DS2705
SHA-1 Authentication Master

www.maxim-ic.com

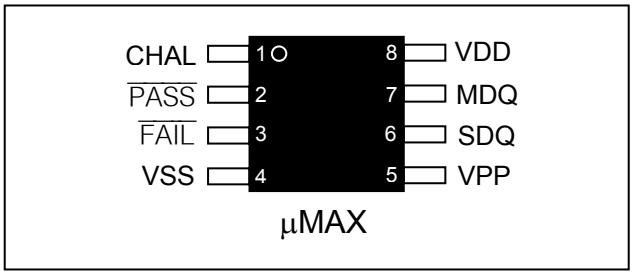
GENERAL DESCRIPTION

The DS2705 provides the master side of a Secure Hash Algorithm (SHA) based token authentication scheme. Hardware-based SHA authentication allows for security without the added cost and complexity of a microprocessor-based system. Batteries and other accessories are authenticated using a single contact through the Dallas 1-Wire® interface. Authentication is performed on demand or automatically, with the pass/fail status reported on open-drain output pins to signal the charge system and/or drive LEDs. The DS2705 stores a predetermined challenge-and-response pair in nonvolatile (NV) EEPROM. The DS2705 works in conjunction with Dallas Battery Management SHA-1 token products, including the DS2703 and DS2704.

APPLICATIONS

Digital Cameras
Portable DVD and Media Players
Cradle and Accessory Chargers
Cell Phones/Smartphones

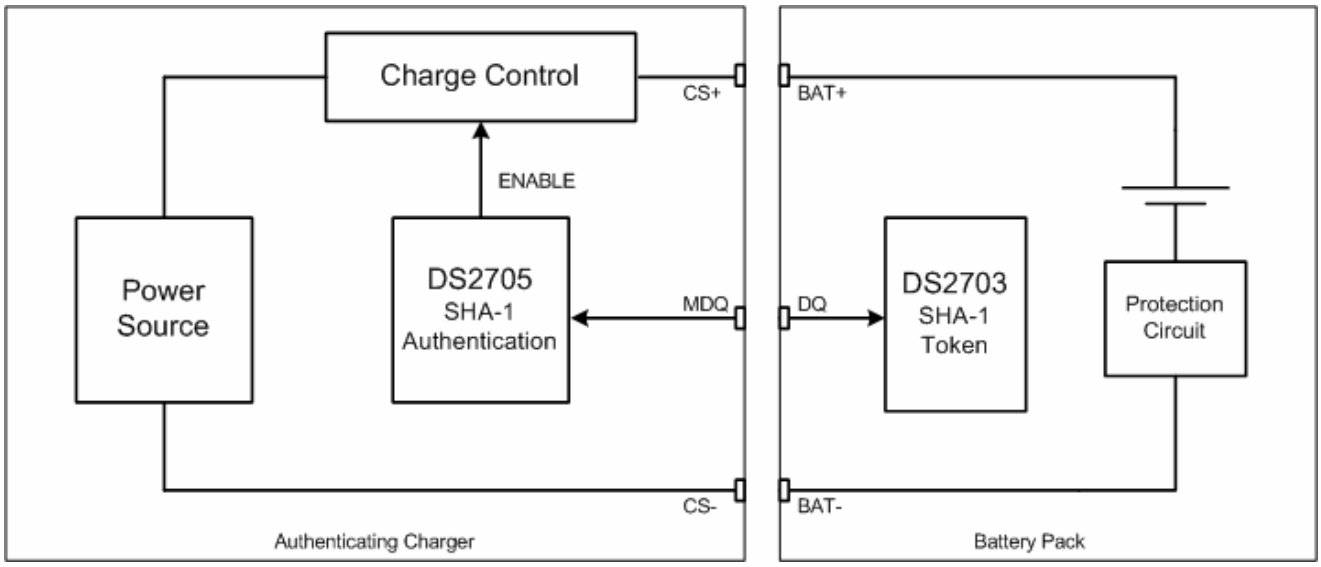
PIN CONFIGURATION



FEATURES

- **Initiates Challenge-and-Response Authentication based on the SHA-1 Algorithm**
- **Dallas 1-Wire Master/Slave Interface Operates at Standard and Overdrive Speeds**
- **Input and Output pins for Initiating Challenge and Reporting Authentication Pass/Fail**
- **Programmable Configuration**
- **Operates from 2.5V to 5.5V Supply**
- **Tiny µMAX Package (Pb-Free)**

APPLICATION EXAMPLE



ORDERING INFORMATION

PART	TEMP RANGE	MARKING	PIN-PACKAGE
DS2705U+	-20°C to +85°C	D2705	µMAX
DS2705U+/T&R	-20°C to +85°C	D2705	DS2705U+ in Tape-and-Reel

+ Denotes lead-free package.
1-Wire is a registered trademark of Dallas Semiconductor.

ABSOLUTE MAXIMUM RATINGS

Voltage Range on All Pins (Except VPP), Relative to V_{SS}	-0.3V to +5.5V
Voltage Range on V_{PP} Pin, Relative to V_{SS}	-0.3V to +18V
Continuous Source Current, MDQ	20mA
Operating Temperature Range	-40°C to +85°C
Storage Temperature Range	-55°C to +125°C
Soldering Temperature	See IPC/JEDEC J-STD-020A Specification

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.

DC ELECTRICAL CHARACTERISTICS

($2.5V \le V_{DD} \le 5.5V$, T_A = -20°C to +85°C.)

PARAMETER	SYMBOL	CONDITIONS	MIN	TYP	MAX	UNITS
Supply Current	I_{DD1}	Active mode, MDQ low, I_{O_MDQ} = 0			2.5	mA
	I_{DD2}	Active mode, MDQ idle, I_{O_MDQ} = 0		90	130	µA
	I_{DD3}	Sleep mode, I_{O_MDQ} = 0 (Note 2)		1	3	µA
		-20°C ≤ T_A ≤ 70°C Sleep mode, I_{O_MDQ} = 0 (Note 2)		1	2	µA
Programming Voltage: V_{PP}	V_{PP}	Program pulse (Notes 1, 3)	14.5		15.0	V
Input Logic High: MDQ, SDQ, CHAL	V_{IH}	(Note 1)	1.8			V
Input Logic Low: MDQ, SDQ, CHAL	V_{IL}	(Note 1)			0.6	V
Output Logic Low: MDQ, SDQ	V_{OL1}	I_{OL} = 4mA (Note 1)			0.4	V
Output Logic Low: $\overline{PASS}$, $\overline{FAIL}$	V_{OL2}	I_{OL} = 10mA (Note 1)			0.4	V
Pulldown: V_{PP}	I_{PD1}			300		µA
Pulldown: SDQ, CHAL	I_{PD2}	(Note 5)		0.125		µA
Pullup: MDQ	I_{OH}	Communication mode (Note 6)	0.25		2.5	mA
	V_{OH}	Computation mode I_{OH} = 2.0mA (Note 7)	V_{DD} - 0.1			V
Input Capacitance: MDQ, SDQ	C_{IN}				60	pF

EEPROM RELIABILITY SPECIFICATION

($2.5V \le V_{DD} \le 5.5V$, T_A = -20°C to +85°C.)

PARAMETER	SYMBOL	CONDITIONS	MIN	TYP	MAX	UNITS
EEPROM Write Time	t_{EEW}	(Note 3)			15	ms
EEPROM Write Endurance	N_{EEC}	(Notes 3, 4)	1,000			Cycles

AC ELECTRICAL CHARACTERISTICS: MASTER 1-Wire INTERFACE

(2.5V ≤ V_{DD} ≤ 5.5V, T_A = -20°C to +85°C.)

PARAMETER	SYMBOL	CONDITIONS	MIN	TYP	MAX	UNITS
STANDARD BUS TIMING						
Time Slot	t_{MSLOT}	(Note 10)		90		µs
Recovery Time	t_{MREC}	(Note 10)	7.5	10	12.5	µs
Write-0 Low Time	t_{MLOW0}	(Note 10)		88.5		µs
Write-1 Low Time	t_{MLOW1}	(Note 10)	1.05	1.5	2.25	µs
Read-Data Sample Window	t_{MRDV}	(Note 10)	4.0	5.5	7.0	µs
Reset-Time Low	t_{MRSTL}	(Note 10)	510	680	850	µs
Presence-Detect High	t_{MPDH}	(Note 10)	2		75	µs
Presence-Detect Low	t_{MPDL}	(Note 10)	2		400	µs
OVERDRIVE BUS TIMING						
Time Slot	t_{MSLOT}	(Note 10)		12		µs
Recovery Time	t_{MREC}	(Note 10)	1	2	2.5	µs
Write-0 Low Time	t_{MLOW0}	(Note 10)		10.5		µs
Write-1 Low Time	t_{MLOW1}	(Note 10)	0.35	0.5	0.65	µs
Read-Data Sample Window	t_{MRDV}	(Note 10)	1.1	1.5	1.9	µs
Reset-Time Low	t_{MRSTL}	(Note 10)	53	70	88	µs
Presence-Detect High	t_{MPDH}	(Note 10)	2		7	µs
Presence-Detect Low	t_{MPDL}	(Note 10)	2		41	µs

AC ELECTRICAL CHARACTERISTICS: SLAVE 1-Wire INTERFACE

(2.5V ≤ V_{DD} ≤ 5.5V, T_A = -20°C to +85°C.)

PARAMETER	SYMBOL	CONDITIONS	MIN	TYP	MAX	UNITS
STANDARD BUS TIMING						
Time Slot	t_{SLOT}		60		120	µs
Recovery Time	t_{REC}		1			µs
Write-0 Low Time	t_{LOW0}		60		120	µs
Write-1 Low Time	t_{LOW1}		1		15	µs
Read-Data Valid	t_{RDV}				15	µs
Reset-Time High	t_{RSTH}		480			µs
Reset-Time Low	t_{RSTL}		480		960	µs
Presence-Detect High	t_{PDH}		15		60	µs
Presence-Detect Low	t_{PDL}		60		240	µs
OVERDRIVE BUS TIMING						
Time Slot	t_{SLOT}		6		16	µs
Recovery Time	t_{REC}		1			µs
Write-0 Low Time	t_{LOW0}		6		16	µs
Write-1 Low Time	t_{LOW1}		1		2	µs
Read-Data Valid	t_{RDV}				2	µs
Reset-Time High	t_{RSTH}		48			µs
Reset-Time Low	t_{RSTL}		48		80	µs
Presence-Detect High	t_{PDH}		2		6	µs
Presence-Detect Low	t_{PDL}		8		24	µs

AC ELECTRICAL CHARACTERISTICS

(2.5V ≤ V_{DD} ≤ 5.5V, T_A = -20°C to +85°C.)

PARAMETER	SYMBOL	CONDITIONS	MIN	TYP	MAX	UNITS
Programming Pulse Width	t_{PPW}		17			ms
Programming Pulse Rise Time	t_{PPR}	(Note 8)	0.5		5	µs
Programming Pulse Fall Time	t_{PPF}	(Note 8)	0.5		5	µs
Strong Pullup Delay Time	t_{SPUD}			2	10	µs
Strong Pullup Period	t_{SPUP}		30.25	34.00	48.00	ms
Challenge Delay Time	t_{CHD}		45	65	85	ms
Authentication Attempt Time	t_{AAT}	(Note 9)	61		490	ms
$\overline{FAIL}$ Pin Pulse Frequency	t_{FPF}	FOM = 1, 50% duty cycle	1.5	2	2.5	Hz

Note 1: All voltages are referenced to V_{SS}.

Note 2: IDD3 Sleep mode conditions:

CHAL pin inactive OR (CHAL active AND (PAA = 0 AND PPT = 00 AND FOM = 0 AND Initial Authentication sequence complete))

[Above conditions disable the internal oscillator]

Note 3: Programming temperature range is T_A = 0°C to 50°C.

Note 4: 5 years data retention at 70°C

Note 5: If CHAL pin left unconnected, CHP bit = 0 required for an authentication attempt to be initiated on power up. See Table 1.

Note 6: Typical Communication mode MDQ pullup behavior equivalent to 3kΩ resistor.

Note 7: Typical Computation mode MDQ pullup behavior approximates a 50Ω resistor.

Note 8: Exceeding maximum rise and fall time specifications may affect device reliability.

Note 9: t_{AAT} = Retries per Attempt x (264bits x 90µs + 3 x (t_{MRSTL} + t_{RSTH}) + t_{SPUD}) = [1 to 8] x (23.7ms + 3.54ms + 34ms)
MAX[7 retries]: 490ms, MIN[no retries]: 61ms with standard timings

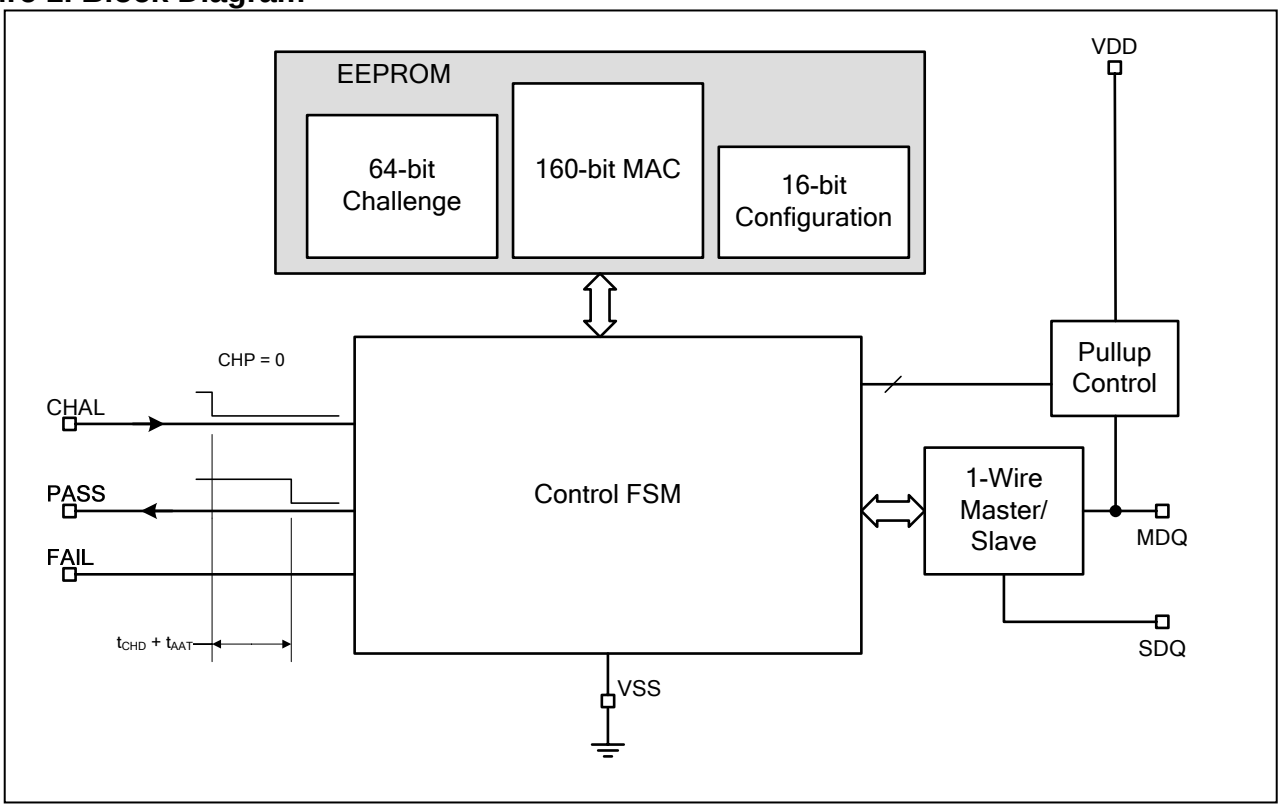
Note 10:

1. 1-Wire Master timings based on ±25% clock tolerance from nominal.
2. t_{RPDT} [defined in design documentation] = t_{MRSTL} + t_{MRSTH}
3. $t_{MPDL-MAX}$ = $t_{MRSTH-MIN}$ – $t_{MPDH-MAX,}$ represents the maximum presence pulse low time allowed from the slave.
4. Bus rise time of ~1µs required to settle to logic high by t_{MRDV} after MDQ released at t_{MLOW1}

PIN DESCRIPTION

PIN		SYMBOL	FUNCTION
µMAX	TDFN		
1	1	CHAL	Challenge Strobe Input Pin. Initiates authentication. Active level/edge set by CHP bit.
2	2	$\overline{PASS}$	Authentication “PASS” Result Open-Drain Output Pin
3	3	$\overline{FAIL}$	Authentication “FAIL” Result Open-Drain Output Pin (Programmable As Low Or Pulse)
4	4	V_{SS}	Supply Return Pin, GND Reference for Logic Signals
5	5	V_{PP}	EEPROM Programming Voltage Input
6	6	SDQ	Slave Serial interface Data I/O Pin. Bidirectional data transmit and receive at 16kbps or 143kbps. Bus master must provide a weak pullup.
7	7	MDQ	Master Serial interface Data I/O Pin. Bidirectional data transmit and receive at 16kbps or 143kbps. Provides a weak pullup in communication mode and strong pullup in computation mode.
8	8	V_{DD}	Supply Input Pin. Bypass to V_{SS} with 0.1µF capacitor.

Figure 1. Block Diagram



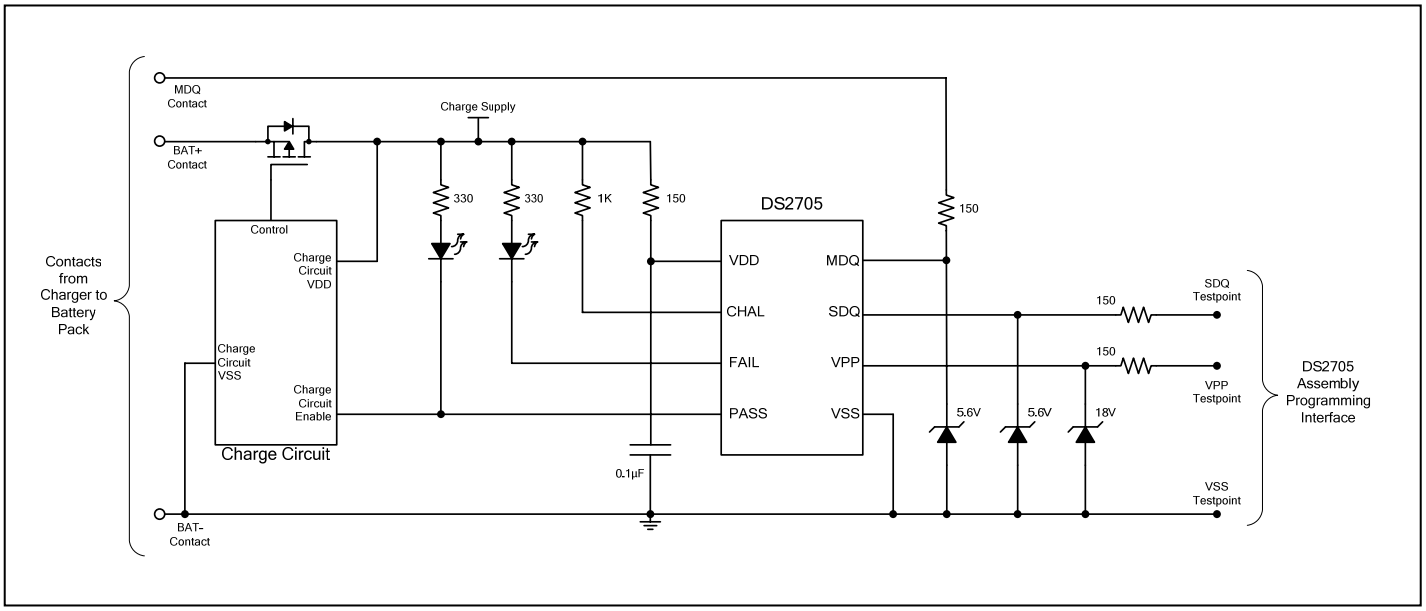
DETAILED DESCRIPTION

The DS2705 orchestrates a challenge/response SHA-1 authentication procedure by accessing a Dallas Battery Management SHA-1 Token product, such as the DS2703 or DS2704. The remote SHA-1 token is accessed with the MDQ pin acting as the 1-Wire bus master. The DS2705 issues the appropriate 1-Wire command sequence on MDQ to write the 64-bit challenge, initiates a SHA-1 computation in the token, and then reads back the 160-bit MAC result. The DS2705 compares the 160-bit MAC received from the battery token with the preprogrammed MAC. An exact bit for bit match is required for the authentication to be successful. The result of the operation, PASS or FAIL, is indicated on active low status output pins which can be used to drive status LEDs and/or enable cell charging.

The DS2705 can be configured to automatically authenticate by detection of a presence pulse on MDQ or authentication can be controlled by the state of the CHAL input pin. The DS2705's SDQ pin is a 1-Wire slave interface for programming the behavior of the I.C.. All EEPROM values can be permanently locked to prevent corruption.

Figure 2 shows a example application circuit for a standalone battery charger. The DS2705 is preprogrammed for automatic authentication on MDQ and also contains a known good challenge/response pair. Programming occurs during assembly through PCB test points shown on the right side of the circuit. When a battery pack is inserted into the charger, a presence pulse on MDQ will cause the DS2705 to automatically authenticate the pack. The result of the authentication will be displayed through the LEDs and the DS2705 will either enable or disable the charging circuit.

Figure 2. Typical Application Circuit



BATTERY TOKEN PRESENCE DETECTION

Authentication of a battery or peripheral first depends on the authentication host detecting the presence or insertion (electrical connection) of the accessory to the host unit. The DS2705 supports insertion detection in four ways, two use the CHAL pin and two use the MDQ pin:

1. CHAL pin at the active logic level on IC power-up (detected after challenge delay time t_{CHD}). Positive or negative logic level is determined by the CHP bit.
2. CHAL pin edge trigger after power-up period. Positive or negative edge trigger is determined by the CHP bit.
3. Detection of Asynchronous 1-Wire Presence Pulse by insertion of battery with 1-Wire device (token).
4. Periodic Authentication Attempt issuing a 1-Wire Reset on MDQ to test for presence of a 1-Wire token.

With cases 1 and 2 above, the CHAL pin acts as a detection trigger when pulled to a logic low or logic high. A split contact on the battery ground or supply terminal can be used to connect the CHAL pin to the positive or negative battery terminal when the battery is present. In case 1, when the battery is connected prior to powering up the host system (which occurs often since the battery typically powers the host), presence is detected by sensing the logic level on CHAL immediately after power-up of the DS2705. A configuration bit, CHP, allows the use of either polarity of the CHAL pin. Table 1 shows the timing and sequence of events for detecting presence on power-up. In case 2 above, the DS2705 monitors the CHAL pin for a signal transition after the power-up period is complete. The DS2705 detects an authentication attempt on a positive or a negative edge of CHAL depending on the state of the CHP bit. Table 2 shows the timing and sequence of detecting presence with an edge on CHAL.

Table 1. Presence Detection/Authentication on Power-up Using CHAL Pin

TIME FROM POWER UP	CHAL PIN	CHP BIT	TOKEN PRESENCE	AUTHENTICATION	DISPLAY
t = N/A	High	0	Not Present	Armed	Hi-Z
$t < t_{CHD}$	Low	0	Present	Initiated	Hi-Z
$t_{CHD} > t > t_{CHD} + t_{AAT}$	Low	0	Present	In Progress	Hi-Z
$t > t_{CHD} + t_{AAT}$	Low	0	Present	Complete	Active
$t > t_{CHD} + t_{AAT}$	Pos Edge	0	Removal	Reset	Reset (Hi-Z)
t = N/A	Low	1	Not Present	Armed	Hi-Z
$t < t_{CHD}$	High	1	Present	Initiated	Hi-Z
$t_{CHD} > t > t_{CHD} + t_{AAT}$	High	1	Present	In Progress	Hi-Z
$t > t_{CHD} + t_{AAT}$	High	1	Present	Complete	Active
$t > t_{CHD} + t_{AAT}$	Neg Edge	1	Removal	Reset	Reset (Hi-Z)

t_{AAT}: Authentication attempt time represents the period for attempting authentication and is dependent on the RTA1:0 bits. Minimum time is t_{SHA}, maximum time is $8*t_{SHA}$.

Table 2. Insertion Detection/Authentication Using Transition On CHAL Pin

CHAL PIN	CHP BIT	TOKEN PRESENCE	AUTHENTICATION	DISPLAY
High	0	Not Present	Armed	Hi-Z
Neg Edge	0	Insertion	Initiated	Hi-Z
$Low < t_{CHD} + t_{AAT}$	0	Present	In Progress	Hi-Z
$Low > t_{CHD} + t_{AAT}$	0	Present	Complete	Active
Pos Edge	0	Removal	Reset	Reset
Low	1	Not Present	Armed	Hi-Z
Pos Edge	1	Insertion	Initiated	Hi-Z
High < 0.5s	1	Present	In Progress	Hi-Z
High > 0.5s	1	Present	Complete	Active
Neg Edge	1	Removal	Reset	Reset

Detection cases 3 and 4 occur through a 1-Wire Reset/Presence Detect sequence on the MDQ pin. In case 3, an asynchronous 1-Wire presence pulse occurs when a battery with a 1-Wire device is connected to the DS2705. The DS2705 responds with the authentication sequence. Case 4 is a user configuration option where a 1-Wire reset is periodically issued on MDQ which then monitors the bus for the presence pulse issued by any/all 1-Wire slave devices on the bus. If the DS2705 detects a presence pulse, it begins an authentication sequence. The DS2705 can also be configured to periodically test for the continued presence of a 1-Wire slave device once successful authentication has completed. This allows the status display to be automatically reset when a slave token has been removed. Table 3 shows the sequence and display activity for presence detection on MDQ.

Table 3. Asynchronous And Periodic Presence Detection Using MDQ Pin

PD	TOKEN PRESENCE	AUTHENTICATION	DISPLAY
No PD	Not Present	Reset	Hi-Z
PD	Insertion	Initiated	Hi-Z
	Present	In Progress	Hi-Z
		Complete	Active
No PD	Removal	Reset	Reset (Hi-Z)

AUTHENTICATION SEQUENCE

Following the detection of the battery, the DS2705 initiates the authentication sequence. The sequence is executed in whole each time authentication is initiated. See Figure 4.

1. Test for presence with 1-Wire RESET.
2. Issue SKIP ROM (SKIP NET ADDRESS) command.
3. Issue Write Challenge command with 64-bit Challenge data.
4. Issue Compute MAC without ROMID command to SHA-1 token.
5. Provide strong pullup on DQ output.
6. Issue 8 write 0 timeslots.
7. Issue read time slots to receive MAC from token.
8. Compare local and token MAC results.
9. If configured for multiple attempts, re-try until authentication complete.
10. Test for presence with 1-Wire RESET.
11. Update status on $\overline{\text{PASS}}$ or $\overline{\text{FAIL}}$ pins.

Note: If the DS2705 does not receive a presence pulse after presence has been established, or the presence test in step 9. fails, then the status is reported as not present with both the $\overline{\text{PASS}}$ and $\overline{\text{FAIL}}$ pins hi-Z.

PREPROGRAMMED CHALLENGE AND RESPONSE

A challenge response authentication system does not require a truly random set of challenges. The set of unique challenges must be sufficiently large that it precludes the use of a lookup table type of attack. If a large enough set of unique challenges is dispersed over a population of portable devices, then each portable device does not need to store the secret key and duplicate the computation of the MAC. It need only store one challenge response pair to provide a practical barrier to battery clones. This system requires that every battery contain the secret key and SHA-1 algorithm so that it is compatible with any portable device it might be required to power.

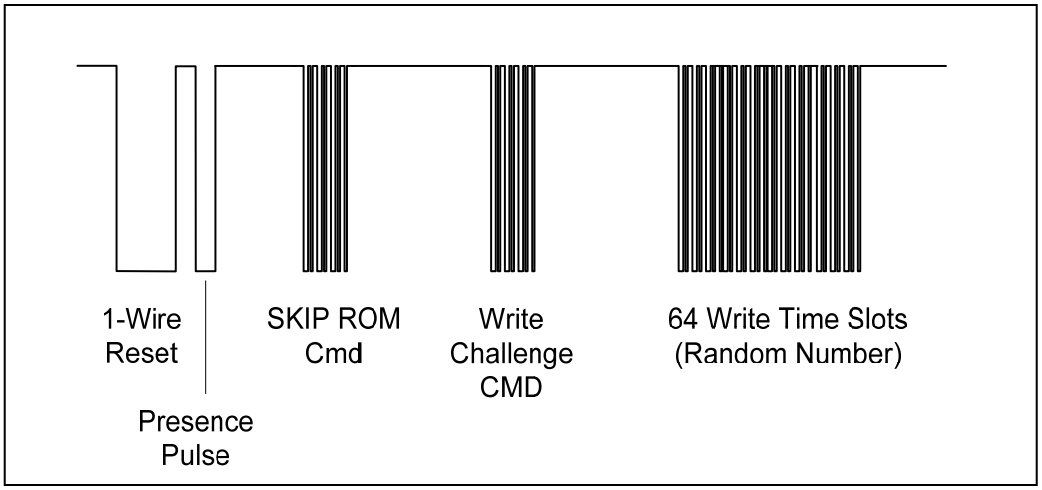
The DS2705 stores the preprogrammed challenge and response MAC. This serves to lower the cost and increase the secrecy of the key since the key does not have to be programmed into the DS2705. Dallas Semiconductor recommends not using any challenge response pair where either the challenge or MAC is all ‘0’s or all ‘1’s to prevent accidental authentication of an open or shorted communication bus.

MASTER PORT (MDQ) FUNCTION COMMANDS

MASTER MODE WRITE CHALLENGE COMMAND

Write Challenge [0Ch, XXXXXXXXXXXXXXXX]. The master mode Write Challenge command sends the 8-byte (64-bit) challenge to the remote token in preparation for a Compute MAC command.

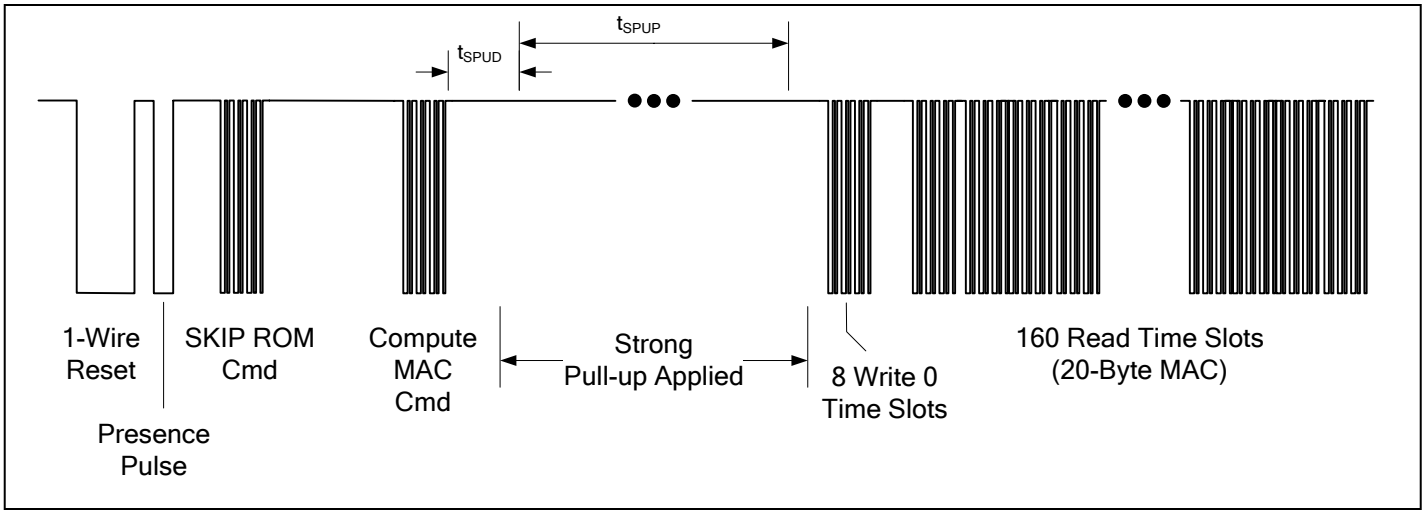
Figure 3. Write Challenge (MDQ)



MASTER MODE COMPUTE MAC W/O ROM ID COMMAND

Compute MAC without ROM ID [36h, XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX].
The Compute MAC command executes a MAC computation in the remote token and reads back the 20-byte result.

Figure 4. Compute and Return MAC (MDQ)



MAC Comparison

After the SHA-1 computation is completed by the remote token, the DS2705 and remote SHA-1 token both contain a MAC result based on the secret key. The results are compared by the DS2705 on a bit by bit basis as the MAC data is read in from the remote token. Note that the secret is never transmitted on the bus and thus cannot be captured by observing bus traffic.

Multiple Authentication Attempts

The DS2705 is configurable for multiple authentication attempts or re-tries to avoid reporting authentication failure in the event of contact bounce or a noisy communication channel. When configured for more than one retry, the status outputs are kept at the previous state until one attempt succeeds or all attempts fail. It is always recommended to configure the DS2705 for at least one retry.

Signaling Authentication Results

Authentication results are signaled on the open drain $\overline{\text{PASS}}$ and $\overline{\text{FAIL}}$ output pins. During an authentication attempt, both outputs remain at their previous state. After authentication is complete, the pass or fail status is reported until the display is cleared by one of the following conditions:

- CHAL pin returning to inactive logic level.
- Battery token removal detected when no 1-Wire Presence Pulse is returned in response to a 1-Wire Reset.

Table 4. PASS/FAIL Outputs

CONDITION	FOM BIT	$\overline{\text{PASS}}$ OUTPUT	$\overline{\text{FAIL}}$ OUTPUT
Token Not Present	x	Hi-Z	Hi-Z
Authentication in Progress	x	No Change	No Change
Complete: Pass	x	LOW	Hi-Z
Complete: Fail	0	Hi-Z	LOW
	1	Hi-Z	Pulse

PROGRAMMING AND CONFIGURING

The DS2705 requires a configuration step prior to deployment to program the 64-bit challenge, 160-bit response and to set up desired configuration options. Configuration is performed in slave mode using the SDQ and VPP pins. The Challenge-and-Response pair, and option data are programmed in on-chip EEPROM that requires an externally supplied programming voltage. After programming and verifying the EEPROM data, setting of the Lock bits is recommended to prevent future modification. SDQ and VPP have internal pull downs which prevent the pins from floating during normal operation.

Table 5. Configuration Register

FIELD	NAME	DESCRIPTION	DEFAULT
CR[1:0]	**RTA1:0**	Re-Tries Per Authentication Attempt Each re-try includes: OWR, PD, Skip ROM, Write Challenge, Read MAC, Compare MAC, Final OWR/PD 0 0 0 Re-try (1 attempt per initiation) 0 1 1 Re-tries (2 attempts per initiation) 1 0 3 Re-tries (4 attempts per initiation) 1 1 7 Re-tries (8 attempts per initiation) $\overline{PASS}$ output hi-Z until authentication complete. Authentication complete after first occurrence of a PASS result or all re-tries are a FAIL result	00b
CR[3:2]	**PAA1:0**	Periodic Authentication Attempt Each Attempt performed with the programmed number of re-tries: 0 0 No Periodic Attempts 0 1 Attempt every 1s 1 0 Attempt every 8s 1 1 Attempt every 16s $\overline{PASS}$ and $\overline{FAIL}$ pins retain previous states until updated when authentication completed. If presence not detected, status outputs are cleared to hi-Z.	00b
CR[5:4]	**PPT1:0**	Periodic Presence Test 1-Wire Presence test performed at programmed period: 0 0 No Periodic Test 0 1 Attempt every 0.25s 1 0 Attempt every 0.5s 1 1 Attempt every 1.0s $\overline{PASS}$ and $\overline{FAIL}$ pins retain previous states if presence detected. $\overline{PASS}$ and $\overline{FAIL}$ pins are cleared to hi-Z and status flags are cleared to zero if presence not detected.	00b
CR[6]	**APA**	Asynchronous Presence Authentication 0 No 1 Yes Authentication sequence initiated t_{CHD} ms delay after Presence Detect from token.	0b
CR[7]	**CHP**	CHAL Pin Polarity Setting 0 High to low transition; active low 1 Low to high transition; active high	0b
CR[8]	**FOM**	FAIL Output Select 0 $\overline{FAIL}$ pin held low 1 $\overline{FAIL}$ pin pulsed low at 2Hz 50% duty cycle	0b
CR[9]	**OWS**	1-Wire Bus Speed 0 Standard 1-wire communication (Master and Slave) 1 Overdrive 1-wire communication (Master and Slave)	0b
CR[11:10]	**LOCK1:0**	EEPROM Lock 0 0 No Operation 0 1 No Operation 1 0 Permanently Lock EEPROM 1 1 No Operation Writing a 10b to the lock bits, followed by an EEPROM copy will permanently lock all EEPROM locations inside the DS2705. Writing any other value to the lock bits will perform no operation.	00b
CR[12]	**—**	RESERVED	0b
CR[13]	**FAILF**	FAIL flag. Mirrors the $\overline{FAIL}$ pin output for test via slave interface (SDQ pin). Set if authentication attempt fails. Cleared when subsequent authentication attempt initiated.	0b
CR[14]	**PASSF**	PASS flag. Mirrors the $\overline{PASS}$ pin output for test via slave interface (SDQ pin). Set if authentication attempt passes. Cleared when subsequent authentication attempt initiated.	0b
CR[15]	**LOCKF**	Displays Lock/Unlock Status. LOCKF = 1 if lock procedure successful.	0b

MEMORY

The DS2705 has a 256 byte linear memory space for the EEPROM memory block that stores the challenge, response and configuration parameters. Addresses designated as “Reserved” typically return FFh when read. These bytes should not be written. EEPROM memory consists of non-volatile EEPROM cells overlaying volatile shadow RAM. The Read Data and Write Data protocols allow the 1-Wire interface to directly accesses the shadow RAM. The Copy Data and Recall Data function commands transfer data between the EEPROM cells and the shadow RAM. In order to modify the data stored in the EEPROM cells, data must be written to the shadow RAM and then copied to the EERPOM. In order to verify the data stored in the EEPROM cells, the EEPROM data must be recalled to the shadow RAM and then read from the shadow. After issuing the Copy Data function command, a programming pulse is required on the VPP pin.

Figure 5. EEPROM Access via Shadow RAM

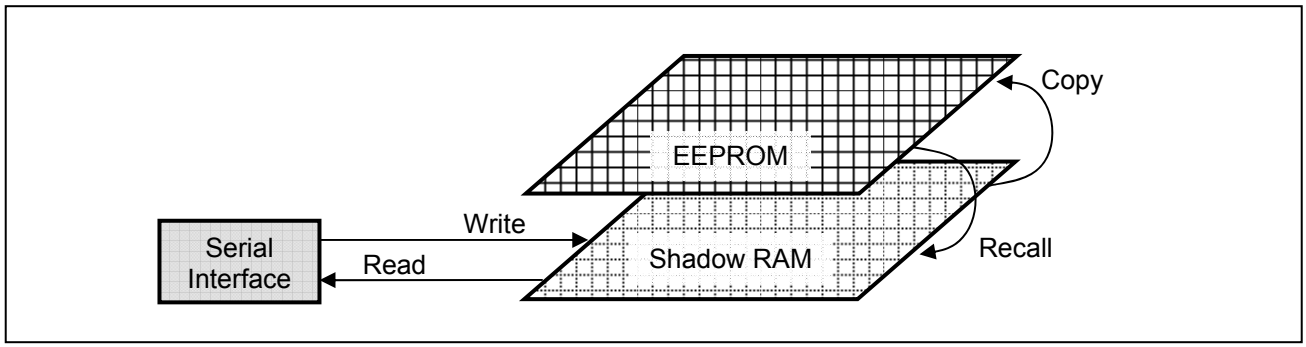


Table 6. Memory Map

ADDRESS (HEX)	DESCRIPTION	READ/WRITE
00 to 07	64-bit Challenge	R/W
08 to 1B	160-bit Response (Local MAC)	R/W
1C to 1D	Configuration Register	R/W
1E to FF	Reserved	—

1-Wire BUS SYSTEM

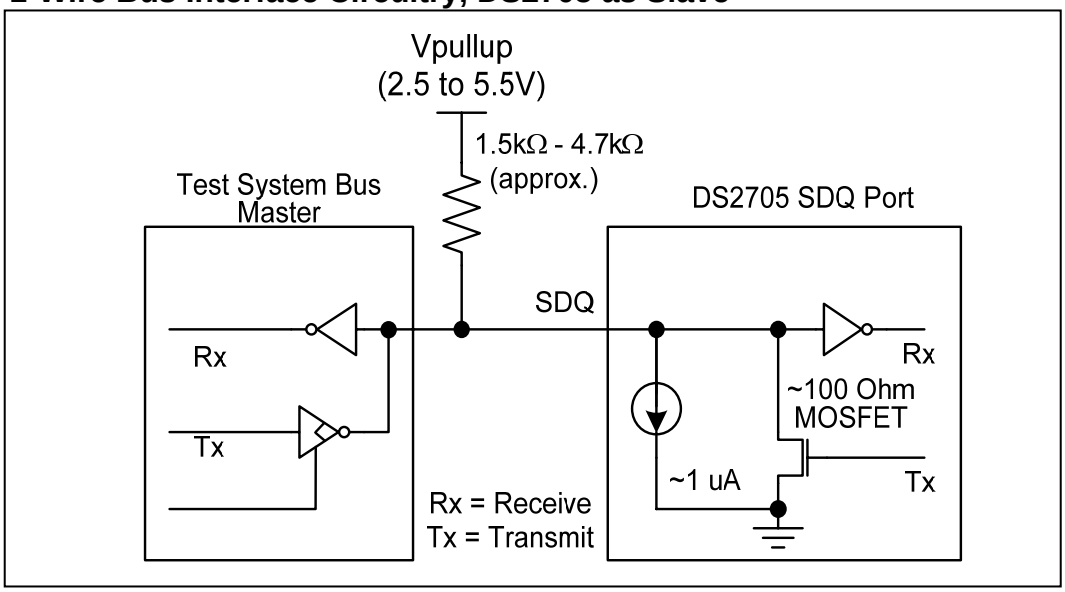
The 1-Wire bus is a system that has a single bus master and one or more slaves. A multidrop bus is a 1-Wire bus with multiple slaves, while a single-drop bus has only one slave device. The DS2705 acts as a bus master on the MDQ pin and as a slave device on the SDQ pin. In both cases, the DS2705 requires a single-drop bus configuration. The discussion of the 1-Wire bus system consists of three topics: hardware configuration, transaction sequence, and 1-Wire signaling.

HARDWARE CONFIGURATION

Because the 1-Wire bus has only a single line, 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 connect to the bus with open-drain or tri-state output drivers. The DS2705 uses an open-drain output driver as part of the bidirectional interface circuitry shown in Figure 6. If a bidirectional pin is not available to act as the bus master when communicating with the DS2705 as a slave on the SDQ pin, separate output and input pins can be connected together.

The 1-Wire bus must have a pullup resistor at the bus-master end of the bus. The DS2705 internally provides the pullup for communication as a master on the MDQ pin. The bus master communicating with the DS2705 on SDQ is responsible for providing an external pullup . The idle state for the 1-Wire bus is high. If, for any reason, a bus transaction must be suspended, the bus must be left in the idle state to properly resume the transaction later. Note that if the bus is left low for more than t_{LOW0}, slave devices on the bus begin to interpret the low period as a reset pulse, which effectively terminates the transaction.

Figure 6. 1-Wire Bus Interface Circuitry, DS2705 as Slave



TRANSACTION SEQUENCE

The protocol for 1-Wire communication is as follows:

- Initialization
- Net Address Command
- Function Command(s)
- Data Transfer (not all commands have data transfer)

All transactions of the 1-Wire bus begin with an initialization sequence consisting of a reset pulse transmitted by the bus master, followed by a presence pulse transmitted by a slave if it is present on the bus. The presence pulse tells the bus master that a slave device is on the bus and ready to operate. For more details, see the *1-Wire Signaling* section.

NET ADDRESS COMMANDS

Once the bus master has detected the presence of a slave, it can issue the net address command described in the following paragraph. The name of the Net Address command (ROM command) is followed by its 8-bit opcode in square brackets.

Skip Net Address [CCh]. The only net address command supported by the DS2705 is the Skip Net Address command. It is preserved on the DS2705 for compatibility with multidrop enabled slaves such as the DS2703/4. Skip Net Address must also be used after a reset pulse when a bus master is communicating to the DS2705 over the SDQ input.

SLAVE PORT (SDQ) FUNCTION COMMANDS

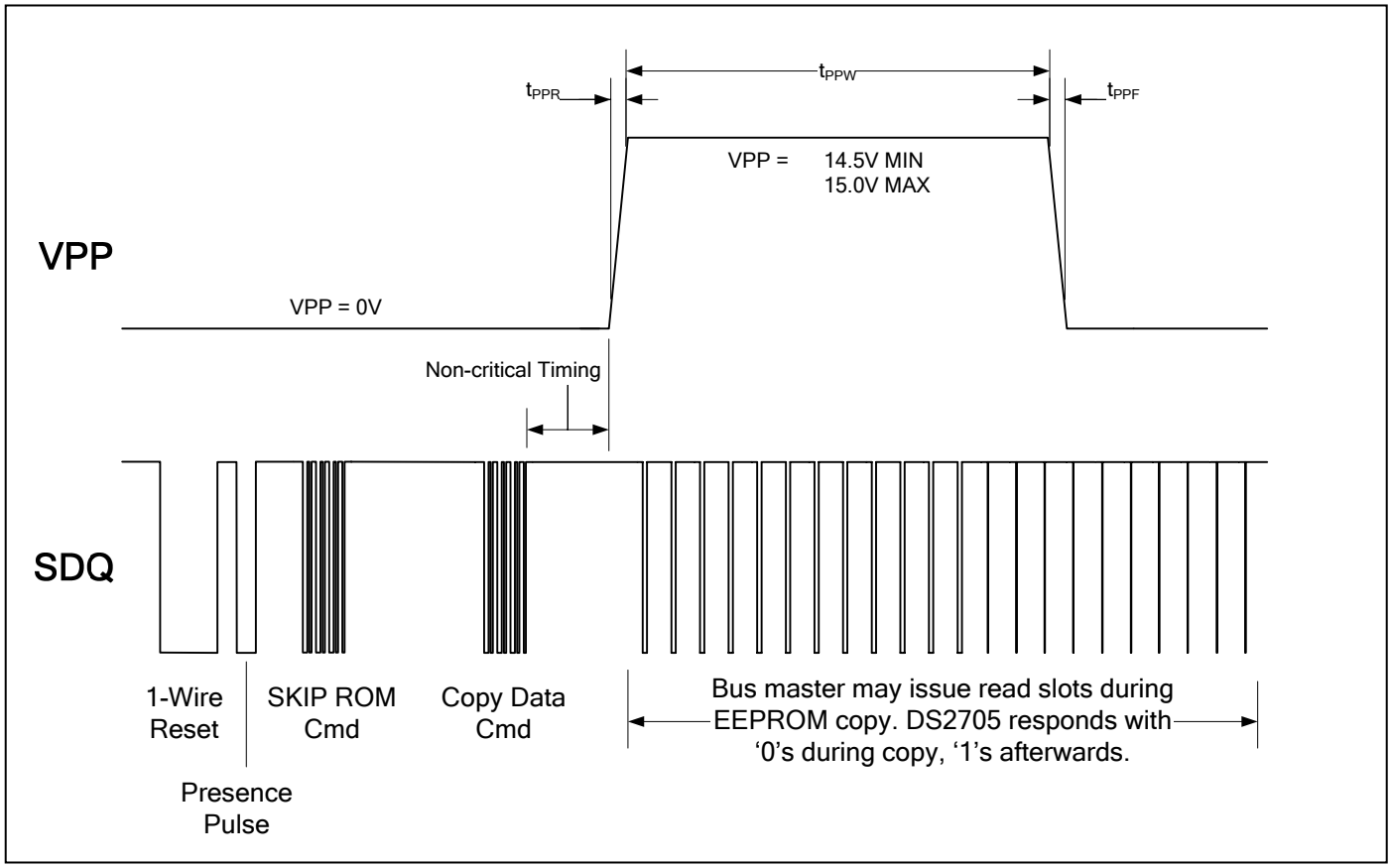
After successfully completing the Skip Net Address command, the bus master can access the features of the DS2705 with any of the function commands described in the following paragraphs. The name of each function is followed by the 8-bit opcode for that command in square brackets. The function commands are summarized in Table 7.

Read Data [69h, XX]. This command reads data starting at memory address XX. The LSb of the data in address XX is available to be read immediately after the MSb of the address has been entered. Because the address is automatically incremented after the MSb of each byte is received, the LSb of the data at address XX + 1 is available to be read immediately after the MSb of the data at address XX. If the bus master continues to read beyond address FFh, data is read starting at memory address 00 and the address is automatically incremented until a reset pulse occurs. Addresses labeled “Reserved” in the memory map contain undefined data values. The read data command can be terminated by the bus master with a reset pulse at any bit boundary. Read Data from returns the data in the shadow RAM. A Recall Data command is required to transfer data from the EEPROM to the shadow. See the *Memory* section for more details.

Write Data [6Ch, XX]. This command writes data starting at memory address XX. The LSb of the data to be stored at address XX can be written immediately after the MSb of address has been entered. Because the address is automatically incremented after the MSb of each byte is written, the LSb to be stored at address XX + 1 can be written immediately after the MSb to be stored at address XX. If the bus master continues to write beyond address FFh, the data starting at address 00 is overwritten. Writes to read-only addresses, reserved addresses and locked EEPROM blocks are ignored. Incomplete bytes are not written. Write Data modifies the shadow RAM. A Copy Data command is required to transfer data from the shadow to the EEPROM. See the *Memory* section for more details. The Write command will cause spurious behavior if issued during an authentication attempt is in progress on the MDQ pin.

Copy Data [48h]. This command copies the contents of all shadow RAM locations to EEPROM cells. After the copy command is issued a high voltage pulse must be applied to the VPP pin for a time period of t_{PPW}. See Figure 7 for example bus timing of an EEPROM program function. During the pulse, the bus master can issue read timeslots on the bus. The DS2705 will respond with '0's while the EEPROM copy is in progress, and '1's after the copy is complete. A reset on SDQ at any time during the copy sequence will prematurely terminate the operation.

Figure 7. Copy EEPROM Sequence



Recall Data [B8h]. This command recalls the contents of all EEPROM cell locations to the shadow RAM memory. Following the Recall command, SDQ must be driven low for a minimum of t_{RSTL}. SDQ can be driven low indefinitely after the Recall command. The Recall command will cause spurious behavior if issued while an authentication attempt is in progress on the MDQ pin.

Table 7. Slave Function Commands

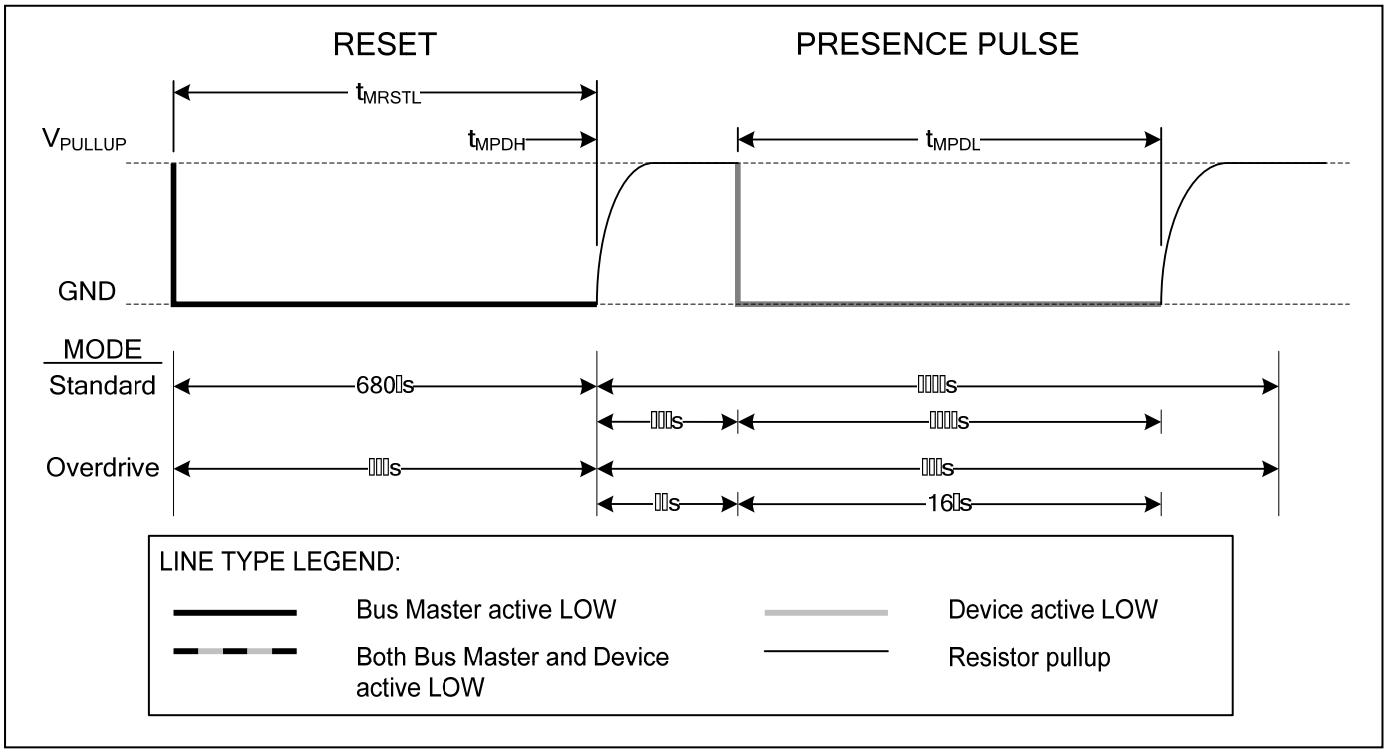
COMMAND	DESCRIPTION	COMMAND PROTOCOL	BUS STATE AFTER COMMAND PROTOCOL	BUS DATA
Read Data	Reads data from memory starting at address XX	RESET CCh 69h Address	Master Rx	Up to 256 bytes of data
Write Data	Writes data to memory starting at address XX	RESET CCh 6Ch Address	Master Tx	Up to 256 bytes of data
Copy Data	Copies shadow RAM data to EEPROM	RESET CCh 48h Program Pulse	Master Rx	Read data = 0 until command completes
Recall Data	Recalls EEPROM to shadow RAM	RESET CCh B8h	Master Reset	None

I/O SIGNALING

The 1-Wire bus requires strict signaling protocols to ensure data integrity. The four protocols used in 1-Wire communication are as follows: the initialization sequence (reset pulse followed by presence pulse), write 0, write 1, and read data. The 1-Wire bus master initiates all these types of signaling except the presence pulse.

The initialization sequence required to begin any 1-Wire communication is shown in Figure 8. A presence pulse following a reset pulse indicates that the 1-Wire slave is ready to accept a net address command. The bus master transmits (Tx) a reset pulse for t_{RSTL}. The bus master then releases the line and goes into receive mode (Rx). The 1-Wire bus line is then pulled high by the pullup resistor. After detecting the rising edge on the DQ pin, the slave waits for t_{PDH} and then transmits the presence pulse for t_{PDL}.

Figure 8. 1-Wire Initialization Sequence



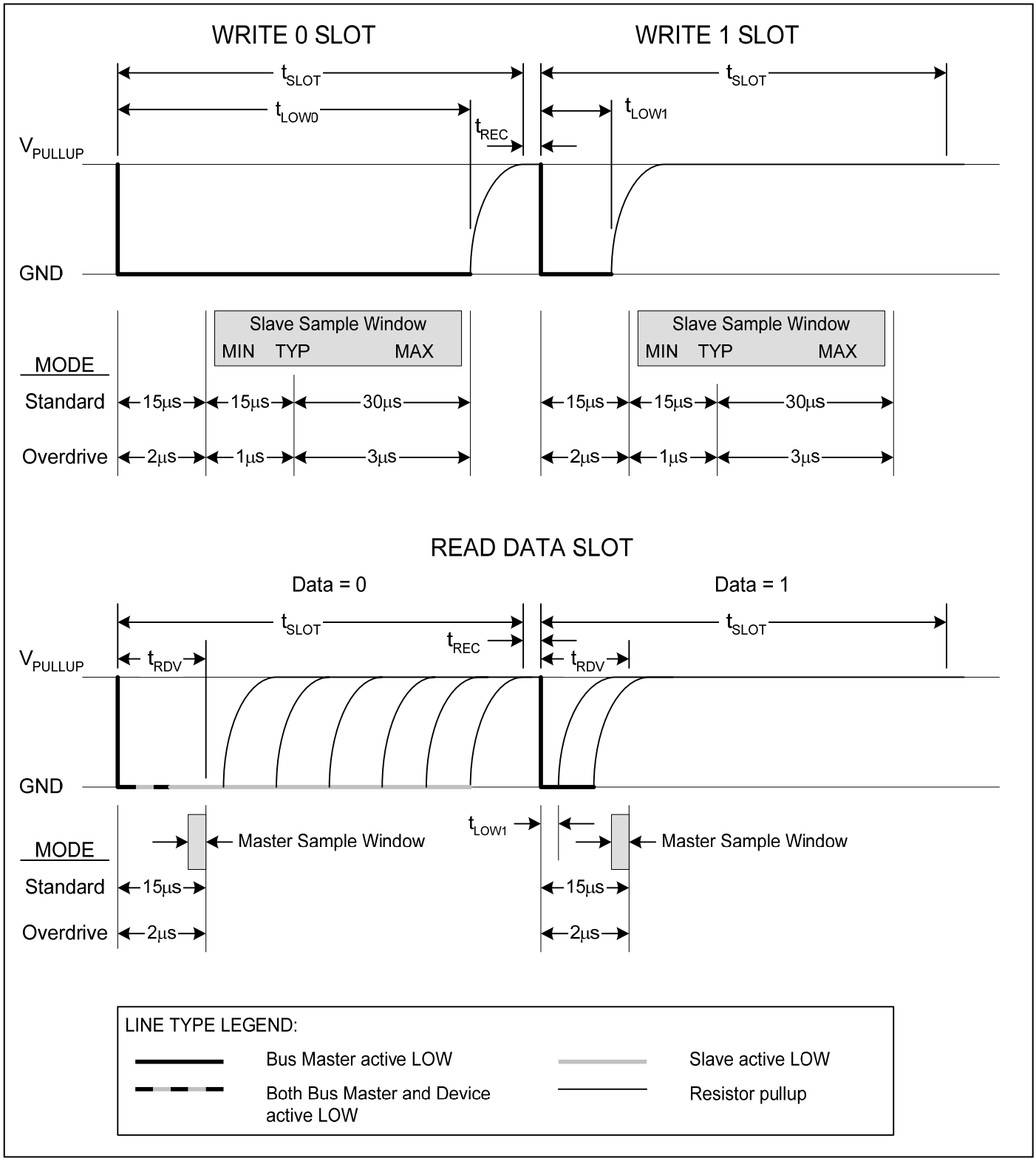
WRITE-TIME SLOTS

A write-time slot is initiated when the bus master pulls the 1-Wire bus from a logic-high (inactive) level to a logic-low level. There are two types of write-time slots: write 1 and write 0. All write-time slots must be t_{SLOT} in duration with a 1µs minimum recovery time, t_{REC}, between cycles. The slave samples the 1-Wire bus line between t_{LOW1_MAX} and t_{LOW0_MIN} after the line falls. If the line is high when sampled, a write 1 occurs. If the line is low when sampled, a write 0 occurs. The sample window is illustrated in Figure 9. 1-Wire Write and Read-Time Slots. For the bus master to generate a write 1 time slot, the bus line must be pulled low and then released, allowing the line to be pulled high less than t_{RDV} after the start of the write time slot. For the host to generate a write 0 time slot, the bus line must be pulled low and held low for the duration of the write-time slot.

READ-TIME SLOTS

A read-time slot is initiated when the bus master pulls the 1-Wire bus line from a logic-high level to a logic-low level. The bus master must keep the bus line low for at least 1µs and then release it to allow the slave to present valid data. The bus master can then sample the data t_{RDV} from the start of the read-time slot. By the end of the read-time slot, the slave releases the bus line and allows it to be pulled high by the external pullup resistor. All read-time slots must be t_{SLOT} in duration with a 1µs minimum recovery time, t_{REC}, between cycles. See Figure 9 and the timing specifications in the Electrical Characteristics table for more information.

Figure 9. 1-Wire Write and Read-Time Slots



PACKAGE INFORMATION

(For the latest package outline information, go to **www.maxim-ic.com/DallasPackInfo**.)