ETAS RTA-FBL_STLA v2.0.0

Release Notes

www.etas.com

Copyright

ETAS RTA-FBL_STLA 2.0.0 - Release Notes R01 EN – 07.2024

Contents

1 Introduction

The objective of this document is a prototype release with the current status of RTA-FBL STLA Port 2.0.0 developed by ETAS. The objective of this project is provide our customers with the current status of the project for **testing/debug** purpose only and **not for any production use** (please refer to attached EULA for more details).

1.1 Definitions and Abbreviations

Term/Abbreviation	Definition
CR	Change Request
CS	Cert Store
FBL	Flash Bootloader
ECU	Electronic Control Unit
CAN	Controller Area Network
CAN-FD	Controller Area Network Flexible Datarate
MCAL	Microcontroller Abstraction Layer
UDS	Unified Diagnostic Services
NA	Not Applicable
NvM	Non-Volatile Memory
DID	Data Identifier
BSW	Basic Software
OS	Operative System
OI	Open Issue
SFB	Signed Firmware Block
SFBH	Signed Firmware Block Header
SFBD	Signed Firmware Block Data
STLA	Stellantis
SW	Software
SWG	Software Gateway
TBT	Trusted Boot Table
TS	Trust Store

1.2 References

Document Name	Description	Version
[1] CS.00101_ECU FLASH Reprogramming Requirements	STLA Reprogramming spec	Rev. D
[2] CS.00102_Standardized Diag Data	Diagnostic Data spec	Rev. F
[3] CS.00099_Diag Reqs UDS	Diagnostic Requests	Rev. E

[4] CS.00100_Diagnostic Services	Diagnostic Services spec	Rev. D
[5] CS.00092_AUTHENTICATED DIAGNOSTIC ACCESS	ADA	Rev. B

1.3 Conventions

The following typographical conventions are used in this document:

Choose **File** → **Open**.	Menu commands are shown in boldface.
Click **OK**.	Buttons are shown in boldface.
Press <Enter>.	Keyboard commands are shown in angled brackets.
The “Open File” dialog box is displayed.	Names of program windows, dialog boxes, fields, etc. are shown in quotation marks.
Select the file setup.exe	Text in drop-down lists on the screen, program code, as well as path- and file names are shown in the Courier font.
A distribution is always a one-dimensional table of sample points.	General emphasis and new terms are set in italics.

1.4 User Documentation

The RTA-FBL STLA Port user's documentation in PDF format can be found as part of the Documentation of this product after installation.

2 Product Definition

2.1 Functions at a glance

This FBL port implements features of the STLA FBL specifications given in [1].

2.2 Intended Use

The scope of the project is to implement a Flash Bootloader for STLA OEM. A Flash Bootloader is a piece of software that resides in a permanent partition of the ECU's flash memory. The purpose of Flash Bootloader is to establish the ECU entry point upon power up or power on reset and to enable flash programming of application software and calibration data via a diagnostic protocol on some physical channel. The Flash Bootloader implements the startup sequence when the ECU is powered up or after power on reset. Flash programming of the ECU is required when application software or calibration data is missing or an update to these is required.

This version is qualified for series production usage.

2.3 Safety-Relevance

The bootloader delivered in this release has been developed to a Quality-Management (QM) level. Therefore, the bootloader software is not certified to any safety level (including any ASIL-x level) and should not be used with any safety-relevant applications.

2.4 General Description

2.4.1 System Prerequisites

The following minimum system prerequisites have to be met:

Required Hardware	1,0 GHz PC 1 GB RAM DVD-ROM drive Network adapter Graphics with a resolution of at least 1024 x 768, 32 MB RAM
Required Operating System	Windows® 10
Required Free Disk Space	500 MB (not including the size for application data)

The following system prerequisites are recommended:

Recommended Hardware	2,0 GHz Dual-Core PC or equivalent 2 GB RAM DVD-ROM drive Network adapter Graphics with a resolution of 1280 x 1024, 128 MB RAM

Recommended Free Disk Space	>2,0 GB

2.5 Delivery

The software is delivered with an installer. All software documentation is available in the Portable Document Format (PDF), which requires Adobe® Reader®. You find the installation link in the Documentation directory on the installation. This document all provides information relevant to installation and licensing of this product.

2.6 Target Environment Description

2.6.1 Software Prerequisites/Dependencies

Software Name	Version No.	Description
Microsoft Windows	10	Software has been fully tested, including the provided GUI configuration tool in this version of Windows.

2.6.2 Software Tools

Tool Name	Version No.	Description
RTA-CAR	9.2.1	AUTOSAR authoring tool.
RTA-BSW	5.1.0	AUTOSAR BSW authoring tool delivered inside the RTA-FBL plugin

2.7 Supported Buses

This FBL Port supports the following communication buses:

Bus Type	Specifications
CAN	CAN 2.0B, CAN-FD 1.0

2.8 Integration Notes

Refer to User Manual for notes on integration with application software.

3 Product Limitation

3.1 Not Supported Features

Currently this release of RTA-FBL STLA Port is not supporting the following features:

Feature Name	Description
Compression	This version of RTA-FBL is currently not implementing any compression method. This feature is indicated as optional by [1].
SW Interlock	This version of RTA-FBL is currently not implementing any Software Interlock method. The SW interlock method indicated by STLA spec is the separate download of the flash driver and is indicated as optional in [1].
HTA Update	The HTA update feature is currently not supported.
Request Upload	This version of RTA-FBL is currently not implementing the request upload (0x35) diagnostic service. This feature is indicated as optional by [1].
Secure Log	DID 0x2032 for secure logging and HSM support to Secure logging is not available.
Secure boot DIDS	**The following DIDs are not supported:** - 0xF1BE (ECU Cybersecurity Operational Mode) - 0xF1C2 (HSM/HTA Software Version) - 0xF1C6 (Cert Store List) - 0xF1C7 (Chip Set ID Version) - 0x2950 (Calibration Header Info) - 0x2951 (CertStore Header UUID) - 0x2955 (CertStore Header Info) - 0x2956 (Calibration Header UUID) - 0x2957 (Hosted App/Firmware Header Info) - 0x2958 (Hosted App/Firmware Header UUID) - 0x2959 (Hosted Bootlader Header Info) - 0x295A (Hosted Bootlader Header UUID) - 0x295B (HTA Header Info) - 0x295C (HTA Header UUID) - 0x295D (DCL Header Info) - 0x295E (DCL Header UUID)

FOTA DIDs	**The following DIDs are not supported:** - 0x2038 (FOTA Target Information)
Generic DIDs	**The following DIDs are not supported:** - 0xF1F0 (ECU-Unique Identification).

3.2 Not Supported ECU Category

Currently this release of RTA-FBL STLA Port is not supporting the following ECU Categories described in [2]:

Not Supported Category	Description
C2	Must be implemented only by VIN Master ECU (BCM) only
C3	Mandatory for an ECU that supports the Response on Event (RoE) feature.
C4	For applicability see CS.00101, writing shall be protected with Level $01
C6	Mandatory for an Instrument Panel Cluster
C7	Mandatory for PROXI (BCM) / Vehicle Configuration Master
C8	Mandatory for ECU that manages the MIL
C9	Mandatory for ECU that manages the High Coolant Temperature Indication
C10	Mandatory for ECU using a Vector Basic Software
C11	Mandatory for an ECU that supports security access mode 3, 5, 7 or 9
C12	Mandatory for Odometer Master ECU
C14	Mandatory only when Firmware Over-The-Air (FOTA) is supported by ECU Big Target
C15	Mandatory for ECUs shipped in a generic or ECU Code unprogrammed state, otherwise DID is optional
C18	Mandatory for CAN-FD ECUs if ECU does not transmit any data frames greater than 64 bytes. Optional for CAN 2.0 (standard CAN) ECUs.
C19	Mandatory only for ECUs that communicate via AVB (Audio Video Bridging)
C20	Mandatory only if ECU is partitioned to support application code data
C21	Mandatory for CAN classic ECUs only (per supported CAN bus)
C22	Mandatory for CAN-FD ECUs only (per supported CAN bus) when supporting Network Management wake-ups. ECUs that do not wake-up via CAN bus message or hard-wire input (e.g. door ajar switch, etc.) are not required to support.

C24	Mandatory only if there are any features or functions which require tool qualification (show/hide), whether based on PROXI data, ECU hardware, ECU application software or other means.
C26	Security levels are $05/06 if ADA is not supported. Otherwise, if ADA is supported, security levels are $11/12.
C27	Mandatory only if ECU is designated FOTA Master
C28	Mandatory only if legislated by market/country (i.e. data records)
C29	Reserved
C30	Mandatory for ECUs supporting CS.00095 - Authenticity of In-Vehicle Messages
C31	Mandatory support if micro-controller supports CAN overrun notification.
C33	Mandatory for ECU Supporting CS.00129 - Intrusion Detection System
C35	Mandatory for Security Gateway Module
C36	Mandatory only for Supervisory controller Modules (VDCM,HCP,EVCU) and Motors controllers (MCPx) on Electrified Vehicles
C37	Mandatory for ECUs supporting Autosar time synchronization
C38	Mandatory for ECU Supporting CS.00165 - ECU Security Identity except FOTA Small Target ECUs
C39	Mandatory for ECU Supporting Plug and Charge as for ISO 15118-2
C40	Mandatory for ECU supporting EDR (i.e. ORC, etc)

4 Cybersecurity features

4.1 Security Solution Dependencies

The RTA-FBL STLA port has a strong dependency from the Security Stack integrated in the FBL project (i.e. Security Solution). There are two identified use case related to the Security Solution integration and dependency:

- Escrypt Solution
- 3rd Party Solution

4.1.1 Escrypt Solution

If the user chooses to use Escrypt Security Solution, RTA-FBL is able to automatically generate the cybersecurity integration code. This will result in a much easier integration process, as the user needs only to copy and paste the Escrypt components inside the FBL project.

The Table below illustrates the Escrypt components and versions fully tested with this release:

Security Component	Version No.	Description
FSM	2.4.0.r0	FCA Security Manager
CycurHSM	2.7.13.r0	HSM Driver and Host interface

4.1.2 3rd Party Solution

If the user chooses to use a 3rd party solution, it has to comply with the FBL Cybersecurity interface. More details can be found in the User Documentation.

5 Changes, Fixes and Issues

This chapter describes changes with respect to the previous versions of this software.

5.1 What's New

This delivery of RTA-FBL contains the following modifications:

- Renaming of the product from RTA-FBL_FCA to RTA-FBL_STLA.
- Fix Secure Boot extended reset management.
  - Before the fix, If a block is marked with the extended reset and the HSM verification fails, the validity flag in NvM was not correctly set. The logic to set the NvM validity flag is updated.
  - Before the fix, the FBl remains blocked in the Sec_Hal_StartAuth-BootVerif function if extended reset was used and ecy_fhwp_HSM_-MAX_NUMBER_OF_POLLING was not properly set. The return value of the CycurHsm api is checked to prevent the infinite loop.
- Fix DID 0x2031 content. The DCL is reported correctly.
- Fix DID 0x2951 content. The SFB UUID location is reported correctly.
- Fix Functional request management. Service 27, 28 and 85 are added to the unsupported service on functional requested and a negative response with NRC 0x72 is sent.
- Fix download sequence. Check programming dependencies can be requested after the hash.
- Update ECDSA signature management
  - Update DID 0xF1B7 and 0xF1B8
  - Added NvM entries for signature and digest of both SW and HW
- Fix support to Infineon FEE
- Update DID F10D default value
- Fix P2 timeout:
  - DcmTimStrP2ServerAdjust is set to 0.03
  - Force pending response before calling the MCAL blocking Erase routine
  - In the Ecu type C, after a jump from app to boot is performed, the ADA verification is performed during the dcm warm startup before sending the positive response.
- Implementation improvements
  - Typedef moves to header file.
  - code changes due to product qualification.
  - removed obsolete functions, variable and define (Fbl_Port_Manage-TimerSlow, FBL_FOTA_Sec_GetCSRLength)
- Fix Boot updater integration of the CycurHsm suspension api.

The following table contains all the modifications to the files.

Folder or file	Info
.ecu_configbswinternalDiag_EcucValues.arxml	Fix P2 timeout
.fbloutputFblBootloaderBootMincFBL_BootM.h	Code refactory
.fbloutputFblBootloaderBootMsrcFBL_BootM.c	Code refactory
.fbloutputFblBootloaderDataMsrcFBL_DataMPrvCfg.c	Update DID F10D default value
.fbloutputFblBootloaderProgMsrcFBL_ProgMCfg.c	Fix P2 timeout
.fbloutputFblINFRAOsincOs_Ipc.h	Code refactory
.fbloutputFblINFRAOsincOs_Sch.h	Code refactory
.fbloutputFblINFRAOsincOs_SchTbl.h	Code refactory
.fbloutputFblINFRAOsincOs_TimeServices.h	Code refactory
.fbloutputFblINFRAOsincOs_Tasks.c	Code refactory
.fbloutputFblINFRAPortsrcADAADA_Manager.c	Code refactory
.fbloutputFblINFRAPortsrcADAFBL_FOTA_SecStackInterface.h	Code refactory
.fbloutputFblINFRAPortsrcADAFBL_FOTA_SecStackInterface.c	Code refactory and ECDSA signature management updates
.fbloutputFblINFRAPortsrcADAFBL_FOTA_SecStackUserCode.c	Code refactory
.fbloutputFblINFRAPortincSecurityFBL_Security_Prv.h	Code refactory
.fbloutputFblINFRAPortsrcSecurityFBL_Security_Did.c	Code refactory and Fix on DID 0x2951
.fbloutputFblINFRAPortincFBL_Port_Cfg.h	Code refactory
.fbloutputFblINFRAPortincFBL_Port_Rollback.h	Code refactory
.fbloutputFblINFRAPortsrcFBL_Port.c	Code refactory, functional request management updates, download sequence updates
.fbloutputFblINFRAPortsrcFBL_Port_Did.c	Code refactory
.fbloutputFblINFRAPortsrcFBL_Port_PFlash.c	Code refactory
.fbloutputFblINFRASecHALincSec_Hal.h	Code refactory
.fbloutputFblINFRASecHALincSec_Hal_PrvCfg.h	Code refactory
.fbloutputFblINFRASecHALincSec_Hal_TBT.h	Code refactory
.fbloutputFblINFRASecHALsrcSec_Hal.c	Code refactory and Secure Boot extended reset management updates
.fbloutputFblINFRASecHALsrcSec_Hal_PrvCfg.c	Code refactory
.fbloutputFblINFRASecHALsrcSec_Hal_PrvCfg.c	Code refactory
.fbloutputFblINFRASecHALsrcSec_Hal_Target.c	Code refactory

.fbloutputFblINFRASecHALsrcSec_Hal_TBT.c	Code refactory and Secure Boot extended reset management updates
.fbloutputFblINFRASecStackFsmincecy_fhwp_config.h	FSM default configuration is updated to support the check on target name and signing OID

5.2 Fixed Problems

Customer Issue Tracking No.	Internal Issue Tracking No.	Issue Name	Description
N/A	RTAFBL-1529	FBL BSW generation is not consistent with EcuC values	Modifying any parameters that trigger BSW changes, the corresponding EcuC arxml is generated but the code generated using RTA Code Generator window does not reflect the new EcuC file. As a workaround, you should generate the BSW twice after any FBL configuration changes that modify the BSW configuration.
N/A	RTAFBL-1527	Only one plugin allowed to be installed	It is not possible to install and use multiple OEM plugins at the same time.
RHU-2527	RTAFBL-2934	Service $27 11/12 configuration in Bootloader	Bootloader does not handle all use cases to respond NRC (such as invalid Key 0x35) if the certificate for service 0x27/11 is invalid.
RHU-2547	RTAFBL-2964	The implementation of DID $F111 is wrong	The callback to retrieve DID $F111 reads the wrong appUUIDaddress and it should compare the regional node value before responding with 1 byte code.
RHU-2559	RTAFBL-2963	Generated UUID address in DID $2951 is wrong	The callback to retrieve DID $2951 is pointing to the wrong address.
RHU-2629	RTAFBL-3138	Bootloader responds with NRC 0x33 to RID $D003	Using Stellantis CDA tool, it executes authenticated reprogramming from the application and then ECU jumps into the bootloader, responding positively to Programming Session. Going on with the reprogramming, the bootloader responds to RID $D003 with NRC 0x33.

RHU-2747	RTAFBL-3215	DID $201F does not return correct value	If multiple logical blocks failed the cybersecurity startup check, DID $201F returns only the first one detected. If more than 8 logical blocks are configured, only byte #0 is actually managed.
RHU-3842	RTAFBL-4670	RTA FBL 2.0 proto4 - Sporadic Flash Failure	Sporadic failure occurs during signature verification or ADA verification. This failure is due to the CycurHsm leave request management.
N/A	RTAFBL-3967	TrustStore verification fails after full download	TrustStore is not updated after the download of the certstore."
N/A	RTAFBL-3989	Add TS check in the Secure Boot	If both the main TrustStore and the back copy of the TrustStore, the FBL doesn't prevent the execution of the Application software and another download.
RHU-3974	RTAFBL-4730	FOTA/Rollback related points - RTA FBL 2.0 proto5	Change requests and bug fixes related to the Rollback. Logical block validity flags and DID 0x2010 are not updated during Rollback process. Multiple requests are allowed while a previous rollback process is pending. A successful Rollback shall not trigger a reset.
RHU-4068	RTAFBL-4994 RTAFBL-4996 RTAFBL-5000	RTA FBL 2.0 Proto6 findings	Sec_Hal_StartAuthBootVerif function remains blocked after invalid Application block download if marked as TB_BOOT_MODE_AUTHENTIC-_EXTENDED_RESET and ecy_fhw-p_HSM_MAX_NUMBER_OF_POLLING is not properly set Wrong block index invalidation in NvM for AUTHENTIC_EXTENDED_RESET blocks. DID 0x2031 content doesn't report the DCL content."
N/A	RTAFBL-5364	P2 is not respected after jump to boot from app	The verification of the ADA certificate that is a blocking function, is triggered after the positive response is sent to the tester.
N/A	RTAFBL-5366	BootUpdater CycurHsm supension issue on flash operation	Sporadic failure occurs during boot updater. These failiure are due to the CycurHsm suspension. After 500ms the suspension is automatically terminated by the CycurHsm and it's possible to have a concurrent access to the pflash.

5.3 Known Issue Reports

If a product issue develops, ETAS will prepare a Known Issue Report (KIR) and post it on the internet. The report includes information regarding the technical impact and status of the solution. Therefore, you must check the KIR applicable to this ETAS product version and follow the relevant instructions prior to operation of the product.

The Known Issue Report (KIR) can be found here:

http://www.etas.com/kir

5.4 Known Issues

Customer Issue Tracking No.	Internal Issue Tracking No.	Issue Name	Description
N/A	RTAFBL-1274	Security Access delay timer	Depending on the ECU type and configuration, the delay timer may be slightly inaccurate.
N/A	RTAFBL-1278	Service $37 – wrong NRC	If service $37 is not correctly sent as part of the download sequence, the wrong NRC is returned.
N/A	RTAFBL-5286	Download sequence error	The download sequence doesn't report any error if the the step after the Erase are not executed in sequence.
N/A	RTAFBL-3843	Signature validation of external region.	Signature validation of external regions is not supported.
N/A	RTAFBL-5293	FblBlockSize validation.	FblBlockSize depends on some target parameters not managed by the plugin (Ex:minimum size of the pflash that can be written). Check your target guide for more infomration.

5.5 Known Limitations

Limitation Tracking No.	Issue Name	Description
RTAFBL-1530	String input cannot be padded with spaces	If a string input parameters ends with spaces, the spaces are truncated during FBL generation.
RTAFBL-432	Service $34 - NRC in case of wrong AALFI	AALFI is evaluated before DataFormatIdentifier, and NRC returned is $13 instead of $31.

RTAFBL-1326	SPRMIB	If a UDS request without sub function is received after SPRMIB was set to TRUE, the SPRMIB is managed as TRUE until a new UDS request with a sub function is received.
RTAFBL-4399	Download size is not checked during Transfer-Exit	During the Transfer Exit, the BSW checks that downloaded area is equal to the area defined in the Request Download and if it's not the case it reports a negative response. The user can download an area smaller than the block size but if an ECU type A is used, it may cause an exception during the next Verify Download. This issue is target dependent.
RTAFBL-5265	S3 is not reset if service response is not allowed	When the DcmAppl_ManufacturerNotification returns with DCM_E_REQUEST_NOT_ACCEPTED, the dcm timeout is set to the P2 timing instead of the S3 timing. A reset is triggered in non default session and the FBL enters default session.
RTAFBL-5287	Consecutive frames not supported on functional addresses	Some target have a limited support on can hardware. Check your target guide for more information.
RTAFBL-5288	$27 12 doesn't report the NRC 0xFA (Revoked certificate)	Authenticated security access doesn't check that the ADA certificate is in the DCL list since ADA certificate life cycle is short. If the ADA certificate is added to the DCL, a positive response is still obtained.

6 ETAS Contact Addresses

6.1 ETAS HQ

ETAS GmbH Borsigstraße 24 Phone: +49 711 3423-0
70469 Fax: +49 711 3423-2106
Germany Internet: www.etas.com

6.2 ETAS Subsidiaries and Technical Support

For details of your local sales office as well as your local technical support team and product hotlines, take a look at the ETAS website: www.etas.com/hotlines