FIRMWARE PATCH LOADING

Product Family: **EM9301**

Part Number: EM9301

Keywords:

Table of Contents

1. INTRODUCTION

The EM9301 is a low-voltage, low-power, fully-integrated, single-chip Bluetooth Low Energy (BLE) controller featuring a low-power physical layer, a link layer with an embedded security engine, a Host/Controller Interface (HCI).
The link layer is controlled by a BLE internal firmware stored in ROM memory. Some parts of this firmware (up to 6KB) can be changed to modify the system behavior.

This document describes the format of the firmware patch hex file, the HCI commands used for loading and checking the firmware patch, and the CRC algorithm used to ensure the patch data have been successfully loaded.

2. FIRMWARE PATCH AND HEX FILE FORMAT

The firmware patch for the EM9301 is provided in the hex file with the following format:
33FFFB
377970
3F3F1C
3EE595
…

Each line as indicated above consists of 3 parts.
The black part contains 8 bits (two highest bits are always zero) and it is marked as MSB. MSB is the most significant byte in the given line (bits 23..16).
The blue part contains 8 bits and it is marked as B1. B1 is the second least significant byte in the given line (bits 15..8).
The red part contains 8 bits and it is marked as B0. B0 is the least significant byte in the given line (bits 7..0).

3. PROGRAMMING COMMANDS

For loading firmware patch three dedicated HCI commands are available in EM9301.
As defined in [BT spec 4.0], the OGF reserved for vendor specific commands is 0x3F.

3.1 HCI_EM_WRITE_PROGRAM

The OCF of this command is 0x80.
This command is available only in ISP (In System Programming) mode.

Command parameters:

Parameter	Size	Description
Row	1	Target row
Sector	1	Target sector
Cache_Bxx	32	Cache content – byte B00 - B31
Cache_MSBxx	16	Cache content – byte MSB00 - MSB16

Return parameters:

Parameter	Size	Description
Status	1	Standard BT error codes

Returned events: Command Complete

3.2 HCI_EM_CALC_CRC_CODE

The OCF of this command is 0x81.
This command is available only in ISP (In System Programming) mode.

Command parameters:

Parameter	Size	Description
Start_address	2	Start address
Stop_address	2	Stop address

Return parameters:

Parameter	Size	Description
Status	1	Standard BT error codes
CRC	2	Calculated CRC

Returned events: Command Complete

3.3 HCI_EM_WRITE_DATA

The OCF of this command is 0x00.

Command parameters:

Parameter	Size	Description
Address	2	Internal register address
Data	1-32	Data to be written

Return parameters:

Parameter	Size	Description
Status	1	Standard BT error codes

Returned events:
Command Complete

4. FIRMWARE PATCH LOADING PROCEDURE

The procedure for loading the firmware patch consists in 4 parts:
1) Enter ISP mode.
2) Load firmware patch.
3) Calculate CRC over loaded patch.
4) Leave ISP mode.

The parameters of the HCI command allowing to enter the ISP mode are different between EM9301V02 and EM9301V01/22. It is therefore important to ensure which version of EM9301 is being used.

4.1 EM9301 VERSION

The EM9301 is available in three hardware versions:
v01: DCDC version which allows operation on a single 1.5V battery cell
v02: noDCDC version which allows operation on a single 3V battery cell
v22: noDCDC version which allows operation on a single 3V battery or other supplies down to 1.9V

For the differences between those versions, please refer to the EM9301 datasheet, or contact EM Microlectronic.

Those versions are differentiated by the package marking (first 2 digits of the 2nd line of the package marking, please refer to the EM9301 datasheet). They can be also identified using the HCI command HCI_READ_LOCAL_VERSION_INFORMATION:

Chip version	HCI_Revision value *	LMP_Subversion value *
02	MSB: 0x06; LSB: 0x19	MSB: 0x06; LSB: 0x19
22	MSB: 0x0b; LSB: 0x92	MSB: 0x25; LSB: 0x00

4.2 ENTERING ISP MODE

The ISP mode is entered by performing following sequence:
1) Send HCI command HCI_EM_Write_Data with parameters:
   -address=0x1FFE
   -data=0x0000 for EM9301v02.
   -data=0xAA55 for EM9301v22.
2) Wait for Command Complete event (expected return code is 0x00).
3) Reset chip by sending HCI_Reset command or asserting RST pad to '1' for a while.
4) Wait for HCI_Hardware_Error event (expected error code is 0x80).

4.3 FIRMWARE PATCH LOADING

16 lines in hex file form one row. One row is the smallest memory element which can be programmed. 64 rows form one sector. The numbering of rows and sectors as follows:

Lines in hex file	Row number	Sector number
0...15	0	0
16...31	1	0
32...47	2	0
...	...	...
1008...1023	63	0
1024...1039	0	1
1040...1056	1	1
...	...	...
2032...2047	63	1

The firmware is loaded by using the HCI_EM_Write_Program command. The parameters of this command shall be formed as follows:

HCI command parameter	Byte/Index	Value
Row	0	row_number (allowed range 0...63)
Sector	0	sector_number (allowed range 0...1)
Cache_Bxx	0	B0 from line N, N = 16*row_number + 1024*sector_number
	1	B1 from line N, N = 16*row_number + 1024*sector_number
	2	B0 from line N, N = 16*row_number + 1024*sector_number + 1
	3	B1 from line N, N = 16*row_number + 1024*sector_number + 1
	...	
	30	B0 from line N, N = 16*row_number + 1024*sector_number + 15
	31	B1 from line N, N = 16*row_number + 1024*sector_number + 15
Cache_MSBxx	0	MSB from line N, N = 16*row_number + 1024*sector_number
	1	MSB from line N, N = 16*row_number + 1024*sector_number + 1
	...	
	15	MSB from line N, N = 16*row_number + 1024*sector_number + 15

4.4 CRC CALCULATION

The CRC polynomial used is CCITT X-25 (0x1021) with initial value of 0xFFFF.

The CRC is calculated in the following way:
1) CRC value is initialized to value 0xFFFF.
2) B0 is submitted to CRC calculator.
3) B1 is submitted to CRC calculator.
4) MSB is submitted to CRC calculator (even if two most significant bits in MSB are always zero they are also submitted to CRC calculator).
5) Loop 2-4 is repeated for other lines from hex file.

There is no padding of data before submitting to CRC calculation, the CRC is updated just for one byte. Submitting data serially means that CRC shift register is shifted 8 times per one byte, and 24 times per one line from hex file.

The CRC calculation using HCI command HCI_EM_Calc_CRC_Code requires two parameters: Start_address and Stop_address. These addresses correspond to line number in hex file.

4.5 LEAVING ISP MODE

The ISP mode is left by performing following sequence:
1) Send HCI command HCI_EM_Write_Data with parameters (address=0x1FFE, data=0x55AA).
2) Wait for Command Complete event (expected return code is 0x00).
3) Reset chip by sending HCI_Reset command or asserting RST pad to '1' for a while.
4) Wait for HCI_EM_Power_Mode_Idle event if chi was reset by RST pad or wait for Command Complete event related to previously sent HCI_Reset command.