S32K1_S32M24x Real-Time Drivers AUTOSAR R21-11 Version 3.0.0 QLP01

Version 3.0.0 QLP01

6 May 2025 **Release notes**

1 Getting Started

1.1 Package content

This release contains the NXP S32K1_S32M24x Real-Time Drivers Version 3.0.0 QLP01:

- "eclipse/plugins/<mod>_TS_T40D2M30I0R0" directories - Tresos Plugins, 1 per module.
- "SW32K1_S32M24x_RTD_R21-11_3.0.0_QLP01_D2505.exe"
- "SW32K1_S32M24x_RTD_R21-11_3.0.0_QLP01_D2505_ReleaseNotes.pdf" - This file.
- "SW32K1_S32M24x_RTD_R21-11_3.0.0_QLP01_D2505_SCR.txt"
- "SW32K1_S32M24x_RTD_R21-11_3.0.0_QLP01_D2505_DesignStudio_updatesite.zip"
- "SW32K1_S32M24x_RTD_R21-11_3.0.0_QLP01_D2505_SafetyPackage.zip" - contains FMEA reports and Safety Manual.
- "SW32K1_S32M24x_RTD_R21-11_3.0.0_QLP01_D2505_QualityPackage.zip"
- Various other files: GettingStarted.htm start page and associated images, the license.txt EULA file and the Uninstall.exe utility for removing the RTD installation.

1.2 Installation Design Studio

1.2.1 Bundled in S32 Design Studio

S32 RTD is delivered bundled in the S32 Design Studio. In this case, it's already configured and ready to use. New S32DS project wizard and New S32DS project from Example can be used to create S32 RTD based projects.

1.2.2 Delivered as an extension for S32 Design Studio

S32 RTD is delivered as an Update Site for S32 Design Studio "*S32DS 3.6.0*". In this case, it must be installed by opening Help -> S32 Design Studio Extensions and Updates -> Add Update Sites and selecting the archive file containing the S32 RTD software and then check the S32 RTD software package to be installed and continue the installation process. After it is installed, New S32DS project wizard and New S32DS project from Example can be used to create S32 RTD based projects.

1.3 Installation EB Tresos

Follow the installer steps. By default the installer will create a link between the installation target directory and a selected EB Tresos installation. If you choose not to create a link, you can later create one manually or you can copy all "<mod>_TS_T40D2M30I0R0" directories and .JAR files to the "<Tresos Install Path>\plugins" directory.

2 Release Specifics

The S32K1_S32M24x Real-Time Drivers Version 3.0.0 QLP01 is AUTOSAR R21-11 compliant. The AUTOSAR Configuration ARXML specification takes precedence over AUTOSAR SWS PDF Specifications if there are discrepancies.

The S32K1_S32M24x Real-Time Drivers Version 3.0.0 QLP01 can be used also in non-AUTOSAR environment, as a collection of peripheral drivers designed to simplify and accelerate application development on NXP microcontrollers.

2.1 Release Details

This is the S32K1_S32M24X Real-Time Drivers release Version 3.0.0 QLP01, This release contains Crypto Driver supporting AUTOSAR R21-11 and non-AUTOSAR, with functionality and testing on S32K1 and S32M24x family of processor.

This release contains a deviation from AUTOSAR recommended version check inside source files.

This release has RFP quality status in terms of testing and quality documentation. RFP qualified drivers can be used in production.

This release was developed and tested using:

- Silicon Chip S32K116 (0N96V), 48 LQFP
- Silicon Chip S32K118 cut 1.0 (0N97V), 64 LQFP
- Silicon Chip S32K142 cut 1.0 (0N33V), 100 LQFP
- Silicon Chip S32K144 cut 2.1 (0N57U), 100 LQFP
- Silicon Chip S32K144W SWLH (0P64A) CTXP1950B
- Silicon Chip S32K146 cut 1.0 (0N73V), 144 LQFP
- Silicon Chip S32K148 cut 1.0 (0N20V), 144 LQFP
- Silicon Chip P32M244CC WKHS 0P69K 20231008
- Silicon Chip P32M244LC WKHS 0P69K 20231008
- Silicon Chip P32M242CC MKHS 0P69K 20231201
- Silicon Chip P32M242LC WKHS 0P69K 20231201
- S32K-MB PCB 28767 RevA SCH RevB
- S32K1XXCVD-Q048 PCB 30838 RevX1 SCH RevA
- S32K14XCVD-Q064 PCB 29454 RevX2 SCH RevA1
- S32K144-100LQFP PCB 28768 Revx1 SCH RevA
- XS32K14XCVD-Q144 PCB 29559 RevX2 SCH RevB
- XS32M2XXCVB-Q064 PCB 53099 RevX1 SCH RevA

In all source files, Software Version values are checked (major, minor, patch). AUTOSAR release or SWS versions are not checked during preprocessing/template generation.

The correct SWS versions are exported by each module.

The functions contained in the CSM and CryIf plugins are sample stub functions.

These functions should be replaced by the user developed code during integration.

The Resource module is needed to select the MCU derivative.

The derivatives supported can be found in the Resource module definition file, parameter 'ResourceSubderivative'.

The following limitations are present in this release:

Known issue with GCC compiler, all RTD drivers

Warning regarding enum size is thrown by the linker due to usage of "-fno-short-enums" option: "use of enum values across objects may fail". The drivers do not use any library enum types - no functional impact.

Known issue with IAR compiler, all RTD drivers

Warning regarding stack usage is thrown for reference implementations of core exceptions in startup files when drivers are compiled with IAR. These functions are provided as reference code and can be replace/modified by the application.

Due to RAM size on devices S32K11x it is not recommend to build the RTD drivers project targeting RAM.

Usage of IAR compiler option "-enable_stack_usage " will issue warnings regarding uncalled functions (eg : interrupt handlers). This should be disregarded.

During this SW product development, the achieved code coverage is between 88.57% min and 96.23% max, as it can be seen in the individual Code Coverage Summary reports. Nevertheless, the whole code went through a diligently inspection-based review.

For the following functions the code coverage is below 80% during the SW product development.

- Crypto_43_CSEC_CheckForErrorsInProcessJobStepII
- Crypto_43_CSEC_CheckRedirectionConfig
- Crypto_43_CSEC_CopyDataFromPubValKeyElementToUser
- Crypto_43_CSEC_GetJobErrorForSecondaryOutputPtr
- Crypto_43_CSEC_GetJobErrorForTertiaryInputPtr
- Crypto_43_CSEC_GetNonKeyMaterialElement
- Crypto_43_CSEC_Init
- Crypto_43_CSEC_KeyCopy
- Crypto_43_CSEC_KeySetValid
- Crypto_43_CSEC_MarkKeyAsInvalid
- Crypto_43_CSEC_MarkKeyAsValid
- Crypto_43_CSEC_ProcessJobAndCheckNonDetErrorsStepII
- Crypto_43_CSEC_ProcessKeyElementCopy
- Crypto_43_CSEC_ReportErrorToDet
- Crypto_43_CSEC_VerifyKeyValidity
- Crypto_Ipw_CopyOutputResult
- Crypto_Ipw_EncDec
- Crypto_Ipw_MacVerify
- Crypto_Ipw_PushJobFromCdoQueueToCsec
- Crypto_Ipw_TranslateCsecResponse
- Crypto_43_CSEC_Util_RedirectInputOutput
- Csec_Ip_ClearErrorFlags
- Csec_Ip_ContinueGenMACCmd
- Csec_Ip_ContinueVerifMACCmd
- Csec_Ip_StartVerifMACCmd

2.2 Used Documentation

This release was developed and tested with the following documents:

Table 1. Reference Manuals

Document Title	Version and Date
S32K1xx Series Reference Manual	Rev.14.1, 01/2024
S32M24x Reference Manual	Rev. 5, 12/2024
S32K1xx Data Sheet	Rev. 14, 08/2021
S32M2xx Data Sheet	Rev. 7, 12/2024

Table 2. Implemented Errata

Document Title	Maskset	Date
S32K116 Mask Set Errata for Mask	0N96V	Rev. 17/JAN/2024, 1/2024
S32K118 Mask Set Errata for Mask	0N97V	Rev. 15/JAN/2024, 1/2024
S32K142 Mask Set Errata for Mask	0N33V	Rev. 15/JAN/2024, 1/2024
S32K144W Mask Set Errata for Mask	0P64A	Rev. 03/JUL/2024, 7/2024
S32K144 Mask Set Errata for Mask	0N57U	Rev. 15/JAN/2024, 1/2024
S32K146 Mask Set Errata for Mask	0N73V	Rev. 15/JAN/2024, 1/2024
S32K148 Mask Set Errata for Mask	0N20V	Rev. 15/JAN/2024, 1/2024
S32M244 Mask Set Errata for Mask	P64A+P69K	Rev.1, 8/2024
S32M242 Mask Set Errata for Mask	N33V+P69K	Rev.1, 8/2024

2.3 Supported Derivatives

The software described in this document is intended to be used with the following microcontroller devices of NXP :

- s32k116_qfn32
- s32k116_lqfp48
- s32k118_lqfp48
- s32k118_lqfp64
- s32k142_lqfp48
- s32k142_lqfp64
- s32k142_lqfp100
- s32k142w_lqfp48
- s32k142w_lqfp64
- s32k144_lqfp48
- s32k144_lqfp64
- s32k144_lqfp100
- s32k144_mapbga100
- s32k144w_lqfp48
- s32k144w_lqfp64
- s32k146_lqfp64
- s32k146_lqfp100
- s32k146_mapbga100
- s32k146_lqfp144
- s32k148_lqfp100
- s32k148_mapbga100

- s32k148_lqfp144
- s32k148_lqfp176
- s32m244_lqfp64
- s32m243_lqfp64
- s32m242_lqfp64
- s32m241_lqfp64

The mapping between MWCT1xxxS parts and S32K1XX is showed in the table below:

MWCT1xxxS derivative	S32K1xx derivative
MWCT1014S_LQFP64	S32K144_LQFP64
MWCT1014S_LQFP100	S32K144_LQFP100
MWCT1015S_LQFP100	S32K146_LQFP100
MWCT1015S_MAPBGA100	S32K146_MAPBGA100
MWCT1016S_MAPBGA100	S32K148_MAPBGA100

Note: MWCT part numbers contain NXP confidential IP for Qi Wireless Power, and they are tested with:

- Silicon Chip S32K144 cut 2.1 (maskset 0N57U), 100 LQFP (FS32K144UAVLL)

2.4 Modules Configuration

2.4.1 EB Tresos

Modules configurations were developed and tested using the Tresos Configuration Tool version "*EB tresos Studio 29.0.0 b220329-0119*"

Configuration definition files were developed according to AUTOSAR 4.7.0, AUTOSAR_EcucParamDef.arxml

A folder named "<mod>_TS_TtDdMmIiRr" exists for each delivered module (<mod>). It is called a Tresos plugin for the module. A plugin contains the AUTOSAR module definition file (epd), the Tresos Xpath Data Model module definition file (xdm), the module user and integration manuals, the module configuration generation template source files, and the module driver static source files. Additional necessary Tresos specific tooling files are also included.

Plugin Encoding: <mod>_TS_TtDdMmIiRr

Important change related to the plugin notation:
- "m" = coding major and minor version number, can contain 1 or more digits
- "i" = patch number.
The major version number will be left out, if it is "0", in this case "m" contains 1 digit only,
otherwise it contains 2 digits

For this release:

- t=40, CortexM Architecture
- d=2, S32K1XX (derivative)
- m=30, Release major and minor version
- i=0, Release patch version
- r=0, Reserved

2.4.2 S32 Design Studio

Configuration components were developped using "*S32DS 3.6.0*".

The components are split in three tools inside S32 Design Studio: Pins Tool, Clocks Tool, Peripherals tool which enable the generation of configuration structures to be used by both Autosar and low-level drivers.

2.5 Support and Driver Plugins Delivered

Table 3. Support and Driver Plugins Delivered

Plugin	Low level interface	SW Version	Description
Crypto	Csec_Ip	sw version 3.0.0 QLP01	Driver, Crypto
CryIf	N/A	sw version 3.0.0 QLP01	Support Stub, Crypto Interface
CSM	N/A	sw version 3.0.0 QLP01	Support Stub, Crypto Service Manager

2.6 Module Plugin Folder Structure

Table 4. Module Plugin Folder Structure

Folder or file	Description
<mod>_TS_TtDdMmIiRr\anchors.xml	Tresos Configuration tooling documentation data file
<mod>_TS_TtDdMmIiRr\plugin.xml	Tresos Configuration tooling data file
<mod>_TS_TtDdMmIiRr\ant_generator.xml	Tresos Configuration tooling data file
<mod>_TS_TtDdMmIiRr\autosar\<mod>.epd	Module Parameter Definition in AUTOSAR format
<mod>_TS_TtDdMmIiRr\config\<mod>.xdm	Module Parameter Definition in Tresos XDM format
<mod>_TS_TtDdMmIiRr\config_ext\<mod>PreConfiguration.xdm	Module Parameter Default Configuration in Tresos XDM format[1]
<mod>_TS_TtDdMmIiRr\doc\AUTOSAR_RTD_<mod>_IM.pdf	Module Integration Manual
<mod>_TS_TtDdMmIiRr\doc\AUTOSAR_RTD_<mod>_UM.pdf	Module User's Manual
<mod>_TS_TtDdMmIiRr\generate_PB	Post-build source files (only if applicable)
<mod>_TS_TtDdMmIiRr\generate_PB\src	Post-build source file templates (only if applicable)
<mod>_TS_TtDdMmIiRr\generate_PB\include	Post-build source file header templates (only if applicable)
<mod>_TS_TtDdMmIiRr\generate_LT	Link-time source files (only if applicable)
<mod>_TS_TtDdMmIiRr\generate_LT\src	Link-time source file templates (only if applicable)
<mod>_TS_TtDdMmIiRr\generate_LT\include	Link-time source file templates (only if applicable)
<mod>_TS_TtDdMmIiRr\generate_PC\	Pre-compile source files
<mod>_TS_TtDdMmIiRr\generate_PC\src	Pre-compile source files templates
<mod>_TS_TtDdMmIiRr\generate_PC\include	Pre-compile source files templates
<mod>_TS_TtDdMmIiRr\generate_swcd	Module BSWMD file
<mod>_TS_TtDdMmIiRr\include\	Module driver header files
<mod>_TS_TtDdMmIiRr\META-INF	Tresos Configuration tooling data and signature files

Table 4. Module Plugin Folder Structure*...continued*

Folder or file	Description
<mod>_TS_TtDdMmIiRr\src\	Module driver source files[2]

Notes:

[1] Not available for all plugins.

[2] The Support Stub Resource contains the "resource" folder instead of the "src" folder.

2.7 Compiler Options

This release was developed and tested with:

- NXP GCC 10.2.0 20200723 (Build 1728 Revision g5963bc8)
- Green Hills Multi 7.1.6d / Compiler 2020.1.4
- IAR ANSI C/C++ Compiler V8.40.3.228/W32 for ARM Functional Safety

2.8 Examples and Demos

The drivers provide a set of examples. For details, please refer to Examples\...\readme.txt file from each driver folder.

3 Known Issues for S32K1_S32M24x RTD 3.0.0 QLP01

3.1 Known Issues for S32K1_S32M24x RTD 3.0.0 QLP01

ID	Headline
N/A	N/A

4 Changes List for S32K1_S32M24x RTD 3.0.0 QLP01

4.1 Change List for S32K1_S32M24x RTD 3.0.0 QLP01

ID	Subtype	Headline and Description
ARTD-174424	Bug	Code implementation of Csec_Ip_IrqHandler function and update of CPR_RTD_00011
ARTD-177476	Bug	[CRYPTO NG] Crypto_KeyElementGet() not compliant with AUTOSAR
ARTD-176388	Bug	Variable declared but value not updated in function CheckParamAndConfForKeyElementCopy
ARTD-174418	Bug	Function Crypto_43_CSEC_CheckKeyCopyValid always return CRYPTO_E_KEY_READ_FAIL on CSEC driver
ARTD-174417	Bug	Function KeyElementCopyPartial for CSEC does not contain actual implementation for copying key elements
ARTD-174420	Bug	[Crypto SEC NG] Hard fault happens when the driver assigns a value to the address stored in the pointer Crypto_43_CSEC_aKeyList[u32CryptoKeyIdx].KeyStatus

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.

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.

Suitability for use in automotive applications — This NXP product has been qualified for use in automotive applications. If this product is used by customer in the development of, or for incorporation into, products or services (a) used in safety critical applications or (b) in which failure could lead to death, personal injury, or severe physical or environmental damage (such products and services hereinafter referred to as "Critical Applications"), then customer makes the ultimate design decisions regarding its products and is solely responsible for compliance with all legal, regulatory, safety, and security related requirements concerning its products, regardless of any information or support that may be provided by NXP. As such, customer assumes all risk related to use of any products in Critical Applications and NXP and its suppliers shall not be liable for any such use by customer. Accordingly, customer will indemnify and hold NXP harmless from any claims, liabilities, damages and associated costs and expenses (including attorneys' fees) that NXP may incur related to customer's incorporation of any product in a Critical Application.

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.

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