ICP Programmer User Manual

Introduction

This user manual gives an overview of Artery ICP Programmer. ICP Programmer acts as a graphic interface application designed to facilitate the use of Artery MCU. AT-Link or J-Link simulator is required to operate Artery MCU device.

Contents

List of tables

List of figures

1 Introduction

1.1 Environmental requirements

- **Software requirements**

Windows XP, Windows 7 and above is required.
.Net framework 4.0 is required. For some operating systems without .Net framework 4.0, it is required to be installed.
There is no need to install a driver when using the AT-Link simulator.
A driver is required when using the J-Link simulator. J-Link V6.20C and above is used. The version below J-Link V6.20C will not work with this software.

- **Hardware requirements**

AT-Link simulator
J-Link simulator
PC/AT compatible, Pentium or higher CPU
XVGA (1024 * 768) color display.
At least 512 M RAM
At least 20 M disk space

1.2 Glossary

- **ICP:**

ICP (in-circuit programming). It allows users to update the Flash of MCU through software without the need of removing the MCU from the target PCB.

- **AT-Link simulator:**

AT-Link is a simulator developed by Artery to support the simulation of the kernel chip.

- **J-Link simulator:**

J-Link is a simulator developed by SEGGER to support the simulation of the kernel chip.

2 Installation

- **Software installation**

No need to install software, just run the executable program "ArteryICPProgrammer.exe" directly.

- **Hardware installation**

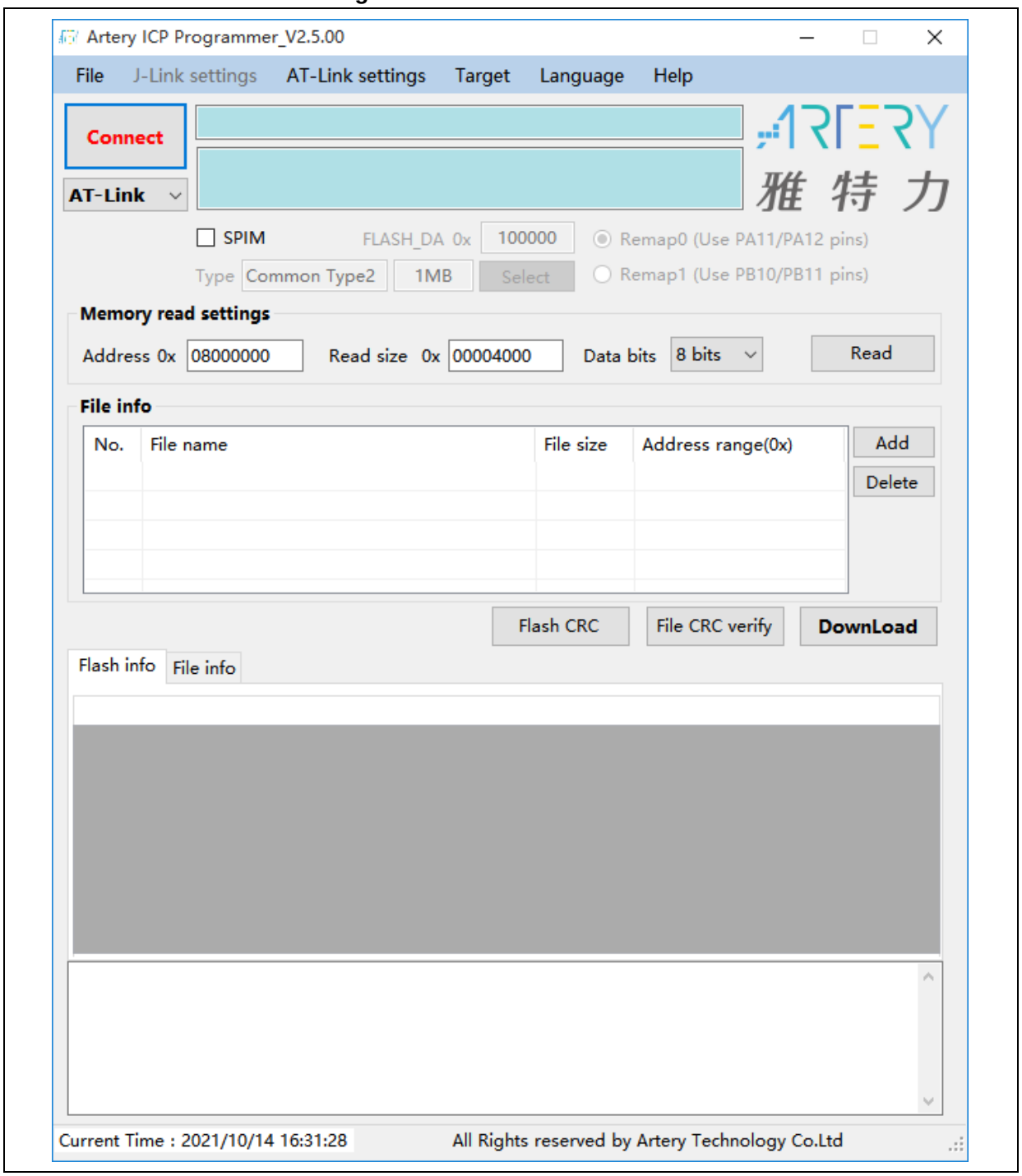
Step 1: connect the AT-Link/ J-Link simulator to the USB interface of PC.

Step 2: connect the AT-Link/ J-Link simulator to the ICE interface of the target development board.

3 Function overview

This section gives an overview of tool operations. The main interface is shown in Figure 1:

Figure 1. Main window



3.1 Menu bar

The content of Menu Bar is shown in Figure 2. (This section only gives a brief description of menu bar, and the specific functions will be detailed in subsequent chapters).

Figure 2. Menu bar

■ "***File***" menu

— Save file as: save the data in the "***File Info***" as a file in the format of *.bin/ *.hex/*.srec/*.s19.

— Save flash data as: save the memory data in the "Flash Info" as a file in the format of *.bin/*.hex/*.srec /*.s19.

— Make encryption file: encrypt the bin file as a benc file, hex file as a henc file, srec and s19 file as a senc file.(encrypted files are suited to AT-Link)

— Exit: exit the software.

■ "J-Link Setting" menu:

J- Link simulator settings.

■ "AT-Link Setting" menu:

AT- Link simulator settings.

■ "Target" menu:

— Mass erase: erase the whole main flash. When SPIM is selected, the whole SPIM will also be erased (AT32F403/F413/F403A/F407). When the boot memory is in AP mode, the boot memory is also erased (AT32F415/F421/F425).

— Erase main flash: erase the whole main flash.

— Erase SPIM: erase the whole SPIM.

— Erase boot memory: erase the boot memory (AT32F415/F421/F425 AP mode)

— Erase sector: users select the sector to erase.

— User system data: User system data settings, including access protection and erase and program protection, etc.

— Access protection:
For AT32F403/F413/F403A/F407/F435/F437, enable / disable access protection.
For AT32F415/F421/F425, enable access protection, high level access protection (access protection and user system data erase protection) and disable access protection. (AT32F425 high level access protection is irreversible. Once enabled, it will never be unlocked, with its debugging interface permanently disabled. Please use with caution.)

— sLib status: the user can check the current status (enabled or disabled) of sLib, and disable sLib (AT32F413/F415/F403A/F407/F421/F435/F437/F425).

— Boot memory AP mode: the boot memory is set in AP mode (AT32F415/F421/F425). The boot memory cannot be restored after being set as AP mode.

— Download: set download options and download files to flash.

— Flash CRC: calculate the CRC value for the selected sectors in flash.

■ "Language" menu:

- English
- Chinese (Simplified)

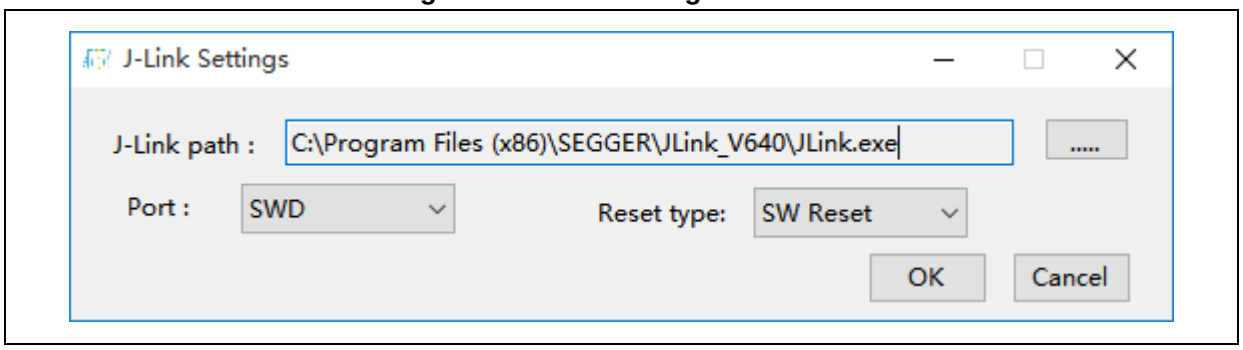
■ “Help” menu:

- User manual: open the user manual of this software.
- AT-Link firmware manual upgrade: the user needs to manually select the file to upgrade AT-Link firmware.
- AT-Link firmware online upgrade: automatic online upgrade AT-Link firmware. The computer must be connected to the Internet.
- ICP new version download: automatically detect whether there is a new version of ICP software, if so, download it. The computer must be connected to the Internet.
- Artery MCU resources download: provide links to download Artery MCU resources. The computer must be connected to the Internet.
- Version: check the software version.

3.2 J-Link settings

This section shows how to set J-Link. (Menu bar — "***J-Link Settings***")
(As shown in Figure 3)

Figure 3. J-Link settings



- **J-Link path:** if J-Link driver is installed, the software will automatically obtain the installation path. The user can also select it manually.
- **Port:** SWD and JTAG are available.
- **Reset type:** software reset or hardware reset. It is effective when using J-Link to operate the device.
- **OK:** make the setting take effect and close the dialog box.
- **Cancel:** cancel the setting and close the dialog box.

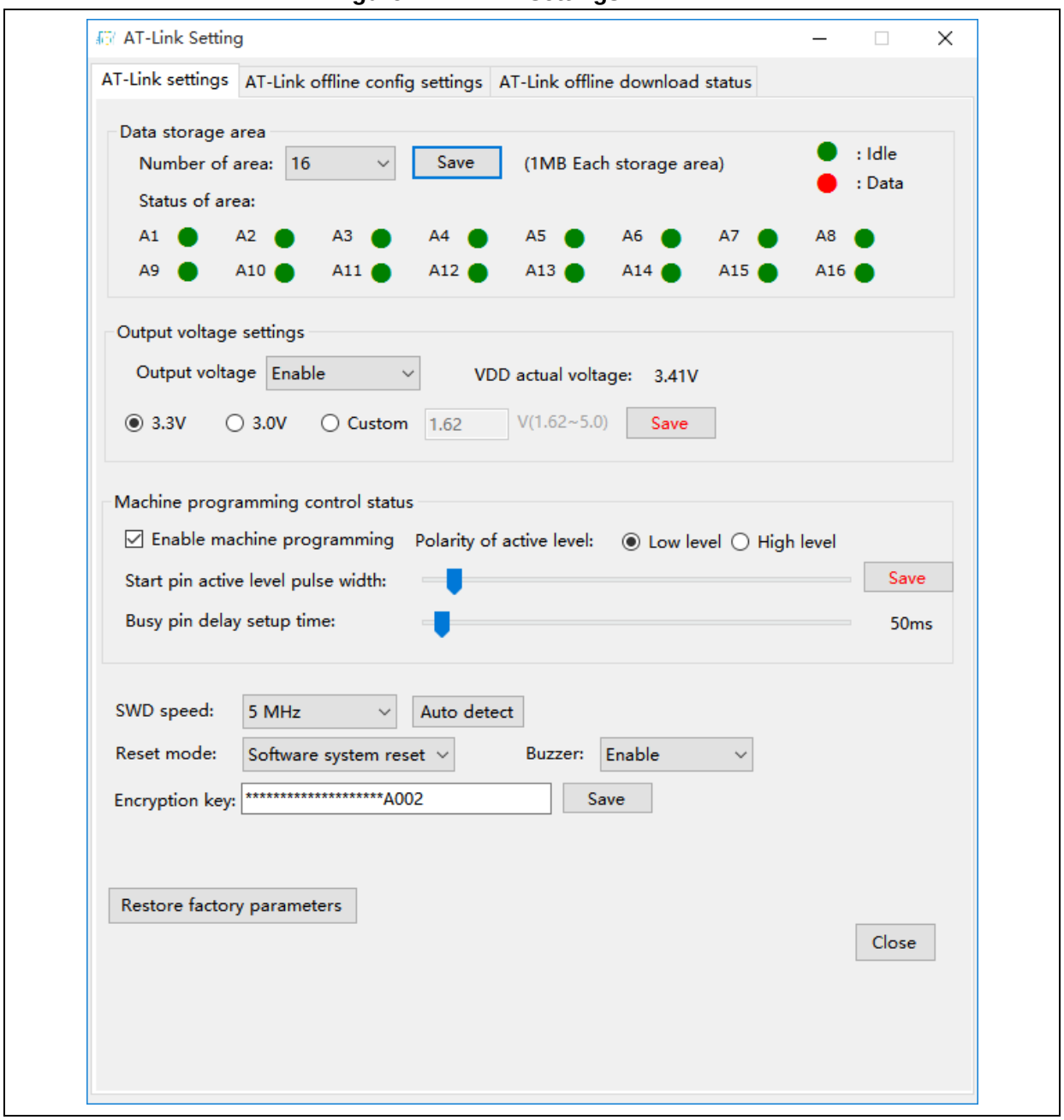
3.3 AT-Link settings

This section shows how to set AT-Link. (Menu bar — "***AT-Link Settings***")

3.3.1 Parameter settings

This section gives an overview of the configuration of AT-Link parameters. (As shown in Figure 4)

Figure 4. AT-Link settings



- Number of area

This represents the number of codes stored offline, supporting 1/2/4/8/16, and the maximum capacity corresponding to each code is 16/8/4/2/1 MB, respectively. Offline download also supports downloading multi-section code files (up to 5) at a time. Multi-section code files will occupy multiple storage areas.

Note: modifying this option will clear all offline stored project data.

- Output voltage settings

This option is for the enable and range selection of output voltage, and the customized range is 1.65V-5V.

- Machine programming control status

Enable machine programming: enable or disable.
Polarity of active level: low level or high level
Start pin active level pulse width: 20-1000ms.
Bus pin delay setup time: 20-1000ms.

- SWD speed

Configure the SWD transmission speed for non-IDE operation, and 100kHz/500kHz/1MHz/2MHz/5MHz are available for selection.

- Auto detect

SWD speed will be automatically detected.

- Reset mode

It contains software system reset and hardware NRST pin reset, which are mainly used for reset after the target board download is completed or some operations that need to be reset, such as FAP, EPP operations.

- Buzzer

Buzzer enable option. When this function is disabled, all other operations are silent except for power-on initialization.

- Encryption key

Support the combination configuration of 6-24 bytes of letters or numbers, which is customized by AT-Link users. The initial default value is a 24-byte AT-Link serial number.
Note: modifying this option will clear all existing offline project data.

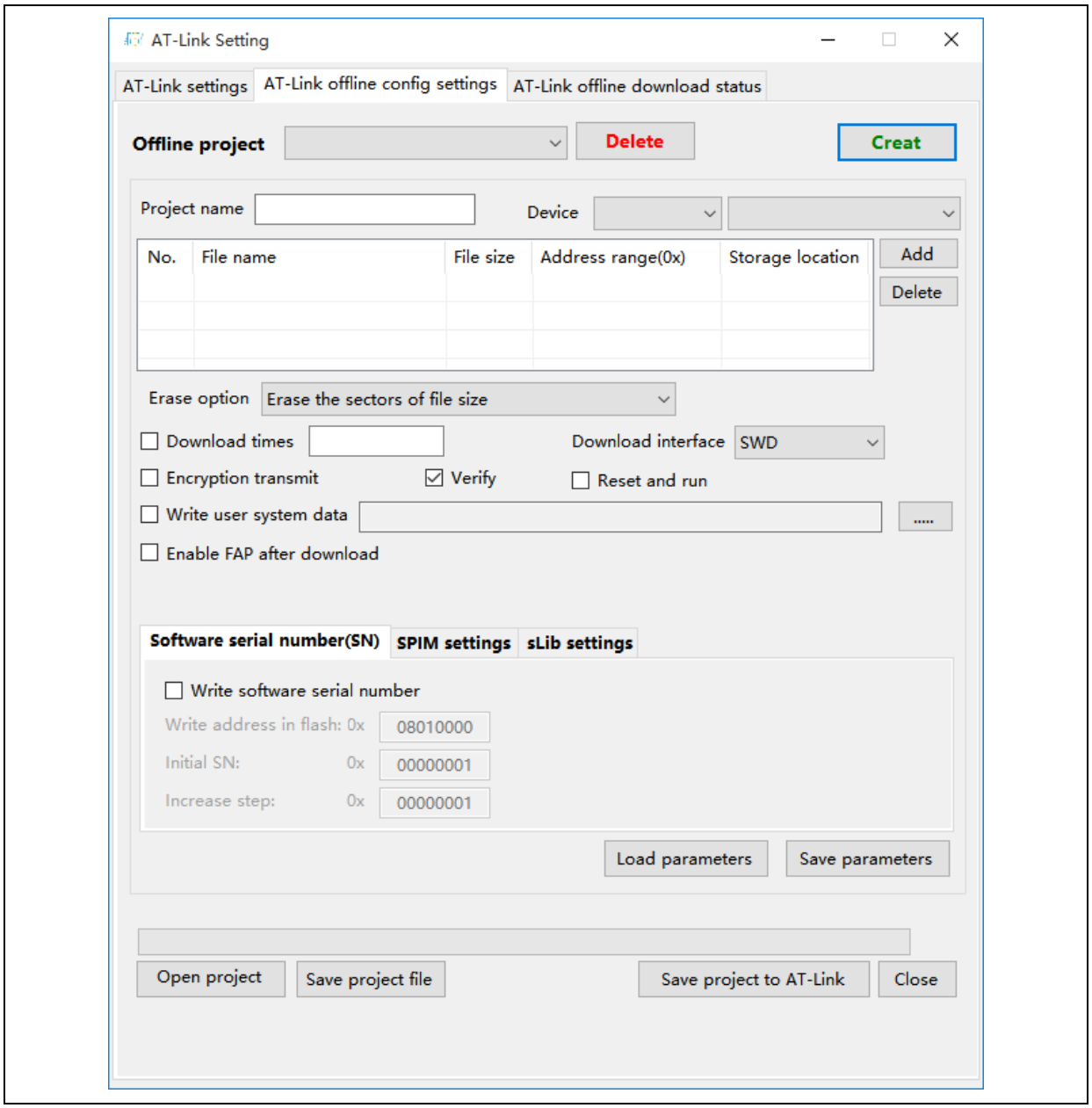
- Restore factory parameters

Clear all AT-Link parameters and stored data, and restore to factory default values.

3.3.2 AT-Link offline project settings

This section describes how to configure the content of offline projects (As shown in Figure 5).

Figure 5. Offline config settings



- Offline project

It displays the currently stored offline projects.

Select from the drop-down menu to view the configuration parameters of project.

- Delete/Create

Delete the selected project in the drop-down menu or create a new one.

- Project name

Customize the project name when creating a new project, supporting up to 16 bytes length.

- Device

When creating a new project, it allows the user to only download the target MCU of a specific model of certain series. However, if AT32F413-Universal is selected, it means that all the MCUs of AT32F413 series are allowed to download.

- Add/Delete

When creating a new project, add and delete the code file to be downloaded. The format can be bin/hex/srec/s19/benc/henc/senc. Multi -section code file configuration is supported. The address of multi-section code files cannot be on the same Flash sector. The maximum length of file name is 32 bytes.

- Erase option

Configure as required. Support various erase operations before download.

- Download interface

Select SWD or ISP interface when downloading the project offline.

- Download times

If this option checked, the total number of downloads will be limited in the range of 1-4000000. Both success and failure are included in the total number.If the total number is exceeded, no more downloads are allowed.

- Reset and run

After the project download is completed, it will reset and run. This option and enable FAP after download option cannot be enabled at the same time

- Encryption transmit

The download process works with the Hex Encryption function of Artery MCU to implement encryption transmit to ensure the security of data during the transmission.

- Verify

Verify whether the data is correct after download, and a hardware verify method will be used during encryption transmit to ensure data security.

- Enable FAP after download

Enable this option when the download is completed. For AT32F415/F421/F425, users can choose to enable access protection and high level access protection (access protection and user system data erase protection). (AT32F425 high level access protection is irreversible. Once enabled, it will never be unlocked, with its debugging interface permanently disabled. Please use with caution.)

- Boot memory AP mode (AT32F415/F421/F425)

Configure the boot memory as AP mode. Some MCUs can configure the boot memory as an extended user code area for user code storage.
Note: this mode setting is irreversible and can only be modified once.

- Write user system data

Users can select to download user system data file at the same time. The format can only be bin or

hex.

■ Write software serial number

32-bit data. The address can be customized. The address and code address cannot be on the same flash sector. Serial number value = initial serial number + number of successful downloads x each increment value, if overflow occurs, the high bit will be cleared and the low 32 bit will be reserved.

■ SPIM settings (AT32F415/F421/F435/F437/F425 does not support)

If there are files with the address range in SPIM (including code or serial number), users need to select the corresponding external Flash model, IO mapping, and external encryption programming range and other information.

■ sLib settings (AT32F403 does not support)

Configure sLib-related parameters, including disabling the existing sLib before download and enabling a new sLib during download, and users need to set sLib password and sLib range.

■ Save parameters (valid only for new projects)

When creating a new project, users can save various parameters of project configuration to a file. It is convenient for users to configure multi-projects with the same or similar parameters next time.

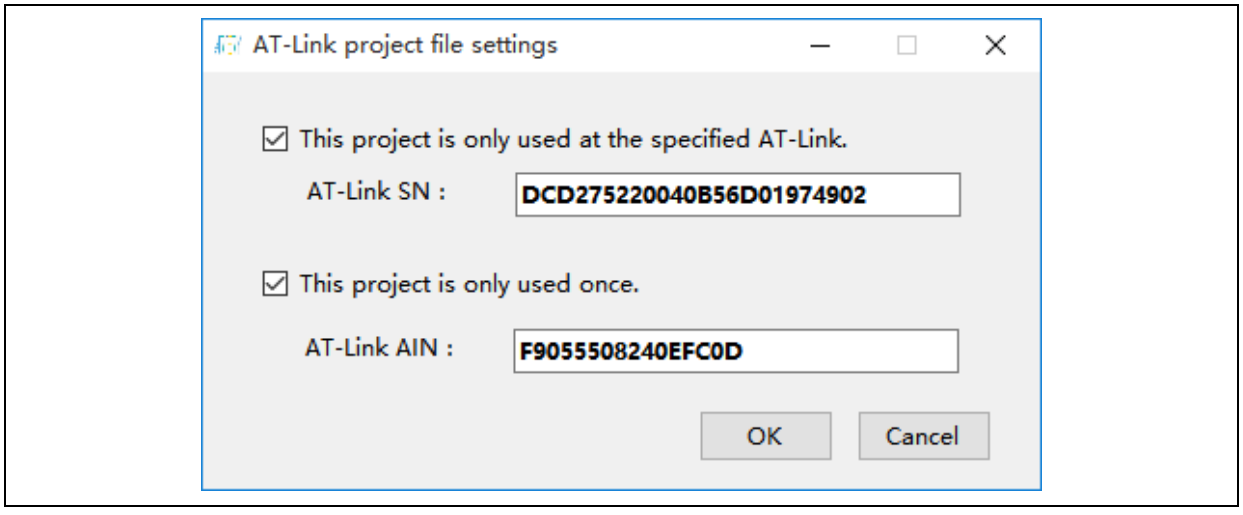
■ Load parameters (valid only for new projects)

When creating a new project, user can load the stored parameter files so as to configure project conveniently and quickly (Save and load function only refer to the parameters, rather than save or load the downloaded documents).

■ Save project file

After all the above files and parameters configuration are completed, they can be packaged to generate an encrypted project file in the format of * .atcp for remote transmission or local storage. When saving project file, the following settings can be made: (As shown in Figure 6)

Figure 6. Project file settings



— This project is only used at the specified AT-Link:

This project is bound to AT-Link and can only be used in the specified AT-Link. The AT-Link serial number must be set.

— This project is only used once:

This project can only be used once, and is used in conjunction with “This project is only used at the specified AT-Link”, and AT-Link SN and AIN is required.

■ Open project:

Open an existing project file in * .atcp format and load its configuration into the software for viewing.

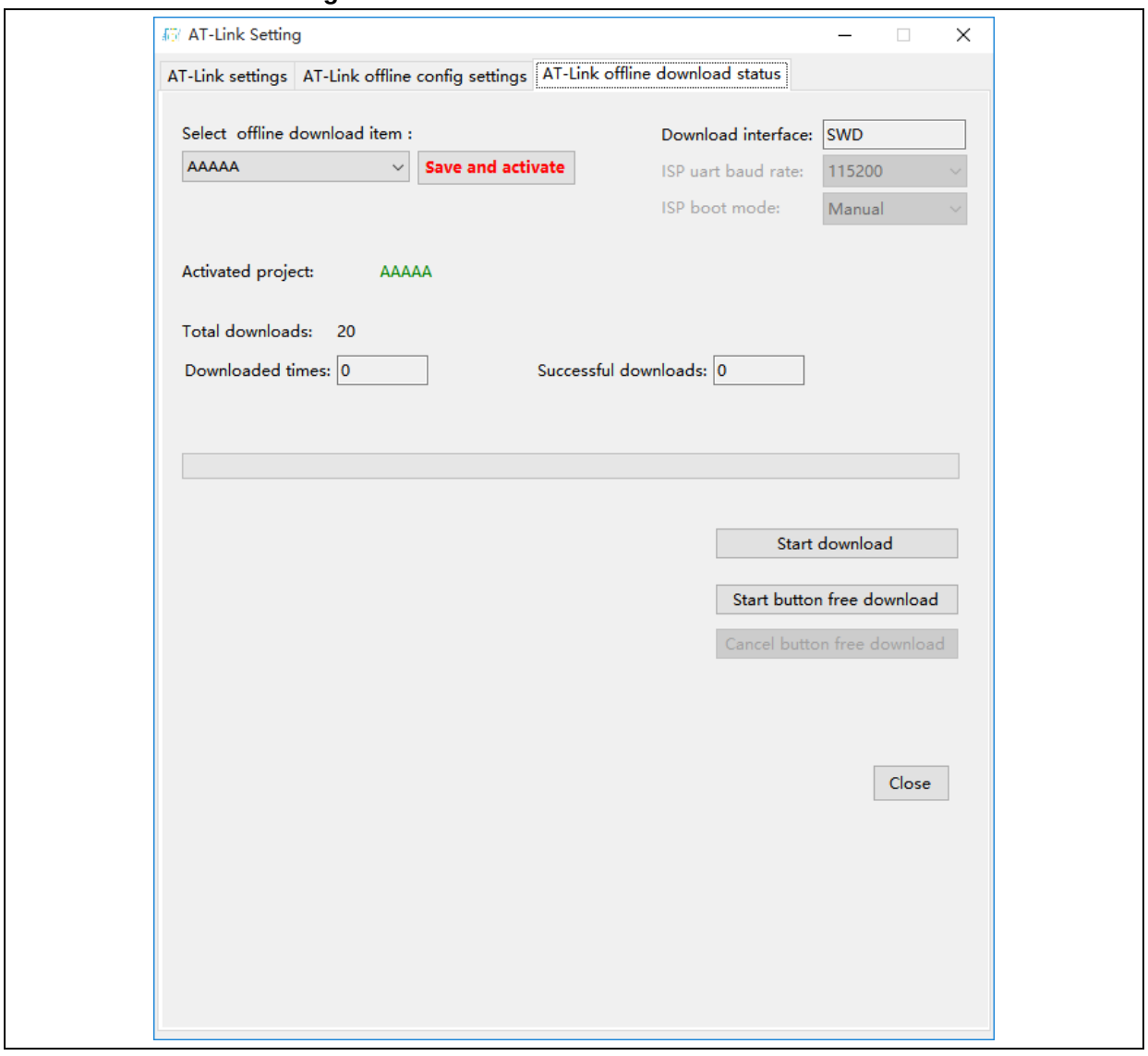
■ Save project to AT-Link

Save the configured project or opened project in the AT-Link through a dynamic encryption algorithm for offline download.

3.3.3 AT-Link offline download

As shown in Figure 7:

Figure 7. Offline download window



■ Select offline download item

At-Link can store multiple offline projects. Users need to select one project to activate. The

activated project will be selected for downloading. If the current active project is deleted, select it again. Click on "Save and activate" to take effect.

- Download interface

Only displays the interface of the activated project, and this cannot be changed. If it is an ISP interface, the baud rate and boot mode can be changed according to the target board circuit.

- Total downloads

Set the total number of downloads.

- Downloaded times

Displays the number of downloads of the activated project, including the number of successes and failures. When the total downloads are reached, the project file can no longer be downloaded.

- Successful downloads

Displays the number of successful downloads of the activated project.

- Start download

Start a single offline download, and the corresponding message will pop up according to the download progress. If failed, error message will be displayed.

- Start/Cancel button free download

This feature means that there is no need to operate the ICP interface, only need to replace the target board MCU according to the prompt message to complete the automatic continuous download.

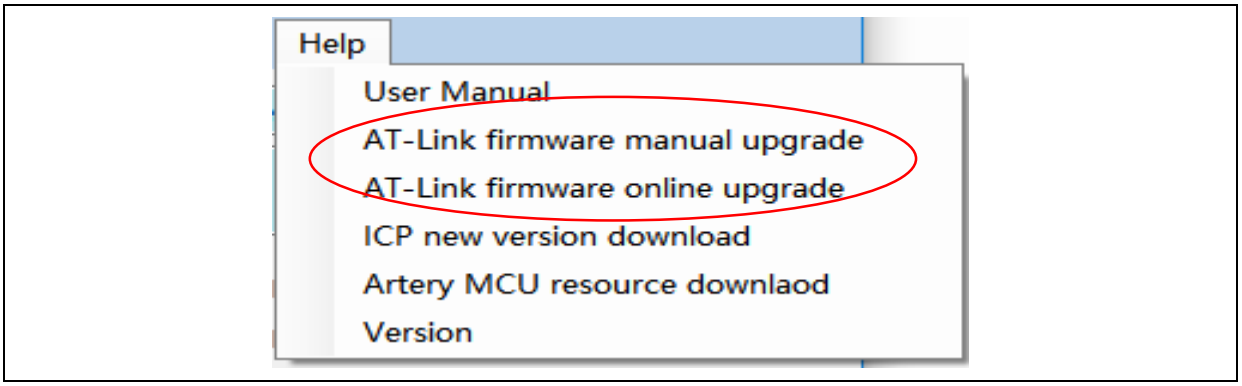
This option allows the switching of Start/Cancel only when AT-Link is in idle state.

Note: other operations are not allowed in button free mode. Users must cancel the button free mode before operation.

3.4 AT-Link firmware upgrade

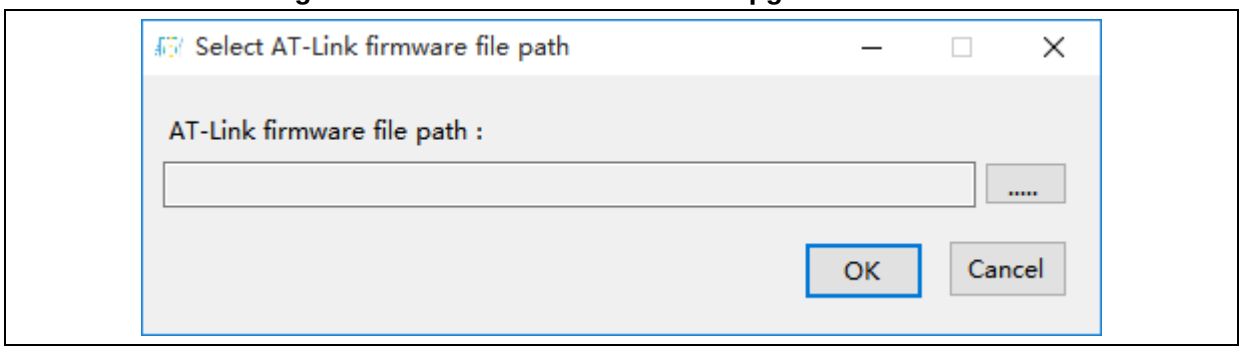
This option can be found in the "***Help***" menu. (As shown in Figure 8)

Figure 8. AT-Link firmware upgrade



- AT-Link firmware manual upgrade (As shown in Figure 9)

Figure 9. AT-Link firmware manual upgrade



Need to select the path where the firmware file in * .benc format is.

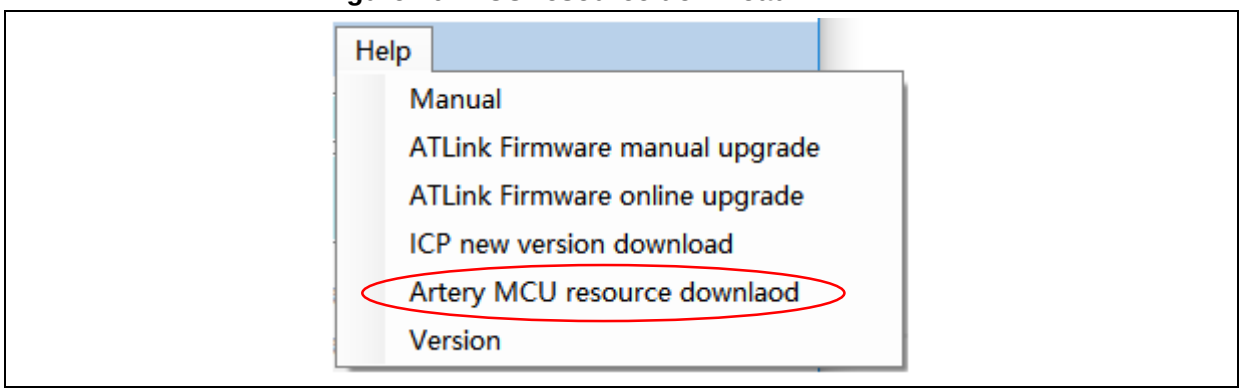
- AT-Link firmware online upgrade

It will automatically upgrade AT-Link firmware via internet. The computer must be connected to the Internet.

3.5 Artery MCU resources download

Artery MCU resources download option can be found in the "***Help*** "menu (this function is available when the computer is connected to the Internet), (As shown in Figure 10)

Figure 10. MCU resource download



The download link is as shown in Figure 11:

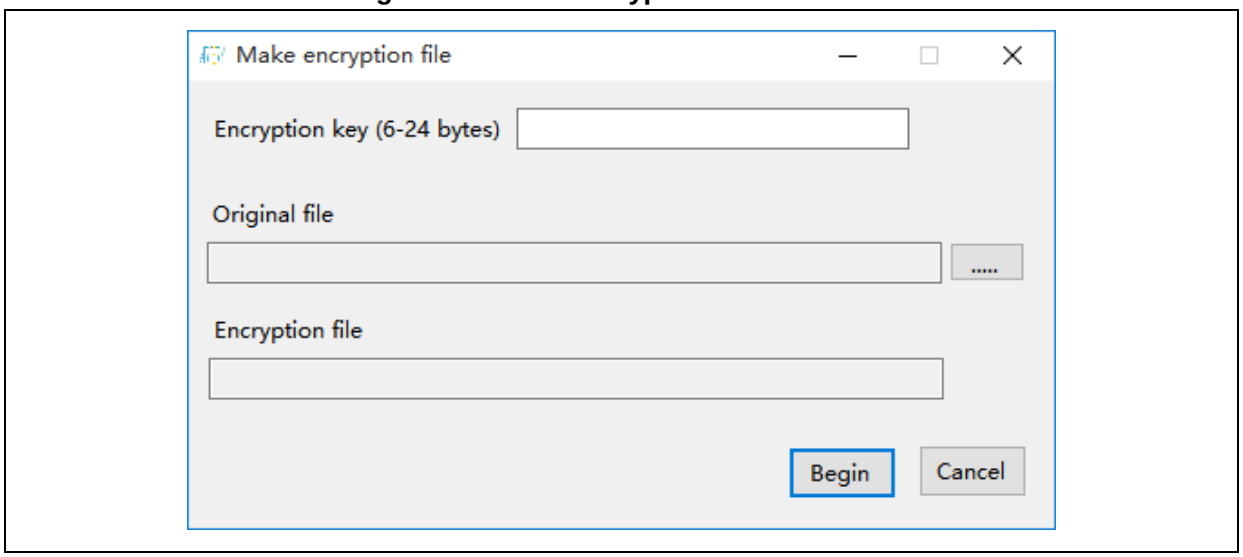
Figure 11. MCU download link

Click the above link to enter the corresponding webpage.

3.6 Make encryption file

"***File***"-"***Make encryption file***". The encryption files are mainly used for AT-Link. J-Link does not support downloading encryption files, as shown in Figure 12:

Figure 12. Make encryption file



- Encryption key

It is the encryption key for making encryption files, 6 to 24 bit letters or numbers.

- Original file

It means the original file that needs to be encrypted. Support in the format of*.bin, *.hex, *.srec and *.s19.

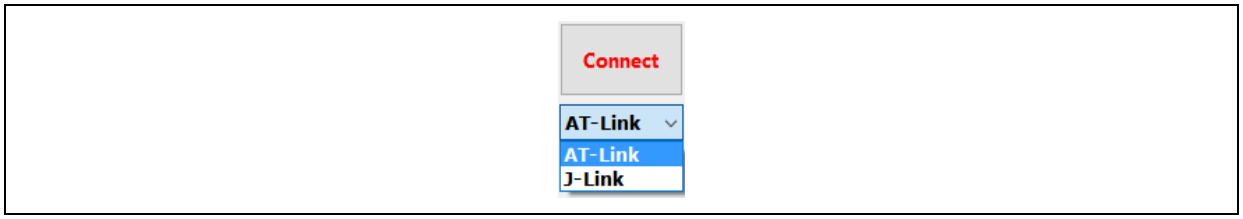
- Encryption file

It means the encrypted file in the format of * .benc/* .henc/* .senc.

3.7 Device connection

Please select the simulator to be used before connecting. (As shown in Figure 13)

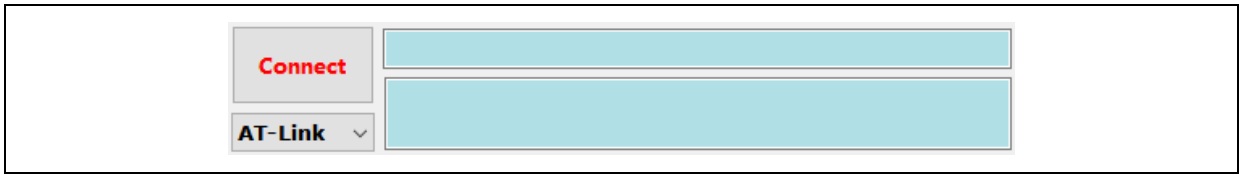
Figure 13. Make encryption file



3.7.1 AT-Link connected to device:

- Before connecting ------- no device is available at this time. (As shown in Figure 14)

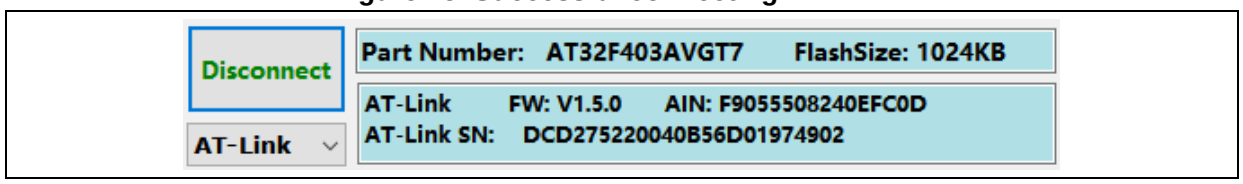
Figure 14. Before connecting



Click on "***Connect***" to connect to device.

- Successful connection------- the device is correctly identified at this time. (As shown in Figure 15)

Figure 15. Successful connecting

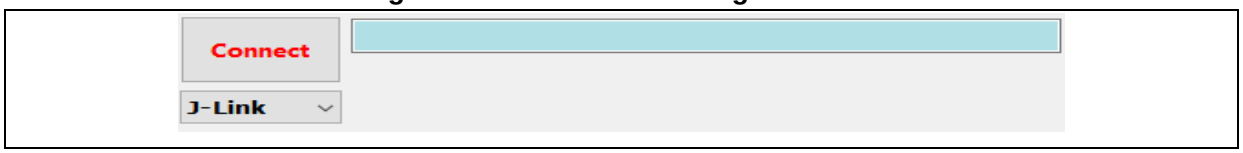


After successful connection, AT-Link related information will be displayed, including AT-Link part number, firmware version, AT-Link AIN; and MCU related information, including MCU part number, Flash size, etc.If click on "***Disconnect***", you can disconnect from the device

3.7.2 J-Link connected to device:

- Before connecting ------- no device is available at this time. (As shown in Figure 16)

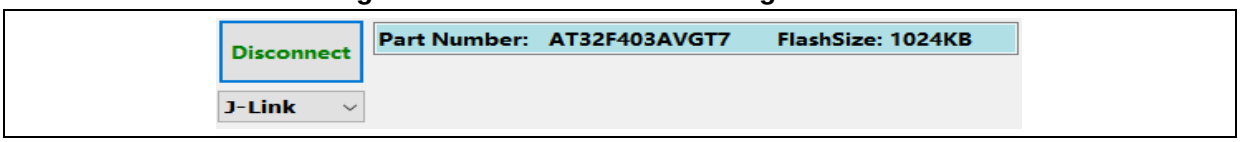
Figure 16. Before connecting



Click on "***Connect***" to connect to the device.

- Successful connection ------- the device is correctly identified at this time, (As show in Figure 17)

Figure 17. Successful connecting



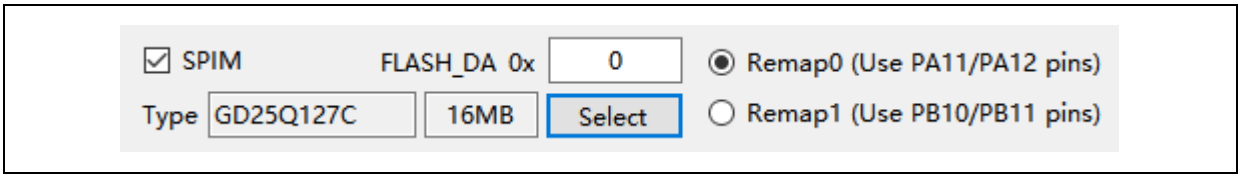
After successful connection, MCU related information will be displayed, including MCU part number, Flash size, etc. If click on "Disconnect", you can disconnect from the device.

3.8 SPIM setting

(AT32F415/F421/F435/F437/F425 does not support)

The SPIM must be set before using, otherwise it will not work normally. (As shown in Figure18)

Figure 18. SPIM settings



- Checked "***SPIM***"

SPIM operation is allowed.

- Uncheck "***SPIM***"

SPIM operation is not allowed.

- FLASH_DA

Set the encryption range when downloading files to the SPIM, and the encryption range is calculated starting from the address 0x08400000

- Remap 0 (use PA11/PA12 pins)
- Remap 1 (use PB10/PB11 pins)

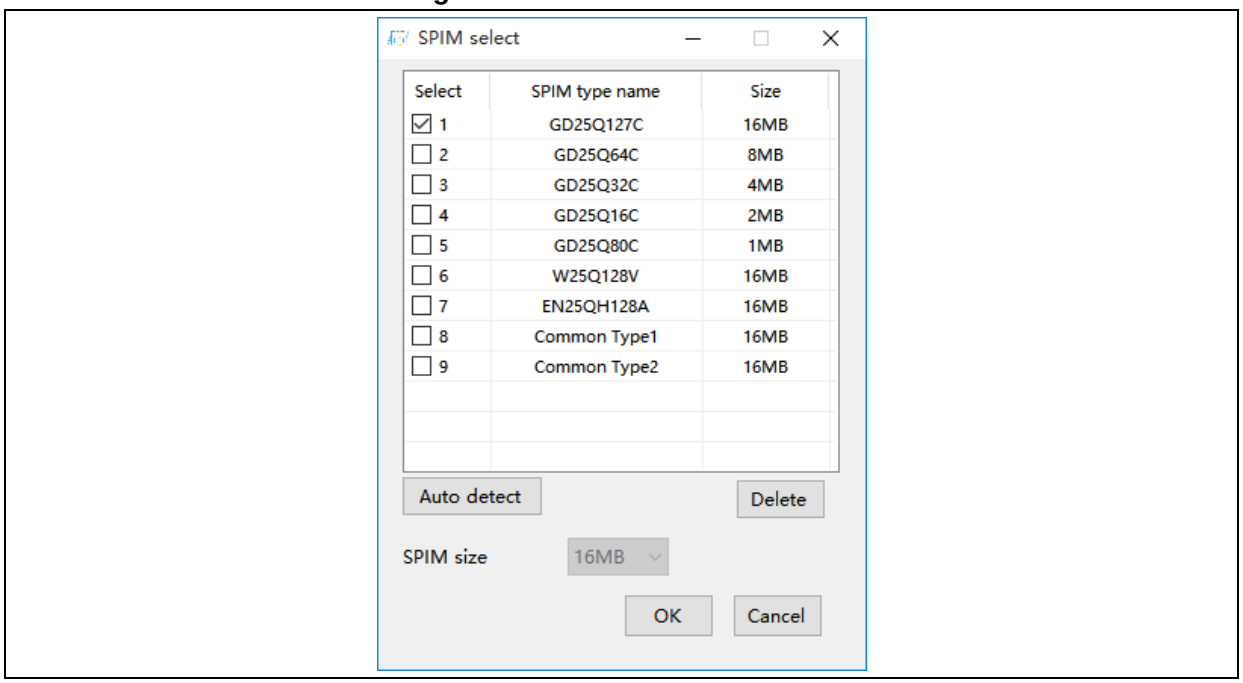
Select SPIM connection pins.

- Type

Users can select the SPIM type through "Select" button.

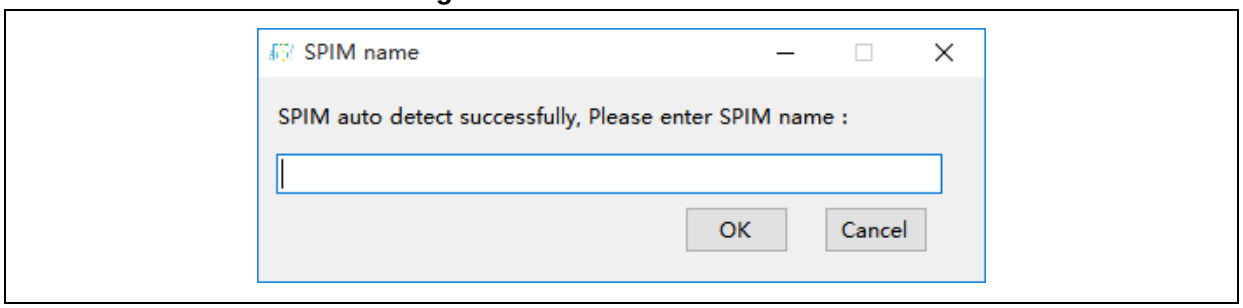
Click on the "Select" button, a dialog box pops up. (As shown in Figure 19)

Figure 19. SPIM select



Auto detect: it will automatically detect whether the SPIM meets the requirements of this software Operation (Auto detect will overwrite some data of SPIM, please use it with caution)
If Auto detect is successful, a dialog box will pop up. (As shown in Figure 20)

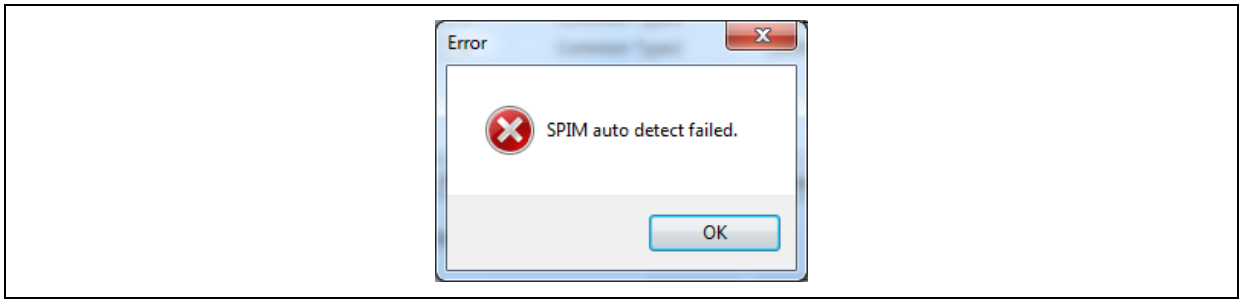
Figure 20. SPIM name



Click on "***OK***" to add the detected SPIM to the SPIM list.
Click on "***Cancel***" to cancel auto detect.

If auto detect failed, a failure dialog box will pop up. (As shown in Figure 21)

Figure 21. SPIM auto detect failed

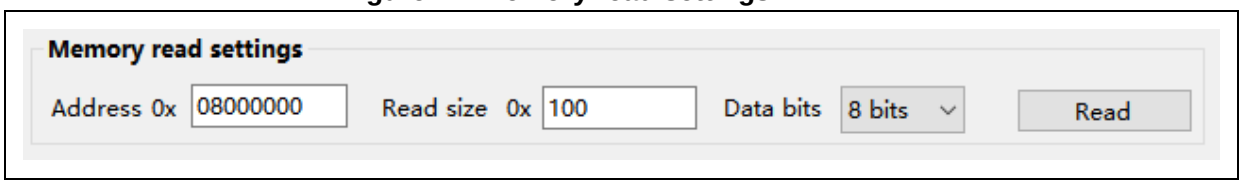


- SPIM size: select the SPIM size, except for the default type.
- Delete: delete the selected SPIM in the list, except for the default type.
- OK: SPIM selected.
- Cancel: cancel.

3.9 Memory read settings

This function is used to read the content of flash memory. (As shown in Figure 22)

Figure 22. Memory read settings



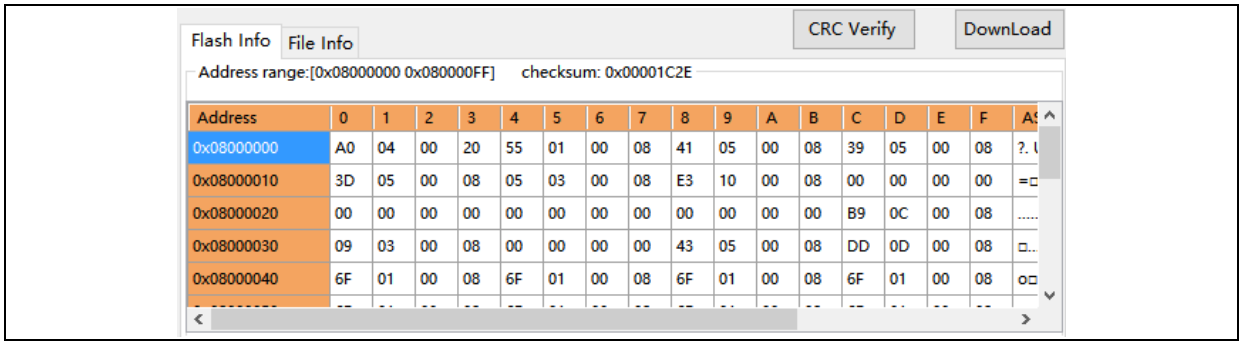
- Address: the start address of the flash memory to be read.
- Read size: the range of memory to be read
- Data bits:

8-bit: read and display flash data in 8-bit mode. At the same time, the files are displayed in 8-bit mode.
16-bit: read and display flash data in 16-bit mode. At the same time, the files are displayed in 16-bit mode.
32-bit: read and display flash data in 32-bit mode. At the same time, the files are displayed in 32-bit mode.
Once selected, the “Read” operation will be performed automatically.

- Read: read flash and display flash data.

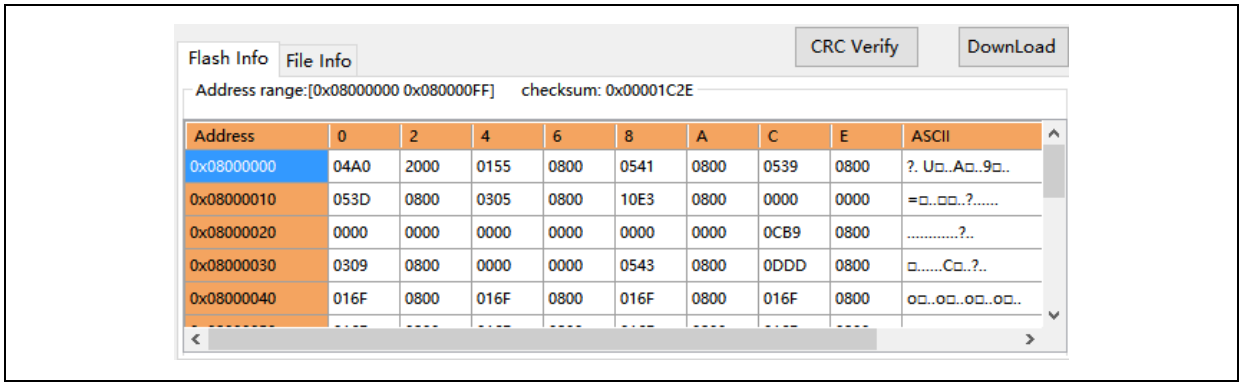
In 8-bit mode. (As shown in Figure 23)

Figure 23. 8-bit data



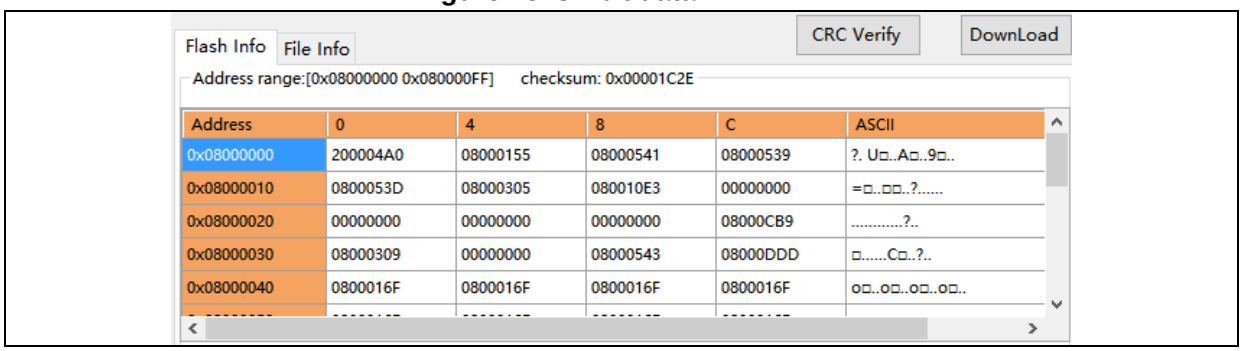
In 16-bit mode. (As shown in Figure 24)

Figure 24. 16-bit data



In 32-bit mode. (As shown in Figure 25)

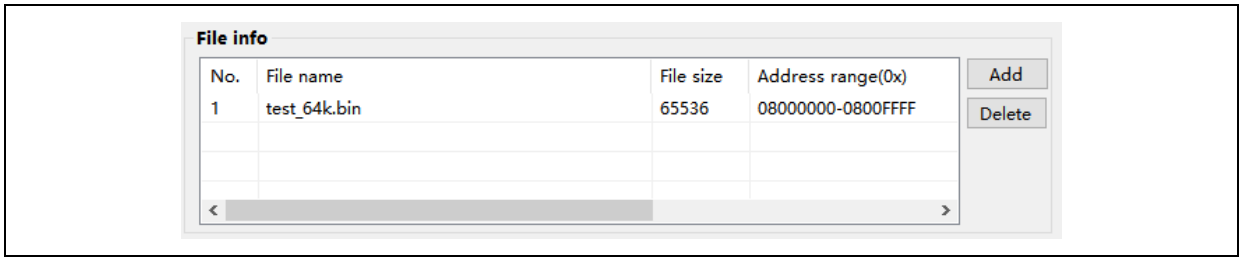
Figure 25. 32-bit data



3.10 File info

Display the file info to be downloaded, including file name, file size, download location, etc. Support *. bin, *. hex, *. srec, *. s19, *. benc, *. Henc and *. senc files. (As shown in Figure 26)

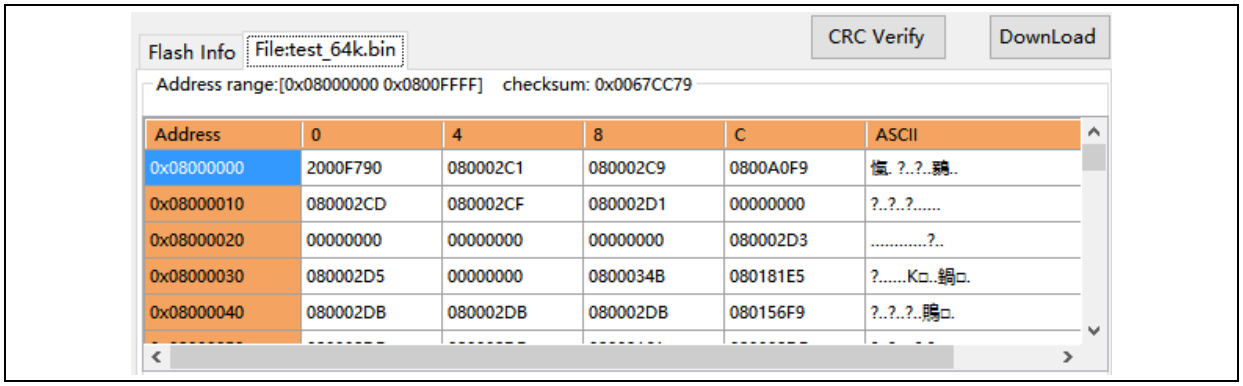
Figure 26. File info



- Add

Add files to the download list and display the file data in the “file info “list. It can support up to 5 files.When the file is successfully opened, the file content is automatically displayed in the "File Info”. (As shown in Figure 27)

Figure 27. File info data

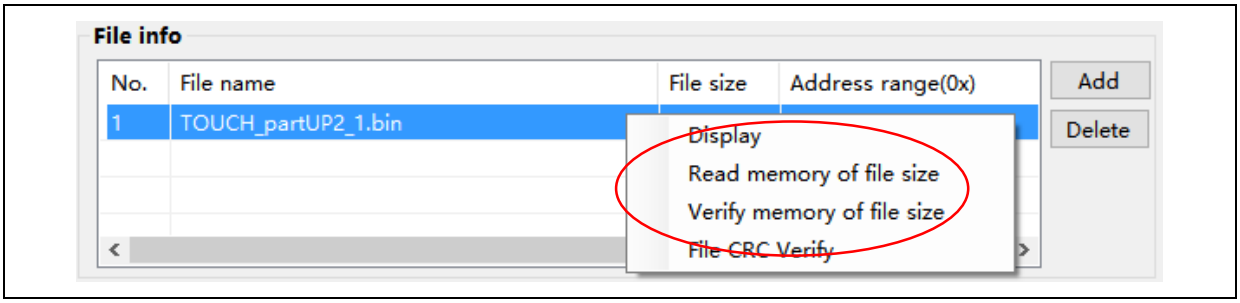


- Delete

Delete the selected files in the file list.

- Right click menu

Figure 28. Right click menu



- Display: displays the content of the selected file in the "File Info" list.
- Read memory of file size: read the data of the selected file from the memory.
- Verify memory of file size: read and select the data from the files for verification.
- Flash CRC Verify: CRC check between the selected file and the corresponding memory data. (AT32F403 does not support)

3.11 Erase function

Erase the main Flash and SPIM. (Menu bar — "***Target***")

■ Mass erase

Erase the whole main flash.

When SPIM is selected, the whole SPIM will be erased. (AT32F403/F413/F403A/F407)

When the boot memory is in AP mode, erase the boot memory. (AT32F415/F421/F425)

■ Erase main flash

Erase the whole main Flash.

■ Erase SPIM

Erase the whole SPIM.

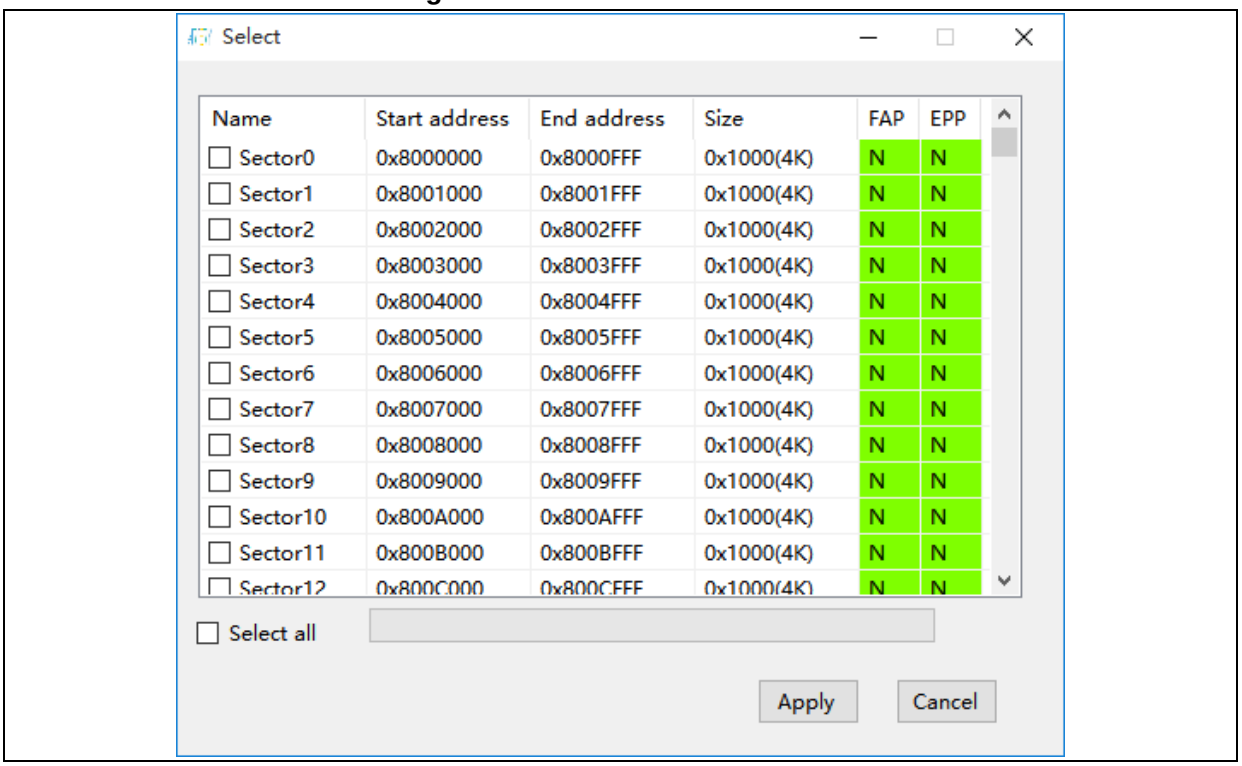
■ Erase boot memory

When the boot memory is in AP mode, erase the boot memory. (AT32F415/F421/F425)

■ Erase sectors

User selects sectors to erase. ***"Target***" - "***Erase sectors"***. (As shown in Figure 29)

Figure 29. Sector erase

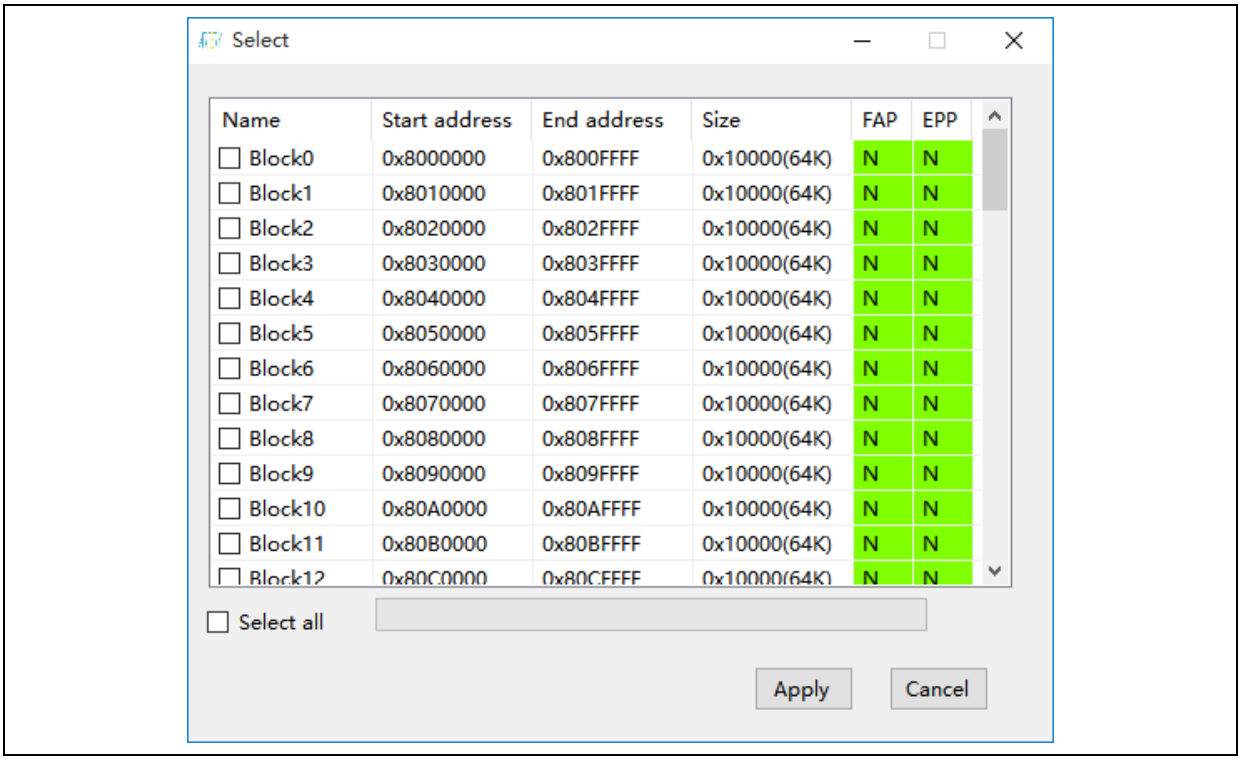


- Apply: erase the selected sectors.
- Cancel: cancel the erase operation during the erase process.

■ Erase blocks

User selects blocks to erase. ***"Target***" - "***Erase blocks"***. (As shown in Figure 30)

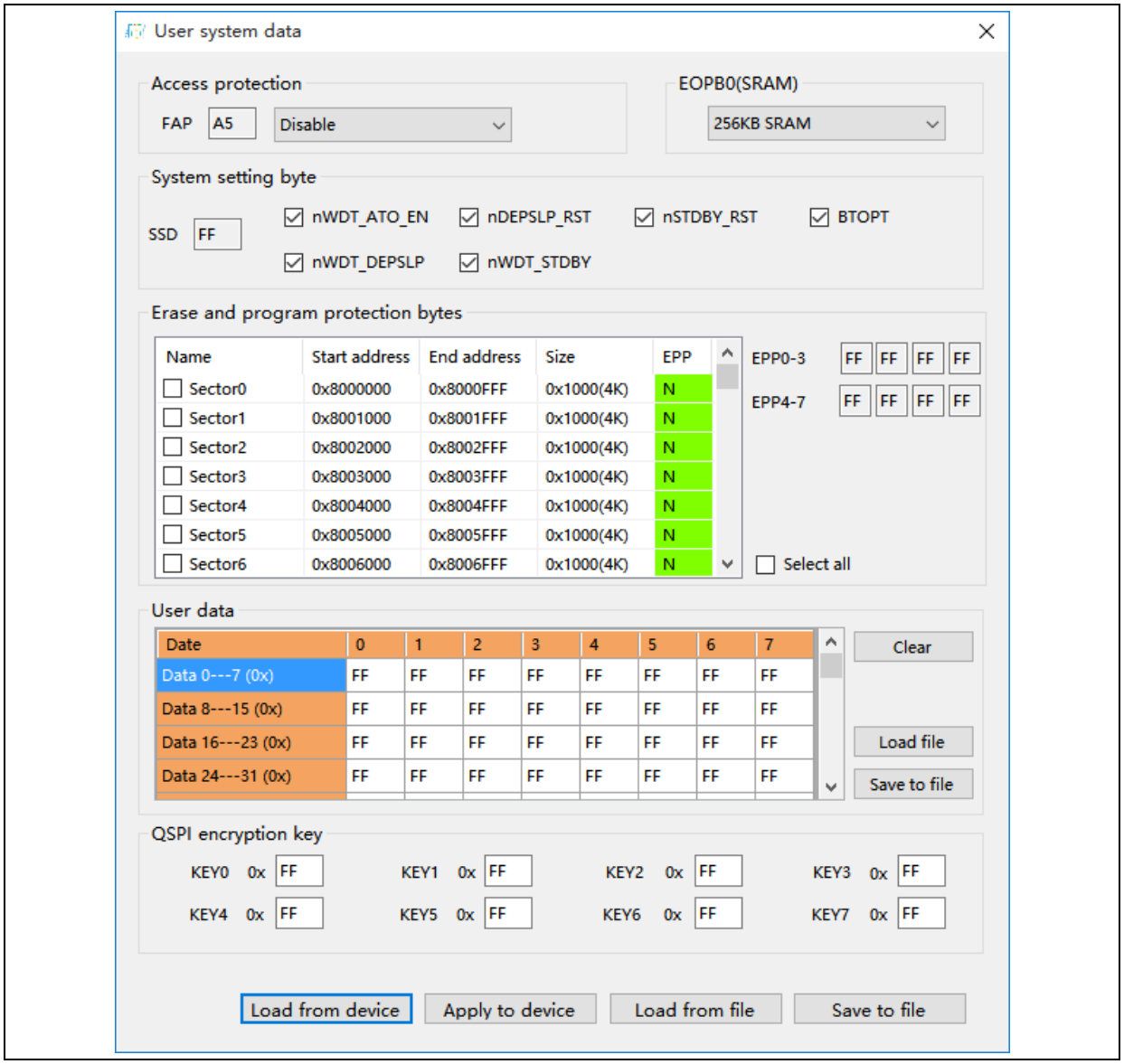
Figure 30. Block erase



3.12 User system data

This is for the programming of user system data, (Menu bar — "***Target***" — "***User system data***"). (As shown in Figure 31)

Figure 31. User system data config



■ Access protection: Enable / disable access protection.

AT32F403/F413/F403A/F407/F435/F437:

Enabled: FAP----0xFF

Disabled: FAP---0xA5

AT32F415/F421/F425:

Access protection: FAP----0xFF.

High level access protection: FAP----0xCC. (Access protection and user system data erase protection) (AT32F425 high level access protection is irreversible. Once enabled, it will never be unlocked, with its debugging interface permanently disabled. Please use with caution.)

Disabled: FAP----0xA5.

When access protection is enabled, neither flash nor the user system data will be readable. The

operation can only be performed after the access protection is disabled.
When access protection is disabled, both the main flash and the user system data will be erased.

■ System setting byte

nWDT_ATO_EN:
Unchecked—Hardware watchdog.
Checked—Software watchdog.

nDEPSLP_RST:
Unchecked—Reset occurs when entering Deep Sleep mode.
Checked—No reset occurs when entering Deep Sleep mode.

nSTDBY_RST:
Unchecked—Reset occurs when entering Standby mode.
Checked—No reset occurs when entering Standby mode.

BTOPT (AT32F403/F413/F403A/F407/F435/F437)
Unchecked—when the device is set to boot from flash memory bank 1 or bank 2, if bank 2 has no startup program, boots from bank 1, otherwise, bank 2.
Checked—when the device is set to boot from flash memory (default value), it starts from bank 1.

nBOOT1 (AT32F421/F425)
Boot mode is determined together with BOOT0, and when BOOT0 = 1,
Unchecked----SRAM is selected as boot space.
Checked---Boot memory is selected as boot space.

nWDT_DEPSLP:
Unchecked----WDT stop count when entering Deep Sleep mode.
Checked---WDT does not stop count when entering Deep Sleep mode.

nWDT_STDBY:
Unchecked---- WDT stop count when entering Standby mode.
Checked--- WDT does not stop count when entering Standby mode.

■ EOPB0(SRAM)

AT32F403/F403A/F407: (AT32F403CBT6 not support)
224 KB SRAM—SRAM 224 KB.
96 KB SRAM—SRAM 96 KB.

AT32F413: (AT32F413C8T7/AT32FEBKC8T7 not support)
64 KB SRAM—SRAM 64 KB.
32 KB SRAM—SRAM 32 KB.
16 KB SRAM—SRAM 16 KB.

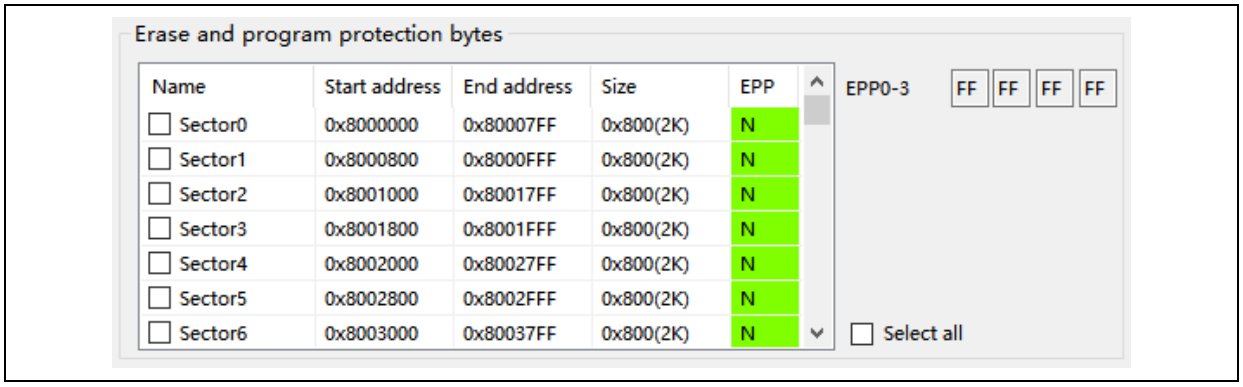
AT32F415/F421/F425: (not support)

AT32F435/F437:
Flash size 256K and below:
512 KB SRAM—SRAM 512 KB.
448 KB SRAM—SRAM 448 KB.
384 KB SRAM—SRAM 384 KB.
Flash size 1024K and above:
512 KB SRAM—SRAM 512 KB.
448 KB SRAM—SRAM 448 KB.
384 KB SRAM—SRAM 384 KB.
320 KB SRAM—SRAM 320 KB.
256 KB SRAM—SRAM 256 KB.
192 KB SRAM—SRAM 192 KB.
128 KB SRAM—SRAM 128 KB.

- Erase and program protection bytes

Users can select the sector that needs to be erase and program protected. (As shown in Figure 32)

Figure 32. Erase and program protection bytes



EPP0:
AT32F403/F413/F403A/F407: controls the erase and program protection of sectors in the range of Flash 1K-32K.
AT32F415: controls the erase and program protection of Sector0-Sector15.
AT32F421: controls the erase and program protection of Sector0-Sector31.
AT32F435/F437: controls the erase and program protection of sectors in the range of Flash 1K-32K. Each bit protects 4K bytes sectors.
AT32F425: controls the erase and program protection of Sector0-Sector31.

EPP1:
AT32F403/F413/F403A/F407: controls the erase and program protection of sectors in the range of Flash 33K-64K.
AT32F415: controls the erase and program protection of Sector16-Sector31.
AT32F421: controls the erase and program protection of Sector32-Sector63.
AT32F435/F437: controls the erase and program protection of sectors in the range of Flash 33K-64K. Each bit protects 4K bytes sectors.
AT32F425: controls the erase and program protection of Sector32-Sector63.

EPP2:

AT32F403/F413/F403A/F407: controls the erase and program protection of sectors in the range of Flash 65K-96K.
AT32F415: controls the erase and program protection of Sector32-Sector47.
AT32F435/F437: controls the erase and program protection of sectors in the range of Flash 65K-96K. Each bit protects 4K bytes sectors.

EPP3:
AT32F403/F413/F403A/F407:
Bit 0-6 controls the erase and program protection of sectors in the range of 97K-124K;
Bit 7 controls the erase and program protection of all Sectors after Flash 124K, including SPIM.
AT32F415:
Bits 0-6 control the erase and program protection of Sector48-Sector61;
Bit 7 controls the erase and program protection of all subsequent sectors, including boot memory (boot memory in AP mode).
AT32F421: Bit 7 controls the boot memory area (boot memory in AP mode)
AT32F435/F437: controls the erase and program protection of sectors in the range of Flash 97K-128K. Each bit protects 4K bytes sectors.
AT32F425: Bit 7 controls the boot memory area (boot memory in AP mode)

EPP4:
AT32F435/F437: controls the erase and program protection of sectors in the range of Flash 129K-1152K. Each bit protects 128K bytes sectors.

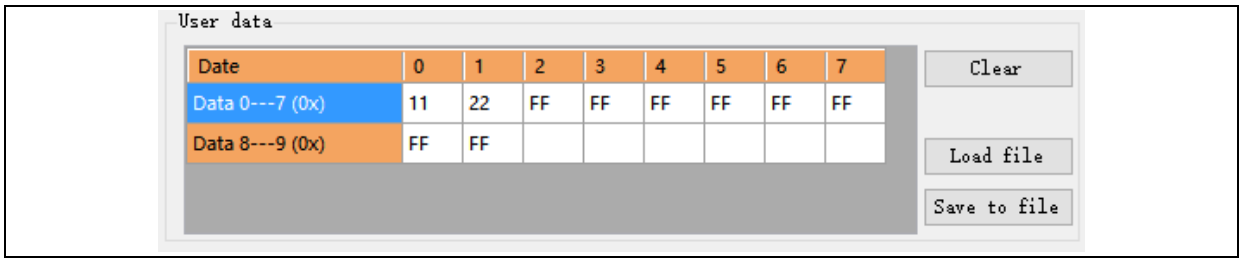
EPP5:
AT32F435/F437: controls the erase and program protection of sectors in the range of Flash 1153K-2176K. Each bit protects 128K bytes sectors.

EPP6:
AT32F435/F437: controls the erase and program protection of sectors in the range of Flash 2177K-3200K. Each bit protects 128K bytes sectors.

EPP7:
AT32F435/F437: Bit 0-6 controls the erase and program protection of sectors in the range of Flash 3201K-4032K. Each bit protects 128K bytes sectors.

- User data

Figure 33. User data



AT32F403/F413/F403A/F407: user data 8 bytes.
AT32F415: user data 506 bytes.
AT32F421: user data 250 bytes.

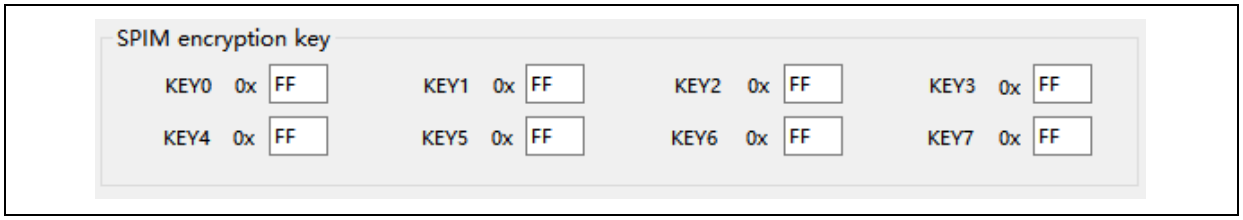
AT32F435/F437: Flash size is less than 4032K, user data 220 bytes. Flash size 4032K, user data 2012 bytes.
AT32F425: user data 250 bytes.

Clear： Reset all user data to 0xFF, which is not saved to the device
Load file：Load the user data file into the table for display
Save to file：Save the user data in the table to the file.

- SPIM encryption key (AT32F403/F413/F403A/F407)

Users can set the encryption key when downloading. (As shown in Figure 34)

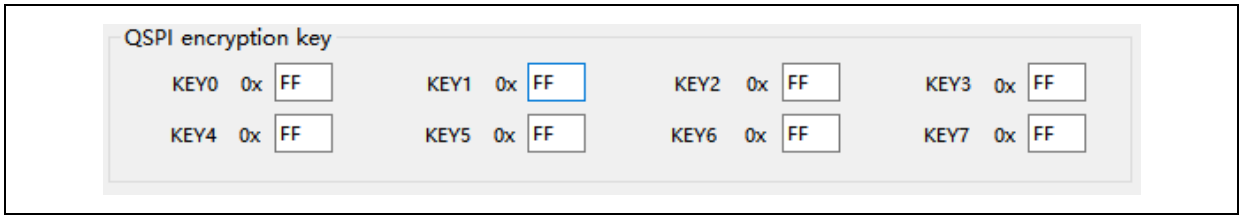
Figure 34. SPIM encryption key config



- QSPI encryption key (AT32F435/F437)

Users can set the encryption key when downloading. (As shown in Figure 35)

Figure 35. QSPI encryption key config



- Load from device

Read the user system data from the device and update it to the interface for display.

- Apply to device

Save the settings of the user system data to the device.

- Load from file

Load the content of the saved user system data file and update it to the interface for display.

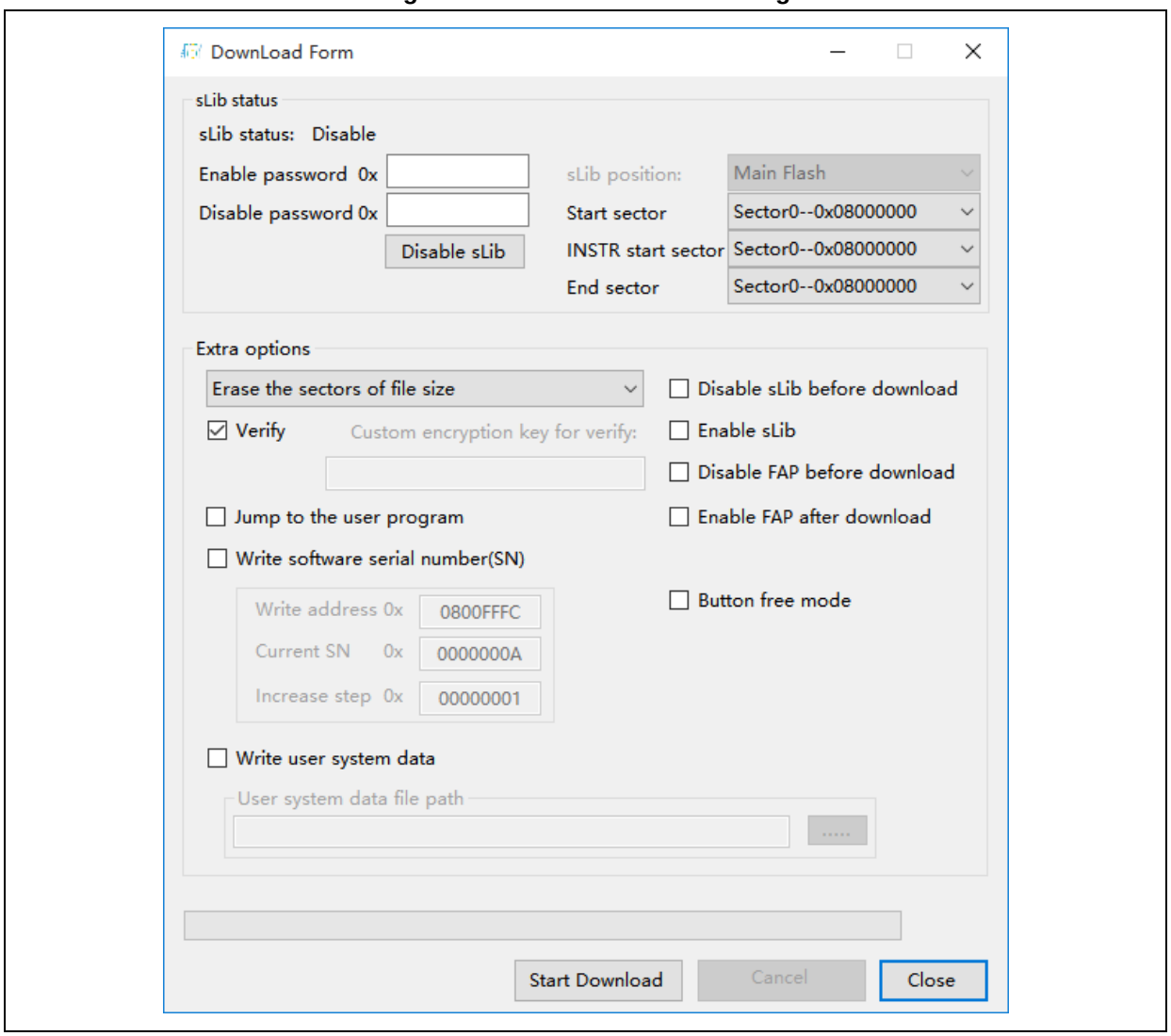
- Save to file

Save the user system data settings to file.

3.13 Download function

Users can go to "***Menu bar***" — "***Target***" — "***Download***", or click on "***Download***" on the main interface.
(As shown in Figure 36)

Figure 36. Online download config



1) sLib Setting

（AT32F403 not support sLib function）

■ sLib status

Displays the current sLib status, disable or enable.

■ Remaining usage times (AT32F413/F403A/F407)

It means the remaining usage times of sLib, and it can be used up to 256 times, which will be reduced one by one after each use. When the remaining time is 0, the sLib function will not be available.

■ Enable password

It refers to the password when the sLib is enabled.

- Disable password

It is the password when the sLib is disabled.

- sLib position (AT32F415/F421/F425)

sLib can be configured in main flash or boot memory (boot memory is in AP mode).

- Start sector

AT32F413/F415/F403A/F407：

The start position of sLib area. The instruction area is the area from "Start sector" to "DATA start sector" (excluding DATA start sector). Once sLib is enabled, the data in this area cannot be erased, written or read.

AT32F421/F435/F437/F425：

The start position of sLib area. The area from “Start sector” to “INSTR start sector” (not including “INSTR start sector”) is a mixed instruction and data (read only area). Once sLib is enabled, the data in this area cannot be erased, written, but can be read.

- DATA start sector/ INSTR start sector

AT32F413/F415/F403A/F407：

The start sector of sLib data area. The data area is from "DATA start sector" to "End sector" (including "End sector"). After sLib is enabled, the data in this area cannot be erased or written, but can be read. When it is set to "none", it is no data area.

AT32F421/F435/F437/F425：

The start sector of sLib instruction area. The instruction area is from "INSTR start sector" to "End sector" (including "End sector"). After sLib is enabled, the data in this area cannot be erased, written or read. When it is set to "none", it is no instruction area.

- End sector

The end position of the sLib area.

- Disable sLib

Disable sLib. Users need to enter the password that last enabled. When sLib is successfully disabled, the whole chip will be erased.

2) Extra options

- Mass erase for Main Flash

If the download address of the file is located in main flash, the whole main flash will be erased.

- Mass erase for SPIM

If the download address of file is located in SPIM, the whole SPIM will be erased.

- Mass erase for Main Flash and SPIM

If the download address of the file is located in both the main flash and the SPIM, the main

flash and the SPIM will be completely erased.

- Mass erase for Main Flash and Boot memory (AT32F415/F421/F425)

If the download address of the file is located in both the main flash and the boot memory, the main flash and the boot memory will be completely erased.

(For "Mass erase for Main Flash", " Mass erase for SPIM", " Mass erase for Main Flash and SPIM", and “Mass erase for Main Flash and Boot memory", these four options will be selected automatically based on the download files)

- Erase the sectors of file size

According to the download address of the file, it will automatically determine which sector needs to be erased.

- Disable sLib before download

To disable sLib before download, you need to enter the password you last enabled.

- Enable sLib

Enable the sLib function when download. It is necessary to enter sLib password, start sector, DATA start sector/ INSTR start sector, and end sector.

- Disable FAP before download (for button free download)

If the chip is in the access protection state, the access protection will be automatically disabled before download.

- Verify

After the download is completed, the corresponding data in the memory is read and then verified to determine whether the download is successful.If this option is unchecked, no verify is performed after download, so it is impossible to determine whether the downloaded content is correct.

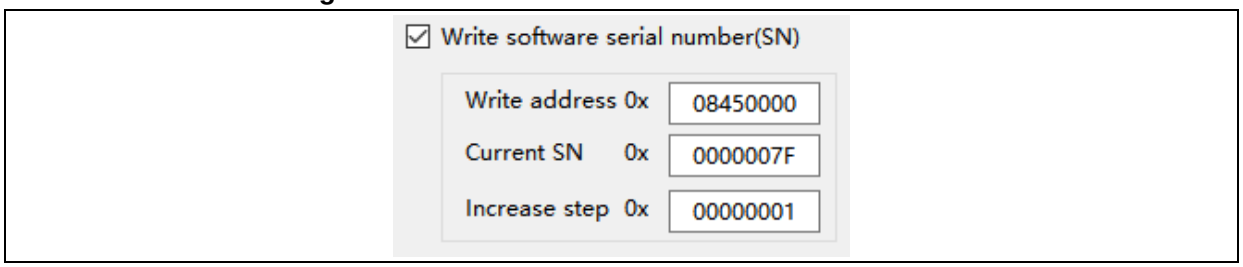
- Jump to the user program

After the download is complete, the code downloaded to the Flash address 0x08000000 will be executed.

- Write software serial number(SN)

Select this option to automatically program the serial number for each device after the program file is downloaded. This can be set as Figure 37:

Figure 37. Write software serial number

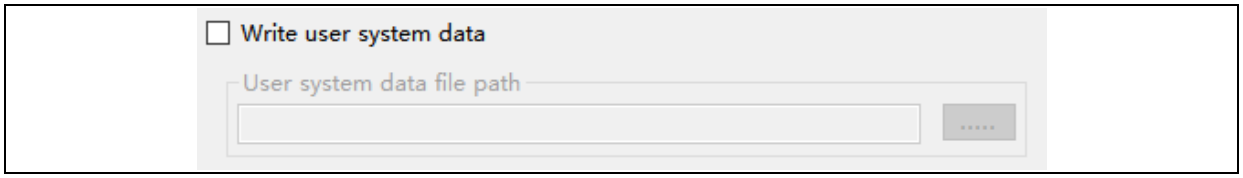


- Write address: the address where the serial number is programmed into the memory.
- Current SN: the serial number of the current programming.
- Increase step: this is the amount added to the next serial number after each serial number is programmed.

■ Write user system data

Select this option to automatically write user system data to the device after the program file is downloaded and the serial number is programmed. This can be set as in Figure 38:

Figure 38. User system data file selection



: Select the user system data file. BIN and HEX formats are supported.

■ Enable FAP after download

After the above operations such as download are completed, enable access protection. AT32F415/F421/F425 can be set to enable access protection and high level access protection (access protection and user system data erase protection). (AT32F425 high level access protection is irreversible. Once enabled, it will never be unlocked, with its debugging interface permanently disabled. Please use with caution.)

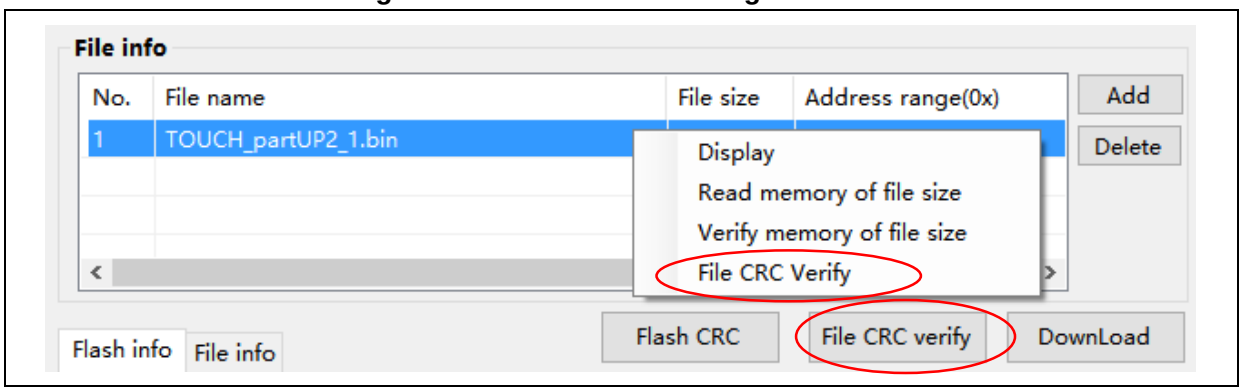
■ Button free mode (Only for AT-Link)

After one device download is completed, replace it with another device for continuous downloading

3.14 File CRC verify function

(AT32F413/F415/F403A/F407/F421/F435/F437/F425 support CRC check function (SPIM not supported)) (As shown in Figure 39)

Figure 39. CRC function config



■ Method 1:

Select the file to be checked, right click, and select "***File CRC verify***" in the right-click menu.

■ Method 2:

Select the file to be verified and click "***File CRC verify***" button directly.

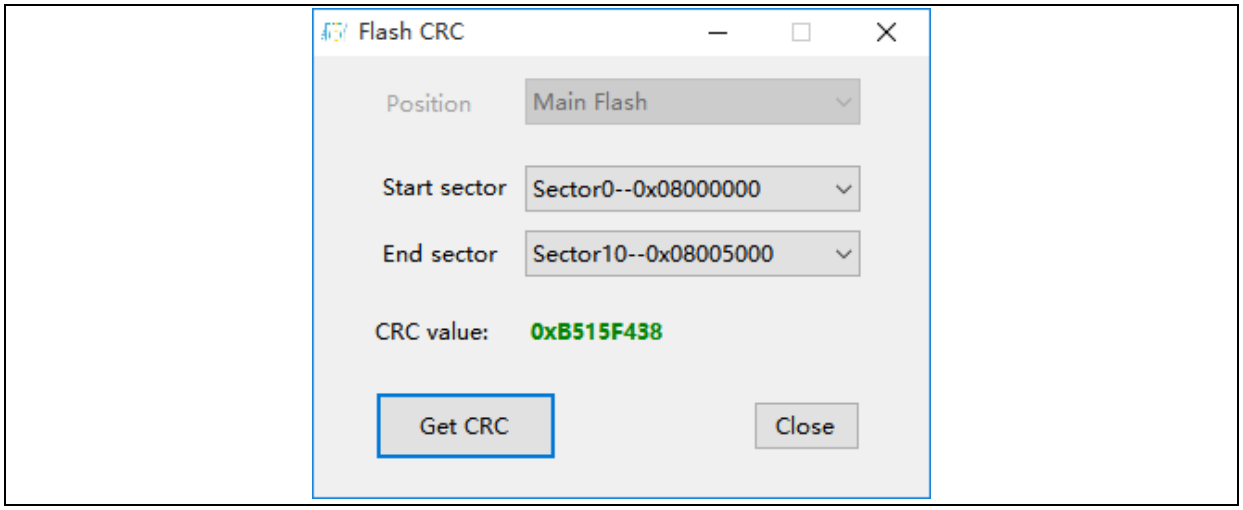
3.15 Flash CRC

AT32F413/F415/F403A/F407/F421/F435/F437/F425 series support Flash CRC function (SPIM does not support)

(Menu bar---"***Target***"---"***Flash CRC***") or (Main interface---"***Flash CRC***")

As shown in below Figure 40

Figure 40. Flash CRC



— Calculation area: main Flash and boot memory (AT32F415/F421/F425 in AP mode)

— Start sector: the start sector of calculating CRC

— End sector: the end sector of calculating CRC

— CRC value: the calculated CRC value

- Obtain CRC: start calculating CRC value.

- Close: close this dialog box.

3.16 SPIM encryption download

SPIM encryption principle:

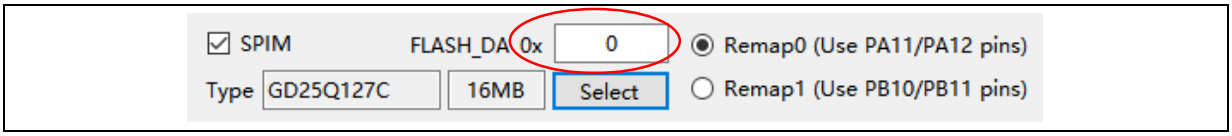
When SPIM encrypted download is required, users must first configure the SPIM FLASH_DA and SPIM encryption key (Key is set in the user system data) before download. In this case, the MCU will encrypt the downloaded original data according to the SPIM FLASH_DA and encryption key as well as the algorithm set in the MCU, then write the encrypted data to SPIM.

When need to read the encrypted data of the SPIM, users also need to configure the SPIM FLASH_DA and encryption key. Based on the SPIM FLASH_DA and encryption key, MCU uses the MCU's internal algorithm to decrypt the encrypted data and restore it to the correct original data.

When downloading files to SPIM, the following steps can be set to encrypt the downloaded content. (AT32F415/F421/F435/F437/F425 not support SPIM)

Step 1: set the FLASH_DA of the SPIM. (As shown in Figure 41)

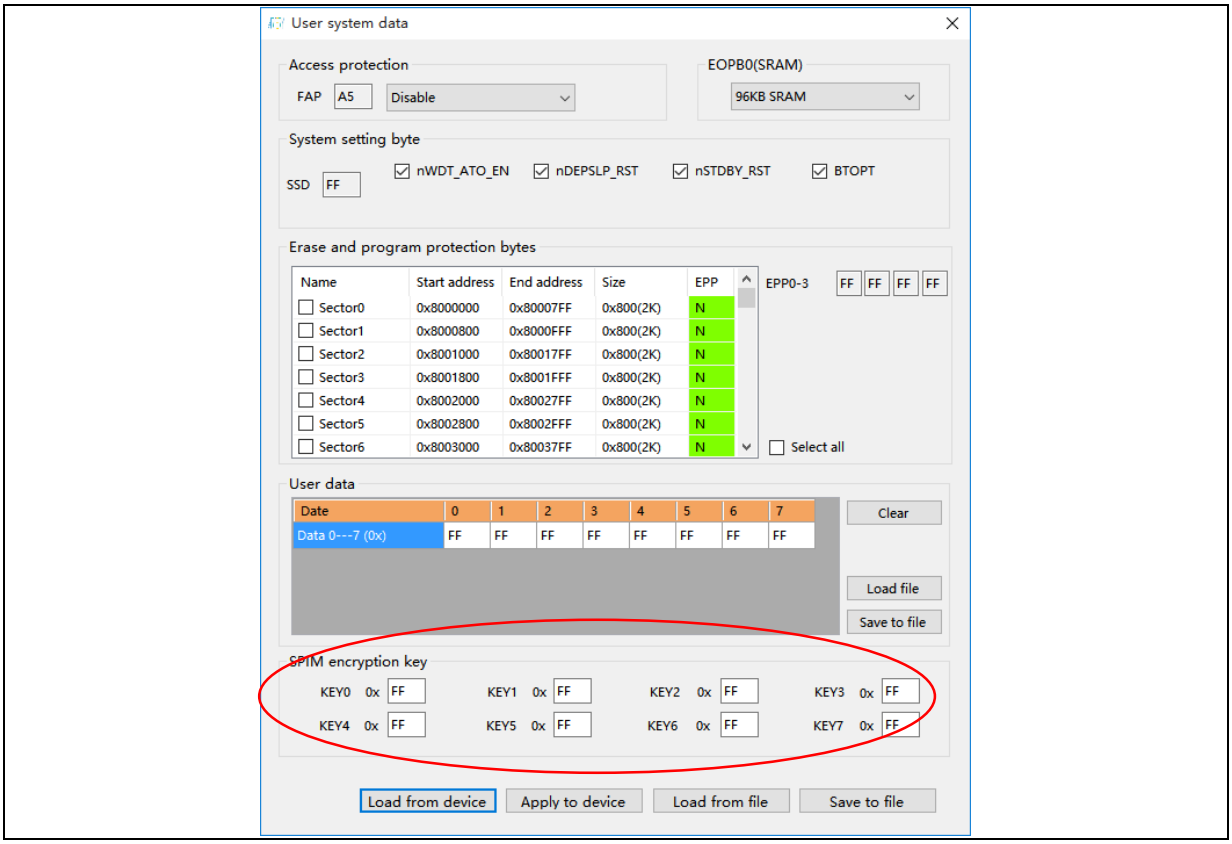
Figure 41. SPIM encryption range config



Users can set the range to be encrypted starting from 0x08400000.
If encryption is not required, set to 0.

Step 2: set the SPIM encryption key through the "user system data" page. (As shown in Figure 42)

Figure 42. SPIM encryption key config



This is the encryption / decryption key for downloading and reading data in the encrypted range of the SPIM. When the access protection is disabled, the key is also erased.

Step 3: Download the file to SPIM normally to implement encrypted download.

4 Revision history

Table 1. Document revision history

Date	Revision	Changes
2021.10.13	V2.00	1. Initial release. Support for AT32F403/F413/F415/F421/F403A/F407/F435/F437.
2021.11.26	V2.01	1. Support for AT32F425. 2. Support for AT32F403AVGW.

IMPORTANT NOTICE – PLEASE READ CAREFULLY

Purchasers understand and agree that purchasers are solely responsible for the selection and use of Artery's products and services.

Artery's products and services are provided "AS IS" and Artery provides no warranties express, implied or statutory, including, without limitation, any implied warranties of merchantability, satisfactory quality, non-infringement, or fitness for a particular purpose with respect to the Artery's products and services.

Notwithstanding anything to the contrary, purchasers acquires no right, title or interest in any Artery's products and services or any intellectual property rights embodied therein. In no event shall Artery's products and services provided be construed as (a) granting purchasers, expressly or by implication, estoppel or otherwise, a license to use third party's products and services; or (b) licensing the third parties' intellectual property rights; or (c) warranting the third party's products and services and its intellectual property rights.

Purchasers hereby agrees that Artery's products are not authorized for use as, and purchasers shall not integrate, promote, sell or otherwise transfer any Artery's product to any customer or end user for use as critical components in (a) any medical, life saving or life support device or system, or (b) any safety device or system in any automotive application and mechanism (including but not limited to automotive brake or airbag systems), or (c) any nuclear facilities, or (d) any air traffic control device, application or system, or (e) any weapons device, application or system, or (f) any other device, application or system where it is reasonably foreseeable that failure of the Artery's products as used in such device, application or system would lead to death, bodily injury or catastrophic property damage.