nanotron
TECHNOLOGIES

**swarm bee LE Firmware
Update Native Serial**

AN0507

Document Information

Document Title:	swarm bee LE Firmware Update Native Serial
Document Version:	AN0507
Current Date:	2014-11-04
Print Date:	2014-11-04
Document ID:	NA-14-0267-0017-1.0
Document Author:	Nanotron Technologies

Disclaimer

Nanotron Technologies GmbH believes the information contained herein is correct and accurate at the time of release. Nanotron Technologies GmbH reserves the right to make changes without further notice to the product to improve reliability, function or design. Nanotron Technologies GmbH does not assume any liability or responsibility arising out of this product, as well as any application or circuits described herein, neither does it convey any license under its patent rights.

As far as possible, significant changes to product specifications and functionality will be provided in product specific Errata sheets, or in new versions of this document. Customers are encouraged to check the Nanotron website for the most recent updates on products.

Trademarks

All trademarks, registered trademarks, and product names are the sole property of their respective owners.

This document and the information contained herein is the subject of copyright and intellectual property rights under international convention. All rights reserved. No part of this document may be reproduced, stored in a retrieval system, or transmitted in any form by any means, electronic, mechanical or optical, in whole or in part, without the prior written permission of nanotron Technologies GmbH.

Copyright © 2014 nanotron Technologies GmbH.

Contents

1. General introduction

A standard *swarm* bee LE module is delivered with the latest firmware on the day of the swarm bee module production. Firmware update is possible through the bootloader via a USB-to-serial converter cable or via its native serial interface through a host controller. When the swarm is embedded in a custom system only the second option is possible.

This document provides a guide on how to update the firmware on a *swarm* bee LE module via the native serial interface. The following chapters show the required resources and neccesary steps.

2. What is a Bootloader?

The bootloader is integrated in the firmware of all swarm bee LE modules and it is the piece of software that takes care of the firmware initialization.
During initialization of the module (after it is powered or reseted) the bootloader checks the first RTC backup register. Depending on the value of this register it will know whether the firmware on the board is correct or its update was not complet. If is correct it goes to the memory address where the application starts. The module will start then operating.

There are three ways the module can be set in bootloader mode:

1. If during initialization, the bootloader detects the firmware was not correctly updated it directly goes to bootloader mode.

2. In the hardware: if during initialization the UART RX line is held low for more than 100ms a break condition will occur and the module will go on bootloader mode.

3. In software: the API command **bldr** sent by the host controller

2.1. Bootloader Commands

Once the module is in bootloader mode, it can be contolled via a terminal software. The bootloader command line can be recognized when a question mark (?) is shown as a prompt character. The following commands are available to operate with teh bootloader:

- **help:** prints out the list of supported commands
- **info:** prints out the current firmware version
- **xmld:** starts an xmodem protocol session and waits for an appropriate xmodem command that starts the transmission of a firmware-image. When the image is successfully received it is decrypted and written to the appropriate address.
- **erfl:** erases the flash memory
- **boot:** goes out of bootloader mode by starting the installed firmware (i.e. setting the instruction pointer to the start address of the firmware-image).

3. What is XMODEM-CRC protocol?

XMODEM-CRC is a file tranfer protocol widely used due to its simplicity. It breaks up the original data into a series of packets and sends them one by one.
Each packet consist of:
       3-byte header: <SOH>
       packet number from 1 to 255
       'inverse' packet number: 255 - packet number
       payload:128 bytes of the actual file
       16-bit CRC

The transmission is receiver–driven and it occurs as follows:
- The sender waits for a signal from the receiver.

- The receiver sends and NACK (not-acknowledgement).
- When the sender receives the NACK it starts the transmission of packets one by one. It takes the first block, calculates the CRC, and creates the first packet. It sends the packet and waits.
- The receiver receives the packet. It checks the CRC and the block number.
  - o   If both are correct it sends back an ACK (acknowledgement) and waits for next packet
  - o   If one of them is not correct it sends a NACK and waits for the appropiate packet.
- When the sender receives the ACK sends the next packet. If it receives and NACK sends again the corresponding packet.
- After the last packets has been sent and acknowledged, the sender sends an EOT (end of transmission)
- The receiver finalises with an ACK

A typical file transmission is reprensented in Figure 1. The file is 612 bytes long, thus the last packet is completed with zeros.

```
    SENDER                                    RECEIVER

                                    <--   NACK
    SOH 01 FE Data[128] CRC         -->
                                    <--   ACK
    SOH 02 FD Data[128] CRC         -->
                                    <--   ACK
    SOH 03 FC Data[128] CRC         -->
                                    <--   ACK
    SOH 04 FB Data[128] CRC         -->
                                    <--   ACK
    SOH 05 FA Data[100] CPMEOF[28] CRC  -->
                                    <--   ACK
    EOT                             -->
                                    <--   ACK
```

Figure 1. Typical file transmission in XMODEM

# 4. Firmware Update via UART

The user should write its own application running in the host controller to send the new firmware image through the UART using XMODEM-CRC protocol. Said application should follow the next steps:

1. Send command *bldr*
This will put the the swarm radio in bootloader mode by sending

2. Send command *xmld*
It starts a XMODEM communication with the swarm radio as a receiver.

3. Wait untill the receiver indicates the start of the transmission by sending a NACK.

5. Transmit the new firmware image to the swarm following the XMODEM-CRC protocol (chapter 3).

6. Send command *boot*
After the EOT has been sent and its corresponding ACK received the host should send the command boot, so that the swarm will restart with the new firmware.
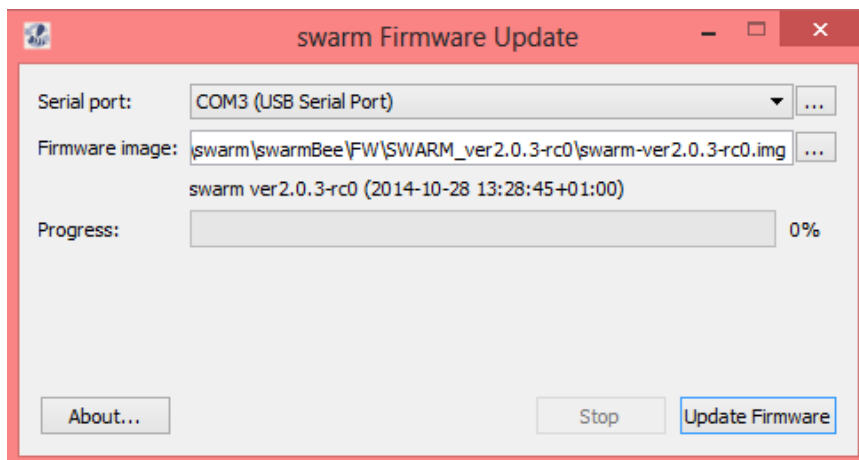
5. Firmware Update via USB

The process to update the firmware via the USB port has been considerably simplified by the 'swarm Firmware Update' software. The steps to use it are the following:

1. Connect the swarm to the PC via the USB

2. Open 'swarm Firmware Update' by executing swarm-fwupdate.exe
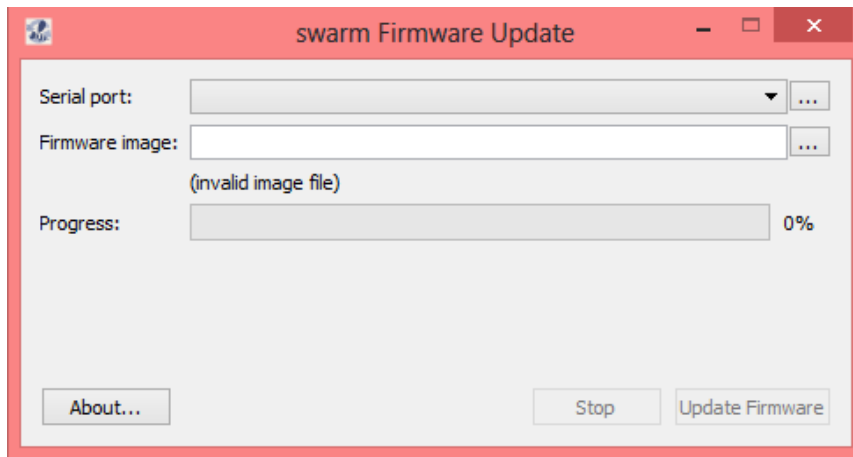
3. Select the serial port

4. Browse for the firmware image to be flashed into the swarm

5. Once both the serial port and the image have been selected the 'Update Firmware' button will be active. When this button is pressed the firmware update starts.

6. When the Progress bar is completely green the firmware update is finished.

End of Document

Document History

Date	Authors	Version	Description
2014-09-30			How to update the swarm firmware through the native serial interface using the host controller

Life Support Policy

These products are not designed for use in life support appliances, devices, or systems where malfunction of these products can reasonably be expected to result in personal injury. Nanotron Technologies GmbH customers using or selling these products for use in such applications do so at their own risk and agree to fully indemnify nanotron Technologies GmbH for any damages resulting from such improper use or sale.

About Nanotron Technologies GmbH

Nanotron Technologies is a leading provider of wireless products that help to *protect* and *find* people, animals and valuable assets. They create highly accurate location information and energy-efficiently transmit data with a single, low-cost chip. Nanotron's technology is patent-protected and follows ISO and IEEE standards for global asset tracking. Nanotron's solutions are used in a wide range of applications and industry verticals including child safety in public places, livestock monitoring & management, mine safety, virtual fencing and transit yard management. Nanotron's products are available on two distinct platforms: *protect* and *find*. The *protect* platform monitors proximity. The *find* platform locates people, animals and valuable assets. Both platforms create reliable and efficient visibility. Nanotron supports its customers and channel partners to adapt the *protect* and *find* products to the needs of their vertical markets.

Further Information

For more information about products from nanotron Technologies GmbH, contact a sales representative at the following address:

nanotron Technologies GmbH
Alt-Moabit 60
10555 Berlin, Germany
Phone: +49 30 399 954 – 0
Fax: +49 30 399 954 – 188
Email: sales@nanotron.com
Internet: www.nanotron.com