EVALUATION KIT AVAILABLE

MAX66242 DeepCover Secure Authenticator with ISO 15693, I^{2}C, SHA-256, and 4Kb User EEPROM

General Description

DeepCover® embedded security solutions cloak sensitive data under multiple layers of advanced physical security to provide the most secure key storage possible.

The DeepCover Secure Authenticator (MAX66242) is a transponder IC that combines an ISO/IEC 15693 and ISO 18000-3 Mode 1-compatible RF front-end, an I^{2}C front-end, a FIPS 180-based SHA-256 engine and 4096 bits of user EEPROM in a single chip. A bidirectional security model enforces two-way authentication between a host system and the MAX66242. Each device has its own guaranteed unique 64-bit ROM ID that is factory programmed into the chip. This ROM ID is used as a fundamental input parameter for cryptographic operations and serves as an electronic serial number within the application.

In addition to the RF interface, the MAX66242 also has an I^{2}C interface, which can operate as a slave or master port. When acting as a master, the MAX66242 can gather information from a connected sensor or peripheral device and relay its data via the RF port. When acting as a slave, the device can serve as an intermediary between a connected host and an RF reader. The MAX66242 can harvest energy from an active RF field. The configurable supply output can deliver up to 5mA given adequate field strength.

Applications

- Access Control
- Asset Tracking
- Printer Cartridge Configuration and Monitoring
- Medical Sensor Authentication and Calibration
- System Intellectual Property Protection

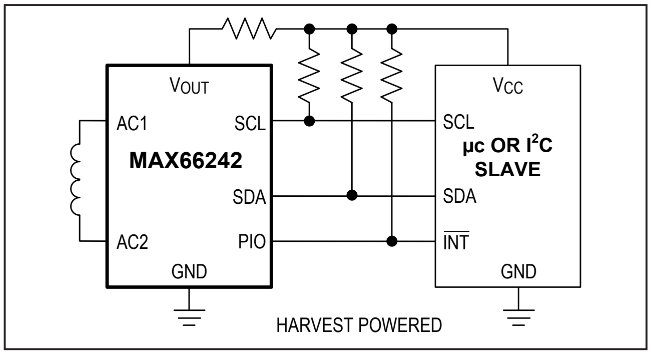
***Ordering Information* appears at end of data sheet.**

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

Benefits and Features

- Complete Counterfeit/Cloning/IP Protection Engine
  - SHA-256 Engine Runs a Symmetric Key-Based Bidirectional Secure Authentication
  - Strong Authentication Achieved with a High Bit Count, User-Programmable Secret, and Input Challenge
  - Batteryless RF Communication
  - 4096 Bits of User EEPROM with User-Programmable Memory
  - Memory R/W Protection Options Including OTP/EPROM Emulation Mode
  - Unique Factory-Programmed 64-Bit Identification Number
  - Integrated 32-Byte SRAM Buffer Enables Faster HF-to-I^{2}C Transactions
- Flexible Connection and Communication Capabilities Support a Wide Range of Applications
  - Programmable I/O (PIO) Can Be Configured as a Wake-Up or Monitoring/Control Signal
  - HF Standards ISO/IEC 15693 and 18000-3 MODE1 Compatible (13.56 MHz ±7kHz Carrier Frequency)
  - I^{2}C Interface—Master/Slave Port Eliminates Host Microcontroller for Sensor-Tag Applications
  - Energy Harvesting V_{OUT} Pin for Powering External Components
  - Optional 3.3V Supply Voltage Fits Line and Battery-Powered Applications
  - -40°C to +85°C Operating Temperature Range
- Enables Robust Design
  - ±4kV HBM ESD Protection on PIO, ±2kV on All Other Pins

Typical Application Circuits



***Typical Application Circuits* continued at end of data sheet.**

Absolute Maximum Ratings

Voltage Range on Any Pin Relative to GND	-0.5V to +4.0V
Maximum Current Into Any Pin Except AC1 or AC2	20mA
Maximum RMS Current, AC1 to AC2	30mA
Maximum Incident Magnetic Field Strength (ISO/IEC 7810-compliant antenna)	141.6dBμA/m
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)	+260°C

Stresses beyond those listed under “Absolute Maximum Ratings” may cause permanent damage to the device. These are stress ratings only, and functional operation of the device at these or any other conditions beyond those indicated in the operational sections of the specifications is not implied. Exposure to absolute maximum rating conditions for extended periods may affect device reliability.

Package Thermal Characteristics (Note 1)

SO	
Junction-to-Ambient Thermal Resistance (θ_{JA})	136°C/W
Junction-to-Case Thermal Resistance (θ_{JC})	38°C/W
TDFN	
Junction-to-Ambient Thermal Resistance (θ_{JA})	60°C/W
Junction-to-Case Thermal Resistance (θ_{JC})	30°C/W

Note 1: 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

(T_A = -40°C to +85°C, unless otherwise noted.) (Note 2)

PARAMETER	SYMBOL	CONDITIONS	MIN	TYP	MAX	UNITS
Supply Voltage	V_{CC}		2.97	3.3	3.63	V
Active Supply Current	I_{CCA}	(Note 3)			110	μA
Standby Supply Current	I_{CCS}				100	μA
Power-Up Time	t_{POR}				1	ms
SHA-256 ENGINE						
Computation Current	I_{CSHA}	V_{CC} = 3.63V (Note 4)			1.5	mA
Computation Time	t_{CSHA}	(Note 5)			2	ms
EEPROM						
Programming Current	I_{PROG}	V_{CC} = 3.63V (Note 4)			1.5	mA
Programming Time for a 32-Bit Page Block or Protection	t_{PROG}	(Note 6)			10	ms
Write/Erase Cycling Endurance	N_{CY}	T_A = +85°C (Notes 7, 8)	100k			—
Data Retention	t_{DR}	T_A = +85°C (Notes 9, 10, 11)	10			Years
PIO PIN						
Input Current with Input Voltage Between 0.1V_{CC} and 0.9V_{CCMAX}	I_{I_PIO}				1	μA
Input Low Voltage	V_{IL_PIO}		-0.3		0.4	V
Input High Voltage	V_{IH_PIO}		1.62			V
Output Low Voltage	V_{OL_PIO}	4mA sink current			0.4	V
RF PORT						
Carrier Frequency	f_C	(Note 12)	13.553	13.560	13.567	MHz
Internal Tuning Cap	C_{TUN}	f = 13.56 MHz (Note 13)		27.5		pF

Electrical Characteristics (continued)

(T_A = -40°C to +85°C, unless otherwise noted.) (Note 2)

PARAMETER	SYMBOL	CONDITIONS	MIN	TYP	MAX	UNITS
Operating Field	H_{ISO}	(Note 12)	150		5000	mA/m
Activation Field Strength	H_{MIN_10}	10%–30% modulation index (Note 13)		100		dBμA/m
Activation Field Strength	H_{MIN_100}	100% modulation index (Note 13)		101.2		dBμA/m
Write/SHA Field Strength	H_{WR}	(Notes 13, 14)		113		dBμA/m
V_{OUT} Field Strength	H_{MINOUT}	(Note 13)		122		dBμA/m
V_{OUT} Transition Time	t_{VOUT}	(Notes 13, 15)		250		μs
RF Access In Progress Time	t_{RFAIP}	(Notes 16)		1.1		ms
10% Carrier Modulation Index Min MI = (A - B)/(A + B)	CMI_10_{MIN}	(Notes 12, 13, 17)		10		%
10% Carrier Modulation Index Max MI = (A - B)/(A + B)	CMI_10_{MAX}	(Notes 12, 13)			30	%
100% Carrier Modulation Index MI = (A - B)/(A + B)	CMI_100	(Notes 12, 13)	95		100	%
10% Modulation Min Pulse Width	t_1 MIN	Refer to ISO 15693-2 Section 7.1 (Notes 13, 18)		7.0		μs
10% Modulation Max Pulse Width	t_1 MAX	Refer to ISO 15693-2 Section 7.1 (Note 13)			9.44	μs
10% Modulation Min Low Time	t_2 MIN	Refer to ISO 15693-2 Section 7.1 (Notes 13, 18)		7.0		μs
10% Modulation Max Low Time	t_2 MAX	Refer to ISO 15693-2 Section 7.1 (Note 13)			9.44	μs
10% Modulation Min Rise Time	t_3 MIN	Refer to ISO 15693-2 Section 7.1 (Note 13)	0			μs
10% Modulation Max Rise Time	t_3 MAX	Refer to ISO 15693-2 Section 7.1 (Notes 13, 18)		2.5		μs
100% Modulation Min Pulse Width	t_1 MIN	Refer to ISO 15693-2 Section 7.1 (Notes 13, 18)		6.5		μs
100% Modulation Max Pulse Width	t_1 MAX	Refer to ISO 15693-2 Section 7.1 (Note 13)			9.44	μs
100% Modulation Min Low Time	t_2 MIN	Refer to ISO 15693-2 Section 7.1 (Notes 13, 18)		6.5		μs
100% Modulation Max Low Time	t_2 MAX	Refer to ISO 15693-2 Section 7.1 (Note 13)			9.44	μs
100% Modulation Min Rise Time	t_3 MIN	Refer to ISO 15693-2 Section 7.1 (Note 13)	0			μs
100% Modulation Max Rise Time	t_3 MAX	Refer to ISO 15693-2 Section 7.1 (Notes 13, 18)		3.0		μs
RF Timeout	$t_{RF\_TIMEOUT}$	(Note 13)		45		ms

Electrical Characteristics (continued)

(T_A = -40°C to +85°C, unless otherwise noted.) (Note 2)

PARAMETER	SYMBOL	CONDITIONS		MIN	TYP	MAX	UNITS
SCL, SDA PINS (Note 21)							
Low Level Input Voltage	V_{IL}			-0.3		0.10 x V_{CC}	V
High Level Input Voltage	V_{IH}			0.8 x V_{CC}		V_{CC} + 0.3	V
Hysteresis of Schmitt Trigger Inputs	V_{HYS}	(Note 13)			0.3		V
Output Low Voltage	V_{OL}	4mA sink current	T_A = -20°C to +85°C			0.10 x V_{CC}	V
			T_A = -40°C to -20°C			0.40	
Output Fall Time from V_{IHMIN} to V_{ILMAX} with a Bus Capacitance from 10pF to 400pF	t_{OF}	(Note 13)			150		ns
Input Current with Input Voltage Between 0.1V_{CC} and 0.9V_{CCMAX}	I_I	(Note 20)		-1		+1	µA
SCL Clock Frequency	f_{SCL}	(Notes 13, 21)				400	kHz
Master Mode Frequency	f_{MSTR}	f_C = 13.56MHz			53		kHz
I2C Timeout	$t_{I2C\_TIMEOUT}$	(Note 21)		25		50	ms
Hold Time (Repeated) START Condition.	$t_{HD:STA}$			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
Setup Time for a Repeated START Condition	$t_{SU:STA}$			0.6			µs
Data Hold Time	$t_{HD:DAT}$	(Notes 13, 22, 23)				0.9	µs
Data Setup Time	$t_{SU:DAT}$	(Notes 24)		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	(Notes 12, 13)				400	pF

Electrical Characteristics (continued)

(T_A = -40°C to +85°C, unless otherwise noted.) (Note 2)

Note 2: Limits are 100% production tested at T_A = +25°C 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 at 25°C.

Note 3: Operating current continuously reading the Memory/MAC Read/Write Register at 400kHz with no RF power.

Note 4: Current drawn during the EEPROM programming interval or SHA-256 computation.

Note 5: For commands where the t_{CSHA} interval occurs see the applicable Communication Examples sections. For RF commands, the interval begins after the EOF of a valid request frame. For I^2C commands the interval begins after the Acknowledge bit of the last data byte. The interval ends once the device's self-timed SHA-256 computation cycle is complete.

Note 6: For commands where the t_{PROG} interval occurs see the applicable Communication Examples sections. For RF commands, the interval begins after the EOF of a valid request frame. For I^2C commands the interval begins after the Acknowledge bit of the last data byte. The interval ends once the device's self-timed EEPROM write cycle is complete.

Note 7: Write-cycle endurance is tested in compliance with JESD47G.

Note 8: Not 100% production tested; guaranteed by reliability qualification.

Note 9: Data retention is tested in compliance with JESD47G.

Note 10: Guaranteed by 100% production test at elevated temperature for a shorter time; equivalence of this production test to the data sheet limit at operating temperature range is established by reliability testing.

Note 11: EEPROM writes can become nonfunctional after the data-retention time is exceeded. Long-term storage at elevated temperatures is not recommended.

Note 12: System requirement.

Note 13: Guaranteed by design, and/or characterization only. Not production tested.

Note 14: Applies to Read/Write Scratchpad (writing), Write Memory, Compute and Read Page MAC, Set Protection, Authenticated Write Memory RF Setup, Authenticated Write Memory RF Execute, Authenticated Set Protection RF Setup, Authenticated Set Protection RF Execute, and Configuration Write commands.

Note 15: Measured from V_{OUT} = 1.8V to V_{OUT} = 3.3V at 2.5A/m with a 0.1μF load.

Note 16: The t_{RFAIP} interval begins immediately after an EOF for a valid ISO15693 request frame and ends before SOF of the response frame. A pulse of width t_{RFAIP} will only occur only for Read/Write Scratchpad (writing) and Control Write.

Note 17: CMI_10 > 15% is suggested.

Note 18: Field strength between 350mA/m and 5A/m.

Note 19: All I^2C timing values are referred to $V_{IH\ MIN}$ and $V_{IL\ MAX}$ levels.

Note 20: I/O pins of the MAX66242 do not obstruct SDA and SCL lines if V_{CC} and the RF fields are switched off.

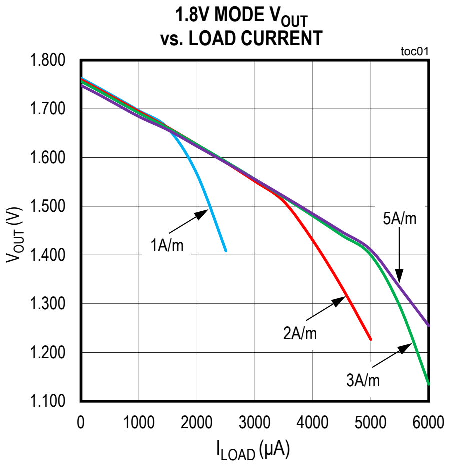
Note 21: The minimum SCL clock frequency is limited by the I^2C timeout feature. If SCL remains low longer than this interval, the MAX66242 behaves as though it has sensed a STOP condition. SDA has no affect on this timeout condition.

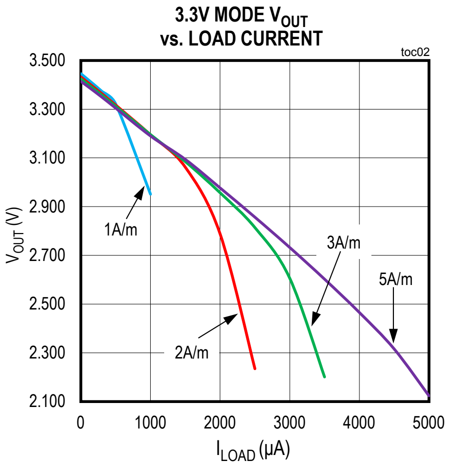
Note 22: The MAX66242 provides a hold time of at least 200ns for the SDA signal (referred to the V_{IHMIN} of the SCL signal) to bridge the undefined region of the falling edge of SCL.

Note 23: The master can provide a hold time of 0ns minimum when writing to the device.

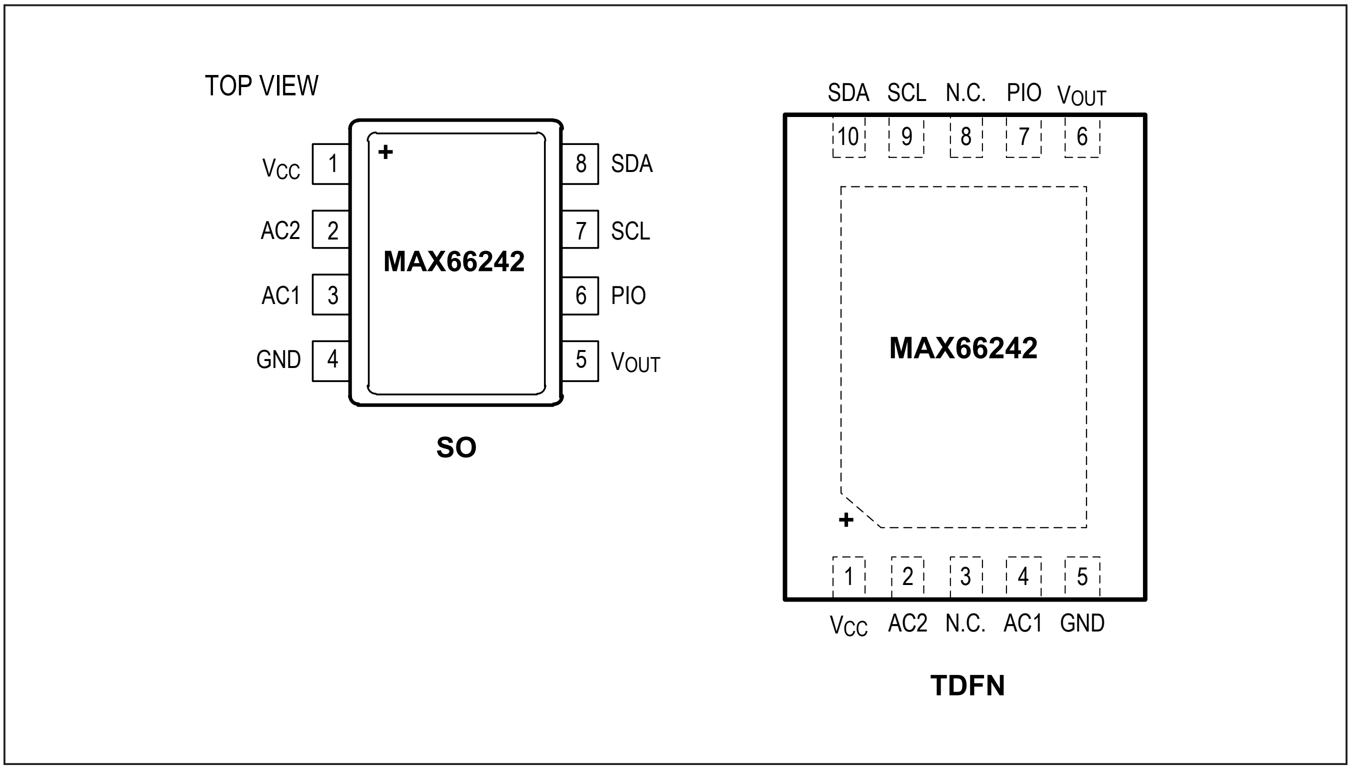
Note 24: A fast-mode I^2C-bus device can be used in a standard-mode I^2C-bus system, but the requirement $t_{SU:DAT} \geq 250ns$ must then be met. This is automatically the case if the device does not stretch the LOW period of the SCL signal. If such a device does stretch the LOW period of the SCL signal, it must output the next data bit to the SDA line $t_{RMAX} + t_{SU:DAT}$ = 1000 + 250 = 1250ns (according to the standard-mode I^2C-bus specification) before the SCL line is released.

Typical Operating Characteristics





Pin Configurations



Pin Descriptions

PIN		NAME	FUNCTION
SO	TDFN		
1	1	V_{CC}	Power-Supply Input
2	2	AC2	Antenna Connection
3	4	AC1	Antenna Connection
4	5	GND	Ground Reference
5	6	V_{OUT}	Energy Harvesting Pin. See the *PIO and Energy Harvesting Output* section.
6	7	PIO	Multipurpose Open-Drain Pin. See the *PIO and Energy Harvesting Output* section.
7	9	SCL	I2C Serial Clock Input
8	10	SDA	I2C Serial Data Input/Output
—	3, 8	N.C.	Not Connected

Detailed Description

The MAX66242 transponder combines an ISO 15693 RF front-end, a SHA-256 engine, 4096 bits of user EEPROM organized as 16 256-bit pages, protection control, status memory, and a 64-bit ROM ID in a single chip. A 256-bit scratchpad assists when installing a new secret or stores the challenge when computing a page MAC. In addition to the RF interface, the part also has an I2C interface, which can operate as slave port or as master port.

It is common for a secure authentication IC to be attacked using a variety of sophisticated die-level methods to extract secure data, reverse device settings, etc., in an effort to compromise a system security implementation. To provide the highest affordable protection against this inevitable malicious attack, the MAX66242 employs proprietary die-level physical techniques, circuits, and crypto methods to protect sensitive data, control signals, and control settings.

There are multiple programmable options for the 4Kb user array including unrestricted read/write and four protection modes: read protection, write protection, EPROM emulation mode, and authentication protection. Read protection prevents user read-access to the memory, which effectively extends the secret into the protected memory. The data remains accessible only for the SHA-256 engine. Write protection prevents changes to the memory data. EPROM emulation mode logically ANDs memory data with incoming new data, which allows changing bits from 1 to 0, but not vice versa. By changing one bit at a time, this mode could be used to create a nonvolatile, nonresettable counter. EPROM emulation mode requires that the memory is not write protected. Authentication protection, if activated, requires that the host prove itself as authentic (i.e., knows the MAX66242 secret) to modify the memory by supplying a correct MAC that is based on the device secret, its ROM ID, memory data, and the new data to be copied to EEPROM. If the authentication hurdle is passed, the write protection and EPROM emulation mode protections still determine the effect of the write access. Any protection, if activated, applies to individual memory pages. As a factory default, none of the protections is activated. Once authentication protection is activated, the reader must authenticate itself for memory writes as well as for additional changes to the memory protection.

In addition to its important use as a unique data value in cryptographic SHA-256 computations, the device's 64-bit ROM ID can be used to electronically identify the object to which the MAX66242 is associated. Applications of the MAX66242 include, access control, asset tracking, printer cartridge configuration and monitoring, medical sensor authentication and calibration, and system intellectual property protection.

Overview

The block diagram in Figure 1 shows the relationships between the major control and memory sections of the MAX66242. The device has six main data components: 16 256-bit pages of user EEPROM, a 256-bit secret, protection control/status memory, 512-bit SHA-256 engine, 64-bit ROM ID, and a 256-bit scratchpad.

Figure 2 shows the applicable commands and the affected data fields. The network function commands allow the reader to identify all transponders in its range and to change their state, e.g., to select one for further communication. The protocol required for these network function commands is described in the *Network Function Commands* section. The memory and control functions fall into seven categories: ISO 15693 generic commands, secret installation, memory access, protection setting, MAC computation, configuration and control with verification, and I2C master port operation. The protocol for these commands is described in the *Memory and Control Function Commands* section. All data is read and written least significant bit (LSb) first, starting with the least significant byte (LSB).

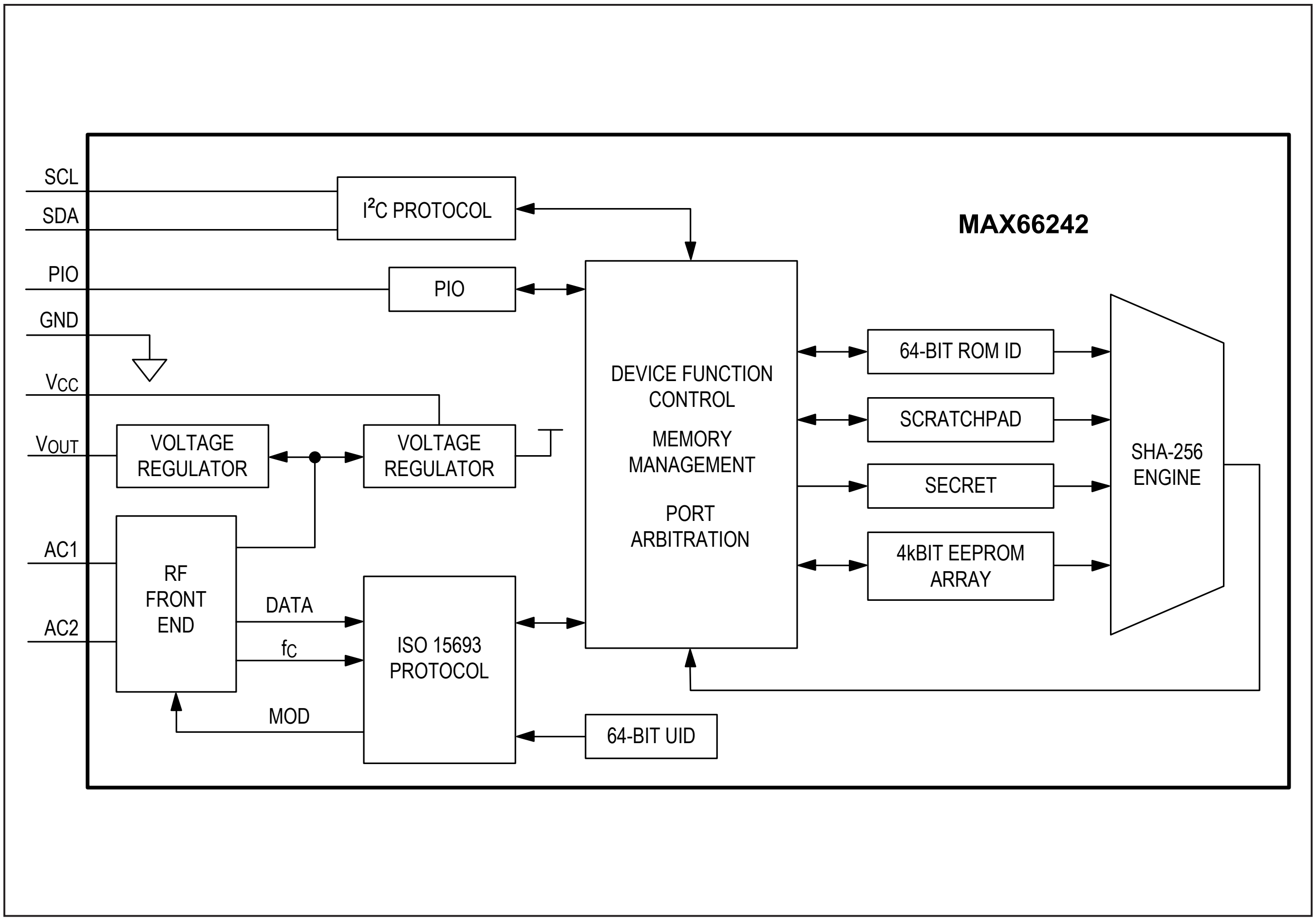


Figure 1. Block Diagram

COMMAND TYPE:	AVAILABLE COMMANDS:	DATA FIELD AFFECTED:
NETWORK FUNCTION COMMANDS	INVENTORY	UID, AFI, DSFID
	STAY QUIET	UID
	SELECT	UID
	RESET TO READY	(N/A)
MEMORY AND CONTROL FUNCTION COMMANDS	GET SYSTEM INFORMATION	UID, AFI, DSFID, CONSTANTS
	WRITE MEMORY	MFGCODE, USER MEMORY, PROTECTION SETTINGS
	READ MEMORY	MFGCODE, USER MEMORY, PROTECTION SETTINGS
	READ SINGLE BLOCK	SELECTED MEMORY BLOCK, PROTECTION SETTINGS
	READ MULTIPLE BLOCKS	SELECTED MEMORY BLOCKS, PROTECTION SETTINGS
	SET PROTECTION	MFGCODE, PROTECTION SETTINGS
	READ STATUS	MFGCODE, PROTECTION SETTINGS, PERSONALITY BYTES
	READ/WRITE SCRATCHPAD	MFGCODE, SCRATCHPAD
	LOAD AND LOCK SECRET	MFGCODE, SECRET AND LOCK STATUS, SCRATCHPAD
	COMPUTE AND LOCK SECRET	MFGCODE, SECRET AND LOCK STATUS, USER MEMORY, SCRATCHPAD, PROTECTION SETTING
	COMPUTE AND READ PAGE MAC	MFGCODE, SECRET, ROM ID, USER MEMORY, SCRATCHPAD
	AUTHENTICATED WRITE MEMORY RF SETUP	MFGCODE, USER MEMORY, PAGE BLOCK NUMBER, SECRET, PROTECTION SETTINGS
	AUTHENTICATED WRITE MEMORY RF EXECUTE	MFGCODE, USER MEMORY
	AUTHENTICATED SET PROTECTION RF SETUP	MFGCODE, MEMORY PAGE NUMBER, SECRET, PROTECTION SETTINGS
	AUTHENTICATED SET PROTECTION RF EXECUTE	MFGCODE, PROTECTION SETTINGS
	CONFIGURATION WRITE	MFGCODE, EEPROM CONFIGURATION BYTE
	CONFIGURATION READ	MFGCODE, EEPROM CONFIGURATION BYTE
	CONTROL WRITE	MFGCODE, SRAM CONTROL BYTE, PIO PORTS
	CONTROL READ	MFGCODE, SRAM CONTROL BYTE, PIO PORTS
	GET 1-WIRE ROM ID	MFGCODE, ROM ID
	PERIPHERAL TRANSACTION	MFGCODE, I²C PORT MASTER MODE
	WRITE AFI	AFI BYTE
	LOCK AFI	AFI LOCK STATUS
	WRITE DSFID	DSFID BYTE
	LOCK DSFID	DSFID LOCK STATUS

Figure 2. Commands Overview

Parasite Power

The MAX66242 can receive all energy necessary for its operation from the surrounding RF field, which needs to have a minimum strength as specified in the *Electrical Characteristics* table. If the field is strong enough, the device can harvest energy and provide a supply, e.g., to a microcontroller or other low power devices (see the *Typical Application Circuits*).

Unique Identification Number (UID)

Each MAX66242 contains a factory-programmed and locked identification number that is 64 bits long (Figure 3). The lower 28 bits are the serial number of the chip. The upper 36 bits are fixed at E02B00800h. The code in bit locations 49 to 56 identifies the chip manufacturer, according to ISO/IEC 7816-6/AM1. This code is 2Bh for Maxim. The UID is read accessible through the Inventory and Get System Information commands.

ROM ID

The read-only ROM ID is similar to the UID (Figure 4). The first 8 bits are a family code, which is E0h. The next 28 bits are a unique serial number. The next 20 bits are fixed at 2B000h. The last 8 bits are a cyclic redundancy check (CRC) of the first 56 bits. The CRC is generated using the polynomial $X^8 + X^5 + X^4 + 1$ (Figure 5). Additional information about this CRC is available in Application Note 27: *Understanding and Using Cyclic Redundancy Checks with Maxim iButton® Products*. The ROM ID is part of the input data to the SHA-256 engine. It is read accessible through the command Get 1-Wire ROM ID.

MSb					LSb
64 57	56 49	48 45	44 37	36 29	28 1
E0h	2Bh	0h	08h	00h	Serial Number

Figure 3. 64-Bit UID

MSb					LSb
8-bit CRC Code	2Bh	0h	00h	28-bit Serial Number	8-bit Family Code (E0h)
MSb LSb				MSb LSb	MSb LSb

Figure 4. 64-Bit ROM ID

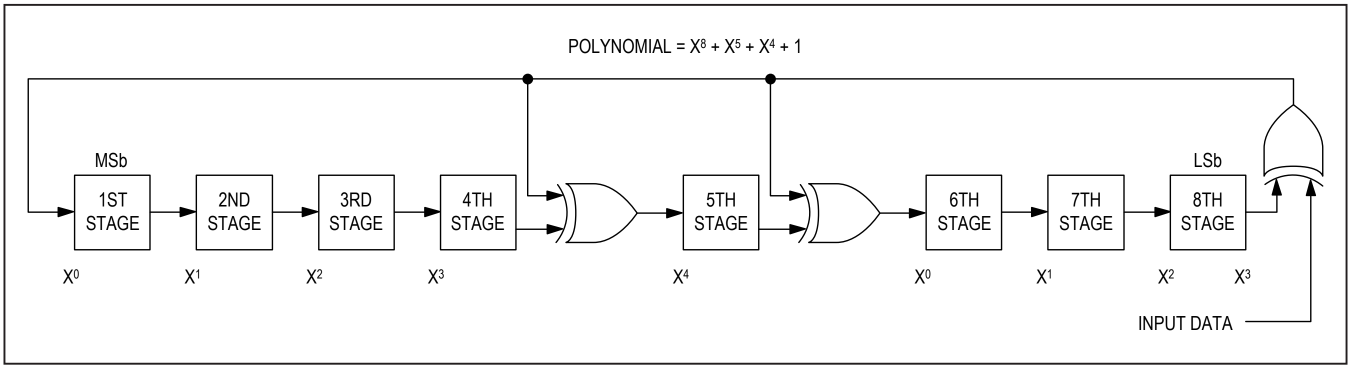


Figure 5. 8-Bit CRC for the ROM ID

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

Memory Resources

The memory of the MAX66242 consists of user EEPROM, secret memory, an SRAM scratchpad, personality registers, ROM ID, and two ISO 15693-specific bytes. Table 1 shows the size, access mode, and purpose of the various memory areas. Brackets around an access mode indicate possible restrictions, such as write protection or read protection.

The user memory is organized as 16 pages of 32 bytes each (Figure 6). A page is divided into 8 page blocks of 32 bits each. With the MAX66242, the page protection applies to individual memory pages. The user memory is written in page blocks. If not read protected, the memory can be read starting at any page block of any page. The protocol allows reading multiple page blocks and pages up to the end of the memory in a single read command flow.

The secret is either directly written (loaded) or computed. This write access always encompasses the entire 32-byte secret. To protect against transmission errors, the new secret (loading) or a partial secret (computing) is first written to the scratchpad from where it can be read for verification. As the name implies, the secret memory is not user readable. To protect a secret from changes, it must be write protected (locked).

Page protection control is activated through the Write Page Protection command. Besides write protection, read protection and EPROM emulation mode, the MAX66242 supports authentication protection. If authentication protection is activated, changes to the page protection settings as well as writing to the protected user memory require that the reader provide a valid MAC for the operation. Once a protection is activated, it cannot be reversed. The protection settings as well as the personality registers are read accessible through the Read Status command. See the *Memory and Control Function Commands* section for command flow details.

Depending on the command, the ROM ID may be required in the MAC computations. This makes the MAC generated by a MAX66242 or written to the MAX66242 (if authentication protection is activated) device-specific, even if the values of all other data elements are identical. Instead of requiring the reader to derive the ROM ID from the UID, the MAX66242 supports a special command to read the ROM ID directly.

Note that the ISO 15693 standard commands Read Single Block and Read Multiple Blocks do not address the user memory by page number and page block number. Instead, they use absolute block numbers counting from 0 to 127. Figure 7 shows how these absolute numbers map to the user memory.

Table 1. Memory Resources

NAME	SIZE (BYTES)	ACCESS MODE	PURPOSE
User Memory (EEPROM)	512	(Read), (Write), Internal Read	Application-specific data storage; also used for MAC computations.
Scratchpad (SRAM)	32	Read, Write, Internal Read	Intermediate data storage when installing a secret; also used to store the challenge for a MAC computation.
Personality Registers	4	Read, Internal Read	Lock status indicator for the secret and read access to the device's manufacturer ID (factory preprogrammed parts).
ROM ID	8	Read, Internal Read	Used for MAC computations.
Application Family Identifier (AFI)	1	Read, (Write), RF port only	Can be used during the inventory phase to narrow the number of transponders that participate in the discovery or anti-collision process.
Data Storage Format Identifier (DSFID)	1	Read, (Write), RF port only	User byte that can provide details on how the data in the user memory is structured.

	PG. BLOCK 7				PG. BLOCK 6				PG. BLOCK 5				PG. BLOCK 4				PG. BLOCK 3				PG. BLOCK 2				PG. BLOCK 1				PG. BLOCK 0			
	B3	B2	B1	B0	B3	B2	B1	B0	B3	B2	B1	B0	B3	B2	B1	B0	B3	B2	B1	B0	B3	B2	B1	B0	B3	B2	B1	B0	B3	B2	B1	B0
Page 0																																
Page 1																																
Page 2																																
Page 3																																
Page 4																																
Page 5																																
Page 6																																
Page 7																																
Page 8																																
Page 9																																
Page 10																																
Page 11																																
Page 12																																
Page 13																																
Page 14																																
Page 15																																

Figure 6. User Memory Map

	PG. BLOCK 7	PG. BLOCK 6	PG. BLOCK 5	PG. BLOCK 4	PG. BLOCK 3	PG. BLOCK 2	PG. BLOCK 1	PG. BLOCK 0
Page 0	Block 7	Block 6	Block 5	Block 4	Block 3	Block 2	Block 1	Block 0
Page 1	Block 15	Block 14	Block 13	Block 12	Block 11	Block 10	Block 9	Block 8
Page 2	Block 23	Block 22	Block 21	Block 20	Block 19	Block 18	Block 17	Block 16
Page 3	Block 31	Block 30	Block 29	Block 28	Block 27	Block 26	Block 25	Block 24
Page 4	Block 39	Block 38	Block 37	Block 36	Block 35	Block 34	Block 33	Block 32
Page 5	Block 47	Block 46	Block 45	Block 44	Block 43	Block 42	Block 41	Block 40
Page 6	Block 55	Block 54	Block 53	Block 52	Block 51	Block 50	Block 49	Block 48
Page 7	Block 63	Block 62	Block 61	Block 60	Block 59	Block 58	Block 57	Block 56
Page 8	Block 71	Block 70	Block 69	Block 68	Block 67	Block 66	Block 65	Block 64
Page 9	Block 79	Block 78	Block 77	Block 76	Block 75	Block 74	Block 73	Block 72
Page 10	Block 87	Block 86	Block 85	Block 84	Block 83	Block 82	Block 81	Block 80
Page 11	Block 95	Block 94	Block 93	Block 92	Block 91	Block 90	Block 89	Block 88
Page 12	Block 103	Block 102	Block 101	Block 100	Block 99	Block 98	Block 97	Block 96
Page 13	Block 111	Block 110	Block 109	Block 108	Block 107	Block 106	Block 105	Block 104
Page 14	Block 119	Block 118	Block 117	Block 116	Block 115	Block 114	Block 113	Block 112
Page 15	Block 127	Block 126	Block 125	Block 124	Block 123	Block 122	Block 121	Block 120

Figure 7. User Memory Access Using Absolute Block Numbers

Interface Switching and Timeout

The MAX66242 contains both an ISO/IEC 15693 interface and an I2C interface. Only one interface can be active at a time.

The I2C interface becomes active when a valid START condition is received. The I2C interface becomes inactive if SMBUS timeout occurs, or when a valid STOP condition is received that is not followed by tSHA or tPROG, or when all tSHA and tPROG complete for commands such as Install and Lock Secret, Authenticated Write Page Protection, Authenticated Write Memory, etc.

The ISO/IEC 15693 interface becomes active when a valid SOF is received. The ISO/IEC 15693 interface becomes inactive if an ISO/IEC 15693 timeout occurs, at the end of a response frame, at the end of a request frame if there is no response, or when the RF field is removed.

A delay of 1ms is required when switching between I2C and ISO/IEC 15693.

ISO/IEC 15693 Timeout

If the ISO/IEC 15693 interface becomes active and the reader stops communicating for a duration of $t_{ISO\_TIMEOUT}$, the device resets the ISO/IEC 15693 interface and resets any active command.

I2C (SMBus Style) Timeout

The I2C interface includes a timeout feature that is typically found with SMBus devices. The MAX66242 monitors the activity on the SCL line and, if SCL stays at logic 0 for the duration of $t_{I2C\_TIMEOUT}$, the device resets its I2C interface as if the master had generated a STOP condition, and resets any active command. I2C timeout monitoring is inactive during t_{SHA} or t_{PROG} intervals.

Power Switching

The MAX66242 can be powered by the V_{CC} pin, by the RF field, or by both. A delay of 1ms is required when switching or changing the power connection.

PIO and Energy Harvesting Output (V_{OUT})

The PIO pin and energy harvesting output (V_{OUT}) are controlled by the Control and Configuration registers (Table 2 and Table 3). The volatile Control register controls the current settings. The nonvolatile Configuration register contains defaults that are loaded into the Control register at power-up. These registers are controlled by the Control Write, Control Read, Configuration Write, and Configuration Read commands.

Table 2. Control Register Bitmap

BIT 7	BIT 6	BIT 5	BIT 4	BIT 3	BIT 2	BIT 1	BIT 0
PCFG[3:0]				RBS	X	X	EHOE

Note: Bits 2 and 1 are read only.

Table 3. Configuration Register Bitmap

BIT 7	BIT 6	BIT 5	BIT 4	BIT 3	BIT 2	BIT 1	BIT 0
PCFG[3:0]				RBS	X	X	EHOE

***Note:** The bits marked as X can be 0 or 1.*

Bits [7:4]: Pin Configuration (PCFG[3:0]). These bits specify the PIO mode.

PCFG[3:0]	PIO MODE
1XXX	PIO_CONTROL mode
000X	RF_BUSY mode
001X	RF_AIP mode

Note: The bits marked as X can be 0 or 1. Other PCFG settings must not be used.

Bit 3: Read Back Selection (RBS). This bit affects the outcome of the Control Read command. If PCFG[3] is 1 (PIO_CONTROL mode) and RBS is 1, PCFG[1] will read back the value written to the Control register. If PCFG[3] is 1 (PIO_CONTROL mode) and RBS is 0, PCFG[1] will read back the value of the PIO pin. If PCFG[3] is 0, RBS has no effect.

Bit 0: Energy Harvesting Output Enable (EHOE). This bit specifies whether the voltage at the energy harvesting pin VOUT is 1.8V or 3.3V. If EHOE is 1 and field strength is greater than Hminout, the output voltage is 3.3V nominally. If EHOE is 0, the output voltage is 1.8V nominally.

PIO_CONTROL Mode

In PIO_CONTROL mode, the PIO pin is set to high impedance if PCFG[1] is 1, and is pulled low if PCFG[1] is 0.

RF_BUSY Mode

In RF_BUSY mode, the PIO pin defaults to high impedance. When a request frame SOF is received, PIO is pulled low. If the command will result in no response, PIO is released after the request frame EOF is received. If the command will result in a response, PIO is held low until the response frame EOF is transmitted. See Figure 8.

RF_AIP mode

In RF_AIP mode, the PIO pin defaults to high impedance. When volatile or nonvolatile memory is being written by an ISO/IEC 15693 command, the PIO pin pulses low. Commands that write volatile memory (Read/Write Scratchpad, Control Write) will pulse low for t_{RFAIP}. See Figure 9. Commands that write nonvolatile memory (Write AFI, Lock AFI, Write DSFID, Lock DSFID, Set Protection, Authenticated Set Protection RF Setup, Authenticated Set Protection RF Execute, Write Memory, Authenticated Write Memory RF Setup, and Authenticated Write Memory RF Execute) will pulse low for t_{PROG}. See Figure 10. Load and Lock Secret and Compute and Lock Secret pulses low for t_{PROG} 8 times if the secret is not locked. It pulses low for t_{PROG} 9 times if the secret is locked.

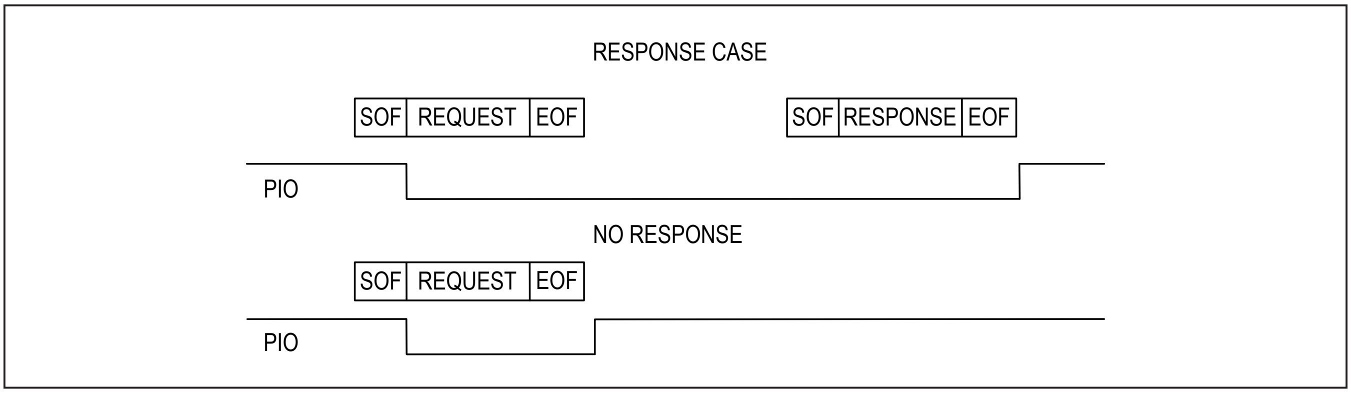


Figure 8. PIO Signaling in RF_BUSY Mode

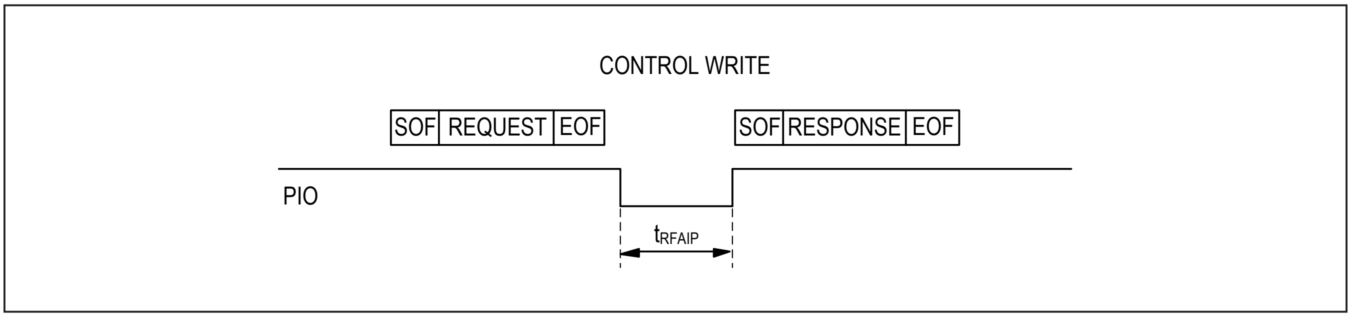


Figure 9. PIO Signaling in RF_AIP Mode, Cases Read/Write Scratchpad, Control Write

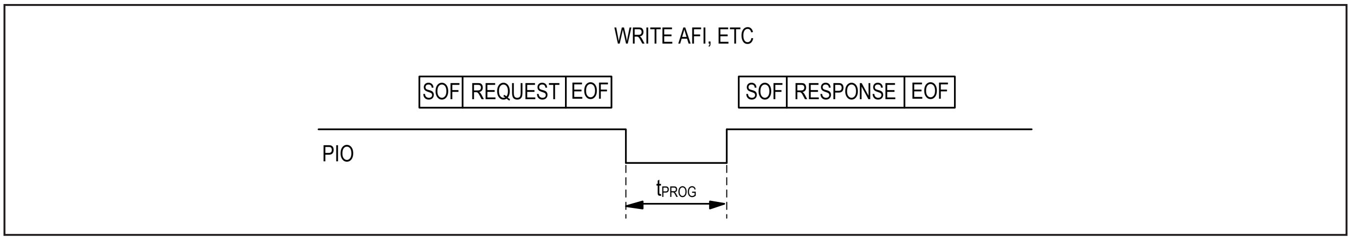


Figure 10. PIO Signaling in RF_AIP Mode, Writing to Nonvolatile Memory

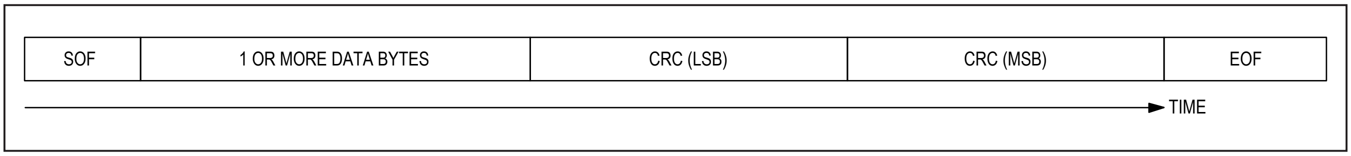


Figure 11. ISO/IEC 15693 Frame Format

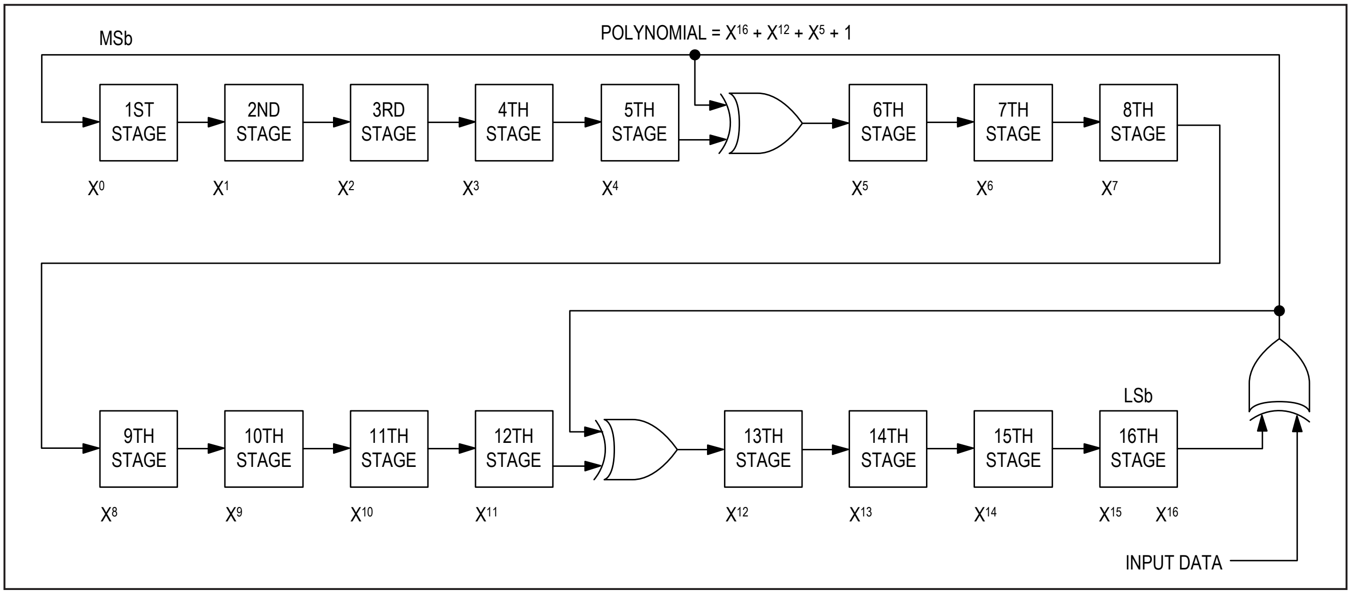


Figure 12. CRC-16-CCITT Generator

V_{OUT}

The V_{OUT} pin requires a 100Ω series isolation if the application requires switching from 3.3V to 1.8V. The RF field must be stronger than H_{MINOUT} for the 3.3V setting to be used. A wait time t_{VOUT} is required when changing the output voltage from 1.8V (nominal) to 3.3V (nominal). Communication with the device may be affected when a load is present.

ISO/IEC 15693 Interface

The communication between an RF reader and MAX66242 (transponder) is a master-transponder type transaction, and is based on the exchange of data packets. The reader initiates every transaction; only one side (reader or transponder) transmits information at any time. Each data packet begins with a start-of-frame (SOF) pattern and ends with an end-of-frame (EOF) pattern. A data packet delimited by an SOF and an EOF is called a frame (Figure 14). The last 2 bytes of an ISO 15693 frame are an inverted 16-bit CRC of the preceding data generated according to the CRC-16-CCITT polynomial X16 + X12 + X5 + 1 (Figure 15). This CRC is transmitted with the LSB first. For more details on the CRC-16-CCITT, refer to ISO 15693-3, Annex C. Frame information is modulated on a 13.56MHz carrier. The subsequent paragraphs are a concise description of the required modulation, coding, and basic timing.

Reader to Transponder Communication

The communication from reader to transponder uses amplitude modulation (Figure 13); the modulation index can be either in the range of 10% to 30% or 100% (ISO 15693-2, Section 7.1). The standard defines two pulse-position data coding modes. The “1 out of 256” data coding mode transmits one byte in 4.833ms, equivalent to a data rate of 1655bps (Figure 14). The location of a modulation pause during the 4.833ms conveys the value of the byte. The “1 out of 4” data coding mode transmits 2 bits in 75.52µs, equivalent to a data rate of 26,484bps (Figure 15). The location of a modulation pause during the 75.52µs conveys the value of the 2 bits. A byte is transmitted as a concatenation of four 2-bit transmissions, with the least significant 2 bits of the byte being transmitted first. The transmission of the SOF pattern also takes 75.52µs. The SOF pattern has two modulation pauses. The position of the second pause determines whether the frame uses the “1 out of 256” or “1 out of 4” data coding mode (Figure 16 and Figure 17, respectively). The transmission of the EOF pattern takes 37.76µs; the EOF is the same for both coding modes and has one modulation pause (Figure 18). For full details, refer to ISO 15693-2, Sections 7 and 8.

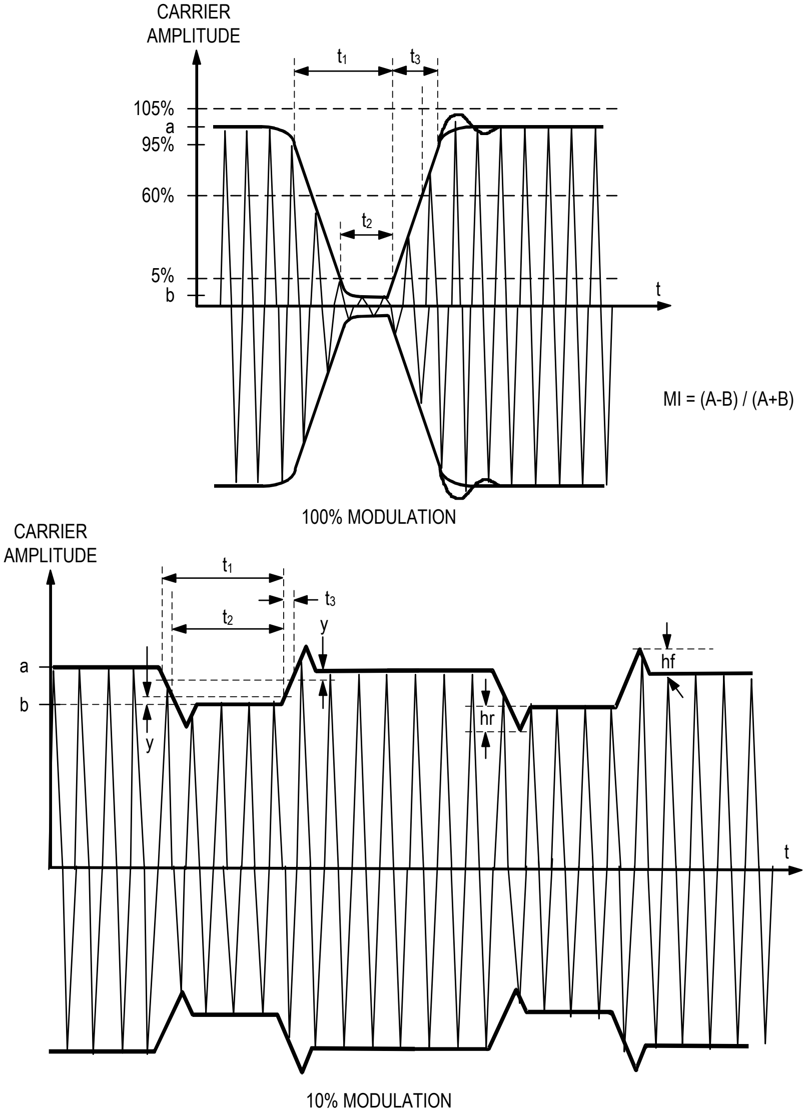


Figure 13. Reader to Transponder Modulation

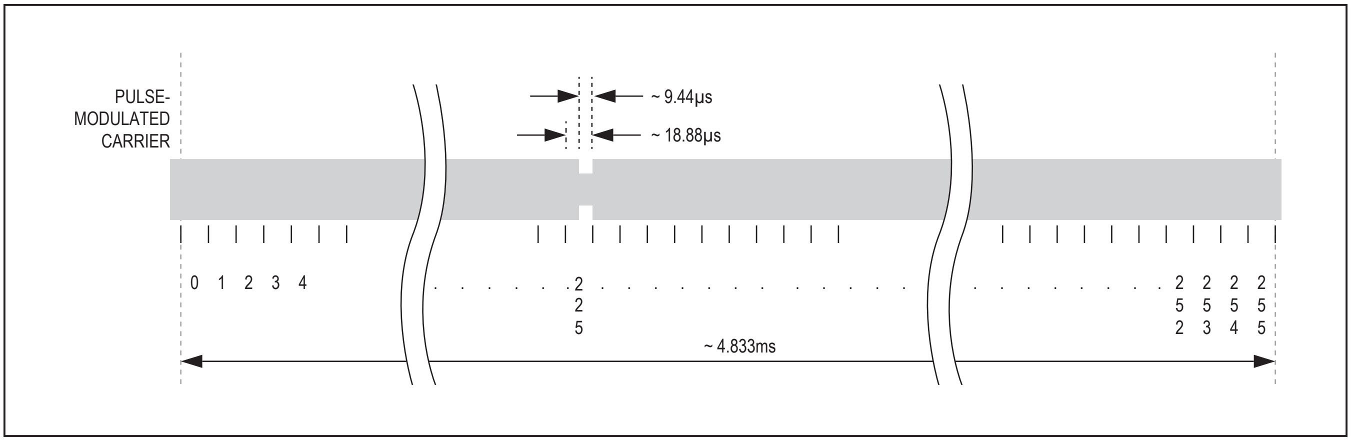


Figure 14. Reader to Transponder "1 Out of 256" Data Coding

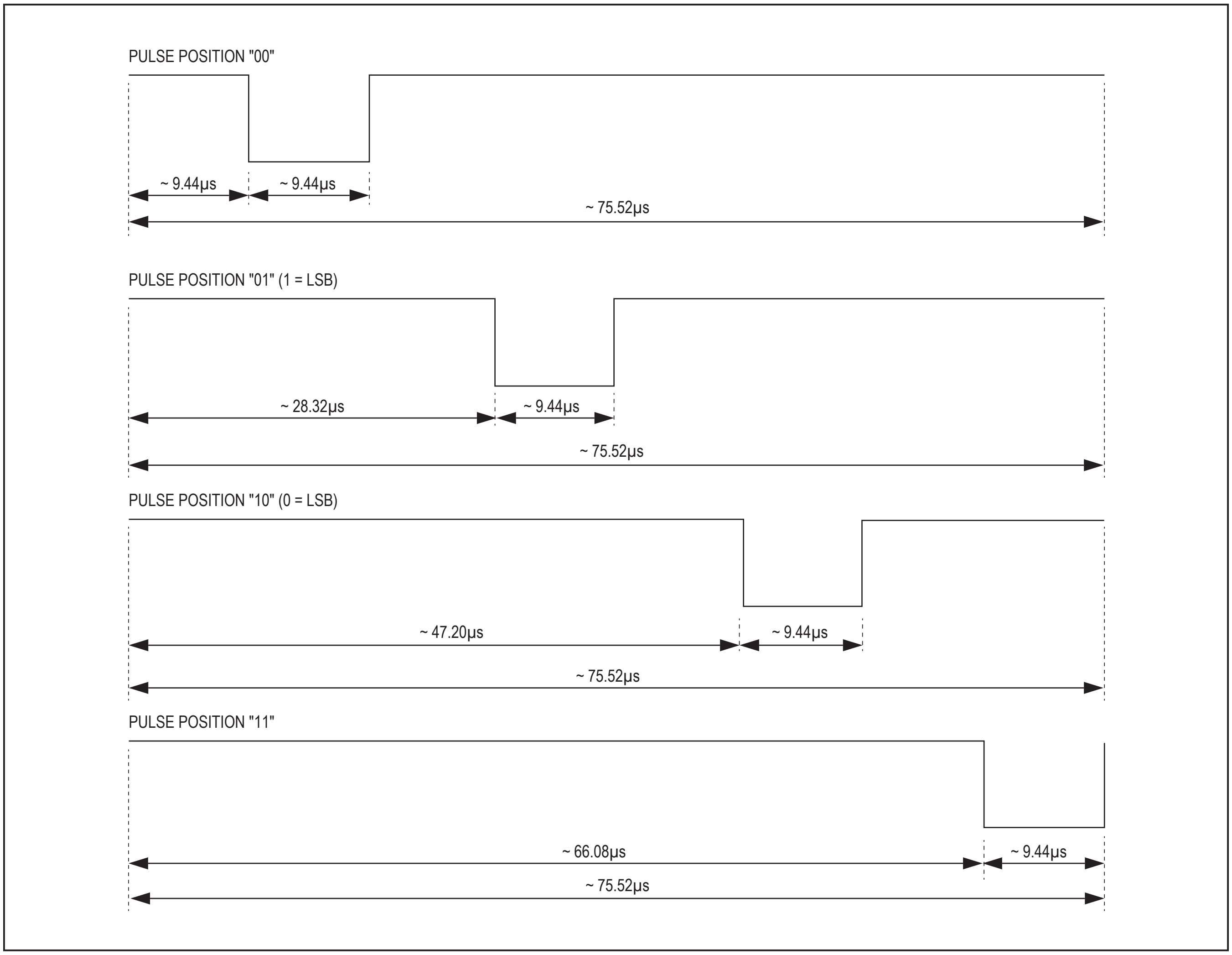


Figure 15. Reader to Transponder "1 Out of 4" Data Coding (Carrier Not Shown)

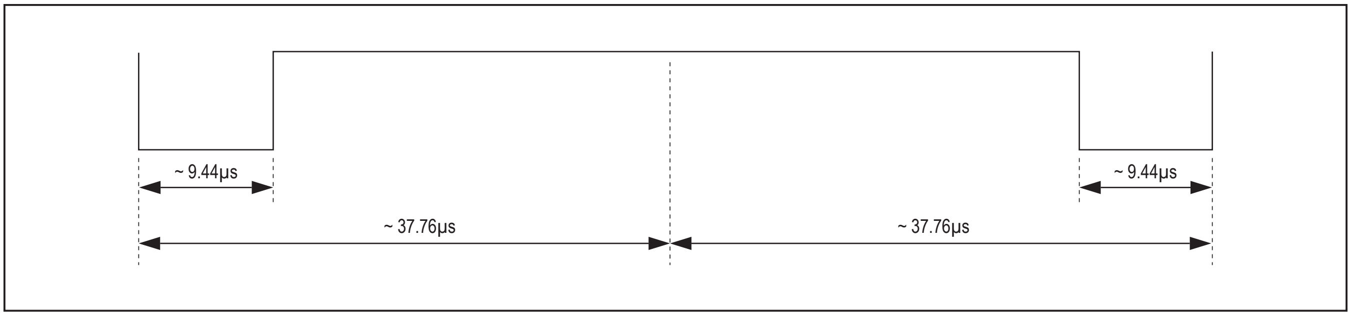


Figure 16. Reader to Transponder SOF for "1 Out of 256" Data Coding (Carrier Not Shown)

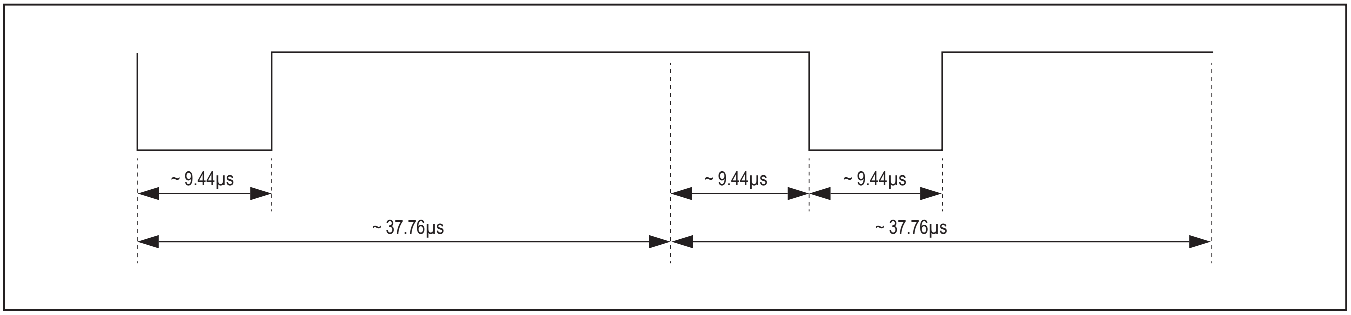


Figure 17. Reader to Transponder SOF for "1 Out of 4" Data Coding (Carrier Not Shown)

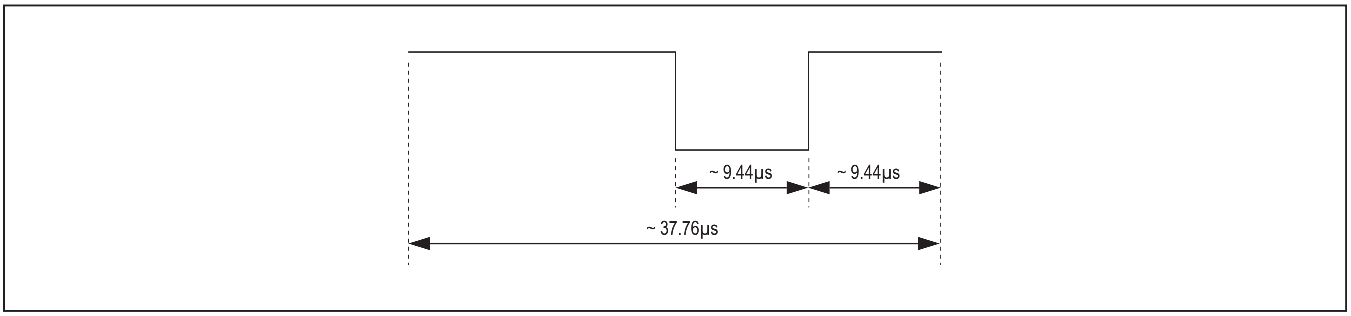


Figure 18. Reader to Transponder EOF (Identical for Both Coding Modes, Carrier Not Shown)

Transponder to Reader Communication

The Subcarrier_flag bit in the request data frame specifies the use of one or two subcarrier in the response frame. For the one subcarrier case, the subcarrier frequency is 423.75kHz. For the two subcarrier case, the subcarrier frequencies are 423.75kHz and 484.28kHz. The Data_rate_flag bit in the request data frame specifies the response frame data rate. Low data rate is approximately 6600bps, and high data rate is approximately 26,500bps. The data rate varies slightly depending on the use of one or two subcarriers. The LSb is transmitted first.

In the single subcarrier high data rate case, one bit is transmitted in 37.76µs. For a logic 0, the transponder modulates for 16 cycles then does not modulate for 16 cycles, which is repeated 8 times. This is followed by 256 cycles of no modulation. For a logic 1, the transponder does not modulate for 256 cycles. It then modulates for 16 cycles then does not modulate for 16 cycles, which is repeated 8 times. An SOF or EOF is transmitted in approximately 151µs. For an SOF, the transponder does not modulate for 768 cycles. It then modulates for 16 cycles then does not modulate for 16 cycles, which is repeated 24 times. This is followed by a logic 1. For an EOF, the transponder sends a logic 0. It then modulates for 16 cycles then does not modulate for 16 cycles, which is repeated 24 times. This is followed by no modulation for 768 cycles. See Figure 19 and Figure 21 for more details. For low data rate, multiply all cycle counts and times by 4.

In the two subcarrier low data rate case, one bit is transmitted in 37.46µs. For a logic 0, the transponder modulates for 16 cycles then does not modulate for 16 cycles, which is repeated 8 times. Next, the transponder modulates for 14 cycles then does not modulate for 14 cycles, which is repeated 9 times. For a logic 1, the transponder modulates for 14 cycles then does not modulate for 14 cycles, which is repeated 9 times. Next, the transponder modulates for 16 cycles then does not modulate for 16 cycles, which is repeated 8 times. An SOF or EOF is transmitted in approximately 149.8µs. For an SOF, the transponder modulates for 14 cycles then does not modulate for 14 cycles, which is repeated 27 times. Next, the transponder modulates for 16 cycles then does not modulate for 16 cycles, which is repeated 24 times. This is followed by a logic 1. For an EOF, the transponder sends a logic 0. It then modulates for 16 cycles then does not modulate for 16 cycles, which is repeated 24 times. Next, the transponder modulates for 14 cycles then does not modulate for 14 cycles, which is repeated 27 times. See Figure 20 and Figure 22 for more details. For low data rate, multiply all cycle counts and times by 4.

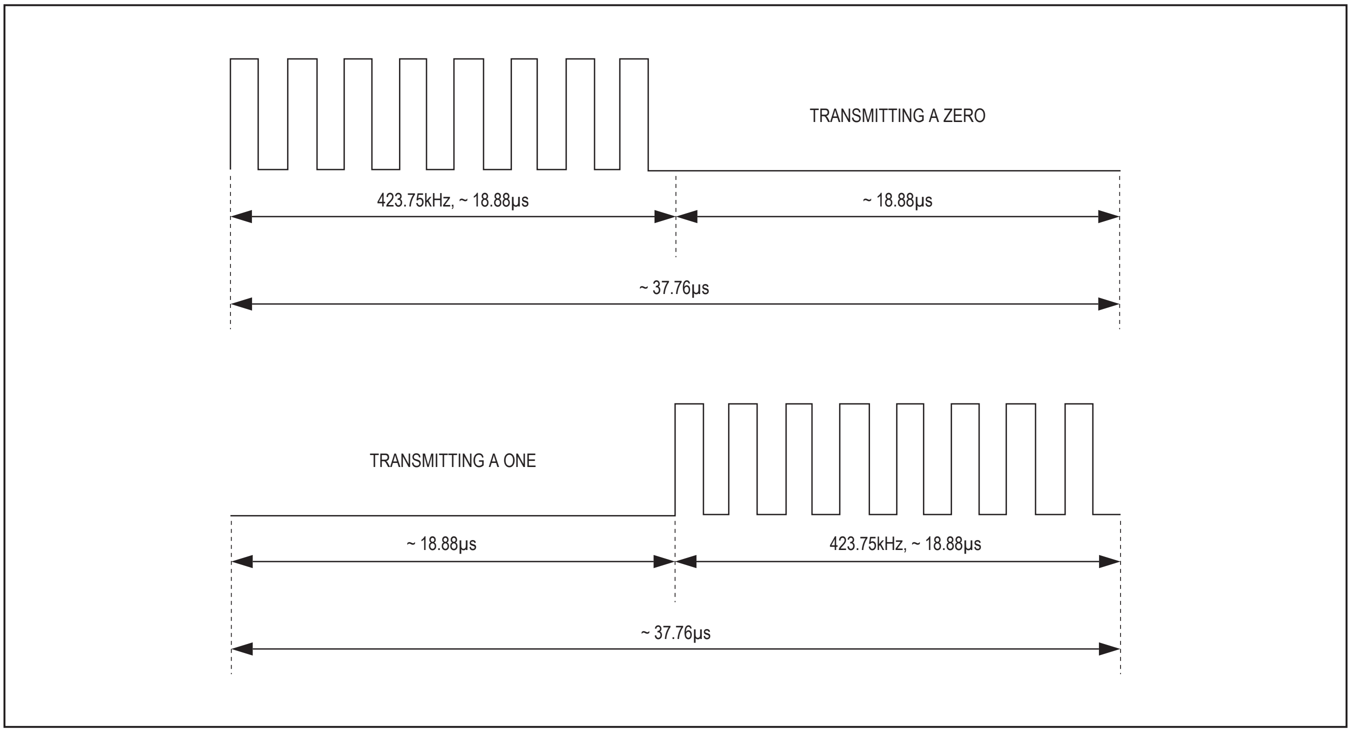


Figure 19. Uplink Coding, Single Subcarrier Bit Coding (High Data-Rate Timing)

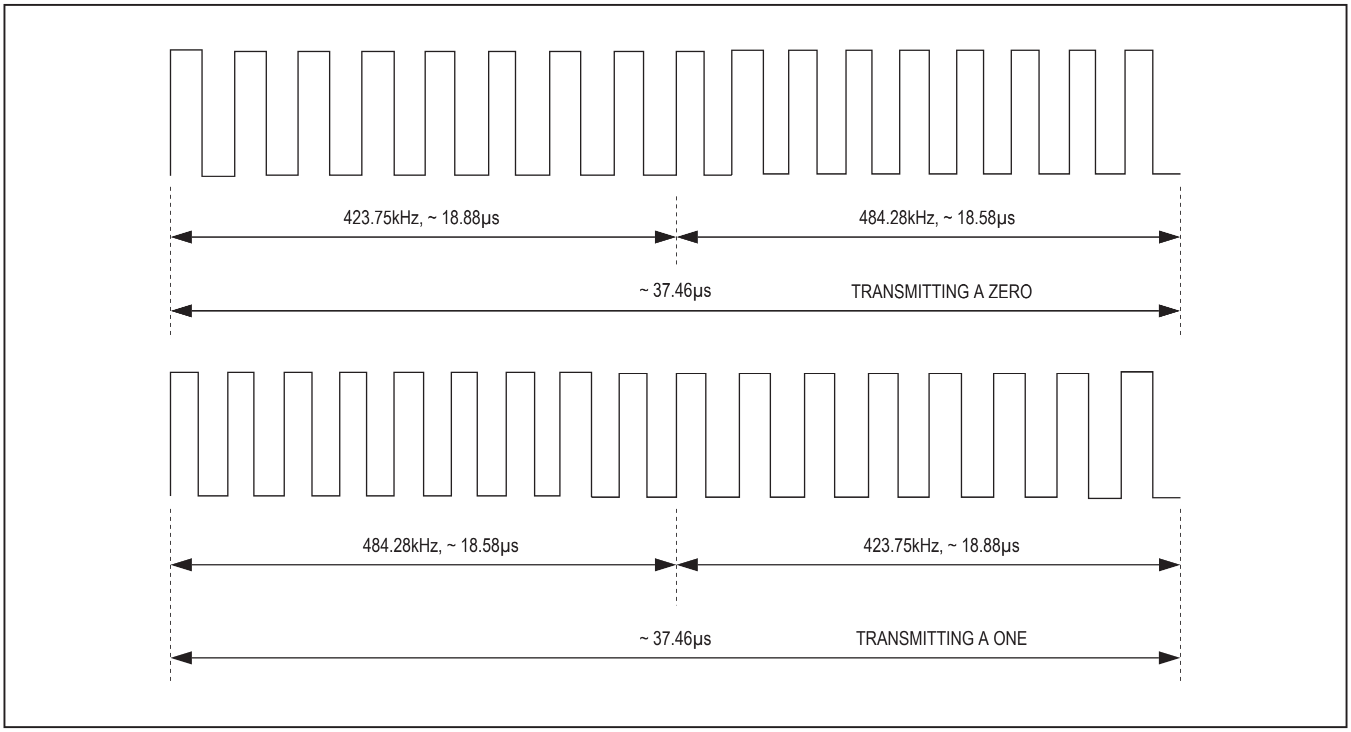


Figure 20. Uplink Coding, Two Subcarriers Bit Coding (High Data-Rate Timing)

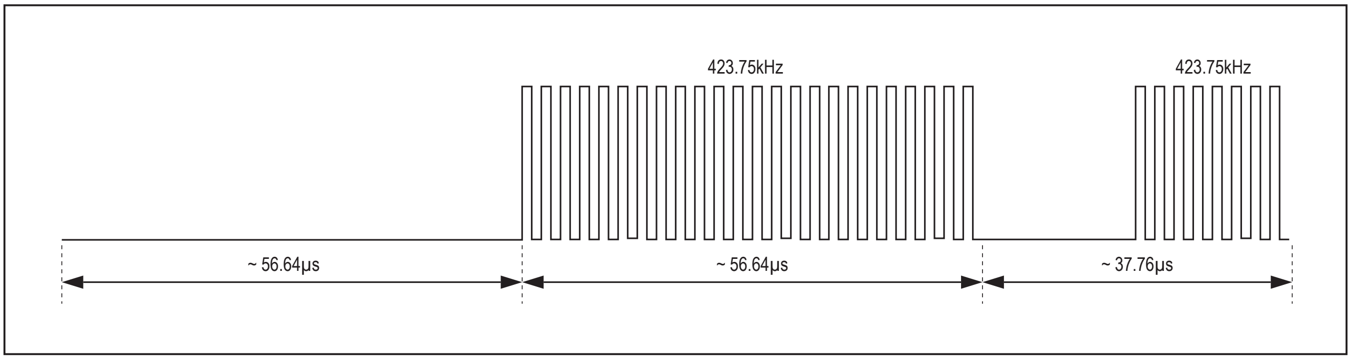


Figure 21. Transponder to Reader SOF, One Subcarrier (High Data Rate)

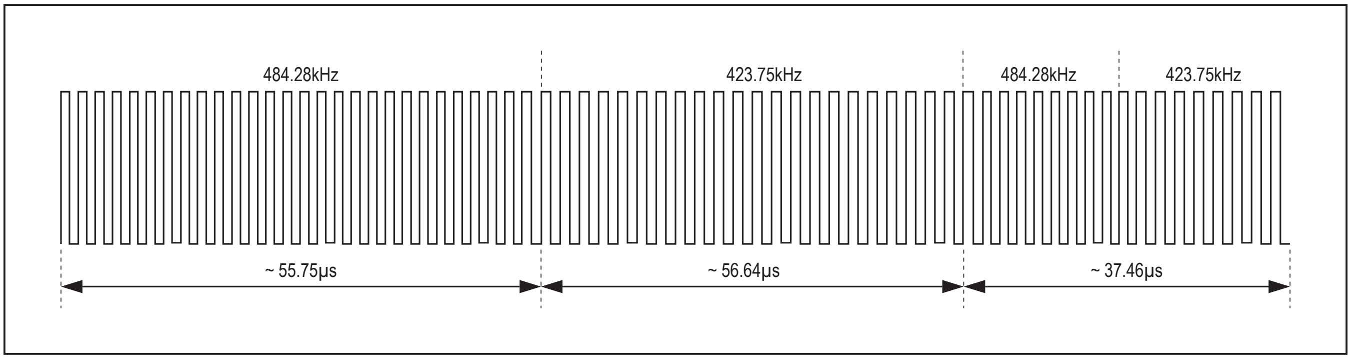


Figure 22. Transponder to Reader SOF, Two Subcarriers (High Data Rate)

ISO 15693 Transponder States and State Transitions

ISO 15693 defines four transponder states and three address modes. The states are power-off, ready, quiet, and selected. The address modes are nonaddressed, addressed, and select. The addressed mode requires that the reader include the transponder's UID in the request. Figure 23 shows how the Reset to Ready, Stay Quiet, and Select commands respond when changing the transponder's state. Table 4 shows how other commands respond depending on address mode and the transponder's state. Note that Stay Quiet never generates a response. For full details, refer to ISO 15693-2, Section 7.

Power-Off State

This state applies if the transponder is outside the reader's RF field. A transponder transitions to the power-off state when leaving the power-delivering RF field. When entering the RF field, the transponder automatically transitions to the ready state.

Ready State

In this state, a transponder has enough power to perform any of its functions. The purpose of the ready state is to have the transponder population ready to process the inventory command as well as other commands sent in the addressed or nonaddressed mode. A transponder can exit the ready state and transition to the quiet or the selected state upon receiving the Stay Quiet or Select command sent in addressed mode.

Quiet State

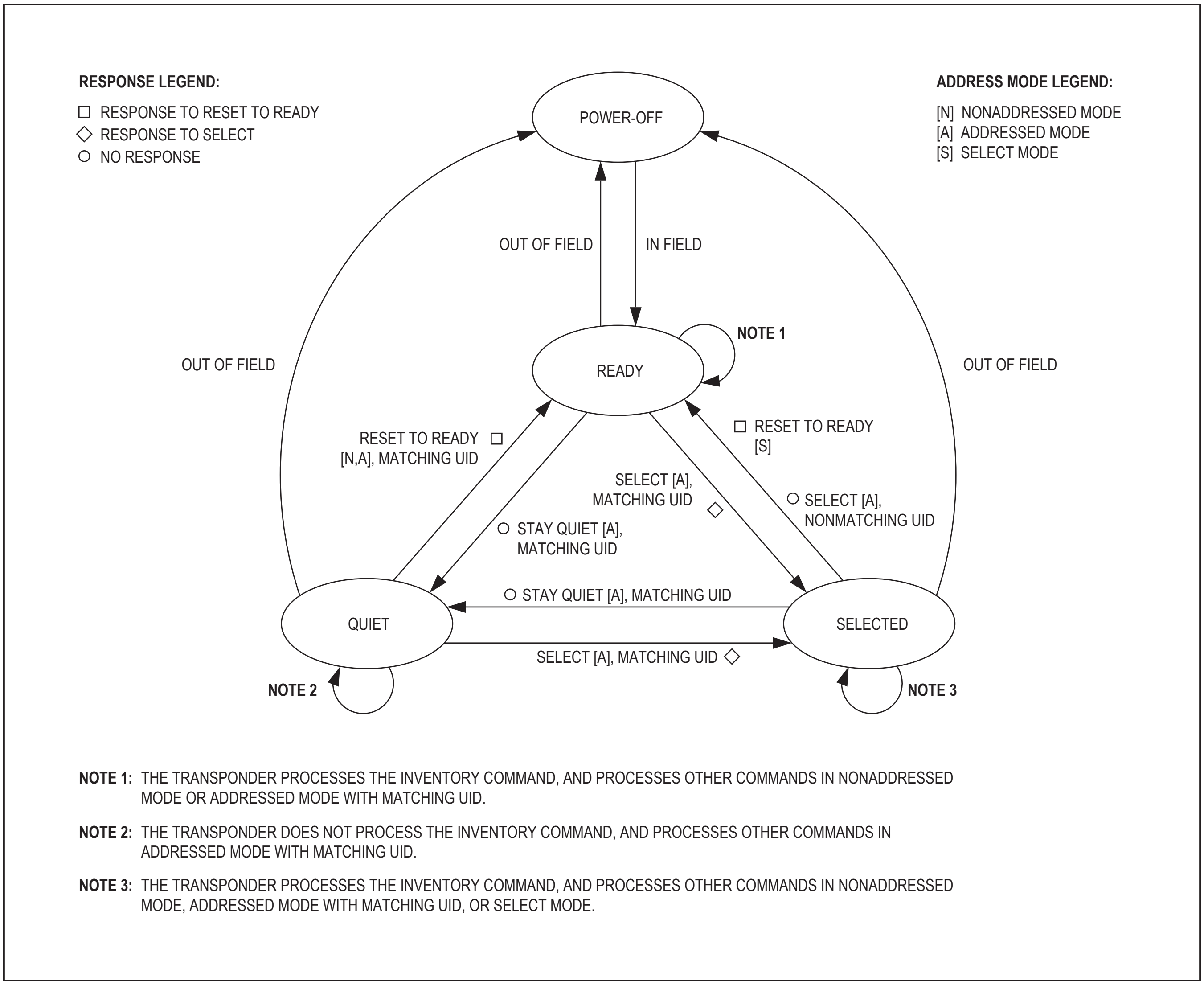
In this state, a transponder has enough power to perform any of its functions. The purpose of the quiet state is to silence transponders with which the reader does not want to communicate. Only commands sent with the addressed mode are processed. This way the reader can use the nonaddressed mode for communication with remaining transponders in the ready state. A transponder can exit the quiet state and transition to the ready state upon receiving the Reset to Ready command in addressed or nonaddressed mode. It can also transition to the selected state upon receiving Select commands sent in addressed mode.

Selected State

In this state, a transponder has enough power to perform any of its functions. The purpose of the selected state is to isolate the transponder with which the reader wants to communicate. Commands are processed regardless of the address mode in which they are sent, including the Inventory command. With multiple transponders in the RF field, the reader can put one transponder in the selected state, leaving all others in the ready state. For a transponder in the selected state, the reader can use the selected mode, which keeps the request data packets as short as with the nonaddressed mode. A new transponder entering the RF field will not disturb communication since it powers up in the ready state. A transponder can exit the selected state and transition to the ready state upon receiving the Reset to Ready command sent in nonaddressed or addressed mode. It can also transition to the quiet state upon receiving the Stay Quiet command sent in the addressed mode. A transponder also transitions from selected to ready upon receiving a Select command if the UID in the request is different from the transponder's own UID. In this case, the reader's intention is to transition another transponder with the matching UID to the selected state. If the transponder already in the selected state does not recognize the command, e.g., due to a bit error, two transponders could be in the selected state. To prevent this from happening, the reader should use the Reset to Ready or the Stay Quiet command to transition a transponder out of the selected state.

Table 4. Command Response vs. Transponder State and Address Mode Combinations

TRANSPONDER STATES	ADDRESS MODES		
	NONADDRESSED MODE (ADDRESS_FLAG = 0; SELECT_FLAG = 0)	ADDRESSED MODE (ADDRESS_FLAG = 1; SELECT_FLAG = 0)	SELECT MODE (ADDRESS_FLAG = 0; SELECT_FLAG = 1)
Power-Off	(Inactive)	(Inactive)	(Inactive)
Ready	Respond	Respond	Do not respond
Quiet	Do not respond	Respond	Do not respond
Selected	Respond	Respond	Respond



NOTE 1: THE TRANSPONDER PROCESSES THE INVENTORY COMMAND, AND PROCESSES OTHER COMMANDS IN NONADDRESSED MODE OR ADDRESSED MODE WITH MATCHING UID.

NOTE 2: THE TRANSPONDER DOES NOT PROCESS THE INVENTORY COMMAND, AND PROCESSES OTHER COMMANDS IN ADDRESSED MODE WITH MATCHING UID.

NOTE 3: THE TRANSPONDER PROCESSES THE INVENTORY COMMAND, AND PROCESSES OTHER COMMANDS IN NONADDRESSED MODE, ADDRESSED MODE WITH MATCHING UID, OR SELECT MODE.

Figure 23. ISO 15693 State Transition Diagram

Request Flags

The first byte in a request is called the request flags. There are two formats for the request flags. The state of the Inventory_flag bit controls the function of the bits in the upper half of the request flags. Table 5 and Table 6 explain the function of the request flags.

Table 5. Request Flags, Inventory_flag Bit Not Set

BIT 7	BIT 6	BIT 5	BIT 4	BIT 3	BIT 2	BIT 1	BIT 0
0	Option_flag	Address_flag	Select_flag	0	Inventory_flag (= 0)	Data_rate_flag	Subcarrier_flag

***Note:** Bits 7 and 3 have no function. They must be sent as 0 for the request flags to be valid.*

Bit 6: Option Flag (Option_flag). Some ISO 15693 commands use this bit to enable alternate functions. The MAX66242 does not support the Option_flag, so it must be 0.

Bit 5: Address Flag (Address_flag). If the Address_flag bit is 0, the request must not include a UID. If the Address_flag bit is 1, the request must include a UID. The request flags are not valid if both the Select_flag and Address_flag are 1.

Bit 4: Select Flag (Select_flag). If the Select_flag bit is 1, the request is processed only by the transponder in the selected state. The request flags are not valid if both the Select_flag and Address_flag are 1.

Bit 2: Inventory Flag (Inventory_flag). This bit must be 1 for the Inventory command only. For all other commands, this bit must be 0.

Bit 1: Data Rate Flag (Data_rate_flag). This bit specifies whether the response data packet is transmitted using the low data rate (bit is 0) or the high data rate (bit is 1).

Bit 0: Subcarrier Flag (Subcarrier_flag). This bit specifies whether the response data packet is transmitted using one subcarrier (bit is 0) or two subcarriers (bit is 1).

Table 6. Request Flags, Inventory_flag Bit Set

BIT 7	BIT 6	BIT 5	BIT 4	BIT 3	BIT 2	BIT 1	BIT 0
0	0	Nb_slots_flag	AFI_flag	0	Inventory_flag (= 1)	Data_rate_flag	Subcarrier_flag

***Note:** Bits 7, 6, and 3 have no function. They must be sent as 0 for the request flags to be valid.*

Bit 5: Slot Counter Flag (Nb_slots_flag). This bit specifies whether the Inventory command is executed using a slot counter (bit is 0) or without using the slot counter (bit is 1).

Bit 4: Application Family Identifier Flag (AFI_flag). This bit specifies whether the Inventory command request frame does not include an AFI byte (bit is 0) or does include an AFI byte (bit is 1).

Bit 2: Inventory Flag (Inventory_flag). This bit must be 1 for the Inventory command only. For all other commands, this bit must be 0.

Bit 1: Data Rate Flag (Data_rate_flag). This bit specifies whether the response data packet is transmitted using the low data rate (bit is 0) or the high data rate (bit is 1).

Bit 0: Subcarrier Flag (Subcarrier_flag). This bit specifies whether the response data packet is transmitted using one subcarrier (bit is 0) or two subcarriers (bit is 1).

Wait Times

ISO 15693 defines several standard wait times. For full details, refer to ISO 15693-2, Section 9.

The wait time from request frame EOF to response frame SOF is t_1. t_1 min is 318.6µs (4320 cycles), t_1 nom is 320.9µs (4352 cycles), and t_1 max is 323.3µs (4384 cycles). Commands that perform MAC calculations or write memory will extend t_1 by a command specific combination of t_{RFAIP}, t_{CSHA}, and t_{PROG}. If a 100% modulation pulse is detected during t_1, the transponder must restart its t_1 counter.

The 10% modulation ignore time after a request frame EOF is received is t_{MIT}. t_{MIT} min is 323.3µs (4384 cycles) + t_{NRT}, where t_{NRT} is the nominal response frame length.

The wait time between a response frame and a subsequent request frame is t_2. t_2 min is 309.2µs (4192 cycles).

The wait time between slot EOFs in an Inventory command where Nb_slots_flag is t_3. For 100% modulation, t_{3MIN} is 323.3µs (4384 cycles) + t_{SOF}, where t_{SOF} is the time requires to transmit a request frame SOF. For 10% modulation, t_3 min is 323.3µs (4384 cycles) + t_{NRT} + t_{2MIN}, where t_{NRT} is the nominal response frame length.

Network Function Commands

The ISO 15693 standard defines four network function commands: Inventory, Stay Quiet, Select, and Reset to Ready. Their purpose is to identify the UIDs of all transponders in the field (to Inventory) and to manage access to these transponders. Figure 23 shows how the network function commands are used to transition a transponder from one state to another.

Network Function Command Errors

Various error conditions can occur. If an error occurs, and the request is sent in addressed mode with matching UID or in select mode with the transponder in the selected state, the transponder will transmit an error response. In any other mode/state combination, an error will result in no response. In case of an error response, the response begins with response flags of 01h, followed by a single-byte error code. Table 7 shows a matrix of commands, errors, and error codes.

Table 7. Network Function Command Error Code Matrix

ERROR EXPLANATION	Invalid Request Packet	Option Flag Set
ERROR CODE	02h	03h
FAILING COMMAND		
Reset to Ready	✓	✓
Select	✓	✓

Detailed Command Descriptions

Inventory

This command allows the reader to learn the UIDs and DSFIDs of all transponders in its RF field in an iterative process.

The AFI_flag determines if the AFI byte must be included in the request frame. The AFI byte is compared to the transponders AFI. The parameter byte determines the length of the mask. The LSb of the mask aligns with the LSb of the transponder's UID. The mask is compared to the transponder's UID. The Nb_slots_flag determines if a slot counter is concantenated with the mask for comparison to the transponder's UID. The slot counter starts at 0000b after the Inventory request frame is transmitted, and increments during the course of the Inventory command with every subsequent EOF sent by the reader. The AFI byte (if used) must match the transponder's AFI or be 00h, and the mask concatenated with the slot counter (if used) must match the transponder's UID for a response to be generated. This allows the reader to select transponders to respond to the Inventory command. The processing of an Inventory command ends if the transponder receives an SOF of a new request frame.

If a transponder meets all conditions to respond, it transmits a response frame. If multiple transponders meet the conditions, the response frames collide and may not be readable. The reader must eliminate the collision.

To identify all transponders in the RF field, the reader could begin with a mask length of 0 and activate the slot counter (Nb_slots_flag = 0). By using this method and going through all 16 slots, the reader has a chance to receive clean responses (i.e., the transponder is identified) as well as colliding responses. To prevent a transponder that has been identified from further participating in the collision management sequence, the reader transitions it to the quiet state. Next, the reader issues another Inventory command where the slot number that previously generated a collision is now used as a 4-bit mask, and runs again through all 16 slots. If a collision is found, another Inventory command is issued, this time with a mask that is extended at the higher bits by the slot counter value that produced the collision. This process is repeated until all transponders are identified. For a full description of the Inventory command processing by the transponder and the timing specifications, refer to ISO 15693 Part 3, Sections 8 to 9.

INVENTORY	
Command Code	01h
Parameter Byte	Mask Length (Table 8)
Conditions, Restrictions	The command is ignored unless the transponder is in the Ready or Selected state.
Protocol Variations	• Nb_slot_flag = 0, AFI_flag = 0, mask length = 0 • Nb_slot_flag = 0, AFI_flag = 0, mask length ≠ 0 • Nb_slot_flag = 0, AFI_flag = 1, mask length = 0 • Nb_slot_flag = 0, AFI_flag = 1, mask length ≠ 0 • Nb_slot_flag = 1, AFI_flag = 0, mask length = 0 • Nb_slot_flag = 1, AFI_flag = 0, mask length ≠ 0 • Nb_slot_flag = 1, AFI_flag = 1, mask length = 0 • Nb_slot_flag = 1, AFI_flag = 1, mask length ≠ 0
Other Notes	For the setting of the request flags (RQF), see Table 6. The mask pattern is transmitted only if the mask length is ≠ 0. The AFI is transmitted only if the AFI_flag bit in the request flags is set to 1.
Error Conditions (Error Response)	An error will result in no response.
t1 (Request Frame to Response Frame Delay)	318.6µs to 323.3µs

Table 8. Parameter Byte Bitmap

BIT 7	BIT 6	BIT 5	BIT 4	BIT 3	BIT 2	BIT 1	BIT 0
MLEN							

Bits [7:0]: Mask Length (MLEN). These bits specify the length of the mask. The mask (MASK) is transmitted only if MLEN is ≠ 0. The maximum mask length is 60 (3Ch, if Nb_slots_flag = 0) or 64 (40h, if Nb_slots_flag = 1).

Stay Quiet

This command addresses an individual transponder and transitions it to the Quiet state. The transponder does not send a response.

STAY QUIET	
Command Code	02h
Parameter Byte	N/A
Conditions, Restrictions	To transition to the Quiet state, the request must be sent in addressed mode with matching UID.
Protocol Variations	None
Other Notes	For the setting of the request flags (RQF), see Table 5.
Error Conditions (Error Response)	An error will result in no response.
t1 (Request Frame to Response Frame Delay)	None

Select

This command addresses an individual transponder and transitions it to the Selected state. The transponder transitioning to the Selected state sends a response. If there was a transponder with a different UID in the Selected state, then that transponder transitions to the Ready state without sending a response.

SELECT	
Command Code	25h
Parameter Byte	N/A
Conditions, Restrictions	To transition to the Selected state, the request must be sent in addressed mode with matching UID.
Protocol Variations	None
Other Notes	For the setting of the request flags (RQF), see Table 5.
Error Conditions (Error Response)	• Request data format error (response error code = 02h) • The Option_flag is set (response error code = 03h)
t1 (Request Frame to Response Frame Delay)	318.6µs to 323.3µs

Reset to Ready

This command addresses an individual transponder and transitions it to the Ready state. The transponder transitioning to the Ready state sends a response.

RESET TO READY	
Command Code	26h
Parameter Byte	N/A
Conditions, Restrictions	To transition from the Quiet state to the Ready state, the request must be sent in nonaddressed mode or in addressed mode with matching UID. To transition from the Selected state to the Ready state, the request must be sent in select mode.
Protocol Variations	• If the transponder is in the Selected state, and the request is sent in addressed mode with non-matching UID, the transponder transitions to the Ready state, but will not respond.
Other Notes	For the setting of the request flags (RQF), see Table 5.
Error Conditions (Error Response)	• Request data format error (response error code = 02h) • The Option_flag is set (response error code = 03h)
t1 (Request Frame to Response Frame Delay)	318.6µs to 323.3µs

Communication Examples—Network Function Commands

See Table 9 and Table 10 for the RF communication legend and data direction codes.

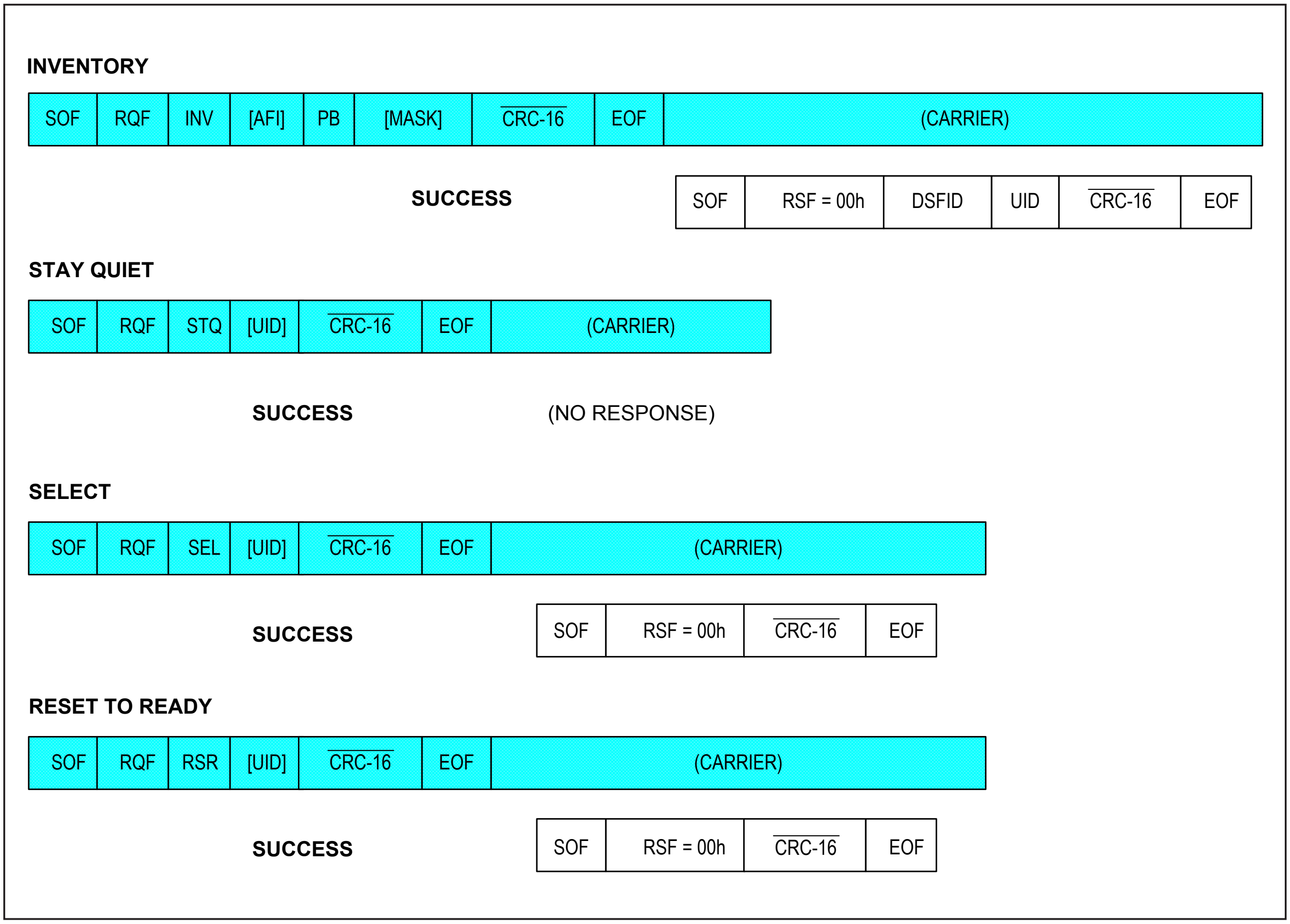
Table 9. RF Communication—Legend for Network Functions

NAME	DESCRIPTION
INV	Command “Inventory”, 01h
STQ	Command “Stay Quiet”, 02h
SEL	Command “Select”, 25h
RSR	Command “Reset to Ready”, 26h
SOF	Start of Frame
RQF	Request Flags Byte
[UID]	Transponder’s Unique 8-Byte Identification Number. The brackets [ ] indicate that the transmission of the UID depends on the request flags (RQF).
$\overline{\text{CRC-16}}$	Transmission of an inverted CRC-16 (2 bytes) generated according to CRC-16-CCITT
EOF	End of Frame
AFI	Application Family Identifier Byte
PB	Parameter Byte (command specific function and bit assignment)
[MASK]	Inventory Mask Field. The brackets [ ] indicate that the transmission of MASK depends on the parameter byte (PB).
RSF	Response Flags Byte

Table 10. Data Direction Color Codes

READER-TO-TRANSPONDER	TRANSPONDER-TO-READER

RF Communication Examples—Network Functions


INVENTORY
SOF | RQF | INV | [AFI] | PB | [MASK] | CRC-16 | EOF | (CARRIER)
SUCCESS
SOF | RSF = 00h | DSFID | UID | CRC-16 | EOF
STAY QUIET
SOF | RQF | STQ | [UID] | CRC-16 | EOF | (CARRIER)
SUCCESS
(NO RESPONSE)
SELECT
SOF | RQF | SEL | [UID] | CRC-16 | EOF | (CARRIER)
SUCCESS
SOF | RSF = 00h | CRC-16 | EOF
RESET TO READY
SOF | RQF | RSR | [UID] | CRC-16 | EOF | (CARRIER)
SUCCESS
SOF | RSF = 00h | CRC-16 | EOF

Memory and Control Function Commands

The MAX66242 supports 25 memory and control function commands. These commands fall into two groups: ISO 15693 standard commands (seven commands) and ISO 15693-compliant custom commands (18 commands). The standard commands provide access to the system information, manage the AFI and DSFID, and provide elementary memory read access (single block, multiple blocks). The custom commands allow read/write access to unprotected information (memory, protection settings, configuration, control), manage the secret's installation, and perform read/write access to authentication protected information (memory, protection settings). The reader can operate the MAX66242's I²C port in master mode, allowing I²C read/write functionality to an I²C slave through the RF interface.

Various error conditions can occur. If an error occurs, and the request is sent in addressed mode with matching UID or in select mode with the transponder in the Selected state, the transponder will transmit an error response. In any other mode/state combination, an error will result in no response. In case of an error response, the response begins with response flags of 01h, followed by a single-byte error code. Table 11 shows a matrix of commands, errors, and error codes.

Table 11. Memory and Control Function Command Error Code Matrix

ERROR EXPLANATION	Invalid Request Packet	Option Flag Set	Invalid Block Number	Already Locked	Already Locked	Authentication protected	Already locked	Write protected	Bad MAC	Problem sending message	Write protected	Bad sequence	Auth.- and Write Protected	Invalid parameter byte	Illegal value for NI2CWR or NI2CRX
ERROR CODE	02h	03h	10h	11h	12h	A0h					A1h		A2h	B0h	
FAILING COMMAND															
Get System Information	✓	✓													
Write Memory	✓	✓				✓					✓		✓	✓	
Read Memory	✓	✓												✓	
Read Single Block	✓	✓	✓												
Read Multiple Blocks	✓	✓	✓												
Set Protection	✓	✓				✓								✓	
Read Status	✓	✓												✓	
Read/Write Scratchpad	✓	✓												✓	
Load and Lock Secret	✓	✓					✓							✓	
Compute and Lock Secret	✓	✓					✓							✓	
Compute and Read Page MAC	✓	✓												✓	
Authenticated Write Memory RF Setup	✓	✓						✓						✓	
Authenticated Write Memory RF Execute	✓	✓							✓			✓			
Authenticated Set Protection RF Setup	✓	✓												✓	
Authenticated Set Protection RF Execute	✓	✓							✓			✓			
Configuration Write	✓	✓													
Configuration Read	✓	✓													
Control Write	✓	✓													
Control Read	✓	✓													
Get 1-Wire ROM ID	✓	✓													
Peripheral Transaction	✓	✓								✓					✓
Write AFI	✓	✓			✓										
Lock AFI	✓	✓		✓											
Write DSFID	✓	✓			✓										
Lock DSFID	✓	✓		✓											

Detailed Command Descriptions

Get System Information

This standard command allows retrieving technical data about the MAX66242. The response contains the transponder's Information Flags (IFLG), UID, data storage format identifier (DSFID), application family identifier (AFI), the number of available memory blocks (NBLK), and the memory block size (MBS), in this order. The Information flags are fixed at 07h. The UID varies from device to device. The DSFID and AFI are user programmable. The number of available memory blocks is fixed at 7Fh. The memory block size is fixed at 03h.

GET SYSTEM INFORMATION	
Command Code	2Bh
Parameter Byte	None
Conditions, Restrictions	None
Protocol Variations	None
Other Notes	See Figure 3 for the structure of the UID. The DSFID and AFI of unprogrammed parts are undefined. The DSFID and AFI are accessible (read/write/lock) only through the RF port.
Error Conditions (Error Response)	• Request data format error (response error code = 02h) • The Option_flag is set (response error code = 03h)
t1 (Request Frame to Response Frame Delay)	318.6μs to 323.3μs
MAC Notes	N/A
Memory Protection Status Affected	None
Secret Protection Status Affected	None

Write Memory

The Write Memory command is used to write a 4-byte block of a memory page.

WRITE MEMORY	
Command Code	55h
Parameter Byte	Page block number, memory page number (Table 12)
Conditions, Restrictions	None
Protocol Variations	None
Other Notes	See Figure 7 for the mapping of page block number and memory page number to the absolute block number, which is used by standard Read Single Block and Read Multiple Blocks commands. The new segment data is transmitted in the sequence B0, B1, B2, and B3. Figure 6 shows how these bytes map to the addressed memory page.
Error Conditions (Error Response)	• Request data format error (response error code = 02h) • The Option_flag is set (response error code = 03h) • Invalid Parameter byte (response error code = B0h) • The memory requires authentication (response error code = A0h) • The memory is write protected (response error code = A1h) • The memory is write protected and requires authentication (response error code A2h) • If the memory is write protected or requires authentication, the memory write cycle does not take place.
t1 (Request Frame to Response Frame Delay)	318.6μs to (1 x t_{PROG})
MAC Notes	N/A
Memory Protection Status Affected	The current protection settings apply.
Secret Protection Status Affected	None

Table 12. Parameter Byte Bitmap

BIT 7	BIT 6	BIT 5	BIT 4	BIT 3	BIT 2	BIT 1	BIT 0
BL#			0	PAGE#			

Note: *Bit 4 must be transmitted as 0 for the parameter byte to be valid.*

Bits [7:5]: Page Block Number (BL#). These bits specify the block within the selected memory page that is to be written to. Valid page block numbers are 000b (start of memory page) to 111b (end of memory page).

Bits [3:0]: Page Number (PAGE#). These bits specify the memory page to be written to. Valid memory page numbers are 0000b (page 0) to 1111b (page 15).

Read Memory

The Read Memory command is used to read a memory page starting at a specified block.

Read Memory	
Command Code	F0h
Parameter Byte	Page block number, memory page number (Table 13)
Conditions, Restrictions	None
Protocol Variations	The length of the response varies depending on the page block number.
Other Notes	See Figure 7 for the mapping of page block number and memory page number to the absolute block number, which is used by standard commands Read Single Block and Read Multiple Blocks. To read an entire memory page, the page block number must be 000b. When reading memory that is read protected, the response contains FFh bytes instead of the memory data.
Error Conditions (Error Response)	• Request data format error (response error code = 02h) • The Option_flag is set (response error code = 03h) • Invalid Parameter byte (response error code = B0h) • If the memory page is read protected, the device delivers FFh bytes instead of the actual memory data.
t1 (Request Frame to Response Frame Delay)	318.6μs to 323.3μs
MAC Notes	N/A
Memory Protection Status Affected	The current protection settings apply.
Secret Protection Status Affected	None

Table 13. Parameter Byte Bitmap

BIT 7	BIT 6	BIT 5	BIT 4	BIT 3	BIT 2	BIT 1	BIT 0
BL#			0	PAGE#			

Note: *Bit 4 must be transmitted as 0 for the parameter byte to be valid.*

Bits [7:5]: Page Block Number (BL#). These bits specify the location within the selected memory page at which the reading begins. Valid page block numbers are 000b (start of memory page) to 111b (end of memory page). The memory page is selected through bits [3:0].

Bits [3:0]: Page Number (PAGE#). These bits specify the memory page from which to be read. Valid memory page numbers are 0000b (page 0) to 1111b (page 15).

Read Single Block

The Read Single Block command is used to read a single memory block.

Read Single Block	
Command Code	20h
Parameter Byte	Absolute block number (Table 14)
Conditions, Restrictions	Option_flag=1 is not supported.
Protocol Variations	None
Other Notes	See Figure 7 for the mapping of the absolute block number to the page block number and memory page number.
Error Conditions (Error Response)	• Request data format error (response error code = 02h) • The Option_flag is set (response error code = 03h) • Invalid Parameter byte (response error code = 10h) • If the memory page is read protected, the device delivers FFh bytes instead of the actual memory data.
t1 (Request Frame to Response Frame Delay)	318.6µs to 323.3µs
MAC Notes	N/A
Memory Protection Status Affected	The current protection settings apply.
Secret Protection Status Affected	None

Table 14. Parameter Byte Bitmap

BIT 7	BIT 6	BIT 5	BIT 4	BIT 3	BIT 2	BIT 1	BIT 0
0	ABL#						

Note: *Bit 7 must be transmitted as 0 for the parameter byte to be valid.*

Bits [6:0]: Absolute Block Number (ABL#). These bits specify the memory block to be read using absolute block numbers. All absolute block numbers are valid.

Read Multiple Blocks

The Read Multiple Blocks command is used to read an arbitrary number of memory blocks, up to the end of memory.

Read Multiple Blocks	
Command Code	23h
Parameter Byte	Absolute block number (Table 15), number of blocks to read (Table 16)
Conditions, Restrictions	Option_flag=1 is not supported.
Protocol Variations	The length of the response varies depending on the number of blocks to be read.
Other Notes	See Figure 7 for the mapping of the absolute block number to the page block number and memory page number. If the sum of ABN and NBLOCK is greater than 127, the command reports all blocks starting at ABN through block 127.
Error Conditions (Error Response)	• Invalid Parameter byte 1 (response error code = 10h) • Request data format error (response error code = 02h) • The Option_flag is set (response error code = 03h) • If the memory page is read protected, the device delivers FFh bytes instead of the actual memory data.
t1 (Request Frame to Response Frame Delay)	318.6µs to 323.3µs
MAC Notes	N/A
Memory Protection Status Affected	The current protection settings apply.
Secret Protection Status Affected	None

Table 15. Parameter Byte 1 Bitmap

BIT 7	BIT 6	BIT 5	BIT 4	BIT 3	BIT 2	BIT 1	BIT 0
0	ABL#						

Note: *Bit 7 must be transmitted as 0 for the parameter byte to be valid.*

Bits [6:0]: Absolute Block Number (ABL#). These bits specify the memory block to start reading from using absolute block numbers. All absolute block numbers are valid.

Table 16. Parameter Byte 2 Bitmap

BIT 7	BIT 6	BIT 5	BIT 4	BIT 3	BIT 2	BIT 1	BIT 0
NBLOCK							

Bits [7:0]: Number of Blocks to Read (NBLOCK). These bits specify the number of memory blocks to be read. All NBLOCK values are valid. The number of blocks in the response is NBLOCK +1 unless a read beyond the end of memory is attempted.

Set Protection

The Set Protection command is used to set the protection for an individual memory page.

SET PROTECTION	
Command Code	C3h
Parameter Byte	Protection settings, memory page number (Table 17)
Conditions, Restrictions	None
Protocol Variations	None
Other Notes	Once set, a protection mode cannot be reset. Write protection invalidates EPROM emulation mode and authentication protection.
Error Conditions (Error Response)	• Request data format error (response error code = 02h) • The Option_flag is set (response error code = 03h) • Invalid Parameter byte (response error code = B0h) • The memory requires authentication (response code = A0h) If the page requires authentication, or if both write and read protection are already set, or if the protections are all set to 0 in the parameter byte, the parameter byte is invalid and the memory write cycle does not take place.
t1 (Request Frame to Response Frame Delay)	318.6μs to (1 x t_{PROG})
MAC Notes	N/A
Memory Protection Status Affected	The current protection settings apply, and protections are updated as specified in the parameter byte.
Secret Protection Status Affected	None

Table 17. Parameter Byte Bitmap

BIT 7	BIT 6	BIT 5	BIT 4	BIT 3	BIT 2	BIT 1	BIT 0
RP	WP	EM	AP	PAGE#			

Bit 7: Read Protection (RP). This bit specifies whether the memory page is to be read protected. If RP is 0 (factory default), the memory page will not be read protected. If RP is 1, the memory page becomes read protected and any read attempt returns FFh. The memory data is always internally accessible as input to the SHA-256 engine.

Bit 6: Write Protection (WP). This bit specifies whether the memory page is to be write protected. If WP is 0 (factory default), the memory page will not be write protected. If WP is 1, the memory page becomes write protected.

Bit 5: EPROM Emulation Mode (EM). This bit specifies whether the memory page is to be set up for EPROM emulation mode, where writing is limited to changing bits from 1 to 0. If EM is 0 and WP is 0 (factory default), the memory page will not be set up for EPROM emulation mode. If EM is 1 and WP is 0, the memory page becomes set up for EPROM emulation mode. Note: Normally, the affected memory page first needs to be programmed to FFh.

Bit 4: Authentication Protection (AP). This bit specifies whether memory write access requires host authentication. If AP is 0 (factory default), the memory page will not be authentication protected, and the page will be write accessible with and without host authentication. If AP is 1, the memory page becomes authentication protected, and the page will be write accessible only with host authentication

Bits [3:0]: Page Number (PAGE#). These bits specify the memory page for which the specified protection is to be set. Valid memory page numbers are 0000b (page 0) to 1111b (page 15).

Read Status

The Read Status command is used to read the memory page protection settings or to read the transponder's two personality bytes (PB1and PB2), which includes the secret protection setting, and the 2-byte Manufacturer ID. The Manufacturer ID reads 0000h unless the device is programmed with customer specific data using the factory preprogramming service.

READ STATUS	
Command Code	AAh
Parameter Byte	Mode selection (page protection or personality bytes), starting memory page number (Table 18)
Conditions, Restrictions	None
Protocol Variations	Reading the page protection Reading the personality bytes
Other Notes	The page protection bytes are reported beginning with the specified starting page and continue through page 15. See Table 19 for the protection byte bitmap. The personality bytes (Table 20) are reported in the sequence PB1, PB2, MAN_ID_L, and MAN_ID_H.
Error Conditions (Error Response)	• Request data format error (response error code = 02h) • The Option_flag is set (response error code = 03h) • Invalid Parameter byte (response error code = B0h)
t1 (Request Frame to Response Frame Delay)	318.6µs to 323.3µs
MAC Notes	N/A
Memory Protection Status Affected	None
Secret Protection Status Affected	None

Table 18. Parameter Byte Bitmap

BIT 7	BIT 6	BIT 5	BIT 4	BIT 3	BIT 2	BIT 1	BIT 0
MS			0	PAGE#			

Note: *Bit 4 must be transmitted as 0 for the parameter byte to be valid.*

Bits [7:5]: Mode selection (MS). These bits specify whether the page protection or the personality bytes are to be read. If MS is 000b, page protection is reported. If MS is 111b, personality bytes (including secret protection) and manufacturer identification number is reported. All other codes are invalid.

Bits [3:0]: Page Number (PAGE#). These bits specify the starting memory page for which the protection is to be reported if MS = 000b. Valid memory page numbers are 0000b (page 0) to 1111b (page 15). The memory page number is irrelevant if MS = 111b.

Table 19. Protection Byte Bitmap

BIT 7	BIT 6	BIT 5	BIT 4	BIT 3	BIT 2	BIT 1	BIT 0
RP	WP	EM	AP	PAGE#			

Bit 7: Read Protection (RP). This bit specifies whether the memory page is read protected. If RP is 0 (factory default), the memory page is not read protected. If RP is 1, the memory page is read protected and any read attempt returns FFh. The memory data is always internally accessible as input to the SHA-256 engine.

Bit 6: Write Protection (WP). This bit specifies whether the memory page is write protected. If WP is 0 (factory default), the memory page is not protected. If WP is 1, the memory page is write protected.

Bit 5: EPROM Emulation Mode (EM). This bit specifies whether the memory page is set up for EPROM emulation mode. If EM is 0 and WP is 0 (factory default), the memory page is not set up for EPROM emulation mode. If EM is 1 and WP is 0, the memory page is set up for EPROM emulation mode.

Bit 4: Authentication Protection (AP). This bit specifies whether the memory page is authentication protected. If AP is 0 and WP is 0, (factory default), the memory page is not authentication protected, and the page is write accessible with and without host authentication. If AP is 1 and WP is 0, the memory page becomes authentication protected, and the page will be write accessible only with host authentication

Bits [3:0]: Page Number (PAGE#). These bits specify the memory page for which the reported protection applies. The page number increments if the reader reads more than one protection byte.

Table 20. Personality Bytes Bitmap

NAME	BIT 7	BIT 6	BIT 5	BIT 4	BIT 3	BIT 2	BIT 1	BIT 0
PB1	0	0	0	0	0	0	1	0
PB2	0	0	0	0	0	0	1	SL
MAN_ID_L	00h (default) or factory programmed							
MAN_ID_H	00h (default) or factory programmed							

Bit 0: Secret Lock Status (SL). This bit specifies whether the secret is write-protected. If the SL bit is 0 (factory default), the secret is not protected. If the SL bit is 1, the secret is write-protected.

Read/Write Scratchpad

The Read/Write scratchpad is used to write data to be loaded as the secret with Load and Lock Secret, to write a "challenge" for use when computing a new secret with Compute and Lock Secret, to write a "challenge" when using Compute and Read Page MAC, or to read the scratchpad.

READ/WRITE SCRATCHPAD	
Command Code	0Fh
Parameter Byte	Read/Write Mode (Table 22)
Conditions, Restrictions	None
Protocol Variations	• Writing 32 bytes to scratchpad • Reading the scratchpad
Other Notes	See Table 21 for the mapping of transmission sequence to scratchpad location. The personality bytes (Table 20) are reported in the sequence PB1, PB2, MAN_ID_L, and MAN_ID_H.
Error Conditions (Error Response)	• Request data format error (response error code = 02h) • The Option_flag is set (response error code = 03h) • Invalid Parameter byte (response error code = B0h) • If the parameter byte is invalid and there is also a request data format error, the error code will be B0h.
t1 (Request Frame to Response Frame Delay)	318.6µs to (1 x t_{RFAIP}) if writing 318.6µs to 323.3µs if reading
MAC Notes	N/A
Memory Protection Status Affected	None
Secret Protection Status Affected	None

Table 21. Mapping of Scratchpad Location to Transmission Sequence

(DB+0):= (TX+0)	(DB+1):= (TX+1)	(DB+2):= (TX+2)	(DB+3):= (TX+3)
(DB+4):= (TX+4)	(DB+5):= (TX+5)	(DB+6):= (TX+6)	(DB+7):= (TX+7)
(DB+8):= (TX+8)	(DB+9):= (TX+9)	(DB+10):= (TX+10)	(DB+11):= (TX+11)
(DB+12):= (TX+12)	(DB+13):= (TX+13)	(DB+14):= (TX+14)	(DB+15):= (TX+15)
(DB+16):= (TX+16)	(DB+17):= (TX+17)	(DB+18):= (TX+18)	(DB+19):= (TX+19)
(DB+20):= (TX+20)	(DB+21):= (TX+21)	(DB+22):= (TX+22)	(DB+23):= (TX+23)
(DB+24):= (TX+24)	(DB+25):= (TX+25)	(DB+26):= (TX+26)	(DB+27):= (TX+27)
(DB+28):= (TX+28)	(DB+29):= (TX+29)	(DB+30):= (TX+30)	(DB+31):= (TX+31)

Legend:

DB+N	Byte N of the scratchpad, 0 ≤ N ≤ 31
TX+N	Byte N as transmitted, 0 ≤ N ≤ 31

Table 22. Parameter Byte Bitmap

BIT 7	BIT 6	BIT 5	BIT 4	BIT 3	BIT 2	BIT 1	BIT 0
0	0	1	0	RWZ			

Note: *Bits 7:4 must be transmitted as shown for the parameter byte to be valid.*

Bits [3:0]: Read/Write Mode (RWZ). These bits specify whether the scratchpad access is a write or read. If RWZ is 0000b, a write is selected. If RWZ is 1111b, a read is selected. All other codes are invalid.

Load and Lock Secret

The Load and Lock Secret command is used to load a predefined secret. This command takes the data (i.e., the secret) in the scratchpad and copies it to the secret memory. The secret can additionally be write protected. Write protection cannot be reset. Since this command may not clear the scratchpad, the scratchpad should be overwritten with dummy data after the command is completed. This command is equivalent to I2C Install and Lock Secret command with L/C = 0.

Load and Lock Secret	
Command Code	33h
Parameter Byte	Lock control (Table 24)
Conditions, Restrictions	The Read/Write Scratchpad command should be issued prior to this command to define the secret.
Protocol Variations	None
Other Notes	Loading the secret copies the entire scratchpad to the secret. See Table 23 for the mapping of scratchpad to secret. If the secret is already locked or the parameter byte is invalid, the memory write cycle does not take place.
Error Conditions (Error Response)	• Request data format error (response error code = 02h) • The Option_flag is set (response error code = 03h) • Invalid Parameter byte (response error code = B0h) • The secret is already locked (response error code = A0h)
t1 (Request Frame to Response Frame Delay)	Not locking secret: 318.6µs to (8 x t_{PROG}) Locking secret: 318.6µs to (9 x t_{PROG})
MAC Notes	N/A
Memory Protection Status Affected	None
Secret Protection Status Affected	The current protection setting applies, and the protection is updated as specified in the parameter byte.

Table 23. Mapping of Scratchpad to Secret (Loaded Secret)

(SS+0):= (DB+0)	(SS+1):= (DB+1)	(SS+2):= (DB+2)	(SS+3):= (DB+3)
(SS+4):= (DB+4)	(SS+5):= (DB+5)	(SS+6):= (DB+6)	(SS+7):= (DB+7)
(SS+8):= (DB+8)	(SS+9):= (DB+9)	(SS+10):= (DB+10)	(SS+11):= (DB+11)
(SS+12):= (DB+12)	(SS+13):= (DB+13)	(SS+14):= (DB+14)	(SS+15):= (DB+15)
(SS+16):= (DB+16)	(SS+17):= (DB+17)	(SS+18):= (DB+18)	(SS+19):= (DB+19)
(SS+20):= (DB+20)	(SS+21):= (DB+21)	(SS+22):= (DB+22)	(SS+23):= (DB+23)
(SS+24):= (DB+24)	(SS+25):= (DB+25)	(SS+26):= (DB+26)	(SS+27):= (DB+27)
(SS+28):= (DB+28)	(SS+29):= (DB+29)	(SS+30):= (DB+30)	(SS+31):= (DB+31)

Legend:

SS+N	Byte N of the secret, 0 ≤ N ≤ 31.
DB+N	Byte N of the scratchpad, 0 ≤ N ≤ 31.

Table 24. Parameter Byte Bitmap

BIT 7	BIT 6	BIT 5	BIT 4	BIT 3	BIT 2	BIT 1	BIT 0
LOCK			0	X	X	X	X

***Note:** Bit 4 must be transmitted as 0 for the parameter byte to be valid. Bits marked as X can be transmitted as 0 or 1 without affecting the command.*

Bits [7:5]: Lock Control (LOCK). These bits specify whether the secret is to be write protected after it is copied to the secret memory. If LOCK is 000b, the secret is not write protected. If LOCK is 111b, the secret is write protected. All other codes are invalid.

Compute and Lock Secret

The Compute and Lock Secret command is used to compute a device-specific secret. A computed secret is recommended; to increase the security level, one can use this command multiple times, each time with a different partial secret written to the scratchpad. When computing the secret, this command uses the scratchpad content together with the data from a selected memory page, the secret already in the device, the device's 64-bit ROM ID (Figure 4), the number of the selected memory page, the manufacturer ID and padding as input for a MAC computation. The resulting MAC is then written to the secret. The computation of the secret involves two 512-bit message blocks and consequently two cycles of the SHA-256 engine. The secret can additionally be write protected. Write protection cannot be reset. Since this command may not clear the scratchpad, the scratchpad should be overwritten with dummy data after the command is completed. This command is equivalent to I2C Install and Lock Secret command with L/C = 1, except for second block M10[31:24].

COMPUTE AND LOCK SECRET	
Command Code	3Ch
Parameter Byte	Lock control, memory page number (Table 25)
Conditions, Restrictions	The Read/Write Scratchpad command should be issued prior to this command to define the partial secret.
Protocol Variations	None
Other Notes	None
Error Conditions (Error Response)	• Request data format error (response error code = 02h) • The Option_flag is set (response error code = 03h) • Invalid Parameter byte (response error code = B0h) • The secret is already locked (response error code = A0h) If the secret is already locked or the parameter byte is invalid, the MAC computation and write cycle do not take place.
t1 (Request Frame to Response Frame Delay)	Not locking secret: 318.6μs to (2 × t_{CSHA} + 8 x t_{PROG}) Locking secret: 318.6μs to (2 × t_{CSHA} + 9 x t_{PROG})
MAC Notes	See Table 26 for the message input that is used for computing the MAC and Table 27 for mapping of the MAC to the secret.
Memory Protection Status Affected	None
Secret Protection Status Affected	The current protection setting applies, and the protection is updated as specified in the parameter byte.

Table 25. Parameter Byte Bitmap

BIT 7	BIT 6	BIT 5	BIT 4	BIT 3	BIT 2	BIT 1	BIT 0
LOCK			0	PAGE#			

Note: *Bit 4 must be transmitted as 0 for the parameter byte to be valid.*

Bits [7:5]: Lock Control (LOCK). These bits specify whether the secret is to be write protected after it is copied to the secret memory. If LOCK is 000b, the secret is not write protected. If LOCK is 111b, the secret is write protected. All other codes are invalid.

Bits [3:0]: Page Number (PAGE#). These bits specify the memory page to be used for the MAC computation. Valid memory page numbers are 0000b (page 0) to 1111b (page 15).

Table 26. SHA-256 Engine Input Data for Compute and Read Page MAC, Compute and Lock Secret

Message, First Block

M0^1[31:24] = (PP+3)	M0^1[23:16] = (PP+2)	M0^1[15:8] = (PP+1)	M0^1[7:0] = (PP+0)
M1^1[31:24] = (PP+7)	M1^1[23:16] = (PP+6)	M1^1[15:8] = (PP+5)	M1^1[7:0] = (PP+4)
M2^1[31:24] = (PP+11)	M2^1[23:16] = (PP+10)	M2^1[15:8] = (PP+9)	M2^1[7:0] = (PP+8)
M3^1[31:24] = (PP+15)	M3^1[23:16] = (PP+14)	M3^1[15:8] = (PP+13)	M3^1[7:0] = (PP+12)
M4^1[31:24] = (PP+19)	M4^1[23:16] = (PP+18)	M4^1[15:8] = (PP+17)	M4^1[7:0] = (PP+16)
M5^1[31:24] = (PP+23)	M5^1[23:16] = (PP+22)	M5^1[15:8] = (PP+21)	M5^1[7:0] = (PP+20)
M6^1[31:24] = (PP+27)	M6^1[23:16] = (PP+26)	M6^1[15:8] = (PP+25)	M6^1[7:0] = (PP+24)
M7^1[31:24] = (PP+31)	M7^1[23:16] = (PP+30)	M7^1[15:8] = (PP+29)	M7^1[7:0] = (PP+28)
M8^1[31:24] = DB+3	M8^1[23:16] = DB+2	M8^1[15:8] = DB+1	M8^1[7:0] = DB+0
M9^1[31:24] = DB+7	M9^1[23:16] = DB+6	M9^1[15:8] = DB+5	M9^1[7:0] = DB+4
M10^1[31:24] = DB+11	M10^1[23:16] = DB+10	M10^1[15:8] = DB+9	M10^1[7:0] = DB+8
M11^1[31:24] = DB+15	M11^1[23:16] = DB+14	M11^1[15:8] = DB+13	M11^1[7:0] = DB+12
M12^1[31:24] = DB+19	M12^1[23:16] = DB+18	M12^1[15:8] = DB+17	M12^1[7:0] = DB+16
M13^1[31:24] = DB+23	M13^1[23:16] = DB+22	M13^1[15:8] = DB+21	M13^1[7:0] = DB+20
M14^1[31:24] = DB+27	M14^1[23:16] = DB+26	M14^1[15:8] = DB+25	M14^1[7:0] = DB+24
M15^1[31:24] = DB+31	M15^1[23:16] = DB+30	M15^1[15:8] = DB+29	M15^1[7:0] = DB+28

Message, Second Block

M0^2[31:24] = (SS+3)	M0^2[23:16] = (SS+2)	M0^2[15:8] = (SS+1)	M0^2[7:0] = (SS+0)
M1^2[31:24] = (SS+7)	M1^2[23:16] = (SS+6)	M1^2[15:8] = (SS+5)	M1^2[7:0] = (SS+4)
M2^2[31:24] = (SS+11)	M2^2[23:16] = (SS+10)	M2^2[15:8] = (SS+9)	M2^2[7:0] = (SS+8)
M3^2[31:24] = (SS+15)	M3^2[23:16] = (SS+14)	M3^2[15:8] = (SS+13)	M3^2[7:0] = (SS+12)
M4^2[31:24] = (SS+19)	M4^2[23:16] = (SS+18)	M4^2[15:8] = (SS+17)	M4^2[7:0] = (SS+16)
M5^2[31:24] = (SS+23)	M5^2[23:16] = (SS+22)	M5^2[15:8] = (SS+21)	M5^2[7:0] = (SS+20)
M6^2[31:24] = (SS+27)	M6^2[23:16] = (SS+26)	M6^2[15:8] = (SS+25)	M6^2[7:0] = (SS+24)
M7^2[31:24] = (SS+31)	M7^2[23:16] = (SS+30)	M7^2[15:8] = (SS+29)	M7^2[7:0] = (SS+28)
M8^2[31:24] = (RN+3)	M8^2[23:16] = (RN+2)	M8^2[15:8] = (RN+1)	M8^2[7:0] = (RN+0)
M9^2[31:24] = (RN+7)	M9^2[23:16] = (RN+6)	M9^2[15:8] = (RN+5)	M9^2[7:0] = (RN+4)
M10^2[31:24] = 00h	M10^2[23:16] = (PAGE#)	M10^2[15:8] = MAN_ID_H	M10^2[7:0] = MAN_ID_L
M11^2[31:24] = 00h	M11^2[23:16] = 00h	M11^2[15:8] = 00h	M11^2[7:0] = 00h
M12^2[31:24] = 00h	M12^2[23:16] = 00h	M12^2[15:8] = 00h	M12^2[7:0] = 00h
M13^2[31:24] = 00h	M13^2[23:16] = 00h	M13^2[15:8] = 00h	M13^2[7:0] = 80h
M14^2[31:24] = 00h	M14^2[23:16] = 00h	M14^2[15:8] = 00h	M14^2[7:0] = 00h
M15^2[31:24] = 00h	M15^2[23:16] = 00h	M15^2[15:8] = 03h	M15^2[7:0] = B8h

Table 26. SHA-256 Engine Input Data for Compute and Read Page MAC, Compute and Lock Secret (continued)

Legend:

Mt	Input buffer of SHA engine; 0 ≤ t ≤ 15; 32-bit words.
(PP+N)	Byte N of selected Memory Page; 0 ≤ N ≤ 31.
DB+N	Byte N of the scratchpad, 0 ≤ N ≤ 31.
(SS+N)	Byte N of Secret; 0 ≤ N ≤ 31.
(RN+N)	Byte N of ROM ID; 0 ≤ N ≤ 7. RN+0 corresponds to the family code.
(PAGE#)	Page number as in the parameter byte, padded with 0000b in the upper bits.
MAN_ID_L MAN_ID_H	16-bit manufacturer ID. The value is 0000h for parts that are not factory preprogrammed.

Table 27. Mapping of the MAC Components to the Bytes of the Computed Secret

(SS+0):= H_7[7:0]	(SS+1):= H_7[15:8]	(SS+2):= H_7[23:16]	(SS+3):= H_7[31:24]
(SS+4):= H_6[7:0]	(SS+5):= H_6[15:8]	(SS+6):= H_6[23:16]	(SS+7):= H_6[31:24]
(SS+8):= H_5[7:0]	(SS+9):= H_5[15:8]	(SS+10):= H_5[23:16]	(SS+11):= H_5[31:24]
(SS+12):= H_4[7:0]	(SS+13):= H_4[15:8]	(SS+14):= H_4[23:16]	(SS+15):= H_4[31:24]
(SS+16):= H_3[7:0]	(SS+17):= H_3[15:8]	(SS+18):= H_3[23:16]	(SS+19):= H_3[31:24]
(SS+20):= H_2[7:0]	(SS+21):= H_2[15:8]	(SS+22):= H_2[23:16]	(SS+23):= H_2[31:24]
(SS+24):= H_1[7:0]	(SS+25):= H_1[15:8]	(SS+26):= H_1[23:16]	(SS+27):= H_1[31:24]
(SS+28):= H_0[7:0]	(SS+29):= H_0[15:8]	(SS+30):= H_0[23:16]	(SS+31):= H_0[31:24]

Legend:

SS+N	Byte N of the secret, 0 ≤ N ≤ 31.

Compute and Read Page MAC

The Compute and Read Page MAC command is used to authenticate the MAX66242 to the reader. The reader computes the MAC from the same data and the expected secret. If both MACs are identical, the device is confirmed authentic within the application. This command uses the scratchpad content as a challenge together with the data from a selected memory page, the secret, the device's 64-bit ROM ID (Figure 4), the number of the selected memory page, the manufacturer ID, and padding as input for a MAC computation. The computation of the MAC involves two 512-bit message blocks and consequently two cycles of the SHA-256 engine. Optionally, the ROM ID can be replaced by FFh bytes, which makes the MAC result device independent (anonymous).

COMPUTE AND READ PAGE MAC	
Command Code	A5h
Parameter Byte	Anonymous indicator, page selection (Table 28)
Conditions, Restrictions	The scratchpad should be written to a known value before executing this command.
Protocol Variations	None
Other Notes	The scratchpad content is used as a "challenge."
Error Conditions (Error Response)	• Invalid Parameter byte (response error code = B0h) • Request data format error (response error code = 02h) • The Option_flag is set (response error code = 03h) If the parameter byte is not valid, the MAC computation does not take place.
t1 (Request Frame to Response Frame Delay)	318.6µs to (2 x t_{CSHA})
MAC Notes	See Table 26 for the message input that is used for computing the MAC. See Table 29 for the MAC byte transmission sequence.
Memory Protection Status Affected	None
Secret Protection Status Affected	None

Table 28. Parameter Byte Bitmap

BIT 7	BIT 6	BIT 5	BIT 4	BIT 3	BIT 2	BIT 1	BIT 0
ANON			0	PAGE#			

Note: *Bit 4 must be transmitted as 0 for the parameter byte to be valid.*

Bits [7:5]: Anonymous Indicator (ANON). These bits specify whether the transponder's ROM ID is to be used for the MAC computation. To use the ROM ID, these bits must be 000b. To make the MAC anonymous by replacing the ROM ID with FFh bytes, these bits must be 111b. All other codes are invalid and, if chosen, cause the parameter byte to be invalid. An anonymous MAC can serve as virtually random data for one-time pad small message encryption and decryption.

Bits [3:0]: Page Selection (PAGE#). These bits specify the memory page to be used for the MAC computation. Valid memory page numbers are 0000b (page 0) to 1111b (page 15).

Table 29. MAC Byte Transmission Sequence

(MB+0):= H_7[7:0]	(MB+1):= H_7[15:8]	(MB+2):= H_7[23:16]	(MB+3):= H_7[31:24]
(MB+4):= H_6[7:0]	(MB+5):= H_6[15:8]	(MB+6):= H_6[23:16]	(MB+7):= H_6[31:24]
(MB+8):= H_5[7:0]	(MB+9):= H_5[15:8]	(MB+10):= H_5[23:16]	(MB+11):= H_5[31:24]
(MB+12):= H_4[7:0]	(MB+13):= H_4[15:8]	(MB+14):= H_4[23:16]	(MB+15):= H_4[31:24]
(MB+16):= H_3[7:0]	(MB+17):= H_3[15:8]	(MB+18):= H_3[23:16]	(MB+19):= H_3[31:24]
(MB+20):= H_2[7:0]	(MB+21):= H_2[15:8]	(MB+22):= H_2[23:16]	(MB+23):= H_2[31:24]
(MB+24):= H_1[7:0]	(MB+25):= H_1[15:8]	(MB+26):= H_1[23:16]	(MB+27):= H_1[31:24]
(MB+28):= H_0[7:0]	(MB+29):= H_0[15:8]	(MB+30):= H_0[23:16]	(MB+31):= H_0[31:24]

Legend:

MB+N	Byte N of the MAC, 0 ≤ N ≤ 31

Authenticated Write Memory RF Setup

The Authenticated Write Memory RF Setup command is the first step required to program a 4-byte block of an authentication protected memory page.

AUTHENTICATED WRITE MEMORY RF SETUP	
Command Code	5Ah
Parameter Byte	Page block number, memory page number (Table 30)
Conditions, Restrictions	This command must be followed by an Authenticated Write Memory RF Execute command
Protocol Variations	None
Other Notes	The new segment data is transmitted in the sequence B0, B1, B2, and B3. Figure 5 shows how these bytes map to the addressed memory page. This command also works on pages that are not authentication protected.
Error Conditions (Error Response)	• Request data format error (response error code = 02h) • The Option_flag is set (response error code = 03h) • Invalid Parameter byte (response error code = B0h) • The memory is write protected (response error code = A0h) If the memory is write protected, the parameter byte is invalid and the MAC computation does not take place.
t1 (Request Frame to Response Frame Delay)	318.6µs to (1 x t_{CSHA})
MAC Notes	N/A
Memory Protection Status Affected	The current protection settings apply.
Secret Protection Status Affected	None

Table 30. Parameter Byte Bitmap

BIT 7	BIT 6	BIT 5	BIT 4	BIT 3	BIT 2	BIT 1	BIT 0
BL#			0	PAGE#			

Note: *Bit 4 must be transmitted as 0 for the parameter byte to be valid.*

Bits [7:5]: Block Number (BL#). These bits specify the location within the selected memory page that is to be written to. Valid page block numbers are 000b (start of memory page) to 111b (last block of memory page). The memory page is selected through bits [3:0].

Bits [3:0]: Page Number (PAGE#). These bits specify the memory page to be written to. Valid memory page numbers are 0000b (page 0) to 1111b (page 15).

Authenticated Write Memory RF Execute

The Authenticated Write Memory RF Execute command is the second step required to program a 4-byte block of an authentication protected memory page. The reader must provide a MAC that is based on the device's secret and other data elements.

AUTHENTICATED WRITE MEMORY RF EXECUTE	
Command Code	5Bh
Parameter Byte	Any value is accepted.
Conditions, Restrictions	This command must be preceded by an Authenticated Write Memory RF Setup command
Protocol Variations	None
Other Notes	None
Error Conditions (Error Response)	• Request data format error (response error code = 02h) • The Option_flag is set (response error code = 03h) • The preceding command was not Authenticated Write Memory RF Setup, or was Authenticated Write Memory RF Setup with an invalid parameter byte, or was Authenticated Write Memory RF Setup to a write protected page (response error code = A1h) • The MAC provided by the reader is not valid (response error code = A0h) If the MAC is not valid, the memory write cycle does not take place.
t1 (Request Frame to Response Frame Delay)	318.6µs to (1 x t_{PROG})
MAC Notes	See Table 31 for the message input that is used for computing the MAC. See Table 29 for the MAC byte transmission sequence.
Memory Protection Status Affected	The current protection settings apply.
Secret Protection Status Affected	None

Table 31. SHA Input Data for I2C Authenticated Write Memory and RF Authenticated Write Memory RF Execute

M0[31:24] = (SS+3)	M0[23:16] = (SS+2)	M0[15:8] = (SS+1)	M0[7:0] = (SS+0)
M1[31:24] = (SS+7)	M1[23:16] = (SS+6)	M1[15:8] = (SS+5)	M1[7:0] = (SS+4)
M2[31:24] = (SS+11)	M2[23:16] = (SS+10)	M2[15:8] = (SS+9)	M2[7:0] = (SS+8)
M3[31:24] = (SS+15)	M3[23:16] = (SS+14)	M3[15:8] = (SS+13)	M3[7:0] = (SS+12)
M4[31:24] = (SS+19)	M4[23:16] = (SS+18)	M4[15:8] = (SS+17)	M4[7:0] = (SS+16)
M5[31:24] = (SS+23)	M5[23:16] = (SS+22)	M5[15:8] = (SS+21)	M5[7:0] = (SS+20)
M6[31:24] = (SS+27)	M6[23:16] = (SS+26)	M6[15:8] = (SS+25)	M6[7:0] = (SS+24)
M7[31:24] = (SS+31)	M7[23:16] = (SS+30)	M7[15:8] = (SS+29)	M7[7:0] = (SS+28)
M8[31:24] = (RN+3)	M8[23:16] = (RN+2)	M8[15:8] = (RN+1)	M8[7:0] = (RN+0)
M9[31:24] = (RN+7)	M9[23:16] = (RN+6)	M9[15:8] = (RN+5)	M9[7:0] = (RN+4)
M10[31:24] = (BL#)	M10[23:16] = (PAGE#)	M10[15:8] = MAN_ID_H	M10[7:0] = MAN_ID_L
M11[31:24] = (OSEG+3)	M11[23:16] = (OSEG+2)	M11[15:8] = (OSEG+1)	M11[7:0] = (OSEG+0)
M12[31:24] = B3	M12[23:16] = B2	M12[15:8] = B1	M12[7:0] = B0
M13[31:24] = 00h	M13[23:16] = 00h	M13[15:8] = 00h	M13[7:0] = 80h
M14[31:24] = 00h	M14[23:16] = 00h	M14[15:8] = 00h	M14[7:0] = 00h
M15[31:24] = 00h	M15[23:16] = 00h	M15[15:8] = 01h	M15[7:0] = B8h

Legend:

Mt	Input buffer of SHA engine; 0 ≤ t ≤ 15; 32-bit words.
(SS + N)	Byte N of Secret; 0 ≤ N ≤ 31.
(RN + N)	Byte N of ROM ID; 0 ≤ N ≤ 7. RN + 0 corresponds to the family code.
(PAGE#)	Page number as in the parameter byte, padded with 0000b in the upper bits.
(BL#)	block number as in the parameter byte, padded with 00000b in the upper nibble.
MAN_ID_L MAN_ID_H	16-bit manufacturer ID. The value is 0000h for parts that are not factory preprogrammed.
(OSEG+N)	Old page block data; 0 ≤ N ≤ 3. N = 0 corresponds to B0 in the user memory map.
BX	Byte X of the new data, 0 ≤ X ≤ 3.

Authenticated Set Protection RF Setup

The Authenticated Set Protection RF Setup command is the first step required to set the protections for an authentication protected memory page.

Authenticated Set Protection RF Setup	
Command Code	CCh
Parameter Byte	Protection settings, memory page number (Table 32)
Conditions, Restrictions	This command must be followed by an Authenticated Set Protection RF Execute command
Protocol Variations	None
Other Notes	Once set, a protection mode cannot be reset. Write protection invalidates EPROM emulation mode and authentication protection. The parameter byte is invalid if all protection bits are 0 (no protection to change) or if both read protection and write protection are already set.
Error Conditions (Error Response)	• Request data format error (response error code = 02h) • The Option_flag is set (response error code = 03h) • Invalid Parameter byte (response error code = B0h) If both write and read protection are already set, or the protections are all set to 0 in the parameter byte, the parameter byte is invalid and the MAC computation does not take place.
t1 (Request Frame to Response Frame Delay)	318.6µs to (1 x t_{CSHA})
MAC Notes	N/A
Memory Protection Status Affected	The current protection settings apply.
Secret Protection Status Affected	None

Table 32. Parameter Byte Bitmap

BIT 7	BIT 6	BIT 5	BIT 4	BIT 3	BIT 2	BIT 1	BIT 0
RP	WP	EM	AP	PAGE#			

Bit 7: Read Protection (RP). This bit specifies whether the memory page is to be read protected. If RP is 0 (factory default), the memory page will not be read protected. If RP is 1, the memory page becomes read protected and any read attempt returns FFh. The memory data is always internally accessible as input to the SHA-256 engine.

Bit 6: Write Protection (WP). This bit specifies whether the memory page is to be write protected. If WP is 0 (factory default), the memory page will not be write protected. If WP is 1, the memory page becomes write protected.

Bit 5: EPROM Emulation Mode (EM). This bit specifies whether the memory page is to be set up for EPROM emulation mode, where writing is limited to changing bits from 1 to 0. If EM is 0 and WP is 0 (factory default), the memory page will not be set up for EPROM emulation mode. If EM is 1 and WP is 0, the memory page becomes set up for EPROM emulation mode. Note: Normally, the affected memory page first needs to be programmed to FFh.

Bit 4: Authentication Protection (AP). This bit specifies whether memory write access requires host authentication. If AP is 0 (factory default), the memory page will not be authentication protected, and the page will be write accessible with and without host authentication. If AP is 1, the memory page becomes authentication protected, and the page will be write accessible only with host authentication

Bits [3:0]: Page Number (PAGE#). These bits specify the memory page for which the specified protection is to be set. Valid memory page numbers are 0000b (page 0) to 1111b (page 15).

Authenticated Set Protection RF Execute

The Authenticated Set Protection RF Execute command is the second step required to set the protections for an authentication protected memory page. The reader must provide a MAC that is based on the device's secret and other data elements.

AUTHENTICATED SET PROTECTION RF EXECUTE	
Command Code	CDh
Parameter Byte	Any value is accepted.
Conditions, Restrictions	This command must be preceded by an Authenticated Set Protection RF Setup command
Protocol Variations	None
Other Notes	None
Error Conditions (Error Response)	• Request data format error (response error code = 02h) • The Option_flag is set (response error code = 03h) • The MAC provided by the reader is not valid (response error code = A0h) • The preceding command was not Authenticated Write Page Protection RF Setup, or was Authenticated Write Page Protection RF Setup with an invalid parameter byte (response error code = A1h) If the MAC provided is not valid, the memory write cycle does not take place.
t1 (Request Frame to Response Frame Delay)	318.6µs to (1 x t_{PROG})
MAC Notes	See Table 33 for the message input that is used for computing the MAC. See Table 29 for the MAC byte transmission sequence.
Memory Protection Status Affected	The current protection settings apply, and protections are updated as specified in the preceding Authenticated Set Protection RF Setup command.
Secret Protection Status Affected	None

Table 33. SHA Input Data for I^{2}C Authenticated Set Protection and RF Authenticated Set Protection RF Execute

M0[31:24] = (SS+3)	M0[23:16] = (SS+2)	M0[15:8] = (SS+1)	M0[7:0] = (SS+0)
M1[31:24] = (SS+7)	M1[23:16] = (SS+6)	M1[15:8] = (SS+5)	M1[7:0] = (SS+4)
M2[31:24] = (SS+11)	M2[23:16] = (SS+10)	M2[15:8] = (SS+9)	M2[7:0] = (SS+8)
M3[31:24] = (SS+15)	M3[23:16] = (SS+14)	M3[15:8] = (SS+13)	M3[7:0] = (SS+12)
M4[31:24] = (SS+19)	M4[23:16] = (SS+18)	M4[15:8] = (SS+17)	M4[7:0] = (SS+16)
M5[31:24] = (SS+23)	M5[23:16] = (SS+22)	M5[15:8] = (SS+21)	M5[7:0] = (SS+20)
M6[31:24] = (SS+27)	M6[23:16] = (SS+26)	M6[15:8] = (SS+25)	M6[7:0] = (SS+24)
M7[31:24] = (SS+31)	M7[23:16] = (SS+30)	M7[15:8] = (SS+29)	M7[7:0] = (SS+28)
M8[31:24] = (RN+3)	M8[23:16] = (RN+2)	M8[15:8] = (RN+1)	M8[7:0] = (RN+0)
M9[31:24] = (RN+7)	M9[23:16] = (RN+6)	M9[15:8] = (RN+5)	M9[7:0] = (RN+4)
M10[31:24] = 00h	M10[23:16] = **PAGE#**	M10[15:8] = MAN_ID_H	M10[7:0] = MAN_ID_L
M11[31:24] = OPROT3	M11[23:16] = OPROT2	M11[15:8] = OPROT1	M11[7:0] = OPROT0
M12[31:24] = NPROT3	M12[23:16] = NPROT2	M12[15:8] = NPROT1	M12[7:0] = NPROT0
M13[31:24] = 00h	M13[23:16] = 00h	M13[15:8] = 00h	M13[7:0] = 80h
M14[31:24] = 00h	M14[23:16] = 00h	M14[15:8] = 00h	M14[7:0] = 00h
M15[31:24] = 00h	M15[23:16] = 00h	M15[15:8] = 01h	M15[7:0] = B8h

Legend:

Mt	Input buffer of SHA engine; 0 ≤ t ≤ 15; 32-bit words.
(SS + N)	Byte N of Secret; 0 ≤ N ≤ 31.
(RN + N)	Byte N of ROM ID; 0 ≤ N ≤ 7. RN + 0 corresponds to the family code.
PAGE#	**Page** number as in the parameter byte, padded with 0000b in the upper bits.
MAN_ID_L MAN_ID_H	16-bit manufacturer ID. The value is 0000h for parts that are not factory preprogrammed.

OPROTn	Old protection state as reported when reading the block protection through the Read Status command or through the I^{2}C Memory Protection Status registers.
	OPROT0: {0000000b, AP}; OPROT1: {0000000b, EM};
	OPROT2: {0000000b, WP}; OPROT3: {0000000b, RP}

NPROTn	New protection state. NPROT3 corresponds to RP, NPROT2 to WP, NPROT1 to EM, and NPROT0 to AP. The upper 7 bits are 0. The RP, WP, EM, and AP bit states of the NPROTn bytes are identical to those in the parameter byte.
	NPROT0: {0000000b, AP}; NPROT1: {0000000b, EM};
	NPROT2: {0000000b, WP}; NPROT3: {0000000b, RP}

Configuration Write

The Configuration Write command is used to write the nonvolatile Configuration register, which is loaded into the Control register at power-up. The Configuration register can be written using the Configuration Write command without affecting the existing Control register configuration of the PIO and V_{OUT} pins.

CONFIGURATION WRITE	
Command Code	40h
Parameter Byte	Configuration register settings (Table 3)
Conditions, Restrictions	None
Protocol Variations	None
Other Notes	None
Error Conditions (Error Response)	• Request data format error (response error code = 02h) • The Option_flag is set (response error code = 03h)
t1 (Request Frame to Response Frame Delay)	318.6µs to (1 x t_{PROG})
MAC Notes	N/A
Memory Protection Status Affected	None
Secret Protection Status Affected	None

Configuration Read

The Configuration Read command is used to read the nonvolatile Configuration register. This command should be used after completion of the Configuration Write command.

CONFIGURATION READ	
Command Code	41h
Parameter Byte	Any value is accepted.
Conditions, Restrictions	None
Protocol Variations	None
Other Notes	See Table 3 for the format of the data read (CFGD)
Error Conditions (Error Response)	• Request data format error (response error code = 02h) • The Option_flag is set (response error code = 03h)
t1 (Request Frame to Response Frame Delay)	318.6µs to 323.3µs
MAC Notes	N/A
Memory Protection Status Affected	None
Secret Protection Status Affected	None

Control Write

The Control Write command is used to write the volatile Control register, which controls the current settings for the PIO and V_{OUT} pins.

CONTROL WRITE	
Command Code	42h
Parameter Byte	Control register settings (Table 2)
Conditions, Restrictions	None
Protocol Variations	None
Other Notes	None
Error Conditions (Error Response)	• Request data format error (response error code = 02h) • The Option_flag is set (response error code = 03h)
t1 (Request Frame to Response Frame Delay)	318.6μs to (1 x t_{RFAIP})
MAC Notes	N/A
Memory Protection Status Affected	None
Secret Protection Status Affected	None

Control Read

The Control Read command is used to read the volatile Control register. This can be used to read the state of the PIO pin, check for interrupts, and verify if the field strength is high enough to enable V_{OUT}.

CONTROL READ	
Command Code	43h
Parameter Byte	Any value is accepted.
Conditions, Restrictions	None
Protocol Variations	None
Other Notes	See Table 2 for the format of the data read (CNTD)
Error Conditions (Error Response)	• Request data format error (response error code = 02h) • The Option_flag is set (response error code = 03h)
t1 (Request Frame to Response Frame Delay)	318.6μs to 323.3μs
MAC Notes	N/A
Memory Protection Status Affected	None
Secret Protection Status Affected	None

Get 1-Wire ROM ID

The Get 1-Wire ROM ID command is an alternative to creating the ROM ID from the UID. The ROM ID is used for all commands that involve the SHA-256 engine.

GET 1-WIRE ROM ID	
Command Code	A0h
Parameter Byte	N/A
Conditions, Restrictions	None
Protocol Variations	None
Other Notes	For the ROM ID format, see Figure 4. The ROM ID is transmitted with the LS byte (= family code E0h) first.
Error Conditions (Error Response)	• Request data format error (response error code = 02h) • The Option_flag is set (response error code = 03h)
t1 (Request Frame to Response Frame Delay)	318.6μs to 323.3s
MAC Notes	N/A
Memory Protection Status Affected	None
Secret Protection Status Affected	None

Peripheral Transaction

The Peripheral Transaction command is used to operate the I2C port of the MAX66242 in master mode. The command can send a sequence of write bytes, or a sequence of writes followed by reads. In this way, the command can create either an I2C write command, or a command that consists of writes (to set the slave address byte and/or memory read address) immediately followed by reads. The command reports whether written bytes are acknowledged by the addressed I2C slave.

PERIPHERAL TRANSACTION	
Command Code	A2h
Parameter Byte	I2C frame parameters (Table 34)
Conditions, Restrictions	None
Protocol Variations	Depending on the requested I2C activity (NI2CRX = 0), the I2CRXD field may be missing in the response packet.
Other Notes	This command uses additional control bytes NI2CWR (number of bytes to be written on the I2C bus) and NI2CRX (number of bytes to be read from the I2C bus). The data bytes to be written on the I²C bus are referenced as I2CWRD. For the description of NI2CWR and NI2CRX, see Tables 35 and 36. For typical control byte value combinations and their uses, see Table 37.
Error Conditions (Error Response)	• Request data format error (response error code = 02h) • The Option_flag is set (response error code = 03h) • Invalid NI2CWR (either 0 or > 24h) or invalid NI2CRX (> 20h) (response error code = B0h) • There was a problem sending the I2C communication, e.g., SCL or SDA were stuck low (response error code = A0h)
t1 (Request Frame to Response Frame Delay)	318.6μs to 12ms for a normal transaction, depending on the length of I2C communication 318.6μs to 45ms if there is a problem sending I2C communication
MAC Notes	N/A
Memory Protection Status Affected	None
Secret Protection Status Affected	None

Table 34. Parameter Byte Bitmap

BIT 7	BIT 6	BIT 5	BIT 4	BIT 3	BIT 2	BIT 1	BIT 0
X	X	X	SP_BIT	X	X	X	X

Note: *The bits marked as X can be transmitted as 0 or 1 without affecting the command.*

Bit 4: Stop Bit Enable (SP_BIT). If SP_BIT is 1, a STOP bit is generated at the end of a sequence. Also, if NI2CWR is ≥ 2, and NI2CRX ≥ 1, a STOP bit and then a START bit is generated before the final written byte. If SP_BIT is 0, no STOP bit is generated at the end of a sequence. Also, if NI2CWR is ≥ 2, and NI2CRX ≥ 1, a repeated START is generated before the final written byte.

Not sending a STOP bit can prevent another I^{2}C master on the bus from taking control. To exit this “locked” state, perform the “Case 3” transaction in Table 37 with parameter byte = 10h.

Table 35. Control Byte 1 Bitmap

BIT 7	BIT 6	BIT 5	BIT 4	BIT 3	BIT 2	BIT 1	BIT 0
0	0	NI2CWR					

Bits [5:0]: Number of bytes to be written on the I^{2}C bus (NI2CWR). The maximum permissible value is 24h (36 decimal). The minimum permissible value is 1. The size of the I2CWRD data field must match the NI2CWR value. The NI2CWR value determines the size of the I2CACKD field (1 to 5 bytes) in the response packet. See Table 38 for the I2CACKD bit assignment.

Table 36. Control Byte 2 Bitmap

BIT 7	BIT 6	BIT 5	BIT 4	BIT 3	BIT 2	BIT 1	BIT 0
0	0	NI2CRD					

Bits [5:0]: Number of bytes to be read from the I^{2}C bus (NI2CRD). The maximum permissible value is 20h (32 decimal). The minimum permissible value is 0.

Table 37. Typical Control Byte Combinations and Their Uses

CASE #	NI2CWR	NI2CRD	I2CWRD	I2CACKD	TYPICAL USE
1	0	≥ 0	0	0	(not usable)
2	≥ 1 (max 24h)	0	≥ 1	1-5	Typical I^{2}C write access
3	1	≥ 1 (max 20h)	1	1	Typical I^{2}C read access. Write slave address, then do reads.
4	3	≥ 1 (max 20h)	3	1	Combination of case 2 and 3. Write slave address byte, then write memory address, then stop + start or repeated start depending on SP_BIT, then do reads.

Note: *The first write byte is normally the I^{2}C slave address with the LS bit set to 0 (write access). See Case 1. For sequences that write a memory address then do reads, the last write byte is normally the I^{2}C slave address with the LS bit set to 1 (read access). See Case 4.*

Table 38. I2CACKD Bit Assignments

BYTE 1	BYTE 2	BYTE 3	BYTE 4	BYTE 5
ACK bits 1 to 8	ACK bits 9 to 16	ACK bits 17 to 24	ACK bits 25 to 32	ACK bits 33 to 36

BYTE 8 ACK	BYTE 7 ACK	BYTE 6 ACK	BYTE 5 ACK	BYTE 4 ACK	BYTE 3 ACK	BYTE 2 ACK	BYTE 1 ACK
MS Bit							LS Bit

If the I2C slave acknowledges a byte, the ACK bit is reported as 0. Otherwise, the ACK bit is 1. Bits not used read 0. The number of I2CACKD bytes depends on NI2CWR.

Write AFI

The Write AFI command writes the AFI byte.

WRITE AFI	
Command Code	27h
Parameter Byte	AFI value
Conditions, Restrictions	The AFI byte must not be write protected (locked).
Protocol Variations	None
Other Notes	None
Error Conditions (Error Response)	• Request data format error (response error code = 02h) • The Option_flag is set (response error code = 03h) • The AFI is already locked (response error code = 12h)
t1 (Request Frame to Response Frame Delay)	318.6μs to (1 x t_{PROG})
MAC Notes	N/A
Memory Protection Status Affected	None
Secret Protection Status Affected	None

Lock AFI

The Lock AFI command write protects the AFI byte.

LOCK AFI	
Command Code	28h
Parameter Byte	N/A
Conditions, Restrictions	The AFI byte must not be write protected (locked).
Protocol Variations	None
Other Notes	None
Error Conditions (Error Response)	• Request data format error (response error code = 02h) • The Option_flag is set (response error code = 03h) • The AFI is already locked (response error code = 11h)
t1 (Request Frame to Response Frame Delay)	318.6µs to (1 x t_{PROG})
MAC Notes	N/A
Memory Protection Status Affected	None
Secret Protection Status Affected	None

Write DSFID

The Write DSFID command writes the DSFID byte.

WRITE DSFID	
Command Code	29h
Parameter Byte	DSFID value
Conditions, Restrictions	The DSFID byte must not be write protected (locked).
Protocol Variations	None
Other Notes	None
Error Conditions (Error Response)	• Request data format error (response error code = 02h) • The Option_flag is set (response error code = 03h) • The DSFID is already locked (response error code = 12h)
t1 (Request Frame to Response Frame Delay)	318.6µs to (1 x t_{PROG})
MAC Notes	N/A
Memory Protection Status Affected	None
Secret Protection Status Affected	None

Lock DSFID

The Lock DSFID command write protects the AFI byte.

LOCK DSFID	
Command Code	2Ah
Parameter Byte	N/A
Conditions, Restrictions	The DSFID byte must not be write protected (locked).
Protocol Variations	None
Other Notes	None
Error Conditions (Error Response)	• Request data format error (response error code = 02h) • The Option_flag is set (response error code = 03h) • The DSFID is already locked (response error code = 11h)
t1 (Request Frame to Response Frame Delay)	318.6µs to (1 x t_{PROG})
MAC Notes	N/A
Memory Protection Status Affected	None
Secret Protection Status Affected	None

Communication Examples—Memory and Control Function Commands

See Table 39 and Table 40 for the RF communication legend and data direction codes.

Table 39. RF Communication—Legend for Memory and Control Functions

SYMBOL	DESCRIPTION
GSI	Command “Get System Information”, 2Bh
WM	Command “Write Memory”, 55h
RM	Command “Read Memory”, F0h
RSB	Command “Read Single Block”, 20h
RMB	Command “Read Multiple Blocks”, 23h
SP	Command “Set Protection”, C3h
RSTAT	Command “Read Status”, AAh
RWS	Command “Read/Write Scratchpad”, 0Fh
LLS	Command “Load and Lock Secret”, 33h
CLS	Command “Compute and Lock Secret”, 3Ch
CRPM	Command “Compute and Read Page MAC”, A5h
AWMRFS	Command “Authenticated Write Memory RF Setup”, 5Ah
AWMRFE	Command “Authenticated Write Memory RF Execute”, 5Bh
ASPRFS	Command “Authenticated Set Protection RF Setup”, CCh
ASRFE	Command “Authenticated Set Protection RF Execute”, CDh
CFGW	Command “Configuration Write”, 40h
CFGR	Command “Configuration Read”, 41h
CONW	Command “Control Write”, 42h

Table 39. RF Communication—Legend for Memory and Control Functions (continued)

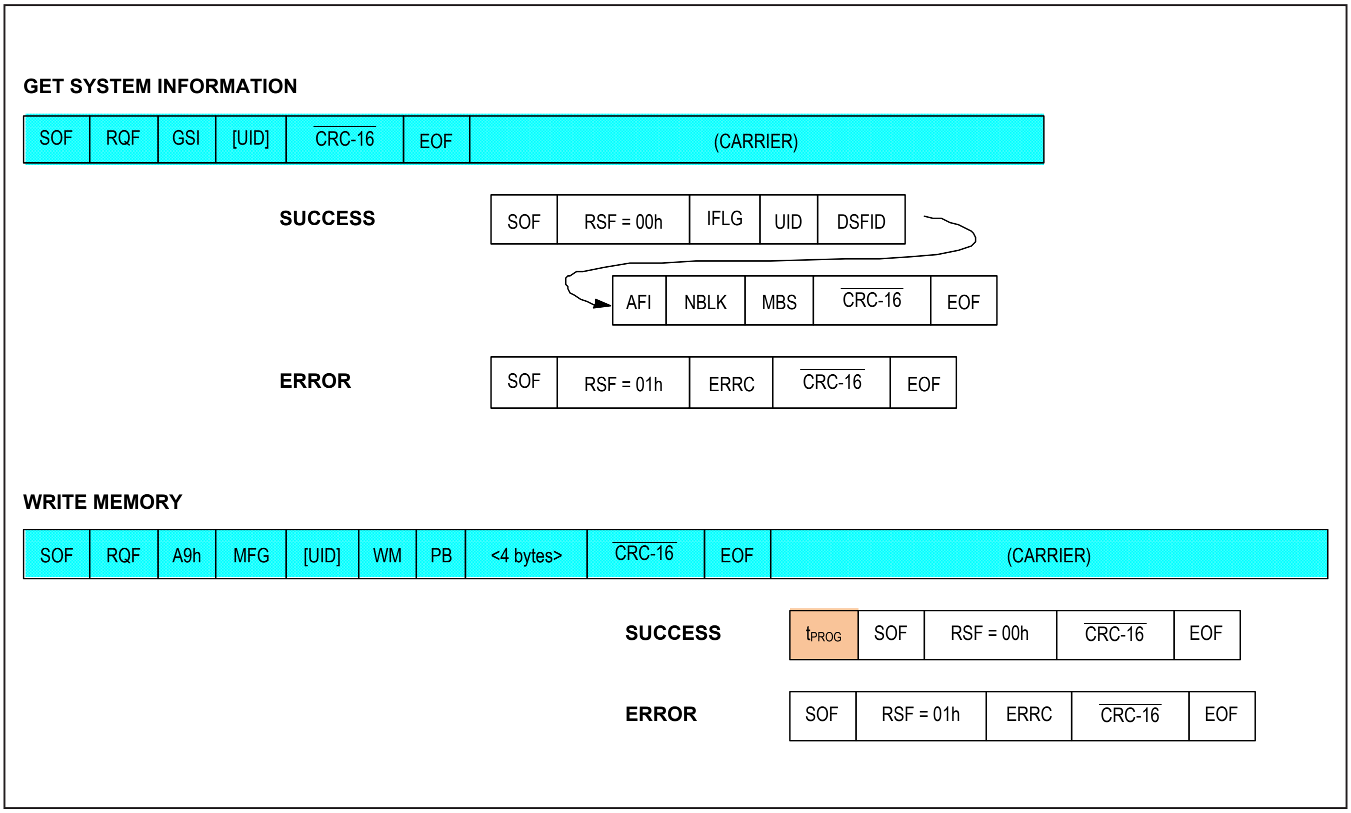
SYMBOL	DESCRIPTION
CONR	Command “Control Read”, 43h
GRID	Command “Get 1-Wire ROM ID”, A0h
PTRA	Command “Peripheral Transaction”, A2h
WAFI	Command “Write AFI”, 27h
LAFI	Command “Lock AFI”, 28h
WDSF	Command “Write DSFID”, 29h
LDSF	Command “Lock DSFID”, 2Ah
SOF	Start of Frame
RQF	Request Flags byte
[UID]	The transponder’s unique 8-byte identification number; could be sent by either the reader or the transponder. The brackets [ ] indicate that the transmission of the UID depends on the request flags (RQF).
$\overline{\text{CRC-16}}$	Transmission of an inverted CRC-16 (2 bytes) generated according to CRC-16-CCITT
EOF	End of Frame
RSF	Response Flags byte (always sent by transponder)
IFLG	Information Flags byte (always sent by transponder)
DSFID	Data Storage Format Identifier byte
AFI	Application Family Identifier byte
NBLK	Number of Blocks byte (transponder memory size indicator)
MBS	Memory Block Size byte (transponder memory block size)
ERRC	Error Code byte (see Table 11)
MFG	Manufacturer Code byte (2Bh)
PB	Parameter Byte (command specific function and bit assignment)
<n bytes>	Transfer of n bytes
NBLOCK	Number of Blocks to Read byte
MAC	32-byte Message Authentication Code (MAC)
CFGD	Configuration Data byte (EEPROM)
CNTD	Control Data byte (volatile)
ROM ID	The transponder’s unique 1-Wire style identification number (8 bytes)
NI2CWR	Number of bytes to be transmitted on the I^{2}C port
I2CWRD	Data bytes to be written on the I^{2}C port (as many bytes as specified by NI2CWR)
NI2CRD	Number of bytes to be read from the I^{2}C port
I2CRDD	Data bytes read from the I^{2}C port (as many bytes as specified by NI2CRX)
I2CACKD	Acknowledge bytes resulting from the I^{2}C port write activity

Table 40. Data Direction and Function Color Codes

READER-TO-TRANSPONDER	TRANSPONDER-TO-READER	SHA COMPUTATION	PROGRAMMING

RF Communication Examples—Memory and Control Functions

The ISO 15693 standard defines three address modes—selected, addressed, and nonaddressed—which are specified through the setting of the Select_flag bit and the Address_flag bit, which are part of the request flags byte RQF (Table 5). The memory and control function commands can be issued in any address mode. To access transponders in the Quiet state, the addressed mode is required. The addressed mode requires that the reader include the transponder's UID in the request.



RF Communication Examples—Memory and Control Functions (continued)

READ MEMORY

SOF	RQF	A9h	MFG	[UID]	RM	PB	$\overline{\text{CRC-16}}$	EOF	(CARRIER)

SUCCESS

SOF	RSF = 00h	<n bytes>	$\overline{\text{CRC-16}}$	EOF

"n" IS A MULTIPLE OF 4, RANGING FROM 4 TO 32, DEPENDING ON THE PARAMETER BYTE.

ERROR

SOF	RSF = 01h	ERRC	$\overline{\text{CRC-16}}$	EOF

READ SINGLE BLOCK

SOF	RQF	RSB	[UID]	PB	$\overline{\text{CRC-16}}$	EOF	(CARRIER)

SUCCESS

SOF	RSF = 00h	<4 bytes>	$\overline{\text{CRC-16}}$	EOF

ERROR

SOF	RSF = 01h	ERRC	$\overline{\text{CRC-16}}$	EOF

READ MULTIPLE BLOCKS

SOF	RQF	RMB	[UID]	PB	NBLOCK	$\overline{\text{CRC-16}}$	EOF	(CARRIER)

SUCCESS

SOF	RSF = 00h	<n x 4 bytes>	$\overline{\text{CRC-16}}$	EOF

"n" IS A MULTIPLE OF 4, RANGING FROM 1 TO 128, DEPENDING ON THE PARAMETER BYTE AND THE NBLOCK BYTE.

ERROR

SOF	RSF = 01h	ERRC	$\overline{\text{CRC-16}}$	EOF

SET PROTECTION

SOF	RQF	A9h	MFG	[UID]	SP	PB	$\overline{\text{CRC-16}}$	EOF	(CARRIER)

SUCCESS

t_{PROG}	SOF	RSF = 00h	$\overline{\text{CRC-16}}$	EOF	

ERROR

SOF	RSF = 01h	ERRC	$\overline{\text{CRC-16}}$	EOF

RF Communication Examples—Memory and Control Functions (continued)

READ STATUS

CASE A: READING PROTECTION BYTES, SUCCESS

SOF	RQF	A9h	MFG	[UID]	RSTAT	PB	$\overline{\text{CRC-16}}$	EOF	(CARRIER)

SUCCESS

SOF	RSF = 00h	<n bytes>	$\overline{\text{CRC-16}}$	EOF

“n” REPRESENTS ALL PROTECTION BYTES STARTING AT PAGE# (SEE PARAMETER BYTE) TO/INCLUDING PAGE 15.

CASE B: READING PERSONALITY BYTES, SUCCESS

SOF	RQF	A9h	MFG	[UID]	RSTAT	PB	$\overline{\text{CRC-16}}$	EOF	(CARRIER)

SUCCESS

SOF	RSF = 00h	<4 bytes>	$\overline{\text{CRC-16}}$	EOF

CASE C: ERROR CONDITION

ERROR

SOF	RSF = 01h	ERRC	$\overline{\text{CRC-16}}$	EOF

READ/WRITE SCRATCHPAD

CASE A: WRITING TO THE SCRATCHPAD, SUCCESS

SOF	RQF	A9h	MFG	[UID]	RWS	PB	<32 bytes>	$\overline{\text{CRC-16}}$	EOF	(CARRIER)

SUCCESS

t_{RFAIP}	SOF	RSF = 00h	$\overline{\text{CRC-16}}$	EOF

CASE B: READING THE SCRATCHPAD, SUCCESS

SOF	RQF	A9h	MFG	[UID]	RWS	PB	$\overline{\text{CRC-16}}$	EOF	(CARRIER)

SUCCESS

SOF	RSF = 00h	<32 bytes>	$\overline{\text{CRC-16}}$	EOF

CASE C: ERROR CONDITION

ERROR

SOF	RSF = 01h	ERRC	$\overline{\text{CRC-16}}$	EOF

LOAD AND LOCK SECRET (NO LOCKING)

SOF	RQF	A9h	MFG	[UID]	LLS	PB	$\overline{\text{CRC-16}}$	EOF	CARRIER

SUCCESS

8 × t_{PROG}	SOF	RSF = 00h	$\overline{\text{CRC-16}}$	EOF

ERROR

SOF	RSF = 01h	ERRC	$\overline{\text{CRC-16}}$	EOF

RF Communication Examples—Memory and Control Functions (continued)

COMPUTE AND LOCK SECRET (NO LOCKING)

SOF	RQF	A9h	MFG	[UID]	CLS	PB	$\overline{\text{CRC-16}}$	EOF	(CARRIER)

SUCCESS

2 × t_{CSHA}	8 × t_{PROG}	SOF	RSF = 00h	$\overline{\text{CRC-16}}$	EOF

ERROR

SOF	RSF = 01h	ERRC	$\overline{\text{CRC-16}}$	EOF

COMPUTE AND READ PAGE MAC

SOF	RQF	A9h	MFG	[UID]	CRPM	PB	$\overline{\text{CRC-16}}$	EOF	(CARRIER)

SUCCESS

2 × t_{CSHA}	SOF	RSF = 00h	MAC	$\overline{\text{CRC-16}}$	EOF

ERROR

SOF	RSF = 01h	ERRC	$\overline{\text{CRC-16}}$	EOF

AUTHENTICATED WRITE MEMORY RF SETUP

SOF	RQF	A9h	MFG	[UID]	AWMRFS	PB	<4 bytes>	$\overline{\text{CRC-16}}$	EOF	(CARRIER)

SUCCESS

t_{CSHA}	SOF	RSF = 00h	$\overline{\text{CRC-16}}$	EOF

ERROR

SOF	RSF = 01h	ERRC	$\overline{\text{CRC-16}}$	EOF

AUTHENTICATED WRITE MEMORY RF EXECUTE

SOF	RQF	A9h	MFG	[UID]	AWMRFE	PB	MAC	$\overline{\text{CRC-16}}$	EOF	(CARRIER)

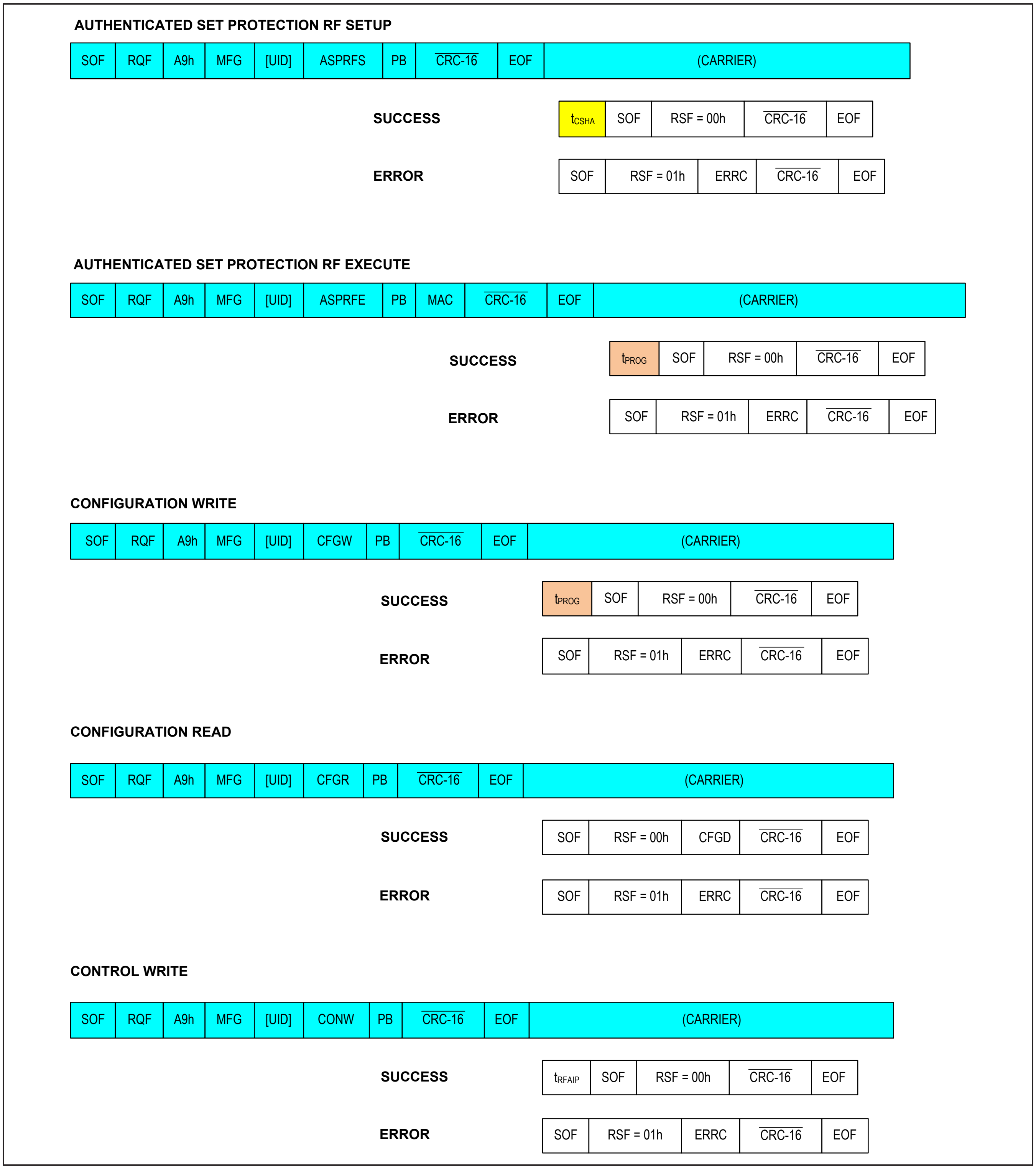
SUCCESS

t_{PROG}	SOF	RSF = 00h	$\overline{\text{CRC-16}}$	EOF

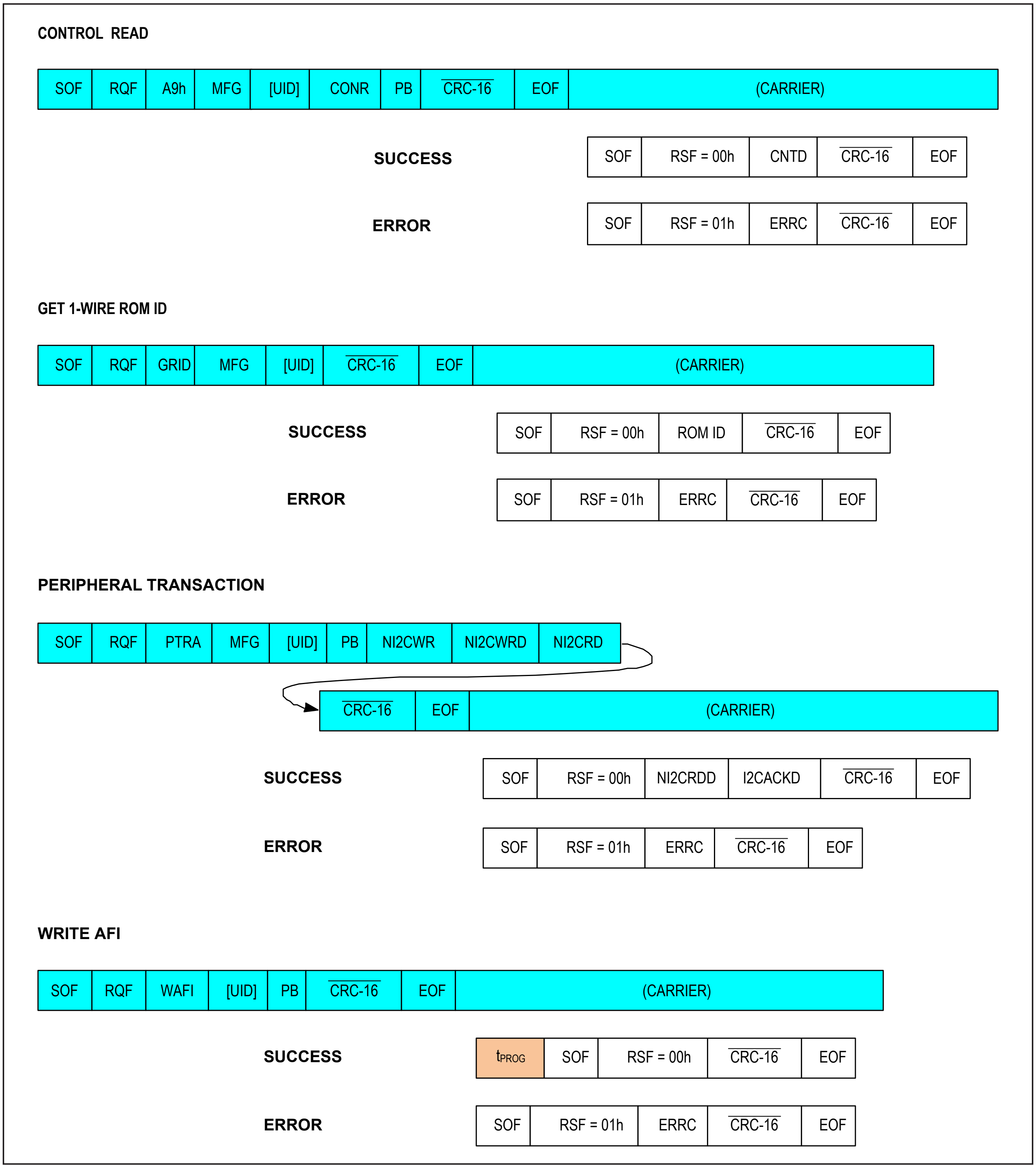
ERROR

SOF	RSF = 01h	ERRC	$\overline{\text{CRC-16}}$	EOF

RF Communication Examples—Memory and Control Functions (continued)


AUTHENTICATED SET PROTECTION RF SETUP
SOF | RQF | A9h | MFG | [UID] | ASPRFS | PB | $\overline{\text{CRC-16}}$ | EOF | (CARRIER)
SUCCESS
t_{CSHA} | SOF | RSF = 00h | $\overline{\text{CRC-16}}$ | EOF
ERROR
SOF | RSF = 01h | ERRC | $\overline{\text{CRC-16}}$ | EOF
AUTHENTICATED SET PROTECTION RF EXECUTE
SOF | RQF | A9h | MFG | [UID] | ASPRFE | PB | MAC | $\overline{\text{CRC-16}}$ | EOF | (CARRIER)
SUCCESS
t_{PROG} | SOF | RSF = 00h | $\overline{\text{CRC-16}}$ | EOF
ERROR
SOF | RSF = 01h | ERRC | $\overline{\text{CRC-16}}$ | EOF
CONFIGURATION WRITE
SOF | RQF | A9h | MFG | [UID] | CFGW | PB | $\overline{\text{CRC-16}}$ | EOF | (CARRIER)
SUCCESS
t_{PROG} | SOF | RSF = 00h | $\overline{\text{CRC-16}}$ | EOF
ERROR
SOF | RSF = 01h | ERRC | $\overline{\text{CRC-16}}$ | EOF
CONFIGURATION READ
SOF | RQF | A9h | MFG | [UID] | CFGR | PB | $\overline{\text{CRC-16}}$ | EOF | (CARRIER)
SUCCESS
SOF | RSF = 00h | CFGD | $\overline{\text{CRC-16}}$ | EOF
ERROR
SOF | RSF = 01h | ERRC | $\overline{\text{CRC-16}}$ | EOF
CONTROL WRITE
SOF | RQF | A9h | MFG | [UID] | CONW | PB | $\overline{\text{CRC-16}}$ | EOF | (CARRIER)
SUCCESS
t_{RFAIP} | SOF | RSF = 00h | $\overline{\text{CRC-16}}$ | EOF
ERROR
SOF | RSF = 01h | ERRC | $\overline{\text{CRC-16}}$ | EOF

RF Communication Examples—Memory and Control Functions (continued)



CONTROL READ

SOF	RQF	A9h	MFG	[UID]	CONR	PB	$\overline{\text{CRC-16}}$	EOF	(CARRIER)

SUCCESS

SOF	RSF = 00h	CNTD	$\overline{\text{CRC-16}}$	EOF

ERROR

SOF	RSF = 01h	ERRC	$\overline{\text{CRC-16}}$	EOF

GET 1-WIRE ROM ID

SOF	RQF	GRID	MFG	[UID]	$\overline{\text{CRC-16}}$	EOF	(CARRIER)

SUCCESS

SOF	RSF = 00h	ROM ID	$\overline{\text{CRC-16}}$	EOF

ERROR

SOF	RSF = 01h	ERRC	$\overline{\text{CRC-16}}$	EOF

PERIPHERAL TRANSACTION

SOF	RQF	PTRA	MFG	[UID]	PB	NI2CWR	NI2CWRD	NI2CRD	$\overline{\text{CRC-16}}$	EOF	(CARRIER)

SUCCESS

SOF	RSF = 00h	NI2CRDD	I2CACKD	$\overline{\text{CRC-16}}$	EOF

ERROR

SOF	RSF = 01h	ERRC	$\overline{\text{CRC-16}}$	EOF

WRITE AFI

SOF	RQF	WAFI	[UID]	PB	$\overline{\text{CRC-16}}$	EOF	(CARRIER)

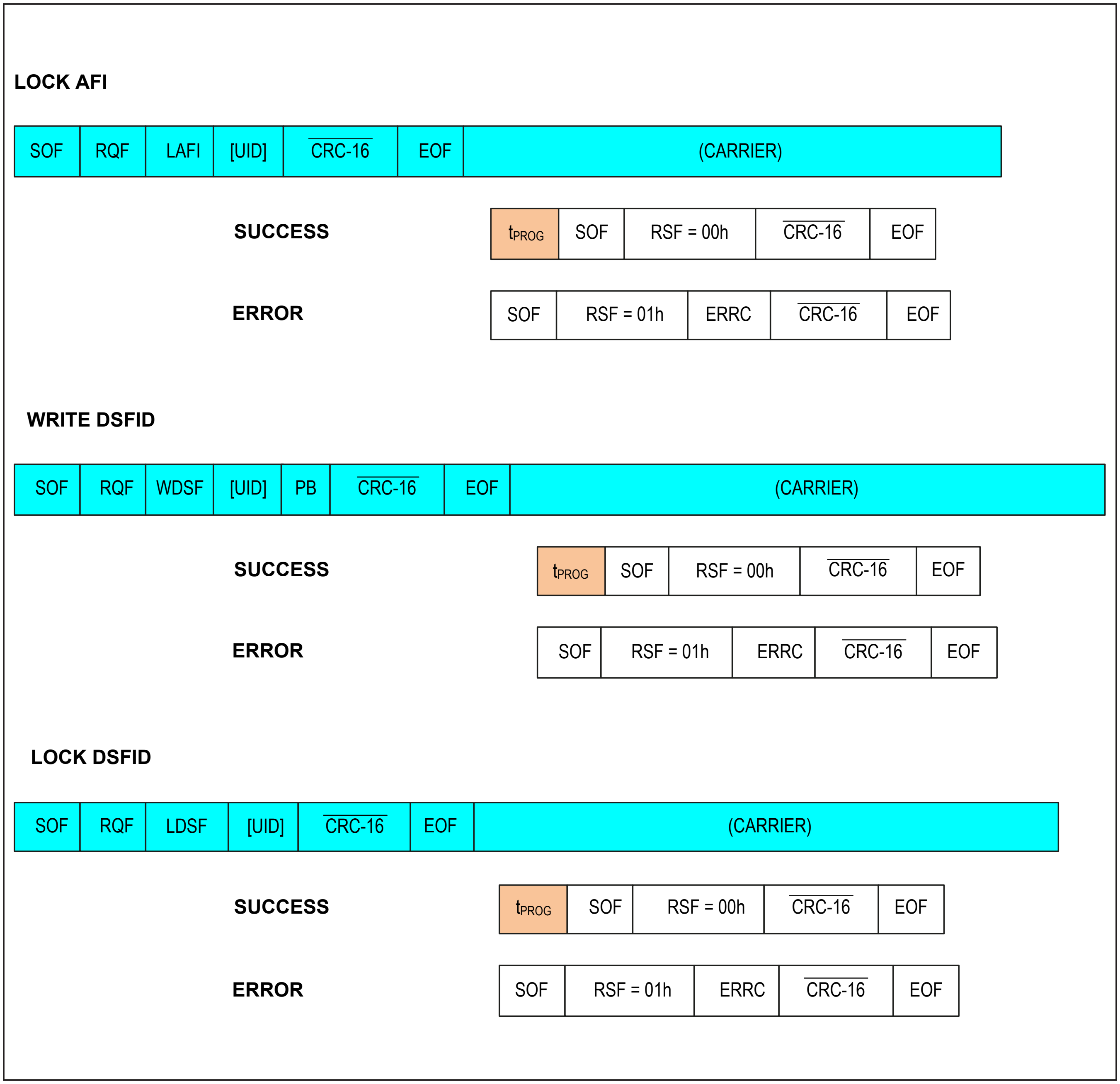
SUCCESS

t_{PROG}	SOF	RSF = 00h	$\overline{\text{CRC-16}}$	EOF

ERROR

SOF	RSF = 01h	ERRC	$\overline{\text{CRC-16}}$	EOF

RF Communication Examples—Memory and Control Functions (continued)



I^{2}C Interface Description

The block diagram in Figure 1 shows the relationships between the major control and memory sections of the MAX66242. The device has six main data components: 16 256-bit pages of user EEPROM, one 256-bit secret, protection-control/status memory, 512-bit SHA-256 engine, 64-bit ROM ID, and a 256-bit scratchpad. Figure 24 shows the applicable commands and the affected data fields.

Memory

The MAX66242 memory consists of three areas: 1) the directly accessible 256-byte address space with the scratchpad, protection status registers, ROM ID, and special function addresses, 2) the indirectly accessible user memory, and 3) the indirectly write-accessible secret memory of 32 bytes.

Figure 25 shows the organization of the directly accessible memory space, which begins at address 00h with the scratchpad. The register section begins at address 40h with the command register, which is followed by the MAC Read/Write Register. The protection status registers begin at address 50h (for memory pages) and 60h (secret). The ROM ID and several other factory programmable registers begin at address 68h. The scratchpad is implemented as volatile SRAM. The address range 50h and higher is nonvolatile.

The directly accessible memory space encompasses three types of memory: read/write, write-only, open read/indirect write, and read-only. To write to or read from the volatile scratchpad, one must begin at address 00h. Writing must take place in block of 4 bytes. The command register is write-only. The protection status registers can be read openly, but require the use of special function commands for writing. The ROM ID, manufacturer ID, and factory byte are read-only.

The EEPROM of the MAX66242 can be programmed using a factory preprogramming service. If this service is used, the Manufacturer ID is different from the 0000h default of unprogrammed parts.

Command Register (40h)

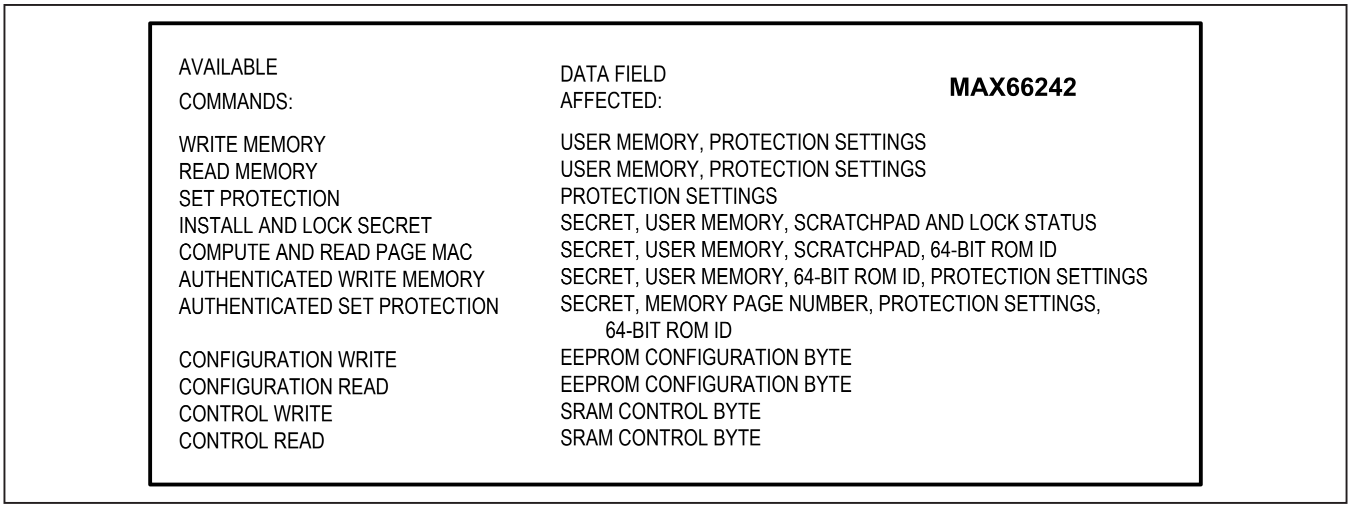
To install the secret, to read from or write to the user memory, or to set the user memory protection, or to compute and read a page MAC, the MAX66242 needs to receive a command from the I^{2}C host. Commands are written one at a time to the Command register. Most commands consist of a command code and a parameter byte. The command code indicates the type of instruction and the position of the read pointer for the next I^{2}C read-access. See the Function Commands section for details.

MAC Read/Write Register (41h)

For authenticated writing (memory, protection), the I^{2}C host must provide a MAC to prove its authenticity to the MAX66242. To verify the MAX66242 authenticity, the Compute and Read Page MAC command delivers a MAC for the host to read. The MAC Read/Write Register is the single address access point for MAC.

Memory Protection Status Registers (50h–5Fh)

Each individual user memory page can be protected in several ways. Protections are activated through the Set Protection command or Authenticated Set Protection command (see the Function Commands section). The Memory Protection Status Registers (Table 41), one for each user memory page, allow the I^{2}C host to verify the protection status. The Memory protection status register at address 50h corresponds to user memory page 0, etc.



MAX66242

AVAILABLE COMMANDS:	DATA FIELD AFFECTED:
WRITE MEMORY	USER MEMORY, PROTECTION SETTINGS
READ MEMORY	USER MEMORY, PROTECTION SETTINGS
SET PROTECTION	PROTECTION SETTINGS
INSTALL AND LOCK SECRET	SECRET, USER MEMORY, SCRATCHPAD AND LOCK STATUS
COMPUTE AND READ PAGE MAC	SECRET, USER MEMORY, SCRATCHPAD, 64-BIT ROM ID
AUTHENTICATED WRITE MEMORY	SECRET, USER MEMORY, 64-BIT ROM ID, PROTECTION SETTINGS
AUTHENTICATED SET PROTECTION	SECRET, MEMORY PAGE NUMBER, PROTECTION SETTINGS, 64-BIT ROM ID
CONFIGURATION WRITE	EEPROM CONFIGURATION BYTE
CONFIGURATION READ	EEPROM CONFIGURATION BYTE
CONTROL WRITE	SRAM CONTROL BYTE
CONTROL READ	SRAM CONTROL BYTE

Figure 24. Commands Overview

ADDRESS RANGE	TYPE	ACCESS	DESCRIPTION
00h–1Fh	SRAM	R/W	Scratchpad
20h–3Fh	—	—	(Reserved)
40h	—	W	Command Register
42h–4Fh	—	—	(Reserved)
50h–5Fh	PROM	R/(W)	Memory Protection Status Registers
61h–67h	—	—	(Reserved)
68h–6Fh	ROM	R	ROM ID, Family Code at Lower Address
70h	ROM	R	Factory Byte
71h–72h	ROM	R	Manufacturer ID
73h–FFh	—	—	(Reserved)

Figure 25. Map of the Directly Accessible Memory Space

Table 41. Memory Page Protection Byte Bitmap

ADDRESS	BIT 7	BIT 6	BIT 5	BIT 4	BIT 3	BIT 2	BIT 1	BIT 0
50h	RP	WP	EM	AP	0	0	0	0
…	…							
5Fh	RP	WP	EM	AP	0	0	0	0

Bit 7: Read Protection (RP). This bit specifies whether the memory page is read protected. If RP is 0 (factory default), the memory page is openly read accessible through the Custom Read Memory command and internally accessible as input to the SHA-256 engine. If RP is 1, the memory page data is only internally accessible. Any read attempt reports FFh for each byte.

Bit 6: Write Protection (WP). This bit specifies whether the memory page is write protected. If WP is 0 (factory default), the memory page is not protected. If WP is 1, the memory page is write protected.

Bit 5: EPROM Emulation Mode (EM). This bit specifies whether the memory page is set up for EPROM emulation mode, where writing is limited to changing bits from 1 to 0. If EM is 0 (factory default), the page can be written normally provided that the page is not write protected. If EM is 1, the EPROM emulation mode is activated provided that the memory page is not write protected (WP = 0).

Bit 4: Authentication Protection (AP). This bit specifies whether memory write access requires host authentication. If AP is 0 (factory default), the memory page is write accessible through the Write Memory and Authenticated Write Memory commands. If AP is 1, the memory page is write accessible only through the Authenticated Write Memory command where the host must know the device secret and deliver a valid MAC for the new data to be accepted.

Note: Once write protection (WP) and read protection (RP) are set to 1, no other protection can be set.

Secret Protection Status Register (60h)

The secret can be write protected. It is read-protected by hardware design. The Secret Protection Status Register (Table 42) allows the I2C host to verify the protection status.

Table 42. Secret Protection Byte Bitmap

ADDRESS	BIT 7	BIT 6	BIT 5	BIT 4	BIT 3	BIT 2	BIT 1	BIT 0
60h	1	WP	0	0	0	0	0	0

Bit 6: Secret Protection (WP). This bit specifies whether the secret is write-protected. If the WP bit is 0 (factory default), the secret is not protected. If the WP bit is 1, the secret is write-protected and its data cannot be changed.

ROM ID (68h–6Fh)

The ROM ID (Figure 4) uniquely identifies each individual MAX66242. The first 8 bits are a 1-Wire family code, which is E0h. The next 28 bits are a unique serial number. The next 20 bits are fixed. The last 8 bits are a cyclic redundancy check (CRC) of the first 56 bits. The family code is stored at the lower address (68h).

Factory Byte (70h)

This byte reads 55h.

Manufacturer ID (71h–72h)

These bytes read 00h unless the device is programmed with customer specific data using the factory preprogramming service.

User Memory

The user memory is organized as 16 pages of 32 bytes each (see Figure 6). A page is divided into 8 page blocks of 32 bits each. The page is the entity for which read/write protection settings apply if activated. The user memory is written in page blocks, one page block at a time. If not read-protected, the memory can be read openly starting at any block of any page. The protocol allows reading multiple page blocks up to the end of a memory page.

Memory and Control Function Commands

The MAX66242 understands 11 function commands that fall into five categories: secret installation, memory access, protection setting, MAC computation, configuration and control setting with verification. The feedback path to the host is controlled by a read pointer, which is set automatically by each function command for the host to efficiently access relevant information. The host processor sends these commands and applicable parameters as strings of one or more bytes using the I2C interface. The I2C protocol requires that each byte be acknowledged by the receiving party to confirm acceptance or not be acknowledged to indicate an error condition (invalid code or parameter) or to end the communication. See the *I2C Interface* section for details of the I2C protocol including acknowledge. The subsequent pages describe the function commands in a concise, table like fashion.

Write Memory

The Write Memory command is used to write a 4-byte block of a memory page.

WRITE MEMORY	
Command Code	55h
Parameter Byte	Page block number, page number (Table 43)
Conditions, Restrictions	None
Other Notes	The new segment data is transmitted in the sequence B0, B1, B2, and B3. Figure 5 shows how these bytes map to the addressed memory page.
Error Conditions (Error Response)	If the memory is write protected or requires authentication, the new data bytes are not acknowledged and the memory write cycle does not take place.
MAC Notes	N/A
I^2C Busy Duration	t_{PROG} counted from the rising SCL edge of the 4th data byte acknowledge bit.
Read Pointer Position	Not affected.
Memory Protection Status Affected	The current protection settings apply.
Secret Protection Status Affected	None

Table 43. Parameter Byte Bitmap

BIT 7	BIT 6	BIT 5	BIT 4	BIT 3	BIT 2	BIT 1	BIT 0
BL#			X	PAGE#			

***Note:** The bit marked as X can be transmitted as 0 or 1 without affecting the command.*

Bits [7:5]: Page Block Number (BL#). These bits specify the block within the selected memory page that is to be written to. Valid page block numbers are 000b (start of memory page) to 111b (end of memory page).

Bits [3:0]: Page Number (PAGE#). These bits specify the memory page to be written to. Valid memory page numbers are 0000b (page 0) to 1111b (page 15).

Read Memory

The Read Memory command is used to read a memory page starting at a specified block.

READ MEMORY	
Command Code	F0h
Parameter Byte	Page block number, page number (Table 44)
Conditions, Restrictions	A repeated start must be used after the parameter byte is written to initiate the read access.
Other Notes	To read an entire memory page, the page block number must be 000b.
Error Conditions (Error Response)	If the memory page is read protected, the device delivers FFh bytes instead of the actual memory data.
MAC Notes	N/A
I^2C Busy Duration	None
Read Pointer Position	Not affected
Memory Protection Status Affected	The current protection settings apply.
Secret Protection Status Affected	None

Table 44. Parameter Byte Bitmap

BIT 7	BIT 6	BIT 5	BIT 4	BIT 3	BIT 2	BIT 1	BIT 0
BL#			0	PAGE#			

Note: *The bit marked as 0 must be transmitted as 0 for the parameter byte to be valid.*

Bits [7:5]: Page Block Number (BL#). These bits specify the block within the selected memory page at which the read begins. Valid page block numbers are 000b (start of memory page) to 111b (last block of memory page).

Bits [3:0]: Page Number (PAGE#). These bits specify the memory page to be read from. Valid memory page numbers are 0000b (page 0) to 1111b (page 15).

Set Protection

The Set Protection command is used to set the protection for an individual memory page.

SET PROTECTION	
Command Code	C3h
Parameter Byte	Page number (Table 45)
Conditions, Restrictions	None.
Other Notes	The new protection settings are specified in the protection byte (Table 46), which is transmitted after the parameter byte. Once set, a protection mode cannot be reset. Write protection invalidates EPROM emulation mode and authentication protection.
Error Conditions (Error Response)	If the page requires authentication, or if both write and read protection are already set, or if the protections are all set to 0 in the protection byte, the protection byte is not acknowledged and the write cycle does not take place.
MAC Notes	N/A
I^2C Busy Duration	1 x t_{PROG} counted from the rising SCL edge of the protection byte acknowledge bit.
Read Pointer Position	Memory protection status register according to the parameter byte (PAGE# + 50h). Undefined if the protection byte is not acknowledged.
Memory Protection Status Affected	The current protection settings apply, and protections are updated as specified in the protection byte.
Secret Protection Status Affected	None

Table 45. Parameter Byte Bitmap

BIT 7	BIT 6	BIT 5	BIT 4	BIT 3	BIT 2	BIT 1	BIT 0
X	X	X	X	PAGE#			

Note: *Bits marked as X can be transmitted as 0 or 1 without affecting the command.*

Bits [3:0]: Page Number (PAGE #). These bits specify the memory page for which the protection is to be set. Valid memory page numbers are 0000b (page 0) to 1111b (page 15).

Table 46. Protection Byte Bitmap

BIT 7	BIT 6	BIT 5	BIT 4	BIT 3	BIT 2	BIT 1	BIT 0
RP	WP	EM	AP	0	X	X	X

Note: *The bit marked as 0 must be transmitted as 0 for the protection byte to be valid. Bits marked as X can be transmitted as 0 or 1 without affecting the command.*

Bit 7: Read Protection (RP). This bit specifies whether the memory page is to be read protected. If RP is 0 (factory default), the memory page will not be read protected. If RP is 1, the memory page becomes read protected and any read attempt returns FFh. The memory data is always internally accessible as input to the SHA-256 engine.

Bit 6: Write Protection (WP). This bit specifies whether the memory page is to be write protected. If WP is 0 (factory default), the memory page will not be write protected. If WP is 1, the memory page becomes write protected.

Bit 5: EPROM Emulation Mode (EM). This bit specifies whether the memory page is to be set up for EPROM emulation mode, where writing is limited to changing bits from 1 to 0. If EM is 0 and WP is 0 (factory default), the memory page will not be set up for EPROM emulation mode. If EM is 1 and WP is 0, the memory page becomes set up for EPROM emulation mode. Note: Normally, the affected memory page first needs to be programmed to FFh.

Bit 4: Authentication Protection (AP). This bit specifies whether memory write access requires host authentication. If AP is 0 and WP is 0 (factory default), the memory page will not be authentication protected, and the page will be write accessible with and without host authentication. If AP is 1 and WP is 0, the memory page becomes authentication protected, and the page will be write accessible only with host authentication

Install and Lock Secret

The Install and Lock Secret command is used to load a predefined secret or to compute a device-specific secret. A computed secret is recommended; to increase the security level, one can compute a new secret using this command multiple times, each time with a different partial secret written to the scratchpad. When loading a predefined secret, this command takes the data in the scratchpad and copies it to the secret memory. When computing the secret, this command uses the scratchpad content together with the data from a selected memory page, the secret already in the device, the device's 64-bit ROM ID (Figure 4), the number of the selected memory page, the manufacturer ID and padding as input for a MAC computation. The resulting MAC is then written to the secret. The computation of the secret involves two 512-bit message blocks and consequently two cycles of the SHA-256 engine. The secret can additionally be write protected. Write protection cannot be reset. The scratchpad should be overwritten with dummy data after this command is completed to avoid exposing secret data.

INSTALL AND LOCK SECRET	
Command Code	33h
Parameter Byte	Locking enable, load/compute, memory page selection for secret computation (Table 47)
Conditions, Restrictions	The scratchpad should be written to a known value before executing this command.
Other Notes	Loading the secret copies the entire scratchpad to the secret memory. See Table 23 for the mapping of scratchpad to secret.
Error Conditions (Error Response)	If the secret is already locked or the parameter byte is invalid, the parameter byte is not acknowledged, and no MAC computation or write cycle takes place.
MAC Notes	Computed secret only. See Table 48 for the message input that is used for computing the MAC and Table 27 for the mapping of the MAC to the secret.
I^2C Busy Duration	Loaded secret, not locked: 8 x t_{PROG} Loaded secret, locked: 9 x t_{PROG} Computed secret, not locked: 2 × t_{CSHA} + 8 x t_{PROG} Computed secret: 2 × t_{CSHA} + 9 x t_{PROG} The duration is counted from the rising SCL edge of the parameter byte acknowledge bit.
Read Pointer Position	Not affected
Memory Protection Status Affected	None
Secret Protection Status Affected	The current protection setting applies plus the protection is updated as specified in the parameter byte.

Table 47. Parameter Byte Bitmap

BIT 7	BIT 6	BIT 5	BIT 4	BIT 3	BIT 2	BIT 1	BIT 0
LE		L/C	0	PAGE#			

Note: *The bit marked as 0 must be transmitted as 0 for the parameter byte to be valid.*

Bits [7:6]: Locking Enable (LE). These bits specify whether the secret is to be automatically write protected (locked) after it is copied to the secret memory. If LE is 00b or 11b, the secret will not be write protected. If LE is 01b or 10b, the secret will be write protected.

Bit 5: Load/Compute (L/C). This bit specifies whether the secret is loaded from the scratchpad or computed. If L/C is 0, the scratchpad content is copied to the secret memory. If L/C is 1, a secret is computed and copied to the secret memory.

Bits [3:0]: Page Number (PAGE#). These bits specify the memory page to be used for the computation of the secret. These bits are relevant only if L/C = 1 (computed secret). Valid memory page numbers are 0000b (page 0) to 1111b (page 15).

Table 48. SHA-256 Engine Input Data for Install and Lock Secret, L/C = 1

Message, First Block

M0^1[31:24] = (PP+3)	M0^1[23:16] = (PP+2)	M0^1[15:8] = (PP+1)	M0^1[7:0] = (PP+0)
M1^1[31:24] = (PP+7)	M1^1[23:16] = (PP+6)	M1^1[15:8] = (PP+5)	M1^1[7:0] = (PP+4)
M2^1[31:24] = (PP+11)	M2^1[23:16] = (PP+10)	M2^1[15:8] = (PP+9)	M2^1[7:0] = (PP+8)
M3^1[31:24] = (PP+15)	M3^1[23:16] = (PP+14)	M3^1[15:8] = (PP+13)	M3^1[7:0] = (PP+12)
M4^1[31:24] = (PP+19)	M4^1[23:16] = (PP+18)	M4^1[15:8] = (PP+17)	M4^1[7:0] = (PP+16)
M5^1[31:24] = (PP+23)	M5^1[23:16] = (PP+22)	M5^1[15:8] = (PP+21)	M5^1[7:0] = (PP+20)
M6^1[31:24] = (PP+27)	M6^1[23:16] = (PP+26)	M6^1[15:8] = (PP+25)	M6^1[7:0] = (PP+24)
M7^1[31:24] = (PP+31)	M7^1[23:16] = (PP+30)	M7^1[15:8] = (PP+29)	M7^1[7:0] = (PP+28)
M8^1[31:24] = SP+3	M8^1[23:16] = SP+2	M8^1[15:8] = SP+1	M8^1[7:0] = SP+0
M9^1[31:24] = SP+7	M9^1[23:16] = SP+6	M9^1[15:8] = SP+5	M9^1[7:0] = SP+4
M10^1[31:24] = SP+11	M10^1[23:16] = SP+10	M10^1[15:8] = SP+9	M10^1[7:0] = SP+8
M11^1[31:24] = SP+15	M11^1[23:16] = SP+14	M11^1[15:8] = SP+13	M11^1[7:0] = SP+12
M12^1[31:24] = SP+19	M12^1[23:16] = SP+18	M12^1[15:8] = SP+17	M12^1[7:0] = SP+16
M13^1[31:24] = SP+23	M13^1[23:16] = SP+22	M13^1[15:8] = SP+21	M13^1[7:0] = SP+20
M14^1[31:24] = SP+27	M14^1[23:16] = SP+26	M14^1[15:8] = SP+25	M14^1[7:0] = SP+24
M15^1[31:24] = SP+31	M15^1[23:16] = SP+30	M15^1[15:8] = SP+29	M15^1[7:0] = SP+28

Table 48. SHA-256 Engine Input Data for Install and Lock Secret, L/C = 1 (continued)

Message, Second Block

M0^2[31:24] = (SS+3)	M0^2[23:16] = (SS+2)	M0^2[15:8] = (SS+1)	M0^2[7:0] = (SS+0)
M1^2[31:24] = (SS+7)	M1^2[23:16] = (SS+6)	M1^2[15:8] = (SS+5)	M1^2[7:0] = (SS+4)
M2^2[31:24] = (SS+11)	M2^2[23:16] = (SS+10)	M2^2[15:8] = (SS+9)	M2^2[7:0] = (SS+8)
M3^2[31:24] = (SS+15)	M3^2[23:16] = (SS+14)	M3^2[15:8] = (SS+13)	M3^2[7:0] = (SS+12)
M4^2[31:24] = (SS+19)	M4^2[23:16] = (SS+18)	M4^2[15:8] = (SS+17)	M4^2[7:0] = (SS+16)
M5^2[31:24] = (SS+23)	M5^2[23:16] = (SS+22)	M5^2[15:8] = (SS+21)	M5^2[7:0] = (SS+20)
M6^2[31:24] = (SS+27)	M6^2[23:16] = (SS+26)	M6^2[15:8] = (SS+25)	M6^2[7:0] = (SS+24)
M7^2[31:24] = (SS+31)	M7^2[23:16] = (SS+30)	M7^2[15:8] = (SS+29)	M7^2[7:0] = (SS+28)
M8^2[31:24] = (RN+3)	M8^2[23:16] = (RN+2)	M8^2[15:8] = (RN+1)	M8^2[7:0] = (RN+0)
M9^2[31:24] = (RN+7)	M9^2[23:16] = (RN+6)	M9^2[15:8] = (RN+5)	M9^2[7:0] = (RN+4)
M10^2[31:24] = **FFh**	M10^2[23:16] = (PAGE#)	M10^2[15:8] = MAN_ID_H	M10^2[7:0] = MAN_ID_L
M11^2[31:24] = 00h	M11^2[23:16] = 00h	M11^2[15:8] = 00h	M11^2[7:0] = 00h
M12^2[31:24] = 00h	M12^2[23:16] = 00h	M12^2[15:8] = 00h	M12^2[7:0] = 00h
M13^2[31:24] = 00h	M13^2[23:16] = 00h	M13^2[15:8] = 00h	M13^2[7:0] = 80h
M14^2[31:24] = 00h	M14^2[23:16] = 00h	M14^2[15:8] = 00h	M14^2[7:0] = 00h
M15^2[31:24] = 00h	M15^2[23:16] = 00h	M15^2[15:8] = 03h	M15^2[7:0] = B8h

Legend:

Mt	Input buffer of SHA engine; 0 ≤ t ≤ 15; 32-bit words.
(PP+N)	Byte N of selected Memory Page; 0 ≤ N ≤ 31.
SP+N	Byte N of the scratchpad, 0 ≤ N ≤ 31.
(SS+N)	Byte N of Secret; 0 ≤ N ≤ 31.
(RN+N)	Byte N of ROM ID; 0 ≤ N ≤ 7. RN+0 corresponds to the family code.
(PAGE#)	Page number as in the parameter byte, padded with 0000b in the upper bits.
MAN_ID_L MAN_ID_H	Manufacturer ID. The value is 0000h for parts that are not factory preprogrammed.

Compute and Read Page MAC

The Compute and Read Page MAC command is used to authenticate the MAX66242 to the I2C host. The host computes the MAC from the same data and the expected secret. If both MACs are identical, the device is confirmed authentic within the application. This command uses the scratchpad content as a challenge together with the data from a selected memory page, the secret, the device's 64-bit ROM ID (Figure 4), the number of the selected memory page, the manufacturer ID, and padding as input for a MAC computation. The computation of the MAC involves two 512-bit message blocks and consequently two cycles of the SHA-256 engine. Optionally, the ROM ID can be replaced by FFh bytes, which makes the MAC result device independent (anonymous). After the computation is completed, the I2C host accesses the MAX66242 in read mode to obtain the MAC for verification.

Compute and Read Page MAC	
Command Code	A5h
Parameter Byte	Anonymous indicator; page number (Table 49)
Conditions, Restrictions	The scratchpad should be written to a known value before executing this command. The MAC must be read immediately after MAC is computed.
Other Notes	The scratchpad content is used as a "challenge." The computed MAC is read from MAC Read/Write register.
Error Conditions (Error Response)	If the parameter byte is not valid, the MAC computation does not take place.
MAC Notes	See Table 26 for the message input that is used for computing the MAC. See Table 29 for the MAC byte transmission sequence.
I2C Busy Duration	2 × t_{CSHA} counted from the rising SCL edge of the parameter byte acknowledge bit
Read Pointer Position	MAC Read/Write register
Memory Protection Status Affected	None
Secret Protection Status Affected	None

Table 49. Parameter Byte Bitmap

BIT 7	BIT 6	BIT 5	BIT 4	BIT 3	BIT 2	BIT 1	BIT 0
ANON			0	PAGE#			

Note: *The bit marked as 0 must be transmitted as 0 for the parameter byte to be valid.*

Bits [7:5]: Anonymous Indicator (ANON). These bits specify whether the device's ROM ID is to be used for the MAC computation. If ANON is 000, the ROM ID is used. If ANON is 111b, the ROM ID is replaced with FFh bytes. All other codes are invalid.

Bits [3:0]: Page Number (PAGE#). These bits specify the memory page to be used for the MAC computation. Valid memory page numbers are 0000b (page 0) to 1111b (page 15).

Authenticated Write Memory

The Authenticated Write Memory command is used to program a 4-byte block of an authentication protected memory page. The I2C host must provide a MAC that is based on the device's secret and other data elements.

AUTHENTICATED WRITE MEMORY	
Command Code	5Ah
Parameter Byte	Page block number, page number (Table 50)
Conditions, Restrictions	None
Other Notes	The new segment data is transmitted in the sequence B0, B1, B2, and B3. Figure 5 shows how these bytes map to the addressed memory page. This command also works on pages that are not authentication protected.
Error Conditions (Error Response)	If the memory is write protected, the new data bytes are not acknowledged and the MAC computation does not take place. If the MAC provided in the second step is not valid, the memory write cycle does not take place.
MAC Notes	See Table 31 for the message input that is used for computing the MAC. See Table 29 for the MAC byte transmission sequence.
I2C Busy Duration	**Issuing the command:** 1 × t_{CSHA} counted from the rising SCL edge of the 4th data byte acknowledge bit. **Providing the MAC:** 1 x t_{PROG} counted from the rising SCL edge of the last MAC byte acknowledge bit.
Read Pointer Position	Not affected
Memory Protection Status Affected	The current protection settings apply.
Secret Protection Status Affected	None

Table 50. Parameter Byte Bitmap

BIT 7	BIT 6	BIT 5	BIT 4	BIT 3	BIT 2	BIT 1	BIT 0
BL#			0	PAGE#			

Note: *The bit marked as 0 must be transmitted as 0 for the parameter byte to be valid.*

Bits [7:5]: Page Block Number (BL#). These bits specify the block within the selected memory page that is to be written to. Valid page block numbers are 000b (start of memory page) to 111b (end of memory page).

Bits [3:0]: Page Number (PAGE#). These bits specify the memory page to be written to. Valid memory page numbers are 0000b (page 0) to 1111b (page 15).

Authenticated Set Protection

The Authenticated Set Protection command is set the protection for an individual memory page that is already authentication protected. The parameter byte specifies the memory page number for which the protection is to be modified and the desired protection modes. Once set, a protection cannot be reset. To authenticate itself to the MAX66242, the I²C host must provide a MAC that is based on the device's secret and other data elements.

AUTHENTICATED SET PROTECTION	
Command Code	CCh
Parameter Byte	Page selection (Table 51)
Conditions, Restrictions	None
Other Notes	The new protection settings are specified in the protection byte (Table 52), which is transmitted after the parameter byte. Once set, a protection mode cannot be reset. Write protection invalidates EPROM emulation mode and authentication protection. This command also works on pages that are not authentication protected.
Error Conditions (Error Response)	If both write and read protection are already set, or if the protections are all set to 0 in the protection byte, the protection byte is not acknowledged and the MAC computation does not take place. If the MAC provided in the second step is not valid, the memory write cycle does not take place.
MAC Notes	See Table 33 for the message input that is used for computing the MAC. See Table 29 for the MAC byte transmission sequence.
I²C Busy Duration	**Issuing the command:** 1 × t_{CSHA} counted from the rising SCL edge of the protection byte acknowledge bit. **Providing the MAC:** 1 x t_{PROG} counted from the rising SCL edge of the last MAC byte acknowledge bit.
Read Pointer Position	Memory protection status register according to the parameter byte (PAGE# + 50h). Undefined if the protection byte is not acknowledged.
Memory Protection Status Affected	The current protection settings apply, and protections are updated as specified in the protection byte.
Secret Protection Status Affected	None

Table 51. Parameter Byte Bitmap

BIT 7	BIT 6	BIT 5	BIT 4	BIT 3	BIT 2	BIT 1	BIT 0
X	X	X	0	PAGE#			

Note: *Bits marked as X can be transmitted as 0 or 1 without affecting the command. The bit marked as 0 must be transmitted as 0 for the parameter byte to be valid.*

Bits [3:0]: Page Number (PAGE #). These bits specify the memory page number for which the protection is to be set. Valid memory page numbers are 0000b (page 0) to 1111b (page 15).

Table 52. Protection Byte Bitmap

BIT 7	BIT 6	BIT 5	BIT 4	BIT 3	BIT 2	BIT 1	BIT 0
RP	WP	EM	AP	0	X	X	X

Note: *The bit marked as 0 must be transmitted as 0 for the protection byte to be valid. Bits marked as X can be transmitted as 0 or 1 without affecting the command.*

Bit 7: Read Protection (RP). This bit specifies whether the memory page is to be read protected. If RP is 0 (factory default), the memory page will not be read protected. If RP is 1, the memory page data becomes read protected and any read attempt returns FFh. The memory data is always internally accessible as input to the SHA-256 engine.

Bit 6: Write Protection (WP). This bit specifies whether the memory page is to be write protected. If WP is 0 (factory default), the memory page will not be write protected. If WP is 1, the memory page becomes write protected.

Bit 5: EPROM Emulation Mode (EM). This bit specifies whether the memory page is to be set up for EPROM emulation mode, where writing is limited to changing bits from 1 to 0. If EM is 0 and WP is 0 (factory default), the memory page will not be set up for EPROM emulation mode. If EM is 1 and WP is 0, the memory page becomes set up for EPROM emulation mode. Note: Normally, the affected memory page first needs to be programmed to FFh.

Bit 4: Authentication Protection (AP). This bit specifies whether memory write access requires host authentication. If AP is 0 and WP is 0 (factory default), the memory page will not be authentication protected, and the page will be write accessible with and without host authentication. If AP is 1and WP is 0, the memory page becomes authentication protected, and the page will be write accessible only with host authentication

Configuration Write

The Configuration Write command is used to write the nonvolatile Configuration register, which is loaded into the Control register at power-up. The Configuration register can be written using the Configuration Write command without affecting the existing Control register configuration of the PIO and V_{OUT} pins.

CONFIGURATION WRITE	
Command Code	40h
Parameter Byte	Configuration register settings (Table 3)
Conditions, Restrictions	None
Other Notes	None
Error Conditions (Error Response)	None
MAC Notes	N/A
I2C Busy Duration	1 x t_{PROG} counted from the rising SCL edge of the parameter byte acknowledge bit.
Read Pointer Position	Not affected
Memory Protection Status Affected	None
Secret Protection Status Affected	None

Configuration Read

The Configuration Read command is used to read the nonvolatile Configuration register. This command should be used after completion of the Configuration Write command.

CONFIGURATION READ	
Command Code	41h
Parameter Byte	Any value is accepted.
Conditions, Restrictions	A repeated start must be used after the parameter byte is written to initiate the read access.
Other Notes	See Table 3 for the format of the data read (CFGD)
Error Conditions (Error Response)	None
MAC Notes	N/A
I^2C Busy Duration	None
Read Pointer Position	Not affected
Memory Protection Status Affected	None
Secret Protection Status Affected	None

Control Write

The Control Write command is used to write the volatile Control register, which controls the current settings for the PIO and V_{OUT} pins.

CONTROL WRITE	
Command Code	42h
Parameter Byte	Control register settings (Table 2)
Conditions, Restrictions	None
Other Notes	None
Error Conditions (Error Response)	None
MAC Notes	N/A
I^2C Busy Duration	None
Read Pointer Position	Not affected
Memory Protection Status Affected	None
Secret Protection Status Affected	None

Control Read

The Control Read command is used to read the volatile Control register. This can be used to read the state of the PIO pin, check for interrupts, and verify if the field strength is high enough to enable V_{OUT}.

Control Read	
Command Code	43h
Parameter Byte	Any value is accepted.
Conditions, Restrictions	A repeated start must be used after the parameter byte is written to initiate the read access.
Other Notes	See Table 2 for the format of the data read (CNTD)
Error Conditions (Error Response)	None
MAC Notes	N/A
I^{2}C Busy Duration	None
Read Pointer Position	Not affected
Memory Protection Status Affected	None
Secret Protection Status Affected	None

I^{2}C Interface

General Characteristics

The I^{2}C 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 I^{2}C bus can be transferred at rates of up to 100kbps in standard mode and up to 400kbps in fast mode. The MAX66242 works in both modes.

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 or I^{2}C host. 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 26). 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 MAX66242 responds is shown in Figure 27. 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 0, subsequent data flows from master to slave (write access); when set to 1, data flows from slave to master (read access).

I^{2}C Definitions

The following terminology is commonly used to describe I^{2}C data transfers. The timing references are defined in Figure 28.

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 28). 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 28) 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.

Acknowledged by Slave: A slave device, when addressed, is usually obliged to generate an acknowledge after the receipt of each byte. The master must generate the clock pulse for each acknowledge bit. A slave that acknowledges must pull down the SDA line during the acknowledge clock pulse so that it remains stable low during the high period of this clock pulse. Setup and hold times $t_{SU:DAT}$ and $t_{HD:DAT}$ must be taken into account.

Acknowledged by Master: To continue reading from a slave, the master is obliged to generate an acknowledge after the receipt of each byte. The master must generate the clock pulse for each acknowledge bit. A master that acknowledges must pull down the SDA line during the acknowledge clock pulse so that it remains stable low during the high period of this clock pulse. Setup and hold times $t_{SU:DAT}$ before the rising edge of SCL and $t_{HD:DAT}$ after the falling edge of SCL must be taken into account.

Not Acknowledged by Slave: A slave device may be unable to receive or transmit data, for example, because it is busy performing a real-time function such as MAC computation or EEPROM write cycle. In this case, the slave does not acknowledge its slave address and leaves the SDA line high. A slave that is ready to communicate acknowledges at least its slave address. However, some time later the slave may refuse to accept data, possibly because of an invalid command code or an error condition. In this case, the slave device does not acknowledge any of the bytes that it refuses and leaves SDA high. In either case, after a slave has failed to acknowledge, the master first should 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. 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.

Read and Write

To write to the MAX66242, the master must access the device in write access mode, i.e., the slave address must be sent with the direction bit set to 0. The next byte to be sent in write access mode is an address byte to select the register or memory address to be written to or to set the address for a subsequent read access (dummy write). To read from the MAX66242, the master must access the device in read access mode, i.e., the slave address must be sent with the direction bit set to 1. The read address is determined either from a preceding write access or implied from a function command.

The MAX66242 has different types of memory. Some areas allow unrestricted read/write access [R/W], others are write-only [W], or read-only [R]. The Memory Protection Status Registers and Secret Protection Status Register are writable through special commands rather than standard I^{2}C write access [R/(W)]. As a consequence, the read and write behavior is address dependent. Figure 29 shows details.

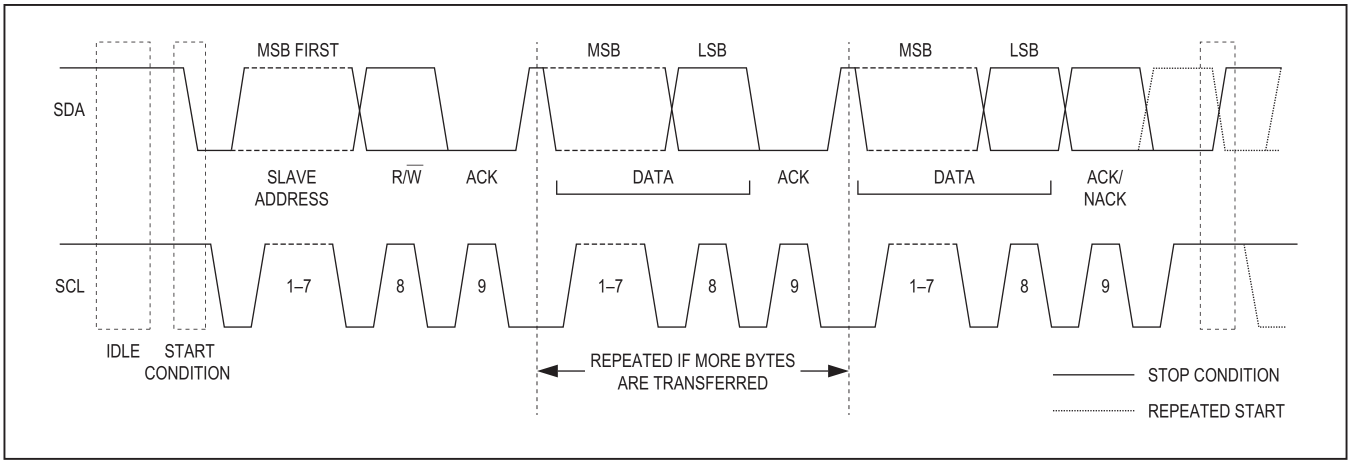


Figure 26. I2C Protocol Overview

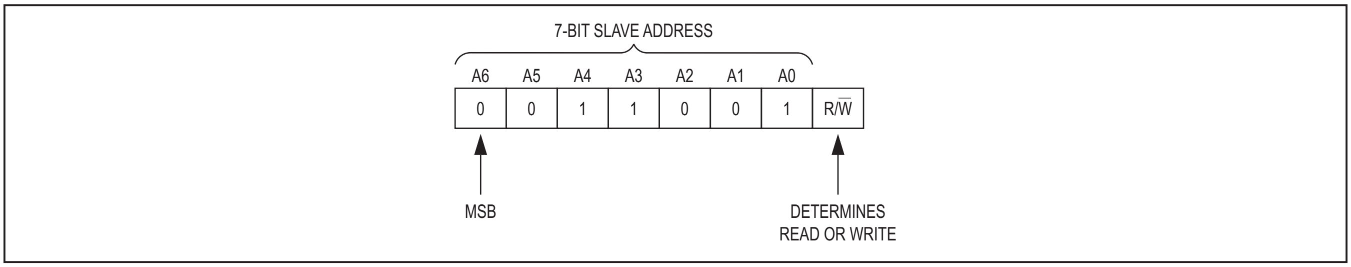
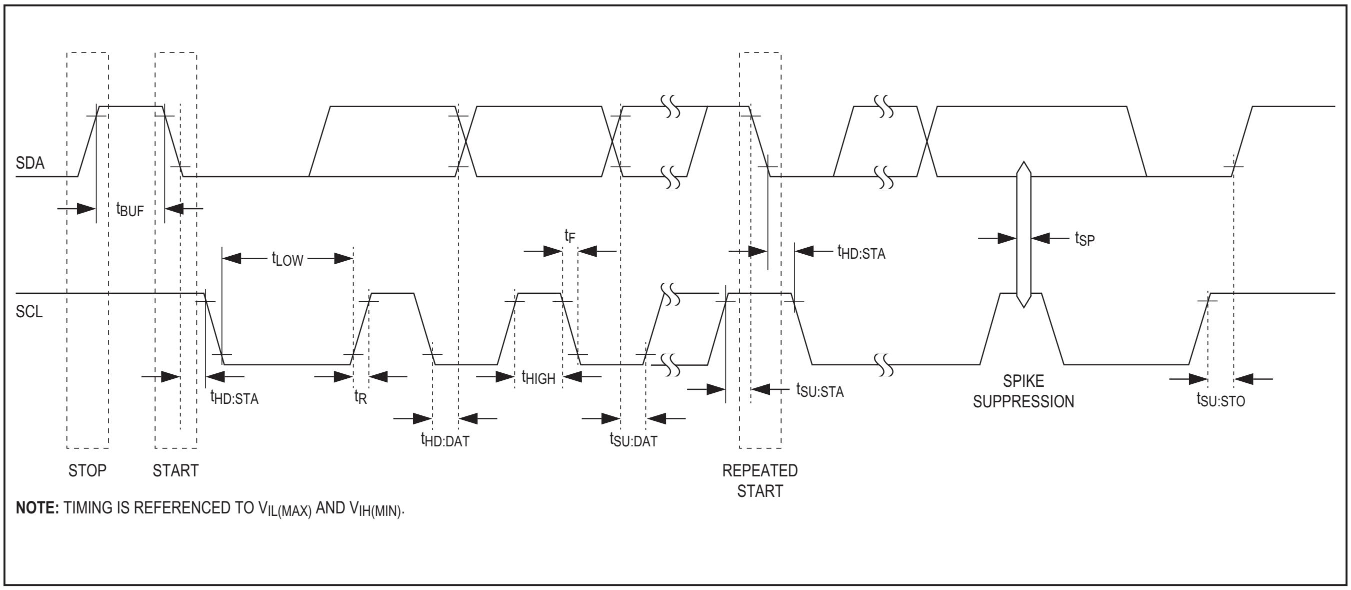


Figure 27. MAX66242 Slave Address



NOTE: TIMING IS REFERENCED TO $V_{IL(MAX)}$ AND $V_{IH(MIN)}$.

Figure 28. I2C Timing Diagram

ADDRESS RANGE	ACCESS	READ/WRITE BEHAVIOR	NOTES
00h–1Fh	R/W	Type 1	Scratchpad
20h–3Eh	—	Type 2	Reserved. Data written is not stored. Data read is indeterminate.
3Fh	—	—	Reserved. Data written is not stored. Data read is indeterminate. Address does not increment.
40h	W	Type 3	Command Register
42h–4Fh	—	Type 2	Reserved. Data written is not stored. Data read is indeterminate.
50h–5Fh	R/(W)	Type 2	Memory Protection Status Registers
61h–67h	—	Type 2	Reserved. Data written is not stored. Data read is indeterminate.
68h–6Fh	R	Type 2	ROM ID, Family Code at Lower Address
70h	R	Type 2	Factory Byte
71h–72h	R	Type 2	Manufacturer ID
73h–FFh	—	Type 2	Reserved. Data written is not stored. Data read is indeterminate.

Figure 29. Address-Specific Read and Write Behavior

Type 1 Behavior

The common I2C address auto-increment applies. Data must be written and read starting at address 00h. Data is written in 4-byte blocks.

Type 2 Behavior

The common I2C random access read/write protocol with data acknowledge applies, but data bytes are discarded. Write mode access is used to set the address for a subsequent read access (dummy write); the address increments after a data byte has been acknowledged. When accessed in read mode, the address increments after a byte is transmitted.

Type 3 Behavior

This behavior applies to the command register, the address to which commands and parameter bytes and command specific data are written, e.g., to activate the SHA engine or write to the user memory. When accessed in write mode, the address does not increment. The subsequent read position is implied by the command code that the master writes.

Type 4 Behavior

This behavior applies to the Memory/MAC Read/Write register. When accessed in read mode or write mode, the address does not increment. If the MAX66242 is not busy, any data written to this address is acknowledged.

I2C Communication Examples

See Table 53 and Table 54 for the I2C communication legend and data direction color codes.

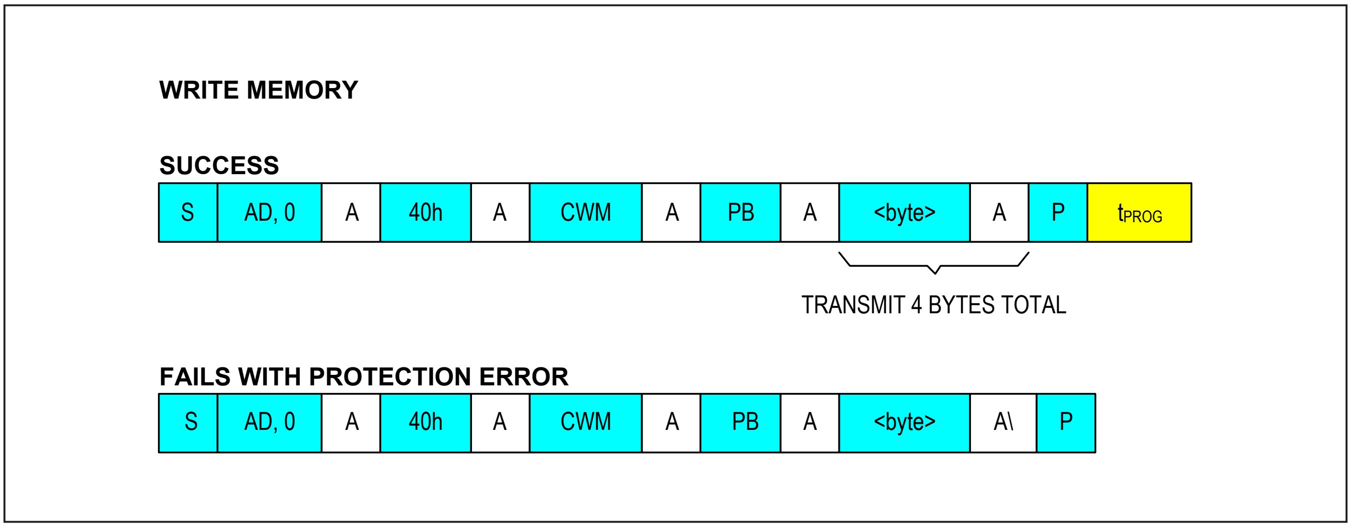
Table 53. I2C Communication—Legend

SYMBOL	DESCRIPTION
S	START Condition
AD, 0	Select MAX66242 for Write Access
AD, 1	Select MAX66242 for Read Access
Sr	Repeated START Condition
P	STOP Condition
A	Acknowledged
A\	Not Acknowledged
(Idle)	Bus Not Busy
PB	Parameter Byte
CWM	Command “Write Memory”, 55h
CRM	Command “Read Memory”, F0h
SP	Command “Set Protection”, C3h
ILS	Command “Install and Lock Secret”, 33h
CRPM	Command “Compute and Read Page MAC”, A5h
AWM	Command “Authenticated Write Memory”, 5Ah
ASP	Command “Authenticated Set Protection”, CCh
CFGW	Command “Configuration Write”, 40h
CFGR	Command “Configuration Read”, 41h
CONW	Command “Control Write”, 42h
CONR	Command “Control Read”, 43h
40h	Transfer byte “40h”
41h	Transfer byte “41h”
CFGD	Configuration Data (1 Byte)
CNTD	Control Data (1 Byte)
<byte>	Transfer of 1 Byte

Table 54. Data Direction Color Codes

MASTER TO SLAVE	SLAVE TO MASTER	(MAX66242 BUSY)

I²C Communication Examples



WRITE MEMORY

SUCCESS

S	AD, 0	A	40h	A	CWM	A	PB	A	<byte>	A	P	t_{PROG}

FAILS WITH PROTECTION ERROR

S	AD, 0	A	40h	A	CWM	A	PB	A	<byte>	A\	P

I2C Communication Examples (continued)

READ MEMORY

S	AD,0	A	40h	A	CRM	A	PB	A	Sr	AD,1	A	<byte>	A	<byte>	A\	P

FIRST n-1 BYTES OF PAGE DATA

LAST BYTE OF PAGE DATA

"n" IS A MULTIPLE OF 4, RANGING FROM 4 TO 32, DEPENDING ON THE PARAMETER BYTE.

SET PROTECTION

SUCCESS

S	AD,0	A	40h	A	SP	A	PB	A	<byte>	A	P	t_{PROG}

FAILS BECAUSE OF INVALID PROTECTION BYTE OR AUTHENTICATION IS REQUIRED

S	AD,0	A	40h	A	SP	A	PB	A	<byte>	A\	P

INSTALL AND LOCK SECRET

LOADED SECRET, SUCCESS (NO LOCKING)

S	AD,0	A	40h	A	ILS	A	PB	A	P	8 × t_{PROG}

COMPUTED SECRET, SUCCESS (NO LOCKING)

S	AD,0	A	40h	A	ILS	A	PB	A	P	2 × t_{CSHA}	8 × t_{PROG}

FAILS BECAUSE SECRET IS LOCKED

S	AD,0	A	40h	A	ILS	A	PB	A\	P

COMPUTE AND READ PAGE MAC

SUCCESS

S	AD,0	A	40h	A	CRPM	A	PB	A	P	2 × t_{CSHA}

S	AD,1	A	<byte>	A	<byte>	A\	P

FIRST 31 BYTES OF MAC

LAST BYTE OF MAC

FAILS DUE TO INVALID PARAMETER BYTE

S	AD,0	A	40h	A	CRPM	A	PB	\A	P	S	AD,1	A	<FF>	A	<FF>	A\	P

REPEAT UNTIL STOP

I2C Communication Examples (continued)

AUTHENTICATED WRITE MEMORY

SUCCESS

S	AD,0	A	40h	A	AWM	A	PB	A	<byte>	A	P	t_{CSHA}

TRANSMIT 4 BYTES TOTAL

S	AD,0	A	41h	A	<byte>	A	P	t_{PROG}

TRANSMIT 32-BYTE MAC

FAILS DUE TO INVALID MAC

S	AD,0	A	40h	A	AWM	A	PB	A	<byte>	A	P	t_{CSHA}

TRANSMIT 4 BYTES TOTAL

S	AD,0	A	41h	A	<byte>	A	<byte>	A\	P	(IDLE)

TRANSMIT 32-BYTE MAC (LAST BYTE NACK'D)

FAILS DUE TO PROTECTION ERROR

S	AD,0	A	40h	A	AWM	A	PB	A	<byte>	A\	P

AUTHENTICATED SET PROTECTION

SUCCESS

S	AD,0	A	40h	A	ASP	A	PB	A	<byte>	A	P	t_{CSHA}

S	AD,0	A	41h	A	<byte>	A	P	t_{PROG}

TRANSMIT 32-BYTE MAC

FAILS DUE TO INVALID MAC

S	AD,0	A	40h	A	ASP	A	PB	A	<byte>	A	P	t_{CSHA}

S	AD,0	A	41h	A	<byte>	A	<byte>	A\	P	(IDLE)

TRANSMIT 32-BYTE MAC (LAST BYTE NACK'D)

FAILS DUE TO PROTECTION BYTE ERROR

S	AD,0	A	40h	A	ASP	A	PB	A	<byte>	A\	P

I²C Communication Examples (continued)

CONFIGURATION WRITE

S	AD,0	A	40h	A	CFGW	A	PB	A	P	t_{PROG}

CONFIGURATION READ

S	AD,0	A	40h	A	CFGR	A	PB	A	Sr	AD,1	A	CFGD	A\	P

CONTROL WRITE

S	AD,0	A	40h	A	CONW	A	PB	A	P

CONTROL READ

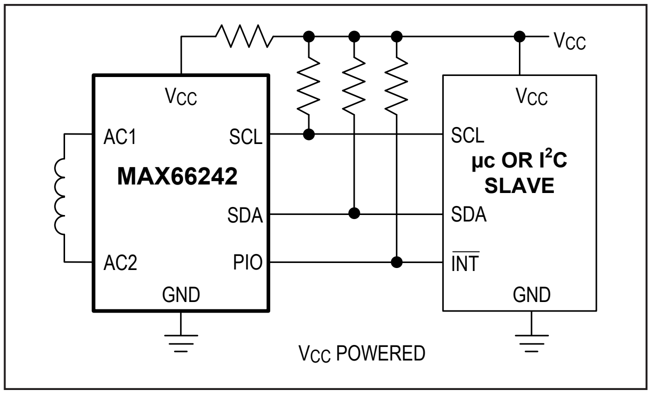
S	AD,0	A	40h	A	CONR	A	PB	A	Sr	AD,1	A	CNTD	A\	P

Ordering Information

PART	TEMP RANGE	PIN-PACKAGE
MAX66242ESA+	-40°C to +85°C	8 SO
MAX66242ESA+T	-40°C to +85°C	8 SO (2.5k pcs)
MAX66242ETB+	-40°C to +85°C	10 TDFN
MAX66242ETB+T	-40°C to +85°C	10 TDFN (2.5k pcs)
MAX66242E/W+†	-40°C to +85°C	AU bumped, tested, diced wafer
MAX66242/W+†	-40°C to +85°C	Tested wafer

+Denotes a lead(Pb)-free/RoHS-compliant package.
T = Tape and reel.
†Contact factory for further details.

Typical Application Circuits (continued)



Package Information

For the latest package outline information and land patterns (footprints), go to www.maximintegrated.com/packages. Note that a "+", "#", or "-" in the package code indicates RoHS 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	OUTLINE NO.	LAND PATTERN NO.
8 SO (150 mils)	S8+2	21-0041	90-0096
10 TDFN (3mm x 4mm)	T1034N+1	21-0268	90-0247
Wafer	—	—	—

Errata

ISO 15693-3 Section 9.1 specifies that if the VICC detects a carrier modulation during time t_1, it shall reset its t_1 timer and wait for a further time t_1 before starting to transmit its response to a VCD request or to switch to the next slot when in an inventory process. The MAX66242 is not compliant with this specification.

ISO15693-3 Section 9.4.2 specifies that during an inventory process, when the VCD has received no VICC response, it shall wait a time t_3 before sending a subsequent EOF to switch to the next slot. If the VCD sends a 100% modulated EOF, the minimum value of t_3 is 4384/fc (323.3µs) + tsof. The MAX66242 is not compliant with this specification. The MAX66242 requires a minimum t_3 = 4384/fc (323.3µs) + tnrt + t2min, where tsof is the time duration for a VICC to transmit an SOF to the VCD, and tnrt is the nominal response time of a VICC. tnrt and tsof are dependent on the VICC-to-VCD data rate and subcarrier modulation mode.

The peripheral transaction command responds with an A0h error when Address_Flag = 0.

Revision History

REVISION NUMBER	REVISION DATE	DESCRIPTION	PAGES CHANGED
0	2/14	Initial release	—
1	9/14	Updated *Features and Benefits* and *Ordering Information* sections, typical operating characteristic graphs 1 and 2, revised *Electrical Characteristics* table to meet the new die revision, removed any information on bits INT_S and EHVOUT	1, 2–5, 6, 14–17, 91
2	12/14	Updated *Benefits and Features* section	1
3	4/18	Updated *Benefits and Features*, *Absolute Maximum Ratings*, *Electrical Characteristics* global conditions, *Electrical Characteristics* table, *Ordering Information*, and *Package Information* sections	1–5, 90

For pricing, delivery, and ordering information, please contact Maxim Direct at 1-888-629-4642, or visit Maxim Integrated's website at www.maximintegrated.com.

Maxim Integrated cannot assume responsibility for use of any circuitry other than circuitry entirely embodied in a Maxim Integrated product. No circuit patent licenses are implied. Maxim Integrated reserves the right to change the circuitry and specifications without notice at any time. The parametric values (min and max limits) shown in the Electrical Characteristics table are guaranteed. Other parametric values quoted in this data sheet are provided for guidance.