AN15071

Implementation of Optical module CMIS protocol over I3C on the MCX N947

Rev. 1.0 — 20 July 2026 Application note

Document information

Information	Content
Keywords	AN15071, optical module, CMIS 5.3, bootloader, I3C
Abstract	This application note explains implementing and testing a CMIS-over-I3C demo on FRDM-MCXN947 using MCXN236 as a USB-to-I3C bridge controller for transactions.

1 Introduction

In the optical module use case, I3C becomes a must-have interface to support faster data transfer requirements. CMIS (Common Management Interface Specification) protocol is used in optical module use cases to handle information and firmware management tasks.

This application note introduces how to implement the CMIS protocol demo on an MCX N947 microcontroller using the I3C interface.

MCX N series MCU provides rich resources that can implement optical module use case, including:

- *Dual-core Cortex-M33 architecture* runs at 150 MHz core clock, enables high performance and parallel processing of CMIS/Command Data Block (CDB) control and system tasks
- *Flexible communication interfaces*, including I3C and I2C interface, supporting flexible and future-proof optical module connectivity
- *Large on-chip memory* with up to dual bank 2 MB Flash and 512 kB SRAM, to support complex protocol stacks and firmware management
- *Integrated hardware accelerators*, which reduce CPU load for diagnostics and data processing
- *Built-in security features* for secure firmware updates and authentication aligned with modern CMIS requirements
- *High integration and low power consumption*, making the device suitable for compact and thermally constrained optical modules

1.1 CMIS 5.3 protocol introduction

This demo on MCX N947 is based on the CMIS 5.3 specification. The Common Management Interface Specification (CMIS) is a standard defined by the Optical Internetworking Forum (OIF). It provides a management interface for communication between a host system and pluggable optical modules, such as QSFP-DD and OSFP.

CMIS is designed to solve several key engineering problems, including:

- Multivendor interoperability
- Unified management across different module form factors
- Support for increasing complexity, including multilane operation, PAM4 signaling, and Forward Error Correction (FEC)
- Advanced diagnostics and firmware management
- Scalable management bandwidth, where I3C (SDR 12.5 Mbit/s) delivers approximately 30× I2C bandwidth, along with Dynamic Address Assignment (DAA) and in-band interrupt support
- Security and authenticity, including CRC32 validation and extensible CDB authentication guard against counterfeit modules and unauthorized firmware

2 MCX N947 optical module CMIS over I3C demo introduction

The MCX N947 optical module CMIS protocol demo is based on the CMIS 5.3 specification and supports 12.5 Mbit/s I3C transaction speed. The PC communicates with the FRDM-MCXN236 board, which runs USB-to-I3C bridge firmware, available at: Github.

The FRDM-MCXN236 appears on the PC as a USB CDC virtual COM port. The bridge converts host commands to I3C controller transactions. The FRDM-MCXN947 runs the CMIS protocol over I3C demo as an I3C target and receives CMIS serial framing packets over the I3C bus.

Figure 1 shows the hardware block diagram of the MCX N947 CMIS protocol demo setup:

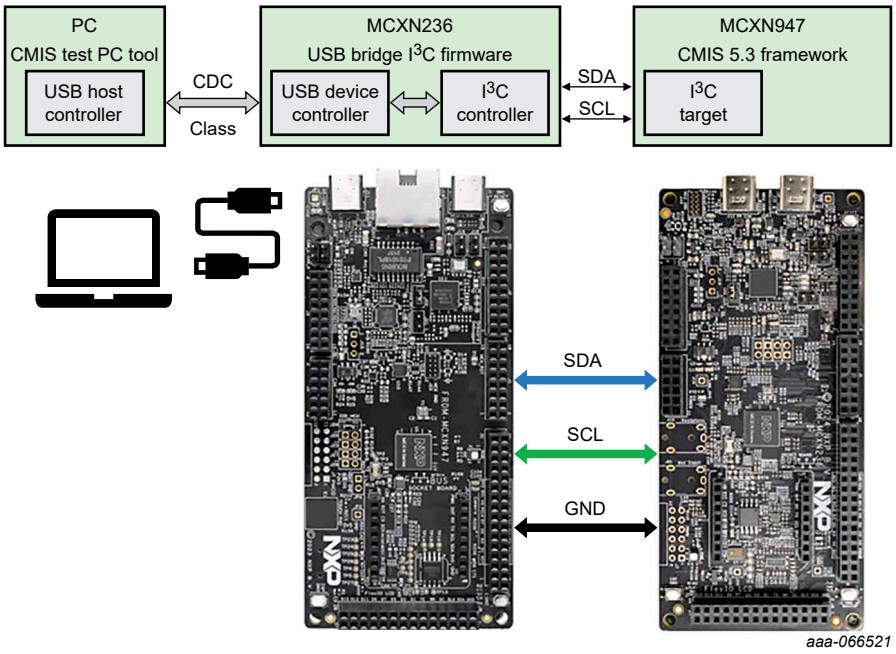


Figure 1. MCX N947 CMIS protocol demo hardware block diagram

2.1 MCX N947 optical module CMIS over I3C software demo introduction

The software architecture of the MCX N947 consists of multiple functional layers, including the application/runtime layer, I3C target transport layer, CMIS protocol layer, command processing layer, and storage/services layer. These layers are built on top of the platform support layer.

Figure 2 shows the software layout of MCX N947 optical module CMIS protocol over I3C software:

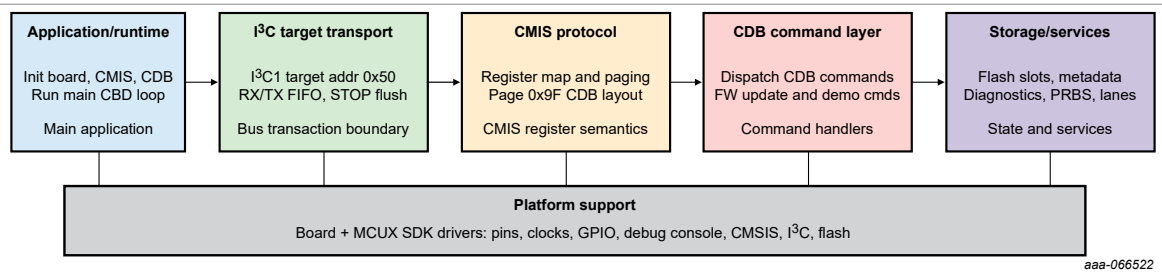


Figure 2. MCX N947 CMIS protocol demo software layout

2.1.1 I3C transaction support

In this demo, the I3C target layer is designed to match common CMIS register-access patterns:

- Current address read: The host reads from the current register pointer without sending a new offset.
- Random read: The host writes the register offset and then issues a repeated start read.
- Sequential read: Starting from the current or random start address, the ISR continues filling TX FIFO and advances the pointer, wrapping at 0xFF.
- Single Byte Write: The first received byte is the register offset; the following one byte is written to the CMIS protocol layer upon detection of a STOP condition.
- Sequential Bytes Write: The first byte is the offset; subsequent bytes are buffered and flushed to the CMIS protocol layer upon a STOP condition.

The firmware models a CMIS 5.3 paged memory space. Lower memory bytes (from 0 to 127) are always directly accessible. Upper memory bytes (from 128 to 255) are redirected through the selected *BankSelect* and *PageSelect pair*.

In this demo, the I3C target layer is designed to support common CMIS register access patterns:

Table 1. CMIS memory map and register access implementation

Register/Region	Address	Implementation
Lower page	0x00-0x7F	Always accessible, independent of the selected bank or page. Initialized with QSFP-DD style module identity, CMIS revision 5.3, ready state, monitor values, thresholds, vendor name, and CDB status fields.
BankSelect	0x7E (byte 126)	Selects current bank. The demo limits *CMIS_MAX_BANKS* to 1 to conserve SRAM.
PageSelect	0x7F (byte 127)	Selects current upper page. Page 0x9F is used for CDB.
Upper page	0x80-0xFF	Backed by upperPages[bank][page][offset]. Sequential access wraps within the 256-byte address space.
CDB Page 9Fh	0x80-0xFF (when page 0x9F is selected)	Contains command header, reply header, and local payload area for CDB commands.

Table 2. CDB page 9Fh format and field definitions

Page 9Fh byte	Field	Writer/Meaning
128 to 129	CMDID	The host writes 16-bit command code.
130 to 131	EPL length	Host-supplied extended payload length fields. EPL is advertised as not supported in this firmware-management implementation.
132	LPL length	Host-supplied local payload length.
133	CDB check code	Host check code. The firmware accepts the command only when (sum of bytes 128-132 + command LPL + CdbChk Code) = 0 (modulo 256).
134	RPL length	Module reply payload length.
135	RPL check code	Module reply check code, computed over reply payload bytes.
136 to 255	LPL/RPL payload	The 120-byte local payload area used by host command payload and module reply payload.

2.1.2 Implemented CDB functions

Table 3 summarizes the actual implemented command set, which is implemented in this demo.

Table 3. CDB commands supported in the demo

Category	Command IDs	Implemented behavior
Query/Status	0x0000	Queries CDB status and returns a basic CDB status payload.
Feature discovery	0x0040, 0x0041	Reports the module features bitmask and firmware-management feature information.

Table 3. CDB commands supported in the demo...*continued*

Category	Command IDs	Implemented behavior
Firmware management	0x0100, 0x0101, 0x0102, 0x0103, 0x0107, 0x0109, 0x010A	Retrieves firmware information; supports download, start/abort, write firmware block through LPL, complete download, run firmware image, and commit image.
Vendor/demo loopback and PRBS	0x8001-0x800B	Retrieves loopback capabilities; start/stop host/media loopback, retrieves PRBS generator/checker capabilities, start/stop PRBS generator/checker, and read checker result.
Vendor/demo diagnostics	0x800C-0x800F	Retrieve diagnostic capabilities, start simulated diagnostic, retrieves diagnostic result, and accept diagnostic selection criterion.
Vendor/demo lane features	0x8010-0x8017	Retrieve lane monitor capability, read lane monitor values, set/get lane controls, set/get lane TX equalization, and set/get lane RX equalization.
Vendor extension	0x8000-0xFFFF	External handlers can be registered with `CMIS_CDB_RegisterVendorHandler()` for vendor-specific ranges not handled by built-in demo commands.

2.1.3 Firmware update implementation

The firmware-update feature is the most complete CDB path in this demo. It supports downloading a new image into the inactive internal flash region, validates it, optionally jumps to it, and can persist boot metadata after committing it. This demo can also support the Dual Bank Remap function.

Table 4 summarizes the key parameters and behavior of the firmware update implementation used in this demo.

Table 4. Firmware update parameters and behavior

Item	Value/Behavior
Active image base	0x00000000, corresponding to PROGRAM_FLASH0 in this project.
Inactive image base	0x00100000, corresponding to PROGRAM_FLASH1.
Metadata address	0x001FE000, located in the last 8 kB sector of PROGRAM_FLASH1.
Maximum inactive image size	0x000FE000, leaving the metadata sector reserved.
Flash program page size	512 bytes; firmware blocks are accumulated in a page buffer before programming.
CDB block payload	For Page 9Fh, the LPL maximum is 120 bytes. The Write FW Block uses a 4-byte block offset plus up to 116 bytes of firmware data per CDB command.
Validation	The download complete command validates received size, optional expected CRC32, stored image CRC32, and Cortex-M vector table stack/reset-handler addresses.
Run image	The Run FW Image command validates inactive image and transfers execution through a real application jump/remap path rather than only swapping version fields.
Commit image	The Commit operation writes metadata selecting slot B as committed, so startup can boot the committed inactive image.

2.2 MCX N947 optical module CMIS over I3C demo hardware setup

To perform the MCX N947 optical module CMIS protocol over I3C demo, use one FRDM-MCXN236 board as the USB-to-I3C controller bridge and one FRDM-MCXN947 board as the CMIS protocol over I3C target device.

Table 5 describes the hardware connections between the FRDM-MCXN236 USB-to-I3C bridge and the FRDM-MCXN947 CMIS-over-I3C target device.

Table 5. Hardware connection details for MCX N947 CMIS-over-I3C demo

Signal	FRDM-MCXN236 (USB-to-I3C bridge)	FRDM-MCXN947 (Optical module CMIS protocol target)
I3C SDA	P1_16/I3C_SDA/J9[4]	P1_16/J9[4], configured as I3C1_SDA
I3C SCL	P1_17/I3C_SCL/J9[3]	P1_17/J9[3], configured as I3C1_SCL
Ground	GND	Common GND with FRDM-MCXN236
USB	Connect to PC	Power/debug connection as needed

Figure 3 shows the physical hardware setup of the MCX N947 CMIS-over-I3C demo, including the interconnection between the FRDM-MCXN236 and FRDM-MCXN947 boards.

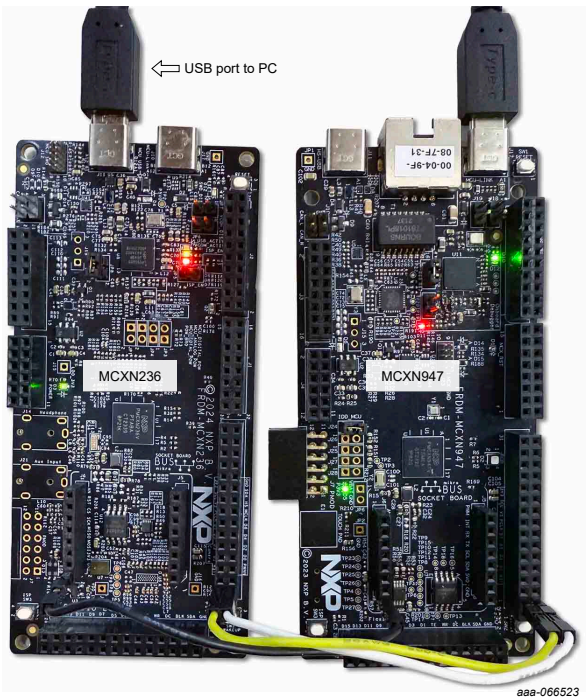


Figure 3. MCX N947 optical module CMIS over I3C demo hardware setup

2.2.1 Function test

To run the MCX N947 CMIS-over-I3C demo, follow the steps below:

1. Ensure that the hardware setup is completed, as described in Table 5 and Figure 3.
2. Flash the `mcxn236-usb-bridge-to-i3c` firmware to FRDM-MCXN236 and `mcxn947_optical_module_cmis_over_i3c_demo` to FRDM-MCXN947 board.
3. Connect the FRDM-MCXN236 USB port (J11) to the PC. The PC counts two USB-CDC COM ports with consecutive COM numbers. Run the `cmis_test_tool.exe` tool from the `mcxn947_optical_module_cmis_over_i3c_demo\scripts` directory. On the test system, the PC counts two usb-bridge-i3c demo COM ports (COM5 and COM6), as shown in Figure 4. Select the second COM port (COM6) and click **Connect**.
   The tool also allows configuration of the I3C target address and the I3C controller transfer type.

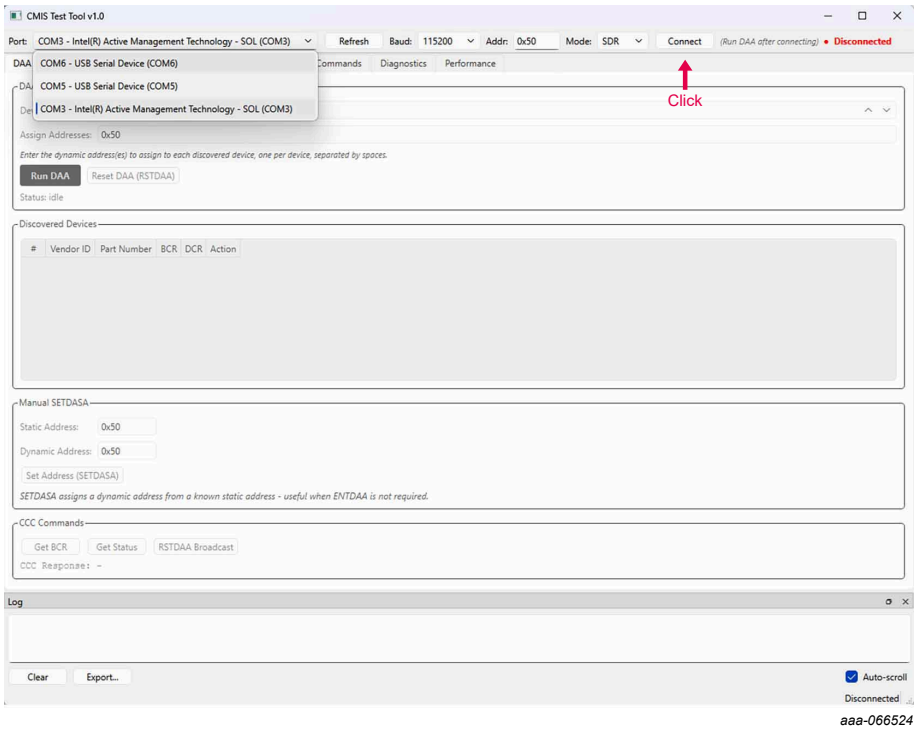


Figure 4. CMIS test PC tool setup

Note: *When the mode is set to I2C, the static address set in the* ***Addr*** *field can be used without requiring dynamic address assignment. Otherwise, dynamic address assignment must be performed after each hardware reset of the I3C target device.*

4. After the USB COM port is connected, select **DAA/Bus Setup** to set the **Device count** and **Assign Addresses**, then click **Run DAA**. After the ENTDAA procedure is complete, a status message such as **Status: DAA found 1 device(s) (8 bytes received)** is displayed. The vendor ID, part number, BCR, and DCR of the discovered I3C target device are shown in the **Discovered Devices** tab. After each DAA process, the I3C address is set to the assigned dynamic address and is used for all subsequent communication.

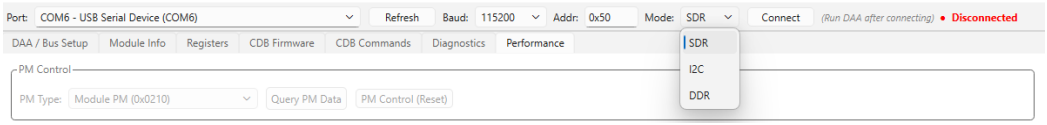


Figure 5. CMIS test PC tool I3C controller setup

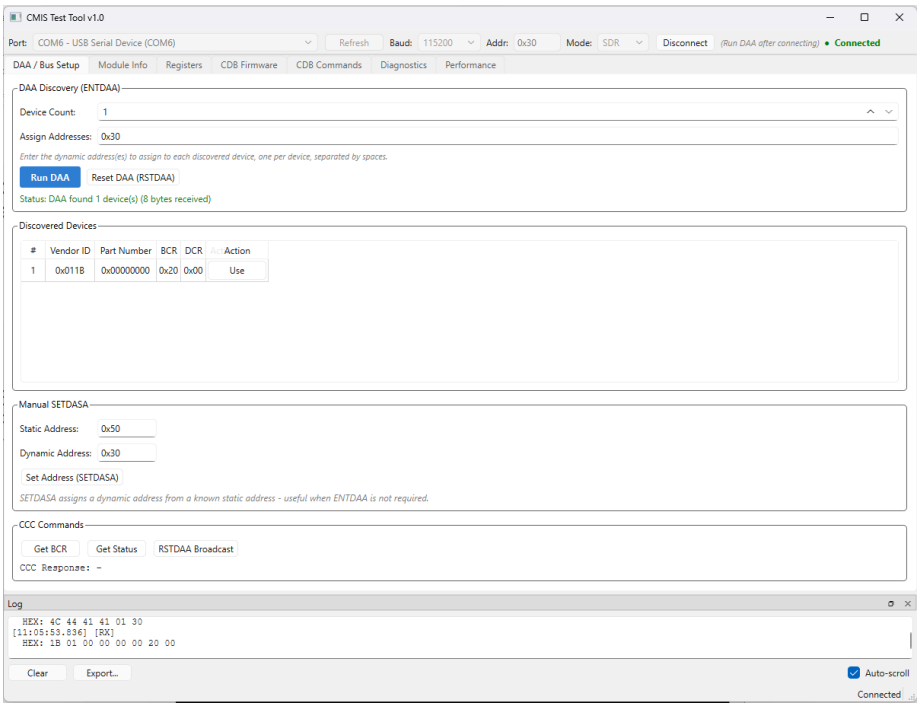
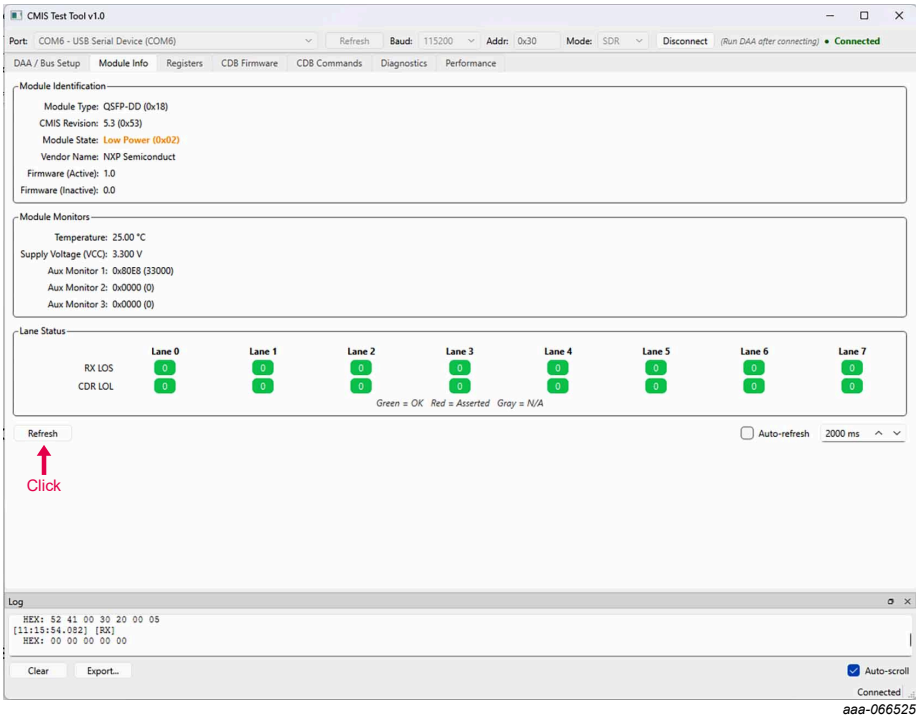


Figure 6. CMIS test PC tool I3C DAA setup

5. Retrieve module information by opening the **Module Info** tab. Then, click **Refresh**, which reads and displays the MCX N947 optical module CMIS protocol over I3C demo information, as shown in Figure 7.



aaa-066525

Figure 7. CMIS test PC tool Module Info tab

6. Read firmware information by opening the **CDB Firmware** tab and clicking **Read FW Info**, and confirm successful communication when a message such as `Get FW Info OK (110B...)` is displayed, as shown in Figure 8.

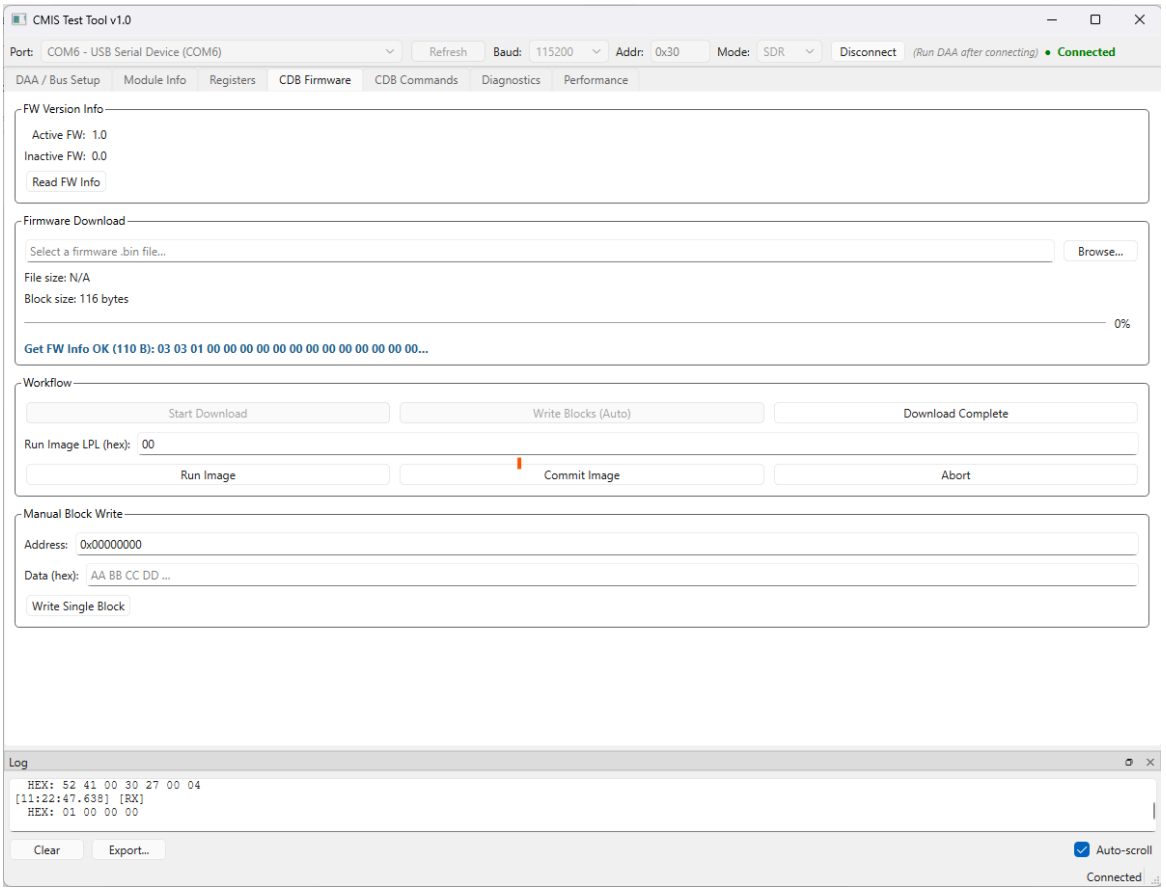


Figure 8. CMIS test PC tool FW information tab

7. Start the firmware update process by following the required sequence: Read FW Info → Start FW Download → Write FW Block (LPL repeatedly) → Download Complete → Run FW Image → Read FW Info/Verify → Commit FW Image. If it is necessary to exit the download state, use Abort FW Download.

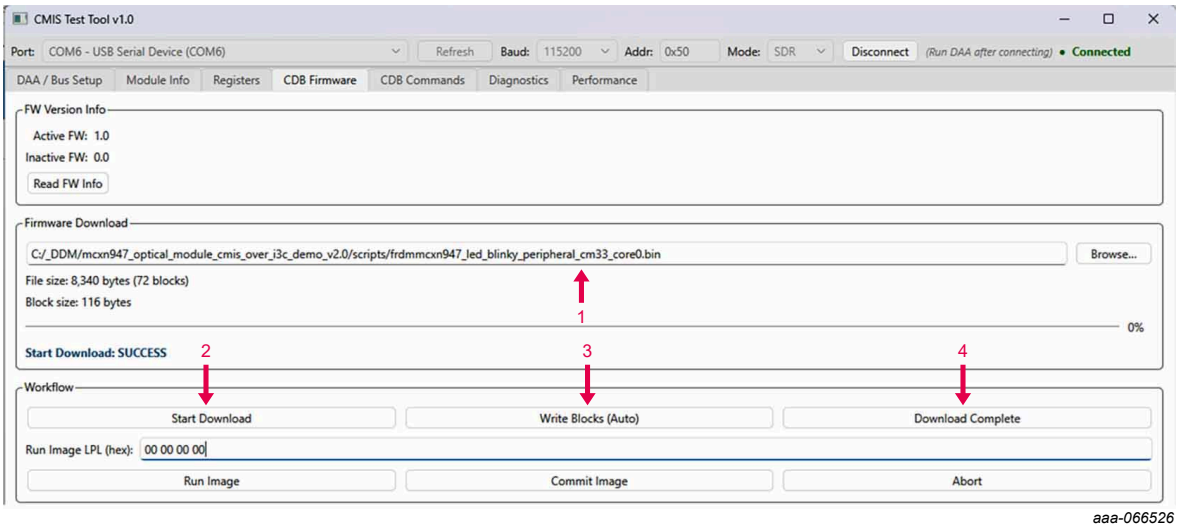


Figure 9. CMIS test PC tool Firmware update sequence

8. Download the firmware image by clicking **Write Blocks (Auto)**. Wait for the progress bar to reach 100 % and verify that the message **Download streamed(Call Download Complete)** is displayed, indicating that the firmware image has been successfully downloaded to the device.

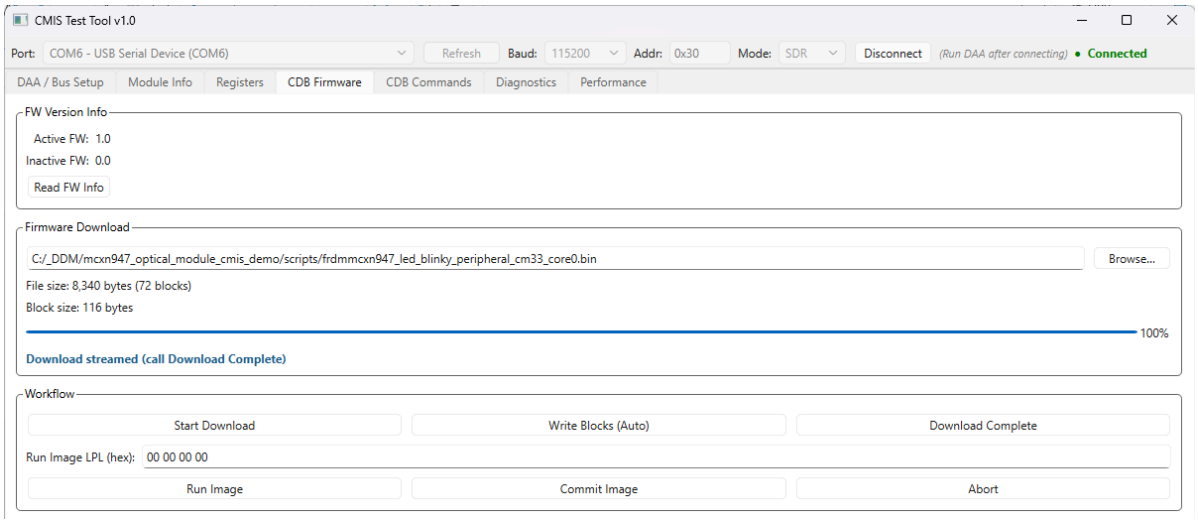


Figure 10. CMIS test PC tool Write Blocks command

9. The user must then click the **Download Complete** command button to verify that the downloaded firmware is valid. After clicking the **Download Complete** button, a log message such as **Download Complete: SUCCESS** is displayed, indicating that the downloaded firmware is valid, as shown in Figure 11.

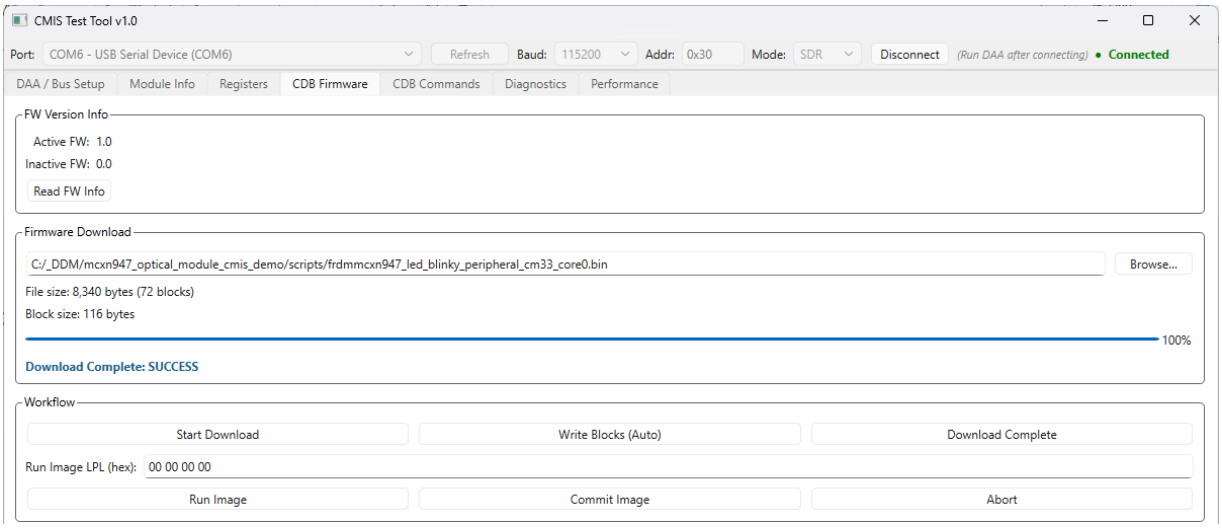


Figure 11. CMIS test PC tool Download Complete command

10. Execute the new firmware by clicking **Run Image** to make the device run to the updated firmware. A temporary message such as **Error: Bridge returned 0/1 bytes (timeout = 1.0 s)** can appear due to the device reset occurring during execution, which is expected behavior, as shown in Figure 12.

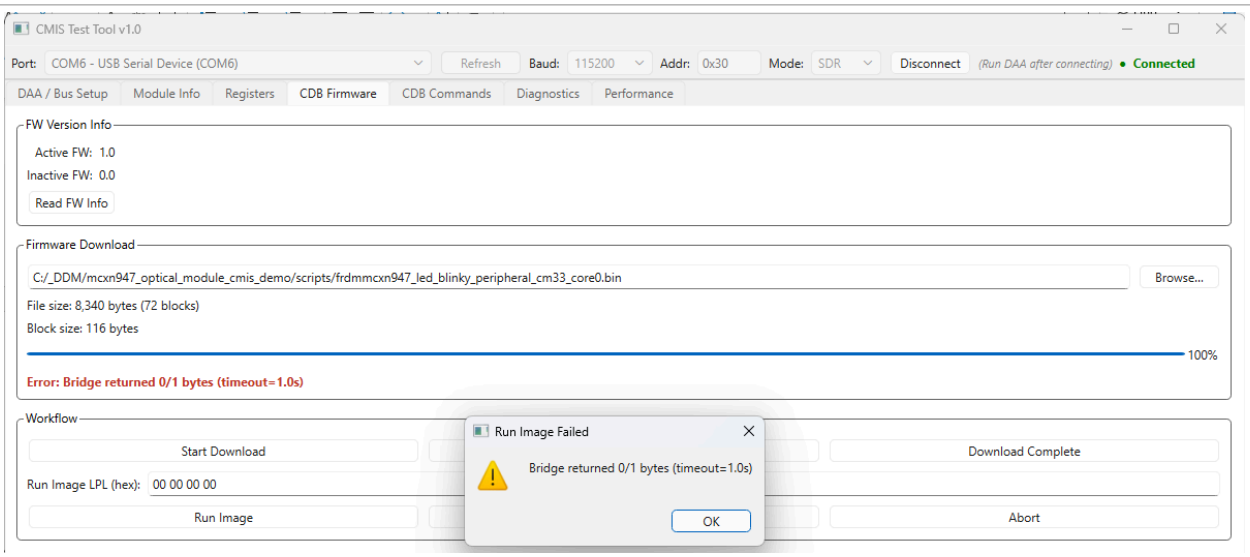


Figure 12. CMIS test PC tool Run image command

Note: *Before clicking the* ***Run Image*** *button, ensure that the* ***Run Image LPL (hex)*** *field is populated according to the CMIS 5.3 specification (Table 9-28). Verify that it contains a valid 4-byte value, as shown in Table 6.*

11. After executing the *Run Image* command, the firmware runs from the Bank1 image by default; to switch back to the Bank0 image. Reset the FRDM-MCXN947 board and make the firmware run to the bank0 image.

Table 6. 9 to 28 CDB Command 0109h: Run Firmware Image

Page	Byte	Field name	Description	Value
CMD header				
9Fh	128 to 129	CMDID	Run FW Image CMD ID	0109h

Table 6. 9 to 28 CDB Command 0109h: Run Firmware Image*...continued*

Page	Byte	Field name	Description	Value
9Fh	130 to 131	EPLLength	EPL is not used	0
9Fh	132	LPLlength	LPL length	4
9Fh	133	CdbChkCode	Check Code for 9Fh: 128 to 132 and LPL. See Table 8-178	complete
9Fh	134	RPLLength	Note: To verify field updates later by the target in the reply, the initiator can fill those reply fields. See Table 8-178	undefined
9Fh	135	RPLChkCode		undefined
CMD data (LPL)				
9Fh	136	-	Reserved	0
9Fh	137	ImageToRun	00h = Traffic affecting Reset to Inactive Image. 01h = Attempt Hitless Reset to Inactive Image 02h = Traffic affecting Reset to Running Image. 03h = Attempt Hitless Reset to Running Image	
9Fh	138 to 139	DelayToReset	U16 indicates a delay in ms after receiving this command before a reset occurs, starting from the time the CDB complete flag is set. Note: When DelayToReset is 0, the module can reset before the host has read the Cdb Status message.	
9Fh	140 to 255	-	No data passed. Content not specified.	undefined
Reply status				
00h	8.6 or 8.7	CdbCmdComplete Flag	Set by module when the CDB command is complete.	1
00h	37 or 38	CdbStatus	**In Progress:** 10 000001b: Busy processing command 10 000010b: Busy processing command 10 000011b: Busy processing command **On Success:** 00 000000b: Success **On Failure:** 01 000000b: Failed 01 000010b: Parameter error 01 000011b: CdbChkCode error	
Reply header				
9Fh	134	RPLLength	See Table 8-179	
9Fh	135	RPLChkCode	See Table 8-179	
Reply data (LPL)				
9Fh	136 to 255	-	No data is returned. Content not specified	undefined

3 Acronyms

Table 7 lists the acronyms used in this document.

Table 7. Acronyms

Term	Description
CDB	Command Data Block
CDB	Command Data Block
CMIS	Common Management Interface Specification
DAA	Dynamic Address Assignment
FEC	Forward Error Correction
OIF	Optical Internetworking Forum

4 Note about the source code in the document

The example code shown in this document has the following copyright and BSD-3-Clause license:

Copyright 2026 NXP Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. Neither the name of the copyright holder nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN

ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

5 Revision history

Table 8 summarizes revisions to this document.

Table 8. Revision history

Document ID	Release date	Description
AN15071 v.1.0	20 July 2026	Initial public release

Legal information

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.

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.

Terms and conditions of commercial sale — NXP Semiconductors products are sold subject to the general terms and conditions of commercial sale, as published at https://www.nxp.com/profile/terms, unless otherwise agreed in a valid written individual agreement. In case an individual agreement is concluded only the terms and conditions of the respective agreement shall apply. NXP Semiconductors hereby expressly objects to applying the customer's general terms and conditions with regard to the purchase of NXP Semiconductors products by customer.

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.

Suitability for use in non-automotive qualified products — Unless this document expressly states that this specific NXP Semiconductors product is automotive qualified, the product is not suitable for automotive use. It is neither qualified nor tested in accordance with automotive testing or application requirements. NXP Semiconductors accepts no liability for inclusion and/or use of non-automotive qualified products in automotive equipment or applications.

In the event that customer uses the product for design-in and use in automotive applications to automotive specifications and standards, customer (a) shall use the product without NXP Semiconductors' warranty of the product for such automotive applications, use and specifications, and (b) whenever customer uses the product for automotive applications beyond NXP Semiconductors' specifications such use shall be solely at customer's own risk, and (c) customer fully indemnifies NXP Semiconductors for any liability, damages or failed product claims resulting from customer design and use of the product for automotive applications beyond NXP Semiconductors' standard warranty and NXP Semiconductors' product specifications.

HTML publications — An HTML version, if available, of this document is provided as a courtesy. Definitive information is contained in the applicable document in PDF format. If there is a discrepancy between the HTML document and the PDF document, the PDF document has priority.

Translations — A non-English (translated) version of a document, including the legal information in that 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.

NXP B.V. — NXP B.V. is not an operating company and it does not distribute or sell products.

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.

Contents