MAX32660 Secure Bootloader User Guide

UG6471; Rev 1; 3/20

Abstract

The MAX32660 secure bootloader user guide provides flow charts; timing diagrams; GPIOs/pin usage; I²C interface protocols and an annotated trace between the host microcontroller; MAX32660 bootloader protocol definitions; and the MAX32660 for in-application programming (IAP).

Table of Contents

List of Figures

List of Tables

Overview

The MAX32660 secure bootloader is embedded firmware that gives the MAX32660 the ability to update application code provided by a host microcontroller. The bootloader can be accessed through the I2C interface. These interfaces provide the data channel and the control channel for communicating between the host microcontroller and the MAX32660. The bootloader application load mode is enabled and disabled by either a serial command or hardware connectivity. The serial command is interpreted by the user application, which configures the device to enter bootloader mode. When using the hardware connectivity option, a single GPIO pin and the RSTN pin on the MAX32660 can be configured to allow the MAX32660 to enter bootloader mode.

Detailed Description

Figure 1 and **Figure 2** show the program flow for the bootloader.

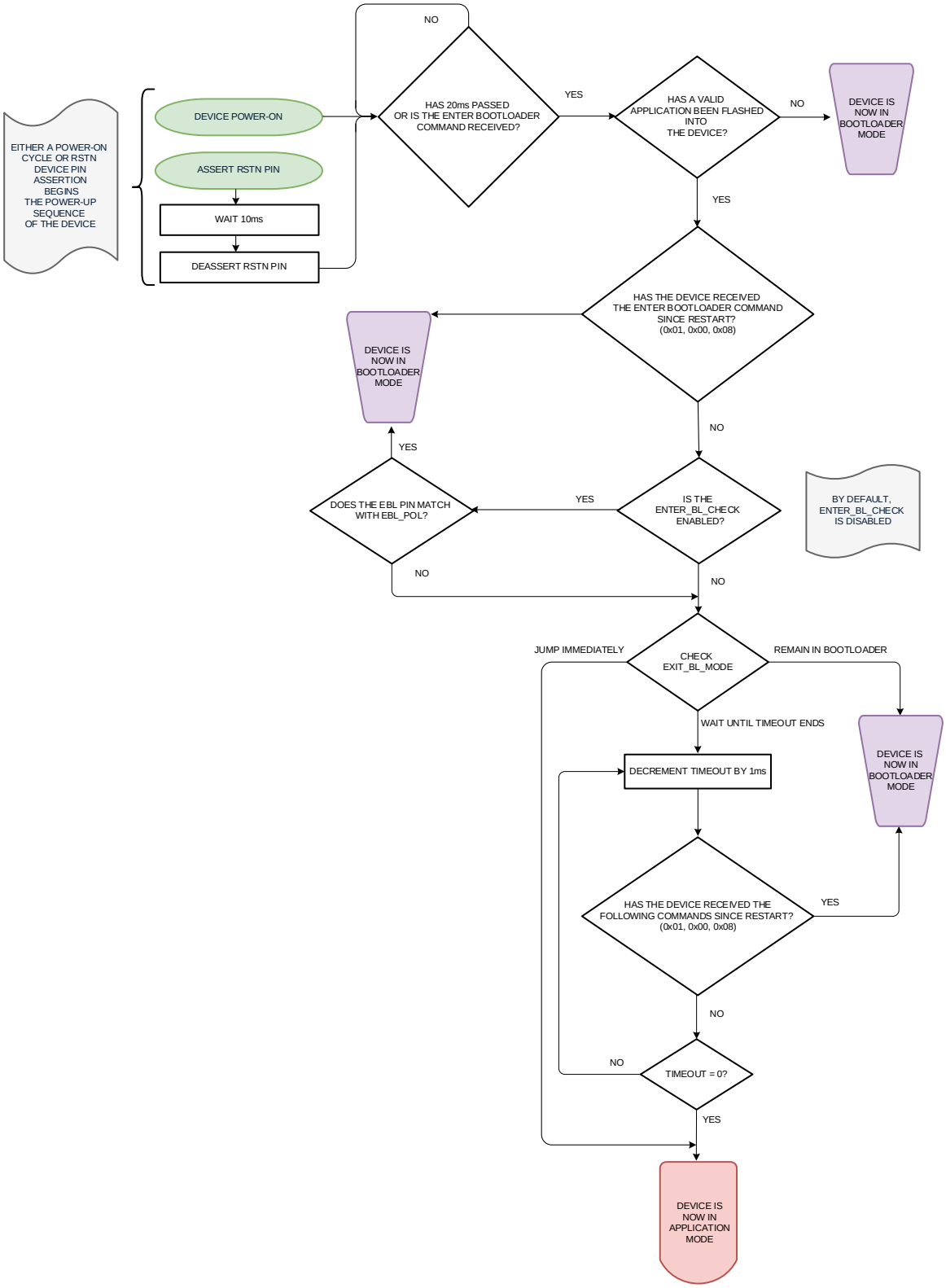


Figure 1. MAX32660 bootloader top-level flow chart.

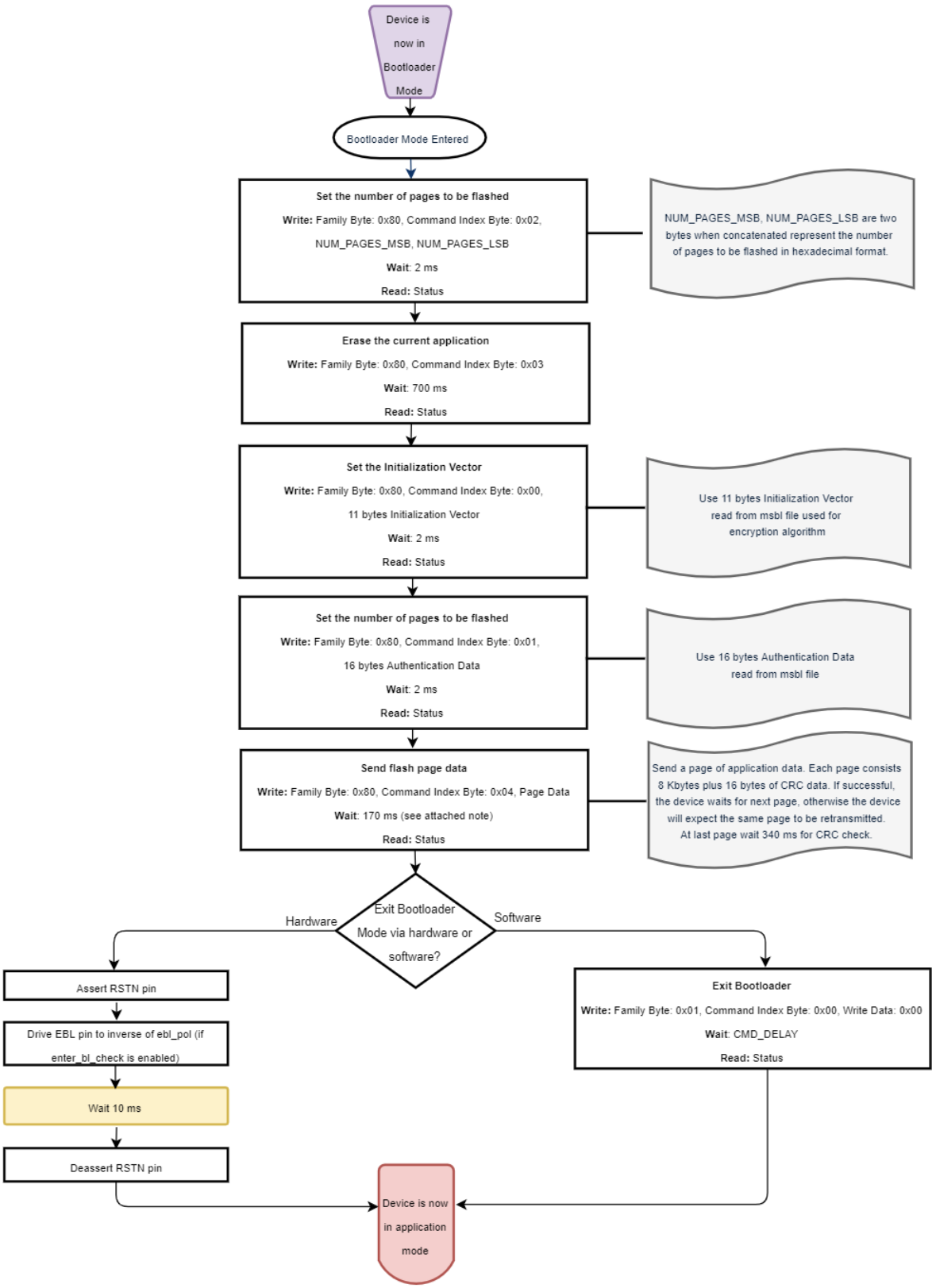


Figure 2. MAX32660 bootloader application loader flow chart.

MAX32660 Bootloader Memory Map

The MAX32660 bootloader uses the first two pages of MAX32660 flash memory and 64 bytes at the end of the flash memory for bootloader data starting from 0x3FFC0, as shown in

Figure 3. The application start address is 0x4000 and the maximum size of an application that can be programmed is 245696 bytes.

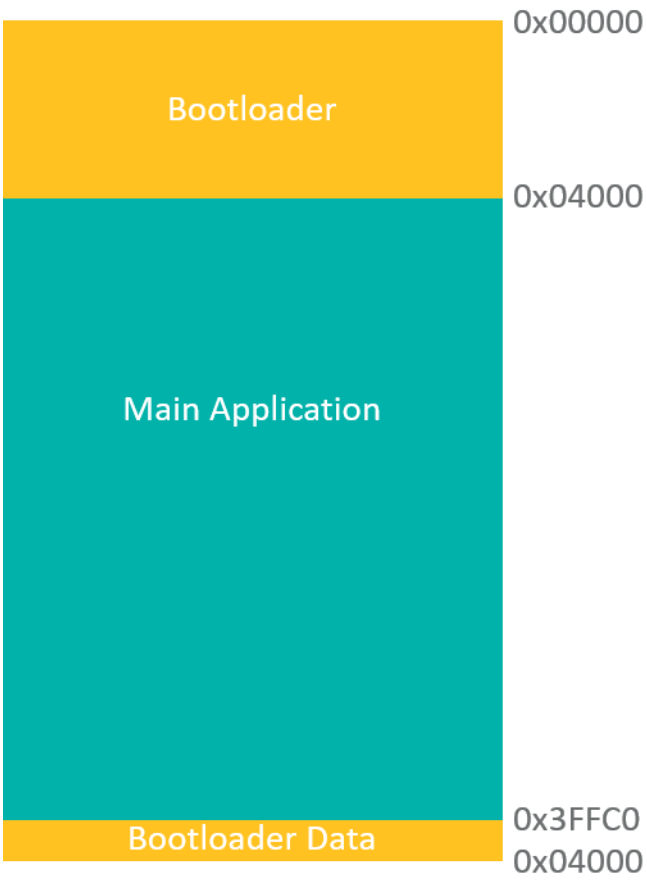


Figure 3. MAX32660 bootloader memory map.

Bootloader Pin Definitions

Table 1 lists the descriptions for the GPIO and RSTN pins of the MAX32660 bootloader.

Table 1. GPIO and RSTN Pin Descriptions

MAX32660	DESCRIPTION	DIRECTION FROM MAX32660 SIDE
Pin RSTN	Reset_N	Input
GPIO P0.0	SWDIO	Input/Output
GPIO P0.1	SWDCLK	Input
GPIO P0.2	I2C0_SCL	Input
GPIO P0.3	I2C0_SDA	Input/Output

Activating the Bootloader

Entering Bootloader Mode from Application Mode

This section defines several methods for entering bootloader mode from application mode.

Host Serial Command Using Power-On or Hard Reset

The MAX32660 can enter bootloader mode by performing the following steps:

1. Power cycle the MAX32660 or perform a hard reset with the RSTN pin.
2. The host microcontroller sends the command 0x01, 0x00, 0x08 over the selected interface to the MAX32660 within 20ms of the reset operation. This is a signal to the cold boot process to enter bootloader mode.

Without Using the RSTN Pin or GPIO Pins

"Boot_mode" is a 4-byte flag located at 0x3FFCC. Change the "boot_mode" flag in the flash memory to 0xAAAAAAAA for staying in the bootloader even when there is a valid application in the memory. The number of write cycles to flash the memory is limited to 10,000 cycles. Consequently, this method should be not be used frequently. In addition, the bootloader firmware can become inoperable if power is lost during this operation or if the code is not implemented correctly.

Using the Enter Bootloader GPIO Pin and the RSTN Pin

Another method for entering bootloader mode is to use the enter bootloader (EBL) GPIO pin and the RSTN pin. The EBL pin is disabled in the bootloader by default and can be enabled by command. The MAX32660 enters bootloader mode based on the sequencing of the RSTN pin and the EBL pin.

The sequence to enter bootloader mode using the EBL GPIO pin and the RSTN pin is as follows:

1. Set the RSTN pin low for 10ms.
2. During that time, set the EBL GPIO pin to low. This polarity is configurable and active-low for bootloader mode by default.
3. After 10ms, set the RSTN pin high.
4. After an additional 20ms, the MAX32660 is in bootloader mode.

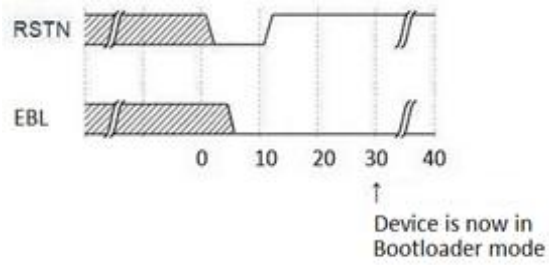


Figure 4. Entering bootloader mode through the EBL GPIO and RSTN pins.

Entering Application Mode from Bootloader Mode

This section discusses various methods of entering application mode from bootloader mode.

A Valid Application Is Programmed

If a valid application is programmed into the MAX32660 using in-application programming (IAP), the bootloader automatically runs the application code (assuming that the EBL GPIO pin is disabled) after reset.

Using the EBL GPIO Pin and the RSTN Pin

The MAX32660 enters application mode based on the sequencing of the EBL GPIO pin and the RSTN pin if there is a programmed valid application. The EBL GPIO pin is disabled in the bootloader by default and can be enabled by the serial commands.

The sequence to enter application mode using the EBL GPIO pin and the RSTN pin is as follows:

1. Set the RSTN pin low for 10ms.
2. During that time, set the EBL GPIO pin to high. This polarity is configurable and active-low for bootloader mode by default.
3. After 10ms, set the RSTN pin high.
4. After an additional 20ms, the MAX32660 is in application mode.

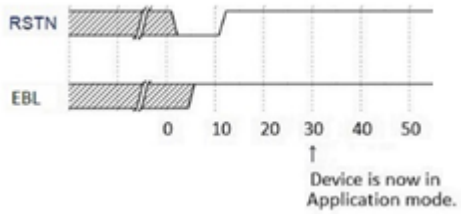


Figure 5. Entering application mode through the EBL GPIO and RSTN pins.

Configuring the Bootloader

Bootloader Configuration Parameters

Bootloader configuration parameters are used to enable and disable some functions of the bootloader. These parameters are located at the memory address 0x3FFD0. The bootloader configuration can be changed by the serial commands. Definitions and default values for the bit fields are provided as follows:

EBL Pin Check (1 bit)

According to the enter_bl_check bit, the bootloader checks the status of the EBL GPIO pin at startup. If the EBL pin is left floating after the EBL pin check is enabled, this can lead to unexpected behavior such as getting stuck in bootloader mode even if there is a valid application.

BIT VALUE	OPERATION
0	Do not check EBL pin (Default)
1	Check EBL pin

EBL Pin Assignment (4 bits)

The ebl_pin bits are used to choose the EBL GPIO pin. The selected pin is checked at bootloader startup to make a decision for staying in the bootloader or jumping to the application if the EBL GPIO pin check is enabled by the enter_bl_check bit.

BIT VALUE	OPERATION
0b0000	P0.0
0b0001	P0.1 (Default)
0b0010	P0.2
0b0011	P0.3
0b0100	P0.4
0b0101	P0.5
0b0110	P0.6
0b0111	P0.7
0b1000	P0.8
0b1001	P0.9
0b1010	P0.10
0b1011	P0.11
0b1100	P0.12
0b1101	—
0b1110	—
0b1111	—

EBL GPIO Pin Polarity (1 bit)

The EBL GPIO pin is used to keep the device at bootloader mode after reset if enter_bl_check is enabled. The ebl_pol bit defines whether the polarity EBL GPIO pin enters bootloader mode.

BIT VALUE	OPERATION
0	Active-low signal puts the device in bootloader mode (Default)
1	Active-high signal puts the device in bootloader mode

Timeout Mode (2 bits)

The exit_bl_mode bits define timeout mode for the bootloader.

BIT VALUE	OPERATION
0b00	Jump after 20ms
0b01	Wait for programmable delay (ebl_timeout) (Default)
0b10	Remain in bootloader mode until exit command is received
0b11	—

Timeout Window (8 bits)

The timeout window is the time to wait for a serial command from a host to stay in bootloader mode before jumping to a valid application. The wait time is calculated according to the following formula:

t_{WAIT} = 20ms + (EBL_TIMEOUT*10)ms

Bootloader Interfaces

I²C Interface

The I²C bus expects SCL and SDA to be open-drain signals and that the SDA and SCL pad circuits are automatically configured as open-drain outputs for the MAX32660 bootloader. The I²C interface supports transfer rates up to 400kbit/s (fast mode). The I²C slave address is 0xAA at default/

I²C Bit Transfer Process

The SDA and SCL signals are open-drain circuits. Each has an external pullup resistor that ensures each circuit is high when idle. The I²C specification states that during data transfer, the SDA line can change state only when the SCL is low, and when the SCL is high, the SDA is stable and able to be read. Typical I²C write/read transactions are shown in **Figure 6**.

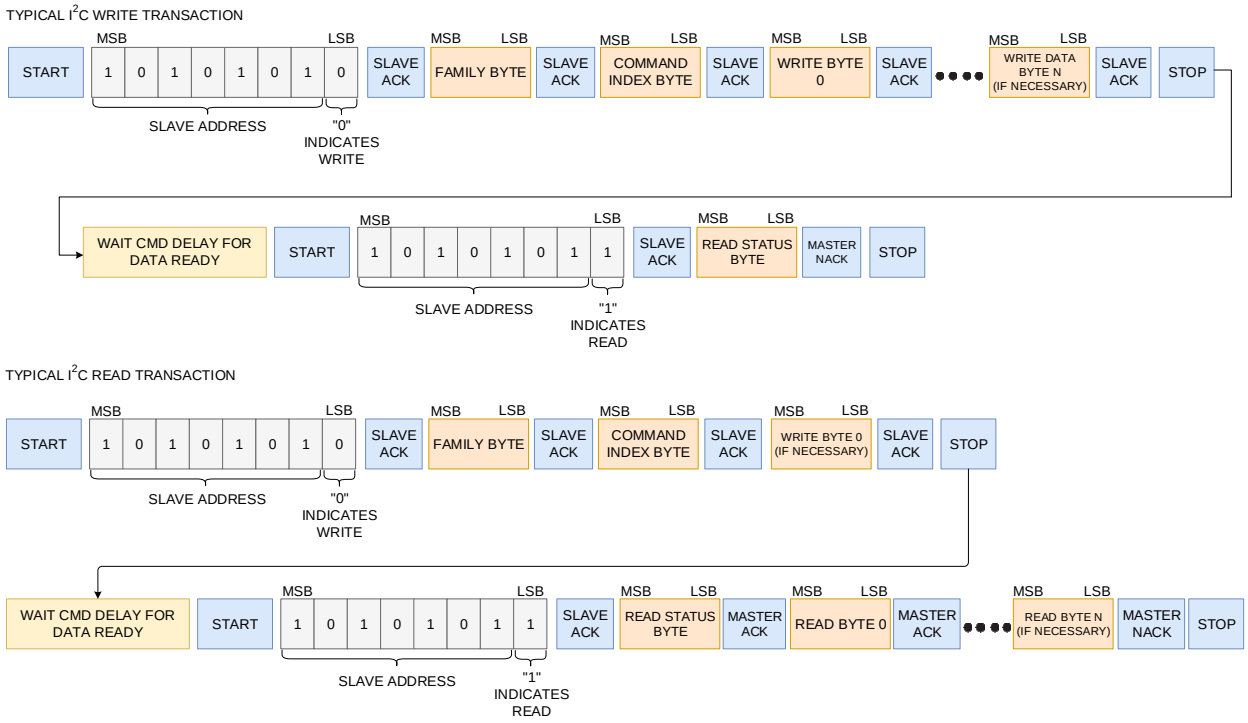


Figure 6. I²C write/read data transfer from host microcontroller.

The read status byte indicates the success or failure of the write transaction. The read status byte must be accessed after each write transaction to the device to ensure that the write transaction process is understood and any errors in the device command handling can be corrected. The read status byte value is summarized in **Table 2**.

Table 2. Read Status Byte Values

READ STATUS BYTE VALUE	DESCRIPTION
0xAA	SUCCESS. The write transaction was successful.
0x01	ERR_UNAVAIL_CMD. Illegal Family Byte and/or Command Byte was used.
0x02	ERR_UNAVAIL_FUNC. This function is not implemented.
0x03	ERR_DATA_FORMAT. Incorrect number of bytes sent for the requested Family Byte.
0x04	ERR_INPUT_VALUE. Illegal configuration value was attempted to be set.
0x80	ERR_BTLDR_GENERAL. General error while receiving/flashing a page during the bootloader sequence.
0x81	ERR_BTLDR_CHECKSUM. Checksum error while decrypting/checking page data.
0x82	ERR_BTLDR_AUTH. Authorization error.
0x83	ERR_BTLDR_INVALID_APP. Application not valid.
0x84	ERR_BTLDR_APP_NOT_ERASED. Application was not erased before trying to flash a new one.
0xFE	ERR_TRY_AGAIN. Device is busy. Try again.
0xFF	ERR_UNKNOWN. Unknown error.

I²C Write

The process for an I²C write data transfer is as follows:

1. The bus master indicates a data transfer to the device with a START condition.
2. The master transmits 1 byte with the 7-bit slave address and a single write bit set to zero. The 8 bits transferred as a slave address for the MAX32660 are 0xAA for a write transaction.
3. During the next SCL clock that follows the write bit, the master releases SDA. During this clock period, the device responds with an ACK by pulling SDA low.
4. The master senses the ACK condition and begins to transfer the Family Byte. The master drives data on the SDA circuit for each of the 8 bits of the Family Byte and then floats SDA during the ninth bit to allow the device to reply with the ACK indication.
5. The master senses the ACK condition and begins to transfer the Command Index Byte. The master drives data on the SDA circuit for each of the 8 bits of the Command Index Byte and then floats SDA during the ninth bit to allow the device to reply with the ACK indication.
6. The master senses the ACK condition and begins to transfer the Write Data Byte 0. The master drives data on the SDA circuit for each of the 8 bits of the Write Data Byte 0 and then floats SDA during the ninth bit to allow the device to reply with the ACK indication.
7. The master senses the ACK condition and can begin to transfer another Write Data Byte if required. The master drives data on the SDA circuit for each of the 8 bits of the Write Data Byte and then floats SDA during the ninth bit to allow the device to reply with the ACK indication. If another Write Data Byte is not required, the master indicates the transfer is complete by generating a STOP condition. A STOP condition is generated when the master pulls SDA from a low to high while SCL is high.
8. The master waits for a period of CMD_DELAY (60µs) for the device to have the data ready.
9. The master indicates a data transfer to the slave with a START condition.
10. The master transmits 1 byte with the 7-bit slave address and a single write bit set to one. This is an indication from the master to read the device from the previously written location

defined by the Family Byte and the Command Index. The master then floats SDA and allows the device to drive SDA to send the Status Byte. The Status Byte reveals the success of the previous write sequence. After the Status Byte is read, the master drives SDA low to signal the end of data to the device.

11. The master indicates the transfer is complete by generating a STOP condition.
12. After the completion of the write data transfer, the Status Byte must be analyzed to determine if the write sequence was successful and the device has received the intended command.

I²C Read

The process for an I²C read data transfer is as follows:

1. The bus master indicates a data transfer to the device with a START condition.
2. The master transmits 1 byte with the 7-bit slave address and a single write bit set to zero. The 8 bits transferred as a slave address for the MAX32660 are 0xAA for a write transaction. This write transaction precedes the actual read transaction to indicate to the device which section is to be read.
3. During the next SCL clock that follows the write bit, the master releases SDA. During this clock period, the device responds with an ACK by pulling SDA low.
4. The master senses the ACK condition and begins to transfer the Family Byte. The master drives data on the SDA circuit for each of the 8 bits of the Family Byte and then floats SDA during the ninth bit to allow the device to reply with the ACK indication.
5. The master senses the ACK condition and begins to transfer the Command Index Byte. The master drives data on the SDA circuit for each of the 8 bits of the Command Index Byte and then floats SDA during the ninth bit to allow the device to reply with the ACK indication.
6. The master senses the ACK condition and begins to transfer the Write Data Byte if necessary for the read instruction. The master drives data on the SDA circuit for each of the 8 bits of the Write Data Byte and then floats SDA during the ninth bit to allow the device to reply with the ACK indication.
7. The master indicates the transfer is complete by generating a STOP condition.
8. The master waits for a period of CMD_DELAY (60µs) for the device to have its data ready.
9. The master indicates a data transfer to the slave with a START condition.
10. The master transmits 1 byte with the 7-bit slave address and a single write bit set to 1. This is an indication from the master to read the device from the previously written location defined by the Family Byte and the Command Index. The master then floats SDA and allows the device to drive SDA to send the Status Byte. The Status Byte reveals the success of the previous write sequence. After the Status Byte is read, the master drives SDA low to acknowledge the byte.
11. The master floats SDA and allows the device to drive SDA to send Read Data Byte 0. After Read Data Byte 0 is read, the master drives SDA low to acknowledge the byte.
12. The master floats SDA and allows the device to drive SDA to send the Read Data Byte N. After Read Data Byte N is read, the master drives SDA low to acknowledge the byte. This process continues until the device has provided all the data that the master expects based upon the Family Byte and Command Index Byte definition.

13. The master indicates the transfer is complete by generating a STOP condition.

Communicating with the Bootloader

MAX32660 Bootloader Message Protocol Definitions

Table 3 lists the MAX32660 bootloader message protocol definitions.

Table 3. MAX32660 Bootloader Message Protocol Definitions

HOST COMMAND					MAX32660 BOOTLOADER
FAMILY NAME	**DESCRIPTION**	**FAMILY BYTE**	**INDEX BYTE**	**WRITE BYTES**	**RESPONSE BYTES**
Device Mode	Select the device operating mode.	0x01	0x00	**0x00**: Exit bootloader mode. **0x02**: Reset. (The application must implement this.) **0x08:** Enter bootloader mode. (The application must implement this. See section Host Serial Command using Power-On or Hard Reset.)	—
Device Mode	Read the device operating mode.	0x02	0x00	(The application must implement this.)	**0x00**: Application operating mode. **0x08**: Bootloader operating mode.
Bootloader Flash	Set the initialization vector bytes. This is not required for a non-secure bootloader.	0x80	0x00	Use the 11 bytes 0x28 to 0x32 from the .msbl file.	—
Bootloader Flash	Set the authentication bytes. This is not required for a non-secure bootloader.	0x80	0x01	Use the 16 bytes 0x34 to 0x43 from the .msbl file.	—
Bootloader Flash	Set the number of pages.	0x80	0x02	**0x00:** Number of pages specified by byte 0x44 from the .msbl file. (Total of 2 bytes)	—
Bootloader Flash	Erase the application flash memory.	0x80	0x03	—	—
Bootloader Flash	Send the page values.	0x80	0x04	The first page is specified by byte 0x4C from the .msbl file. The total bytes for each message protocol is the page size + 16 bytes (consisting of the page CRC32 and 12 dummy bytes).	—
Bootloader Flash	Erase Page Memory	0x80	0x05	**0x00:** Number of pages to be erased. (Total of 2 bytes)	—

HOST COMMAND					MAX32660 BOOTLOADER
FAMILY NAME	**DESCRIPTION**	**FAMILY BYTE**	**INDEX BYTE**	**WRITE BYTES**	**RESPONSE BYTES**
Bootloader Information	Get the bootloader version.	0x81	0x00	—	Major version byte, Minor version byte, Revision byte
Bootloader Information	Get the page size in bytes.	0x81	0x01	—	Upper byte of page size, Lower byte of page size
Bootloader Configuration	Save bootloader configurations. Write this command after changes are made to any of the Bootloader Configuration settings. The bootloader should be restarted for the new configuration to be active.	0x82	0x00	—	—
Bootloader Configuration	Select enter_bl_check. Configure the device to check the state of the EBL GPIO pin to decide whether to enter bootloader mode.	0x82	0x01	**0x00, 0x00:** The device does not check the state of the EBL GPIO pin. (Default) **0x00, 0x01:** The device checks the state of the EBL GPIO pin before entering bootloader mode.	—
Bootloader Configuration	Select the EBL GPIO pin (ebl_pin). Select which pin to use as the EBL GPIO pin. This command is only used if the Bootloader Configuration enter bootloader check is set to 1 (0x82 0x01 0x00 0x01).	0x82	0x01	**0x01, 0x00–0x09:** Acceptable range for the 16-bump WLP package. **0x01, 0x00–0x0B:** Acceptable range for the 20-pin TQFN-EP and the 24-pin TQFN-EP.	—
Bootloader Configuration	Select the active state for the EBL GPIO pin (ebl_pol). This command is only used if the Bootloader Configuration enter bootloader check is set to 1 (0x82 0x01 0x00 0x01).	0x82	0x01	**0x02, 0x00:** Active-low. The device enters bootloader mode if the EBL GPIO pin is held low during power-on or during a RSTN device pin cycle. (Default) **0x02, 0x01:** Active-high. The device enters bootloader mode if the EBL GPIO pin is held high during power-on or during a RSTN device pin cycle.	—

HOST COMMAND					MAX32660 BOOTLOADER
FAMILY NAME	**DESCRIPTION**	**FAMILY BYTE**	**INDEX BYTE**	**WRITE BYTES**	**RESPONSE BYTES**
Bootloader Configuration	Exit bootloader mode (exit_bl_mode). Determine how the bootloader enters application mode.	0x82	0x02	**0x00, 0x00:** Enter application mode if an application is present and valid. If EBL GPIO pin was used to enter bootloader mode, the jump does not occur until the EBL GPIO pin is in a non-active state (Default). **0x00, 0x01:** Wait for a programmable delay. If no commands are received and a valid application is present, enter application mode. **0x00, 0x02:** Stay in bootloader mode.	—
Bootloader Configuration	Configure timeout exit (ebl_timeout). Set the length of the additional programmable timeout to use when the Bootloader Configuration exit bootloader mode is set to 1 (AA 82 02 01). The system requires a 20ms non-programmable delay to switch to application mode.	0x82	0x02	**0x01,0x00–0xFF:** Timeout Note: Timeout is cancelled if any commands are received during this period.	—
Bootloader Configuration	Read bootloader check configuration (enter_bl_check). Read the device configuration to check the state of the EBL GPIO pin to decide whether to enter bootloader mode.	0x83	0x01	0x00	**0x00:** The device does not check the state of the EBL GPIO pin. **0x01:** The device checks the state of the EBL GPIO pin before entering bootloader mode.

HOST COMMAND					MAX32660 BOOTLOADER
FAMILY NAME	**DESCRIPTION**	**FAMILY BYTE**	**INDEX BYTE**	**WRITE BYTES**	**RESPONSE BYTES**
Bootloader Configuration	Read the EBL GPIO pin (ebl_pin). Read which pin is used as the EBL GPIO pin. This command is only used if the Bootloader Configuration enter bootloader check is set to 1 (AA 82 01 00 01).	0x83	0x01	0x01	**0x00–0x09:** Expected range for the 16-bump WLP package. **0x00–0x0B:** Expected range for the 20-pin TQFN-EP and the 24-pin TQFN-EP
Bootloader Configuration	Read the active state for the EBL GPIO pin (ebl_pol).	0x83	0x01	0x02	**0x00:** Active-low. The device enters bootloader mode if the EBL GPIO pin is held low during power-on or during a RSTN device pin cycle. **0x01:** Active-high. The device enters bootloader mode if the EBL GPIO pin is held high during power-on or during a RSTN device pin cycle.
Bootloader Configuration	Read exit bootloader mode configuration. Read how the bootloader enters application mode.	0x83	0x02	0x00	**0x00:** If an application is present and valid, enter application mode. If the EBL GPIO pin was used to enter bootloader mode, the jump does not occur until the EBL GPIO pin is in a non-active state. (Default) **0x01:** Wait for a programmable delay. If no commands are received and a valid application is present, enter application mode. **0x02:** Stay in bootloader mode.
Bootloader Configuration	Read exit timeout configuration (ebl_timeout). Read the timeout to use when the Bootloader Configuration exit bootloader mode is set to 1 (AA 82 02 01). Timeout is cancelled if any commands are received during this period.	0x83	0x02	0x01	**0x00–0xFF:** Timeout
Identity	Read the MCU type.	0xFF	0x00	—	**0x00:** MAX32625 **0x01:** MAX32660/MAX32664

MAX32660 In-Application Programming, Annotated Trace

The MAX32660 bootloader firmware supports IAP.

This section shows the necessary commands to flash the application to MAX32660. Each 8192-byte page data is appended with 4-byte CRC32 of the page and 12 bytes of 0x00, therefore payload of the bootloader flash page message is 8208 bytes for each page. The number of pages can be found by computing:

$$\left\lceil \frac{\langle \text{binary\_size} \rangle}{8192} \right\rceil + 1$$

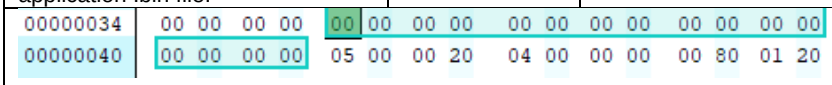
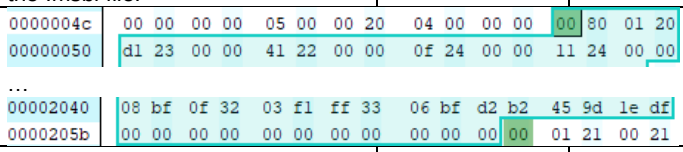
Necessary commands to flash an application image of 25922 (0x6542) bytes are shown in the following example, where the number of pages is calculated as:

$$\left\lceil \frac{25922}{8192} \right\rceil + 1 = 5$$

Table 4 shows how to download the application by using the .msbl file. See Appendix A for more details about the .msbl file.

Table 4. Application Programming Example by Using the .msbl File

HOST COMMAND	COMMAND DESCRIPTION	MAX32660 BOOTLOADER RESPONSE	RESPONSE DESCRIPTION
0x01 0x00 0x08*	Set mode to 0x08 for bootloader mode. Note that this is one of the alternative methods for entering bootloader mode. If this command is used, the EBL pin is not necessary See the Entering Bootloader Mode from the Application Mode section for alternative ways to enter bootloader mode.	0xAA	No error.
0x02 0x00*	Read mode.	0xAA 0x08	No error. Mode is bootloader.
0xFF 0x00+	Get ID and MCU type.	0xAA 0x01	No error. MCU is MAX32660/MAX32664.
0x81 0x00	Read bootloader firmware version.	0xAA 0xXX 0xXX 0xXX	No error. Version is XX.XX.XX
0x81 0x01	Read bootloader page size.	0x00 0x20 0x00	No error. Page size is 8192.
0x80 0x02 0x00 0x05*	Bootloader flash. Set the number of pages to 5 based on byte 0x44 from the application .msbl file, which is created from the user application .bin file.	0xAA	No error.
	00000044 00 00 00 00 **05** 00 00 20 04 00 00 00 00 80 01 20		
0x80 0x03*	Bootloader flash. Erase application.	0xAA	No error.
0x80 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00	Bootloader flash. Set Initialization Vector based on the bytes 0x28 to 0x32 from the application .msbl file, which is created from the user application .bin file.	0xAA	No error.
	00000028 00 00 00 00 00 00 00 00 **00 00 00 00 00 00 00 00** 00000030 **00 00 00 00** 00 00 00 00 00 00 00 00 00 00 00 00		

HOST COMMAND	COMMAND DESCRIPTION	MAX32660 BOOTLOADER RESPONSE	RESPONSE DESCRIPTION
0x80 0x01 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00	Bootloader flash. Set Authentcation based on the bytes 0x34 to 0x43 from the application .msbl file, which is created from the user application .bin file.	0xAA	No error.
			
0x80 0x04 0x00 0x80 0x01 ... 0x00 0x00 0x00*	Bootloader flash. Send first page bytes 0x4C to 0x205B from the .msbl file.	0xAA	No error.
			
0x80 0x04 0x01 0x21 0x00 ... 0x00 0x00 0x00*	Bootloader flash. Send second page bytes 0x205C to 0x406B from the .msbl file.	0xAA	No error.
0x80 0x04 0x02 0x02 0xC1 ... 0x00 0x00 0x00*	Bootloader flash. Send third page bytes 0x406C to 0607B from the .msbl file.	0xAA	No error.
0x80 0x04 0xEO 0x6C 0x1C ... 0x00 0x00 0x00*	Bootloader flash. Send fourth page bytes 0x607C to 0x808B from the .msbl file.	0xAA	No error.
0x80 0x04 0xFF 0xC3 0x0D ... 0x00 0x00 0x00*	Bootloader flash. Send fifth page bytes 0x808C to 0XA09B from the .msbl file.	0xAA	No error.
0x01 0x00 0x00*	Exit bootloader mode and jump to application. Note: Sending the bootloader command is not mandatory. The microcontroller can be reset and the EBL pin can be set to reverse the polarity to jump on the application.	0xAA	No error.

**Mandatory*

+Recommended

Appendix A: Maxim Special Bootloader (.msbl) File Format

The .msbl file is a special binary file format that is generated from the application update .bin file by using the MAX32660 bootloader. The .msbl file has the following sections:

- Header

  The header consists of the following:

  - 4-byte magic value (.msbl)
  - 4-byte RFU
  - 16-byte target type (e.g., MAX32660)
  - 16-byte Encryption Algorithm (e.g., AES-192)
  - 11-byte Initialization Vector
  - 1-byte RFU
  - 16-byte Authentication Data
  - 2-byte number of pages (LSB first) (e.g., 0x05 0x00 means there are six pages)

    $$\text{Number of pages} = \left\lceil \frac{\langle \text{bin file size} \rangle}{\text{page size}} \right\rceil + 1 \text{ (for sending application information)}$$

  - 2-byte page size (LSB first) (e.g., 0x00 0x20 means the page size is 8192)
  - 1-byte CRC byte size (0x04 means 4 bytes and denotes CRC32)
  - 3-byte RFU

  Figure 7 shows an example of the format of the raw hex header data in the .msbl file.

```
Address  0  1  2  3  4  5  6  7  8  9  a  b  c  d  e  f  Dump
00000000 6d 73 62 6c 00 00 00 00 4d 41 58 33 32 36 36 30 msbl....MAX32660
00000010 00 00 00 00 00 00 00 00 41 45 53 2d 31 39 32 00 ........AES-192.
00000020 00 00 00 00 00 00 00 00 8d 5d e0 92 d1 fd e9 96 .........]à'Ñý-
00000030 69 e5 0d 00 a4 72 60 d1 a7 4c 8e fc 08 e4 86 87 iå..¤r`Ñ§LŽü.ä†‡
00000040 16 a1 58 65 05 00 00 20 04 00 00 00 66 58 91 c8 .¡Xe... ....fX'È
```

  Figure 7. Hex header data in the .msbl.

- (Number of pages – 1) × Page Data:

  - Page Data 1: First 8192-byte data from the .bin file + 4-byte CRC32 of the first 8192-byte data + 12-byte dummy data (0x00)
  - Page Data 2: Second 8192-byte data from the .bin file + 4-byte CRC32 of the first 8192-byte data + 12-byte dummy data (0x00)
  - Page Data 3: Third 8192-byte data from the .bin file + 4-byte CRC32 of the first 8192-byte data + 12-byte dummy data (0x00)

    …

- Page Data (Number of pages – 1): (Number of pages – 1)th 8192-byte data from the .bin file + 4-byte CRC32 of the first 8192-byte data + 12-byte dummy data (0x00)

- Application information: 4-byte CRC32 of the application + 4-byte length of the application + 8184-byte dummy data (0x00) + 4-byte CRC32 + 12-byte dummy data (0x00)
- 4-byte CRC32 of the .msbl file which is the CRC32 value of the total .msbl file

Table 5 shows the .msbl file format for an application with a size of 17384 bytes.

Table 5. Example .msbl File Format

ADDRESS	LENGTH (bytes)	NAME	DESCRIPTION
0x0000	4	Magic (.msbl)	A marker that indicates the beginning of the .msbl file
0x0004	4	RFU	Reserved for future use (Fill 0x00)
0x0008	16	Target Type	Target microcontroller. For example, MAX32660 with zeros appended.
0x0018	16	Encryption Algorithm	Defines used Encryption Algorithm (e.g AES-192)
0x0028	11	Initialization Vector	Initialization Vector used for encryption algorithm
0x0033	1	RFU	Reserved for future use (Fill 0x00)
0x0034	16	Authentication Data	Authentication Data of the all image
0x0044	2	Number of pages	Number of pages (0x04 for this application)
0x0046	2	Page size	Number of bytes per page. Always 0x2000 (8192 as a decimal).
0x0048	1	CRC byte size	0x04 bytes denoting CRC32
0x0049	3	RFU	Reserved for future use (Fill 0x00)
0x004C	8192	First 8192 bytes of the .bin file	The first page of application data
0x204C	4	CRC32 of the first page	Calculated CRC32 value for the first page of application data
0x2050	12	RFU	Reserved for future use (Fill 0x00)
0x205C	8192	Second 8192 bytes of the .bin file	Second page of application data
0x405C	4	CRC32 of the second page	Calculated CRC32 value for the second page of application data appended with 0x00
0x4060	12	RFU	Reserved for future use (Fill 0x00)
0x406C	8192	Last 1000 bytes of the .bin file appended with 7192 bytes of 0x00	The last page of application data
0x606C	4	CRC32 of the last page	Calculated CRC32 value for the last page of application data
0x6070	12	RFU	Reserved for future use (Fill 0x00)
0x607C	4	CRC32 of complete .bin file	CRC32 of application
0x6080	4	Length of .bin file	Length of .bin file (0xE8, 0x43, 0x00, 0x00) (17384 as decimal)
0x6084	8184	RFU	Reserved for future use (Fill 0x00)
0x807C	4	CRC32 of application data	Calculated CRC32 value of 8192 bytes starting from 0x607C
0x8080	12	RFU	Reserved for future use (Fill 0x00)
0x808C	4	CRC32 of .msbl file	CRC32 of all data up to this point in the .msbl file

Appendix B: Converting the .bin File to the .msbl File Format

The .msbl file is generated automatically by using a .msbl generator.

Enter the following command in a MinGW® window to convert the .bin application program to a .msbl file:

msblGenWin32.exe myapplication.bin MAX32660 8192 keys.txt

Be sure that the correct linker file is used for generating the .bin file. A sample linker file, max32660.ld, can be found under the Hello_World example folder.

MinGW is a registered trademark of Software in the Public Interest, Inc.

Appendix C: Entering Download Mode in Application

Under normal circumstances, the bootloader checks the boot memory section on flash and jumps to the application if valid. However, there is a special pattern in the boot memory section to make the bootloader stay in bootloader mode after reboot. This special pattern can be used as a signal from an application to make the device enter download mode. The provided pseudo code snippet shows an usage example of boot memory to enter download mode. Actual implementation of the set_boot_mode_and_reset function can be found in the Enter Bootloader example source code.

```
/* Application code listening for enter download mode command */
application_main()
{
    wait_for_cmd();
    if (enter_download_cmd_received()){
        set_boot_mode_and_reset();
    }
}

/* Host code for entering download mode and flashing */
flash_application()
{
    send_enter_download_cmd();
    wait_for_reboot();
    flash_msbl_file();
    /* If flashed successfully, boot_mode will be cleared to jump to app
*/
}
```

Revision History

REVISION NUMBER	REVISION DATE	DESCRIPTION	PAGES CHANGED
0	03/20	Initial release	—