 Bits (First Five Pages Compatible)
  - 64-Bit Scratchpad Buffer for Compatible Secure Writing with Offset and Individual Addressing
  - ±8kV HBM ESD Protection (typ) for IO Pin
- Efficient Secure Hash Algorithm to Authenticate Peripherals
  - FIPS 202-Compliant SHA-3 Algorithm for Challenge/Response Authentication and Device Disable
  - FIPS 198-Compliant Keyed-Hash Message Authentication Code (HMAC)
  - Optional HMAC SHA3-256 Authenticated Write Protection of EEPROM
- Supplemental Features for Easy Integration into End Applications
  - 17-Bit, One-Time Settable, Nonvolatile Decrement-Only Counter with Authenticated Read
  - Secure Storage for Secret
  - 2.25KBits of Secure EEPROM for User Data and Secret
  - Unique and Unalterable, Factory-Programmed, 64-Bit Identification Number (ROM ID)
  - Advanced 1-Wire Protocol Minimizes Interface to Single Contact
  - Standard and Overdrive Communication Speed
  - Internal Parasite Power Capacitor
  - Operating Range: 2.8V to 5.25V, -40°C to +85°C
  - SFN, SFN 6x6, TDFN-EP, TSOC, and TO92 Packages
  - 4.0µA (typ) Input Load Current

Simplified Application Diagram



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

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

19-101573; Rev 2; 9/24

Absolute Maximum Ratings

Voltage Range on Any Pin Relative to GND..... -0.5V to 6.0V
Maximum Current into Any Pin ..... -20mA to 20mA
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) ..... +250°C

Note 1: Template only. Add Note text here.

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 TSOC

Package Code	**D6+1**
Outline Number	*21-0382*
Land Pattern Number	*90-0321*
Thermal Resistance, Four-Layer Board	
Junction to Ambient (θ_{JA})	127°C/W
Junction to Case (θ_{JC})	37°C/W

3 TO-92

Package Code	**Q3+1 (Bulk), Q3+4 (T&R)**
Outline Number	*21-0248* (Bulk), *21-0250* (T&R)
Land Pattern Number	—
Thermal Resistance, Four-Layer Board:	
Junction to Ambient (θ_{JA})	N/A
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

Package Code	**T23A6N+1**
Outline Number	*21-0575*
Land Pattern Number	*90-0431*
Thermal Resistance, Four-Layer Board:	
Junction to Ambient (θ_{JA})	95.15°C/W
Junction to Case (θ_{JC})	N/A

2 SFN 6x6

Package Code	**G266N+1**
Outline Number	*21-0390*
Land Pattern Number	*90-100212*
Thermal Resistance, Four-Layer Board:	
Junction to Ambient (θ_{JA})	95.15°C/W
Junction to Case (θ_{JC})	N/A

For the latest package outline information and land patterns (footprints), go to www.analog.com/en/resources/packaging-quality-symbols-footprints/package-index.html. 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.

Electrical Characteristics

(All specifications and characteristics apply across the entire operating conditions range unless otherwise noted.)

PARAMETER	SYMBOL	CONDITIONS	MIN	TYP	MAX	UNITS
IO PIN: GENERAL DATA						
1-Wire Pull-up Voltage	V_{PUP}	System requirement	2.8		5.25	V
1-Wire Pull-up Resistance	R_{PUP}	(*Note 2*)	0.3		2.2	kΩ
Input Capacitance	C_{IO}	(*Note 2*, *Note 3*)		12		nF
Input Load Current	I_L	IO pin at V_{PUP}		4	20	µA
High-to-Low Switching Threshold	V_{TL}	(*Note 4*, *Note 5*)		0.55 x V_{PUP}		V
Input Low Voltage	V_{IL}	(*Note 6*)			0.18 x V_{PUP}	V
Low-to-High Switching Threshold	V_{TH}	(*Note 4*, *Note 7*)		0.65 x V_{PUP}		V
Switching Hysteresis	V_{HY}	(*Note 4*, *Note 8*)		0.3		V
Output Low Voltage	V_{OL}	I_{OL} = 4mA (*Note 9*)			0.4	V
IO PIN: 1-Wire INTERFACE						
Recovery Time (*Note 10*, *Note 12*)	t_{REC}	Standard speed, R_{PUP} = 2.2kΩ	5			µs
		Overdrive speed, R_{PUP} = 2.2kΩ	3			
		Overdrive speed, directly prior to reset pulse; R_{PUP} = 2.2kΩ	5			
Rising-Edge Hold-off Time	t_{REH}	Standard speed (*Note 20*)		1		µs
		Overdrive speed (*Note 20*)		N/A (0)		
	t_{SLOT}	Standard speed	65			µs

(All specifications and characteristics apply across the entire operating conditions range unless otherwise noted.)

PARAMETER	SYMBOL	CONDITIONS	MIN	TYP	MAX	UNITS
Time Slot Duration (*Note 11*)		Overdrive speed	9			
IO PIN: 1-Wire RESET, PRESENCE-DETECT CYCLE						
Reset Low Time	t_{RSTL}	Standard speed	480		640	µs
		Overdrive speed	48		80	
Presence Detect High Time (*Note 12*)	t_{PDH}	Standard speed	15		60	µs
		Overdrive speed	2		6	
Presence Detect Low Time (*Note 12*)	t_{PDL}	Standard speed	60		240	µs
		Overdrive speed	8		24	
Presence-Detect Sample Time (*Note 13*)	t_{MSP}	Standard speed	60		75	µs
		Overdrive speed	6		10	
IO PIN: 1-Wire WRITE						
Write-Zero Low Time (*Note 14*)	t_{W0L}	Standard speed	60		120	µs
		Overdrive speed	6		15.5	
Write-One Low Time (*Note 14*)	t_{W1L}	Standard speed	1		15	µs
		Overdrive speed	0.25		2	
IO PIN: 1-Wire READ						
Read Low Time (*Note 15*)	t_{RL}	Standard speed	5		15 - δ	µs
		Overdrive speed	0.25		2 - δ	
Read Sample Time (*Note 15*)	t_{MSR}	Standard speed	t_{RL} + δ		15	µs
		Overdrive speed	t_{RL} + δ		2	
STRONG PULL-UP OPERATION						
Strong Pull-up Current (*Note 16*)	I_{SPU}				3.5	mA
Strong Pull-up Voltage (*Note 16*)	V_{SPU}		1.71			V
Programming Current (*Note 16*)	i_{PROG}	Valid during t_{PROG} of Copy Scratchpad			1.2	mA
Programming Time	t_{PROG}				10	ms
Read Memory Time	t_{RM}				35	ms
Write Status Time	t_{WS}				50	ms
Write Memory Time	t_{WM}				75	ms
Computation Time	t_{CMP}				75	ms
EEPROM						
Write/Erase Cycles (Endurance)	N_{CY}	(*Note 17*)	100k			
Data Retention	t_{DR}	T_A = +85°C (*Note 18*)	25			years
POWER-UP						
Power-up Time	t_{OSCWUP}	System requirement (*Note 19*)			2	ms

Note 2: System requirement. Maximum allowable pull-up 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 typical parasite capacitance when V_{PUP} is first applied. Once the parasite capacitance is charged, it does not affect normal communication.

Note 4: V_{TL}, V_{TH}, and V_{HY} are functions of the internal supply voltage, which are functions 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 5: Voltage below which, during a falling edge on IO, a logic 0 is detected.

Note 6: The voltage on IO must be always less than or equal to V_{ILMAX} when the controller is driving IO to a logic 0 level.

Note 7: Voltage above which, during a rising edge on IO, a logic 1 is detected.

Note 8: 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 0.

Note 9: The I-V characteristic is linear for voltages less than 1V.

Note 10: System requirement. Applies to a single device attached to a 1-Wire line.

Note 11: Defines maximum possible bit rate. Equal to $1/(t_{W0LMIN} + t_{RECMIN})$.

Note 12: An additional reset or communication sequence cannot begin until the reset high time (t_{RSTH}) has expired.

Note 13: System requirement. Interval after t_{RSTL} during which a bus controller 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 it completes within 2ms after power-up.

Note 14: System requirement. ε in *Figure 5* represents the time required for the pull-up circuitry to pull the voltage on IO up from V_{IL} to V_{TH}. The actual maximum durations for the controller to pull the line low are $t_{W1LMAX} + t_F - \varepsilon$ and $t_{W0LMAX} + t_F - \varepsilon$, respectively.

Note 15: System requirement. δ in *Figure 5* represents the time required for the pull-up circuitry to pull the voltage on IO up from V_{IL} to the input-high threshold of the bus controller. The actual maximum duration for the controller to pull the line low is $t_{RLMAX} + t_F$.

Note 16: Current drawn from IO during a SPU operation interval. The pull-up 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 17: Write-cycle endurance is tested in compliance with JESD47H.

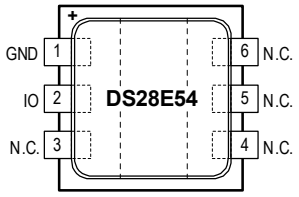
Note 18: Data retention is tested in compliance with JESD47H.

Note 19: 1-Wire communication should not take place for at least t_{OSCWUP} after V_{PUP} reaches V_{PUP} (min).

Note 20: The earliest recognition of a negative edge is possible at t_{REH} after V_{TH} has been previously reached.

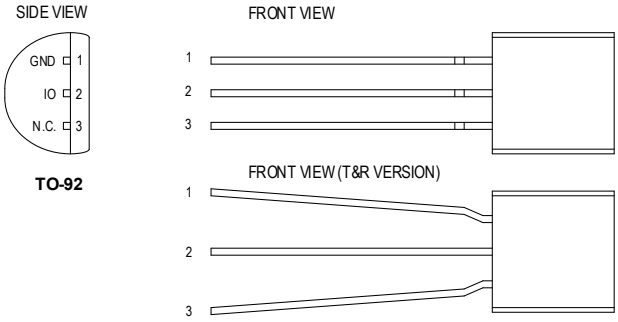
Pin Configurations

6 TSOC



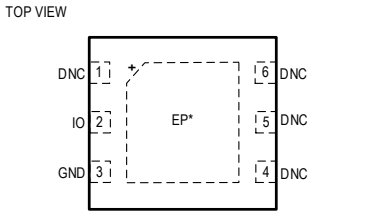
TSOC

TO-92



TO-92

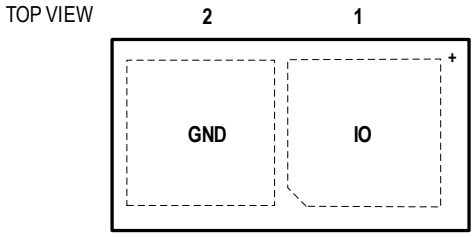
TDFN-EP



TDFN-EP
(3mm × 3mm)

*EP = EXPOSED PAD

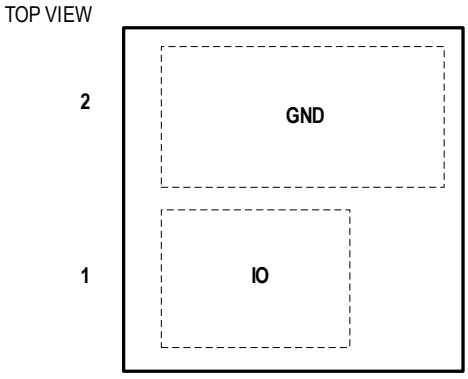
SFN



SFN
(3.5mm x 6.5mm x 0.75mm)

NOTE: THE SFN PACKAGE IS QUALIFIED FOR ELECTRO-MECHANICAL CONTACT APPLICATIONS ONLY, NOT FOR SOLDERING. FOR MORE INFORMATION, REFER TO THE "ATTACHMENT METHODS FOR ELECTRO-MECHANICAL 1-Wire Contact PACKAGE" APPLICATION NOTE.

SFN 6x6



SFN
(6mm x 6mm x 0.9mm)

NOTE: THE SFN PACKAGE IS QUALIFIED FOR ELECTRO-MECHANICAL CONTACT APPLICATIONS ONLY, NOT FOR SOLDERING. FOR MORE INFORMATION, REFER TO THE "ATTACHMENT METHODS FOR ELECTRO-MECHANICAL 1-Wire CONTACT PACKAGE" APPLICATION NOTE.

Pin Descriptions

PIN					NAME	FUNCTION
TSOC	TO-92	TDFN-EP	SFN	SFN 6X6		
3, 4, 5, 6	3	1, 4, 5, 6	—	—	N.C.	Not Connect
2	2	2	1	1	IO	1-Wire IO
1	1	3	2	2	GND	Ground. Connect all contacts to ground.
—	—	—	—	—	EP	Exposed Pad (TDFN only). Solder evenly to the board's ground plane for proper operation. Refer to the *Exposed Pads: A Brief Introduction* application note for additional information.

Detailed Description

Overview

The DS28E54 integrates the Analog Devices' DeepCover® capability to protect all device-stored data from invasive discovery. In addition to the SHA-3 engine for signatures, the DS28E54 includes 2.25Kbit 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. See the block diagram in *Figure 1*.

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

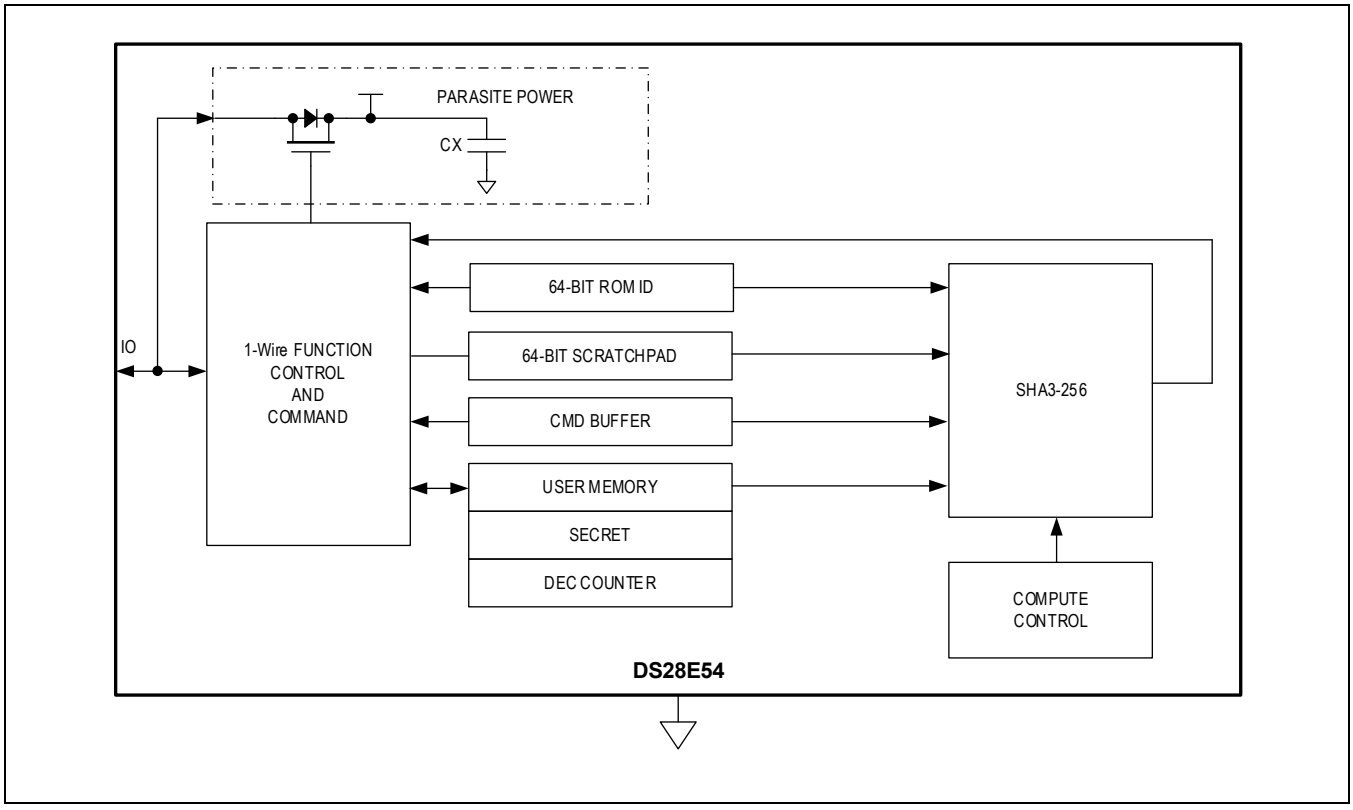


Figure 1. Block Diagram

Memory

A secured 2.25Kbit EEPROM array is configured to provide five pages of DS2431/DS28E07 compatible memory and six pages for SHA3-256 and decrement counter features.

Table 1. Memory Map

PAGE	STARTING ADDRESS TA2 TA1	SIZE (BYTES)	REGION	MEMORY TYPE	DEFAULT PROTECTION	CONFIGURABLE PROTECTION	DS2431/DS28E07 COMPATIBLE
0	0000h	32	User page	EE**	—	WP, EM*	Yes
1	0020h	32	User page	EE	—		Yes
2	0040h	32	User page	EE	—		Yes
3	0060h	32	User page	EE	—		Yes
4	0080h	32	Configuration	EE	—	Individual bytes auto WP depending on value	Yes
5	00A0h	32	Refer to the *DS28E54 Security User's Guide*				

6	00C0h	32	
7	00E0h	32	
8	0100h	32	
9	0120h	32	
10	0140h	32	

**All protection is write once.*

***Electrically erasable programmable memory.*

Table 2. Protect Types

PROTECTION	DESCRIPTION
RP	Read protect
WP	Write protect
EM	EPROM emulation (only set bits to 0)
Refer to the *DS28E54 Security User's Guide*	

Each DS28E54 contains a unique, 64-bit long ROM_ID. The ROM_ID is a fundamental input parameter for most cryptographic operations. The first 8 bits are a 1-Wire family code (2Dh). 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 2* for details. The 1-Wire CRC is generated using a polynomial generator consisting of a shift register and XOR gates. The polynomial is $x^8 + x^5 + x^4 + 1$. Additional information about the 8-bit 1-Wire CRC is available in the *Understanding and Using Cyclic Redundancy Checks with Maxim 1-Wire and iButton Products* application note.

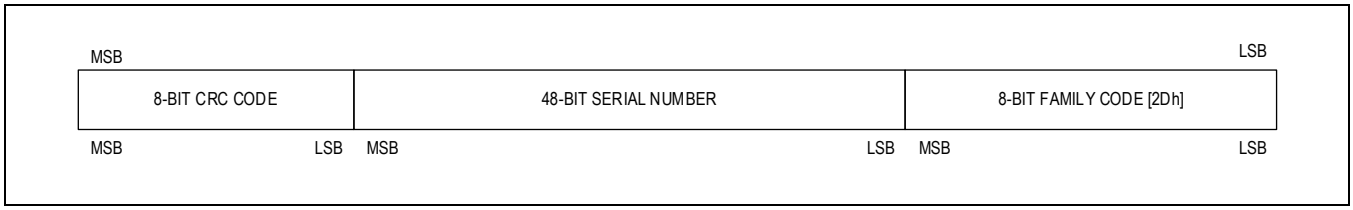


Figure 2. 64-Bit ROMID

Configuration Page

The configuration page 4 contains the DS2431/DS28E07 backward-compatible protection bytes, optional manufacturer ID, and device flavor. The protection byte behavior is described in the following table:

Table 3. Configure Page 4 for User Pages 0 to 3

ADDRESS	DESCRIPTION	WRITE BEHAVIOR	READ BEHAVIOR	OTHER BEHAVIOR
0080h	Protection Control Byte Page 0	Write 55h	55h	Locks byte, set (WP) write protection on page 0.
		Write AAh	AAh	Locks byte, set (EM) EPROM mode protection on page 0.
		All other values	Value stored	—
0081h	Protection Control Byte Page 1	Write 55h	55h	Locks byte, set (WP) write protection on page 1.
		Write AAh	AAh	Locks byte, set (EM) EPROM mode protection on page 1.

		All other values	Value stored	—
0082h	Protection Control Byte Page 2	Write 55h	55h	Locks byte, set (WP) write protection on page 2.
		Write AAh	AAh	Locks byte, set (EM) EPROM mode protection on page 2.
		All other values	Value stored	—
0083h	Protection Control Byte Page 3	Write 55h	55h	Locks byte, set (WP) write protection on page 3.
		Write AAh	AAh	Locks byte, set (EM) EPROM mode protection on page 3.
		All other values	Value stored	—
0084h	Copy Protection Byte	Write 55h	55h	Locks 0080h-008Fh. Any pages with no protection set have protection (NONE) set.
		Write AAh	AAh	
		All other values	Value stored	—
0085h	Factory Byte. Set at factory.	N/A	55h	Address 0086h and 0087h NOT write protected.
		N/A	AAh	Address 0086h and 0087h write protected.
0086h to 0087h	User Byte/Manufacturer ID	See 0085h factory byte.		
0088h to 008Dh	Reserved	No writes	N/A	Reserved locations, value may vary.
008Eh	Flavor	No writes	FXXXXXXXb	Bit7, flavor ‘F’ = 1 for DS28E54 and 0 for DS2431/DS28E07
0008Fh	Reserved	No writes	N/A	Reserved locations, value may vary.
0090h to 009Fh	Reserved	No writes	FFh	Always reads FFh.

1-Wire Bus System

The 1-Wire bus is a system with a single bus controller and one or more peripherals. In all instances, the DS28E54 is a peripheral device. The bus controller 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 initiated on the falling edge of sync pulses from the bus controller.

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 DS28E54 is open drain with an internal circuit equivalent.

A multidrop bus consists of a 1-Wire bus with multiple peripherals attached. The DS28E54 supports both standard and overdrive communication speeds of 11.7kbps (max) and 62.5kbps (max), respectively. The value of the pull-up resistor primarily depends on the network size and load conditions. The DS28E54 requires a pull-up resistor of 2.2kΩ (max) at any speed (*Figure 3*).

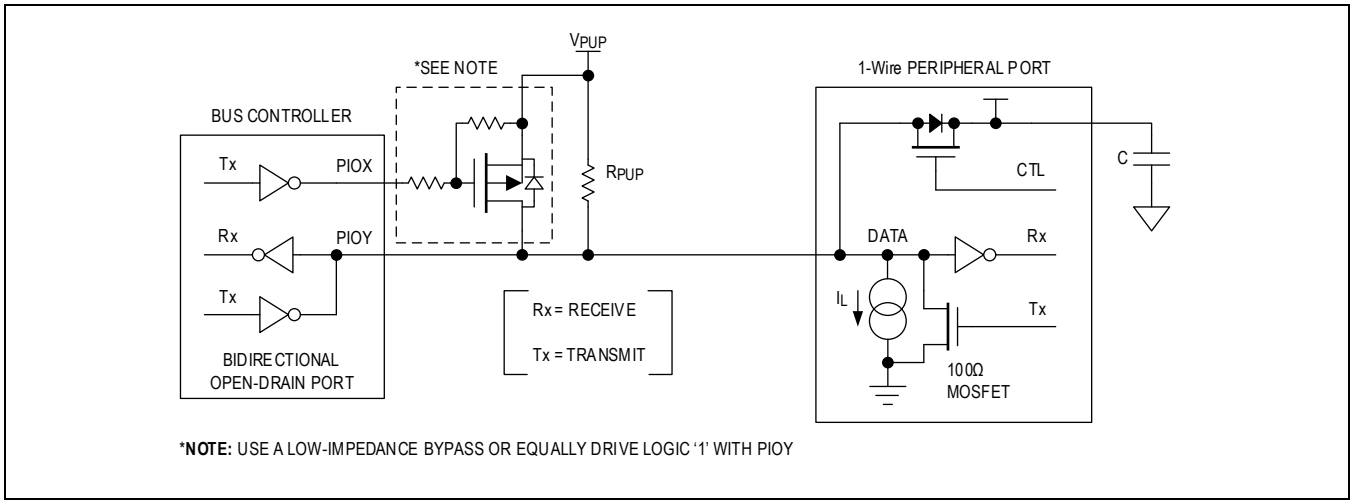


Figure 3. Hardware Configuration

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 15.5µs (overdrive speed) or more than 120µs (standard speed), one or more devices on the bus can be reset.

Transaction Sequence

The protocol for accessing the DS28E54 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 controller, followed by presence pulse(s) transmitted by the peripheral(s). The presence pulse lets the bus controller know that the DS28E54 is on the bus and is ready to operate. For more details, see the *1-Wire Signaling and Timing* section.

1-Wire Signaling and Timing

The DS28E54 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 controller initiates all falling edges. The DS28E54 can communicate at two speeds: standard and overdrive. If not explicitly set into the overdrive mode, the DS28E54 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 4* as ε, and its duration depends on the pull-up resistor (R_{PUP}) used and the capacitance of the 1-Wire network attached. The voltage V_{ILMAX} is relevant for the DS28E54 when determining a logical level, not triggering any events.

Figure 4 shows the initialization sequence required to begin any communication with the DS28E54. A reset pulse followed by a presence pulse indicates that the DS28E54 is ready to receive data, given the correct ROM and device function command. If the bus controller 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 DS28E54 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 controller releases the line, it goes into the receive mode. Then, the 1-Wire bus is pulled to V_{PUP} through the pull-up resistor or, in the case of a special driver chip, through the active circuitry. Next, the 1-Wire bus is pulled to V_{PUP} through the pull-up resistor. When the threshold V_{TH} is crossed, the DS28E54 waits and then transmits a presence pulse by pulling the line low. To detect a presence pulse, the controller must test the logical state of the 1-Wire line at t_{MSP}.

Immediately after t_{RSTH} expires, the DS28E54 is ready for data communication. In a mixed-population network, t_{RSTH} should be extended to a minimum of 480µs at standard speed and 48µs at overdrive speed to accommodate other 1-Wire devices.

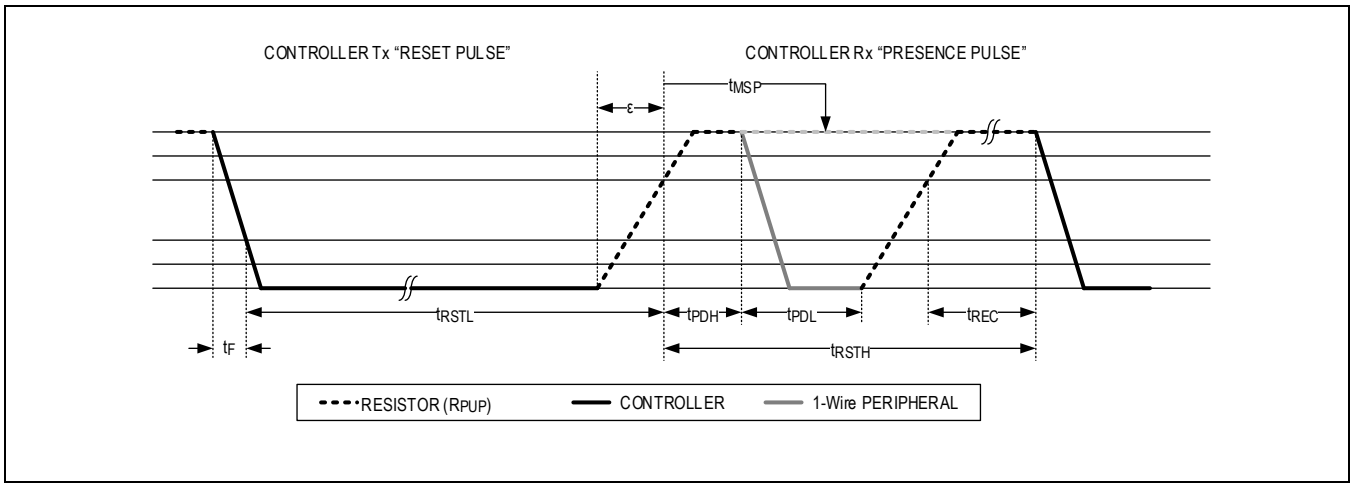


Figure 4. Initialization Procedure: Reset and Presence Pulse

Read/Write Time Slots

Data communication with the DS28E54 takes place in time slots that carry a single bit each. Write time slots transport data from the bus controller to peripheral. Read time slots transfer data from the peripheral to controller. *Figure 5* illustrates the definitions of the write and read time slots.

All communication begins with the controller pulling the data line low. As the voltage on the 1-Wire line falls below the threshold V_{TL}, the DS28E54 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.

Controller to Peripheral

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} expires. 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} expires. For 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 is crossed, the DS28E54 needs a recovery time t_{REC} before it is ready for the next time slot.

Peripheral to Controller

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} expires. During the t_{RL} window, when responding with a 0, the DS28E54 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 DS28E54 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 DS28E54 on the other side define the peripheral sampling window (t_{MSRMIN} to t_{MSRMAX}), in which the controller must perform a read from the data line. For the most reliable communication, t_{RL} should be as short as permissible, and the controller should read close to, but no later than t_{MSRMAX}. After reading from the data line, the peripheral must wait until t_{SLOT} expires. This guarantees sufficient recovery time t_{REC} for the DS28E54 to get ready for the next time slot. Note that t_{REC} specified herein applies only to a single DS28E54 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 pull-up during the 1-Wire recovery time, such as the special 1-Wire line drivers, can be used.

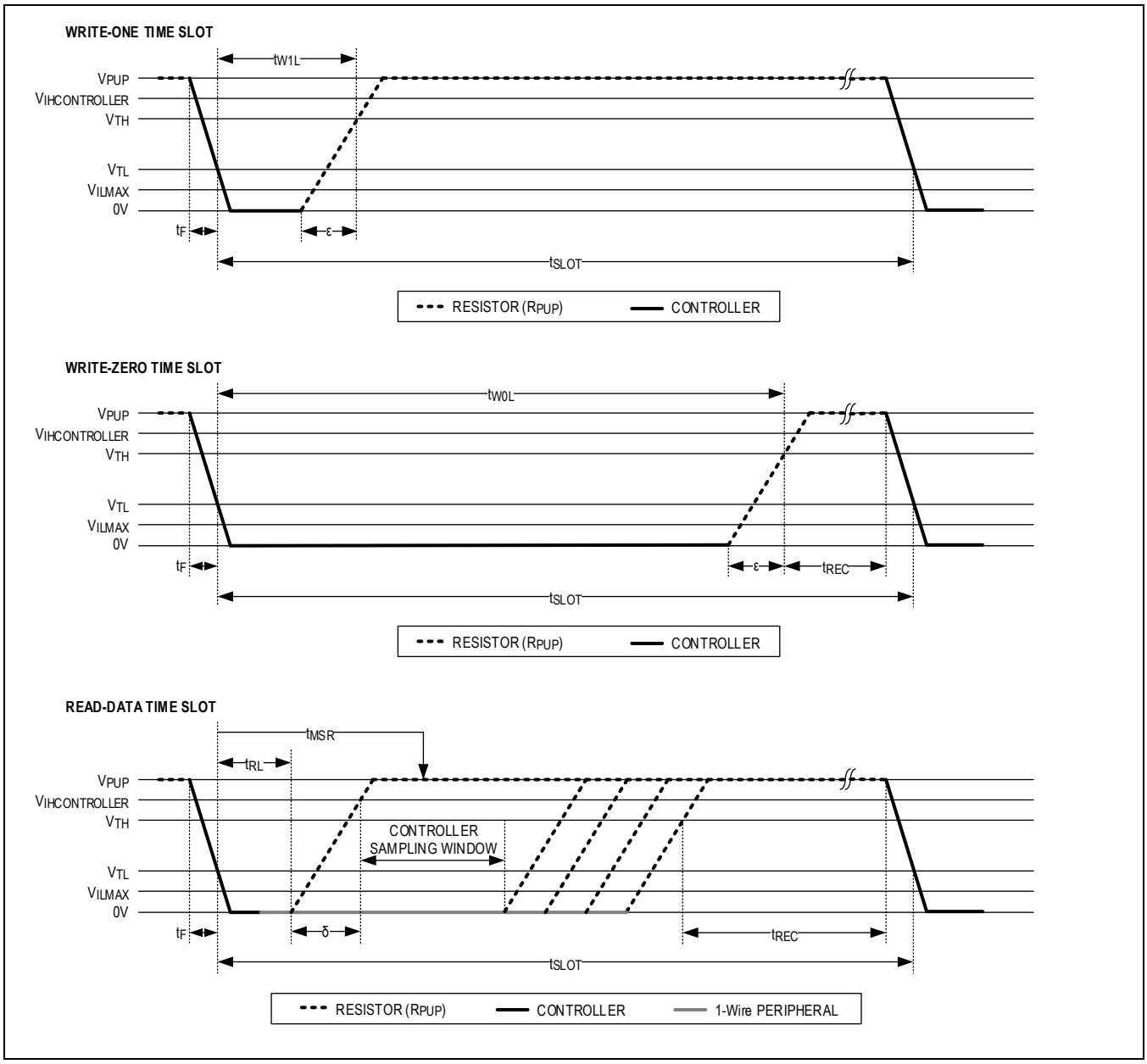


Figure 5. Read/Write Timing Diagrams

1-Wire ROM Commands

Once the bus controller detects a presence, it can issue one of the seven ROM function commands that the DS28E54 supports. All ROM function commands are 8 bits long. For operational details, see *Figure 6* and *Figure 7*. A descriptive list of these ROM function commands follows in the subsequent sections and the commands are summarized in *Table 4*.

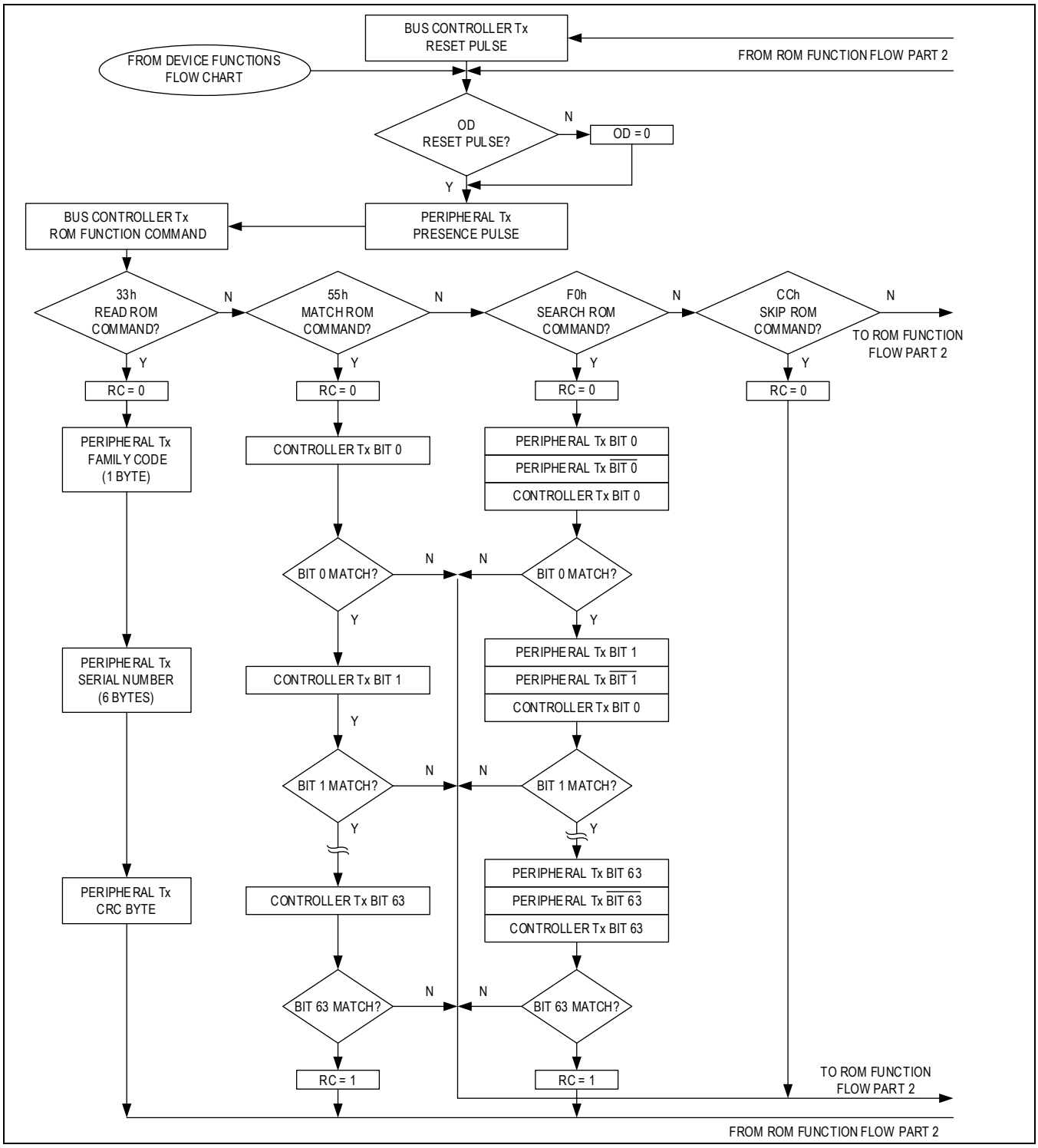


Figure 6. ROM Function Flow, Part 1

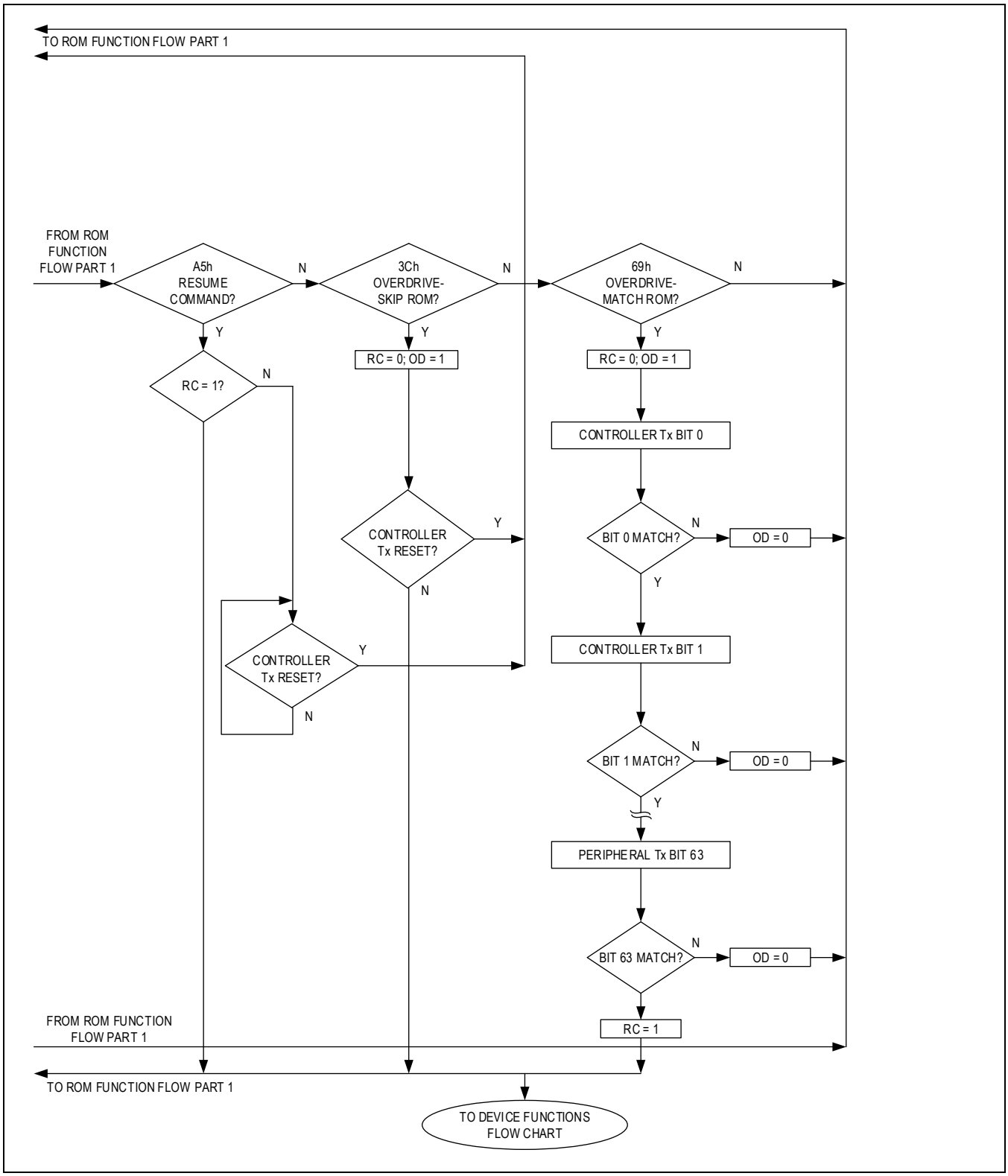


Figure 7. ROM Function Flow, Part 2

Table 4. 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.
Overdrive Skip ROM	3Ch	Put all devices in overdrive.
Overdrive Match ROM	69h	Put the device with the ROM in overdrive.

Search ROM [F0h]

When a system is initially brought up, the bus controller 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 controller can use a process of elimination to identify the ID of all peripheral devices. For each bit in the ID number, starting with the least significant bit, the bus controller issues a triplet of time slots. On the first slot, each peripheral device participating in the search outputs the true value of its ID number bit. On the second slot, each peripheral device participating in the search outputs the complemented value of its ID number bit. On the third slot, the controller writes the true value of the bit to be selected. All peripheral devices that do not match the bit written by the controller stop participating in the search. If both of the read bits are 0, the controller knows that peripheral devices exist with both states of the bit. By choosing which state to write, the bus controller branches in the search tree. After one complete pass, the bus controller knows the ROM ID number of a single device. Additional passes identify the ID numbers of the remaining devices. Refer to the *1-Wire Search Algorithm* application note for a detailed discussion, including an example.

Read ROM [33h]

The Read ROM command allows the bus controller to read the DS28E54'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 peripheral on the bus. If more than one peripheral is present on the bus, a data collision occurs when all peripherals 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 controller to address a specific DS28E54 on a multidrop bus. Only the DS28E54 that exactly matches the 64-bit ROM sequence responds to the subsequent device function command. All other peripherals 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 controller to access the device functions without providing the 64-bit ROM ID. If more than one peripheral 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 peripherals transmit simultaneously (open-drain pull-downs 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, 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 controller to access the device functions without providing the 64-bit ROM ID. Unlike the normal Skip ROM command, the Overdrive-Skip ROM command sets the DS28E54 into 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 peripheral 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 peripherals transmit simultaneously (open-drain pull-downs 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 controller to address a specific DS28E54 on a multidrop bus and to simultaneously set it into overdrive mode. Only the DS28E54 that exactly matches the 64-bit ROM sequence responds to the subsequent device function command. Peripherals already in overdrive mode from a previous Overdrive-Skip ROM or successful Overdrive-Match ROM command remain in overdrive mode. All overdrive-capable peripherals 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.

Improved Network Behavior

In a 1-Wire environment, line termination is possible only during transients controlled by the bus controller (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 peripheral device to lose synchronization with the controller 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 DS28E54 uses a 1-Wire front end that is less sensitive to noise. The IO 1-Wire front-end has hysteresis, and a rising edge hold off delay.

- On the low-to-high transition, if the line rises above V_{TH} but does not go below V_{TL}, the glitch is filtered (*Figure 8*, Case A).
- The rising edge hold-off delay (standard speed, nominally 1µs), t_{REH}, filters glitches that go below V_{TL} before t_{REH} expires (*Figure 8*, Case B). Effectively, the device does not see the initial rise, and the t_{REH} delay resets when the line goes below V_{TL}.
- If the line goes below V_{TL} after t_{REH} expires, the glitch is not filtered and is taken as the beginning of a new time slot (*Figure 8*, Case C).

Independent of the time slot, the falling edge of the presence pulse has a controlled slew rate to reduce ringing.

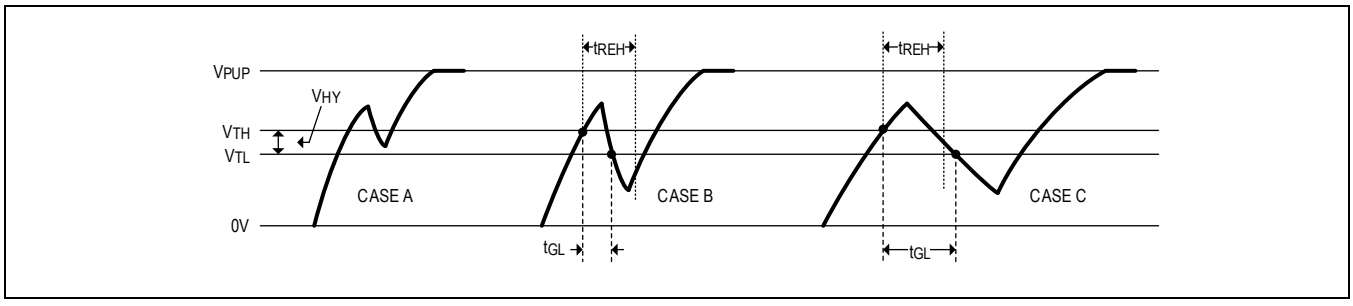


Figure 8. Noise Suppression Scheme

Device Function Commands

After a 1-Wire Reset/Presence cycle and ROM function command sequence are successful, a device function command can be accepted. The DS28E54 provides the standard DS2431/DS28E07 compatible commands. Additionally, new SHA-3 commands are provided for authentication (refer to the *DS28E54 Security User's Guide*). Data transfer is verified when writing and reading by a CRC of the 16-bit type (CRC-16). The CRC-16 is computed as described in the Understanding and *Using Cyclic Redundancy Checks with Maxim 1-Wire and iButton Products* application note.

Table 5. Device Function Compatibility Command Summary

COMMAND	CODE	DESCRIPTION
Read Memory	F0h	Read memory.
Write Scratchpad	0Fh	Write data to scratchpad buffer.
Read Scratchpad	AAh	Read data from scratchpad buffer.
Copy Scratchpad	55h	Copy data from scratchpad buffer to EE.

Compatibility Commands

The DS2431/DS28E07 compatibility commands operate only on memory pages 0 to 4.

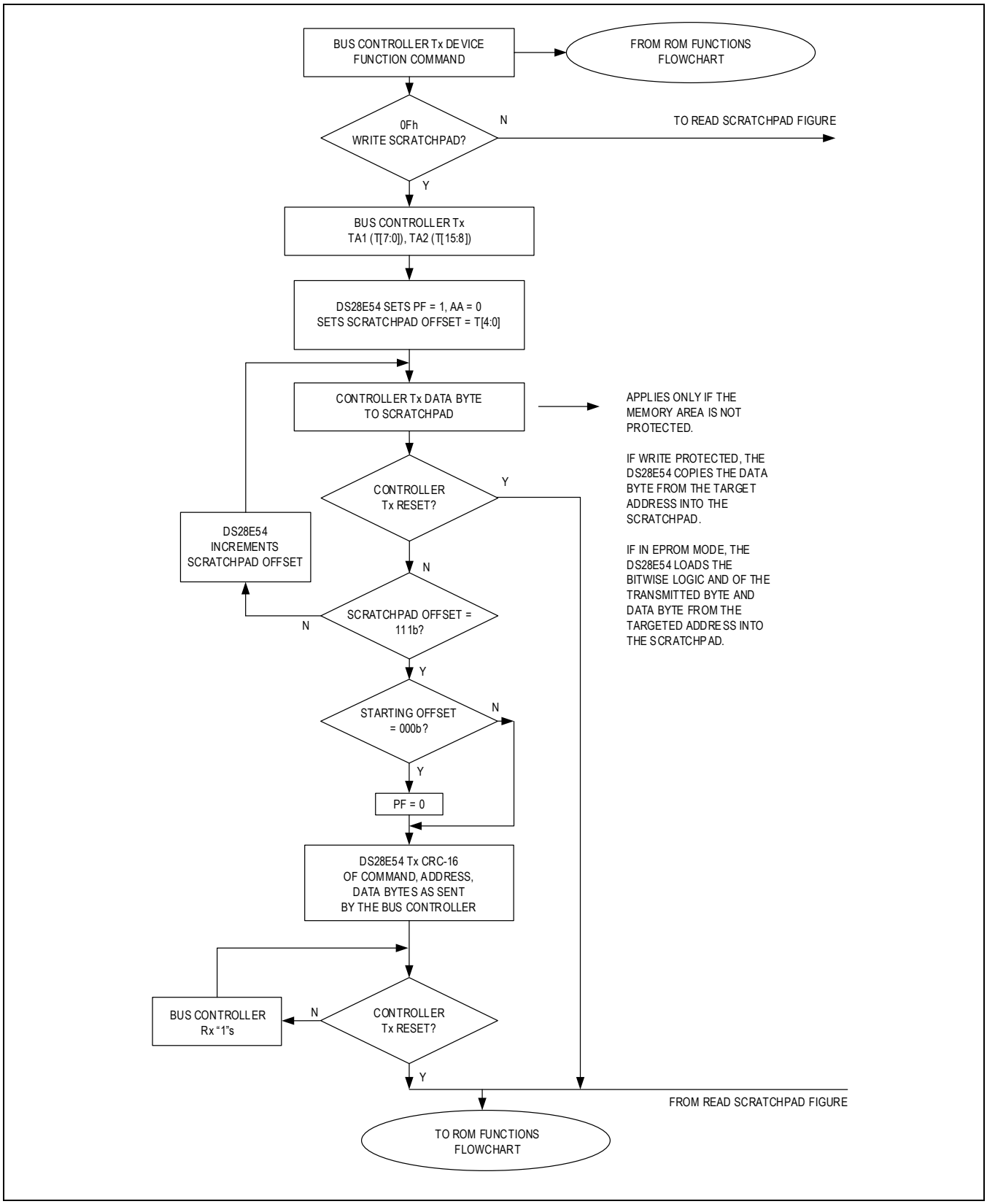


Figure 9. Compatibility Command Write Scratchpad

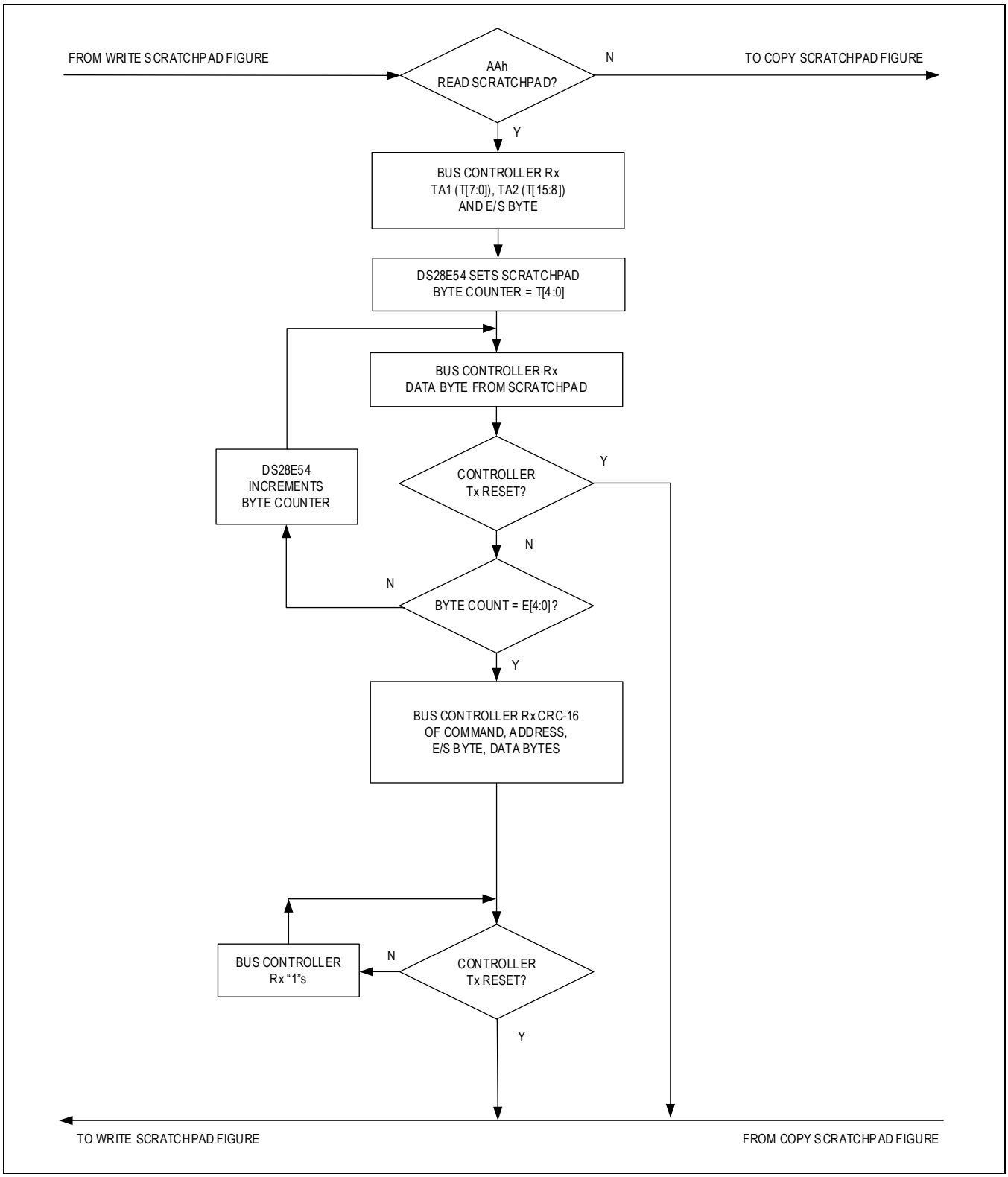


Figure 10. Compatibility Command Read Scratchpad

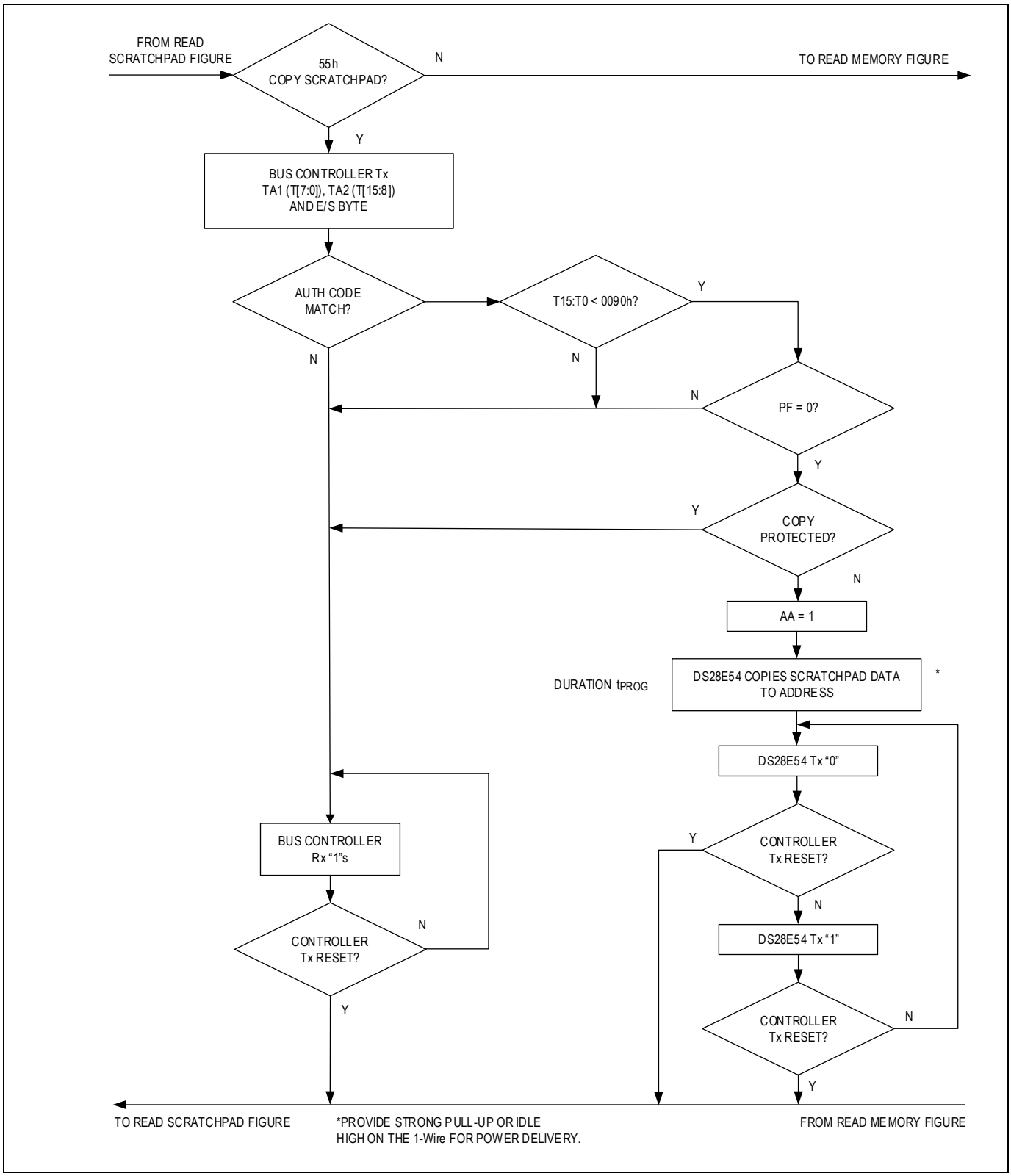


Figure 11. Compatibility Command Copy Scratchpad

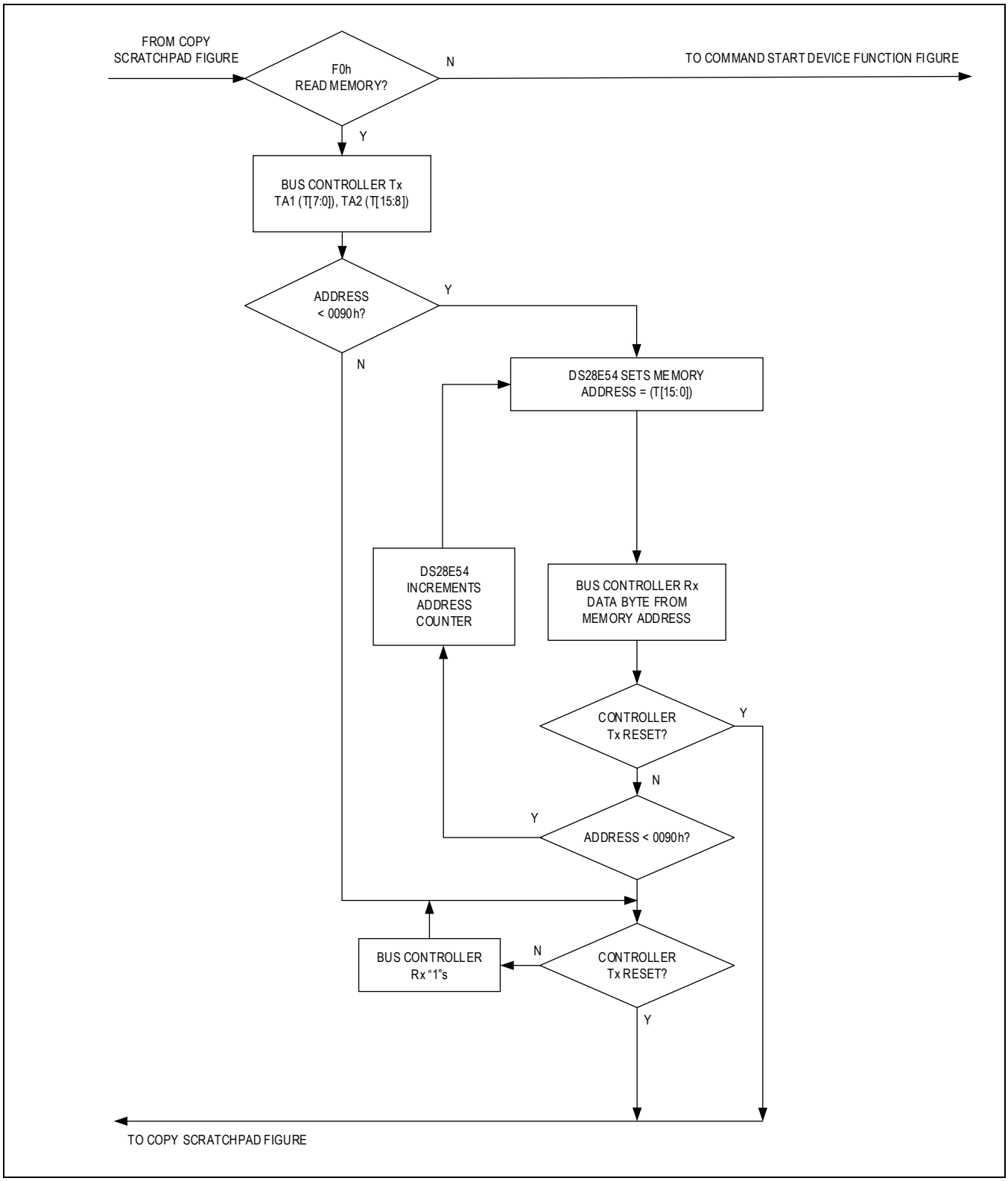


Figure 12. Compatibility Command Read Memory

Write Scratch Pad (0Fh)

The Write Scratchpad command loads data to the scratchpad so it can be subsequently copied to the EEPROM. After the command code, the controller provides the 2-byte target address, followed by the data to write to the scratchpad. The data is written to the scratchpad starting at byte offset (T2:T0). The ending offset (E2:E0) is the byte offset at which the controller stops writing data. Only full data bytes are accepted. To be valid for a copy, full 8 bytes of scratchpad data must be written from starting offset T2:T0 = 000b to ending offset E2:E0 = 111b.

When executing the Write Scratchpad command, the CRC generator inside the DS28E54 calculates a CRC over the entire data stream, starting at the command code and ending at the last data byte sent by the controller. Incomplete bytes are not computed in the CRC. This CRC is generated using the CRC-16 polynomial by first clearing the CRC generator and then shifting in the command code (0FH) of the Write Scratchpad command, the target addresses TA1 and TA2 as supplied by the controller, and all of the data bytes. The controller can end the Write Scratchpad command at any time. However, if the ending offset is 111b, the controller can send 16 read time slots and receive the CRC that is generated by the DS28E54.

The Write Scratchpad command accepts invalid addresses, but subsequent Copy Scratchpad commands are blocked.

If a Write Scratchpad command is attempted to a write-protected location, the scratchpad is loaded with the data already existing in memory rather than the data transmitted. Similarly, if the target address page is in EPROM mode, the scratchpad is loaded with the bitwise logical AND of the transmitted data and data already existing in memory.

Table 6. Target Address (TA1)

BIT 7	BIT 6	BIT 5	BIT 4	BIT 3	BIT 2	BIT 1	BIT 0
T7	T6	T5	T4	T3	T2	T1	T0

Bits 7:0: Target Address (T). 8 least significant bits for target address.

Table 7. Target Address (TA2)

BIT 7	BIT 6	BIT 5	BIT 4	BIT 3	BIT 2	BIT 1	BIT 0
T15	T14	T13	T12	T11	T10	T9	T8

Bits 7:0: Target Address (T). 8 most significant bits for target address.

Table 8. Ending Address with Data Status (E/S) (Read Only)

BIT 7	BIT 6	BIT 5	BIT 4	BIT 3	BIT 2	BIT 1	BIT 0
AA	0	PF	0	0	E2	E1	E0

Bits 7: Authorization Accepted (AA). Flag to indicate data stored in scratchpad is already copied to memory.

Bits 5: Partial Flag (PF). Flag to indicate the scratchpad is not valid because it is partial.

Bits 2:0: Ending Offset (E). 3 least significant bits of the end address.

Table 9. Write Scratchpad Command

WRITE SCRATCHPAD	
Command Code	0Fh
Parameter Byte(s)	TA1, TA2 target address and data.
Usage	Write Scratchpad for DS2431/DS28E07 compatibility.
Command Restrictions	To be valid for a copy, a full 8 bytes of scratchpad data must be written from starting offset T2:T0 = 000b to ending offset E2:E0 = 111b, and the target must be in the compatibility memory pages 0 to 4. This function continues to work on a disabled device.
Device Operation	Update target address. Update scratchpad data. Update the ES byte. Optionally, send the CRC-16 if ending offset is 111b.
Command Duration	N/A
Result Byte	N/A

Table 10. Write Scratchpad Sequence

Reset
Presence Pulse
<ROM Select>
Tx: Command 0Fh (Write Scratchpad)
Tx: TA1
Tx: TA2
Tx: Data (up to 8d bytes)
Rx: CRC-16 when E[4:0] = 111b (command, address, data)
Reset

Read ScratchPad (AAh)

This command verifies scratchpad data and target address. The first two bytes read are the target address. The next byte is the ending offset/data status byte (E/S), followed by the scratchpad data beginning at the byte offset (T4:T0). The data follows. Reading beyond the data results in reading an inverted CRC-16 of the target address, ending offset flag byte, and data. See the command flow in *Figure 10*.

Table 11. Read Scratchpad Command

READ SCRATCHPAD	
Command Code	AAh
Parameter Byte(s)	None
Usage	Read Scratchpad for DS2431/DS28E07 compatibility. Scratchpad TA1, TA2, ES, and data are read, followed by CRC-16.
Command Restrictions	Scratchpad data must first be written to be valid. This function continues to work on a disabled device.

READ SCRATCHPAD	
Device Operation	Read target address. Read ending offset and flags. Read data. Send the inverted CRC-16 after data.
Command Duration	N/A
Result Byte	N/A

Table 12. Read Scratchpad Sequence

Reset
Presence Pulse
<ROM Select>
Tx: Command AAh (Read Scratchpad)
Rx: TA1
Rx: TA2
Rx: E/S
Rx: Data (up to 8d bytes)
Rx: CRC-16 Byte Counter = E[2:0] ([command, TA1, TA2, E/S, data])
Reset

Copy Scratchpad (55h)

The Copy Scratchpad command copies data from the scratchpad to the DS2431/DS28E07 compatibility memory. After issuing the Copy Scratchpad command, the controller must provide a 3-byte authorization pattern, which can be obtained by an immediately preceding Read Scratchpad command. This 3-byte pattern must exactly match the data contained in the three address registers (TA1, TA2, E/S, in that order). If the pattern matches, the target address is valid, PF flag is not set, target memory is not copy protected, AA flag is set, and copy begins. All 8 bytes of scratchpad contents are copied to the target memory location. The duration of the device's internal data transfer is t_{PROG}, during which the voltage on the 1-Wire bus must not fall below V_{SPU} minimum. The best practice is to generate a strong pull-up that turns on after the Copy Scratchpad sequence for the duration of t_{PROG} to enhance power delivery. A pattern of alternating 0s and 1s are transmitted after the data is copied until the controller issues a reset pulse. If the PF flag is set or the target memory is copy protected, the copy does not begin, and the AA flag is not set.

The data to be copied is determined by the three address registers. The scratchpad data from the beginning offset through the ending offset is copied to memory, starting at the target address. Anywhere from 1 to 8 bytes can be copied to memory with this command. See the command flow in *Figure 11*.

Table 13. Copy Scratchpad Command

COPY SCRATCHPAD	
Command Code	55h
Parameter Byte(s)	TA1, TA2 target address, and ES byte. Must match scratchpad TA1, TA2, and ES values.
Usage	Copy Scratchpad for DS2431/DS28E07 compatibility. Copies 8 bytes of scratchpad data to the targeted memory location.

COPY SCRATCHPAD	
Command Restrictions	The target must be in the compatibility memory pages 0 to 4. The page must not be write-protected. The scratchpad must not be partial. This function continues to work on a disabled device.
Device Operation	Verify the destination address and E/S. Copy scratchpad data to memory. Set AA flag. Read alternating 1's and 0's toggle.
Command Duration	t_{PROG}
Result Byte	N/A

Table 14. Copy Scratchpad Sequence

Reset
Presence Pulse
<ROM Select>
Tx: Command 55h (Copy Scratchpad)
Tx: TA1
Tx: TA2
Tx: E/S
<Strong pull-up delay, t_{PROG}>
Rx: AAh Toggle loop (01b…)
Reset

Read Memory (F0h)

The Read Memory command reads compatibility memory starting at the provided address. Data can be read to the end of compatibility memory (page 4). See the command flow in *Figure 12*.

Table 15. Read Memory Command

READ MEMORY	
Command Code	F0h
Parameter Byte(s)	TA1 and TA2 starting address for read. TA1 is the lower address byte. TA2 is the upper address byte.
Usage	Read Memory for DS2431/DS28E07 compatibility.
Command Restrictions	Only compatibility memory pages 0 to 4 can be read using this command. This function continues to work on a disabled device.
Device Operation	Read out pages 0 to 4 data. When reading beyond page 4, read FFh.
Command Duration	N/A
Result Byte	N/A

Table 16. Read Memory Sequence

Reset
Presence Pulse
<ROM Select>
Tx: Command F0h (Read Memory)
Tx: TA1
Tx: TA2
Rx: Data (up to end of page 4 followed by FFh's)
Reset

Ordering Information

PART NUMBER	TEMP RANGE	PIN-PACKAGE
DS28E54P+	-40°C to +85°C	6 TSOC
DS28E54P+T	-40°C to +85°C	6 TSOC (4k pcs)
DS28E54+	-40°C to +85°C	3 TO-92
DS28E54+T	-40°C to +85°C	3 TO-92
DS28E54Q+U	-40°C to +85°C	6 TDFN-EP
DS28E54Q+T	-40°C to +85°C	6 TDFN-EP (2.5pcs)
DS28E54GA+U	-40°C to +85°C	2 SFN (3.5mm x 6.5mm)
DS28E54GA+T	-40°C to +85°C	2 SFN (3.5mm x 6.5mm) (2.5k pcs)
DS28E54G+U	-40°C to +85°C	2 SFN (6mm x 6mm)
DS28E54G+T	-40°C to +85°C	2 SFN (6mm x 6mm) (2.5k pcs)

Note: *The leads of TO-92 packages on tape and reel are formed to approximately 100-mil (2.54mm) spacing. For details, refer to the package outline drawing.*

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

T Denotes tape-and-reel.

Revision History

REVISION NUMBER	REVISION DATE	DESCRIPTION	PAGES CHANGED
0	6/22	Initial release	—
1	6/23	Added 6x6 SFN package; updated temperature range; updated Ordering Information table	1, 3–5, 8, 9, 31
2	9/24	Added iPROG parameter	4