78xBT Family Over The Air (OTA) Programming

The 78xBT family is based on a Cypress/Infineon CYBLE-212006-01 AIROC Bluetooth module. This device utilizes the Arm Cortec MO. It contains 256kBytes of FLASH, and 32kBytes of SRAM. It is possible to reprogram the device's FLASH using OTA rather than with a hardwired programmer.

Programming file format
The programming files are provided in the Cypress Application Code (CYACD) format.
Example programming file name "78xBT_1_0_2.cyacd"
(Latest CYCAD firmware file is available at http://60.250.79.19/)

The first line of the file is decoded as Silicon ID (4-bytes), Silicon Revision (1-Byte) and Checksum Type (1-Byte)

For example: 1A6E11AA0000

Silicon ID: 1A6E11AA
Silicon Rev: 00
CS Type: 00

The following shows the second line from the above example programming file. It contains 131 records, each 256 Bytes (0x100) in length.

:0001850100008000201185010 0D1B20100D1B2010010B5024B83F3088802F002FF0080002070
B512222B4B1A6004F01CFA2A4805F06BFF012004F040FA182003F0D7FC274A274B1A60274C
8023DB052360264A116802230B431360254A254B1A600025254B1D60254A136808218B431360
FA20C00003F06EFD214803F0AFFC214A214B1A60214B224A1A60C8214901214A1160214A1A
6080221206204B1A60204B1D6041221F4B1A60013A1F4B1A601F4A1F4B1A601F4B236080221
2011E4B1A601D4B1B681B05FBD4802252001A4B1A60EF3A014B1A6070BD30001040001BB7
000600008004010B400C020B4078002E40D0D000007C002E4064F02E406CF02E40DC050000
FE

Where:
0x000185 - Address
0x0100 - Length Bytes
0x00800020 …. 0000 - Programming Data
0xFE - Checksum (simple sum)

The data is programmed into the FLASH by sending a Send Data (0x37) command, followed by a Program Row (0x39) command. The first WRITE_WITH_RESP_MAX_DATA_SIZE = 133 (0x0085) Bytes are sent using the Send Data, and the remaining with the Program Row. After each set of Data and Row is sent, the Verify Row (0x3A) command is sent.

Application commands are sent using the UUID: 0003cdd4-0000-1000-8000-00805f9b0131
Meter sends measurements using notification with the UUID: 0003cdd5-0000-1000-8000-00805f9b0131
UUID: 00060001-f8ce-11e4-abf4-0002a5d5c51b is used for sending boot loader commands. The boot loader will respond with notifications using this same UUID.

Bootloader commands

PACKET_START = 0x01;
PACKET_END = 0x17;
BASE_CMD_SIZE = 0x07; // PACKET_START (1) + CmdCode(1) + DataLength(2) + Checksum(2) + PACKET_END (1);
WRITE_WITH_RESP_MAX_DATA_SIZE = 133;

Status	Label	Description
0x31	VERIFY_CHECK_SUM	Verify the checksum of the bootloadable project
0x32	Get FLASH size	Get the number of flash rows in the target device
0x34	Erase row	Erases the contents of the specified flash row
0x35	Sync bootloader	Resets the bootloader to a clean state. Any data which was buffered in will be thrown out. This command is needed only if the bootloader and the host go out of sync with each other
0x37	Send data	The received data bytes will be buffered by the bootloader in anticipation of the Program row command.
0x38	Enter bootloader	Silicon ID, 4 bytes;Silicon Rev, 1 byte;Bootloader version, 3 bytes;All the commands are ignored until this command is received.
0x39	Program row	After sending multiple bytes of data to the bootloader using Send data command, the last chunk of data is sent along with this command.
0x3A	Verify row	Returns the checksum of the specified row.
0x3B	Exit bootloader	This command is not acknowledged.

Checksum

Enter Bootloader Example: 01,38,0000,c7ff,17

01 - Packet_Start
38 – Command
0000 - Payload
C7FF - Checksum
17 - Packet_End

Checksum is calculated on the command and payload, 38,00,00. These are converted to unsigned 16-bit values and summed:

0x0038+0x0000+0x0000 = 0x0038

This value is then bitwise inverted to yield 0xFFC7. Finally, this value is byte swapped to form the 16-bit checksum 0xC7FF.

Command: 0x32 - Get FLASH size

Returns the "first row number (2 bytes) and the last row number (2 bytes) of the boot loadable FLASH.

Example: 01,32,010000,ccff,17
Response: 01,00,0400,8501ff01,75fe,17

01 - Packet_Start
00 - Error code
0004 - Length
0185 - First row number, which matches the CYACD programming file's first address of 000185
01ff - Last row number
Fe75 - Checksum
17 - Packet_End

Command: 0x38 – Enter bootloader

All other commands ignored until this is sent.

Example: 01,38,0000,c7ff,17
Response: 01,00,0800,aa116e1a,00,320101,80fe,17

01 - Packet_Start
00 - Error code
0008 - Length (aa,11,6e,1a,00,32,01,01 = 8 bytes,
1A6E11AA = Silicon ID, 00=Silicon Revision, 010132= Bootloader Version)
80fe - Checksum
17 - Packet_End

Command: 0x37 – Send data

The received data bytes will be buffered by the bootloader in anticipation of the Program row command.

01,37,8500,**0080002011850100d1b20100d1b2**
010010b5024b83f3088802f002ff00800020
70b512222b4b1a6004f01cfa2a4805f06bff
012004f040fa182003f0d7fc274a274b1a60
274c8023db052360264a116802230b431360
254a254b1a600025254b1d60254a13680821
8b431360fa20c00003f06efd214803f0affc
214a214b1a60214b224a1a,02d5,17

0x01- Packet_Start,
0x37 - Command,
0x0085 - 133 dec, total number of data Bytes
008000 … 4a1a - data Bytes from CYACD programming file
0xd502 - Checksum
0x17 - Packet_End

Command: 0x39 – Program Row

After sending multiple bytes of data to the bootloader using Send data command, the last chunk of data is sent along with this command.

01,39,7e00,**00850160c8214901214a1160214a**
1a6080221206204b1a60204b1d6041221f4b
802212011e4b1a601d4b1b681b05fbd48022
52001a4b1a60ef3a014b1a6070bd30001040
001bb7000600008004010b400c020b407800
2e40d0d000007c002e4064f02e406cf02e40
dc050000,88e0,17

0x01- Packet_Start,
0x39 - Command,
0x007e - 126 dec, total number of data Bytes
008501 - Address from CYACD file (000185, next row is 000186 and so on)
00C860 …. 0000 - Data Bytes from CYACD programming file
0xe088 - Checksum
0x17 - Packet_End

Command: 0x3A – Verify Row

Returns the Returns the checksum of the specified row.

Example: 01,3a,0300,01ff01,c1fe,17
Response: 01,00010060,9eff,17

Command: 0x31 - Verify Checksum

Verify the checksum value of the bootloadable project.
Example: 01,31,0000,ceff,17
Response: 01,00010001,fdff,17

Command: 0x3B – Exit Bootloader

Exit the bootloader and restart the target program. This command is not acknowledged

Example: 01,3b,0000,c4ff,17

Expected response data bytes

Status	Label	Description
0x00	CYRET_SUCCESS	The command was successfully received and executed
0x02	BOOTLOADER_ERR_VERIFY	The verification of flash failed
0x03	BOOTLOADER_ERR_LENGTH	The amount of data available is outside the expected range
0x04	BOOTLOADER_ERR_DATA	The data is not of the proper form
0x05	BOOTLOADER_ERR_CMD	The command is not recognized
0x06	BOOTLOADER_ERR_DEVICE	The expected device does not match the detected device
0x07	BOOTLOADER_ERR_VERSION	The bootloader version detected is not supported
0x08	BOOTLOADER_ERR_CHECKSUM	The checksum does not match the expected value
0x09	BOOTLOADER_ERR_ARRAY	The flash array ID is not valid
0x0A	BOOTLOADER_ERR_ROW	The flash row number is not valid
0x0C	BOOTLOADER_ERR_APP	The application is not valid and cannot be set as active
0x0D	BOOTLOADER_ERR_ACTIVE	The application is currently marked as active
0x0F	BOOTLOADER_ERR_UNK	An unknown error occurred

Programming sequence

Get BLE firmware version, command 0x0004
Get Model Series ID, command 0x0116
Enter OTA standby mode, command 0x0040 (Once the OTA mode is entered, the DMM will begin to advertise. Program will then need to reconnect to the meter. The password is not resent.)

ENTER_BOOTLOADER, command 0x38
GET_FLASH_SIZE, command 0x32

SEND_DATA, command 0x37
PROGRAM_ROW, command 0x39
VERIFY_ROW, command 0x3A

SEND_DATA, command 0x37
PROGRAM_ROW, command 0x39
VERIFY_ROW, command 0x3A

.
.
.

SEND_DATA, command 0x37
PROGRAM_ROW, command 0x39
VERIFY_ROW, command 0x3A

VERIFY_CHECK_SUM, command 0x31
EXIT_BOOTLOADER, command 0x3B

Once programming is complete, toggle the BLE select on the meter. You should be able to then reconnect with the meter and verify the firmware revision.