*Click here for production status of specific part numbers.*

# DS28C50

# DeepCover® I²C Secure SHA-3 Authenticator with ChipDNA PUF Protection

## General Description

The DS28C50 secure authenticator combines FIPS202-compliant secure hash algorithm (SHA-3) challenge and response authentication with Maxim's patented ChipDNA™ technology, a physically unclonable function (PUF) to provide a cost-effective solution with the ultimate protection against security attacks. The ChipDNA implementation utilizes the random variation of semiconductor device characteristics that naturally occur during wafer fabrication. The ChipDNA circuit generates a unique output value that is repeatable over time, temperature, and operating voltage. Attempts to probe or observe ChipDNA operation modifies the underlying circuit characteristics, thus preventing discovery of the unique value used by the chip cryptographic functions. The DS28C50 utilizes the ChipDNA output as key content to cryptographically secure all device-stored data. With ChipDNA capability, the device provides a core set of cryptographic tools derived from integrated blocks including a SHA-3 engine, a FIPS/NIST compliant true random number generator (TRNG), 2Kb of secured EEPROM, a decrement-only counter and a unique 64-bit ROM identification number (ROM ID). The unique ROM ID is used as a fundamental input parameter for cryptographic operations and serves as an electronic serial number within the application. The DS28C50 communicates over a I²C network.

## Applications

- Authentication of Medical Sensors and Tools
- Secure Management of Limited Use Consumables
- IoT Node Crypto-Protection
- Accessory and Peripheral Secure Authentication
- Printer Cartridge Identification and Authentication

## Benefits and Features

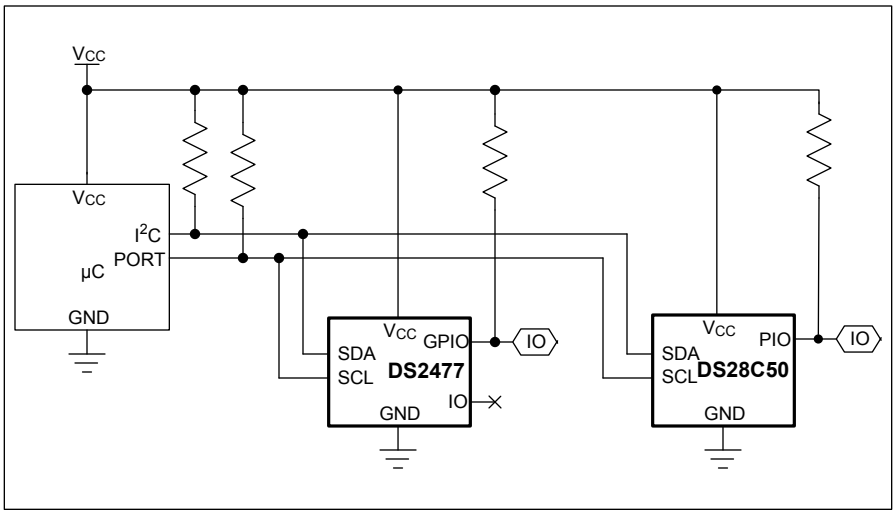
- Robust Countermeasures Protect Against Security Attacks
  - Patented Physically Unclonable Function Secures Device Data
  - Actively Monitored Die Shield Detects and Reacts to Intrusion Attempts
  - All Stored Data Cryptographically Protected from Discovery
- Efficient Secure Hash Algorithm Authenticates Peripherals
  - FIPS 202-Compliant SHA-3 Algorithm for Challenge/Response Authentication
  - FIPS 198-Compliant Keyed-Hash Message Authentication Code (HMAC)
  - TRNG with NIST SP 800-90B Compliant Entropy Source
- Supplemental Features Enable Easy Integration into End Application
  - 17-Bit One-Time Settable, Nonvolatile Decrement Only Counter with Authenticated Read
  - One GPIO Pin with Optional Authentication Control
  - 2Kb of EEPROM for User Data, Key, and Control Registers
  - Unique and Unalterable Factory Programmed 64-Bit Identification Number (ROM ID)
  - Operating Range: 3.3V ±10%, -40°C to +85°C
  - 6-Pin TDFN-EP Package (3mm x 3mm)
  - I²C Communication, Up to 1MHz

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



*19-100643; Rev 0; 9/19*

## Typical Application Circuit



# TABLE OF CONTENTS

General Description . . . 1
Applications . . . 1
Benefits and Features . . . 1
Typical Application Circuit . . . 2
Absolute Maximum Ratings . . . 5
Package Information . . . 5
6 TDFN-EP . . . 5
Electrical Characteristics . . . 5
Pin Configuration . . . 8
6 TDFN-EP . . . 8
Pin Description . . . 8
Detailed Description . . . 9
Design Resource Overview . . . 9
Memory Description . . . 9
Open-Drain GPIO . . . 9
Decrement Counter . . . 10
I2C . . . 10
General Characteristics . . . 10
Slave Address . . . 10
I2C Definitions . . . 11
Bus Idle or Not Busy . . . 11
START Condition . . . 11
STOP Condition . . . 11
Repeated START Condition . . . 11
Data Valid . . . 11
Ordering Information . . . 13
Revision History . . . 14

## LIST OF FIGURES

Figure 1. Block Diagram . . . . . 9
Figure 2. I2C Protocol Overview . . . . . 10
Figure 3. I2C Slave Address . . . . . 11
Figure 4. I2C Timing Diagram . . . . . 12

## Absolute Maximum Ratings

Voltage Range on Any Pin Relative to GND ..... -0.5V to 4.0V
Maximum Current into Any Pin..... -20mA to 20mA
Operating Temperature Range.....-40°C to 85°C
Lead Temperature (soldering, 10s).....+300°C

## 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 ($\theta_{JA}$) | 55ºC/W |
| Junction to Case ($\theta_{JC}$) | 9ºC/W |
| **Thermal Resistance, Four-Layer Board:** | |
| Junction to Ambient ($\theta_{JA}$) | 42ºC/W |
| Junction to Case ($\theta_{JC}$) | 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/or $T_A$ = +85°C. Limits over the operating temperature range and relevant supply voltage range are guaranteed by design and characterization. Typical values are not guaranteed.)

| PARAMETER | SYMBOL | CONDITIONS | MIN | TYP | MAX | UNITS |
|---|---|---|---|---|---|---|
| Supply Voltage | $V_{CC}$ | (*Note 1*) | 2.97 | 3.3 | 3.63 | V |
| Supply Current | $I_{CC}$ | Standby | | | 400 | µA |
| | | Communicating/Active | | | 10 | mA |
| **I²C SCL AND SDA PINS (*Note 2*)** | | | | | | |
| Low-Level Input Voltage | $V_{IL}$ | | -0.3 | | 0.2 × $V_{CC}$ | V |
| High-Level Input Voltage | $V_{IH}$ | | 0.7 × $V_{CC}$ | | $V_{CC}$ + 0.3V | V |
| Hysteresis of Schmitt Trigger Inputs | $V_{HYS}$ | (*Note 3*) | | 0.05 × $V_{CC}$ | | V |
| Low-Level Output Voltage at 4mA Sink Current | $V_{OL}$ | (*Note 4*) | | | 0.4 | V |
| Output Fall Time from $V_{IH(MIN)}$ to $V_{IL(MAX)}$ with a Bus Capacitance from 10pF to 400pF | $t_{OF}$ | (*Note 3*) | | 30 | | ns |
| Pulse Width of Spikes that are Suppressed by the Input Filter | $t_{SP}$ | (*Note 3*) | | | 50 | ns |

## Electrical Characteristics (continued)

(Limits are 100% production tested at $T_A$ = +25°C and/or $T_A$ = +85°C. Limits over the operating temperature range and relevant supply voltage range are guaranteed by design and characterization. Typical values are not guaranteed.)

| PARAMETER | SYMBOL | CONDITIONS | MIN | TYP | MAX | UNITS |
|---|---|---|---|---|---|---|
| Input Current with an Input Voltage Between $0.1V_{CCmax}$ and $0.9V_{CCmax}$ | $I_I$ | (*Note 3*, *Note 5*) | -1 | | +1 | µA |
| Input Capacitance | $C_I$ | (*Note 3*) | | 10 | | pF |
| SCL Clock Frequency | $f_{SCL}$ | (*Note 1*) | 0 | | 1 | MHz |
| Hold Time (Repeated) START Condition | $t_{HD:STA}$ | | 0.45 | | | µs |
| Low Period of the SCL Clock | $t_{LOW}$ | (*Note 6*) | 0.65 | | | µs |
| High Period of the SCL Clock | $t_{HIGH}$ | (*Note 3*) | 0.35 | | | µs |
| Setup Time for a Repeated START Condition | $t_{SU:STA}$ | (*Note 3*) | 0.35 | | | µs |
| Data Hold Time | $t_{HD:DAT}$ | (*Note 3*, *Note 6*, *Note 7*) | | | 0.35 | µs |
| Data Setup Time | $t_{SU:DAT}$ | (*Note 3*, *Note 6*, *Note 8*) | 100 | | | ns |
| Setup Time for STOP Condition | $t_{SU:STO}$ | (*Note 3*) | 0.35 | | | µs |
| Bus Free Time Between a STOP and START Condition | $t_{BUF}$ | (*Note 3*) | 0.6 | | | µs |
| Capacitive Load for Each Bus Line | $C_B$ | (*Note 1*, *Note 9*) | | | 400 | pF |
| Warm-Up Time | $t_{OSCWUP}$ | (*Note 1*, *Note 10*) | | | 1 | ms |
| **GPIO PIN** | | | | | | |
| GPIO Output Low | $PIOV_{OL}$ | $PIOI_{OL}$ = 4mA (*Note 4*) | | | 0.4 | V |
| GPIO Input Low | $PIOV_{IL}$ | | -0.3 | | 0.2 x $V_{CC}$ | V |
| GPIO Master Sample | $PIOV_{IH}$ | | 0.70 x $V_{CC}$ | | $V_{CC}$ + 0.3 | V |
| GPIO Switching Hysteresis | $PIOV_{HY}$ | | | 0.05 x $V_{CC}$ | | V |
| GPIO Leakage Current | $PIOI_L$ | | -1 | | +1 | µA |
| **CRYPTO FUNCTIONS** | | | | | | |
| Computation Current | $I_{CMP}$ | | | | 10 | mA |
| Read Memory | $t_{RM}$ | | | | 50 | ms |
| Write Memory | $t_{WM}$ | | | | 100 | ms |
| Blockwise Write Memory | $t_{WM\_BL}$ | Page data changes limited to one of four 8-byte blocks (refer to *DS28C50 Security User Guide*) | | | 60 | ms |
| Write State | $t_{WS}$ | | | | 60 | ms |

## Electrical Characteristics (continued)

(Limits are 100% production tested at $T_A$ = +25°C and/or $T_A$ = +85°C. Limits over the operating temperature range and relevant supply voltage range are guaranteed by design and characterization. Typical values are not guaranteed.)

| PARAMETER | SYMBOL | CONDITIONS | MIN | TYP | MAX | UNITS |
|---|---|---|---|---|---|---|
| Computation Time (HMAC) | $t_{CMP}$ | | | | 5 | ms |
| TRNG Generation | $t_{RNG}$ | | | | 25 | ms |
| TRNG On-Demand Check | $t_{ODC}$ | | | | 50 | ms |
| **EEPROM** | | | | | | |
| Write/Erase Cycles (Endurance) | $N_{CY}$ | (*Note 11*) | 100K | | | |
| Data Retention | $t_{DR}$ | $T_A$ = +85°C (*Note 12*) | 10 | | | Years |

**Note 1:** System requirement.

**Note 2:** All I²C timing values are referred to $V_{IH(MIN)}$ and $V_{IL(MAX)}$ levels.

**Note 3:** Guaranteed by design and/or characterization only. Not production tested.

**Note 4:** The I-V characteristic is linear for voltages less than 1V.

**Note 5:** I/O pins of the DS28C50 do not obstruct the SDA and SCL lines if $V_{CC}$ is switched off.

**Note 6:** $t_{LOW}$ min = $t_{HD:DAT}$ max + 200ns for rise or fall time + $t_{SU:DAT}$ min. Values greater than these can be accommodated by extending $t_{LOW}$ accordingly.

**Note 7:** The DS28C50 provides a hold time of at least 100ns for the SDA signal (referenced to the $V_{IH(MIN)}$ of the SCL signal) to bridge the undefined region of the falling edge of SCL.

**Note 8:** The DS28C50 can be used in a standard-mode I²C-bus system, but the requirement $t_{SU:DAT} \geq 250ns$ must then be met. Also the acknowledge timing must meet this setup time (I²C bus specification Rev. 03, 19 June 2007).

**Note 9:** $C_B$ = Total capacitance of one bus line in pF. The maximum bus capacitance allowable may vary from this value depending on the actual operating voltage and frequency of the application (I²C bus specification Rev. 03, 19 June 2007).

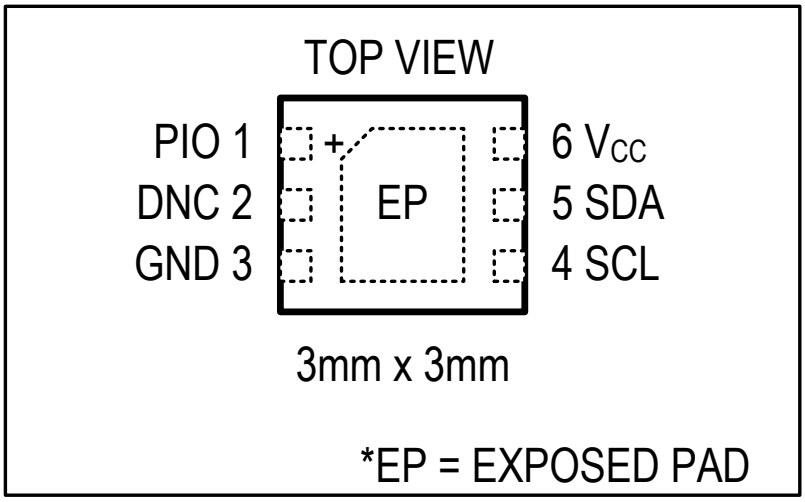
**Note 10:** I²C communication should not take place for the max $t_{OSCWUP}$ time following a power-on reset.

**Note 11:** Write-cycle endurance is tested in compliance with JESD47G.

**Note 12:** Data retention is tested in compliance with JESD47G.

## Pin Configuration

### 6 TDFN-EP




## Pin Description

| PIN | NAME | FUNCTION |
|---|---|---|
| 1 | PIO | General-Purpose IO |
| 2 | DNC | Do Not Connect |
| 3 | GND | Ground |
| 4 | SCL | I²C Clock. Connect to $V_{CC}$ with pullup resistor. |
| 5 | SDA | I²C Data. Connect to $V_{CC}$ with pullup resistor. |
| 6 | $V_{CC}$ | Supply Voltage |
| — | 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 DS28C50 integrates the Maxim ChipDNA capability to protect all device stored data. In addition to the PUF and SHA-3 engines for signatures, the device integrates a FIPS/NIST compliant TRNG, 2Kb EEPROM for user memory, SHA-3 secret storage, and control registers. One user page can optionally be designated as a decrement-only counter. The PIO pin can be independently operated under command control and includes configurability supporting authenticated and nonauthenticated operation. The device operates from a I2C interface in standard mode or in fast mode.

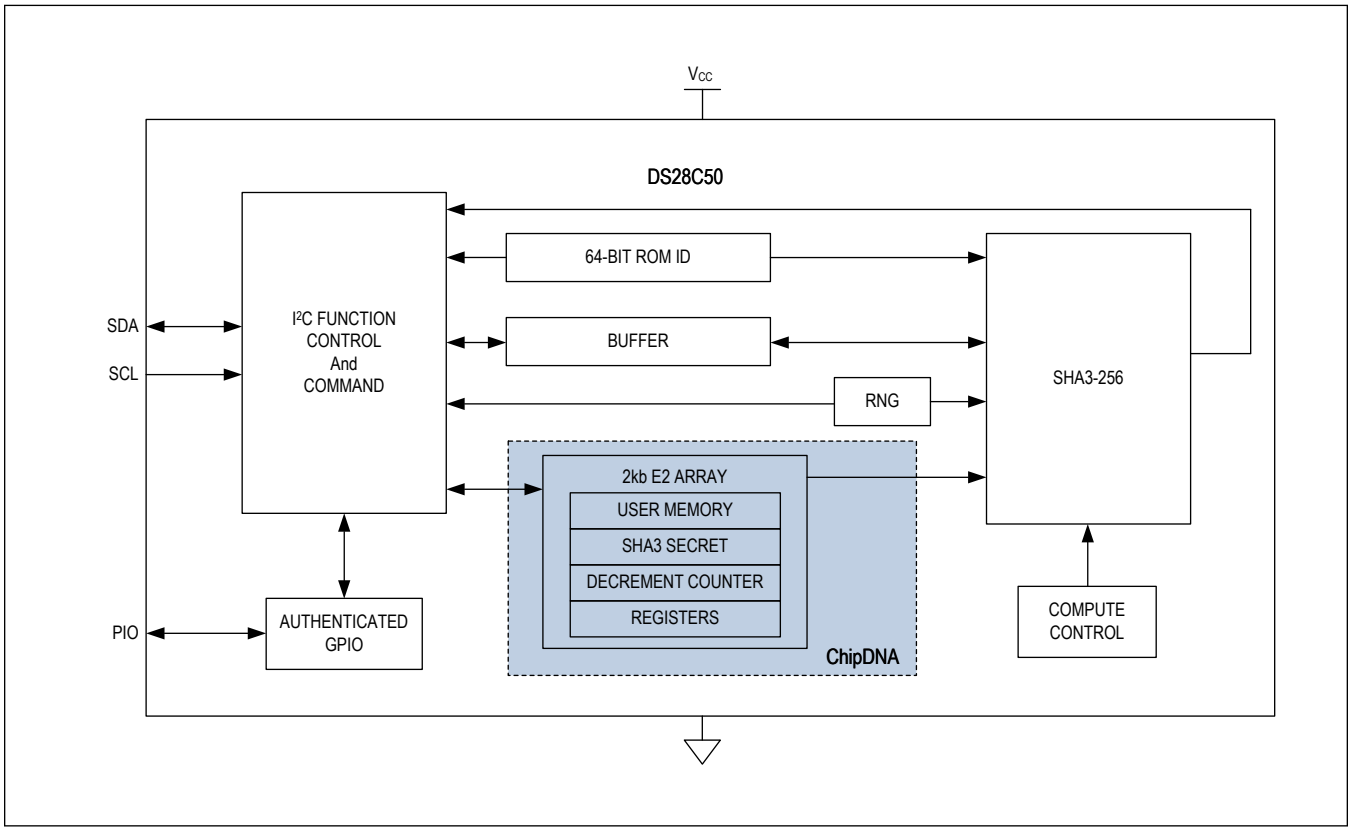



*Figure 1. Block Diagram*

### Design Resource Overview

Operation of the DS28C50 involves use of device EEPROM and execution of commands. The following sections provide an overview, including the decrement counter. Refer to the *DS28C50 Security User Guide* for details.

### Memory Description

A 2Kb secured EEPROM array provides SHA-3 secret storage, along with a decrement counter, and/or general-purpose, user-programmable memory. Depending on the memory space, there are either default or user-programmable options to set protection modes.

### Open-Drain GPIO

The open-drain PIO pin can be read and controlled in an authenticated or nonauthenticated manner. Authenticated operation includes measures to prevent replay attacks. Upon power-up, the default state for the PIO pin is in high impedance.

### Decrement Counter

The optional 17-bit decrement counter can be written one time on a dual-purpose page of memory. A dedicated 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.

## I2C

### General Characteristics

The I2C bus uses a data line (SDA) plus a clock signal (SCL) for communication. Both SDA and SCL are bidirectional lines, connected to a positive supply voltage through a pullup resistor. When there is no communication, both lines are high. The output stages of devices connected to the bus must have an open drain or open collector to perform the wired-AND function. Data on the I2C bus can be transferred at rates of up to 100kbps in standard mode and up to 400kbps in fast mode. The DS28C50 works in both modes or up to a clock rate of 1MHz. A device that sends data on the bus is defined as a transmitter, and a device receiving data is defined as a receiver. The device that controls the communication is called a master. The devices that are controlled by the master are slaves. To be individually accessed, each device must have a slave address that does not conflict with other devices on the bus. Data transfers can be initiated only when the bus is not busy. The master generates the serial clock (SCL), controls the bus access, generates the START and STOP conditions, and determines the number of data bytes transferred between START and STOP (Figure 2). Data is transferred in bytes with the most significant bit being transmitted first. After each byte follows an acknowledge bit to allow synchronization between master and slave.

### Slave Address

The slave address to which the DS28C50 responds is shown in Figure 3. The slave address is part of the slave address/control byte. The last bit of the slave address/control byte (R/W) defines the data direction. When set to 0, subsequent data flows from master to slave (write access); when set to 1, data flows from slave to master (read access).

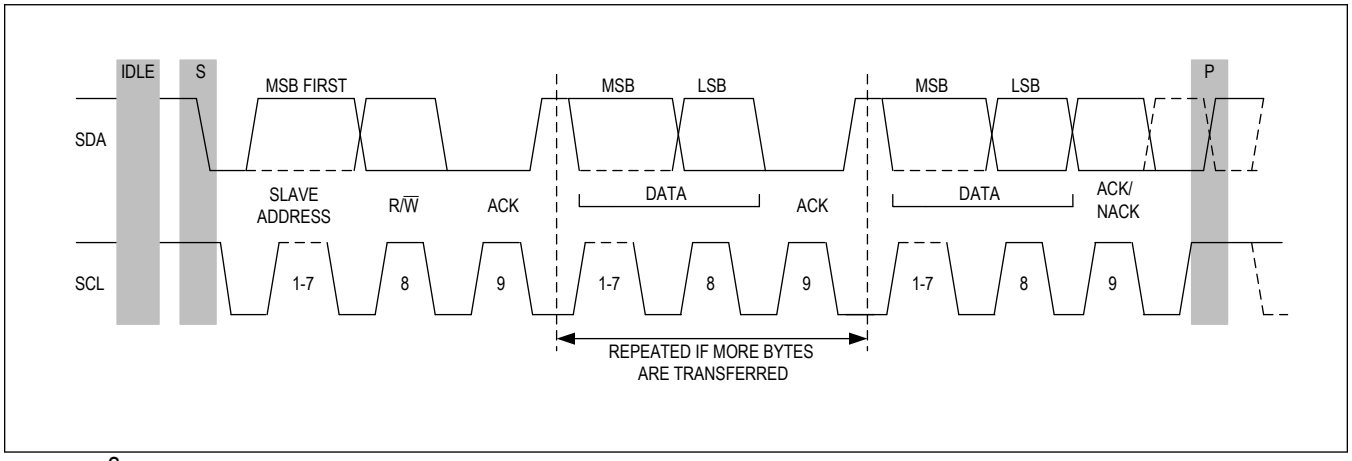



*Figure 2. I2C Protocol Overview*

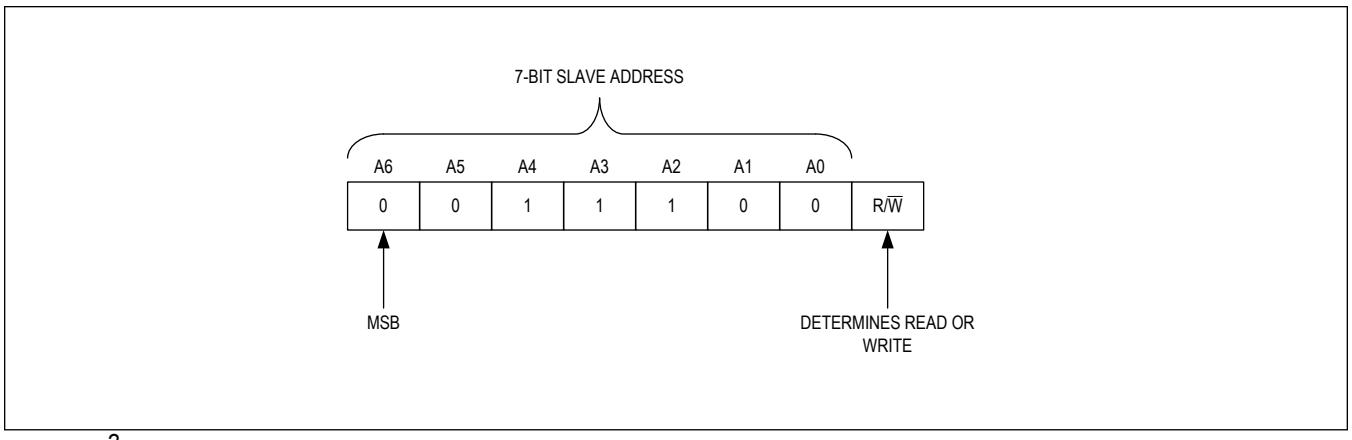



*Figure 3. I2C Slave Address*

### I2C Definitions

The following terminology is commonly used to describe I2C data transfers. The timing references are defined in Figure 4.

### Bus Idle or Not Busy

Both SDA and SCL are inactive and in their logic-high states.

### START Condition

To initiate communication with a slave, the master must generate a START condition. A START condition is defined as a change in state of SDA from high to low while SCL remains high.

### STOP Condition

To end communication with a slave, the master must generate a STOP condition. A STOP condition is defined as a change in state of SDA from low to high while SCL remains high.

### Repeated START Condition

Repeated STARTs are commonly used for read accesses after having specified a memory address to read from in a preceding write access. The master can use a repeated START condition at the end of a data transfer to immediately initiate a new data transfer following the current one. A repeated START condition is generated the same way as a normal START condition, but without leaving the bus idle after a STOP condition.

### Data Valid

With the exception of the START and STOP condition, transitions of SDA can occur only during the low state of SCL. The data on SDA must remain valid and unchanged during the entire high pulse of SCL plus the required setup and hold time ($t_{HD:DAT}$ after the falling edge of SCL and $t_{SU:DAT}$ before the rising edge of SCL; see Figure 4). There is one clock pulse per bit of data. Data is shifted into the receiving device during the rising edge of the SCL pulse.

When finished with writing, the master must release the SDA line for a sufficient amount of setup time (minimum $t_{SU:DAT}$, + $t_R$ in Figure 4) before the next rising edge of SCL to start reading. The slave shifts out each data bit on SDA at the falling edge of the previous SCL pulse and the data bit is valid at the rising edge of the current SCL pulse. The master generates all SCL clock pulses, including those needed to read from a slave.

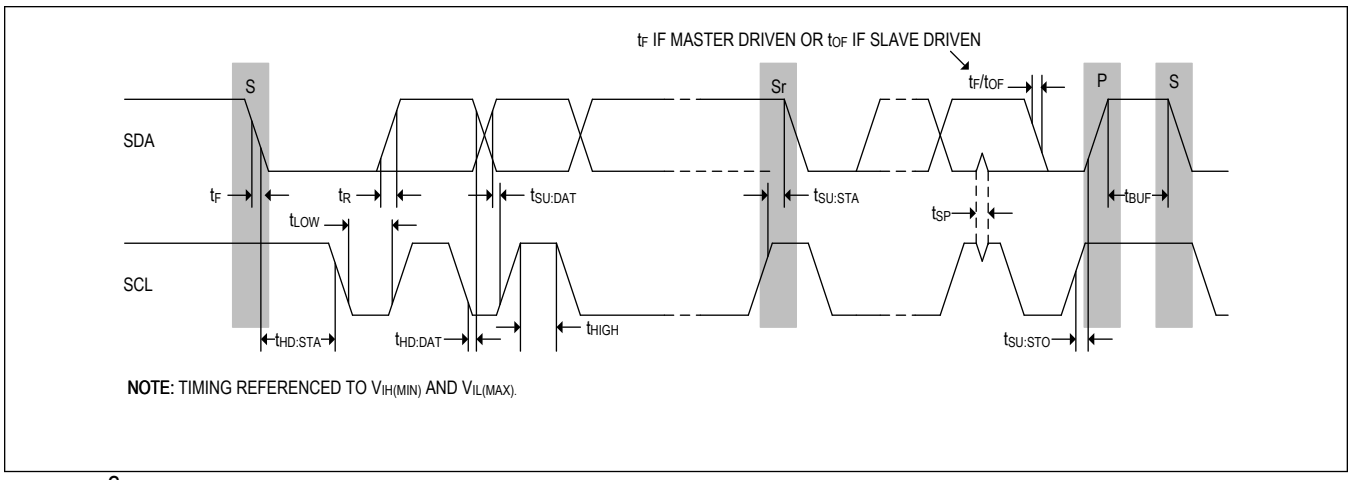



*Figure 4. I2C Timing Diagram*

## Ordering Information

| PART NUMBER | TEMP RANGE | PIN-PACKAGE |
|---|---|---|
| DS28C50Q+T | -40°C to +85°C | 6 TDFN (2.5k pcs reel) |

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

*T = Tape and reel.*

## Revision History

| REVISION NUMBER | REVISION DATE | DESCRIPTION | PAGES CHANGED |
|---|---|---|---|
| 0 | 9/19 | Initial release | — |