Abridged Data Sheet

DS2460
SHA-1 Coprocessor with EEPROM

www.maxim-ic.com

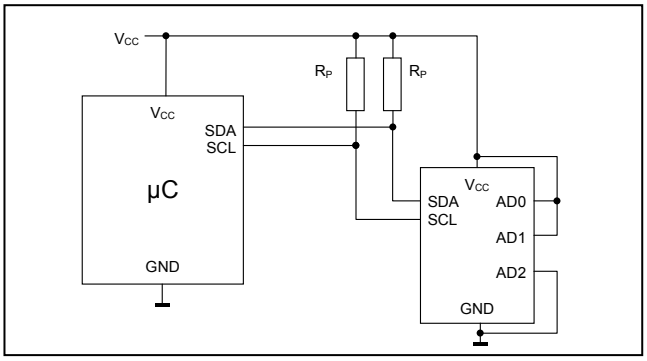
GENERAL DESCRIPTION

The DS2460 SHA-1 Coprocessor with EEPROM is a hardware implementation of the ISO/IEC 10118-3 Secure Hash Algorithm (SHA-1), eliminating the need to develop software to perform the complex SHA computation required for authenticating SHA devices and for performing the validation of digitally signed service data. The DS2460 communicates with a microcontroller through the popular I²C interface. Applications include hosts of access control and electronic payment systems for token authentication and service data validation as well as generation of one-time-use encryption keys for short message encryption and decryption for messages not exceeding the length of a SHA-1 result, which is 20 bytes.

APPLICATIONS

License Management
Secure Feature Control
System Authentication
Clone Prevention
Door Locks
Utility Meters

TYPICAL OPERATING CIRCUIT



FEATURES

- Dedicated Hardware-Accelerated SHA Engine for Generating SHA-1 MACs
- 112 Bytes User EEPROM for Storing End Equipment Property Data
- I²C Host Interface, Supports 100kHz and 400kHz Communication Speeds
- Three Address Inputs for I²C Address Assignment
- Single-Byte to 8-Byte EEPROM Write Sequences
- 64-Bit Unique Registration Number
- EEPROM Endurance: 200k Cycles per 8-Byte Block at 25°C
- 10ms max EEPROM Write Cycle
- Wide Operating Range: 2.7V to 5.5V, -40°C to +85°C
- ±4kV IEC 1000-4-2 ESD Protection Level on All Pins
- 8-Pin SO (150 mils) Package

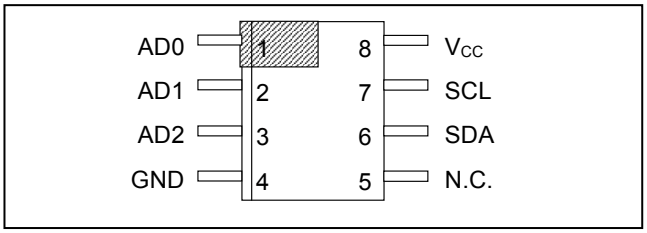
ORDERING INFORMATION

PART	TEMP RANGE	PIN-PACKAGE
DS2460S	-40°C to +85°C	8 SO (150 mils)
DS2460S/T&R	-40°C to +85°C	8 SO (150 mils)
DS2460S+	-40°C to +85°C	8 SO (150 mils)
DS2460S+T&R	-40°C to +85°C	8 SO (150 mils)

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

Request full data sheet at:
www.maxim-ic.com/fullds/DS2460

PIN CONFIGURATION



Note: *Some revisions of this device may incorporate deviations from published specifications known as errata. Multiple revisions of any device may be simultaneously available through various sales channels. For information about device errata, click here: www.maxim-ic.com/errata.*

ABSOLUTE MAXIMUM RATINGS

Voltage Range on Any Pin Relative to Ground	-0.5V, +6V
Maximum Current Into Any Pin	±20mA
Operating Temperature Range	-40°C to +85°C
Junction Temperature	+150°C
Storage Temperature Range	-55°C to +125°C
Soldering 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 the absolute maximum rating conditions for extended periods may affect device.

ELECTRICAL CHARACTERISTICS

(-40°C to +85°C, see Note 1)

PARAMETER	SYMBOL	CONDITIONS	MIN	TYP	MAX	UNITS
Supply Voltage	V_{CC}		2.7		5.5	V
Standby Current	I_{CCS}	Bus idle			3	µA
		Bus idle, +25°C			1	
Operating Current	I_{CCA}	Bus active at 400kHz		250	500	µA
Programming Current	I_{PROG}	(Note 9)		500	1000	µA
SHA-1 Computation Current	I_{SHA}	See full version of data sheet				mA
SHA-1 Engine						
SHA-1 Computation Time	t_{SHA}	See full version of data sheet				ms
EEPROM						
Programming Time	t_{PROG}				10	ms
Endurance	N_{CYCLE}	At +25°C (Notes 2, 3)	200k			
Data Retention	t_{RET}	At +85°C (Notes 4, 5, 6)	40			years
I²C-Pins (Note 7) See Figure 6						
LOW Level Input Voltage	V_{IL}	(Note 8)	-0.5		0.3 × V_{CC}	V
HIGH Level Input Voltage	V_{IH}	(Notes 8, 9)	0.7 × V_{CC}		V_{CC} + 0.5V	V
Hysteresis of Schmitt Trigger Inputs	V_{hys}	(Note 9)	0.05 × V_{CC}			V
LOW Level Output Voltage at 4mA Sink Current	V_{OL}				0.4	V
Output Fall Time from V_{Ihmin} to V_{ILmax} with a Bus Capacitance from 10pF to 400pF	t_{of}	(Note 9)	20 + 0.1Cb		250	ns
Pulse Width of Spikes that are Suppressed by the Input Filter	t_{SP}	SDA and SCL pins only (Note 9)			50	ns
Input Current Each I/O Pin with an Input Voltage Between $0.1V_{CCmax}$ and $0.9V_{CCmax}$	I_i	(Notes 8, 10)	-10		10	µA
Input Capacitance	C_i	(Notes 8, 9)			10	pF
SCL Clock Frequency	f_{SCL}		0		400	kHz
Hold Time (Repeated) START Condition. After this Period, the First Clock Pulse is Generated.	$t_{HD:STA}$		0.6			µs
LOW Period of the SCL Clock	t_{LOW}		1.3			µs
HIGH Period of the SCL Clock	t_{HIGH}		0.6			µs

PARAMETER	SYMBOL	CONDITIONS	MIN	TYP	MAX	UNITS
Setup Time for a Repeated START Condition	$t_{SU:STA}$		0.6			µs
Data Hold Time	$t_{HD:DAT}$	(Notes 11, 12)			0.9	µs
Data Setup Time	$t_{SU:DAT}$	(Note 13)	100			ns
Setup Time for STOP Condition	$t_{SU:STO}$		0.6			µs
Bus Free Time Between a STOP and START Condition	t_{BUF}		1.3			µs
Capacitive Load for Each Bus Line	C_B	(Note 14)			400	pF

Note 1: Specification at -40°C is guaranteed by design and characterization only and not production tested.
Note 2: Write-cycle endurance is degraded as T_A increases.
Note 3: Not 100% production-tested; guaranteed by reliability monitor sampling.
Note 4: Data retention is degraded as T_A increases.
Note 5: Guaranteed by 100% production test at elevated temperature for a shorter amount of time; equivalence of this production test to data sheet limit at operating temperature range is established by reliability testing.
Note 6: EEPROM writes can become nonfunctional after the data-retention time is exceeded. Long-term storage at elevated temperatures is not recommended; the device can lose its write capability after 10 years at +125°C or 40 years at +85°C.
Note 7: All values are referred to V_{IHmin} and V_{ILmax} levels.
Note 8: Applies to SDA, SCL, AD2, AD1, AD0.
Note 9: Guaranteed by simulation only, not production tested.
Note 10: I/O pins of the DS2460 do not obstruct the SDA and SCL lines if V_{CC} is switched off.
Note 11: The DS2460 provides a hold time of at least 300ns for the SDA signal (referred to the V_{IHmin} of the SCL signal) to bridge the undefined region of the falling edge of SCL.
Note 12: The maximum $t_{HD:DAT}$ has only to be met if the device does not stretch the LOW period (t_{LOW}) of the SCL signal.
Note 13: A Fast-mode I²C-bus device can be used in a standard-mode I²C-bus system, but the requirement $t_{SU:DAT} \geq$250ns must then be met. This is automatically the case if the device does not stretch the LOW period of the SCL signal. If such a device does stretch the LOW period of the SCL signal, it must output the next data bit to the SDA line tr max + $t_{SU:DAT}$ = 1000 + 250 = 1250ns (according to the standard-mode I²C-bus specification) before the SCL line is released.
Note 14: C_B = total capacitance of one bus line in pF. If mixed with HS-mode devices, faster fall-times according to I²C-Bus Specification v2.1 are allowed.

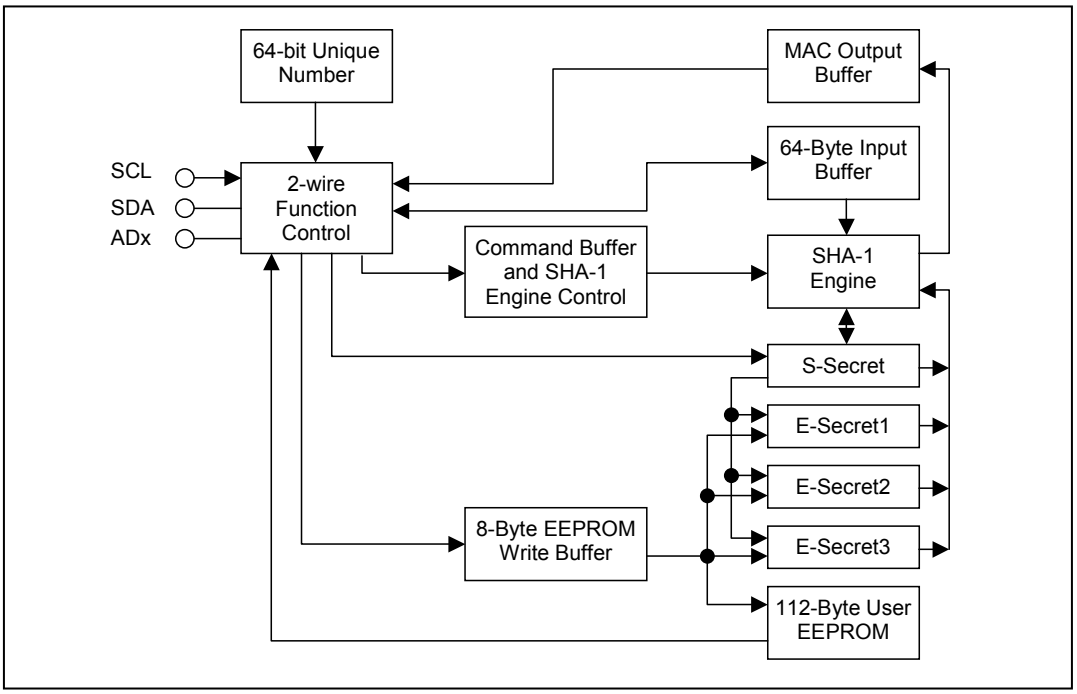
PIN DESCRIPTION

PIN	NAME	FUNCTION
1	AD0	I²C Address Inputs; must be tied to VCC or GND. These inputs determine the I²C slave address of the device, see Figure 5.
2	AD1	
3	AD2	
4	GND	Ground Reference
5	NC	Not Connected
6	SDA	I²C Serial Data Input/Output; must be tied to V_{CC} through a pullup resistor.
7	SCL	I²C Serial Clock Input; must be tied to V_{CC} through a pullup resistor.
8	V_{CC}	Power Supply Input

OVERVIEW

The block diagram in Figure 1 shows the relationships between the major control and memory sections of the DS2460. The DS2460 communicates with a host processor through its I²C bus interface in standard-mode or in fast-mode. The logic state of three address pins determines the I²C slave address of the DS2460, allowing up to 8 devices to operate on the same bus segment without requiring a hub. For more information (including Figure 2) refer to the full version of the data sheet.

Figure 1. Block Diagram



DETAILED REGISTER DESCRIPTION

For this section (including Figure 3) please refer to the full version of the data sheet.

DEVICE OPERATION

The typical use of the DS2460 in an application involves writing, reading, running the SHA-1 engine, transferring secrets and comparing MACs. All these activities are controlled through the I²C serial interface.

I²C Serial Communication Interface

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 the Standard-mode, up to 400kbps in the Fast-mode. The DS2460 works in both modes.

A device that sends data on the bus is defined as a transmitter, and a device receiving data 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 may 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 4). 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 DS2460 responds is shown in Figure 5. The logic states at the address pins AD0, AD1 and AD2 determine the value of the address bits A0, A2, and A4. The address pins allow the device to respond to one of eight possible slave addresses. The slave address is part of the slave-address/control byte. The last bit of the slave-address/control byte (R/$\overline{W}$) defines the data direction. When set to a 0, subsequent data will flow from master to slave (write access mode); when set to a 1, data will flow from slave to master (read access mode).

Figure 4. I²C Protocol Overview

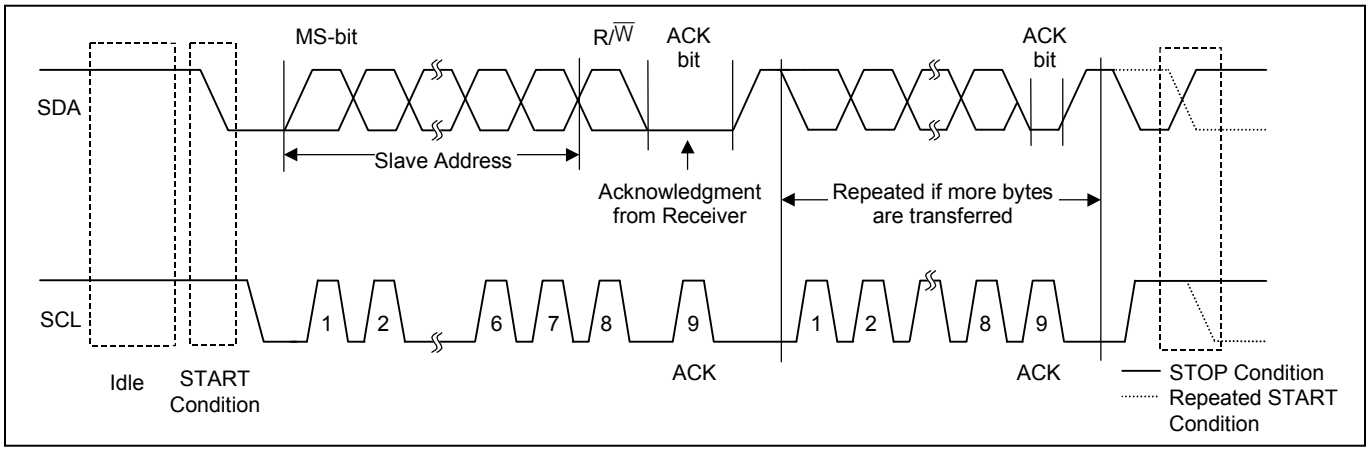
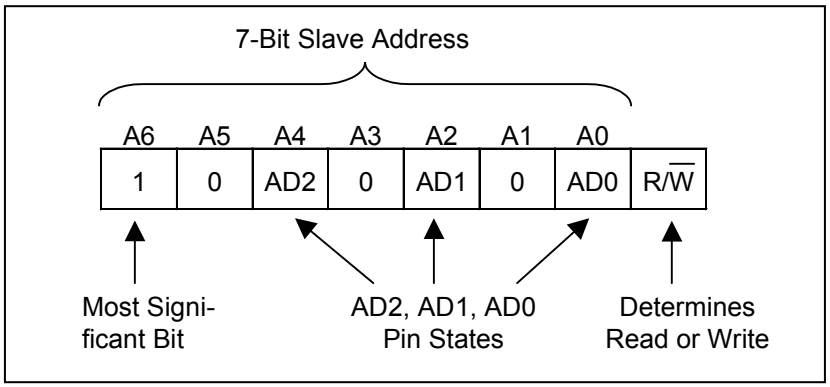


Figure 5. DS2460 Slave Address



I²C Definitions
The following terminology is commonly used to describe I²C data transfers. The timing references are defined in Figure 6.

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 has to generate a START condition. A START condition is defined as a change in state of SDA from HIGH to LOW while SCL remains HIGH. A valid slave address must be sent by the master and acknowledged by the slave before subsequent START conditions are recognized.

STOP Condition
To end communication with a slave, the master has to generate a STOP condition. A STOP condition is defined as a change in state of SDA from LOW to HIGH while SCL remains HIGH. A valid slave address must be sent by the master and acknowledged by the slave before subsequent STOP conditions are recognized.

Repeated START Condition
Repeated starts are commonly used for read accesses to select a specific data source or address to read from. 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 may 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 6). 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 6) 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.

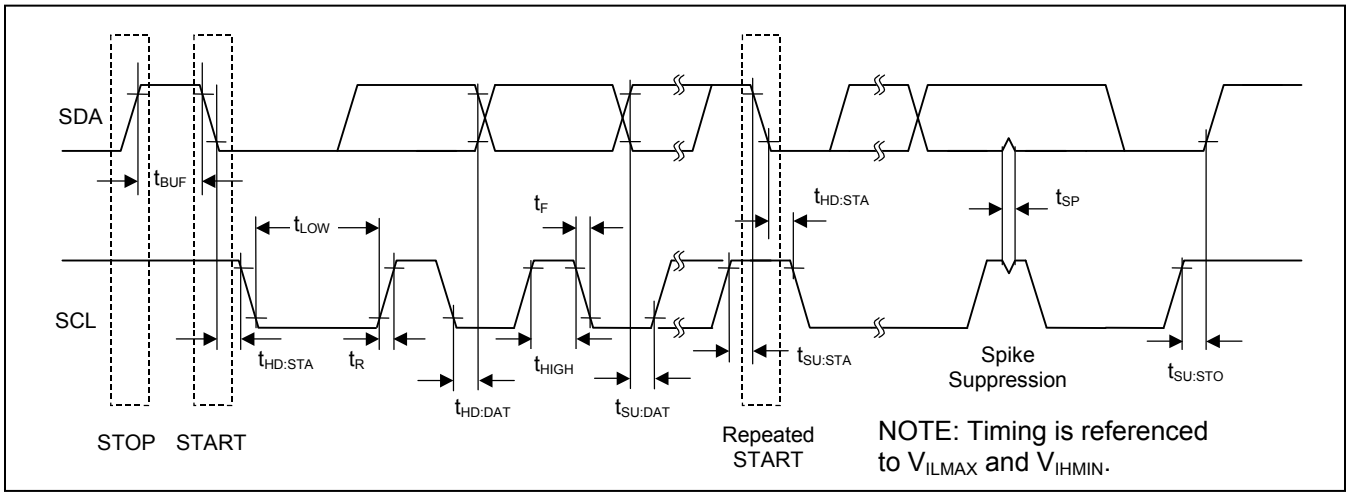
Acknowledge
Usually, a receiving device, when addressed, is obliged to generate an acknowledge after the receipt of each byte. The master must generate a clock pulse that is associated with this acknowledge bit. A device that acknowledges must pull SDA LOW during the acknowledge clock pulse in such a way that SDA is stable LOW during the HIGH period of the acknowledge-related clock pulse 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).

Not Acknowledged by Slave
A slave device may be unable to receive or transmit data, e.g., because it is busy performing a real-time function, such as MAC computation or EEPROM write cycle. In this case the slave device will not acknowledge its slave address and leave the SDA line HIGH.

A slave device that is ready to communicate will acknowledge at least its slave address. However, some time later the slave may refuse to accept data, e.g., because of an invalid command or access mode, or to signal a non-matching MAC. In this case the slave device will not acknowledge any of the bytes that it refuses and will leave SDA HIGH. In either case, after a slave has failed to acknowledge, the master first needs to generate a repeated START condition or a STOP condition followed by a START condition to begin a new data transfer.

Not Acknowledged by Master
At some time when receiving data, the master must signal an end of data to the slave device. To achieve this, the master does not acknowledge the last byte that it has received from the slave. In response, the slave releases SDA, allowing the master to generate the STOP condition.

Figure 6. I²C Timing Diagram



Read and Write

This section discusses the read and write behavior of the various registers and the EEPROM. Please refer to the full data sheet for details.

SHA-1 Engine Control

This section describes the user's view of the SHA-1 engine and how to operate it. For details refer to the full data sheet (includes Figures 7 to 9 and Tables 1 and 2).

SHA-1 COMPUTATION ALGORITHM

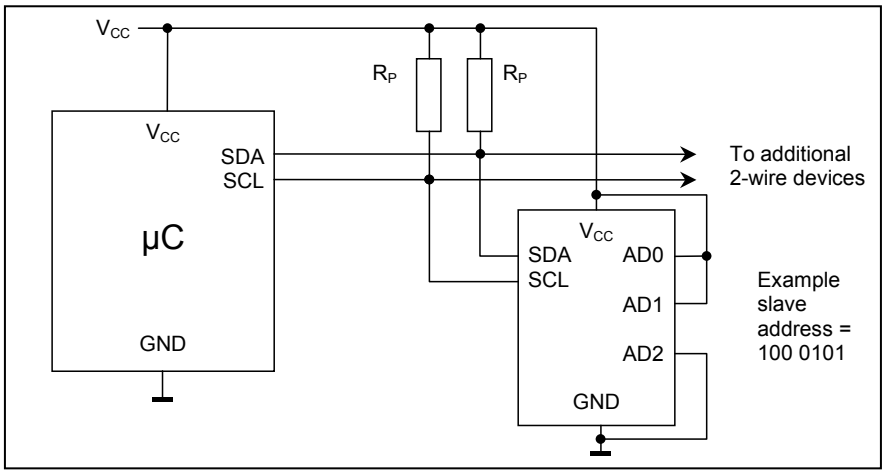
This description of the SHA computation is adapted from the Secure Hash Standard SHA-1 document that can be downloaded from the NIST website (www.itl.nist.gov/fipspubs/fip180-1.htm). Further details are found in the full version of the data sheet.

Application Information

SDA and SCL Pullup Resistors

SDA is an open-drain output on the DS2460 that requires a pullup resistor (Figure 10) to realize high logic levels. Because the DS2460 uses SCL only as input (no clock stretching) the master can drive SCL either through an open-drain/collector output with a pullup resistor or a push-pull output.

Figure 10. Application Schematic



Pullup Resistor R_P Sizing

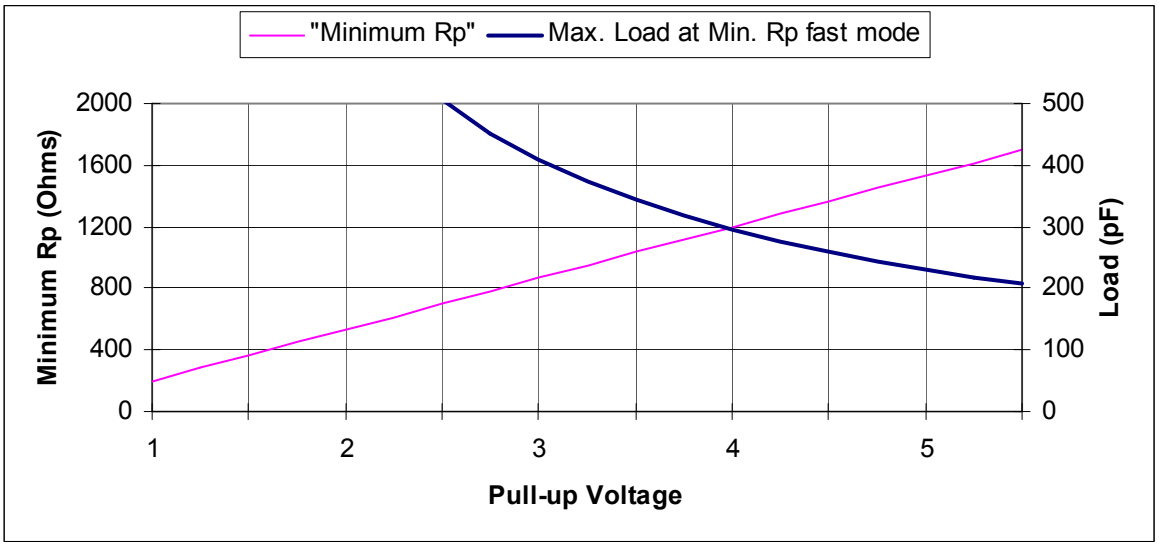
According to the I²C specification, a slave device must be able to sink at least 3mA at a V_{OL} of 0.4V. This DC condition determines the minimum value of the pullup resistor: **$R_{PMIN} = (V_{CC} - 0.4V)/3mA$.** With an operating voltage of 5.5V, the minimum value for the pullup resistor is 1.7kΩ. The "Minimum R_P" line in Figure 11 shows how the minimum pullup resistor changes with the operating (pull-up) voltage.

For I²C systems, the rise time and fall time are measured from 30% to 70% of the pullup voltage. The maximum bus capacitance C_B is 400pF. The maximum rise time must not exceed 300ns. Assuming maximum rise time, the maximum resistor value at any given capacitance C_B is calculated as: **$R_{PMAX} = 300ns/(C_B*ln(7/3))$**. For a bus capacitance of 400pF the maximum pullup resistor would be 885Ω.

Since a 885Ω pullup resistor, as would be required to meet the rise time specification at 400pF bus capacitance, is lower than R_{PMIN} at 5.5V, a different approach is necessary. The "Max. Load…" line in Figure 11 is generated by first calculating the minimum pullup resistor at any given operating voltage ("Minimum R_P" line) and then calculating the respective bus capacitance that yields a rise time of 300ns.

Only for pullup voltages of 3V and lower can the maximum permissible bus capacitance of 400pF be maintained. A reduced bus capacitance of 300pF is acceptable for pullup voltages of 4V and lower. For fast speed operation at any pullup voltage, the bus capacitance must not exceed 200pF. The corresponding pullup resistor value at the voltage is indicated by the "Minimum R_P " line.

Figure 11. I²C Fast Speed Pullup Resistor Selection Chart



I²C Bus Compliance

Although the I²C protocol definition does not explicitly forbid a START - STOP - START sequence, the DS2460 does not tolerate it. If a START, STOP, START sequence has been issued, transmit the following sequence before communicating with the DS2460: START, 10xxxxxx byte (x = don't care bits), ACK/NACK bit, STOP.

PACKAGE INFORMATION

For the latest package outline information and land patterns, go to www.maxim-ic.com/packages. Note that a "+", "#", or "-" in the package code indicates RoHS status only. Package drawings may show a different suffix character, but the drawing pertains to the package regardless of RoHS status.

PACKAGE TYPE	PACKAGE CODE	DOCUMENT NO.
8 SO	S8+4	**21-0041**

REVISION HISTORY

REVISION DATE	DESCRIPTION	PAGES CHANGED
4/09	Original release	—
8/07	• Extended *Storage Temperature Range* to -55°C to +125°C, • Added Note 6 to t_{RET} and changed specification value to 40 years minimum.	2, 3
3/10	• Soldering temperature changed from referencing JEDEC J-STD-020 to actual temperatures for soldering and reflow. • Note 9 added to I_{PROG} specification. • Below Figure 11, inserted section *I²C Bus Compliance*.	2, 9

Maxim Integrated Products, 120 San Gabriel Drive, Sunnyvale, CA 94086 408-737-7600

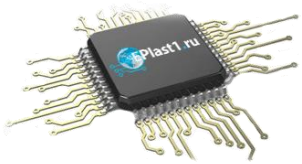
Компания «ЭлектроПласт» предлагает заключение долгосрочных отношений при поставках импортных электронных компонентов на взаимовыгодных условиях!

Наши преимущества:

- Оперативные поставки широкого спектра электронных компонентов отечественного и импортного производства напрямую от производителей и с крупнейших мировых складов;
- Поставка более 17-ти миллионов наименований электронных компонентов;
- Поставка сложных, дефицитных, либо снятых с производства позиций;
- Оперативные сроки поставки под заказ (от 5 рабочих дней);
- Экспресс доставка в любую точку России;
- Техническая поддержка проекта, помощь в подборе аналогов, поставка прототипов;
- Система менеджмента качества сертифицирована по Международному стандарту ISO 9001;
- Лицензия ФСБ на осуществление работ с использованием сведений, составляющих государственную тайну;
- Поставка специализированных компонентов (Xilinx, Altera, Analog Devices, Intersil, Interpoint, Microsemi, Aeroflex, Peregrine, Syfer, Eurofarad, Texas Instrument, Miteq, Cobham, E2V, MA-COM, Hittite, Mini-Circuits,General Dynamics и др.);

Помимо этого, одним из направлений компании «ЭлектроПласт» является направление «Источники питания». Мы предлагаем Вам помощь Конструкторского отдела:

- Подбор оптимального решения, техническое обоснование при выборе компонента;
- Подбор аналогов;
- Консультации по применению компонента;
- Поставка образцов и прототипов;
- Техническая поддержка проекта;
- Защита от снятия компонента с производства.



Как с нами связаться

Телефон: 8 (812) 309 58 32 (многоканальный)
Факс: 8 (812) 320-02-42
Электронная почта: org@eplast1.ru
Адрес: 198099, г. Санкт-Петербург, ул. Калинина, дом 2, корпус 4, литера А.