Firmware Upgrade Application User Guide

Application Note for 32-bit NuMicro®Family

Document Information

Abstract	Demonstratehow to implement the firmware upgrade application under the M2L31 architecture.
Apply to	NuMicro® M2L31 Series.

The information described in this document is the exclusive intellectual property of
Nuvoton Technology Corporation and shall not be reproduced without permission from Nuvoton.

Nuvoton is providing this document only for reference purposes of NuMicromicrocontroller based system design.
Nuvoton assumes no responsibility for errors or omissions.

All data and specifications are subject to change without notice.

For additional information or questions, please contact: Nuvoton Technology Corporation.

www.nuvoton.com

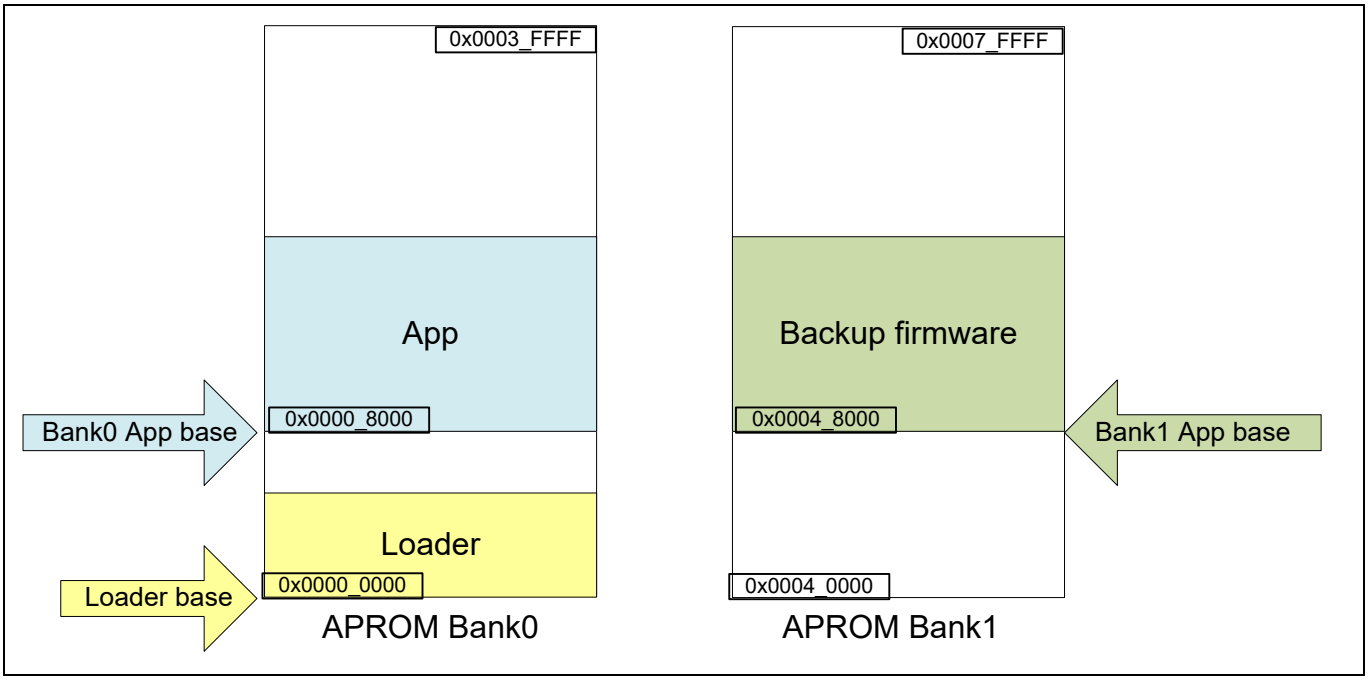
Table of Contents

1 Sample CodeIntroduction

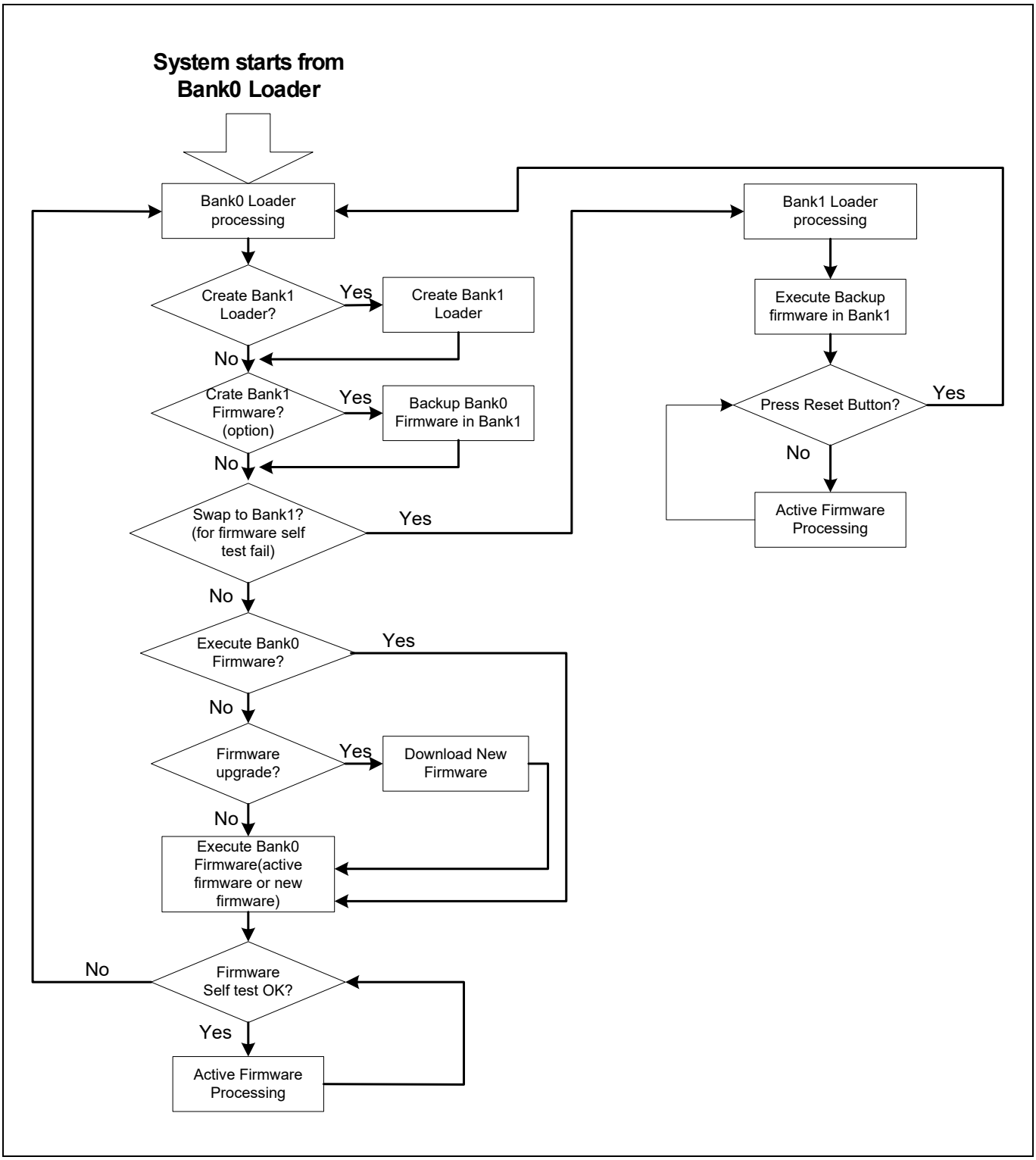
M2L31 BSP provides a firmware upgrade application sample codein:
\bsp\SampleCode\StdDriver\RMC_FwUpgradeApplication

This sample code implements a firmware upgrade application under the Dual Bank APROM architecture of the M2L31. There are three main programs:

- BackupApp:
  A backup programwhich can be executed correctly. It is placed in the program execution area of APROM Bank1, which is the Bank1 App base in the figure below.
- Loader:
  A program which performs the control flow of system startup and firmware upgraded. It is placed at the starting address of APROM Bank0, which is the Loader base in the figure below.
- App:
  An executable program that is placed in the program execution area of APROM Bank0, which is the Bank0 App base in the figure below; it may be active firmware or new firmware.



The system control flow is as follows:



2 The Operation of Firmware Upgrade Sample Code

Before executing the program, first define the firmware naming used in the operation steps:

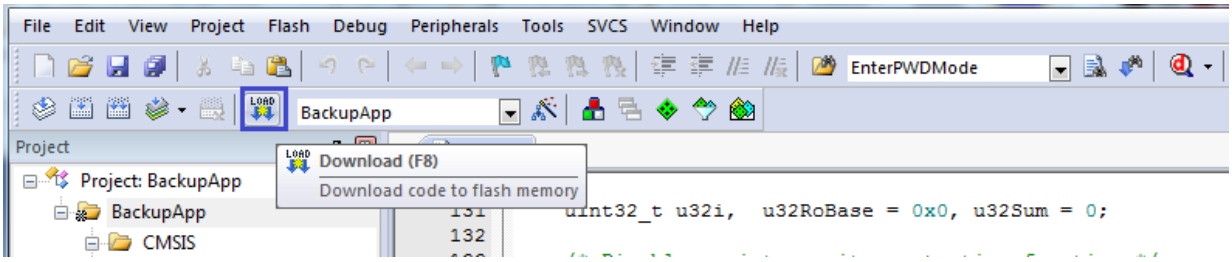
- Active firmware：

  The firmware that was initially placed in the Bank0 App area is also the firmware that the system executes under normal condition.
- New firmware：

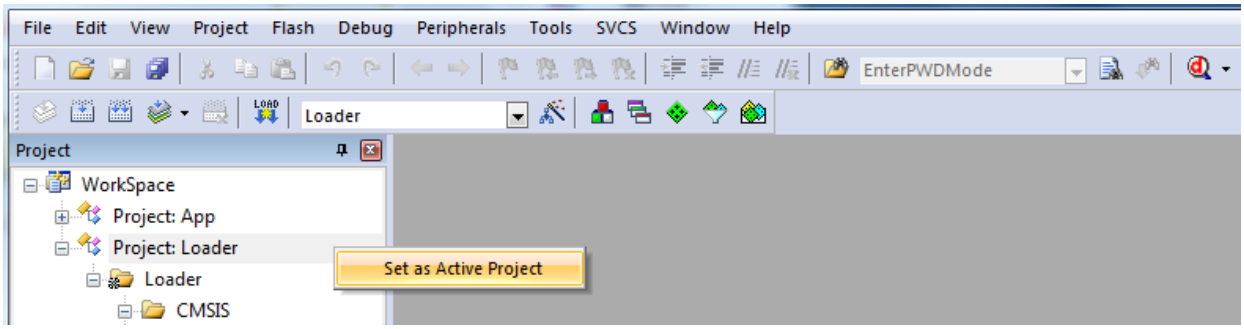
  The new firmware loaded in firmware upgrade process.
- Backup firmware：

  A firmware that allows the system to resume the normal execution when active firmware or new firmware fails to executed.

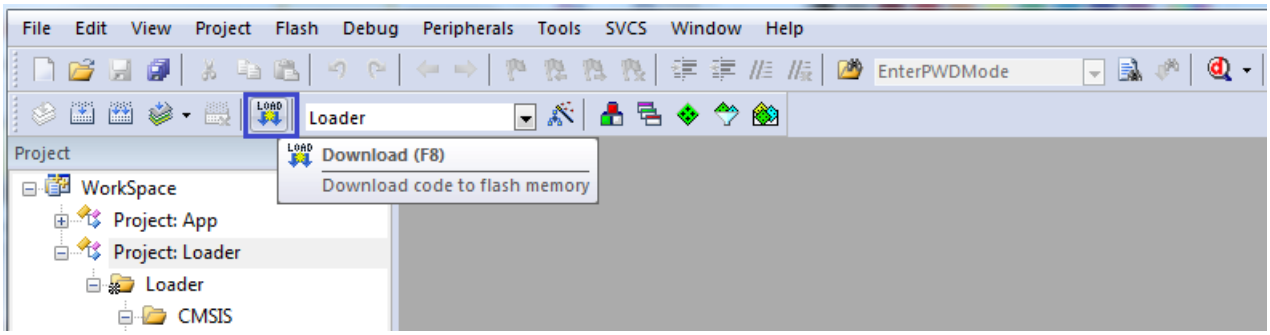
Then start the executionof the program. First, load the backup executable program into the program execution area of Bank1.
In \bsp\SampleCode\StdDriver\RMC_FwUpgradeApplication\BackupApp\KEIL, open the project BackupApp.uvprojx. After compilingdone, click the “LOAD” button to load the backup firmware into the firmware execution area of Bank1. As shown in the figure below:



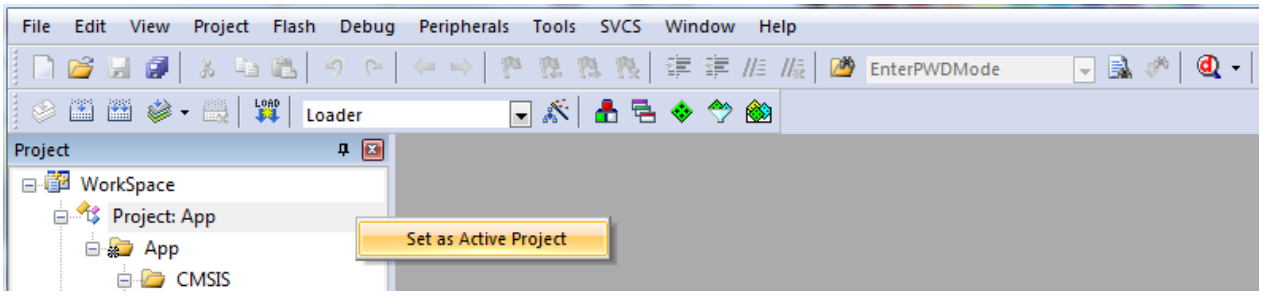
Then back to \bsp\SampleCode\StdDriver\RMC_FwUpgradeApplication，open the project RMC_FwUpgradeApplication.uvmpw. This project has two targets: Loader and App. First select the Loader target. As shown in the figure below:



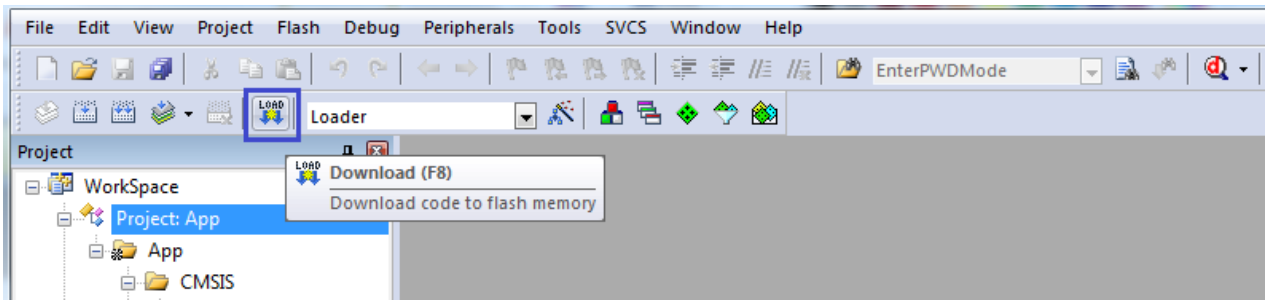
After compiling done, click the “LOAD” button to load the Loader into the Bank0 Loader execution area. As shown in the figure below:



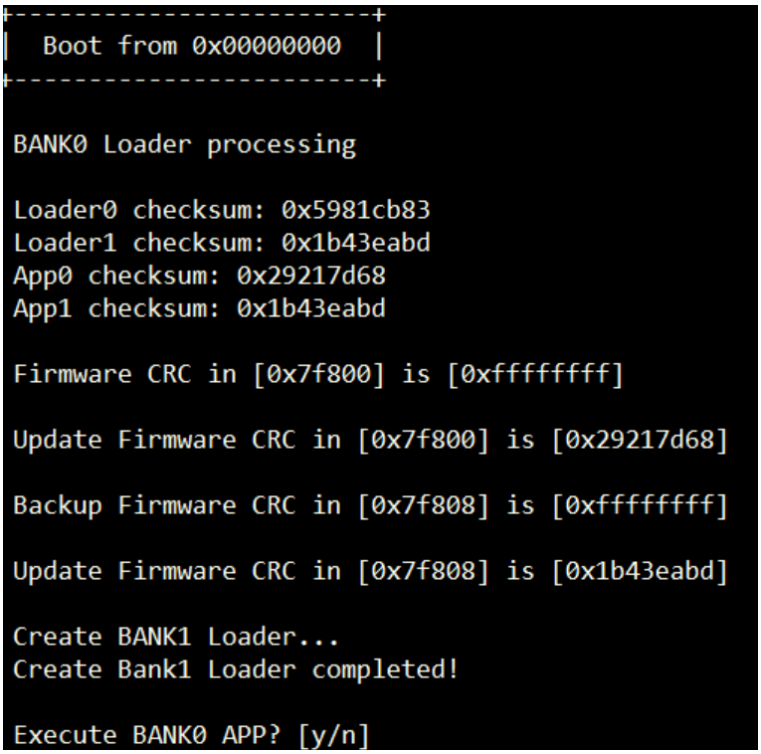
Then select the Apptarget. As shown in the figure below:



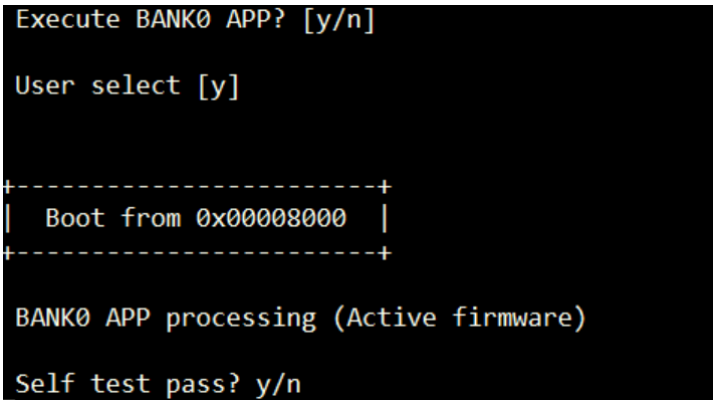
After compiling done, click the “LOAD” button to load the App into the Bank0 App execution area. As shown in the figure below:



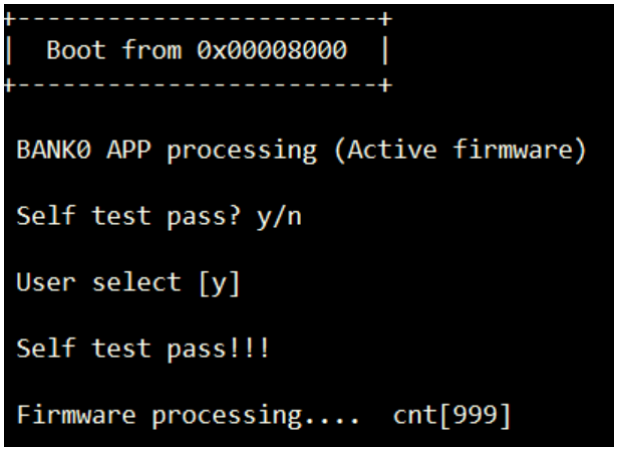
After the three programs being downloaded, press the reset button on the M2L31 to start the system. When the system is started for the first time, the loader of Bank1 will be created for Bank Swap to execute Backup firmware when the firmware upgrade fails. After the Bank1 Loader is created, a dialog message will appear, allowing the user to decide whether to execute Bank0 firmware (Active firmware). As shown in the figure below:



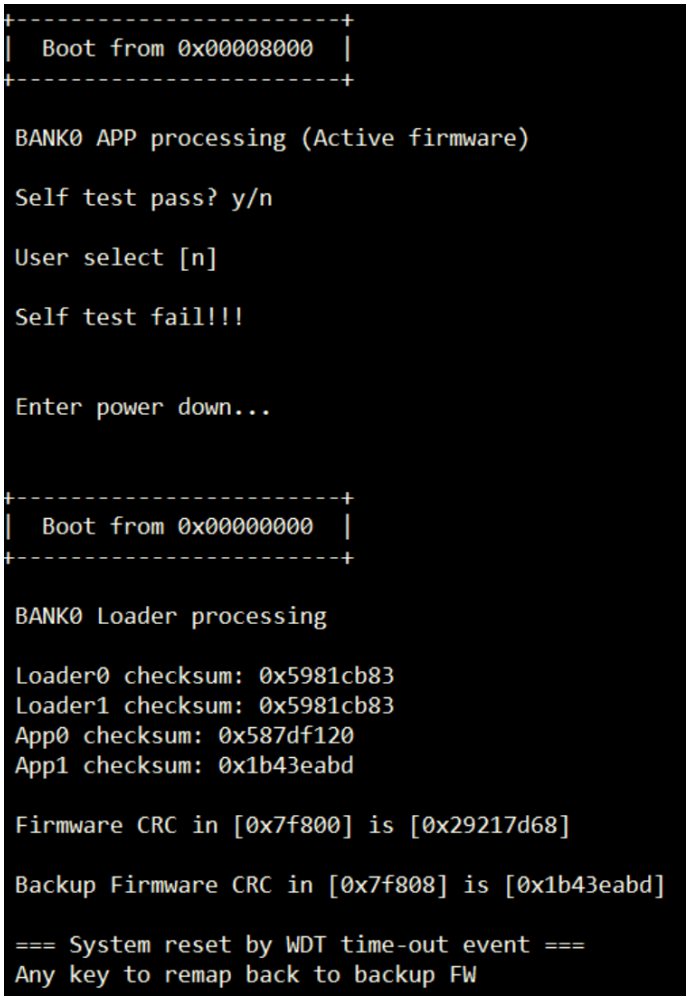
If user selects to execute the active firmware, the system starts the active firmware and a dialog message appears, allowing the user to select to test the success or failure condition. As shown in the figure below:



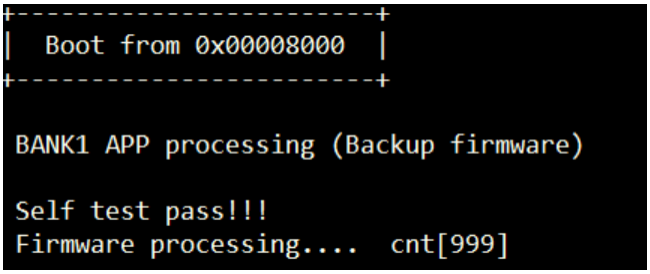
If user selects to test the successful execution of the firmware, a successful message will be shown and the active firmware will continue to run. As shown in the figure below:



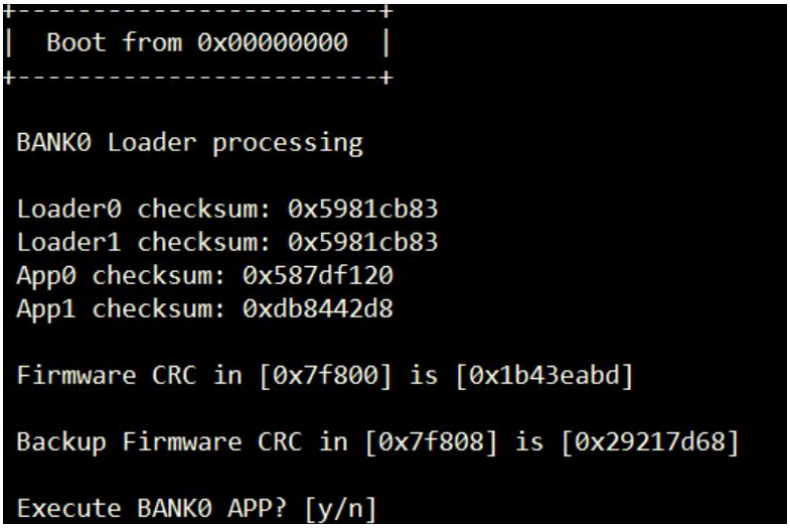
If user selects to test the failure of firmware execution, a failure message will be shown. After Watch Dog determines that the firmware has caused the system to stall for more than its timeout, Watch Dog restarts the Loader. After the Loader is started, it is determined that the execution of the Bank0 firmware has failed, so the user presses any key to execute Bank Swap, and returns to the Backup firmware of Bank1 to execute.As shown in the figure below:



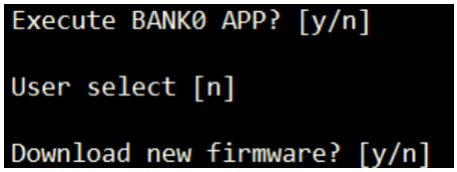
The execution if Backup firmware is shown in the figure below：



The above is the operation flow of executing Active firmware. The following describes how to update the firmware. First, start from the Loader and ask the user whether to execute the Bank0 App. At this time, user must select not to execute the Bank0 App, so that the program continues to execute in the loader.As shown in the figure below:



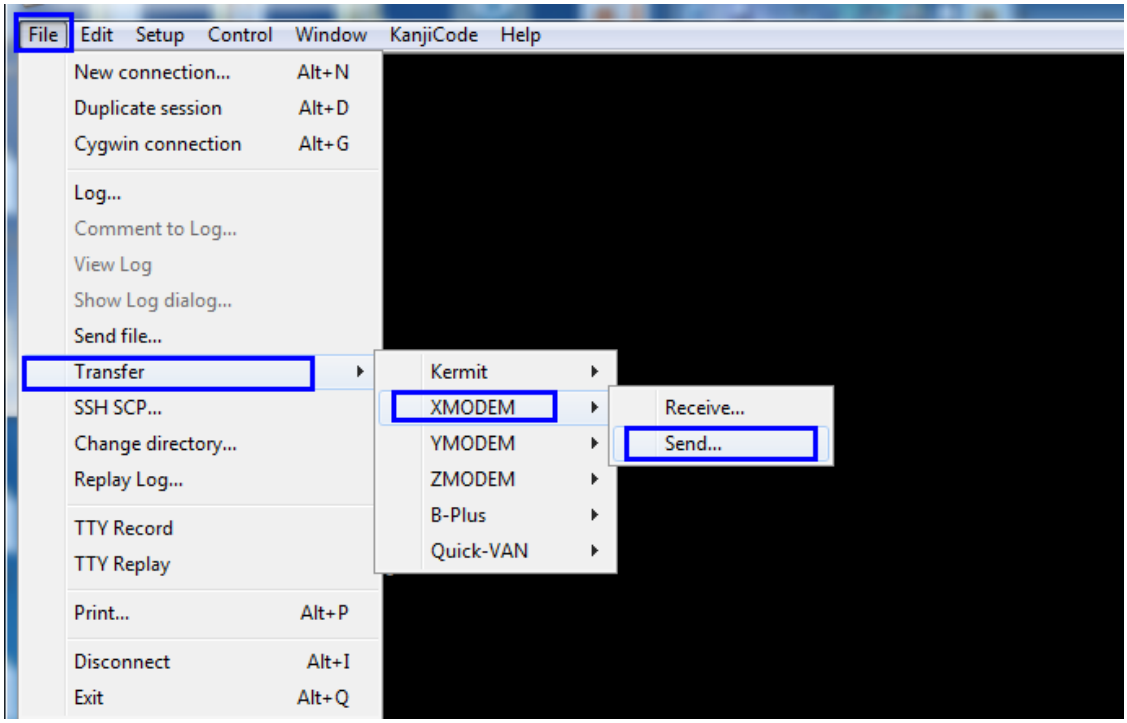
Then a dialog message will appear to let user select whether to update the firmware.As shown in the figure below:



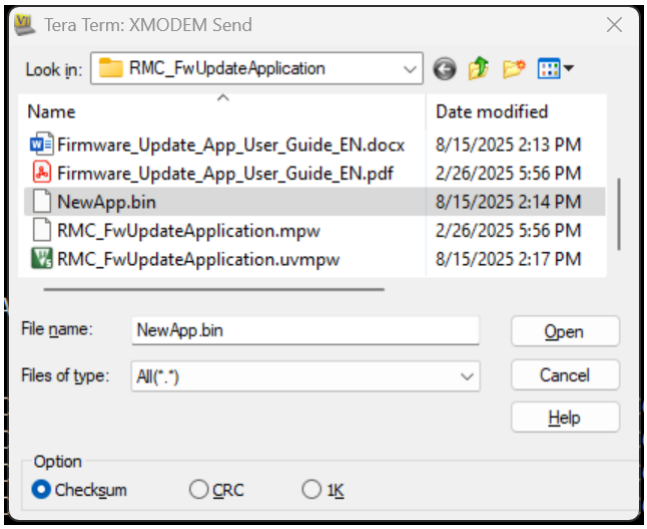
When user selects (y) to execute the firmware update, the Xmodem transmission start character ‘C’ will appear, as shown below:

```
Download new firmware? [y/n]

User select [y]

Bank0 processing, download data to Bank0 APP Base.


CCCCCCCCCCCCCCCC
```

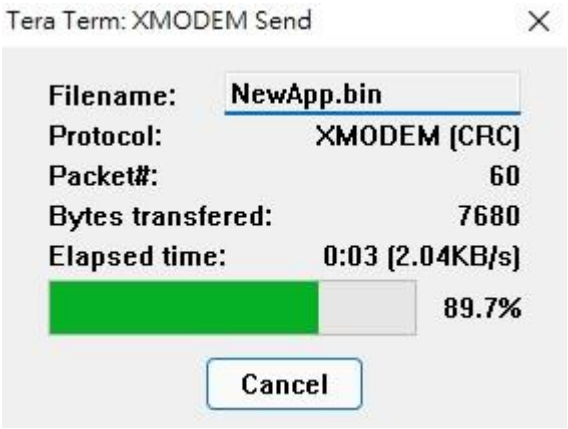
Then select”File→Transfer→XMODOM→Send” in the UART window to start Xmodem transmission, as shown below:



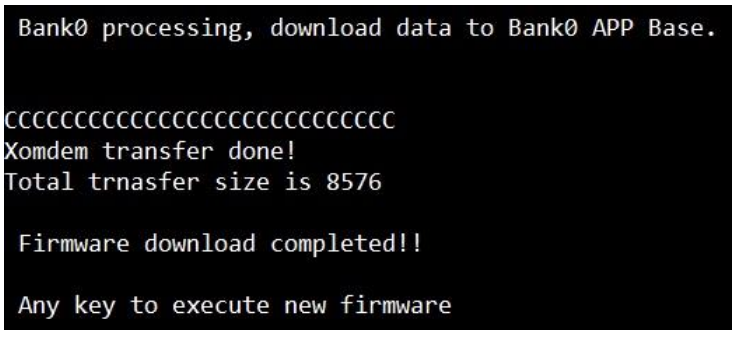
Then a window of XMODEM Send will appear, select NewApp.bin (located in \bsp\SampleCode\StdDriver\RMC_FwUpgradeApplication) provided in Sample code in this window, as shown below:



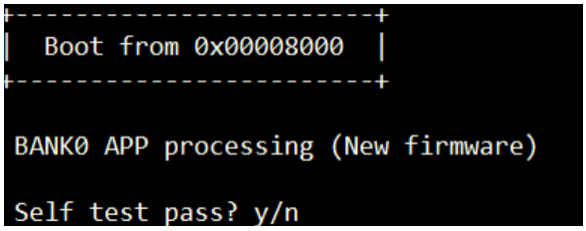
After double-clicking the bin file, the file starts to transfer, as shown in the following figure:



After the transfer being completed, return to the original debug window, and the message "Firmware download completed!!" will appear, indicating that the firmware update is complete. As shown below:



After upgrading the firmware, press any key to execute new firmware.As shown in the figure below:



The execution test of new firmware is the same as the previously described Active firmware. User can select to test the successful or failed firmware execution.

Revision History

Date	Revision	Description
2025.08.15	1.00	1. Initially issued.

Important Notice

Nuvoton Products are neither intended nor warranted for usage in systems or equipment, any malfunction or failure of which may cause loss of human life, bodily injury or severe property damage. Such applications are deemed, "Insecure Usage".

Insecure usage includes, but is not limited to: equipment for surgical implementation, atomic energy control instruments, airplane or spaceship instruments, the control or operation of dynamic, brake or safety systems designed for vehicular use, traffic signal instruments, all types of safety devices, and other applications intended to support or sustain life.

All Insecure Usage shall be made at customer's risk, and in the event that third parties lay claims to Nuvotonas a result of customer's Insecure Usage, customer shall indemnify the damages and liabilities thus incurred by Nuvoton.

Please note that all data and specifications are subject to change without notice.
All the trademarks of products and companies mentioned in this datasheet belong to their respective owners.