AN13042

Firmware flashing via direct SWD access

Rev. 1.03 — 2 June 2021

Application note

Document information

Information	Content
Keywords	SWD, IAP, firmware
Abstract	How to flash the final firmware image into the flash memory of the NHS31xx directly accessing the SWD pins.

Revision history

Rev	Date	Description
v.1.0	20210602	Major format update and refresh of contents
v.0.2	20170209	Changes after review
v.0.1	20170105	Initial version

1 Introduction

This document gives an overview of how to flash the final firmware image into the flash memory of the NHS31xx by directly accessing the SWD pins on the chip.

Universal programmers in an automated programming system cannot use the FlashMagic tool connected with an LPC-Link2 board. In this case, programming can be done via the ROM IAP calls, which are built into the NHS31xx IC family. IAP calls can be issued both from code running within the chip and through a debug interface. All NHS31xx ICs house a two-wired debug interface using SWD. An SWD programmer can then use the debug interface of the chip to program the on-chip FLASH memory directly.

1.1 NHS31xx overview

To program the NHS31xx via IAP calls over direct SWD communication, these characteristics must be taken into account:

- SWD is available on `PIO10` and `PIO11`. These pins are by default configured to carry the `SWCLK` resp. `SWDIO` functionality.
- The NHS31xx houses 30 kB of flash memory which can be freely used by the application firmware. It can be used either to house in-place executable code or to store sensor/sample data in a non-volatile way.
- The flash is divided into 30 sectors of 1 kB each. Each sector is subdivided in flash pages of 64 bytes each.
- The IAP entrance address is `0x1fff 1ff1`.
- All members of the NHS31xx family support the following IAP functions:
  - Read factory settings
  - Read part identity
  - Read device UID
  - Read boot code version
  - Prepare/unlock a flash sector for program/erase
  - Erase one or more contiguous flash sectors
  - Erase one or more contiguous flash pages
  - Blank check sectors
  - Copy data to flash
  - Compare memory sections

More information about the IAP functionality of NHS31xx ICs is found in the "NHS31xx user manual (UM10876; Ref. 1).

2 SWD protocol

SWD is a debug interface defined by Arm.

Of all the extensive debug features, only a small subset is required for programming, enabling these actions:

- Reset, halt, and resume the execution of the processor.
- Modify core registers of the processor to change its execution context and flow.
- Full access to the memory space of the processor to download data to be programmed.

The full specification and detailed information on the SWD protocol can be found in document `IHI0031F` "ARM Debug Interface Architecture Specification" (Ref. 2), created and maintained by Arm.

3 How to program flash using IAP via SWD

The functions provided by the debug interface are sufficient to invoke IAP and so to program the on-chip flash. Figure 1 shows the overall steps of programming.

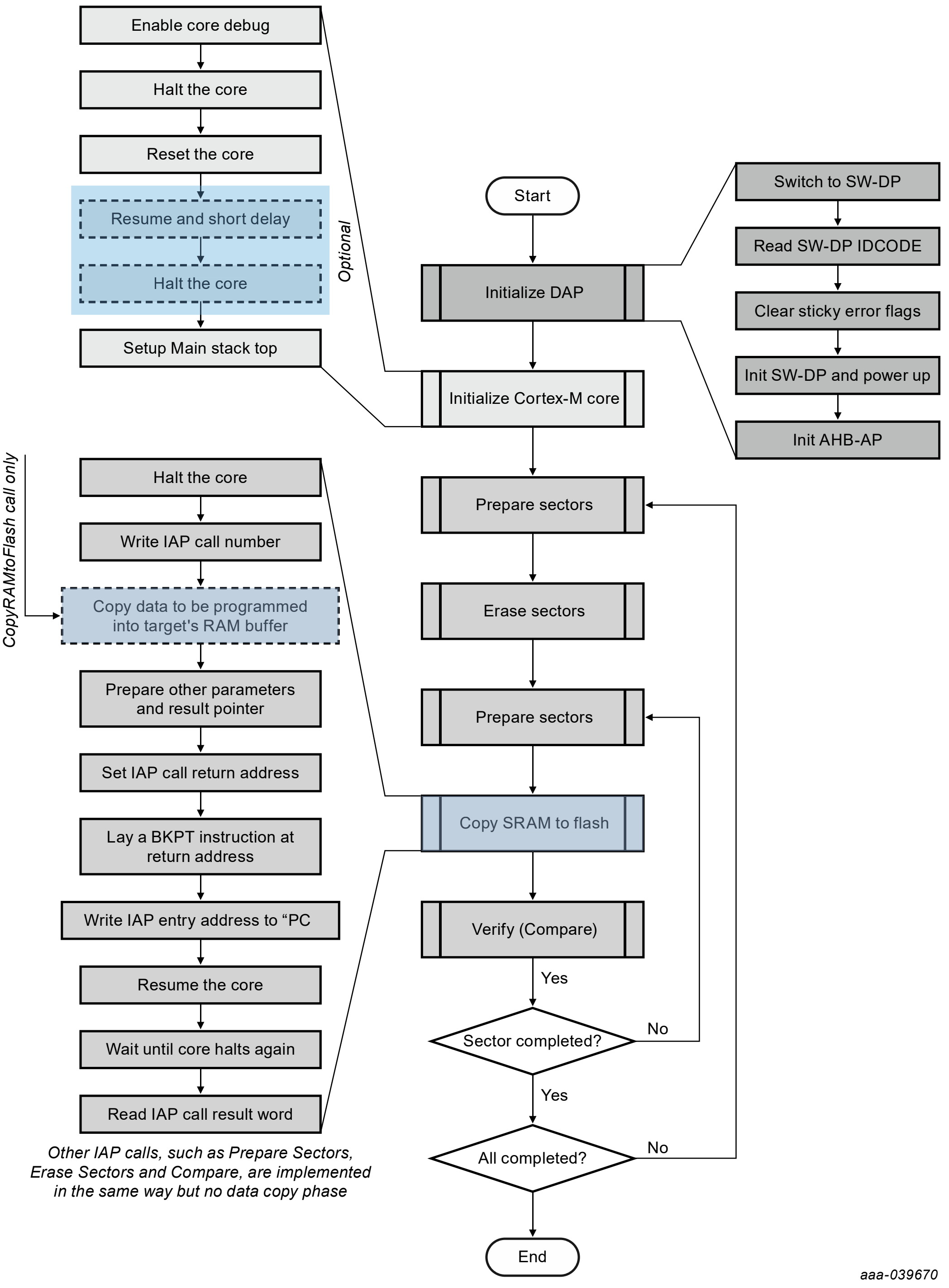

Figure 1. IAP over SWD flow diagram

3.1 Initialization

First, the CPU context must be prepared, which corresponds to the top portion of the flow diagram.

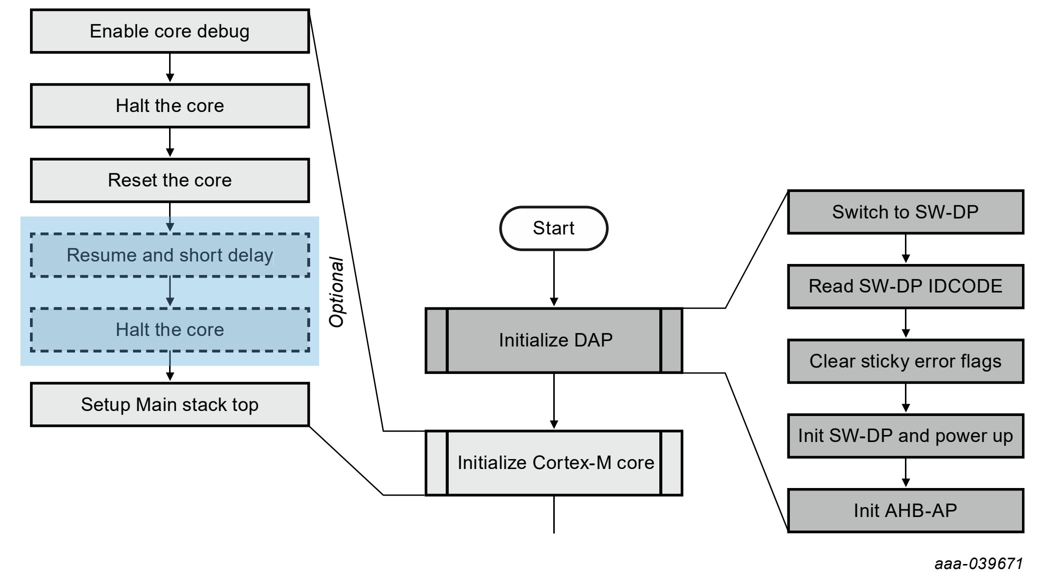

Figure 2. Target initialization for IAP

3.1.1 One-shot initializations

- Initialize the DAP, and enable core debug (see Arm documentation).
- Reset the core, resume the core (in case the core has been halted), and wait a while to ensure the boot loader (ROM code) has completed its initializations (~ 2.8 ms).
- Set up the stack by setting the MSP register of the Cortex-M processor to a proper value. An offset of 1.5 kB above the SRAM base is sufficient.

3.1.2 Prepare the context and invoke IAP

Following the requirements to invoke IAP calls, we allocate:

- 5 words of SRAM to store the command code and parameters
- 5 words of SRAM to store the result of the IAP call
- 1 word of SRAM as the IAP return address
- 1024 bytes buffer for the "Copy (S)RAM to Flash" IAP call

As long as the addresses do not overlap or collide with the stack, they can be arranged from the start of SRAM or anywhere at will. As a rule of thumb, maintain a gap of 256 bytes for the stack.

3.2 IAP calls

Code running within the MCU is intended invoke IAP functions. To invoke these functions via SWD, these key operations must be executed carefully.

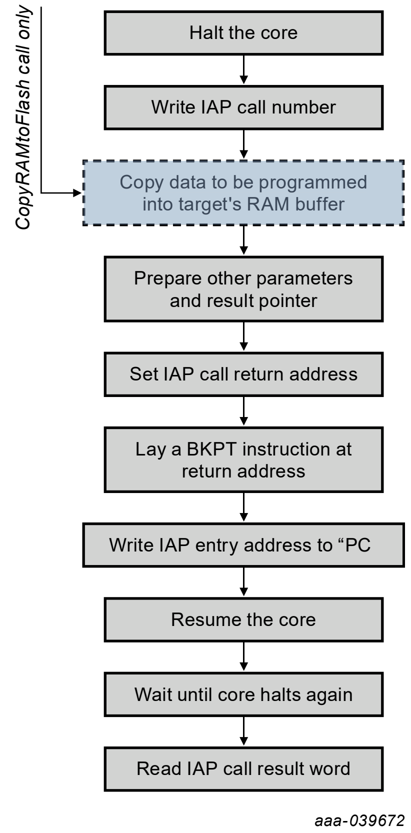
CopyRAMtoFlash call only
Halt the core
Write IAP call number
Copy data to be programmed into target's RAM buffer
Prepare other parameters and result pointer
Set IAP call return address
Lay a BKPT instruction at return address
Write IAP entry address to “PC
Resume the core
Wait until core halts again
Read IAP call result word
aaa-039672

Figure 3. Prepare IAP context

Figure 3 illustrates the "Copy (S)RAM top flash" IAP call. However, all IAP calls share the framework.

- To invoke an IAP function by writing to the SRAM of the target through the SWD debug channel, prepare the parameter list.
- To make the core automatically halt when the IAP function returns, specify the IAP return address (at a known address in SRAM) and lay a breakpoint instruction `BKPT` (a 16-bit integer) at the return address.
- Specify the program counter `PC`: Write the IAP entry address, as such when the core is resumed, the IAP function is executed.
- Resume the core and wait for the core to halt again.
- To examine if the core halts, keep polling the status of the core. After the core has halted again, read the results of this instance of IAP invoke.

4 Abbreviations

Table 1. Abbreviations

Acronym	Description
BKTP	breakpoint
CPU	central processing unit
DAP	debug access port
IAP	in-application programming
MCU	microcontroller unit
MSP	main stack pointer
RAM	random-access memory
ROM	read-only memory
SRAM	static random-access memory
SWD	serial wire debug
UID	unique id

5 References

[1] **UM10876 user manual** — NHS31xx user manual; 2020, NXP Semiconductors

[2] **IHI0031F** — Arm Debug Interface Architecture Specification; 2020, ARM Limited

6 Legal information

6.1 Definitions

Draft — A draft status on a document indicates that the content is still under internal review and subject to formal approval, which may result in modifications or additions. NXP Semiconductors does not give any representations or warranties as to the accuracy or completeness of information included in a draft version of a document and shall have no liability for the consequences of use of such information.

6.2 Disclaimers

Limited warranty and liability — Information in this document is believed to be accurate and reliable. However, NXP Semiconductors does not give any representations or warranties, expressed or implied, as to the accuracy or completeness of such information and shall have no liability for the consequences of use of such information. NXP Semiconductors takes no responsibility for the content in this document if provided by an information source outside of NXP Semiconductors.

In no event shall NXP Semiconductors be liable for any indirect, incidental, punitive, special or consequential damages (including - without limitation - lost profits, lost savings, business interruption, costs related to the removal or replacement of any products or rework charges) whether or not such damages are based on tort (including negligence), warranty, breach of contract or any other legal theory.

Notwithstanding any damages that customer might incur for any reason whatsoever, NXP Semiconductors' aggregate and cumulative liability towards customer for the products described herein shall be limited in accordance with the Terms and conditions of commercial sale of NXP Semiconductors.

Right to make changes — NXP Semiconductors reserves the right to make changes to information published in this document, including without limitation specifications and product descriptions, at any time and without notice. This document supersedes and replaces all information supplied prior to the publication hereof.

Suitability for use — NXP Semiconductors products are not designed, authorized or warranted to be suitable for use in life support, life-critical or safety-critical systems or equipment, nor in applications where failure or malfunction of an NXP Semiconductors product can reasonably be expected to result in personal injury, death or severe property or environmental damage. NXP Semiconductors and its suppliers accept no liability for inclusion and/or use of NXP Semiconductors products in such equipment or applications and therefore such inclusion and/or use is at the customer's own risk.

Applications — Applications that are described herein for any of these products are for illustrative purposes only. NXP Semiconductors makes no representation or warranty that such applications will be suitable for the specified use without further testing or modification.

Customers are responsible for the design and operation of their applications and products using NXP Semiconductors products, and NXP Semiconductors accepts no liability for any assistance with applications or customer product design. It is customer's sole responsibility to determine whether the NXP Semiconductors product is suitable and fit for the customer's applications and products planned, as well as for the planned application and use of customer's third party customer(s). Customers should provide appropriate design and operating safeguards to minimize the risks associated with their applications and products.

NXP Semiconductors does not accept any liability related to any default, damage, costs or problem which is based on any weakness or default in the customer's applications or products, or the application or use by customer's third party customer(s). Customer is responsible for doing all necessary testing for the customer's applications and products using NXP Semiconductors products in order to avoid a default of the applications and the products or of the application or use by customer's third party customer(s). NXP does not accept any liability in this respect.

Export control — This document as well as the item(s) described herein may be subject to export control regulations. Export might require a prior authorization from competent authorities.

Evaluation products — This product is provided on an "as is" and "with all faults" basis for evaluation purposes only. NXP Semiconductors, its affiliates and their suppliers expressly disclaim all warranties, whether express, implied or statutory, including but not limited to the implied warranties of non-infringement, merchantability and fitness for a particular purpose. The entire risk as to the quality, or arising out of the use or performance, of this product remains with customer.

In no event shall NXP Semiconductors, its affiliates or their suppliers be liable to customer for any special, indirect, consequential, punitive or incidental damages (including without limitation damages for loss of business, business interruption, loss of use, loss of data or information, and the like) arising out the use of or inability to use the product, whether or not based on tort (including negligence), strict liability, breach of contract, breach of warranty or any other theory, even if advised of the possibility of such damages.

Notwithstanding any damages that customer might incur for any reason whatsoever (including without limitation, all damages referenced above and all direct or general damages), the entire liability of NXP Semiconductors, its affiliates and their suppliers and customer's exclusive remedy for all of the foregoing shall be limited to actual damages incurred by customer based on reasonable reliance up to the greater of the amount actually paid by customer for the product or five dollars (US$5.00). The foregoing limitations, exclusions and disclaimers shall apply to the maximum extent permitted by applicable law, even if any remedy fails of its essential purpose.

Translations — A non-English (translated) version of a document is for reference only. The English version shall prevail in case of any discrepancy between the translated and English versions.

Security — Customer understands that all NXP products may be subject to unidentified vulnerabilities or may support established security standards or specifications with known limitations. Customer is responsible for the design and operation of its applications and products throughout their lifecycles to reduce the effect of these vulnerabilities on customer's applications and products. Customer's responsibility also extends to other open and/or proprietary technologies supported by NXP products for use in customer's applications. NXP accepts no liability for any vulnerability. Customer should regularly check security updates from NXP and follow up appropriately.

Customer shall select products with security features that best meet rules, regulations, and standards of the intended application and make the ultimate design decisions regarding its products and is solely responsible for compliance with all legal, regulatory, and security related requirements concerning its products, regardless of any information or support that may be provided by NXP.

NXP has a Product Security Incident Response Team (PSIRT) (reachable at PSIRT@nxp.com) that manages the investigation, reporting, and solution release to security vulnerabilities of NXP products.

6.3 Trademarks

Notice: All referenced brands, product names, service names, and trademarks are the property of their respective owners.

NXP — wordmark and logo are trademarks of NXP B.V.

I2C-bus — logo is a trademark of NXP B.V.

MIFARE — is a trademark of NXP B.V.

NTAG — is a trademark of NXP B.V.

Contents

Please be aware that important notices concerning this document and the product(s) described herein, have been included in section 'Legal information'.

For more information, please visit: http://www.nxp.com
For sales office addresses, please send an email to: salesaddresses@nxp.com

Date of release: 2 June 2021
Document identifier: AN13042