Wireless Module Expert

GSM QuecFOTA

Application Note

GSM/GPRS Module Series

Rev. GSM_QuecFOTA_Application_Note_V3.0

Date: 2012-12-05

www.quectel.com

Our aim is to provide customers with timely and comprehensive service. For any assistance, please contact our company headquarter:

Quectel Wireless Solutions Co., Ltd.
Room 501, Building 13, No.99, Tianzhou Road, Shanghai, China, 200233
Tel: +86 21 5108 6236
Mail: info@quectel.com

Or our local office, for more information, please visit:
http://www.quectel.com/quectel_sales_office.html

For technical support, to report documentation errors, please visit:
http://www.quectel.com/tecsupport.aspx

GENERAL NOTES

QUECTEL OFFERS THIS INFORMATION AS A SERVICE TO ITS CUSTOMERS. THE INFORMATION PROVIDED IS BASED UPON CUSTOMERS' REQUIREMENTS. QUECTEL MAKES EVERY EFFORT TO ENSURE THE QUALITY OF THE INFORMATION IT MAKES AVAILABLE. QUECTEL DOES NOT MAKE ANY WARRANTY AS TO THE INFORMATION CONTAINED HEREIN, AND DOES NOT ACCEPT ANY LIABILITY FOR ANY INJURY, LOSS OR DAMAGE OF ANY KIND INCURRED BY USE OF OR RELIANCE UPON THE INFORMATION. ALL INFORMATION SUPPLIED HEREIN ARE SUBJECT TO CHANGE WITHOUT PRIOR NOTICE.

COPYRIGHT

THIS INFORMATION CONTAINED HERE IS PROPRIETARY TECHNICAL INFORMATION OF QUECTEL CO., LTD. TRANSMITTABLE, REPRODUCTION, DISSEMINATION AND EDITING OF THIS DOCUMENT AS WELL AS UTILIZATION OF THIS CONTENTS ARE FORBIDDEN WITHOUT PERMISSION. OFFENDERS WILL BE HELD LIABLE FOR PAYMENT OF DAMAGES. ALL RIGHTS ARE RESERVED IN THE EVENT OF A PATENT GRANT OR REGISTRATION OF A UTILITY MODEL OR DESIGN.

Copyright © Quectel Wireless Solutions Co., Ltd. 2012. All rights reserved.

Quectel Confidential

About the document

History

Revision	Date	Author	Description
3.0	2012-11-29	Bob DENG	Initial

Quectel
Confidential

Contents

Quectel Confidential

Table Index

Quectel
Confidential

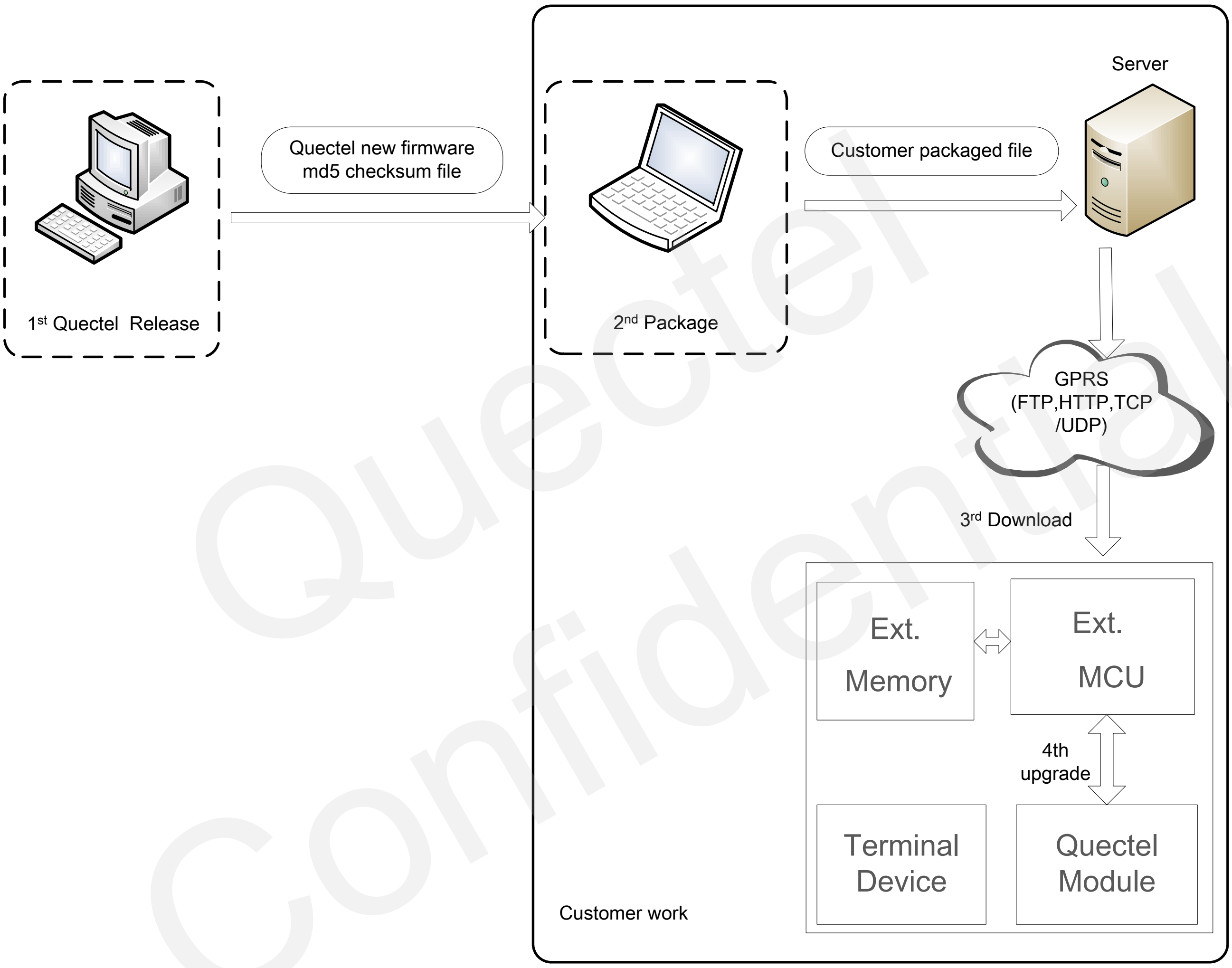
1 Introduction

QuecFOTA provides a solution to update module's firmware by MCU via UART with Quectel protocol. This document describes the procedure of updating. Only Quectel GSM module R2.0 supports QuecFOTA.

Quectel Confidential

2 Overview of QuecFOTA

The QuecFOTA update procedure can be shown as the following Figure 1.

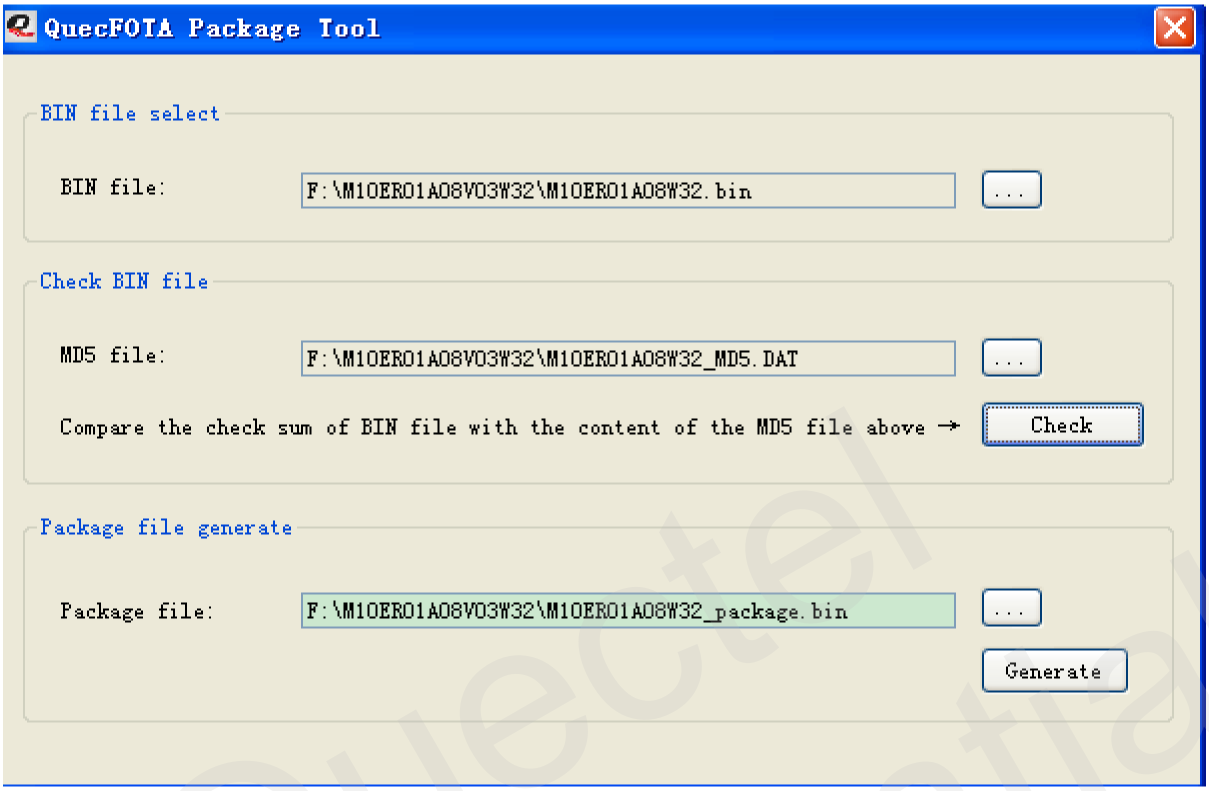


Quectel Confidential

Figure 1: QuecFOTA Overview

2.1. QuecFOTA Release

When you need update the module's firmware, please send the requirements and software version to Quectel via your provider. Quectel will provide appropriate files including new firmware, md5 checksum file and QuceFOTA package tool (As Figure 2: QuecFOTA package tool shown. See the appendix D for more detailed features). For example, M10ER01A08W32.BIN file is new firmware, M10ER01A08W32_MD5.DAT file is the md5 checksum file. You can use “QuecFOTA Package Tool” to check whether the new firmware you received is correct.



BIN file: F:\M10ER01A08V03W32\M10ER01A08W32.bin

MD5 file: F:\M10ER01A08V03W32\M10ER01A08W32_MD5.DAT

Compare the check sum of BIN file with the content of the MD5 file above →

Package file: F:\M10ER01A08V03W32\M10ER01A08W32_package.bin

Figure 2: QuecFOTA Package Tool

2.2. QuecFOTA Package

In the process of downloading and copying, the firmware may be damaged accidentally. So before the new firmware is uploaded to your download server, it is recommended to package the new firmware as the following format with QuecFOTA Package Tool.

Quectel Confidential

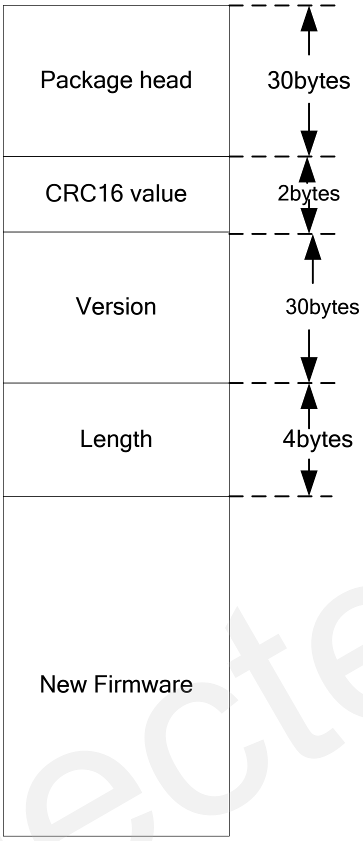


Figure 3: QuecFOTA Package Tool

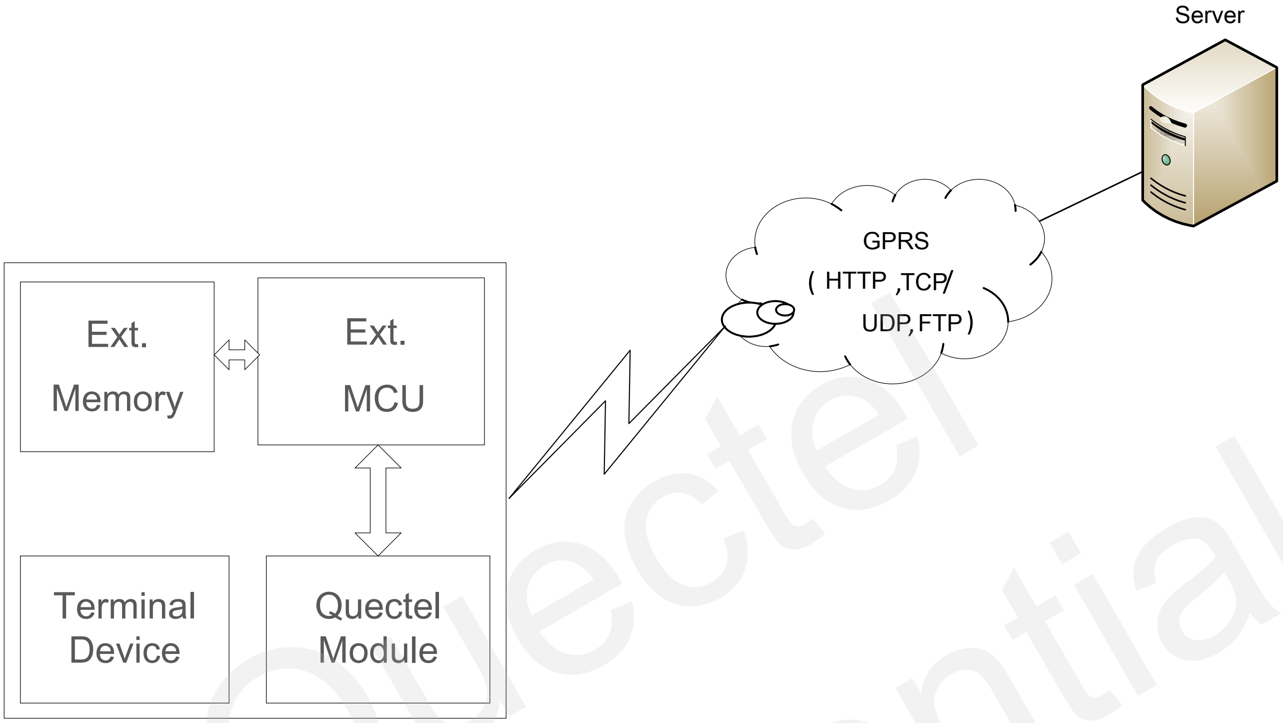
It is necessary to check the completeness and correctness of the new firmware before downloading. The Version field can be used to check the correctness of the new firmware version. The CRC16 field can be used to check the correctness and completeness of the downloaded package after downloading. The CRC16 is calculated with the CRC16 algorithm as Appendix C.

Content	Length(bytes)	Description	Example
Package Head	30	Packet head	“QuectFOTAPackageV0.1\0”, If empty, then fill 0.
CRC16	2	CRC16 checksum value	Including Version, Length and new firmware
Version	30	Version of the new firmware	M10ER01A08W32\0, If empty, then fill 0.
Length	4	Size of the new firmware	
New Firmware	Length	Entire BIN file	M10ER01A08W32.BIN

Quectel Confidential

2.3. Package Downloading

The typical downloading procedure is shown as below:



Quectel
Confidential

Figure 4: Package Download Procedure

- Connection will be established by MCU between Quectel's module and server.
- The packed file will be downloaded from server via TCP/UDP, HTTP or FTP.
- The firmware will be stored in external memory of MCU.
- MCU check the completeness and correctness of the package file with checksum and version in the package file.

2.4. QuecFOTA Upgrade

In this step, MCU will transfer the new firmware from the external memory to the flash of module. Figure 5 is the data roadmap of the QuecFOTA Upgrade. Please refer to chapter 3 for the detailed QuecFOTA Upgrade process.

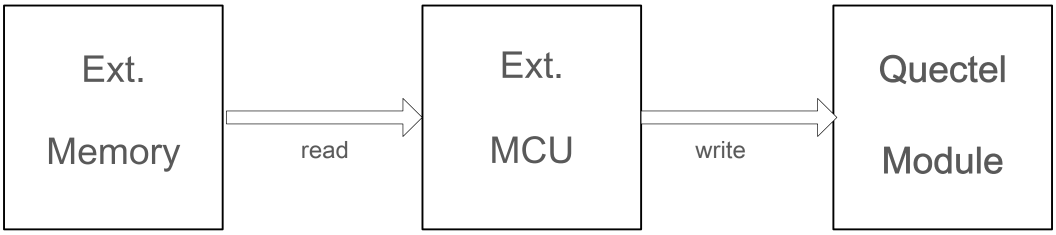


Figure 5: QuecFOTA Upgrade data road map

The following Figure 6 is the overview of QuecFOTA Upgrade.

Quectel
Confidential

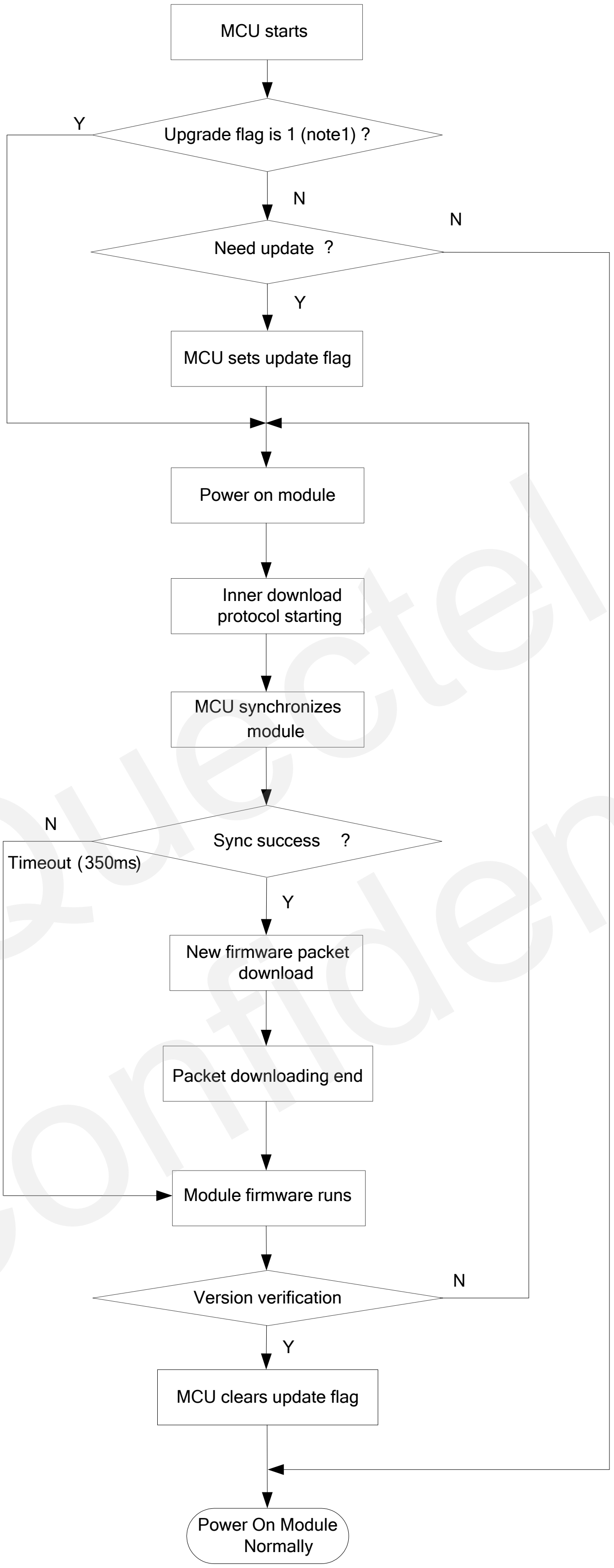


Figure 6: QuecFOTA Upgrade Flow Chart

Quectel Confidential

NOTES

When the upgrade aborted, the MCU needs to perform note1.The abnormal status refers to 3.3.

The update process shall follow these sequences:

- MCU sets upgrade flag
- MCU sends Sync Word.
- Power on the module and keep the PWRKEY in a low during the upgrading process.
- Module is in updating process after receiving the Sync Word sent by MCU.
- Data exchange ends once the firmware downloading has been completed.
- Module Run with new firmware.
- MCU checks the module software version.
- If the software version is right, MCU clear the upgrade flag.
- Normal power on module.

Quectel Confidential

3 QuecFOTA Upgrade Process

The update process includes two steps: QuecFOTA Sync and QuecFOTA Packet. To update the firmware, MCU must synchronize module and let the module enter into command mode. This step is named as QuecFOTA Sync. Then MCU packets the new firmware and sends the packet to the module. This step is named as QuecFOTA Packet.

3.1. QuecFOTA Sync

As Figure 7 shows, the new firmware is stored in the flash of MCU. MCU updates the module's firmware based on the download protocol via the module's UART.

The UART hardware parameter is illustrated as bellow:

- Baud rate: 115200
- Data bit: 8
- Stop bit: 1
- Parity bite: None
- Flow control: Disabled

Quectel Confidential

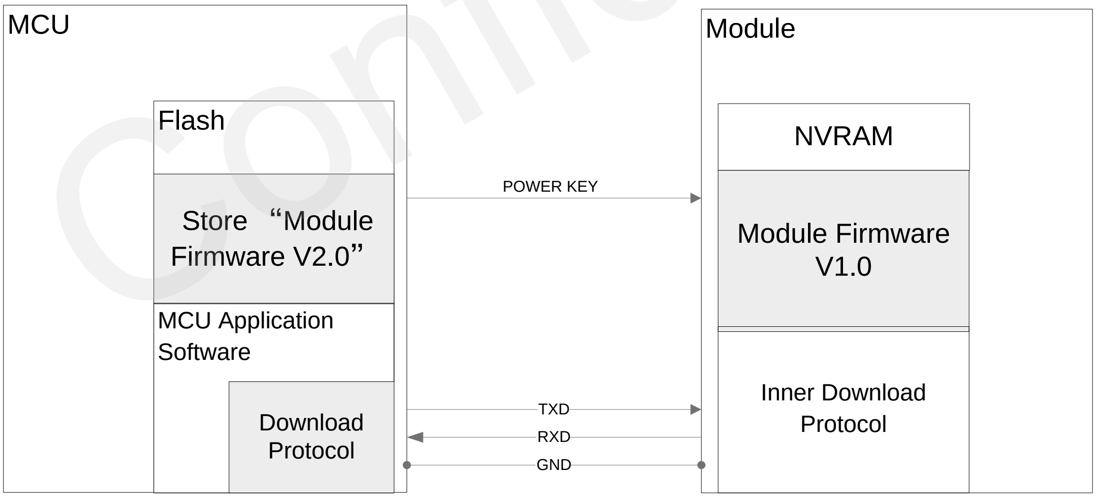


Figure 7: QuecFOTA Sync Framework

The following Figure is QuecFOTA Sync sequence. Firstly, MCU will continuously send SYNC_WORD1 to the module via UART at interval of 20ms. And then powers on the module. With these SYNC_WORD signals, the MCU and module will get synchronized. MCU should discard the unexpected data (such as 0xB6 etc.) sent by module. When the module returns SYNC_WORD_RSP1, MCU sends SYNC_WORD2 and the module responds with SYNC_WORD_RSP2. The baud rate of the interface should be set as 115200. After that, the module will enter into "Command Mode". If the module cannot receive the "synchronous sequence" or finish synchronous negotiation, the module will run the firmware that has been stored in the module.

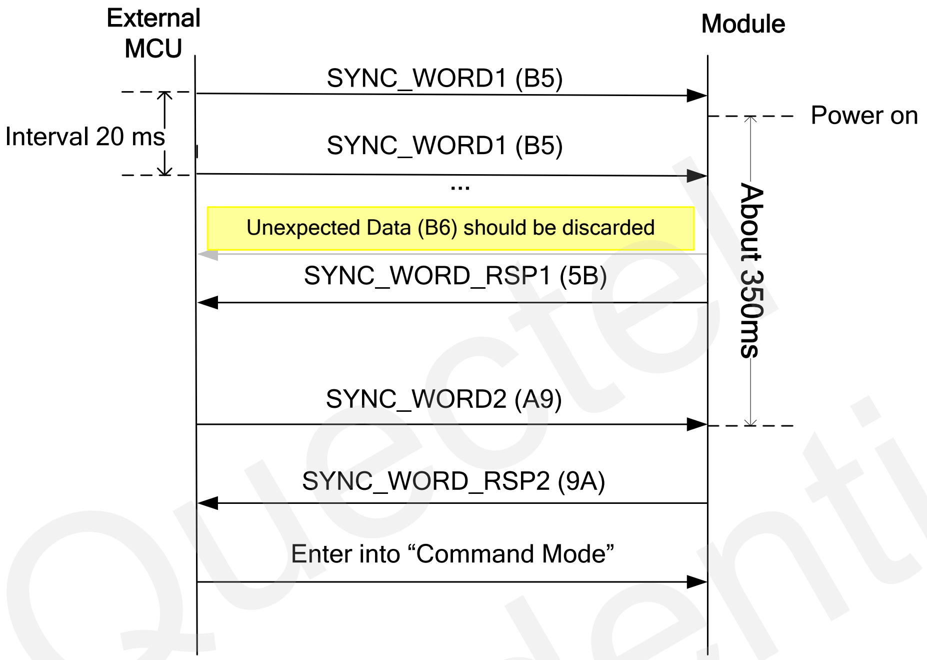


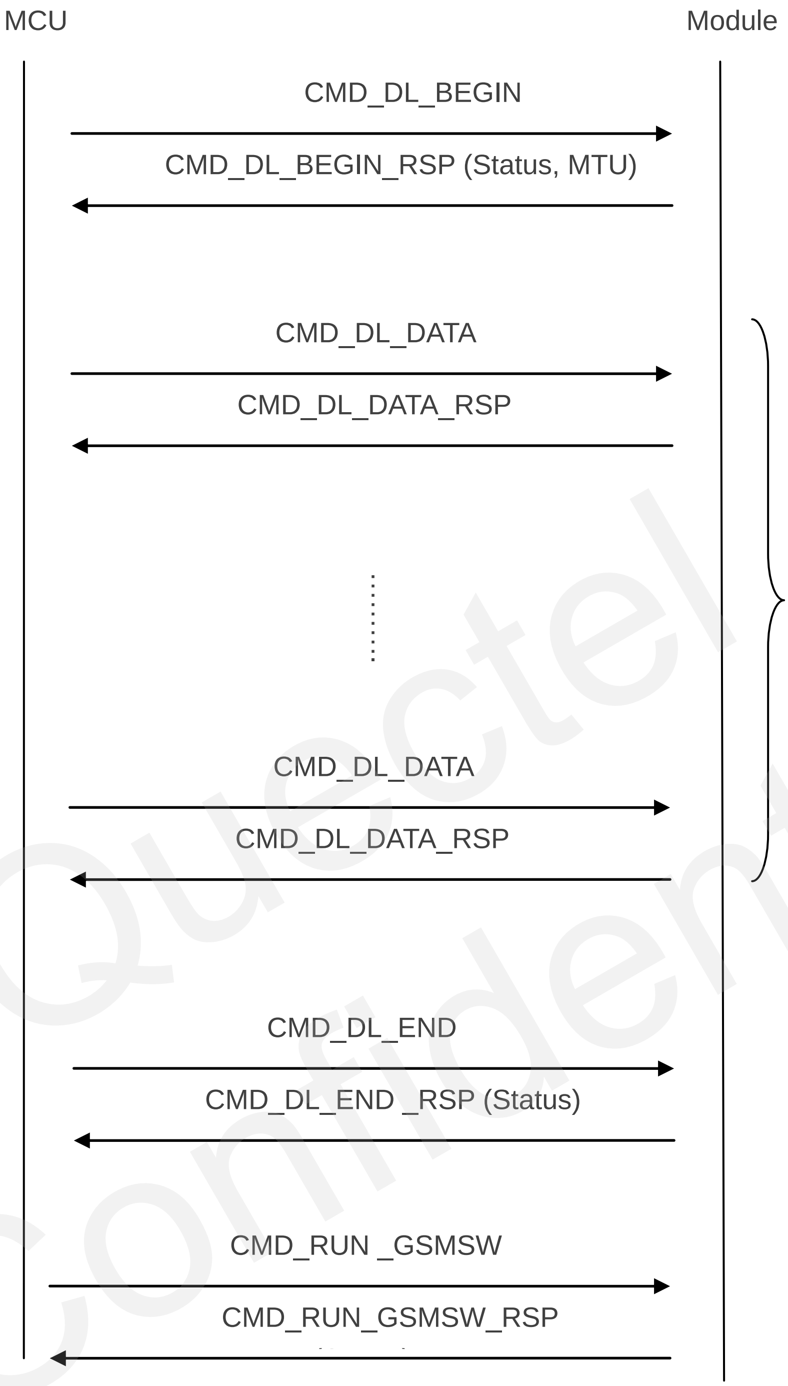
Figure 8: QuecFOTA Sync Sequence

3.2. QuecFOTA Packet

After the module enters into the "Command mode", MCU will packet the new firmware and download the new firmware into the module. QuecFOTA Packet is generated by MCU and the data frame should follow the package type and format. The Annex A is QuecFOTA packet's detailed definition.

In the "Command mode", the MCU can send packets to upgrade the firmware. If MCU does not send any commands, the module will be in the "Command mode" all the time. The Figure 9 is QuecFOTA Upgrade Sequence.

Quectel Confidential



Quectel Confidential

Figure 9: QuecFOTA Upgrade Sequence

Firstly, MCU sends CMD_DL_BEGIN to module and then module returns the CMD_DL_BEGIN_RSP.

Secondly, MCU packs the firmware data (including sequence number and data block) into a data packet and then sends the data packet to the module. The value of the sequence number starts from 0. After the module received the data packet and verified the data has been written successfully, it will return CMD_DL_DATA_RSP (Status=0). Then MCU can send the next data packet. If the module returns

CMD_DL_DATA_RSP (Status=1 or Status=4), MCU must resend the specified data packet. If the module returns CMD_DL_DATA_RSP (Status=2), it means the Flash is error. The MCU must power on the module and re-upgrade the firmware. MCU will read and send the data block of the application software in turn. The length of the other data block must be aligned in even-type, except the last data block.

After MCU downloaded all firmware data packet, it will send CMD_DL_END to module, which means the firmware downloading is finished. The module will return CMD_DL_END_RSP and exit from download mode.

After MCU finished the downloading process, it will inform the module to run the new firmware by sending CMD_RUN_GSMSW to module. Then module will return CMD_RUN_GSMSW_RSP and run the firmware.

NOTE

If MCU fails to receive the response message from module in 3 seconds after sending a command package, the MCU should resend that command package. If MCU does not receive the right response message from the module after sending the same command package for 3 times, the MCU must power off the module and restart the upgrade procedure.

Quectel Confidential

3.3. QuecFOTA Upgrade Error Handle

Possible reasons for firmware updating failure in the QuecFOTA Upgrade Process are as below:

- Power supply is interrupted
- PWRKEY is released during the upgrading process

In these cases, the firmware update process is interrupted and the module’s firmware is invalid. Meanwhile, the module cannot work normally. MCU must restart to upgrade the new firmware and go to the note1 in the Figure-6 QuecFOTA Upgrade Flow Chart.

- Data packet transfer error
- Flash data writing error

If the data or flash error occurred during the upgrading process, MCU must perform error handling process according to the status values. The following figure is the detailed QuecFOTA Upgrade Error Handle Flow Chart.

Please refer to 5.4 for the Status value.

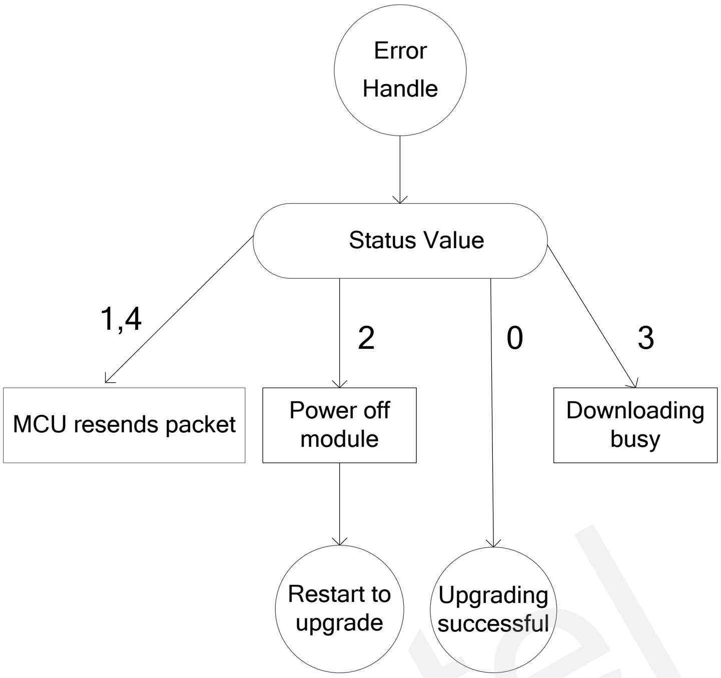


Figure 10: QuecFOTA Upgrade Error Handle Flow Chart

Quectel Confidential

4 Appendix A Reference

Table 1: Terms and Abbreviations

Abbreviation	Description
FOTA	Firmware Over-the-Air
FW	Firmware
Ext.	Extern

Quectel Confidential

5 Appendix B Definition of QuecFOTA Packet

5.1. Format of packet

Table 2: The format of packet:

Head	Type	Length	Data	CRC16
1 byte (0xAA)	2 byte	2 byte	N byte	2 byte

The value of “length” means the length of the data field, which does not include the length of CRC16 whose length is two bytes. The checksum range consists of “Type” field, “Data Length” field and “Data” field.

NOTES

CRC16 Polynomial: CRC-16-CCITT x16 + x12 + x5 + 1.

Quectel Confidential

5.2. Command list

Table 3: Command list

Type	Cmdid	Description	Direction
CMD_DL_BEGIN	0x0001	Begin to download	MCU to Module
CMD_DL_BEGIN_RSP	0x0002	Response to beginning downloading	Module to MCU
CMD_DL_DATA	0x0003	Download data	MCU to Module
CMD_DL_DATA_RSP	0x0004	Response to data downloading	Module to MCU

CMD_DL_END	0x0005	End Downloading	MCU to Module
CMD_DL_END _RSP	0x0006	Response to data downloading ends	Module to MCU
CMD_RUN _GSMSW	0x0007	Require to run application software	MCU to Module
CMD_RUN_GSMSW_RSP	0x0008	Response to running application software	Module to MCU

5.3. Description of Command field

5.3.1. CMD_DL_BEGIN

The length of the data field is defined by the data length field. The content of the data field is defined as below:

Content	Bytes	Description
Application software version data	4	Reserve

Example:
Application software version is 1, and the data packet of the command CMD_DL_BEGIN is shown as below:
0xAA 0x00 0x01 0x00 0x04 x00 0x00 0x00 0x01 0xXX 0xXX

Content	Description
0xAA	Packet head
0x00 0x01	CMD_DL_BEGIN command ID
0x00 0x04	Data length
0x00 0x00 0x00 0x01	Application software version data. Recommend using the default value
0xXX 0xXX	CRC16 value

5.3.2. CMD_DL_BEGIN_RSP

The length of the data field is defined by the data length field. The content of the data field is defined as below:

Quectel Confidential

Content	Bytes	Description
Status	2	Refer to the definition list
MTU	2	The maximum length of command package that module can receive

NOTES

1. Status means whether the module receives the download request.
2. MTU means the maximum length of command package that the module received at a time (the length value consists packer head field, command ID field, length field, data field and CRC field).

Quectel Confidential

Example:
The following is the data package of CMD_DL_BEGIN_RSP. Its status is 0 and MTU is 8224byptes (8K+32).

0xAA 0x00 0x02 0x00 0x04 0x00 0x00 0x20 0x20 0xXX 0xXX

Content	Description
0xAA	Packet head
0x00 0x02	CMD_DL_BEGIN_RSP command ID
0x00 0x04	Data length
0x00 0x00	Status value, please refer “5.4 Definition list”
0x20 0x20	MTU is 8224 in decimal
0xXX 0xXX	CRC16 value

5.3.3. CMD_DL_DATA

The length of the data field is defined by the data length field. The content of the data field is defined as below:

Content	Bytes	Description
Sequence number	4	The sequence number of Module’s data package and begins from 0.

Module data	N-4 bytes	Module data; N is the data length of the command packet.

Example:
The following is the data package of the command CMD_DL_DATA which means Sequence number is 244 and the length of module data is 1024bytes.
0xAA 0x00 0x03 0x04 0x04 0x00 0x00 0x00 0xF4 0xXX 0xXX 0xXX... (1024 bytes) 0xXX 0xXX

Content	Description
0xAA	packet head
0x00 0x03	CMD_DL_DATA command ID
0x04 0x04	Data length 1028 bytes. Note lengths include “Sequence number”4 bytes.
0x00 0x00 0x00 0xF4	Sequence number 244
0xXX 0xXX 0xXX...(1024 bytes)	1024 bytes data
0xXX 0xXX	CRC16 value

NOTES

1. Sequence number: 0x00 0x00 0x00 0xF4.
2. Module Data: 0xXX 0xXX 0xXX... (1024 bytes).
3. Module data Length = (Len) N - (Sequence number Length) 4.
4. Module data requirements for two-byte alignment.
5. If it is not a two-byte alignment, fill 0xff.6. The total length of packet head filed, command ID filed，length filed, sequence number filed, data filed and CRC16 field does not exceed the MTU.

Quectel Confidential

5.3.4. CMD_DL_DATA_RSP

The length of the data field is defined by the data length field. The content of the data field is defined as below:

Content	Bytes	Description
Status	2	Refer to definition list
Next sequence number	4	

Example:
The data package of CMD_DL_DATA_RSP is shown as below. Its status is 0 and the next sequence number is 245.
0xAA 0x00 0x04 0x00 0x06 0x00 0x00 0x00 0x00 0x00 0xF5 0xXX 0xXX

Content	Description
0xAA	Packet head
0x00 0x04	CMD_DL_DATA_RSP command ID
0x00 0x06	Data length
0x00 0x00	Status value, please refer “5.4 Definition list”
0x00 0x00 0x00 0xF5	Next sequence number
0xXX 0xXX	CRC16 value

5.3.5. CMD_DL_END

The command does not have data field. The length of data field is 0.

Example:
The data package of the command CMD_DL_END is shown as below:
0xAA 0x00 x05 0x00 0x00 0xXX 0xXX

Content	Description
0xAA	Packet head
0x00 0x05	CMD_DL_END command ID
0x00 0x00	Data length is 0
0xXX 0xXX	CRC16 value

5.3.6. CMD_DL_END_RSP

The length of the data field is defined by the data length field. The content of the data field is defined as

Quectel Confidential

below:

Content	Bytes	Description
Status	2	Refer to the definition list

Example：
The following is the data package of CMD_DL_END_RSP whose status is 0.
0xAA 0x00 0x06 0x00 x02 0x00 0x00 0xXX 0xXX

Content	Description
0xAA	Packet head
0x00 0x06	CMD_DL_END_RSP command ID
0x00 0x02	Data length is 2 bytes
0x00 0x00	Status value, please refer “5.4 Definition list”
0xXX 0xXX	CRC16 value

5.3.7. CMD_RUN_GSMSW

The command does not have data field. The length of data field is 0.

Example:
The data package of CMD_RUN_GSMSW is shown as below:
0xAA 0x00 0x07 0x00 0x00 0xXX 0xXX

Content	Description
0xAA	Packet head
0x00 0x07	CMD_RUN_GSMSW command ID
0x00 0x00	Data length is 0
0xXX 0xXX	CRC16 value

Quectel Confidential

5.3.8. CMD_RUN_GSMSW_RSP

Content	Bytes	Description
Status	2	Refer to the definition list

Example:
The data package of CMD_RUN_GSMSW_RSP whose status is 3 is shown as below:
0xAA 0x00 0x08 0x00 0x02 0x00 0x03 0xXX 0xXX

Content	Description
0xAA	Packet head
0x00 0x08	CMD_RUN_GSMSW_RSP command ID
0x00 0x02	Data length is 2 bytes
0x00 0x03	Status value, please refer "5.4 Definition list"
0xXX 0xXX	CRC16 value

Quectel Confidential

5.4. Definition list

Status value	Description	Response
0	Success	
1	CRC16 error	MCU retransmits the response sequence number.
2	Flash error	MCU restarts module, and downloads the application software again.
3	Module is in download mode.	
4	Data package error	MCU retransmits the response sequence number.

6 Appendix C CRC-16 Algorithms

6.1. CRC-16-CCITT Coding Table

```
__align (4) unsigned short CRC16_CCITT_tbl [256] = {
0x0,0x1021,0x2042,0x3063,0x4084,0x50a5,0x60c6,0x70e7,0x8108,0x9129,0xa14a,0xb16b,0xc18c,
0xd1ad,0xe1ce,0xf1ef,0x1231,0x210,0x3273,0x2252,0x52b5,0x4294,0x72f7,0x62d6,0x9339,0x8318,
0xb37b, 0xa35a, 0xd3bd, 0xc39c, 0xf3ff,
0xe3de,
0x2462,0x3443,0x420,0x1401,0x64e6,0x74c7,0x44a4,0x5485,0xa56a,0xb54b,0x8528,0x9509,0xe5ee,0
xf5cf,0xc5ac,0xd58d,
0x3653,0x2672,0x1611,0x630,0x76d7,0x66f6,0x5695,0x46b4,0xb75b,0xa77a,0x9719,0x8738,0xf7df,0xe
7fe,0xd79d,0xc7bc,
0x48c4,0x58e5,0x6886,0x78a7,0x840,0x1861,0x2802,0x3823,0xc9cc,0xd9ed,0xe98e,0xf9af,0x8948,0x
9969,0xa90a,0xb92b,
0x5af5,0x4ad4,0x7ab7,0x6a96,0x1a71,0xa50,0x3a33,0x2a12,0xdbfd,0xcbdc,0xfbbf,0xeb9e,0x9b79,0x8
b58,0xbb3b,0xab1a,
0x6ca6,0x7c87,0x4ce4,0x5cc5,0x2c22,0x3c03,0xc60,0x1c41,0xedae,0xfd8f,0xcdec,0xddcd,0xad2a,0xb
d0b,0x8d68,0x9d49,
0x7e97,0x6eb6,0x5ed5,0x4ef4,0x3e13,0x2e32,0x1e51,0xe70,0xff9f,0xefbe,0xdfdd,0xcffc,0xbf1b,0xaf3a,
0x9f59,0x8f78,
0x9188,0x81a9,0xb1ca,0xa1eb,0xd10c,0xc12d,0xf14e,0xe16f,0x1080,0xa1,0x30c2,0x20e3,0x5004,0x4
025,0x7046,0x6067,
0x83b9,0x9398,0xa3fb,0xb3da,0xc33d,0xd31c,0xe37f,0xf35e,0x2b1,0x1290,0x22f3,0x32d2,0x4235,0x5
214,0x6277,0x7256,
0xb5ea,0xa5cb,0x95a8,0x8589,0xf56e,0xe54f,0xd52c,0xc50d,0x34e2,0x24c3,0x14a0,0x481,0x7466,0x
6447,0x5424,0x4405,
0xa7db,0xb7fa,0x8799,0x97b8,0xe75f,0xf77e,0xc71d,0xd73c,0x26d3,0x36f2,0x691,0x16b0,0x6657,0x7
676,0x4615,0x5634,
0xd94c,0xc96d,0xf90e,0xe92f,0x99c8,0x89e9,0xb98a,0xa9ab,0x5844,0x4865,0x7806,0x6827,0x18c0,0
x8e1,0x3882,0x28a3,
0xcb7d,0xdb5c,0xeb3f,0xfb1e,0x8bf9,0x9bd8,0xabbb,0xbb9a,0x4a75,0x5a54,0x6a37,0x7a16,0xaf1,0x1
ad0,0x2ab3,0x3a92,
0xfd2e,0xed0f,0xdd6c,0xcd4d,0xbdaa,0xad8b,0x9de8,0x8dc9,0x7c26,0x6c07,0x5c64,0x4c45,0x3ca2,0x
2c83,0x1ce0,0xcc1,
0xef1f,0xff3e,0xcf5d,0xdf7c,0xaf9b,0xbfba,0x8fd9,0x9ff8,0x6e17,0x7e36,0x4e55,0x5e74,0x2e93,0x3eb2
,0xed1,0x1ef0};
```

Quectel Confidential

6.2. Calculate the CRC Value

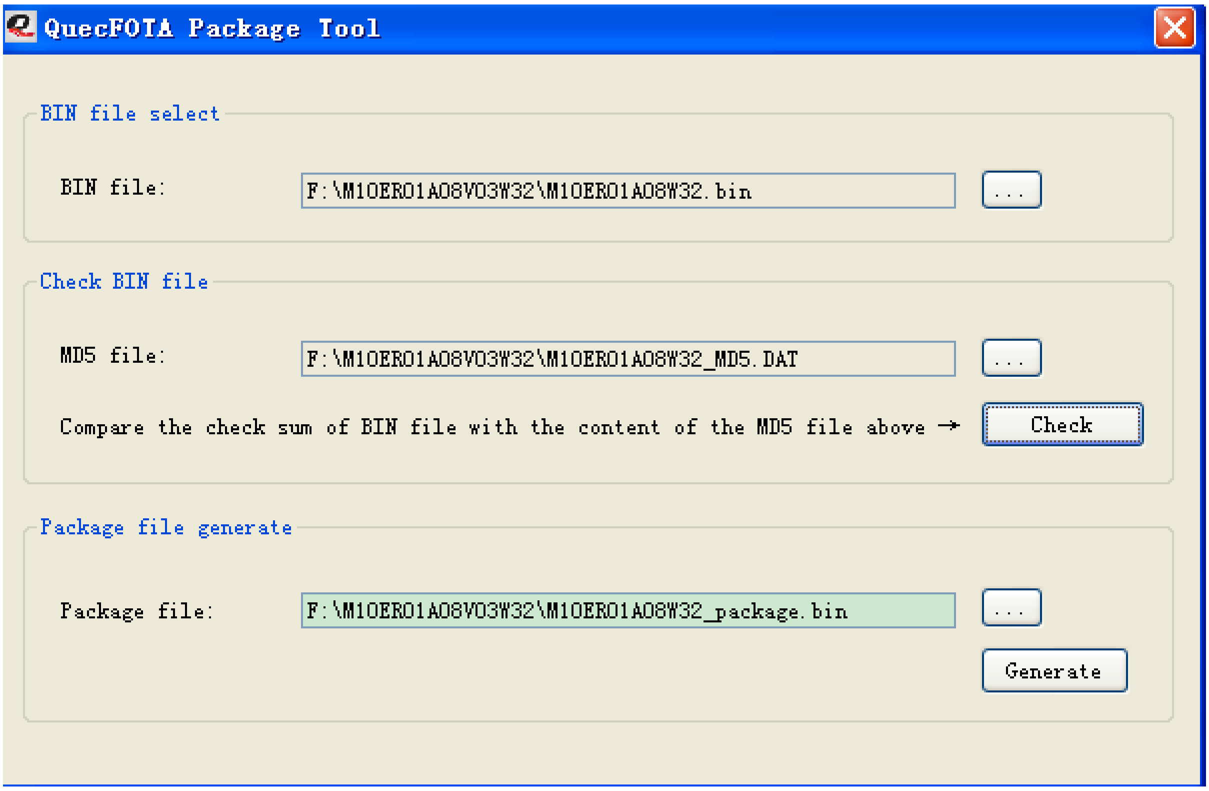
```
void calculate_crc16(unsigned char*    aData, unsigned short  aSize, unsigned char*    Higher,
unsigned char*   Lower)
{
     unsigned short   i;
     unsigned short nAccum = 0;

     for ( i = 0; i < aSize; i++ )
          nAccum = ( nAccum << 8 ) ^ ( unsigned short )CRC16_CCITT_tbl[(( nAccum >> 8 ) ^
*aData++)&0xff];

     *Higher = (unsigned char)((nAccum>>8) & 0xff);
     *Lower = (unsigned char)((nAccum) & 0xff);
}
unsigned long CalculateCRC16(unsigned char*ptr,   unsigned long len)
{
    unsigned char Higher = 0;
    unsigned char Lower = 0;
    calculate_crc16(ptr,len,&Higher,&Lower);
    return (((0x00000000 | Higher) << 8) | Lower);
}
```

6.3. Example

```
unsigned long new_CRC16_value = 0;
new_CRC16_value = CalculateCRC16 ((unsigned char*)pData, nLength);
if(org_CRC16_value != new_CRC16_value)
{
    //CRC checksum failed
    return -1;
}
    else
{
    //CRC checksum successful
    return 0;
}
```

Quectel
Confidential

7 Appendix D QuecFOTA Tool



QuecFOTA Package Tool

BIN file select

BIN file: F:\M10ER01A08V03W32\M10ER01A08W32.bin

Check BIN file

MD5 file: F:\M10ER01A08V03W32\M10ER01A08W32_MD5.DAT

Compare the check sum of BIN file with the content of the MD5 file above →

Package file generate

Package file: F:\M10ER01A08V03W32\M10ER01A08W32_package.bin

Figure 11: QuecFOTA Package Tool

The QuecFOTA package tool has three parts:

- First part is “BIN file select”. Take the M10ER01A08W32.BIN file as an example.
- Second part is “Check BIN file”. Check whether BIN is correct or not with MD5 file. For example, select the M10ER01A08W32_MD5.DAT, then push “Check” button to check whether the M10ER01A08W32.BIN is correct or not.
- Third part is “Package file generate”. Generate the QuecFOTA package file”.
  First, you can type “M10ER01A08W32_package.bin”, then push “Generate” button to generate the M10ER01A08W32_package.bin file with the M10ER01A08W32.BIN file.