

# Flash Bootloader GM

## Technical Reference

CANfbl GM SLP6

Version 6.2.1

Authors	Andreas Wenckebach / Dennis O'Donnell
Status	Released

## Document Information

### History

Author	Date	Version	Remarks
Andreas Wenckebach	2013-08-07	--	Pre release
Andreas Wenckebach	2014-10-10	06.00.00	Creation
Andreas Wenckebach	2015-06-24	06.01.00	Chapter for Partition Erasure handling
Andreas Wenckebach	2016-02-22	06.02.00	Add Basic NBID handling configuration and general NVM handling strategies
Andreas Wenckebach	2016-03-29	06.02.01	Improvements

### Reference Documents

No.	Source	Title	Version
[1]	General Motors	GB6000 Unified Diagnostic Service Specification	V0.9 - 1.x
[2]	General Motors	GB6002 Global-B Bootloader Specification	May - December 2014
[3]	Vector-Informatik GmbH	Flash Bootloader User Manual	v2.7
[4]	Vector-Informatik GmbH	vFlash Manual	-
[5]	Hersteller Initiative Software (HIS)	Functional Specification of a Flash Driver	Version 1.3, June 6, 2002 <a href="http://www.automotive-his.de/">http://www.automotive-his.de/</a>
[6]	Vector-Informatik GmbH	Flash Bootloader OEM Technical Reference – CANfbl GM – Programmable Data File Creation	
[7]	Vector-Informatik GmbH	TechnicalReference_NvWrapper.pdf	
[8]	General Motors	CG3532 ECU Security Requirements	Issue 115 2014-10-27
[9]	Vector-Informatik GmbH	AN-ISC-8-1173 Share FEE Blocks Between Application and Bootloader	1.00.00



#### Caution

We have configured the programs in accordance with your specifications in the questionnaire. Whereas the programs do support other configurations than the one specified in your questionnaire, Vector's release of the programs delivered to your company is expressly restricted to the configuration you have specified in the questionnaire.

## Contents

<b>1</b>	<b>Introduction .....</b>	<b>11</b>
<b>2</b>	<b>FBL Software Architecture .....</b>	<b>12</b>
2.1	Components.....	12
2.1.1	Core Files.....	12
2.1.2	User modifiable application files .....	14
2.1.3	Generated Files.....	14
2.1.4	Other delivery content .....	15
2.2	Memory Layout .....	17
2.2.1	The GM File-Container.....	17
2.2.1.1	The Operating S/W File-Container.....	17
2.2.1.2	Calibration Module File-Container .....	17
2.2.1.3	Boot Info Block .....	18
2.2.2	Operating S/W Interrupt Vector Table .....	19
2.2.3	Logical Block table .....	19
2.2.4	Partitions .....	19
2.2.5	Presence Patterns / Programmed State Indicator.....	19
2.3	Run-Time Details.....	20
2.3.1	Power-On Reset.....	20
2.3.2	Start from Operating Software .....	20
2.3.3	Download Sequence .....	20
<b>3</b>	<b>Configuration of the GM Flash Bootloader .....</b>	<b>22</b>
3.1	Overview .....	22
3.2	Starting with GENy .....	22
3.3	CAN Configuration .....	26
3.4	Bootloader Configuration.....	27
3.4.1	FblDrvCan component .....	27
3.4.2	FblCan_Gm_Global_B configuration .....	31
3.5	Memory Configuration .....	35
3.5.1	Device Types.....	36
3.5.2	Flash Block Definition.....	38
3.5.3	Logical Block Definition .....	39
3.5.3.1	Correct Presence Pattern Addresses.....	40
3.6	Mandatory Delivery Preconfig .....	41
3.7	Handling of NVM data .....	44
3.7.1	vFlashBasic NVM handling .....	45
3.7.1.1	SBAT in basic NNVM handling configuration .....	46

3.7.2	Fee integration to FBL.....	47
3.7.3	Alternative NV-Wrapper Configuration.....	47
3.8	typical use case to handle Security Module configuration.....	48
3.8.1	Running the Generator.....	49
<b>4</b>	<b>Adapting the FBL Implementation .....</b>	<b>50</b>
4.1	Hardware, Input/Output and miscellaneous Callbacks.....	51
4.1.1	ApplFblCanBusOff .....	51
4.1.2	ApplFblCanParamInit .....	52
4.1.3	ApplFblCanWakeUp .....	52
4.1.4	ApplFblCheckProgConditions.....	53
4.1.5	ApplFblEnterStopMode .....	53
4.1.6	ApplFblInit .....	53
4.1.7	ApplFblInitErrStatus .....	54
4.1.8	ApplFblRamIntegrityCheck.....	55
4.1.9	ApplFblReset .....	56
4.1.10	ApplFblResetVfp .....	56
4.1.11	ApplFblRomIntegrityCheck.....	57
4.1.12	ApplFblSetVfp .....	57
4.1.13	ApplFblSleepModeAllowed .....	58
4.1.14	ApplFblStartup .....	58
4.1.15	ApplFblTask .....	59
4.1.16	ApplFblTpErrorInd.....	59
4.1.17	ApplTrcvrHighSpeedMode .....	60
4.1.18	ApplTrcvrNormalMode .....	61
4.1.19	ApplTrcvrSleepMode .....	61
4.1.20	ApplFblStartApplication .....	62
4.1.21	ApplFblFatalError .....	62
4.1.22	ApplFblCheckDataFormatIdentifier.....	63
4.1.23	ApplFblInitDataProcessing .....	63
4.1.24	ApplFblDataProcessing.....	64
4.1.25	ApplFblDeinitDataProcessing.....	64
4.2	Diagnostic Service Callbacks .....	64
4.2.1	ApplFblEnablePrgMode .....	65
4.2.2	ApplFblInitiateDiagnosticOperation .....	65
4.2.3	ApplFblReadDataByIdentifier .....	66
4.2.4	ApplFblReportProgrammedState .....	66
4.2.5	ApplFblRdbidProgrammedStateInd .....	67
4.3	Module Validation Callbacks.....	67
4.3.1	ApplFblExtProgRequest .....	68
4.3.2	ApplFblFillGaps.....	68

4.3.3	ApplFblInvalidateBlock .....	69
4.3.4	ApplFblIsValidApp .....	69
4.3.5	ApplFblValidateBlock.....	70
4.3.6	ApplFblGetProgrammedState .....	70
4.3.7	ApplFblChkOpSwProgrammedState .....	71
4.3.8	ApplFblGetModuleHeaderAddress .....	71
4.3.9	ApplFblGetBaseModulePPRegion.....	72
4.3.10	ApplFblGetPresencePatternBaseAddress.....	73
4.3.11	ApplFblSetModulePresence .....	73
4.3.12	ApplFblClrModulePresence.....	74
4.3.13	ApplFblChkModulePresence .....	74
4.3.14	ApplFblChkPSIState .....	74
4.3.15	ApplFblGetBaseModulePPRegion.....	75
4.3.16	ApplFblUpdateChecksum.....	75
4.3.17	ApplFblFinalizeChecksum .....	76
4.3.18	ApplFblNVMMReadKeyNBID .....	76
4.3.19	ApplFblNVMMWriteKeyNBID .....	77
4.3.20	ApplFblNVMMReadAppNBID.....	77
4.3.21	ApplFblChkModulePresence .....	77
4.3.22	ApplFblNVMMReadECUID .....	78
4.3.23	ApplFblNVMMReadSBATicket .....	78
4.4	Watchdog Callbacks.....	79
4.4.1	Start of Watchdog.....	79
4.4.2	Synchronize Watchdog with application .....	80
4.4.3	Window Watchdogs.....	80
4.4.4	Watchdog triggering during Memory operations .....	80
4.4.5	ApplFblWdInit.....	81
4.4.6	ApplFblWDLong .....	81
4.4.7	ApplFblWDTrigger.....	82
4.5	Callback configuration summary.....	83
4.5.1	Required callback configuration .....	83
4.6	Application Vector Table .....	84
4.7	Transport-Layer Configuration.....	85
4.8	[#hw_wd] – Compiling the Watchdog components .....	85
4.9	[#oem_valfunc] – Flashing After A Reset .....	85
4.10	[#oem_valid] – Proposals for Handling The Validation Area.....	85
4.11	[#oem_start] Startup.....	86
4.12	[#oem_ref] – Label Reference File .....	87
<b>5</b>	<b>Adapting the Operating Software.....</b>	<b>88</b>

<b>6</b>	<b>Device Driver .....</b>	<b>91</b>
6.1	General Information.....	91
6.2	High-Level Device-Driver Functions .....	91
6.2.1	MemDriver_InitSync.....	92
6.2.2	MemDriver_ReraseSync .....	92
6.2.3	MemDriver_ReadSync .....	93
6.2.4	MemDriver_RwriteSync.....	94
6.2.5	MemDriver_VerifySync.....	94
<b>7</b>	<b>Using the Flash Tool for GM .....</b>	<b>96</b>
7.1	Preparing the File-Header .....	96
7.2	Configuring vFlash .....	96
7.2.1	vFlash Communication Tab .....	96
7.2.2	vFlash Miscellaneous Tab .....	98
7.2.3	vFlash Data Tab .....	98
7.3	Starting the flash sequence with vFlash .....	99
<b>8</b>	<b>Miscellaneous.....</b>	<b>100</b>
8.1	[#oem_multi] – Multiple-Identity-Modules .....	100
8.2	Multiple Processor Support .....	100
8.3	PEC error code and Debug-Status .....	100
8.4	[#oem_time] – Stay-In-Boot mode .....	102
8.5	User-Callable Support Functions.....	102
8.5.1	FblStart .....	102
8.5.2	FblReadMem .....	103
8.5.3	GetDiagInProgress.....	104
8.5.4	FblRealTimeSupport .....	104
8.5.5	FblLookForWatchdog .....	105
8.5.6	DiagExRCRResponsePending.....	105
8.5.7	FblMemSegmentNrGet .....	106
8.5.8	GetFbl<XXX>Version .....	106
8.5.9	GetFblDCID<X> .....	107
8.5.10	GetFblSWMI<X> .....	107
8.5.11	GetFblDLS<X> .....	108
8.5.12	GetFblEcuNameAddr .....	108
8.5.13	GetFblSubjNameAddr .....	109
8.5.14	GetFblEculdAddr.....	109
8.5.15	GetFblMode .....	109
8.6	Low Power Mode in the bootloader .....	110
8.6.1	Integrated sleep mode enabled .....	110
8.6.2	Integrated sleep mode enabled with wakeup interrupt.....	110

8.6.3	Integrated Sleep mode handling disabled.....	111
8.7	Example / hints to prepare containers for Ecus programmed with Fbl and Application .....	111
8.8	Security Requirements .....	112
8.8.1	Digital Signature.....	112
8.8.2	Signature-Bypass Authorization (SBA) ticket.....	113
8.8.3	Message Digest .....	114
8.8.3.1	Pipelined Verification .....	114
8.8.3.2	Optional Integrity Word Check.....	114
8.8.4	Signer Info.....	115
8.8.5	Application Software – Not Before Identifier (App-NBID) .....	115
8.8.6	Security Key – Not Before Identifier (Key-NBID).....	116
8.8.7	ECU ID.....	116
8.9	Programming of Unused Flash Space / Gap Fill.....	117
8.10	Partition Erase Status.....	117
8.10.1	Configuration.....	117
<b>9</b>	<b>Limitations.....</b>	<b>119</b>
9.1	CG3532 ECU Security Requirements.....	119
<b>10</b>	<b>Glossary and Abbreviations .....</b>	<b>120</b>
<b>11</b>	<b>Contact.....</b>	<b>123</b>

## Illustrations

Figure 1-1	Manuals and References for the Flash Bootloader .....	11
Figure 2-1	Component overview .....	12
Figure 2-2	User-modifiable Files .....	14
Figure 3-1	Initial GENy main window .....	22
Figure 3-2	GENy Setup Dialog.....	22
Figure 3-3	GENy main window after pre-configuration.....	23
Figure 3-4	GENy Channel Setup .....	23
Figure 3-5	GENy main window after channel setup .....	24
Figure 3-6	GENy Components.....	25
Figure 3-7	GENy directory selection .....	26
Figure 3-8	GENy CAN Configuration .....	27
Figure 3-9	FblDrvCan configuration example.....	28
Figure 3-10	GM Fbl configuration Settings.....	31
Figure 3-11	GM-Specific Configuration .....	33
Figure 3-12	GM Modules and Boot Info Block Detail Configuration.....	35
Figure 3-13	Memory Configuration .....	35
Figure 3-14	Typical Logical Block partition .....	36
Figure 3-15	GENy Device Types.....	37
Figure 3-16	Example Device Type .....	38
Figure 3-17	GENy Flash Block Table .....	38
Figure 3-18	GENy Logical Block Table.....	39
Figure 3-19	Presence Pattern Address configuration .....	41
Figure 3-20	SysService_WrapperNv configuration in GENy .....	48
Figure 3-21	SysService_SecModHis configuration .....	48
Figure 5-1	Standard transition from application to bootloader .....	89
Figure 7-1	Example vFlash Communication Configuration Dialogue.....	97
Figure 7-2	Example vFlash Miscellaneous Configuration dialog .....	98
Figure 7-3	Example vFlash Data Configuration Dialogue .....	99
Figure 8-1	Multi-Processor logical block table configuration.....	100
Figure 8-2	Application and Calibration signed header structures and signature calculation. "Signature" represents the digital signature .....	113
Figure 8-3	Signature-Bypass Authorization Header structure and signature calculation. ....	113
Figure 8-4	Application and Calibration Message Digest.....	114
Figure 8-5	Signer Info Structure and signature calculation.....	115

## Tables

Table 2-1	FBL Files .....	13
Table 2-2	Generated Files .....	15
Table 2-3	Other delivery content.....	15
Table 2-4	Example Memory Layout .....	17
Table 2-5	Boot Info Block configuration .....	18
Table 3-1	Bootloader Configuration .....	31
Table 3-2	GENy configuration of the Logical Block Table.....	40
Table 3-3	Mandatory Delivery Preconfig .....	42
Table 3-4	Mandatory Delivery Preconfig .....	43
Table 3-5	GM NVM element overview with possible solutions .....	44
Table 3-6	Mandatory configuration items for basic NVM handling. Configure them e.g. via user configuration file .....	46



Table 3-7	Optional configuration items for basic NVM handling. Configure them e.g. via user configuration file .....	46
Table 3-8	Security Module configuration.....	49
Table 3-9	Generated File contents .....	49
Table 4-1	User-Modifiable file contents.....	50
Table 4-2	Miscellaneous Callback functions .....	51
Table 4-3	ApplFblCanBusOff .....	51
Table 4-4	ApplFblCanParamInit.....	52
Table 4-5	ApplFblCanWakeUp .....	52
Table 4-6	ApplFblCheckProgConditions .....	53
Table 4-7	ApplFblEnterStopMode.....	53
Table 4-8	ApplFblInit .....	54
Table 4-9	ApplFblInitErrStatus.....	55
Table 4-10	ApplFblRamIntegrityCheck .....	56
Table 4-11	ApplFblReset .....	56
Table 4-12	ApplFblResetVfp.....	57
Table 4-13	ApplFblRomIntegrityCheck .....	57
Table 4-14	ApplFblSetVfp.....	58
Table 4-15	ApplFblSleepModeAllowed .....	58
Table 4-16	ApplFblStartup.....	59
Table 4-17	ApplFblTask.....	59
Table 4-18	ApplFblTpErrorInd .....	60
Table 4-19	ApplTrcvrHighSpeedMode .....	61
Table 4-20	ApplTrcvrNormalMode .....	61
Table 4-21	ApplTrcvrSleepMode .....	62
Table 4-22	ApplFblStartApplication .....	62
Table 4-23	ApplFblFatalError .....	63
Table 4-24	ApplFblCheckDataFormatIdentifier .....	63
Table 4-25	ApplFblInitDataProcessing.....	63
Table 4-26	ApplFblDataProcessing .....	64
Table 4-27	ApplFblDeinitDataProcessing .....	64
Table 4-28	Diagnostic Callback Functions.....	65
Table 4-29	ApplFblEnablePrgMode .....	65
Table 4-30	ApplFblInitiateDiagnosticOperation .....	65
Table 4-31	ApplFblReadDataByIdentifier.....	66
Table 4-32	ApplFblReportProgrammedState .....	67
Table 4-33	ApplFblRdbidProgrammedStateInd .....	67
Table 4-34	Module Validation Callbacks .....	67
Table 4-35	ApplFblExtProgRequest .....	68
Table 4-36	ApplFblFillGaps .....	69
Table 4-37	ApplFblInvalidateBlock .....	69
Table 4-38	ApplFblIsValidApp.....	70
Table 4-39	ApplFblValidateBlock .....	70
Table 4-40	ApplFblGetProgrammedState .....	71
Table 4-41	ApplFblChkOpSwProgrammedState.....	71
Table 4-42	ApplFblGetModuleHeaderAddress .....	72
Table 4-43	ApplFblGetBaseModulePPRegion .....	72
Table 4-44	ApplFblGetPresencePatternBaseAddress .....	73
Table 4-45	ApplFblSetModulePresence .....	73
Table 4-46	ApplFblClrModulePresence .....	74
Table 4-47	ApplFblChkModulePresence .....	74
Table 4-48	ApplFblChkPSIState .....	75
Table 4-49	ApplFblGetBaseModulePPRegion .....	75
Table 4-50	ApplFblUpdateChecksum .....	76

Table 4-51	ApplFblUpdateChecksum .....	76
Table 4-52	ApplFblNVMReadKeyNBID .....	76
Table 4-53	ApplFblNVMWriteKeyNBID .....	77
Table 4-54	ApplFblNVMReadAppNBID .....	77
Table 4-55	ApplFblChkModulePresence .....	78
Table 4-56	ApplFblNVMReadECUID .....	78
Table 4-57	ApplFblNVMReadSBATicket .....	79
Table 4-58	Watchdog Callbacks .....	81
Table 4-59	ApplFblWdInit .....	81
Table 4-60	ApplFblWDLONG .....	82
Table 4-61	ApplFblWDTrigger .....	83
Table 5-1	Parameters passed to FBL by Operating Software .....	88
Table 6-1	MemDriver_InitSync .....	92
Table 6-2	MemDriver_ReraseSync .....	93
Table 6-3	MemDriver_RreadSync .....	93
Table 6-4	MemDriver_RwriteSync .....	94
Table 6-5	MemDriver_VerifySync .....	95
Table 7-1	Parameter description of the communication tab in vFlash .....	97
Table 7-2	Parameter description of the miscellaneous tab in vFlash .....	98
Table 8-1	Response for debug-status request .....	101
Table 8-2	FblStart .....	103
Table 8-3	FblReadMem .....	104
Table 8-4	GetDiagInProgress .....	104
Table 8-5	GetDiagInProgress .....	104
Table 8-6	FblLookForWatchdog .....	105
Table 8-7	DiagExRCRResponsePending .....	106
Table 8-8	FblMemSegmentNrGet .....	106
Table 8-9	GetFbl<XXX>Version .....	107
Table 8-10	GetFblDCID<X> .....	107
Table 8-11	GetFblSWMI<X> .....	108
Table 8-12	GetFblDLS<X> .....	108
Table 8-13	GetFblEcuNameAddr .....	108
Table 8-14	GetFblSubjNameAddr .....	109
Table 8-15	GetFblEculdAddr .....	109
Table 8-16	GetFblMode .....	110

# 1 Introduction

This document covers the GM-specific **particularities** of the Flash Bootloader. The bootloader is designed to comply with all requirements defined in references [1] and [2]. The documentation complements the explanations started in the user manual with OEM-specific details. All references there are resumed here in this document again and explained in detail.

The connection between a reference in the user manual and its specific description in this document is the headline. Both the reference and its explanation can be found below the same headline.

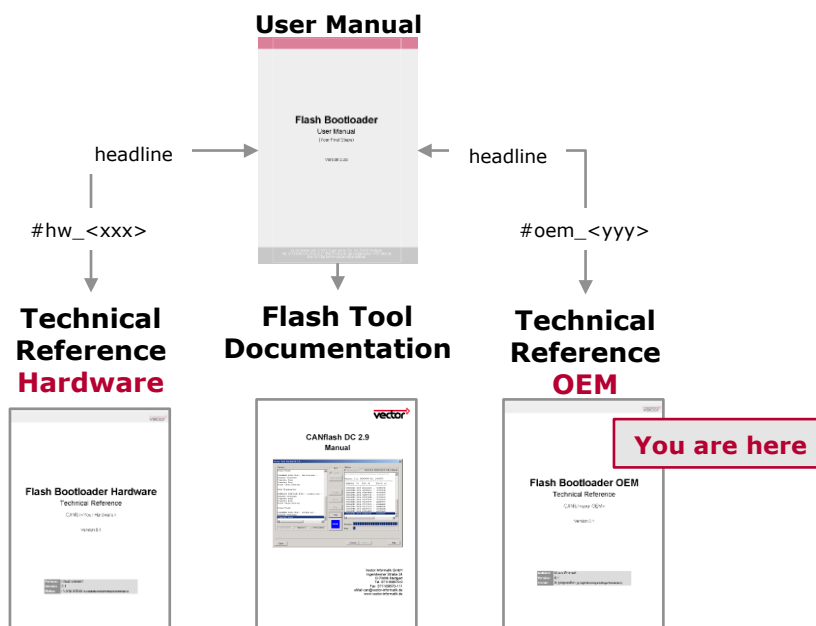


Figure 1-1 Manuals and References for the Flash Bootloader

Additionally this headline is marked with the ID of the reference from the User Manual. This ID looks like: **[#oem\_<yyy>]**.

## 2 FBL Software Architecture

### 2.1 Components

The Flash Bootloader (FBL) is a complete, self-contained application made up of several software components. Each component is contained in individual .c and .h files. The components interact as shown below:

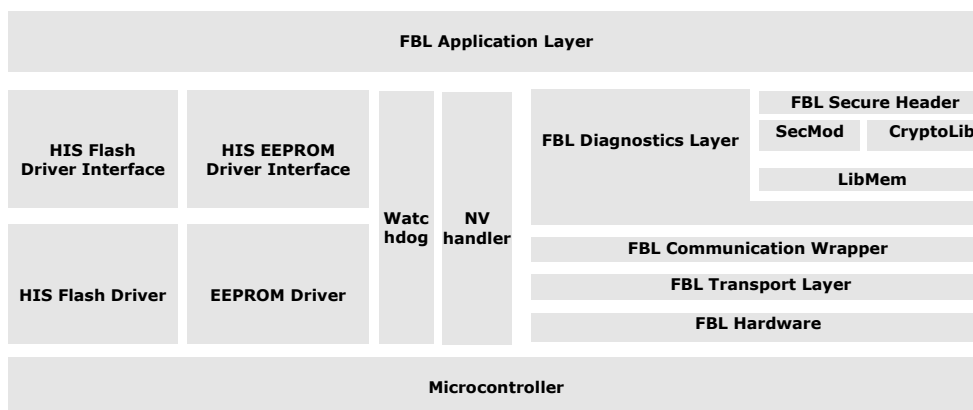


Figure 2-1 Component overview

**[#oem\_files]** A high-level description of each component follows. The components are grouped in three categories. The first group contains components found in the FBL, Flash, SecMod, Eep, and \_Common folders of your delivery (inside BSW if you have a new layout delivery). These are the Fbl Core Files. Do not modify the contents of the files in this group without prior written permission from Vector (modification of these files will void your warranty).



#### Note

There may be additional folders if non-standard components were also ordered (e.g. data flash driver, EEPROM manager, etc.).

#### 2.1.1 Core Files

Component/File	Description
applvect.h	Definition of Application-Vector-Table data structure
fbl_can.h	CAN parameter macros
fbl_def.h	Common data-type and structure definitions used by the FBL.
fbl_diag	Module implements diagnosis service functions. The implementation is specific to requirements defined by GM (reference [1]).

Component/File	Description
fbl_flio	Flash I/O routines provide interface to flash driver
fbl_hdr	Module for Gm header parsing. The implementation is specific to requirements defined by GM (reference [2])
fbl_hw	Hardware dependent code (CAN communication and H/W Timer)
fbl_main	Main module with main loop
fbl_mem	Module for Diagnostic buffer handling and programming. Upon request the module can be delivered in order to support: Encryption / Compression / Pipelined Programming (interleaved data transfers). In standard configuration none of these features are supported.
fbl_mio	General purpose API to device-drivers (MIO == Memory Input/Output)
fbl_tp	Transport Layer – Combines (and splits) diagnostics requests (and responses) across multiple CAN message frames.
fbl_vect	FBL vector table – defines all Interrupt Service vectors (usually this cannot be modified – See Section 4.5).
fbl_wd	Watchdog support module
flashdrv, eepdrv, EepIO, etc.	Non-volatile memory device-driver. You should not modify any source found in the device-driver folder(s).
Flashrom	C-array of the flash driver executable. This is linked to ROM and then copied to RAM at the appropriate time.
lotypes	Type definitions used by the memory Input/Output component
Sec_*	Security module. Used for required signature/hash calculations. The object files in Secmod/obj must be set to link with the rest of the bootloader source files.
v_def	ECU and compiler-specific type-definitions and macros used to abstract fundamental data types, pointers, and subroutine declarations.
v_ver.h	Version information of all delivered/licensed components.
WrapNv.h	Structures and macros used by the non-volatile wrapper.

Table 2-1 FBL Files

### 2.1.2 User modifiable application files

The second group consists of components that must be customized for your hardware and application. The files may be found in the FBL\\_Template folder. You should copy these files to your bootloader project folder, and rename them, removing the leading underscore from the filename.

Component/File	Description
_fbl_applvect.c	Application vector table – Jump table to all Interrupt Service Routines in Operating Software.
_fbl_ap	Hardware specific callback routines
_fbl_apdi	Application specific diagnostic routines
_fbl_apnv	Nonvolatile memory access routines, e.g. for presence-pattern handling.
_fbl_apwd	Application specific watchdog routines
_fbl_inc.h	Include file for including all FBL related include files
_memmap.h	Memory map configuration. Allows for custom memory placement of specific bootloader sections.
_wrapnv_inc.h	Include file for including any files necessary to the WrapNv component.
Application File	Description
_applvect.c	Application vector table configured to link to Operating Software. This will contain the calls to your application interrupt service routines.

Figure 2-2 User-modifiable Files

### 2.1.3 Generated Files

The third set of components is generated by the configuration tool, GENy. You should not modify these files by hand.

Component/File	Description
fbl_apfb.c/.h	Contains the Flash-Block Table. The table defines the regions of memory that may be programmed by the bootloader.
fbl_cfg.h	Bootloader feature switches and parameters.
fbl_mtab.c	Logical Block table configuration file. Contains the Application module address range configuration.
ftp_cfg.h	Transport Layer configuration switches and parameters
v_cfg.h	Hardware and compiler specific switches and parameters.
v_inc.h	Include file for including all version-tracking

Component/File	Description
	include files. Not needed to compile FBL.
v_par	Version information of the Generation Tool (GENy). Not needed to compile FBL.
WrapNv_cfg	Contains macros for accessing non-volatile data.

Table 2-2 Generated Files

Note that you need to configure `_MandatoryDeliveryPreconfig.cfg` in your GENy configuration. The contents of that file will be generated to `fbl_cfg.h`

### 2.1.4 Other delivery content

The delivery also includes some files that are helpful during development / demonstrate things that you need to do in your application.

Component/File	Description
dummySba.c/h	A demo sba-ticket, that was created using the Vector Dummy key information, that can be used for testing the SBA-ticket use case, before you change to the GM provided Public key.
rsakeys_2048.txt	Vector Dummy Key definition containing private/public key information. To be configured to GENy Secmod, if you want to use the Vector dummy public key information in your Fbl. This file is to be configured to the Download Container generation scripts in order to sign download containers. The Bootloader will accept generated modules as long it is configured to the same key.
_Gen_All.bat, _ModGenBase_x.xml, SignerInfoDummyKey.hex	Build environment required to create module containers. Check [6] for details. The file are
seedkey.zip	Transport Layer configuration switches and parameters
vFlashTemplateInstaller_GM_SLP6.exe	Installer for GM UDS specific vFlash template. Note: vFlash tool itself is not part of this delivery and is separately licenced.
Folder "Generators"	SLP specific Generation tool environment (implicitly used by generation tool).
Hexview	Tool used by container build environment (compare [6]). Can be also used to view and manually change download data containers.

Table 2-3 Other delivery content

For more general information about this see the UserManual\_FlashBootloader in the chapter **Extract the files to a folder on your PC.**



## 2.2 Memory Layout

The Flash Bootloader and the Operating Software must share a number of data-structures. The address of these structures must be known to both the Operating Software and the FBL. Since the FBL cannot be changed once released, the starting location in memory of the shared data must not change after release. The figure to the right shows one possible arrangement of the software elements that may be stored in non-volatile memory. Except as noted below, the actual order and location of the elements is unimportant.

### 2.2.1 The GM File-Container

Every module downloaded by the FBL must be attached with a File-Container (compare [2]). The file containers (also referred to as file-headers in this doc) are used to identify the type of the module, and may contain information about where data in the module is written to. The container format will depend on the type of the module. A single module may have 1 or more container layers (known as envelopes in [2]). A complete description of the containers may be found in "Programmable Data Files" (Chapter 9 in reference [2]).

#### 2.2.1.1 The Operating S/W File-Container

Currently the bootloader supports an operating S/W download as a signed application S/W file. In the future, the bootloader will support a signed and compressed application S/W file. Further information can be found in "Supported Data Files" (section 10.2 of [2]).

The operating S/W file container contains information on the location of where to store the operating S/W into flash memory as well as information on the calibration partitions (see section 3.2.4 Partitions).

The Module-ID (MID) field of the header must correspond to one of the values reserved for Operating Software (0x0001, 0x0021, 0x0031, or 0x0041).

#### 2.2.1.2 Calibration Module File-Container

Currently the bootloader supports a calibration download as a signed calibration file. In the future, the bootloader will support a signed and compressed calibration file. Further information can be found in "Supported Data Files" (section 10.2 of [2]).

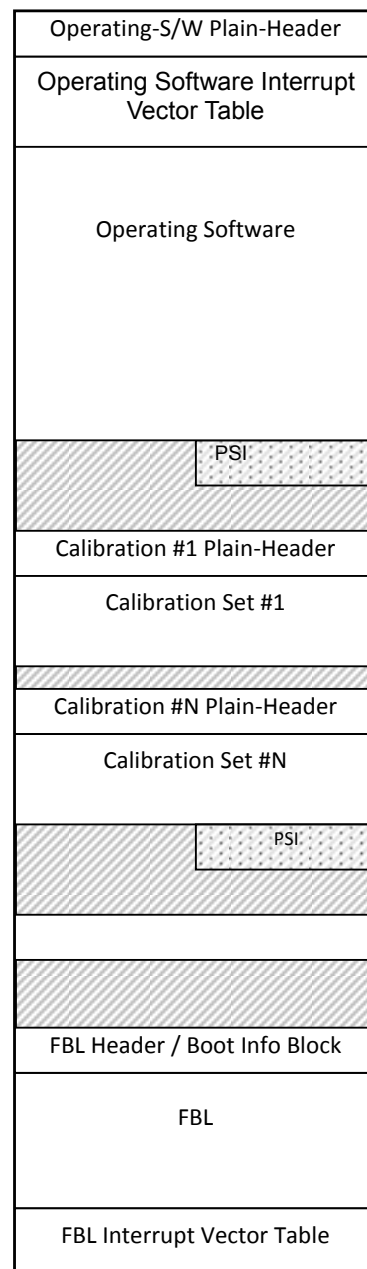


Table 2-4 Example Memory Layout

The Module-ID (MID) field must correspond to the range of values associated with the Operating Software module that determines where the Calibration module is located. For example, use 0x0002 – 0x0014 for modules associated with Operating Software MID 0x0001. The Calibration MIDs must be in sequential order, starting with the value following the Operating Software's MID. For example, the first Calibration module associated with Operating Software MID 0x0021 must be 0x0022. In this example, additional Calibration MIDs are numbered 0x0023, 0x0024, etc.

### 2.2.1.3 Boot Info Block

The Boot Info Block is stored in the protected memory of the bootloader ROM. The values stored are configured as described in the table below.

Component/File	Description
Security Public Key	Input in GENy. This key is used to validate the root signature of the signer info.
Subject Name	Input in GENy. Hexadecimal value that identifies the group of ECUs for which the signer info is applicable.
ECU Name	Input in GENy. ASCII representation of the ECU name.
BCID	Input in GENy. Bootloader compatibility identifier. This is used to establish if the operating software is compatible with the bootloader.
Application Space	Defined by logical block configuration in GENy. A single logical block defines the combined Application and Calibration space of a single operating software and all of its corresponding calibration modules.
Calibration Space	Defined by logical block configuration in GENy. A single logical block defines the combined Application and Calibration space of a single operating software and all of its corresponding calibration modules.
DLS	Input in GENy. Design Level Suffix. Each bootloader software revision shall have a unique DLS.
Hex Part Number	Input in GENy. Bootloader software part number represented in hexadecimal.
ASCII Part Number	ASCII representation of the part number.

Table 2-5 Boot Info Block configuration

If the FBL has been configured with the ROM Integrity check enabled, you will need to calculate the value of the CheckSum field (e.g. using hexview). The algorithm used must match that implemented in the FBL, which is a 2s complement wordsum ( Hexview “CS5” for Big endian ECUs and “CS6” for Little endian ECUs; compare e.g. generated file v\_cfg.h for endianness information ). Checksum implementation is found in callback `ApplFblRomIntegrityCheck()`.

### 2.2.2 Operating S/W Interrupt Vector Table

The Operating Software Interrupt Vector Table is a mirror for the ECU's actual vector table. The FBL distribution usually contains two tables, contained in the files `fbl_applvect.c` and `applvect.c`.<sup>1</sup> The first file, `fbl_applvect.c`, is linked with the FBL, and is used to support ECU sleep/wakeup modes (when available). The latter file, `applvect.c`, is linked with the Operating S/W. This file must be tailored to contain jumps to the application's interrupt service routines (ISR's). The tables may be located anywhere within the segments used for the Operating Software, but the address must be the same for the Operating S/W and FBL (the Op. S/W table replaces the FBL's table). In most cases, the location is established by encapsulating the table in a named section (usually 'APPLVECT'). The linker command directives then define an absolute address for the section. When setting the address of the tables, the linker directives for both the FBL and Operating S/W must be edited.

### 2.2.3 Logical Block table

The Logical block table has to be configured in GENy to contain all modules programmed to flash. Calibration files are not configured separately; they belong to the corresponding application area configured. Multiple application files can be configured (if applicable).

**Note**

The Logical block table contains the Application Space and Calibration Space parameters of the Boot Info Block.

### 2.2.4 Partitions

The memory generally is split into 3 or more partitions (bootloader, operational S/W, and calibration partitions). The application and calibration partitions are determined by the contents of the application plain header. Each calibration module is placed into a calibration partition and a calibration partition may contain multiple calibration modules. See [2] for more information on partitions.

### 2.2.5 Presence Patterns / Programmed State Indicator

Multiple presence-patterns/PSIs are needed if multiple modules (Operating S/W and Calibration) must be downloaded to your ECU. The requirements found in "Programmed State Indicator (PSI)" (Section 12.5.10 of reference [2]) identify how to manage the PSI(s) (Vector term is presence-patterns)..

The presence-patterns are managed in the implementation of the functions `ApplFblValidateBlock()`, `ApplFblInvalidateBlock()`, and `ApplFblIsValidApp()` (all found in `fbl_apnv.c`). Please read section 4.10 ([#oem\_valid] – Proposals for Handling The Validation Area) very carefully for details of how presence-patterns are implemented in the FBL.

Check Figure 3-14 Typical Logical Block partition for a typical example mapping for PSI information.

---

<sup>1</sup> In many deliveries, the vector tables are supplied as assembly-language source code. See also the FBL Release Notes for your delivery.

Downloaded modules are not allowed to overlay the regions containing the presence-patterns. The bootloader will return an error if this is detected.

## 2.3 Run-Time Details

A general description of the order that application and hardware-specific routines are called in may be found in reference [4].

The following sections summarize when callback functions are used during the power-on reset sequence, start from Operating-Software, and Download sequences.

### 2.3.1 Power-On Reset

Upon reset, the FBL will execute the compiler-specific start-up code, followed by a call to main(). The sequence of steps performed by the FBL is shown below:

```
< main >
| < ApplFblInit() >
| | < ApplFblInitErrStatus() >
| < ApplFblExtProgRequest() >--Start-by-O/P sowftaer-->-----|
| < ApplFblIsValidApp() > |
| | -----Op/SW not ready-->-----+
| < ApplFblWDLONG() > |
| < FblTimerStopp() > |
| < JSR_APPL() > /* Start Operating S/W */ |
| |
| < ApplFblStartup(kStartupPreInit) >-----<<-----+
| | < ApplFblRomIntegrityCheck() >
| | | < ApplFblVerifyChecksum() >
| | < ApplFblRamIntegrityCheck() >
| < FblInit() >
| | < FblInitWatchdog() > /* Copy trigger routine to RAM */
| | < ApplFblWDInit() >
| | < ApplFblCanParamInit() >
| | < FblHardwareInit() > /* start timer, CAN, etc */
| | | < ApplTcrvNormalMode() >
| | < FblDiagInit() >
| | | < ApplFblResetVfp() >
| < ApplFblStartup(kStartupPostInit) >
| < FblRepeat() > /* Wait for requests */
```

### 2.3.2 Start from Operating Software

The Operating Software should start the bootloader and pass the required Tester address to the boot. Detailed handling and description of the CAN-Init structure may be found in "STEP3" of chapter 45.

After reset trigger by application, the ECU execution continues as described in section 2.3.1.

The FBL determines if it is started by the Operating Software by calling the function `ApplFblExtProgRequest()`. If this function returns `kProgRequest`, then the application-validation call (`ApplFblIsValidApp()`) is skipped, and the mode-flag `START_FROM_APPL` is set. The macro `GetFblMode()` returns the FBL mode; the returned value may be compared to `START_FROM_APPL` (a bitwise compare) to determine if the FBL was started by the Operating Software.

### 2.3.3 Download Sequence

To download a module, the download tool (such as vFlash) will send a sequence of diagnostics requests. The initial requests are sent to all ECUs on the CAN bus, to prepare the whole network for Programming..A summary of the diagnostics requests done by vFlash (in order of transmission) is shown below:

## Requests sent to all ECUs

```
[ Read Data By Identifier ($22 $F0 $B0) ]  
[ Session Control Extended Session ($10 $03) ]  
[ Communication Control ($85 $82)]  
[ Disable Normal Communication ($28 $03 $F3) ]  
[ Read Data By Identifier ($22 $F0 $F0) ]
```

## Requests sent only to target ECU

```
[ Request Security Seed ($27 $01) ]  
[ Session Control Programming Session ($10 $02) ]  
[ Routine Control Erase Memory($31 $01 $FF $00) ]  
[ Request Download ($34) ]  
[ Transfer Data ($36) ] (N TIMES)  
[ Transfer Data Exit ($37) ]  
[ Routine Control Update PSI ($31 $01 $02 $09) ]
```

## Requests sent to all ECUs

```
[ Session Control Default Session ($10 $01) ]
```

Although not shown, the download tool is required to send Tester-Present (\$3E) requests periodically to keep all ECUs in the network in extended session.

If the Operating Software is running, then it must handle all requests up to Session Control Programming Session (service \$10 \$02). When service \$10 \$02 is received, the Operating Software should send a response-pending response and invoke the FBL (do not send a final response). The FBL will send the final response after it has completely initialized.

## 3 Configuration of the GM Flash Bootloader

### 3.1 Overview

The Fbl is configured using the Generation tool GENy.

A complete description of GENy is beyond the scope of this document. The sections that follow provide a quick tutorial of GENy and details that are specific to the GM Bootloader. Please refer to the on-line help in GENy for complete details.

An example configuration is included with the demonstration FBL included with your delivery.

### 3.2 Starting with GENy

When installing GENy, a link to GENy is added to your PC's Start menu (by default, a project-specific link to start GENy is in Programs/Vector/CANfbl/<project>).

When started, the following window will appear:

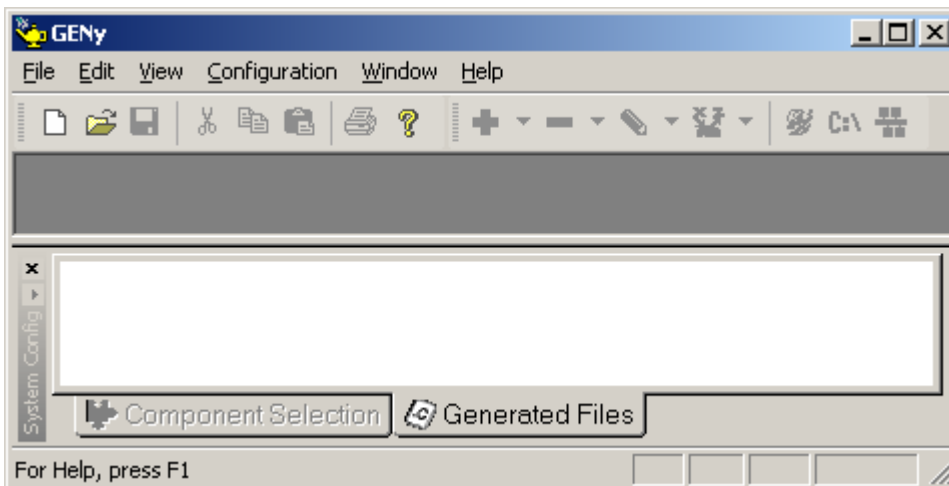


Figure 3-1 Initial GENy main window

To create a new configuration, you should select **New...** from the File menu. The following dialog will appear:

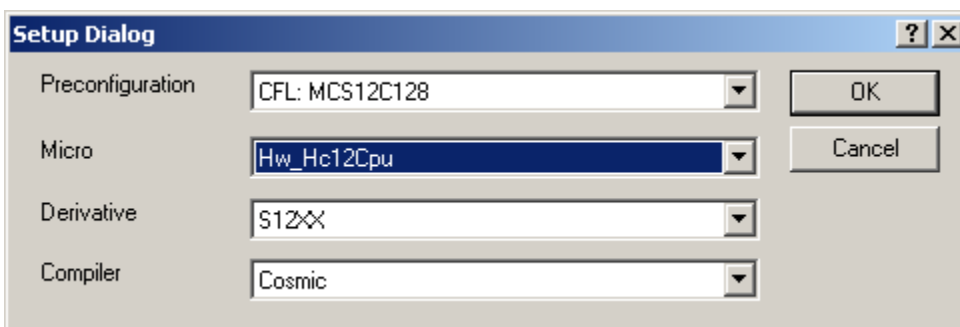


Figure 3-2 GENy Setup Dialog

The actual field values will vary, depending on your delivery license and hardware. In most cases, the default values will be appropriate, and you need only click on **[OK]** to proceed.

The main GENy window will be updated as shown below once the initial setup has been completed.

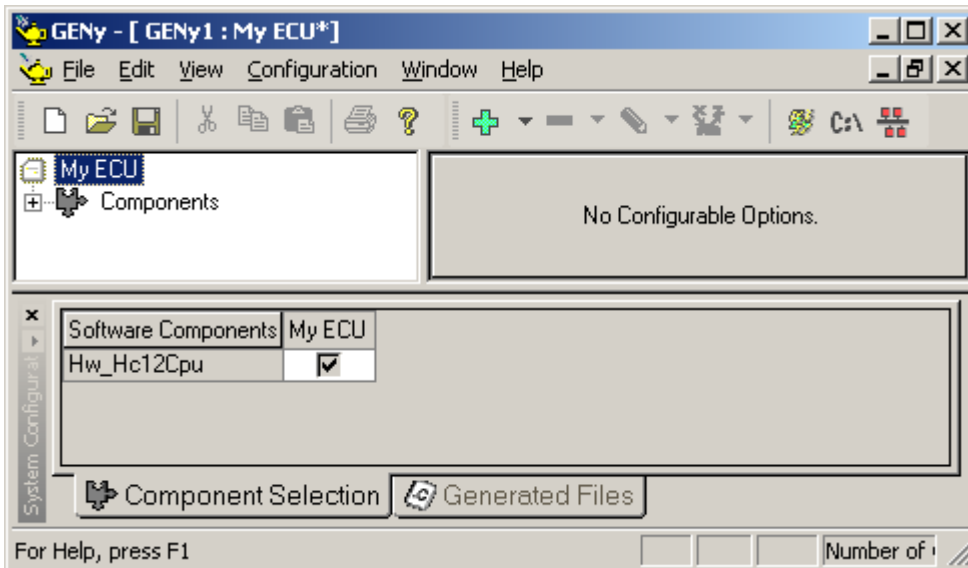


Figure 3-3 GENy main window after pre-configuration

The next step is to define a channel. You may select **Add Channel** from the **Configuration** menu, or you may click on the Plus icon from the tool bar. A dialog like that shown below will appear.

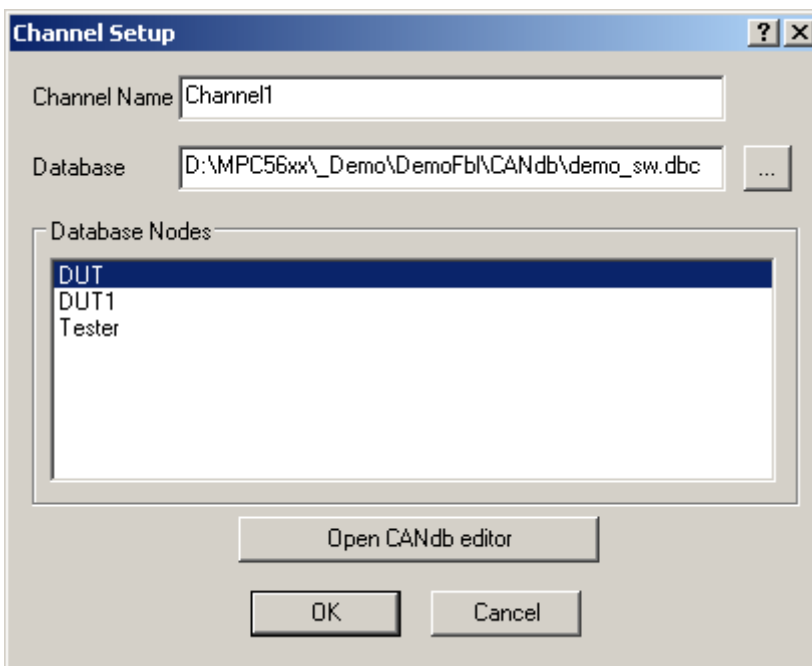


Figure 3-4 GENy Channel Setup

The first step is to select the dummy database (.DBC file) provided by Vector. No parameter from this will get into the configuration, but it is a mandatory step. Once the database has been selected, a list of the ECU Nodes defined by the database will appear in the **Database Nodes** field.

You should select the DUT node. Select DUT and DUT1 if your ECU is used multiple times in the same vehicle. This enables the Multiple-Identity-Module (MIM) feature of the FBL. See also section 8.2.

When you click on **[OK]**, the GENy main window will appear as shown below:

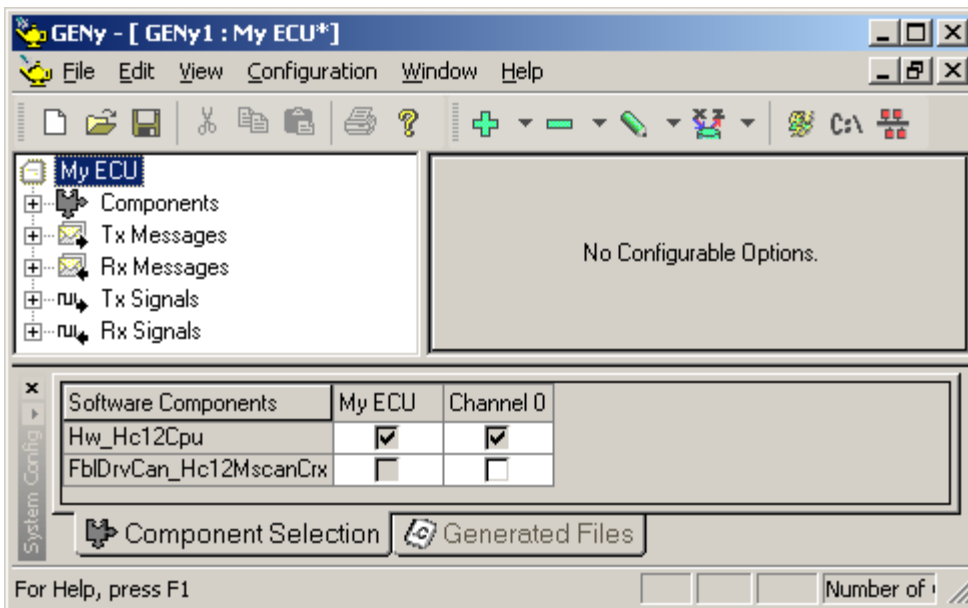


Figure 3-5 GENy main window after channel setup

At this point, you must add the Software Components for the FBL to the channel that was defined. Click on the check-boxes in the **Channel 0** column for each component. You must add the FbiDrvCan\_<hardware>, FbiTplso and FbiCan\_14230\_GM components.

After the Software Components have been selected, you should expand the list-tree in the left-most window to select between the component-configuration windows. The tree is expanded by clicking on the **[+]** button, or by double-clicking on the **Components** label. The expanded tree is shown below:



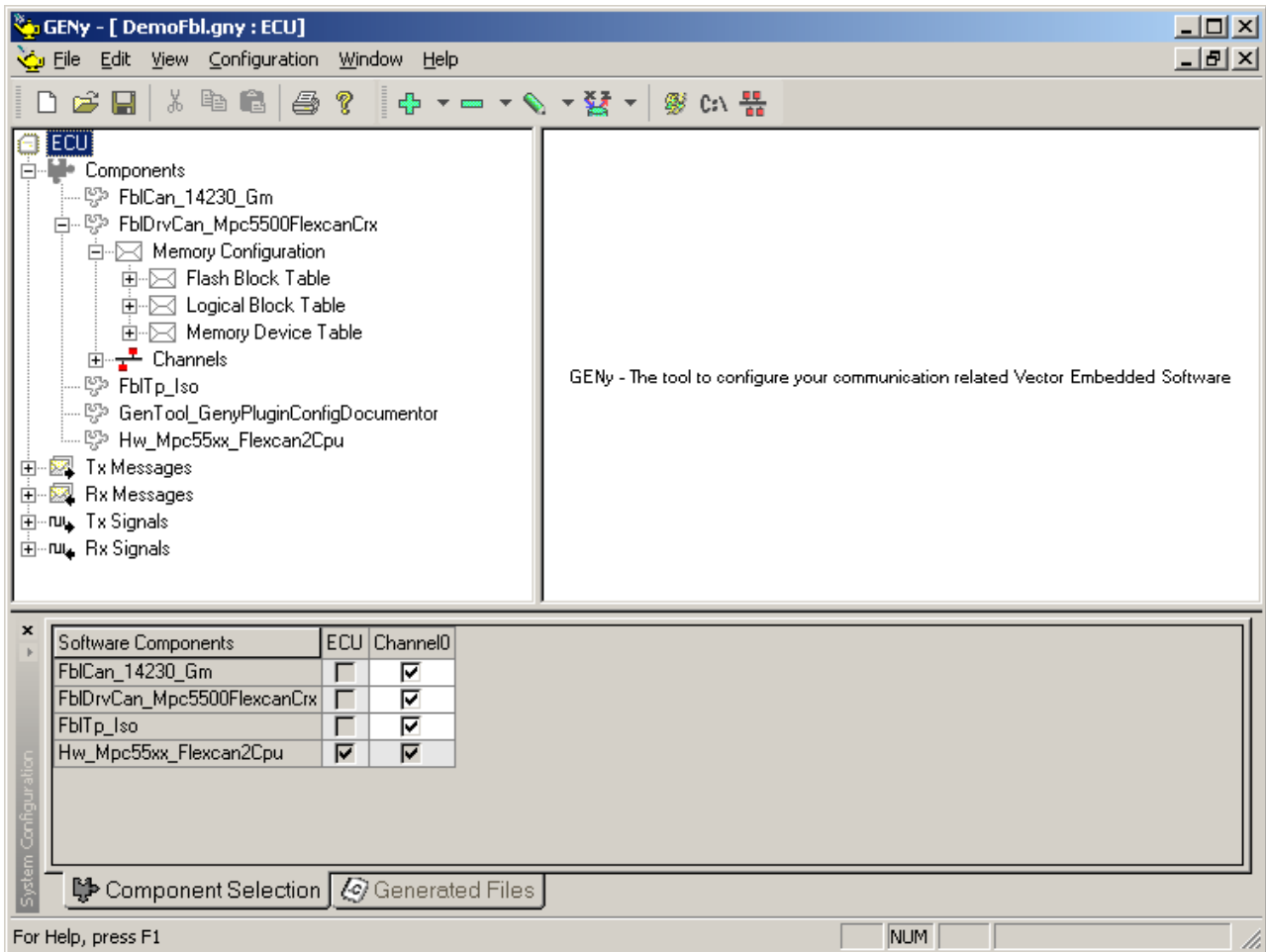


Figure 3-6 GENy Components

Before proceeding to component configuration, you should save the configuration. Select **Save** from the File Menu, or press the floppy-disk icon on the tool bar. GENy will display a standard file-selection dialog box, with the default path set to the directory the database is located in. You may change the path and set the filename as desired. GENy will create a file with a .GNY extension. The folder the file is saved in will be used as the Project Directory.

Once the Project Directory has been established, you should select **Generation Paths...** from the Configuration menu. GENy will display the dialog shown below:

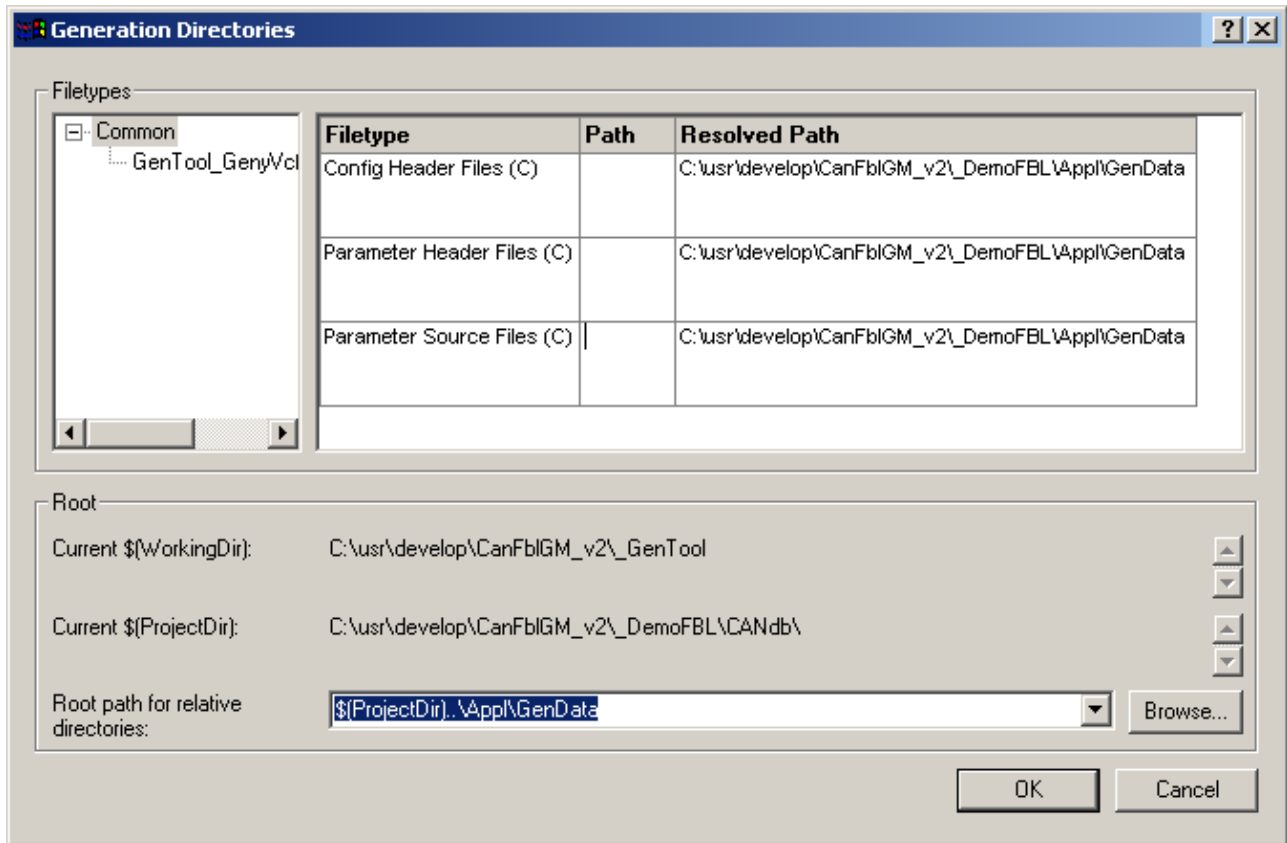


Figure 3-7 GENy directory selection

By default, GENy will place the files it generates into the Project Directory. You may enter a new path relative to the Project Directory (as shown above), enter a path relative to the GENy's working-directory (the directory GENy is executed from), or you may enter an absolute path.

After pressing **[OK]**, you are ready to configure the individual components.

### 3.3 CAN Configuration

The CAN controller is configured by expanding the **Channels** component, and selecting the **Channel 0** component from the list-tree. The contents of the window that appears on the right will be highly dependent on the hardware that has been selected. An example of the CAN configuration window is shown below:



#### Note

Note that the GM Bootloader supports only one channel.

Configurable Options		Channel 0
Type of bussystem	CAN	
Manufacturer	GM	
242A0CD9-284B-4e9a-BA17-D19EF24CA6E8	*	
+ FBL		
- Initialization		
- Init Structures	Add	
- Init Structure	Delete	
Module Control Register 0	0x4	
Module Control Register 1	0x84	
Bus Timing Register 0	0x7b	
Bus Timing Register 1	0x14	
Receiver Interrupt Enable Register	0xc5	
Identifier Acceptance Control Register	0x20	
Acceptance Filter Configuration	...	
Bustiming Configuration	...	
- CAN Controller (HC12)		
Register block offset	0x180	

Figure 3-8 GENy CAN Configuration

For details regarding this window for your hardware, please refer to the document **Technical Reference\_<Hardware>** provided with your delivery.

By default, GENy initializes the CAN hardware as dual-wire (500.0 KBPS). Use the bus timing Configuration dialog to select the appropriate baud-rate.

### 3.4 Bootloader Configuration

The features of the bootloader are configured in two separate components: FblDrvCan\_<hardware> and FblCan\_14230\_GM (see Figure 3-6 GENy Components). Features specific to the component is shown in the right-hand side of the window when the component is selected in the left-hand side of the window.

#### 3.4.1 FblDrvCan component

The FblDrvCan component contains both hardware-specific and hardware independent selections. For details of the hardware-specific features, please refer to the document **Technical Reference\_<Hardware>**.

Configurable Options		FblDrvCan_Mpc5500FlexcanCrx
[- FblDrvCan_Mpc5500FlexcanCrx		
Flash code buffer size (Byte)	0x400*	
Watchdog function size	0x200*	
<i>Additional controller specific configuration may be available..</i>		
[- FBL		
User Config File	D:\usr\usage\Delivery\CBD13x\CBD1300342\DD1\external\Demo\...	
Project State	Integration	
Stay in Boot	<input type="checkbox"/> *	
Maximum Number of Segments	10*	
Sleep Mode	<input type="checkbox"/> *	
Application Task	<input checked="" type="checkbox"/> *	
Bootloader Header Address	0x400*	
Diagnostic Buffer Size [B]	4095*	
Fill Code	0xc3*	
Internal Memory Copy	<input checked="" type="checkbox"/> *	
FblStart Function	<input checked="" type="checkbox"/> *	
[- Download		
Download	...	
[- General Timer Algorithm		
Timer Clock [kHz]	64000*	
[- Download Handling		
Data processing buffer size [B]	512*	
Pipelined programming	<input type="checkbox"/> *	
Write segmentation [B]	256*	
Unaligned data transfer	<input checked="" type="checkbox"/> *	
[- Watchdog		
Watchdog Service	<input checked="" type="checkbox"/> *	
Trigger Cycle [ms]	1*	

Figure 3-9 FblDrvCan configuration example

Each configuration field of FblDrvCan component is described below:

Field Name	Description
Flash Code Buffer Size (Byte)	This configuration is found in the hw specific configuration of every hw platform available. Configure the size of the array to hold the downloaded flashdrv. Recommendation is to add a surplus of 20% or more to allow for larger flashdrv through updates in future.
Watchdog function size	Array size reserved to hold code for the watchdog trigger functionality (FblLookForWatchdog() and ApplFblWDTrigger() ). This configuration may not be offered for your compiler dependent

Field Name	Description
	configuration if a linker based approach to copy watchdog code is used. Check <b>Technical Reference_&lt;Hardware&gt;</b> for details.
User Config File	The path and name of a file to be included in the generated configuration file fbl_cfg.h may be specified. The file may be used to activate features of the FBL that are not included in the GENy components. Please derive your User config from the provided <b>_MandatoryDeliveryPreconfig.cfg, which contains mandatory configuration items for this Fbl.</b>
Project State	<p>When configured to “Integration”, the bootloader helps you find configuration errors and sends out useful information in case of errors (see 8.3). This setting is recommended when starting a configuration or when having issues in the bootloader to support you in finding the root cause. Please use “Integration” when you send us a communication log as it contains useful information.</p> <p>Please make sure you select “Production” when you do not need any Integration support any more, at the latest when you prepare for testing/production. If you do not change to “Production” the bootloader will continue send out data unexpected by GM on 1A 7F service. See details on this configuration in GENy Onscreen Help box.</p>
Stay in Boot	<p>Development feature: Allow forcing bootmode. This is done by checking for a defined message during startup within a given time window.</p> <p>Note that this feature is not allowed by GM and should be disabled for final configuration (This will be verified if you change Integration state to production).</p> <p>For details compare <b>[#oem_time]</b> – Stay-In-Boot mode on page 102)</p>
Maximum number of Segments	Maximum number of address regions allowed in any download module.
Sleep mode	<p>When selected, the FBL will use the CAN-controller’s wake-up interrupt to start the ECU after entering sleep-mode. Not all CAN-controllers support this feature.</p> <p>See the descriptions for <code>ApplFblSleepModeAllowed()</code>, <code>ApplTrcv</code></p>

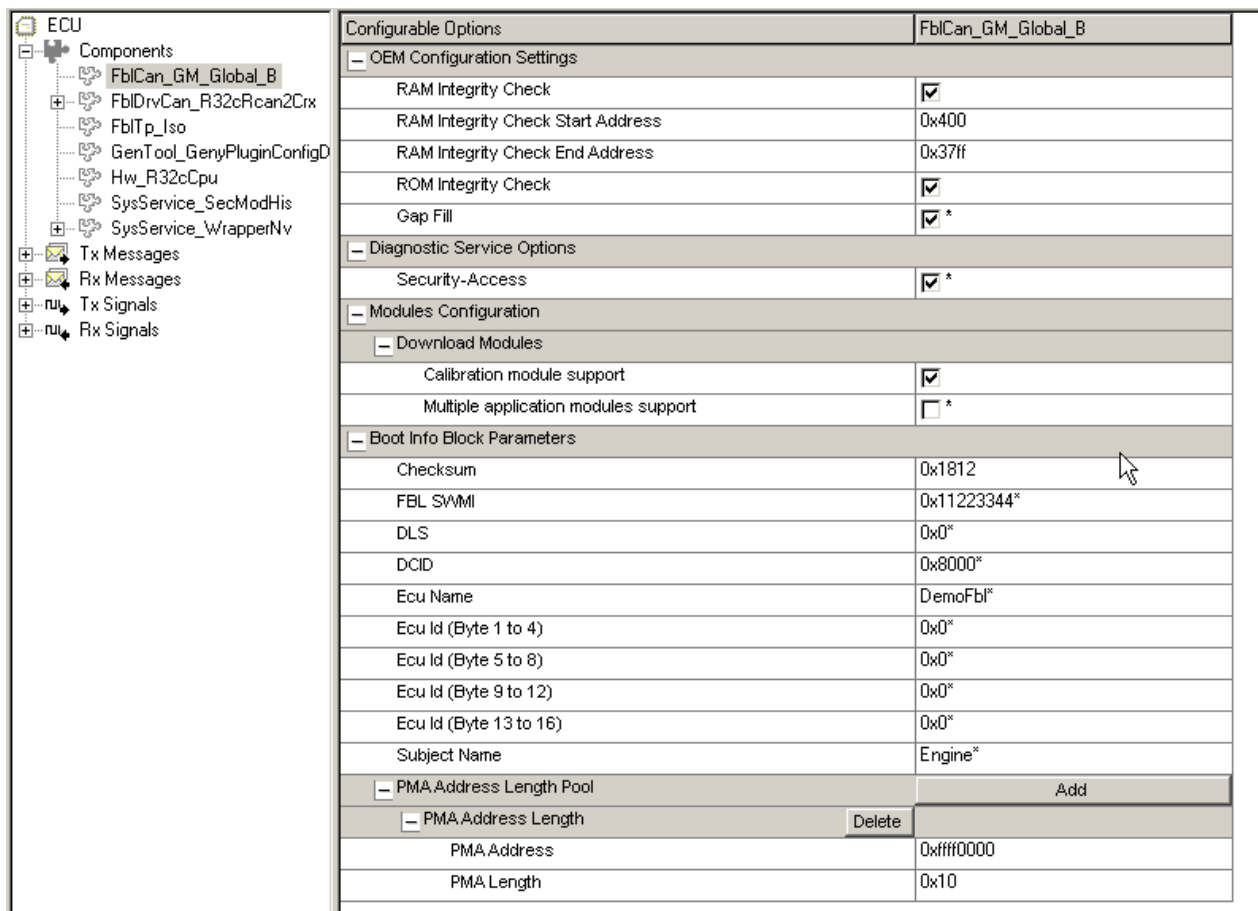
Field Name	Description
	<code>rSleepMode()</code> , <code>ApplFblEnterStopMode()</code> , and <code>ApplFblCanWakeUp()</code> .
Application task	When selected, the FBL will periodically call <code>ApplFblTask()</code> . This function may be customized by you to implement any background operations.
Bootloader Header address	The logical address of the File-Header for the bootloader must be entered here. The value <b>must</b> match the address used by your linker to map the header to its proper location (in most cases, the mapping is resolved by the address associated with a named section, usually FBLSTART).
Diag buffer Size [B]	This is the amount of memory (in bytes) reserved for data in diagnostic request messages. The value may be up to 4095
Fill code	<p>If the Gap-Fill feature is enabled, the FBL will also use this value to fill all unused regions of memory. The value must be between 0x00 and 0xFF (multi-byte fill pattern is not supported).</p> <p>When writing data to a non-volatile device, the number of bytes written must be a multiple of the device's write-segment size. If an address-region does not end on a write-segment boundary, the FBL will fill the unused bytes with the value specified in this field.</p>
FblStart Function	<p>This allows the user to disable standard functionality provided to transition from application to boot mode. Disabling is only required if you want to save code size.</p> <p>The switch can e.g. be disabled if an Eeprom is used instead of a Ram pattern, or if the application already prepares the ram pattern and copies all shared Ram required by the bootloader to transition.</p>
Watchdog Enable	<p>When enabled, the FBL will use the functions <code>ApplFblWDInit()</code>, <code>ApplFblWDLONG()</code>, and <code>ApplFblWDTrigger()</code>, to manage the ECU reset-timer.</p> <p>If not selected, the FBL will assume that the reset timer is not used.</p>
Watchdog time	This specifies the interval, in milliseconds, between calls to the watchdog trigger function, <code>ApplFblWDTrigger()</code> . The value only has meaning if the Watchdog Enable switch is

Field Name	Description
	<p>selected. The value must be less-than the time-out period of the watchdog. The value must be in the range 1 – 65535 and must be an integer multiple of FBL_REPEAT_CALL_CYCLE.</p> <p>Note: Earlier versions of the FBL are limited to a 255 ms watchdog trigger period.</p>

Table 3-1 Bootloader Configuration

### 3.4.2 FblCan\_Gm\_Global\_B configuration

The following tables describe the FblCan\_Gm\_Global\_B specific switches that can be configured.



Configurable Options		FblCan_Gm_Global_B
<b>OEM Configuration Settings</b>		
RAM Integrity Check		<input checked="" type="checkbox"/>
RAM Integrity Check Start Address		0x400
RAM Integrity Check End Address		0x37ff
ROM Integrity Check		<input checked="" type="checkbox"/>
Gap Fill		<input checked="" type="checkbox"/> *
<b>Diagnostics Service Options</b>		
Security-Access		<input checked="" type="checkbox"/> *
<b>Modules Configuration</b>		
<b>Download Modules</b>		
Calibration module support		<input checked="" type="checkbox"/>
Multiple application modules support		<input type="checkbox"/> *
<b>Boot Info Block Parameters</b>		
Checksum		0x1812
FBL SWMI		0x11223344*
DLS		0x0*
DCID		0x8000*
Ecu Name		DemoFbl*
Ecu Id (Byte 1 to 4)		0x0*
Ecu Id (Byte 5 to 8)		0x0*
Ecu Id (Byte 9 to 12)		0x0*
Ecu Id (Byte 13 to 16)		0x0*
Subject Name		Engine*
<b>PMA Address Length Pool</b>		<b>Add</b>
<b>PMA Address Length</b>		<b>Delete</b>
PMA Address		0xffff0000
PMA Length		0x10

Figure 3-10 GM Fbl configuration Settings

Field Name	Description
Enable RAM Integrity Check	<p>When selected, the FBL may invoke <code>ApplFblRamIntegrityCheck()</code> from <code>ApplFblStartup()</code>. The function is responsible for verifying that Random-Access-Memory is functioning properly, and updating any flags used by</p>

Field Name	Description
	<p><code>ApplFblReportProgrammedState()</code> to indicate the result.</p>
RAM Integrity Check Start Address	<p>Start address of RAM region to be checked. Checked Ram should include all RAM used by the bootloader (stack, global variables, flashCode buffer)</p> <p>Note: If several regions are required, only the first region can be configured in GENy, any further regions will have to be configured inside <code>fbl_ap.c ApplFblRamIntegrityCheck()</code> address table.</p>
RAM Integrity Check End Address	<p>End address of RAM region to be checked. Checked Ram should include all RAM used by the bootloader (stack, global variables, flashCode buffer)</p> <p>Note: If several regions are required, only the first region can be configured in GENy, any further regions will have to be configured inside <code>fbl_ap.c ApplFblRamIntegrityCheck()</code> address table.</p>
ROM Integrity Check	<p>The GM "Global Bootloader Specification" requires that the FBL perform an integrity check on FBL ROM, and report the result to the \$A2-Report ProgrammedState requests. When enabled, the FBL will calculate the checksum based on the values in its GM File Header. If disabled, the FBL will not perform the ROM check.</p> <p>Note :</p> <p>The check region will have to be configured inside GENy "GM Bootloader Header" address region. A single region is specified. If an additional region is required, it will have to be manually added inside <code>fbl_ap.c ApplFblRomIntegrityCheck()</code> to the segment list.</p>
Gap Fill	<p>If enabled, the FBL will fill all unused regions of the non-volatile device(s) with "Fill Code" specified in <code>FblDrvCan_XX</code> configuration. The fill happens at the end of the download. The drop box below allows you to configure detailed behavior for this selection.</p> <p>If disabled, unused regions will contain the value resulting from the device's erase operation.</p>



Field Name	Description
	<p>Compare [2] section 7.5, Unused Flash Space: "GM shall determine with the ECU supplier if the Pad bytes will be programmed and what the Pad and Fill bytes value should be."</p> <p>Note that there is the possibility to disable this feature in order to reduce code size and fill your download container with the intended fill value instead.</p> <p>There is also the option to disable this feature and implement a custom gap fill algorithm in the function <code>ApplFblFillGaps</code>. This may allow to reduce code size and decrease execution time of the built in gap fill function. See also section 5.3 and 9.9.</p>
Enable Security-Access	<p>When selected, the FBL will accept Security-Access (service \$27) requests Only SPS-Request-Seed (\$01) subfunction is supported in accordance with the GB6002.</p> <p>If not selected, the FBL will respond to Security-Access requests with a negative response, indicating that the service is not supported (Select this if your ECU does not need \$27 in your application).</p> <p>Note: Independent of this configuration the FBL will never perform a real security access check, just like defined in GB6002.</p>

Figure 3-11 GM-Specific Configuration



**Note**

The "RAM Integrity Check" requires that the check be performed after I/O and CAN initialization has been completed. However, `ApplFblRamIntegrityCheck()` (via `ApplFblStartup()`) is called before the CAN initialization (I/O initialization requirement is satisfied if performed in `ApplFblInit()` or in `ApplFblStartup()` before the check).

Field Name	Description
Calibration module support	Can be disabled if no calibration files are required in order to reduce code size.
Multiple application module support	Bootloader supports multiple application module downloads if enabled. Disable this option in order to reduce code size.

Field Name	Description
	Check chapter 8.28.2 for further configuration aspects.
Checksum	<p>This field defines the compiled-in value of the Checksum (CS) field for the bootloader's File-Header.</p> <p>It is likely that the required value of this field will be different each time the FBL is changed. Therefore you will have to settle this value once the software will not change any more.</p>
FBL SWMI (HexPart Number, Boot Info Block Parameter)	<p>This field defines the compiled-in value of the Software Module Identifier (SWMI) field for the bootloader's File-Header.</p> <p>Per "Boot Info Block" (Section 6.10 in reference [2]), the value of this field shall be your ECUs bootloader part number coded as a 4-byte hexadecimal number. The number is normally determined by agreement between you and General Motors.</p> <p>Note: ASCII representation cannot be configured in GENy, instead this has to be directly implemented/translated in <code>ApplFblReadDataByIdentifier()</code> callback if needed.</p>
DLS (DLS Boot Info Block, parameter)	<p>This field defines the compiled-in value of the Design-Level-Suffix (DLS) field (also known as the Alpha Code) for the bootloader's File-Header.</p> <p>Per "Boot Info Block" (Section 6.10 in reference [2]), the value of this field shall contain two ASCII characters.</p>
DCID (BCID Boot Info Block, parameter)	<p>This field defines the compiled-in value of the Data Compatibility Identifier (DCID) field for the bootloader's File-Header.</p> <p>The value is a two-byte number that may be compared to the DCID field in the Operating Software's File-Header. The value determines that the Operating Software and bootloader interfaces are compatible.</p> <p>The check is not performed if the value of this field is 0xFFFF.</p> <p>The legal range for this field is 0x8000 – 0xFFFF.</p> <p>For additional information, see "Boot Info Block" (Section 6.10 in [2]). Note that reference [2] often refers to this field as either BCID (Bootloader Compatibility ID) or CCID (Calibration Compatibility ID).</p>
ECU Name	ECU name in ASCII. Maximum 8 byte length.

Field Name	Description
Ecu Id (Byte 1 to 4)	Byte 1 to 4 of the ECU ID. Each unique ECU will have a unique ECU ID. Value relevant for development, a process must be in place to override this value uniquely for each ECU.
Ecu Id (Byte 5 to 8)	Byte 5 to 8 of the ECU ID. Each unique ECU will have a unique ECU ID. Compare comment Byte 1-4
Ecu Id (Byte 9 to 12)	Byte 9 to 12 of the ECU ID. Each unique ECU will have a unique ECU ID. Compare comment Byte 1-4
Ecu Id (Byte 13 to 16)	Byte 13 to 16 of the ECU ID. Each unique ECU will have a unique ECU ID. Compare comment Byte 1-4
Subject Name	ECU family name as specified by GM. Input as ASCII. Maximum 16 byte length.
PMA Address	This field defines the logical address of the address-region used by the bootloader.
PMA Length	This field defines the length (in bytes) of the address-region occupied by the bootloader.

Figure 3-12 GM Modules and Boot Info Block Detail Configuration

### 3.5 Memory Configuration

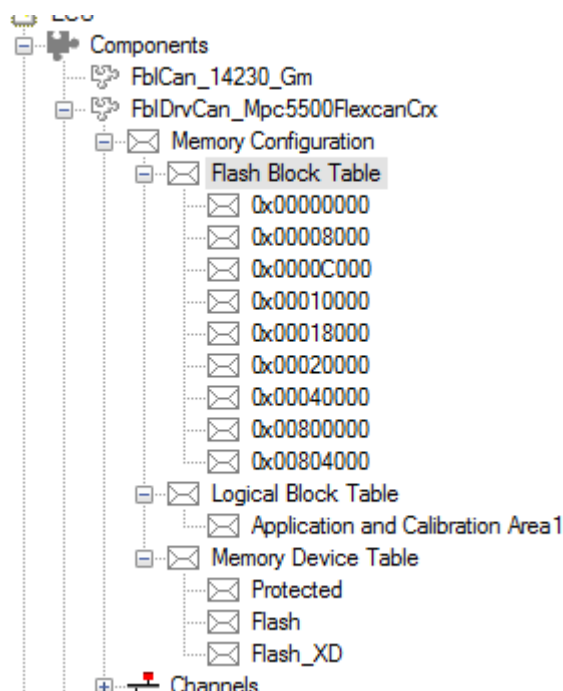


Figure 3-13 Memory Configuration

The Flash Block Table identifies the regions of memory that may be written to by the bootloader. The table also defines the addresses sent to the device-driver(s) when erasing memory.

The Logical Block Table Describes independently erased Module sets. These are

- > Primary Operating Software (+ Calibration modules)<sup>2</sup>
- > Secondary Operating Software (+ Calibration modules)<sup>3</sup>

The Logical Block table hence contains only one entry in standard use case: Primary Operating software (+ calibration files). It contains several entries if Multi-processor environment is required, also compare 8.2.

The typical configuration is one logical block with optional calibration file memory reserved.

Application Header address and Application Presence Pattern address decide on the internal partition for application / calibration file areas. Both blocks touched by these elements must belong to application and hence are reserved for it. The most straight forward configuration is hence two distinct areas:

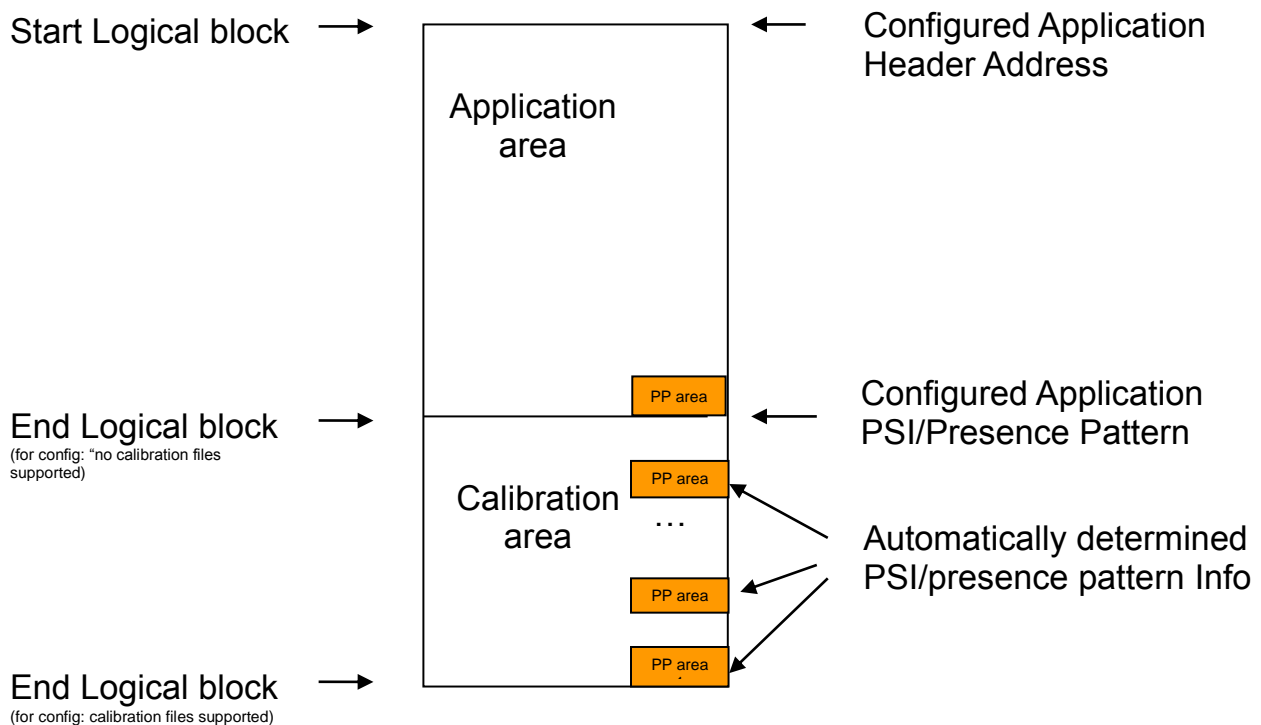


Figure 3-14 Typical Logical Block partition

### 3.5.1 Device Types

The bootloader is capable of programming multiple non-volatile memory devices, such as Flash and EEPROM memory. GENy predefines one non-volatile memory type, Flash. If

<sup>2</sup> Remember: All calibration files are erased upon application download; these are hence not independently erasable.

your ECU supports additional devices, then they should be defined before defining the flash-block table. Devices are added in the FblDrvCan\_<XX> → Memory Configuration → Memory Device Table

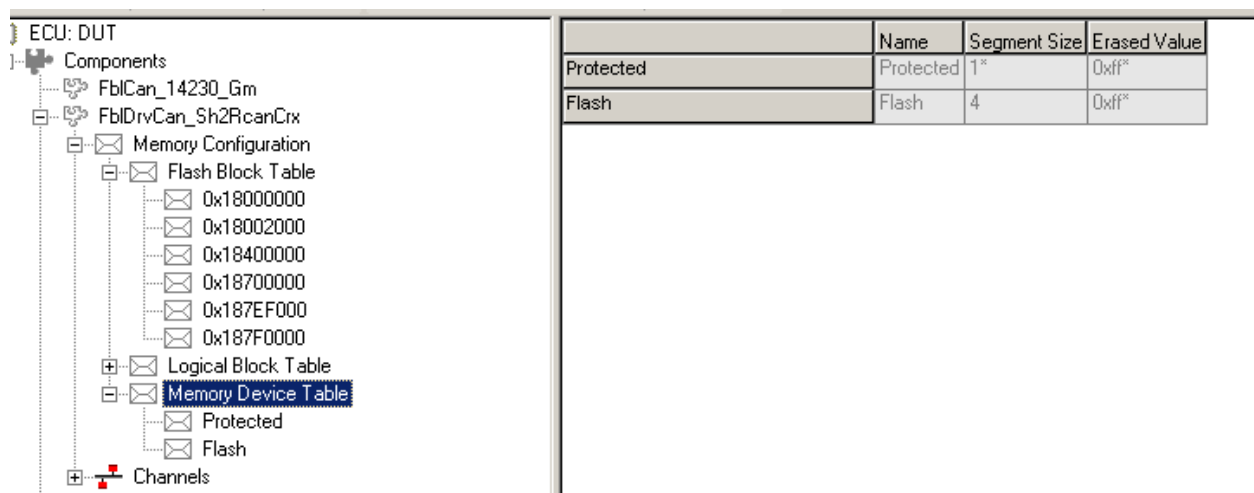


Figure 3-15 GENy Device Types

Two sub-fields will be available: **Device type** and **Segment Size**. For information regarding values for these fields, please refer to the hardware-specific documentation provided with your delivery (Technical Reference Hardware).

The **Device Type** field determines the name of the device, as it will appear in the flash-block table. The name is required to match the device-driver API. The API functions are declared in the device-driver I/O file (For example, fbl\_flio.h or eepIO.h). The file contains a prototypes section defining the API routines for the device. The function names will look like <prefix>Driver\_InitSync, <prefix>Driver\_DeinitSync, <prefix>Driver\_RReadSync, etc. Enter the function prefix into GENy exactly as typed in the header file.



**Note**

There is no need to add the Flash device to the device type table. This device-type is predefined by GENy.

The **Segment Size** field defines the minimum number of bytes that must be written to the device. You should enter the value appropriate for your hardware.

A completed example is shown below:

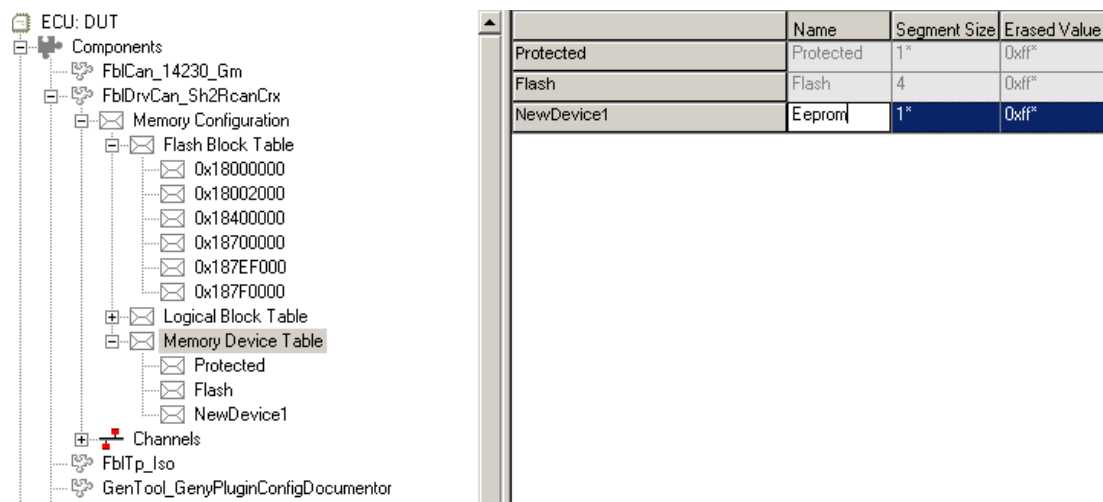


Figure 3-16 Example Device Type

### 3.5.2 Flash Block Definition

The Flash-Block table defines the regions of memory that may be written to by the bootloader. The table consists of 5 columns, and an arbitrary number of rows. Each row defines a block of memory on your ECU. An example is shown below:

Start Address	End Address	Memory Device	Description	Logical Block
0x18000000	0x18001fff	Protected	Renesas Loader Program	*
0x18002000	0x183ffff	Flash	Application	Application and calibration
0x18400000	0x186ffff	Flash	Application	Application and calibration
0x18700000	0x187efff	Flash	Application	Application and calibration
0x187EF000	0x187effff	Flash	4K Calibration area	Application and calibration
0x187F0000	0x187ffff	Protected	CANFbi Vector BootLoader	*

Figure 3-17 GENy Flash Block Table

The **StartAddress** field defines the starting address of a block of memory.

The **EndAddress** field defines the ending address of a block of memory.

The **Memory Device** field identifies the device-driver responsible for reading, writing, and erasing the block of memory. The reserved value **Protected** defines regions that cannot be accessed by the bootloader. At a minimum, you should define the blocks that are occupied by the bootloader as protected.

The **Description** field allows you to enter text that may indicate the purpose of the block. The contents of this field are not passed to the generated files.

There are some constraints on the address boundaries defined by the block table:

1. A block must begin and end on an erase-sector boundary. Hence, a block may not be smaller in size than one sector.
2. A block may span multiple sectors of the device. However, some devices define boundaries that constrain write commands (addresses that cannot be crossed in a single write command). A block definition may not cross such boundaries.

3. If Calibration modules are to be downloaded, you must be careful to partition the blocks such that the calibration modules do not occupy any block occupied by the Operating Software.

The **Logical Block** field associates the FlashBlock to a configured Logical Block (“Logical Block Table” element). Be sure to add all Flashblocks you want to program for a given set of Application + calibration files to one single Logical Block as shown above in Figure 3-17

GENy Flash Block Table

### 3.5.3 Logical Block Definition

At least one logical block is required to describe the programmable space of the main application and all of its calibrations.



#### Note

The logical blocks represent the Application Space and Calibration Space parameters of the Boot Info Block.

	Name	Block Index	Disposability	Start Address	End Address
Application and Calibration Area1	Application and Calibration Area1	0x1*	mandatory <input type="text"/>	0xc000	0x807fff

Header Address	Presence Pattern Address	Verification RAM	Verification ROM	Description
0x0*	0x0*	FblHdrPipelinedVerifyIntegrity*	FblHdrVerifyIntegrity	*

Figure 3-18 GENy Logical Block Table

Logical Block Configuration	
Name	Arbitrary name describing what the logical block represents. This is not generated into source code.
Block Index	Index of the logical block. Must be equivalent to the partition ID of the operating software that it represents (i.e. 0x1 for main application, 0x11 for second application, 0x21 for third application, 0x31 for fourth application).
Disposability	This field is generated to FblLogicalBlockTable but currently not used. It might be used in User callbacks in a Multi Application use case.
Start Address	Start address of logical block. Inherited from the flash block table configuration.
End Address	End address of the logical block. Inherited from the flash block table configuration.
Header Address	Address of the plain header of the application module that uses this logical block. This must be within the address region of the logical block. This value is accessed by the Fbl

Logical Block Configuration	
	through ApplFblGetModuleHeaderAddress.
Presence Pattern Address	Start address of the presence pattern (PSI) location. This must be 2 times the flash segment size less than the end address of any flash block (check 3.5.3.1). This value is accessed by the software through ApplFblGetBaseModulePPRegion, which verifies the above restriction in Project state Integration
Verification RAM	Verification function to verify the message digest. Normally this should not be changed. This should only be changed in case verification needs to be done on an external device (e.g. second microprocessor connected over SPI). In this case contact Vector.
Verification ROM	Verification to verify the integrity word (if enabled). Normally this should not be changed. This should only be changed in case verification needs to be done on an external device (e.g. second microprocessor connected over SPI). In this case contact Vector.

Table 3-2 GENy configuration of the Logical Block Table

Additional Logical Blocks need only be configured for Multi-processor configurations (compare chapter 8.2 for how to add Logical block table entries).

Upon module download the bootloader will check the Logical block table defined region against the addresses found in the header. ApplFblGetModuleHeaderAddress() returns the Module Header address information. Per default this information is taken from the GENy configuration, this way the callback usually does not need to be touched.

### 3.5.3.1 Correct Presence Pattern Addresses

This illustration shall help to understand how you need to configure the presence pattern address for your application (calibration partition patterns are not to be configured).



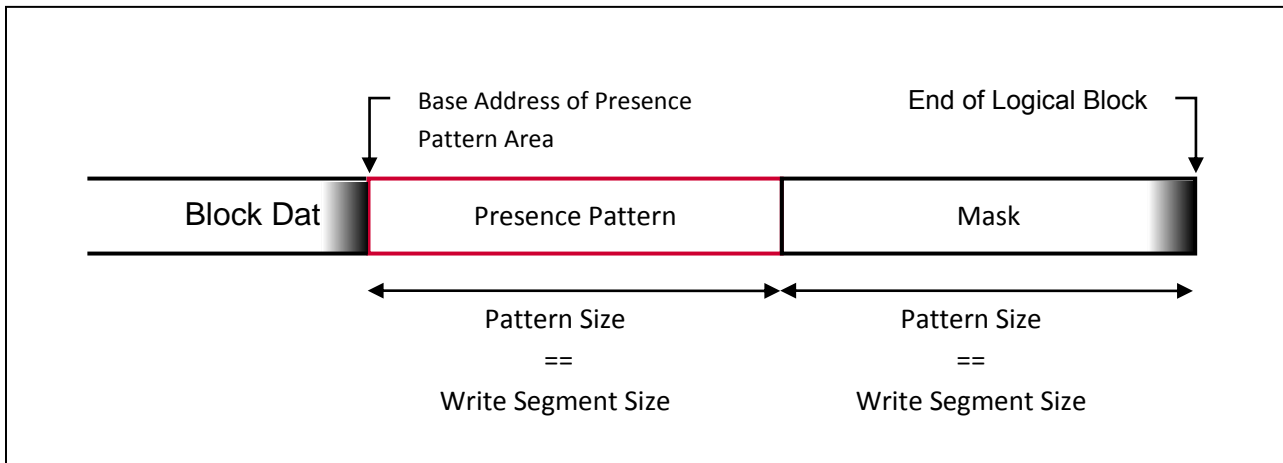


Figure 3-19 Presence Pattern Address configuration

### 3.6 Mandatory Delivery Preconfig

A user config file is required for this release. CanId related items are only required if the provided configuration tool is GENy. The file MandatoryDeliveryPreconfig.cfg is located in the delivery under Demo/DemoFbl/Config. This file need to be included in the GENy configuration as a user config file (see 4.4.1). This file must be configured manually using a source editor.

The following settings must be configured, e.g. using a user config file:

Macro	Description
FBL_CAN_TXID	29bit Tx Id. Use the macro MK_EXTID to form it. Configure it without target address byte (will be set in Com Wrapper). Depending on the kind of the ECU this will be 0x14DA00XX/0x18DA00XX (OBD), where XX is the Ecu node address.
FBL_CAN_RXID	Physical 11 bit Rx Id only used in Fbl, should be 0x6XX, where XX is the Ecu node address.
FBL_CAN_PHYS_CODE	Defines the fix defined bits for the physical 29 bit Rx message. Depending on the kind of the ECU this will be 0x14DAXX00/0x18DAXX00 (OBD), where XX is the Ecu node address.
FBL_CAN_FUNC_CODE	Defines the fix defined bits for the funtional 29 bit Rx message. Depending on the kind of the ECU this will be 0x10DBXX00/0x18DBXX00 (OBD), where XX is the Ecu node address.
FBL_CAN_PHYS_MASK	Defines the bit positions which are left open in the hardware filter. Default is 0x000000FFu (Tester Ids 0-FF allowed by hardware filter). Software filtering can restrict allowed tester further in ApplFblCheckTesterSourceAddr()
FBL_CAN_FUNC_MASK	Defines the bit positions which are left open in the hardware filter. Default is 0x000000FFu

Macro	Description
	(Tester Ids 0-FF allowed by hardware filter). Software filtering can restrict allowed tester further in ApplFblCheckTesterSourceAddr()
FBL_NBID_MEMORY_BASE	See 3.7.1
FBL_NBID_TOTAL_MEMORY_LEN	See 3.7.1

Table 3-3 Mandatory Delivery Preconfig


**Caution**

The FBL\_TEST\_.. macros below are for test purposes only. Remove them for production.

Macro	Description
FBL_TEST_SBA_TICKET	When this is defined the bootloader will write SBA ticket from flash (sbaBlk0) to chosen storage location on startup. Need to be disabled in production state (Bootloader ignores it in production)
FBL_TEST_ECU_ID	When this is defined the ECU ID stored in the bootloader header will be copied to chosen storage location on startup. Need to be disabled in production state (Bootloader ignores it in production)
FBL_TEST_KEY_NBID	This allows to write different start values to key NBID for test/development purpose. When this is defined the bootloader will write 0x0000 key NBID per default on startup. This may be helpful, if NVM is not yet in place. Need to be disabled in production state (Bootloader ignores it in production).
FBL_TEST_APP_NBID	This allows to write different start values to app NBID for test/development purpose. When this is defined the bootloader will write 0x0000 app NBID into NVM on startup. This may be helpful, if NVM is not yet in place. Need to be disabled in production state (Bootloader ignores it in production)
FBL_ENABLE_VERIFY_INTEGRITY_WORD	Optional feature: Required for Integrity Word verification feature. This feature is intended for development to verify the Plain header integrity word. This is not required by GM. Note: configuring this will cause the Bootloader reading the programmed data

Macro	Description
	twice, therefore it is recommended only for development to verify header integrity word configuration.
FBL_HDR_DISABLE_BASIC_NVM_HANDLING	Allows to disable Basic NVM handling described in the following chapters. You should set this, if you plan to use a Fee / other NVM solution and not basic NVM.

Table 3-4 Mandatory Delivery Preconfig

### 3.7 Handling of NVM data

The bootloader accesses several non-volatile data elements, see the below table for details. There are different approaches to handle these elements. Some of the approaches may be used in mixed way:

NVM Element	Fbl access	Appl access	Purpose	Properties	Possible NVM solutions
SBAT (Signature Bypass Authorisation Ticket)	read (on init)	read/write	The SBAT can be programmed to ECU NVM via application WDBI in order to allow programming of non-authorized software via the Fbl. The (unchanged) ticket itself gives authorization to change one single and UNIQUE ECU with any application/cal download, which does not require valid signature or Hash. This way modifications on ECUs with activated security gets possible (e.g. for development, debugging, etc.)	-once successfully written (via WDBI), it shall be available permanently until overwritten/destroyed via WDBI (does not need to be persistent)	FEE, Eep Manager (EepM), EEPROM, Data Flash, Program Flash
App-NBID (Application Not Before Id)	read/write (during download)	<i>not used</i>	This bootloader stored element is read and compared to any newly downloaded application in order to avoid download of applications considered unsecure. The received value within a container needs to be greater or equal to the stored value. A successfully programmed container with a value greater than the currently stored will lead to updating the stored value.	- Possibility to update it at least 16 times (GB6002, Table 10: App SW Info) - value need to be persistent and always accessible. (GB6002, Table 10: App SW Info) - Should not be placed to unsecure memory ( e.g. external EEPROM )	FEE, EepM, (internal) Program Flash, (internal) EEPROM, Data Flash, Fbl Image*
Key-NBID (Key Not Before Id)	read/write (during download)	<i>not used</i>	This bootloader stored element is read and compared to any newly downloaded container in order to avoid download of containers created with a key considered unsecure. The received value within a container needs to be greater or equal to the stored value. A successfully programmed container with a value greater than the currently stored will lead to updating the stored value.	see App-NBID	see App-NBID
ECUID	read (init & download)	<i>read</i>	ECUID has to be unique per single ECU part. The bootloader reads the included ECUID of any downloaded module and SBAT and compares it to it first to 0 (addresses any ECU) and then if it is not 0 to its own unique ID (addresses only our ECU; typically for SBAT use case).	“Easy” use case as read-only value	Like SBAT

Table 3-5 GM NVM element overview with possible solutions

**Note**

Please communicate your desired NVM strategy with your DRE. Please communicate restrictions (e.g. restricted NBID updates through Basic NVM handling, repetitive signed application download through SBAT Ram storage) for acceptance of your DRE.

### 3.7.1 vFlashBasic NVM handling

Your standard delivery includes a module `fbl_nbid.c/h`, that allows non-volatile storage of NBID elements with restricted updates. This can be used to achieve an implementation that does not need any additional NVM manager like Fee. In order to achieve that an erased memory area need to be configured in protected memory, that allows for sufficient update times (typically 64 are guaranteed by the module). This area may be located in a sector partly used by the FBL or in a dedicated sector.

**Caution**

Gm specifies that a minimum of 16 reliable updated is sufficient for NBIDs. Please note that Gm considers it exceptional to not have unlimited update possibility.

**Strong recommendation is:**

If you decide to stick with basic NVM and get acceptance from your DRE, configure the NBID reserved area as large as possible to allow considerable more updates than minimum GM required of 16. This allows for more security related updates of Key and application.

The Formula to get number of possible updates per NBID element (assumption: `FBL_NBID_TOTAL_MEMORY_LEN` is multiple of `FBL_NBID_SEGMENT_SIZE`, otherwise the number can be 1 smaller)):

$$\#UPDATES = \frac{FBL\_NBID\_TOTAL\_MEMORY\_LEN}{(NBID\_ELEMENT\_COUNT * FBL\_NBID\_SEGMENT\_SIZE)}$$

Typically `NBID_ELEMENT_COUNT` is 2 (1 key-NBID + 1 app-NBID).

Configuration items required (preconfigured in Demo)

Configuration item	Description
<code>FBL_NBID_MEMORY_BASE</code>	Start of NBID reserved memory area

	(initially erased)
FBL_NBID_TOTAL_MEMORY_LEN	Length of NBID reserved memory area (initially erased)

Table 3-6 Mandatory configuration items for basic NVM handling. Configure them e.g. via user configuration file

Some optional configuration items exist that allows overwriting default configuration for more detailed configuration.

Configuration item	Description
FBL_NBID_APP_COUNT (1-4, default FBL_MTAB_NO_OF_BLOCKS)	<p>Number of application modules for which the module will have to handle NBIDs.</p> <p>FBL_NBID_APP_COUNT usually should be equal to FBL_MTAB_NO_OF_BLOCKS. Reconfigure to optimize memory usage in case you have non application related Logical Block Table entries (in this case the default configures a larger value than is optimal).</p>
FBL_NBID_MIN_UPDATE_COUNT (16- 65535 default 64 / 0x40)	<p>Allows overwriting the desired minimum update count for NBIDs. This cannot be reduced below the GM required 16.</p> <p>Note that the real possible update count is calculated automatically from number of used NBID elements (FBL_NBID_ELEMENT_COUNT), the configured length (FBL_NBID_TOTAL_MEMORY_LEN) and FBL_NBID_SEGMENT_SIZE.</p> <p>The module will check that the real possible update count is always above the configured FBL_NBID_MIN_UPDATE_COUNT and will set a compile error if this is not possible.</p> <p>Also compare above Note box “Strong recommendation”.</p>
FblNbid_RWriteSync (default FlashDriver_RWriteSync) FblNbid_RReadSync (default FlashDriver_RWriteSync) FBL_NBID_DELETED (default FBL_FLASH_DELETED) FBL_NBID_SEGMENT_SIZE (default FLASH_SEGMENT_SIZE)	(Re-)configure these elements to alternative HIS driver, if you plan to use a different driver than internal flash driver. The used HIS driver is defaulted to internal flash driver.

Table 3-7 Optional configuration items for basic NVM handling. Configure them e.g. via user configuration file

### 3.7.1.1 SBAT in basic NNVM handling configuration

Because SBAT storage is not required to be persistent, rather simple approaches to handle SBAT are possible, e.g. by passing SBAT from application to bootloader on reprogramming event.

To allow passing, the bootloader needs to know where to access application provided SBAT. E.g. CanInitTable.pSbat pointer can be used to provide SBAT storage location from application to bootloader, the bootloader can use this address to copy SBAT to parsing target buffer or write it to Flash. Alternatively application can already copy SBAT to Fbl SBAT target buffer. The Fbl SBAT parsing target buffer is configured by SBA\_TICKET\_PARSE\_BUFFER in Fbl (defaulted to FblRamHeader).

### > Pass SBAT to FBL in Ram and program it to reserved sector

Reserved sector need to be configured to protected.

Within *ApplFblStartup()* each time a different SBAT is received/passed in from application on reprogramming event (do a mem compare to detect the difference) erase reserved sector and program new SBAT within *ApplFblNVMMWriteSBATicket()*

```
IF ((kStartupPreInit == initposition)) && (0 != (GetFblMode() & START_FROM_APPL)) {  
    IF (compare(oldsbat, newsbat) != equal) {  
        ApplFblNVMMWriteSBATicket();  
    }  
}
```

### > Pass SBAT to FBL in Ram only

Note that if it is only hold in RAM, a sequence of signed application download + Write SBAT will need to be repeated whenever an unsigned application download shall happen and the SBAT is no more available to the FBL. Storage to some dedicated RAM buffer may enable you to hold the SBAT over simple software reset.

FblRamHeader is dedicated to SBAT only if no data processing happens during download (e.g. when decompressing), therefore you may consider to only download uncompressed when doing downloads using SBAT.

## 3.7.2 Fee integration to FBL

This is the typical use case to handle NVM in the bootloader. The application note AN-ISC-8-1173 [9] describes the necessary steps to integrate the Vector Fee to Fbl.

You need to configure FBL\_HDR\_DISABLE\_BASIC\_NVM\_HANDLING in order to use alternative NVM configuration (compare 3.6).

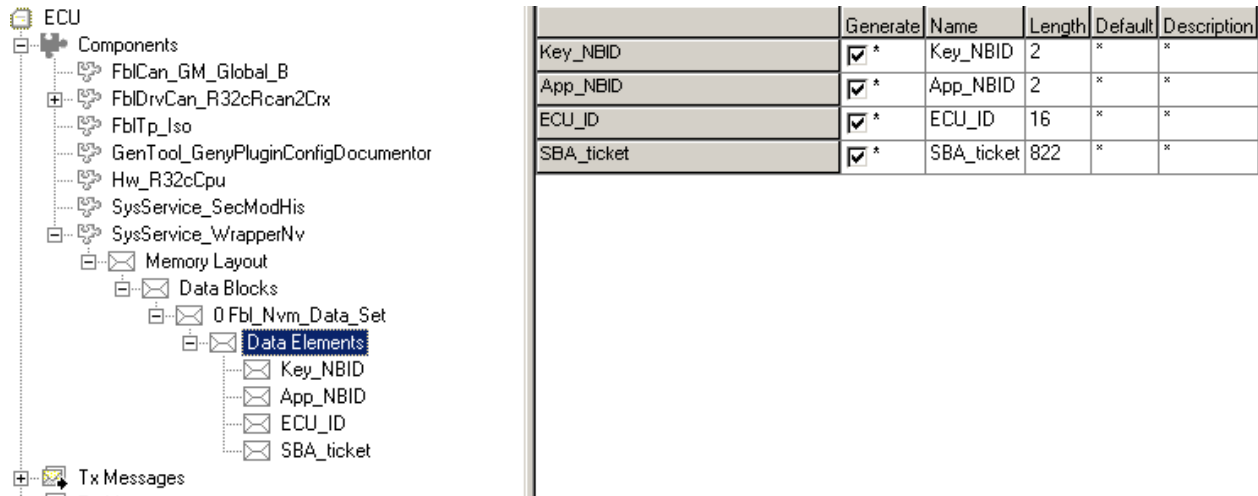
## 3.7.3 Alternative NV-Wrapper Configuration

For Basic NVM and Fee integration approaches no NV-Wrapper configuration is required. The bootloader may support NV-Wrapper Configuration in future for these approaches.

For less typical configuration using real EEPROM or Eepm (Attention: no external device for NBIDs! This allows for external manipulation of security relevant data) the NV-Wrapper is provided as an abstraction layer for non-volatile memory access. This permits the usage of different types of NV-memory with the same interface. The configuration of the NV-information handling is supported by GENy. This section describes the specific settings for the GM Flash-Bootloader. For detailed information, please see [7].

The NV-memory elements required per GB6002 are already preconfigured. What remains to be done is determine the address of the information block if an address-based NV-

memory driver like an EEPROM-driver is used. If a handle-based driver like the EEPROM-Manager or FEE is used, the first handle has to be specified.

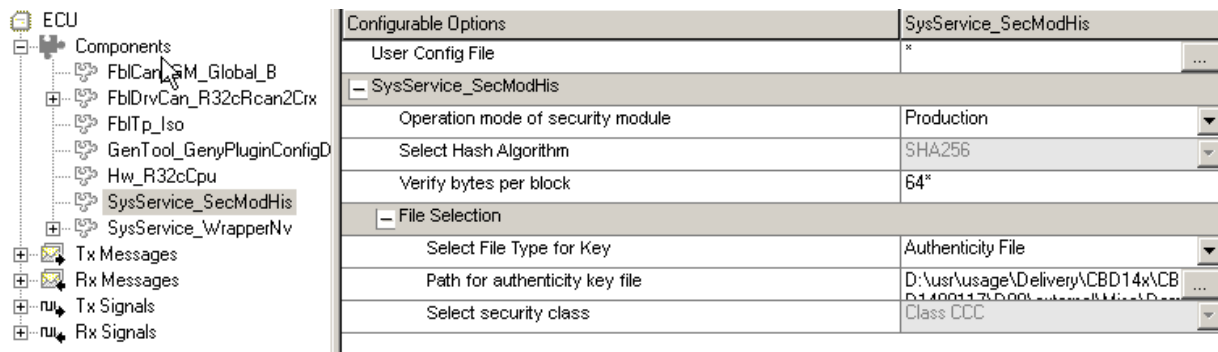


	Generate	Name	Length	Default	Description
Key_NBID	<input checked="" type="checkbox"/>	Key_NBID	2	*	*
App_NBID	<input checked="" type="checkbox"/>	App_NBID	2	*	*
ECU_ID	<input checked="" type="checkbox"/>	ECU_ID	16	*	*
SBA_ticket	<input checked="" type="checkbox"/>	SBA_ticket	822	*	*

Figure 3-20 SysService\_WrapperNv configuration in GENy

You need to configure FBL\_HDR\_DISABLE\_BASIC\_NVM\_HANDLING in order to use alternative NVM configuration (compare 3.6).

### 3.8 typical use case to handle Security Module configuration



Configurable Options		SysService_SecModHis
User Config File		*
SysService_SecModHis		
Operation mode of security module		Production
Select Hash Algorithm		SHA256
Verify bytes per block		64*
File Selection		
Select File Type for Key		Authenticity File
Path for authenticity key file		D:\usr\usage\Delivery\CB014x\CB...
Select security class		Class CCC

Figure 3-21 SysService\_SecModHis configuration

Configurable Parameter	Default	Description
User Config file	empty	User preconfig for security module
Operation Mode	Production	Operation mode Production The mode of the security component is set to
Verify bytes per block	64	Number of bytes that are reserved by the security module for verification. This value determines the number of bytes that are verified in one block operation.
Select file type for key	Authenticity File	Always keep "Authenticity File" format. This allows to read HIS/ASN.1-format keys provided by GM or our Dummy key (as



Configurable Parameter	Default	Description
		configured in our demo)
Path for authenticity key file		Configure Public key information provided by GM (.der) for production, or alternatively Vector dummy key to use during development.

Table 3-8 Security Module configuration



### Caution

It is strongly recommended to use the exact same compiler settings for the application and the Bootloader.

This especially applies to the security module of the FBL, which is delivered as object code; e.g. you can use the Security module through the FblHeader interface in your application like shown in \_appParseSba.c/.h. Different compiler option usage may lead to incompatibilities.

## 3.8.1 Running the Generator

When you have finished your configuration selections, you need to run the generator to produce the files needed to compile the FBL. To generate the files, click on the lightning-bolt button on the toolbar, or select **Generate System** from the Configuration menu. The following table describes the contents of the generated files:

File Name	Description
fbl_apfb.c/.h	Contains the Flash-Block table. If multiple devices are supported, this file also contains a table mapping the block entries to the appropriate device-driver API functions.
Fbl_mtab.c/.h	Logical Block Table definition file
fbl_cfg.h	Contains macro definitions used to configure the bootloader. For the most part, the file defines switches in the form of FBL_ENABLE_<feature> or FBL_DISABLE_<feature>.
V_cfg.h	Contains macro definitions specific to your hardware.
V_inc.h	Includes the generated headers, so that they may be obtained from a single source. This file is not required to compile the FBL.
V_par.c, v_par.h	Contains information about your license. These files are not required to compile the FBL.
WrapNv_cfg	Contains macros for accessing non-volatile data.

Table 3-9 Generated File contents

## 4 Adapting the FBL Implementation

The bootloader includes a number of files that you must review and adapt to fit the needs of your ECU and application. All files found in the FBL\\_Template folder of your delivery may require customization. You should copy all files from FBL\\_Template to your project directory, rename them (removing the leading underscore character), and adapt them for your application. The FBL demo included with your delivery contains examples of these files (in the \_Demo\DemoFbl\Appl\Source and \_Demo\DemoFbl\Appl\Include folders). A brief description of the files is shown below:

File Name	Description
_fbl_ap.c, _fbl_ap.h	Contains hardware-specific, Input/Output, and miscellaneous callback functions.
_fbl_apdi.c, _fbl_apdi.h	Contains callbacks for diagnostic service requests.
_fbl_apnv.c, _fbl_apnv.h	Contains non-volatile operation callbacks. These are used to handle the module (presence-pattern) validation.
_fbl_apwd.c, _fbl_apwd.h	Contains watch-dog callback functions
_fbl_applvect.c	Contains application-vector-table used by FBL. This file should be adapted if Sleep-Mode is enabled (The interrupt vector used to wake-up the ECU must be defined).
_fbl_inc.h	Contains references to all include files used by the FBL.

Table 4-1 User-Modifiable file contents

Special attention must be paid in all of the callback functions. If a routine (such as an EEPROM function) takes a long time to run, it is possible that the ECU's watchdog timer will force the ECU to reset. You should also be careful when using library routines such as `memcpy()`.

To avoid a reset, you must call `FblLookForWatchdog()` at least once per millisecond. More often is desirable. Failure to meet this requirement may lead to unexpected resets while programming the ECU.

For callback functions that are invoked in response to a diagnostics request, you may also need to determine if you need to send a Response-Pending response message. **ECU Timing Parameter P2<sub>CE</sub>** (reference [2]) requires that a response be sent by the ECU within 50 ms (configurable via preconfig). If your callback implementation may execute longer than this period, you should call the function `FblRealTimeSupport()`. This may be used in place of calls to `FblLookForWatchdog()`, and should be called at least once per millisecond. The function will send a response-pending message at the appropriate interval.

## 4.1 Hardware, Input/Output and miscellaneous Callbacks

The file `fbl_ap.c` contains functions to handle hardware-specific operations, such as input/output control, and several miscellaneous callback functions. A complete list of the functions in this component is shown below:

ApplFblCanBusOff	ApplFblCanParamInit *	ApplFblCanWakeUp
ApplFblCheckProgConditions	ApplFblFatalError	ApplFblCheckDataFormatIdentifier
ApplFblEnterStopMode	ApplFblInit *	ApplFblStartApplication
ApplFblInitErrStatus	ApplTrcvrSleepMode	ApplFblRamIntegrityCheck
ApplFblReset	ApplFblResetVfp *	ApplFblRomIntegrityCheck
ApplFblSetVfp *	ApplFblSleepModeAllowed	ApplFblStartup *
ApplFblTask *	ApplFblTpErrorInd	ApplFblInitDataProcessing
ApplFblCheckConditions	ApplTrcvrNormalMode *	ApplFblDataProcessing
ApplFblDeinitDataProcessing		

Table 4-2 Miscellaneous Callback functions

\* These routines are also described in reference [3].

The following pages describe each function. When building your bootloader, you should review the implementation of each function, and adapt them to conform with your ECUs requirements.

### 4.1.1 ApplFblCanBusOff

Prototype	
void <b>ApplFblCanBusOff</b> ( void )	
Parameter	
-	-
Return code	
-	-
Functional Description	
The FBL internally checks for communication errors via <code>FblCanErrorTask()</code> in the main loop. This function is called from <code>FblCanErrorTask()</code> while the CAN controller is in a bus-off state. This is a notification that the ECU cannot transmit messages. No action is required in order to recover.	
Particularities and Limitations	
> None	

Table 4-3 ApplFblCanBusOff

### 4.1.2 ApplFblCanParamInit

Prototype	
void <b>ApplFblCanParamInit</b> ( void )	
Parameter	
-	-
Return code	
-	-
Functional Description	
<p>This function is used if the configuration defines multiple-identities (MIM) – select nodes DUT and DUT1 from dummy dbc. The routine is called as part of the FBL initialization sequence when started from both reset and from the Operating Software.</p> <p>The purpose of the function is to allow the CAN-ID to be set based upon runtime conditions instead of fixed at compile-time.</p>	
Particularities and Limitations	
> -	

Table 4-4 ApplFblCanParamInit

### 4.1.3 ApplFblCanWakeUp

Prototype	
void <b>ApplFblCanWakeUp</b> ( void )	
Parameter	
-	-
Return code	
-	-
Functional Description	
<p>This function is used only if the configuration selects “Enable sleep mode”. The function is called from the ECU’s wake-up interrupt service routine (<code>FblCanWakeUpInterrupt</code>). The implementation should perform any necessary tasks (such as I/O port initialization, timer, watchdog, or phase-lock-loop synchronization) needed to restore the hardware to a normally-running state.</p> <p>If sleep-mode is disabled, this function is not called by the FBL. You may, however, implement your own wake-up interrupt-service-routine (referenced from the application-vector-table) that invokes this function.</p>	
Particularities and Limitations	
<p>&gt; Keep in mind that this function is called in the interrupt-context of your ECU. Special rules apply to such routines, for example: Any external variables altered by this function should be declared volatile to insure data consistency.</p> <p>&gt; See also <code>ApplFblSleepModeAllowed()</code> and <code>ApplFblEnterStopMode()</code></p>	

Table 4-5 ApplFblCanWakeUp

#### 4.1.4 ApplFblCheckProgConditions

Prototype	
<code>tFblResult ApplFblCheckProgConditions ( void )</code>	
Parameter	
-	-
Return code	
kFblOk	Indicates that conditions are appropriate for (re)programming the ECU.
kFblFailed	Indicates that conditions are not correct for programming the ECU.
Functional Description	
<p>The implementation of this function should determine whether or not conditions are correct to enter the programming session.</p> <p>The function is called from Session Control Programming Session main handler</p>	
Particularities and Limitations	
> None	

Table 4-6 ApplFblCheckProgConditions

#### 4.1.5 ApplFblEnterStopMode

Prototype	
<code>void ApplFblEnterStopMode ( void )</code>	
Parameter	
-	-
Return code	
-	-
Functional Description	
<p>This function is called by the FBL when it is time to enter the “low power” mode of the ECU. This occurs if there has been no activity on the CAN bus for 60 seconds. The function should be modified to enter a sleep or stop mode, leave it empty if no low power mode handling is required.</p> <p>Care should be taken when enabling interrupts (to allow wakeup), since an interrupt may be pending when interrupts are enabled. The hardware must be in a valid state before the halt or stop instruction is executed.</p> <p>The code following the halt instruction should disable interrupts before returning control to the FBL.</p>	
Particularities and Limitations	
> See also <code>ApplFblSleepModeAllowed()</code> and <code>ApplFblCanWakeUp()</code>	

Table 4-7 ApplFblEnterStopMode

#### 4.1.6 ApplFblInit

Prototype	
<code>void ApplFblInit ( void )</code>	

Parameter	
-	-
Return code	
-	-
Functional Description	
<p>This function is called from <code>main()</code> immediately after reset (It is also called when the FBL is started from the Operating Software, since the FBL is started via a reset).</p> <p>The function may be used to perform any hardware and I/O initialization. Also, any global variables used exclusively by the callback components should be initialized at this point.</p>	
Particularities and Limitations	
<ul style="list-style-type: none"> <li>&gt; For additional information, see the Flash Bootloader User Manual</li> <li>&gt; You may choose to start the ECU's watchdog timer in this routine. However, the FBL will not start the timer used to call the watchdog-trigger routine (<code>ApplFblWDTrigger()</code>) until much later in the FBL's startup. See also Section 4.4 and <code>ApplFblWDInit()</code>.</li> </ul>	

Table 4-8 ApplFblInit

#### 4.1.7 ApplFblInitErrStatus

Prototype	
void <b>ApplFblInitErrStatus</b> ( void )	
Parameter	
-	-
Return code	
-	-
Functional Description	
<p>This routine is called to initialize the global variables used to save the FBL state when an error occurs. The state may be retrieved by sending a Read-Data-By-Identifier request with a data-identifier of \$7F. See also section 8.3.</p>	

## Particularities and Limitations

The FBL error state is available only when the configuration selects Project State “Integration”.

The variables available for error-state storage are:

```
errStatFlashDrvVersion[]
errStatFlashDrvErrorCode
errStatErrorCode
errStatFblStates
errStatLastServiceId
errStatTpError
errStatFileName
errStatLineNumber
errStatDescriptor
errStatHaveDriver
errStatAddress
```

The following macros/functions are used to set the error-state variables:

```
FblErrStatSetSid( id )
FblErrStatSetState( state )
FblErrStatSetFlashDrvError( error )
FblErrStatSetError( error )
FblErrDebugStatus( error )
FblErrDebugDriver( addr, drvError )
```

The GM FBL does not at this time save or use information in `errStatFlashDrvVersion`, or `errStatDescriptor`. These are reserved for future use.

The variables `errStatFlashDrvErrorCode` and `errStatFblStates` are updated as needed by the FBL, but cannot be retrieved over the CAN bus. They are intended to be accessed only during FBL development.

Table 4-9 ApplFblInitErrStatus

### 4.1.8 ApplFblRamIntegrityCheck

#### Prototype

```
void ApplFblInitErrStatus( void )
```

#### Parameter

-	-
---	---

#### Return code

-	-
---	---

#### Functional Description

This routine tests that there are no errors in Random Access Memory (RAM). By default, the function is called from `ApplFblStartup()`. This routine should set or clear the flag to indicate that a RAM fault has occurred.

### Particularities and Limitations

- > This function is used only if the configuration selects “Enable RAM Integrity Check”.
- > The default implementation verifies that every bit of every byte in RAM may be set and cleared. You are required to obtain approval from GM to use this algorithm. See “RAM Integrity Check”.
- > The default implementation defines a table named `kRamTable`. You must initialize this structure with the starting and ending address of each address region before compiling the FBL. The result of the RAM test is stored in the `kProgrammedStateRamError` bit contained in the global variable `fblProgrammedState`.

Table 4-10 ApplFblRamIntegrityCheck

## 4.1.9 ApplFblReset

### Prototype

```
void ApplFblReset( void )
```

### Parameter

-	-
---	---

### Return code

-	-
---	---

### Functional Description

This function is responsible for resetting the ECU. For example, you may execute a restart instruction (if available), jump to the reset vector, or use the watchdog. The choice is up to you, and depends on your ECU hardware.

This function is called when it is necessary to reset the ECU. For example, when a Session Control Default Session request is received.

### Particularities and Limitations

- > Jumping directly to the ECU's reset vector should be considered a last-choice option. Some ECUs contain registers that may be accessed only once – it is possible that the FBL will be unable to re-initialize them when it is restarted via a jump to the reset vector.

Table 4-11 ApplFblReset

## 4.1.10 ApplFblResetVfp

### Prototype

```
void ApplFblResetVfp( void )
```

### Parameter

-	-
---	---

### Return code

-	-
---	---



Functional Description
<p>The purpose of this routine is to turn off the power supply required to program non-volatile memory. If your ECU does not require an external power source to erase and program memory, then this function may be left empty.</p> <p>The function is called during initialization of the FBL, and when Session Control Default Session is received.</p>
Particularities and Limitations
<p>&gt; See also <code>ApplFblSetVfp()</code>.</p>

Table 4-12 ApplFblResetVfp

#### 4.1.11 ApplFblRomIntegrityCheck

Prototype	
void <b>ApplFblRomIntegrityCheck</b> ( void )	
Parameter	
-	-
Return code	
-	-
Functional Description	
<p>This routine calculates the checksum of the address-regions occupied by the bootloader, and compares the result to the Checksum (CS) field of the FBL’s File-Header. By default, the function is called from <code>ApplFblStartup()</code>. This routine should set or clear the flag to indicate that a ROM fault has occurred.</p>	
Particularities and Limitations	
<ul style="list-style-type: none"><li>&gt; This function is used only if the configuration selects “Enable ROM Integrity Check”.</li><li>&gt; The default implementation stores the result of the ROM test in the <code>kProgrammedStateRomError</code> bit contained in the global variable <code>fblProgrammedState</code>.</li></ul>	

Table 4-13 ApplFblRomIntegrityCheck

#### 4.1.12 ApplFblSetVfp

Prototype	
void <b>ApplFblSetVfp</b> ( void )	
Parameter	
-	-
Return code	
-	-

Functional Description
<p>The purpose of this routine is to turn on the power supply required to program non-volatile memory. If your ECU does not require an external power source to erase and program memory, then this function may be left empty.</p> <p>The function is called when the FBL is started by the Operating Software, and when a Programming-Mode (service \$A5) requesting Enable-Programming-Mode (\$03) is received.</p>
Particularities and Limitations
<p>&gt; See also <code>ApplFblResetVfp()</code>.</p>

Table 4-14 ApplFblSetVfp

#### 4.1.13 ApplFblSleepModeAllowed

Prototype	
tFblResult <b>ApplFblSleepModeAllowed</b> ( void )	
Parameter	
-	-
Return code	
kFblOk	Indicates that conditions are correct to go to sleep.
kFblFailed	Indicates that FBL should not go to sleep.
Functional Description	
This function should determine if it is OK for the ECU to go to sleep.	
Particularities and Limitations	
<ul style="list-style-type: none"><li>&gt; See also ApplFblEnterStopMode() and ApplFblCanWakeUp().</li><li>&gt; In some ECUs, an interrupt vector is required to service the wake-up event. A vector pointing to the appropriate interrupt-service-routine (ISR) in the FBL can be defined in the Application Vector Table (if there is no vector base register). Since the Application Vector Table can be erased and replaced by the Operating Software, the implementation may call blCheckBootVectTablesValid(), to make sure that the table in flash is the “dummy” table compiled into the FBL. This ensures that the vector points to the service-routine in the FBL instead of a service-routine in the Operating Software. If this table is not present, then the ECU is not allowed to go to sleep.</li></ul>	

Table 4-15 ApplFblSleepModeAllowed

#### 4.1.14 ApplFblStartup

Prototype	
void <b>ApplFblStartup</b> ( vuInt8 initposition )	
Parameter	
initposition	Indicates that the function is being called before or after hardware and state initialization. Possible values: kStartupPreInit – Indicates function call before initialization. kStartupPostInit – Indicates function call after initialization.
Return code	
-	-

### Functional Description

This function is called twice during the bootloader startup; See section 2.3.1. The pre-init call occurs after the FBL has determined that the FBL is being started by the Operating Software, or that the Operating Software is not present. The post-init call occurs immediately before the main loop (`FblRepeat()`) is started. You may perform any required hardware and software initialization before and after the CAN control and timer initialization is completed by `main()`.

The default implementation will run the RAM and ROM integrity checks in the post-initialization call, if they are enabled by the FBL configuration.

### Particularities and Limitations

> See also the Flash Bootloader User Manual.

Table 4-16 ApplFblStartup

## 4.1.15 ApplFblTask

### Prototype

```
void ApplFblTask( void )
```

### Parameter

-	-
---	---

### Return code

-	-
---	---

### Functional Description

The purpose of this function is to perform any periodic background tasks.

The FBL invokes this function on a regular periodic basis of 1ms (changes to this may be only on project specific basis).

Only a limited number of tasks are performed during the start delay period if `FBL_ENABLE_STAY_IN_BOOT` is defined. During the delay period, the FBL does not invoke `ApplFblTask`.

Since the timing of all events in the FBL are determined by the ability of the ECU to complete the main loop in less than the period defined by `FBL_REPEAT_CALL_CYCLE`, all code added to `ApplFblTask` must be kept as short as possible. After adding code to this function, you should verify that the time required to execute the main task loop (found in `FblRepeat`), is always less than the call cycle period.

### Particularities and Limitations

- > This function is called only if the configuration selects "Enable ApplTask".
- > This function is only called while the FBL is idling. Calling intervals exceeding the `TpCallCycle` can occur while the FBL handles diagnostic service requests. This normally occurs while erasing and writing non-volatile memory.
- > If you need to call your functionality also during service execution or flashing consider placing it to Ram memory and call it from `ApplFblWDTrigger()`. Again execution time need to be very short.

Table 4-17 ApplFblTask

## 4.1.16 ApplFblTpErrorInd

### Prototype

```
void ApplFblTpErrorInd( uint8 tpErrorCode )
```

Parameter	
tpErrorCode	<p>Indicates the error that was detected by the TP Layer. Possible values are (see also fbl_tp.h):</p> <p><code>kTpErrRxNotIdle</code> A single-frame or first-frame message was received while processing a previous request (i.e. the receive buffer is locked).</p> <p><code>kTpErrRxSFDL</code> A single-frame message was received containing an illegal value in the Data-Length (DL) field of the Protocol-Control-Information (PCI) byte.</p> <p><code>kTpErrRxCFNotExpected</code> A consecutive-frame message was received unexpectedly. CF messages must be preceded by a first-frame message.</p> <p><code>kTpErrRxWrongSN</code> A consecutive-frame message was received containing an illegal or unexpected value in the Sequence-Number (SN) field of the Protocol-Control-Information (PCI) byte.</p> <p><code>kTpErrRxTimeout</code> Too much time elapsed while waiting for a consecutive-frame message to arrive.</p>
Return code	
-	-
Functional Description	
<p>This function is called from the Transport-Protocol layer to indicate that an error has occurred. The cause of the error is supplied in the <code>tpErrorCode</code> argument.</p> <p>The implementation may choose to ignore the error; record the error, or respond to the error.</p> <p>The default implementation saves the error code in the global variable <code>errStatTpError</code>, and then sends a negative response indicating that a general programming error has occurred.</p>	
Particularities and Limitations	
<p>&gt; The TP Layer actually calls <code>TpErrorIndication()</code>. This is a function-like macro defined in <code>ftp_cfg.h</code> that redirects the call to <code>ApplFblTpErrorInd()</code>. The default implementation is to ignore the error.</p> <p>You must update the macro definition in order to call <code>ApplFblTpErrorInd()</code> (which by default will record the error and send a negative-response indicating a General-Programming-Failure).</p>	

Table 4-18 ApplFblTpErrorInd

#### 4.1.17 ApplTrcvrHighSpeedMode

Prototype	
<pre>tFblResult ApplFblCheckConditions(vuint8* pbDiagData, tTpDataType diagReqDataLen)</pre>	
Parameter	
pbDiagData	Pointer to diag service data (after SID!)
diagReqDataLen	Service data length (without SID!)
Return code	
kFblOk	Conditions OK

kFblFailed	Conditions not OK
<b>Functional Description</b>	
<p>This function is called prior to any service execution and allows to perform user specific checks and prohibit service execution and return negative response codes if required.</p> <p>Check DiagGetRequestSId() for current service requested.</p> <p>This can e.g. be used to implement DiagNRCVoltageTooHigh/DiagNRCVoltageTooLow handling on \$36.</p>	
<b>Particularities and Limitations</b>	
<p>&gt; This function is used only if the configuration selects "Enable High-Speed". This is required if your ECU is communicating on the single-wire CAN "Body Bus".</p>	

Table 4-19 ApplTrcvrHighSpeedMode

### 4.1.18 ApplTrcvrNormalMode

<b>Prototype</b>	
void <b>ApplTrcvrNormalMode</b> ( void )	
<b>Parameter</b>	
-	-
<b>Return code</b>	
-	-
<b>Functional Description</b>	
<p>This function is used to configure your CAN bus transceiver for normal CAN communications. You must implement this routine to perform the necessary Input/Output operations to control the transceiver state.</p> <p>This function is called when the FBL is started (either power-on or via Operating Software), when waking-up (if sleep-mode has been enabled).</p>	
<b>Particularities and Limitations</b>	
<p>&gt; None</p>	

Table 4-20 ApplTrcvrNormalMode

### 4.1.19 ApplTrcvrSleepMode

<b>Prototype</b>	
void <b>ApplTrcvrSleepMode</b> ( void )	
<b>Parameter</b>	
-	-
<b>Return code</b>	
-	-

Functional Description
<p>This function is used to configure CAN bus transceiver for low-power (sleep) operation. You must implement this routine to perform the necessary Input/Output operations to control the transceiver state.</p> <p>This function is called from the main loop after the FBL has determined that it is ok to go to sleep (see <code>ApplFblSleepModeAllowed()</code>). Upon waking up, the FBL will call <code>ApplTrcvrNormalMode()</code> to allow normal communications.</p>
Particularities and Limitations
> None

Table 4-21 ApplTrcvrSleepMode

#### 4.1.20 ApplFblStartApplication

Prototype
<code>void ApplFblStartApplication ( void )</code>
Parameter
-
Return code
-
Functional Description
<p>The function is called to start application. It contains an implementation we used for Demo purpose. You may adapt this function if your application needs to be started differently.</p>
Particularities and Limitations
> None

Table 4-22 ApplFblStartApplication

#### 4.1.21 ApplFblFatalError

Prototype
<code>void ApplFblFatalError( FBL_DECL_ASSERT_EXTENDED_INFO(vuint8 errorCode) )</code>
Parameter
-
Return code
-
Functional Description
<p>The function is only available if Project state is "Integration" it is called if an assertion placed in the code is found to be invalid (assertXX-maros found in code). Define an action that makes the wrong condition visible to you (e.g. Led blinking). Per default Fbl enters a while(1) loop.</p>
Particularities and Limitations
> You may change in your debugger the used while condition variable to leave while loop and check where the function has been called from (you also may see by checking errorCode value)

Table 4-23 ApplFblFatalError

### 4.1.22 ApplFblCheckDataFormatIdentifier

Prototype	
tFblResult ApplFblCheckDataFormatIdentifier(vuint8 formatId)	
Parameter	
formatId	Data format identifier from the requestDownload service.
Return code	
tFblResult	-
Functional Description	
<p>This function is called to check the data format identifier value.</p> <p>Data Processing interface function. This function is only required for certain configurations that have to be specifically ordered:</p> <ul style="list-style-type: none"> <li>&gt; Compression</li> <li>&gt; Encryption/decryption (currently no Use case)</li> </ul>	
Particularities and Limitations	
> None	

Table 4-24 ApplFblCheckDataFormatIdentifier

### 4.1.23 ApplFblInitDataProcessing

Prototype	
tFblResult ApplFblInitDataProcessing( tProcParam *procParam )	
Parameter	
tProcParam *procParam	-
Return code	
tFblResult	-
Functional Description	
<p>This function is called to initialize the application specific data processing function.</p> <p>Data Processing interface function. This function is only required for certain configurations that have to be specifically ordered:</p> <ul style="list-style-type: none"> <li>&gt; Compression</li> <li>&gt; Encryption/decryption (currently no Use case)</li> </ul>	
Particularities and Limitations	
> None	

Table 4-25 ApplFblInitDataProcessing

#### 4.1.24 ApplFblDataProcessing

Prototype	
<b>tFblResult ApplFblDataProcessing ( tProcParam *procParam )</b>	
Parameter	
tProcParam *procParam	-
Return code	
tFblResult	-
Functional Description	
Data processing function. This function is only required for certain configurations that have to be specifically ordered:	
<ul style="list-style-type: none"> <li>&gt; Compression</li> <li>&gt; Encryption/decryption (currently no Use case)</li> </ul>	
Particularities and Limitations	
<ul style="list-style-type: none"> <li>&gt; None</li> </ul>	

Table 4-26 ApplFblDataProcessing

#### 4.1.25 ApplFblDeinitDataProcessing

Prototype	
<b>tFblResult ApplFblDeinitDataProcessing ( tProcParam *procParam )</b>	
Parameter	
tProcParam *procParam	-
Return code	
tFblResult	-
Functional Description	
Data Processing deinitialization. This function is only required for certain configurations that have to be specifically ordered:	
<ul style="list-style-type: none"> <li>&gt; Compression</li> <li>&gt; Encryption/decryption (currently no Use case)</li> </ul>	
Particularities and Limitations	
<ul style="list-style-type: none"> <li>&gt; None</li> </ul>	

Table 4-27 ApplFblDeinitDataProcessing

## 4.2 Diagnostic Service Callbacks

The file fbl\_apdi.c contains all the routines used to handle diagnostic service requests. Each diagnostic service is described in detail in reference [1]. The complete list of routines in this component is shown below:



ApplDiagUserService	ApplDiagUserSubFunction
ApplFblReadDataByIdentifier	ApplFblRdbidProgrammedStateInd
ApplFblCheckTesterSourceAddr	

Table 4-28 Diagnostic Callback Functions

\* These routines are also described in reference [3].

### 4.2.1 ApplFblEnablePrgMode

Prototype	
void <b>ApplDiagUserService</b> (vuint8* pbDiagData, tTpDataType diagReqDataLen)	
Parameter	
pbDiagData	Pointer to diag service data (after SID!)
diagReqDataLen	Service data length (without SID!)
Return code	
-	-
Functional Description	
Particularities and Limitations	
> Check carefully with GM if further services are allowed.	

Table 4-29 ApplFblEnablePrgMode

### 4.2.2 ApplFblInitiateDiagnosticOperation

Prototype	
void <b>ApplDiagUserSubFunction</b> ( vuint8 * pbDiagData, tTpDataType diagReqDataLen )	
Parameter	
pbDiagData	Pointer to diag service data (after SID!)
diagReqDataLen	Service data length (without SID)!
Return code	
-	-
Functional Description	
Particularities and Limitations	
> Check carefully with GM if further subfunctions are allowed.	

Table 4-30 ApplFblInitiateDiagnosticOperation

### 4.2.3 ApplFblReadDataByIdentifier

Prototype	
<pre>void <b>ApplFblReadDataByIdentifier</b> (                                 vuint8 *pbDiagData,                                 tTpDataType diagReqDataLen                                 )</pre>	
Parameter	
pbDiagData	Pointer to buffer containing the diagnostic request.
diagReqDataLen	The number of bytes in the diagnostic request. This should be a constant, kDiagRqlReadDataByIdentifier.
Return code	
-	-
Functional Description	
<p>This function is called to handle Read-Data-By-Identifier (service \$22) requests.</p> <p>The routine retrieves the data-identifier(s) (DIDs) one by one to currentDid from the didBuffer, fill the message buffer with the appropriate DIDs response information, and call DiagProcessingDone() with the response length information. Alternatively a Nrc is to be set.</p> <p>Symbolic names for GM standard identifiers may be found in fbl_apdi.h with names like kDiagDid&lt;identifier&gt;. If the DID is not supported, the function should invoke the macro DiagNRCCRequestOutOfRange(). If the DID is supported but not available, the function should invoke the macro DiagNRCCConditionsNotCorrect).</p>	
Particularities and Limitations	
<ul style="list-style-type: none"><li>&gt; Please check which DIDs need to be supported above the preimplemented.</li><li>&gt; The BootSoftwareIdentificationDataIdentifier is not preimplemented, the format is unknown by Vector</li></ul>	

Table 4-31 ApplFblReadDataByIdentifier

### 4.2.4 ApplFblReportProgrammedState

Prototype	
<pre>vuint8 <b>ApplFblCheckTesterSourceAddr</b> ( vuint8 testerId )</pre>	
Parameter	
esterId	Id of tester to be checked
Return code	
kFbIOk	Message to be processed
kFbIFailed	Message not to be processed.
Functional Description	
<p>Check for valid Tester Ids.</p> <p>Configure the valid tester IDs for your ECU inside kValidTesterIdTable.</p> <p>In case of a valid ID, FblDiagCheckTesterSourceAddr needs to be called and its result is returned, else</p>	

**Particularities and Limitations**

- > Check is done against kValidTesterIdTable. Standard entries are configured in GENy user config parameters DIAG\_TESTER\_NODE\_ADDR1- DIAG\_TESTER\_NODE\_ADDR5

Table 4-32 ApplFblReportProgrammedState

**4.2.5 ApplFblRdbidProgrammedStateInd****Prototype**

```
tTpDataType ApplFblRdbidProgrammedStateInd ( void )
```

**Parameter**

vuInt8 * pbDiagData	Pointer to data buffer for response data
------------------------	--

**Return code**

tTpDataType	Length of response data
-------------	-------------------------

**Functional Description**

This function is called to fill the response data upon receiving readDataByIdentifier (0x12) with data identifier ProgrammedStateIndicator (0xF0). The function checks the PSI state of each available partition and places the information in the response buffer.

**Particularities and Limitations**

- > None

Table 4-33 ApplFblRdbidProgrammedStateInd

**4.3 Module Validation Callbacks**

ApplFblExtProgRequest	ApplFblFillGaps	ApplFblChkModulePresence
ApplFblInvalidateBlock	ApplFblChkOpSwProgrammedState	ApplFblChkPSIState
ApplFblValidateBlock	ApplFblGetPresencePatternBaseAddress	ApplFblGetBaseModulePPRegion
ApplFblIsValidApp *	ApplFblSetModulePresence	ApplFblGetModuleHeaderAddress
ApplFblGetProgrammedState	ApplFblClrModulePresence	ApplFblUpdateChecksum
ApplFblINVMReadKeyNBID	ApplFblINVMReadECUID	ApplFblFinalizeChecksum
ApplFblINVMWriteKeyNBID	ApplFblINVMReadAppNBID	ApplFblINVMWriteAppNBID
ApplFblINVMReadSBATicket		

Table 4-34 Module Validation Callbacks

\* These routines are also described in reference [3].

### 4.3.1 ApplFblExtProgRequest

Prototype	
<code>tFblProgStatus <b>ApplFblExtProgRequest</b>( void )</code>	
Parameter	
Return code	
<code>kNoProgRequest</code>	Return this value if the FBL has not been started by the Operating Software
<code>kProgRequest</code>	Return this value if the FBL has been started by the Operating Software
Functional Description	
This function is called during the startup of the ECU to determine if the FBL has been started by the Operating Software.	
Particularities and Limitations	
<ul style="list-style-type: none"><li>&gt; The default implementation uses a macro called <code>FblChkFblStartMagicFlag()</code> to determine if the bootloader was started by the Operating Software. The macro uses a global variable named <code>fblStartMagicFlag[]</code>. This array must be located in a region of memory that is not destroyed when a reset occurs. If located in RAM, the region must not be zeroed by the ECU startup-code.</li><li>&gt; The variable used to indicate startup by the Operating Software (<code>fblStartMagicFlag[]</code>) must be cleared before exiting this routine. The macro <code>FblClrFblStartMagicFlag()</code> may be used for this purpose.</li></ul>	

Table 4-35 ApplFblExtProgRequest

### 4.3.2 ApplFblFillGaps

Prototype	
<code>tFblResult <b>ApplFblFillGaps</b>( void)</code>	
Parameter	
Return code	
<code>kFblOk</code>	Return this if regions of currently downloaded module are successfully filled.
<code>kFblFailed</code>	Return this if regions of currently downloaded module are not successfully filled.
Functional Description	
<p>If the gap fill feature is enabled in GENy then this function calls the build in function <code>FblHdrFillGaps</code> to fill unused memory with the configured fill pattern.</p> <p>If the gap fill feature is disabled in GENy then the user may implement a custom gap fill algorithm in this function. Otherwise, the user can leave the function as is and no gap filling will be performed by the bootloader.</p> <p>See also 9.9.</p>	

**Particularities and Limitations**

- > The starting address of each address-region must be aligned to a write-segment boundary.

Table 4-36 ApplFblFillGaps

**4.3.3 ApplFblInvalidateBlock****Prototype**

```
tFblResult ApplFblInvalidateBlock( tBlockDescriptor blockDescriptor )
```

**Parameter**

--	--

**Return code**

kFblOk	Return this if regions of currently downloaded module are successfully filled.
kFblFailed	Return this if regions of currently downloaded module are not successfully filled.

**Functional Description**

The purpose of this function is to alter the flag(s) used by `ApplFblIsValidApp()` to indicate that the module is not present. The flag(s) used to validate a module is often referred to as a Presence-Pattern.

**Particularities and Limitations**

The implementation provided usually does not have to be changed. If you want to change it please note the following things:

- > See also `ApplFblIsValidApp()` and `ApplFblValidateBlock()`.
- > If a failure occurs while invalidating the module, you must call one of the error-indication macros defined in `fbl_diag.h`. These have the form `DiagNRC<condition>`. For example, `DiagNRCGeneralProgError()`.
- > “Programmed State Indicator (PSI)” (Section 12.5.10 in reference [2]) requires that the PSI be located at the end of the last sector used by the Operating Software and last calibration module. Per default Calibration modules PSI locations are automatically determined to the last `FlashBlock[]` of the calibration partition covered, whereas application pattern locations are to be configured (check `ApplFblGetPresencePatternBaseAddress()`).
- > If using the erase method to invalidate a module, **you must insure that the presence-pattern is erased before any other data in the block.**

Table 4-37 ApplFblInvalidateBlock

**4.3.4 ApplFblIsValidApp****Prototype**

```
tApplStatus ApplFblIsValidApp( void )
```

**Parameter**

--	--

**Return code**

kApplValid	Return this to indicate that the Operating Software and all required supporting (e.g. Calibration) modules have been downloaded and are ready to run.
------------	---

kApplInvalid	Return this if the Operating Software is not ready to run.
<b>Functional Description</b>	
<p>This routine is called to determine if the FBL should start the Operating Software. It is called during the startup of the ECU, after verifying that the FBL is not being started by the Operating Software (see <code>ApplFblExtProgRequest()</code>).</p> <p>The routine should check the presence-pattern flag(s) managed by <code>ApplFblValidateBlock()</code> and <code>ApplFblInvalidateBlock()</code>. If all required modules are present, then the routine should indicate that the application is valid.</p>	
<b>Particularities and Limitations</b>	
> See also <code>ApplFblValidateBlock()</code> , <code>ApplFblInvalidateBlock()</code> , and Section 4.9.	

Table 4-38 ApplFblIsValidApp

### 4.3.5 ApplFblValidateBlock

<b>Prototype</b>	
<code>tFblResult <b>ApplFblValidateBlock</b>( tBlockDescriptor blockDescriptor )</code>	
<b>Parameter</b>	
blockDescriptor	Module-Id (MID) from the File-Header of the module being downloaded.
<b>Return code</b>	
kFblOk	Return this to indicate that the module presence-pattern has been successfully written.
kFblFailed	Return this to indicate that the module presence-pattern cannot be saved to non-volatile memory.
<b>Functional Description</b>	
<p>The purpose of this function is to update the flag(s) used by <code>ApplFblIsValidApp()</code> to indicate that a module has been downloaded. The function is called at the end of a download, after all data has been written and validation (checksum) tests completed.</p>	
<b>Particularities and Limitations</b>	
> See also <code>ApplFblIsValidApp()</code> , <code>ApplFblInvalidateBlock()</code> , and Section 4.9.	

Table 4-39 ApplFblValidateBlock

### 4.3.6 ApplFblGetProgrammedState

<b>Prototype</b>	
<code>vuInt8 <b>ApplFblGetProgrammedState</b>(void)</code>	
<b>Parameter</b>	
-	-
<b>Return code</b>	
kDiagProgStateFullyProgrammed	Appl and all Cals are present

kDiagProgStateNoSoftwareOrCal	Appl not present
kDiagProgStateNoCalibration	Appl present, some Cal is missing
kDiagProgStateDefOrNoStartCal	Appl present, all Cals are present (special Cals) (Will never be reported currently, e.g. change ApplFblCalsPresent() implementation to detect default/no start calls to allow this return value).
<b>Functional Description</b>	
Checks if the application and/or calibration presence pattern of Primary Operating software all set	
<b>Particularities and Limitations</b>	
> -	

Table 4-40 ApplFblGetProgrammedState

### 4.3.7 ApplFblChkOpSwProgrammedState

<b>Prototype</b>	
static uint8 ApplFblChkOpSwProgrammedState(uint8 opSwID)	
<b>Parameter</b>	
opSwID	Id of operation software to get programmed state for.
<b>Return code</b>	
kDiagProgStateFullyProgrammed	Appl and all Cals are present
kDiagProgStateNoSoftwareOrCal	Appl not present
kDiagProgStateNoCalibration	Appl present, some Cal is missing
<b>Functional Description</b>	
Check on given opSwID the Programmed State of OpSW and its calibration files	
<b>Particularities and Limitations</b>	
> -	

Table 4-41 ApplFblChkOpSwProgrammedState

### 4.3.8 ApplFblGetModuleHeaderAddress

<b>Prototype</b>	
tFblAddress ApplFblGetModuleHeaderAddress( uint8 blockNr )	
<b>Parameter</b>	
blockNr	Describes Table entry number of Logical block. Be careful: this is not the "Block Index" information in GENy. It is simply the number of the entry: e.g.: 0 – First entry (usually appl with Block Index/MID of 0x01) 1 – Second entry (e.g. appl2 with MID of 0x15/21)

Return code	
tFblAddress	Address of module header information structure
Functional Description	
<p>This function has to return the address of a module header.</p> <p>Only Application Modules have to be configured in default configuration. These are the modules that have to be configured in Logical Block Table. You may change calibration pattern addresses from automatically determining to static configuration by replacing the call to FblHdrGetCalibrationPPRegion() by returning mid specific addresses.</p>	
Particularities and Limitations	
<p>The module header may be placed at e.g.</p> <ul style="list-style-type: none"> <li>&gt; the beginning of the logical block (offset = +0x00 ) or</li> <li>&gt; with an offset to the beginning of the block (offset = +0xXX)</li> <li>&gt; with an offset to the end of the block (offset = -0xXX)</li> </ul> <p>Add check for blockNr that do not have header information located at the start of the logical block table region.</p>	

Table 4-42 ApplFblGetModuleHeaderAddress

### 4.3.9 ApplFblGetBaseModulePPRegion

Prototype	
<pre>void ApplFblGetBaseModulePPRegion(vuint8 mid, IO_PositionType *pPresPtnAddr, IO_SizeType *pPresPtnLen )</pre>	
Parameter	
mid	Id of base module.
*pPresPtnAddr	Presence Pattern address for the given module
*pPresPtnLen	Presence Pattern Area length for the given module (for mask and pattern)
Return code	
None	
Functional Description	
<p>This function has to return address and length of the covered presence pattern region (mask and pattern).</p> <p>The function need to return presence pattern information only for application modules. The default implementation takes these values from GENy configuration.</p>	
Particularities and Limitations	
<ul style="list-style-type: none"> <li>&gt; The function has got assertions verifying that <ul style="list-style-type: none"> <li>&gt; the GENy configured presence pattern address is within programmable memory</li> <li>&gt; the GENy configured presence pattern address places the patterns really at the end of a flash block</li> </ul> </li> </ul>	

Table 4-43 ApplFblGetBaseModulePPRegion



### 4.3.10 ApplFblGetPresencePatternBaseAddress

Prototype	
<b>static tFblAddress ApplFblGetPresencePatternBaseAddress ( vuint8 blockNr, IO_PositionType *pPresPtnAddr, IO_SizeType *pPresPtnLen)</b>	
Parameter	
blockNr	this is either the module ID of a downloaded module or the virtual blockNbr (starting above MAX_MODULE_ID) of replacement key Descriptor to be stored inside update key section configured to FBL_UPDATEKEY_SEC_START_ADDR a
pPresPtnAddr	Pointer to RAM location to place the address to the presence pattern region begin of
pPresPtnLen	Pointer to the RAM location where the length of the presence pattern shall be stored to.
Return code	
memSegment	memSegment of the presence pattern location or kFblDiagMemSegmNotFound in case of an error
Functional Description	
Returns the base address of the presence pattern and mask and the length of both fields.	
Particularities and Limitations	
> Addresses are automatically calculated for calibration partitions. Addresses for applications are configured in GENy and provided by ApplFblGetBaseModulePPRegion().	

Table 4-44 ApplFblGetPresencePatternBaseAddress

### 4.3.11 ApplFblSetModulePresence

Prototype	
<b>static tFblResult ApplFblSetModulePresence(tBlockDescriptor *blockDescriptor);</b>	
Parameter	
blockDescriptor	Pointer to the logical block descriptor
Return code	
kFblOk	Presence pattern successfully set
kFblFailed	Error writing presence pattern
Functional Description	
Writes the presence pattern into the flash memory. The location of the presence pattern will be taken from the logical block descriptor.	
Particularities and Limitations	
> The function is invoked so that blockDescriptor->blockNr will contain the Module ID of the downloaded module.	

Table 4-45 ApplFblSetModulePresence

### 4.3.12 ApplFblClrModulePresence

Prototype	
static tFblResult <b>ApplFblClrModulePresence</b> (tBlockDescriptor *blockDescriptor);	
Parameter	
blockDescriptor	Pointer to the logical block descriptor
Return code	
kFblOk	Mask for invalidation successfully written
kFblFailed	Error writing invalidation mask
Functional Description	
Sets the mask presence pattern in flash memory to invalidate the block. The location of the presence pattern will be taken from the logical block descriptor.	
Particularities and Limitations	
<p>&gt; The function is invoked so that blockDescriptor-&gt;blockNr will contain the Module ID of the downloaded module</p>	

Table 4-46 ApplFblClrModulePresence

### 4.3.13 ApplFblChkModulePresence

Prototype	
static tFblResult <b>ApplFblChkModulePresence</b> (tBlockDescriptor *blockDescriptor);	
Parameter	
blockDescriptor	Pointer to the logical block descriptor
Return code	
kFblOk	Presence pattern are set and Mask value are OK
kFblFailed	Presence pattern not set or mask flag not correct.
Functional Description	
Checks if mask and value of the presence pattern are set for a valid module.	
Particularities and Limitations	
<p>&gt; Note that other than stated in the function header, the location of the presence pattern is calculated from gmheader regions, and not taken from Logical block table (text is standard Api and cannot be changed).</p>	

Table 4-47 ApplFblChkModulePresence

### 4.3.14 ApplFblChkPSIState

Prototype	
tPartPresState <b>ApplFblChkModulePresence</b> (vuint8 partId);	
Parameter	
partId	Partition ID of module to be checked

Return code	
PSI_PART_PRESENT	Module programmed
PSI_PART_INVALID	Module is invalid
PSI_PART_REVOKED	Module is Revoked
Functional Description	
Checks the PSI of a single module.	
Particularities and Limitations	
> See [2] section 12.5.10.1 “PSI States”	

Table 4-48 ApplFblChkPSIState

### 4.3.15 ApplFblGetBaseModulePPRegion

Prototype	
void <b>ApplFblGetBaseModulePPRegion</b> (vuint8 mid, IO_PositionType *pPresPtnAddr, IO_SizeType *pPresPtnLen);	
Parameter	
mid	Module ID
*pPresPtnAddr	Pointer to presence pattern address
*pPresPtnLen	Pointer to presence pattern length
Return code	
-	
Functional Description	
Get the presence pattern address and length of the base module for the given module ID>	
Particularities and Limitations	
> -	

Table 4-49 ApplFblGetBaseModulePPRegion

### 4.3.16 ApplFblUpdateChecksum

Prototype	
tFblResult <b>ApplFblUpdateChecksum</b> (V_MEMRAM1 vuint16 V_MEMRAM2 * const checksum, SecM_LengthType regLen, const V_MEMRAM1 vuint8 V_MEMRAM2 * const regStartAddr);	
Parameter	
*checksum	Pointer to current checksum value
regLen	Length of buffer
regStartAddr	Pointer to buffer to be added to checksum
Return code	
kFblOk	Checksum properly updated
kFblFailed	Failure updating the checksum

Functional Description
This function adds the values in buffer to the current checksum value.
Particularities and Limitations
> -

Table 4-50 ApplFblUpdateChecksum

### 4.3.17 ApplFblFinalizeChecksum

Prototype	
tFblResult ApplFblFinalizeChecksum (V_MEMRAM1 vuint16 V_MEMRAM2 * const checksum);	
Parameter	
*checksum	Pointer to checksum value
Return code	
kFblOk	Checksum finalized correctly
kFblFailed	Failure finalizing checksum
Functional Description	
This function performs an operation on the checksum after it has been calculated. By default the operation is a twos-complement.	
Particularities and Limitations	
> -	

Table 4-51 ApplFblUpdateChecksum

### 4.3.18 ApplFblNVMReadKeyNBID

Prototype	
tFblResult App1Fb1NVMReadKeyNBID (V_MEMRAM1 tNBIDInfo V_MEMRAM2* const keyNBIDInfo);	
Parameter	
*keyNBIDInfo	Pointer to key NBID info struct
Return code	
kFblOk	Key NBID read successfully
kFblFailed	Failure to read key NBID
Functional Description	
This function is used to read the stored key NBID from NVM.	
Particularities and Limitations	
> -	

Table 4-52 ApplFblNVMReadKeyNBID

### 4.3.19 ApplFbINVMWriteKeyNBID

Prototype	
tFbIResult ApplFbINVMWriteKeyNBID (V_MEMRAM1 tNBIDInfo V_MEMRAM2* const keyNBIDInfo);	
Parameter	
*keyNBIDInfo	Pointer to key NBID info struct
Return code	
kFbIOk	Key NBID written successfully
kFbIFailed	Failure to write key NBID
Functional Description	
This function is used to write the key NBID that was received.	
Particularities and Limitations	
> -	

Table 4-53 ApplFbINVMWriteKeyNBID

### 4.3.20 ApplFbINVMReadAppNBID

Prototype	
tFbIResult ApplFbINVMReadAppNBID ( V_MEMRAM1 tNBIDInfo V_MEMRAM2 * const appNBIDInfo );	
Parameter	
*appNBIDInfo	Pointer to app NBID info struct
Return code	
kFbIOk	Key NBID written successfully
kFbIFailed	Failure to write key NBID
Functional Description	
This function is used to read the stored app NBID.	
Particularities and Limitations	
> -	

Table 4-54 ApplFbINVMReadAppNBID

### 4.3.21 ApplFbChkModulePresence

Prototype	
tFbIResult ApplFbINVMWriteAppNBID (V_MEMRAM1 tNBIDInfo V_MEMRAM2* const appNBIDInfo);	

Parameter	
*appNBIDInfo	Pointer to app NBID info struct
Return code	
kFbIOk	App NBID written successfully
kFbIFailed	Failure to write app NBID
Functional Description	
This function is used to write the app NBID that was received.	
Particularities and Limitations	
> -	

Table 4-55 ApplFbChkModulePresence

### 4.3.22 ApplFbINVMReadECUID

Prototype	
tFbIResult <b>ApplFbINVMWriteAppNBID</b> (V_MEMRAM1 tNBIDInfo V_MEMRAM2* const appNBIDInfo);	
Parameter	
*buffer	Buffer to store ECUID
Return code	
kFbIOk	ECU ID read successfully
kFbIFailed	Failure to read ECU ID
Functional Description	
This function is used to read the ECU ID.	
Particularities and Limitations	
> -	

Table 4-56 ApplFbINVMReadECUID

### 4.3.23 ApplFbINVMReadSBATicket

Prototype	
tFbIResult <b>ApplFbINVMReadSBATicket</b> (V_MEMRAM1 uint8 V_MEMRAM2 * const buffer);	
Parameter	
*buffer	Buffer to store SBA ticket
Return code	
kFbIOk	SBA ticket read successfully
kFbIFailed	Failure to read SBA ticket

Functional Description
This function is used to read the ECU ID from NVM.
Particularities and Limitations
> -

Table 4-57 ApplFblNVMReadSBATicket

## 4.4 Watchdog Callbacks

The watchdog is any hardware device (in most cases, built into the hardware of your ECU) that consists of a timer and a mechanism to reset the ECU when the timer expires. This allows the ECU to recover from situations that prevent the software from functioning properly (such as infinite loops). To prevent a reset, the software must periodically reset the watchdog-timer so that it does not expire.

The FBL configuration tool, GENy, provides a switch to enable or disable watchdog handling. When enabled, you must define how often the timer will be reset (also using GENy). The refresh-period you specify must be less-than the time-out period of the watchdog-timer.

GENy will define the constant `FBL_WATCHDOG_TIME` to represent the refresh-period in terms of how often tasks are performed in `FblRepeat()`. All operations within the bootloader must call either `FblLookForWatchdog()` or `FblRealTimeSupport()` (calls `FblLookForWatchdog()`, additionally may start triggering Response Pending) at least once per millisecond in order to maintain the watchdog. At the appropriate time, `FblLookForWatchdog()` will call the function `ApplFblWDTrigger()` (which you must implement) to reset the watchdog-timer.

### 4.4.1 Start of Watchdog

The watchdog timing is critical for three events: power-on reset of the bootloader, transfer of control from the bootloader to the application, and transfer of control from the application to the bootloader.

When a power-on reset occurs, instructions in the FBL will be performed first. If your ECU starts the watchdog-timer from power-on, you will have to initialize (or halt) the watchdog handling as soon as possible;

Normally, you should start the watchdog-timer in `ApplFblWDInit()`. Normally this function is called after the FBL has decided to stay in the bootloader, so there is no issue of the watchdog-timer expiring while starting the Operating Software (see section 2.3.1). However, you will also need to start the watchdog-timer in your Operating Software's startup-code. If you choose to start the watchdog-timer before application start add the configuration switch `FBL_ENABLE_PRE_WDINIT`, which will call `ApplFblWDInit()` early. You should also configure `FBL_ENABLE_PRE_TIMERINIT` in this case, to guarantee the watchdog triggering starts; this enables the triggering in `FblLookForWatchdog`. To start watchdog early may also be required if `ApplFblInit()` contains long lasting initialization (Eeprom-Manager).

Start watchdog early (before hw-init, before start of operating software)	Define
	<code>FBL_ENABLE_PRE_WDINIT,</code>
	<code>FBL_ENABLE_PRE_TIMERINIT</code>

e.g. via GENy user preconfiguration file.

Start watchdog late (after hw-init, only when default  
executing boot)

#### 4.4.2 Synchronize Watchdog with application

When the bootloader transfers control to the Operating Software, the watchdog-timer must have the maximum amount of time available. This is an issue if the watchdog is started by the hardware at power-on, or if you initialize the watchdog early. You must configure the watchdog hardware so that the watchdog time-out period is large enough to start the Operating Software. Before starting the Operating Software, the FBL will call `ApplFblWDLong()`. You should implement `ApplFblWDLong()` to reset the watchdog-timer and then return. In addition, if you enable the Stay-In-Boot feature, you must reset the watchdog-timer in `ApplFblWDLong()` even if you start it late (alternatively disable it for this development feature).

#### 4.4.3 Window Watchdogs

Some ECUs implement a *Windowed-Watchdog*. In this case, the watchdog-timer cannot be reset at any arbitrary time; it must be reset within a small time period (the *trigger-window*) immediately before the watchdog-timer expires.

When using a windowed-watchdog, you must set the refresh-period in GENy to occur within the trigger-window. When possible, set the refresh period in the middle of the trigger-window; you should avoid setting the period to refresh immediately after the window opens, or immediately before watchdog-timer expires. In this configuration, it is especially important that the watchdog-timer and the refresh-timer are started at the same time.

In addition, you must take care that your implementation of `ApplFblWDLong()` waits until the trigger-window opens. This may be achieved by calling `FblLookForWatchdog()` continuously until it returns `FBL_WD_TRIGGERED`. Finally, you must devise a means of synchronizing the FBL's watchdog refresh-period with your Operating Software's refresh-period. One solution is to define and start an "elapsed-time" timer in `ApplFblWDLong()` that can be read by your Operating Software to determine when the trigger-window opens.

#### 4.4.4 Watchdog triggering during Memory operations

The bootloader faces a unique problem when erase and write operations are performed. In most cases, the ECU is unable to read instructions from the device while waiting for the erase/write to complete. Hence, the code to reset the watchdog-timer, which resides on the same device, cannot be executed. To resolve this issue, the bootloader makes a copy of `FblLookForWatchdog()` and `ApplFblWDTrigger()` in RAM. The device-driver calls the copy in RAM to maintain the system timers and refresh the watchdog-timer. To facilitate running from RAM, your implementation of `ApplFblWDTrigger()` should not contain any conditional operations, loops, or function-calls, especially if your compiler does not generate position-independent code.

Most ECUs initiate a device operation by setting a "command" register and then repetitively check a "status" register to indicate that the operation is complete. The device-driver will call the copy of `FblLookForWatchdog()` (in RAM) while waiting. However, in some systems the device operations are performed by calling a library function provided



by the device manufacturer. In this case, the system timers cannot be maintained while a device operation is performed. You must configure the watchdog-timer period so that it is greater-than the worst-case time need to perform an erase or write operation. Additional callbacks may be available so that the elapsed time spent performing device operations can be accounted for. A detailed description of these functions will be provided in the Hardware Technical-Reference included with your delivery.

ApplFblWDInit \*                      ApplFblWDLong \*                      ApplFblWDTrigger \*

Table 4-58 Watchdog Callbacks

\* These routines are also described in reference [3].

#### 4.4.5 ApplFblWDInit

Prototype	
void <b>ApplFblWDInit</b> ( void )	
Parameter	
-	-
Return code	
-	-
Functional Description	
<p>The purpose of this function is to start the watchdog function of the ECU. The function is called only after the FBL has determined that it will not start the Operating Software (It is called shortly after <code>ApplFblStartup()</code>).</p> <p>If the watchdog is initialized in this routine, then the FBL may start the Operating Software without starting the watchdog. In this case, the Operating Software will be responsible for starting the watchdog itself.</p> <p>The FBL uses a hardware timer to determine when to reset the watchdog (via <code>ApplFblWDTrigger()</code>). The timer is initialized shortly after this routine is called. You must insure that the watchdog timer will not reset the ECU before the FBL can call the trigger function for the first time.</p>	
Particularities and Limitations	
<ul style="list-style-type: none"><li>&gt; In addition to initializing the hardware responsible for the watchdog, the global variable <code>WDTimer</code> must be initialized to the number of “ticks” that define the interval between calls to the trigger function. The interval is determined from your configuration, and is defined by the macro <code>FBL_WATCHDOG_TIME</code>.</li><li>&gt; Use of the watchdog is managed by the configuration switch “Watchdog Enable” (see also section 3.4). You should encapsulate your implementation within conditional-compilation directives to enable or disable the WD as appropriate. For example:<pre>#if defined( FBL_WATCHDOG_ON )     /* Enable Watchdog */ #else     /* Disable Watchdog */ #endif</pre></li></ul>	

Table 4-59 ApplFblWDInit

#### 4.4.6 ApplFblWDLong

Prototype
void <b>ApplFblWDLong</b> ( void )

Parameter	
-	-
Return code	
-	-
Functional Description	
<p>The purpose of this function is to synchronize the start of the Operating Software with the watchdog. The call gives you the opportunity to ensure that the watchdog will not interrupt the Operating Software's startup. The implementation should either wait for the next watchdog trigger-event (to maximize the period to the timeout), or disable the watchdog (Note: You should not disable the WD if your implementation of <code>ApplFblReset()</code> requires the WD to reset the ECU).</p> <p>The function is called just before the bootloader starts your application.</p>	
Particularities and Limitations	
<ul style="list-style-type: none"> <li>&gt; The function is called at the end of a programming session and when the FBL jumps to the Operating Software directly after power-on. Care should be taken if the watchdog (WD) is initialized in <code>ApplFblWDInit()</code>, since this function could be called before the WD is started. See also Section 2.3.1.</li> <li>&gt; Use of the watchdog is managed by the configuration switch "Watchdog Enable". You should encapsulate your implementation within conditional-compilation directives to avoid waiting for a watchdog event that never happens. For example: <pre> #if defined( FBL_WATCHDOG_ON )     /* wait for watchdog event */     /* !! Make sure WD is running before entering this loop (See above)!! */     /* !! This example does not contain the necessary check!! */     while (FblLookForWatchdog() != FBL_WD_TRIGGERED)         ; #endif </pre> </li> </ul>	

Table 4-60 ApplFblWDLONG

#### 4.4.7 ApplFblWDTrigger

Prototype	
<code>void ApplFblWDTrigger( void )</code>	
Parameter	
-	-
Return code	
-	-

Functional Description
<p>The purpose of this function is to reset the watchdog logic to prevent it's timer from resetting the ECU. The function will be called periodically (based on the "Watchdog time (ms)" entry in your configuration).</p> <p>The implementation should not call any other function, nor reference any data outside of RAM!</p> <p>Many non-volatile devices do not allow the ECU to fetch instructions (or any other data) from them while the device is being erased or programmed. Since the FBL often resides in the same device as the Operating Software and other downloaded modules, the routines to erase and write to the device are usually executed from RAM. The FBL also copies this function to RAM, so that it may be invoked from the device-driver while waiting for erase &amp; write operations to complete. During this time any calls to routines resident in the device being programmed will lead to failure.</p>
Particularities and Limitations
<ul style="list-style-type: none"><li>&gt; Not all ECUs allow code to be executed from RAM. Please refer to your hardware-specific FBL documentation for implementation details.</li><li>&gt; Since this function is usually copied from the FBL to RAM, the code must be compiled as position-independent (relocatable). If your compiler does not support this feature, then the implementation in this function must not contain any conditional expressions (any code that results in non-sequential execution, such as calls, <code>if</code>, <code>do</code>, <code>while</code>, and <code>for</code> statements). See also Section 4.8.</li><li>&gt; This function can be called even if your configuration does not enable watchdog handling (for example, the function could be called when waking from sleep-mode).</li><li>&gt; You may use the conditional-compilation switch <code>FBL_WATCHDOG_ON</code> within your implementation to selectively compile the code.</li></ul>

Table 4-61 ApplFblWDTrigger

## 4.5 Callback configuration summary

The Gm bootloader offers a lot of callbacks that are open for user modifications.

Some are required to be filled by you; some allow you to modify the behavior of the bootloader to your specific requirements. Many callbacks are only required for special use cases, or in case of hw-specific requirements. You also may reduce code size in changing them; e.g. by modifying generic implementations to a more specific use case. If you do not run into problems it is generally recommended to use our default implementations.

Several callbacks however need to be touched by you to complete the requirements demanded by the references [1] and [2]. These are listed in the following sub-chapter

### 4.5.1 Required callback configuration

These callbacks need to be checked or touched by you:

- > All hw-related callbacks required for hw-initialisation. These are
  - > ApplFblCanBusOff (define Busoff behavior)
  - > ApplFblInit (hw initialization)
  - > ApplFblReset (hard hw-reset)
  - > ApplFblSetVfp / ApplFblResetVfp (if programming voltage is required; rather rare)
  - > ApplTrcvrSleepMode / ApplTrcvrNormalMode
  - > ApplFblEnterStopMode / ApplFblSleepModeAllowed (for low power mode)
  - > ApplFblRamIntegrityCheck (if more than one check address region)

- > These Diagnostic callbacks:
  - > ApplFblReadDataByIdentifier (check if DIDs are complete, add missing, test read them)
- > All watchdog related callbacks
- > NVM related callbacks to read and write SBA ticket, App/Key not before IDs, ECU ID.
  - > Note that a mechanism need to be in place to uniquely define ECU ID per given ECU.

## 4.6 Application Vector Table

In order to start the bootloader, the reset-vector in the ECU's interrupt vector must **always** point to the startup code of the FBL. To insure that the bootloader is always able to start up, the interrupt vector table should never be erased or reprogrammed. However, if the interrupt vector table cannot be programmed, how can the ECU invoke interrupt service routines in the Operating Software?

The solution to create a second structure, the Application Vector Table, that contains the instructions needed to jump to each interrupt service routine (ISR). This structure is linked with the Operating Software, and is programmed when the Operating Software is programmed. The ECUs vector table, programmed when the bootloader is programmed, will contain a fixed address for each interrupt that points to a corresponding entry in the Application Vector Table.



### Caution

The location of the Application Vector Table cannot be changed once the FBL is programmed into your ECU. All subsequent downloads of the Operating System must use the same address for the Application Vector Table.

Your bootloader delivery contains two files, `applvect.c` and `fbl_applvect.c`. Each contains a definition of the application vector table. The file `fbl_applvect.c` should be linked to your flash bootloader, while `applvect.c` should replace the interrupt vector table in your Operating Software (see Section 5).

When running, the FBL does not use any interrupts. However, on many ECUs an interrupt is required to recover from sleep-mode (this depends on your implementation of `ApplFblEnterStopMode()`). If you require an interrupt to wake-up, but are not using the CAN-controller to manage this ("Enable sleep mode" is disabled in your configuration), you should edit the Application Vector Table in `fbl_applvect.c`, and modify the vector used by your wake-up interrupt to point to your ISR handler. If you are using the CAN-controller to wake-up, and have more than one CAN-cell, you may need to edit `fbl_applvect.c` to call `FblCanWakeUpInterrupt()` from the appropriate CAN vector.

For additional information on sleep-mode, please see the function descriptions for `ApplFblIsSleepModeAllowed()`, `ApplFblEnterStopMode()`, and `ApplFblCanWakeUp()`.

## 4.7 Transport-Layer Configuration

The Transport-Layer configuration switches are generated from GENy to the file `ftp_cfg.h`. There are no OEM specific features in this file. The configuration of the Transport layer usually should not be touched.. Contact us if you require changes.

## 4.8 `[#hw_wd]` – Compiling the Watchdog components

Since the operations that erase and write the flash hardware may take some time, it is necessary for the flash driver to invoke the watchdog handling functions. These functions, initially in flash, may not be accessible while the flash is being erased or written. To resolve this issue watchdog functions `FblLookForWatchdog` and `ApplFblWDTrigger` need to be executed out of RAM. Usually they are copied via a linker mechanism to RAM location.

The mechanism to implement this depends highly on the compiler you are using. You should refer to the hardware-specific manual of your delivery for instructions on how to compile the watchdog components. Also check carefully our Demo (linker file) to see how copying to RAM is done.

## 4.9 `[#oem_valfunc]` – Flashing After A Reset

For more general information about this see the `UserManual_FlashBootloader` in the chapter **Your Application Initiates the Flashing Process**.

The GM FBL uses different names for the callback functions used to manipulate the validation area as those indicated in the general user manual.

Reference [3] defines the function `ApplFblValidateApp()` to write the signature that indicates that a module is present. The GM FBL uses the function `ApplFblValidateBlock()` instead of `ApplFblValidateApp()`.

Reference [3] defines the function `ApplFblInvalidateApp()` to remove the signature that indicates that a module is present. The GM FBL uses the function `ApplFblInvalidateBlock()` instead of `ApplFblInvalidateApp()`.

## 4.10 `[#oem_valid]` – Proposals for Handling The Validation Area

For more general information about this see the `UserManual_FlashBootloader` in the chapter **Proposals for Handling the Validation Area**.

The Vector FBL uses three functions to control the validation area:

`ApplFblIsValidApp()`, `ApplFblInvalidateBlock()`, and `ApplFblValidateBlock()`.

`ApplFblIsValidApp()` is called when the FBL is started up to determine if the Operating Software and all other required partitions are programmed.

`ApplFblInvalidateBlock()` is called at the start of download to invalidate the partition.

`ApplFblValidateBlock()` is called when a download completes to update the area again.

The implementation of the functions provided with the bootloader conforms to the requirements defined in “Programmed State Indicator (PSI)” (Section 12.5.10), which states:

- > The PSI for the application SW shall be located in the last two bytes of application SW partition.
- > For each calibration partition, there shall be one PSI assigned to that partition. The PSI shall be located in the last two bytes for that partition.
- > The number of PSIs is equal to the number of partitions and not the number of programmable modules.

Separate validation areas are used for the Operating Software and Calibration data partitions. Per design, the location of the validation areas for application software is configured in the logical block table, the locations for calibration partitions are automatically determined.

The implementation of the three aforementioned API functions uses several local functions to write the presence patterns. The function `ApplFblGetPresencePatternBaseAddress()` determines the location of the presence pattern. In case of calibration files, the routine calls `FblHdrGetCalibrationPPRegion()` to determine the largest address used by the module, and map the address to an entry in the Flash-Block table to determine the address of the “last 2 bytes”. `ApplFblGetBaseModulePPRegion()` provides the addresses for Operational Software (per default read from logical block table configuration).

Mask and pattern are located in the same block and have to be erased together. You must refer to the documentation supplied by Vector for your device-driver(s) to verify that the erase function is implemented (some drivers, notably the EEPROM drivers, do not implement the erase function – this is integrated into the write routines). In this case, you must modify `ApplFblValidateBlock()` to write the “erase” character to the validation mask.

You may choose to store the presence patterns separately (for example, in EEPROM). In this case, you must explicitly erase (or write the erase character, depending on your device-driver) the presence pattern in `ApplFblValidateBlock()`.

The bottom-line is that the last three bytes (and possibly more, at least two-segments worth of memory, depending on the segment-size of your non-volatile device) of the last block used by each module (application and calibration) cannot be used to store downloaded data. The Fbl will send an NRC 72, Pec error code `Err_Region`, Debug status `kHdrDebugErrIllegalSwRegion`, if it is tried to write to this location.

#### 4.11 [#oem\_start] Startup

The FBL is always started upon a power-on reset, and should be started via a reset (depending on the implementation of `ApplFblReset()`) when started by the Operating Software. The download sequence is completed when the Fbl receives the Default Session Service which will trigger a reset.

Upon startup, the FBL will execute the compiler-specific startup code (which may be customized), and then control will be transferred to the main module.

The compiler-specific startup code is generally responsible for initializing the run-time environment, such as setting RAM to zero, copying the initial value of variables to RAM, and initializing the stack. In some hardware designs, it is necessary to modify the startup source module provided by your compiler vendor in order to initialize special registers, such as the watchdog, memory configuration, and system timing (PLL). In some instances, the special registers and/or instructions used in the startup code may only be executed immediately after reset.

When configuring the FBL, keep in mind that the ECU's reset vector will always point to the startup compiled as part of the bootloader. If your Operating Software uses non-default startup code, it may not be able to modify the special configuration registers or execute certain instructions. Attempting to do so may reset your ECU.

If your Operating Software contains a customized startup module, you should move/copy your initialization from the Operating Software to the bootloader.

The main module will perform some minimal hardware initialization, and then perform a check to determine if the bootloader is being started by the Operating Software. If not, the FBL will determine if the Operating Software is ready to run. If so, then the FBL will transfer control to the Operating Software via the reset jump vector in the Application Vector Table.

If the FBL is being started by the Operating Software, or if the Operating Software is not ready, the FBL will continue with hardware initialization (for example, start the CAN controller and hardware timers), and then proceed to the main-loop, where it will wait for CAN messages to arrive.

Initialization of the Bus controller depends on your FBL configuration. When started by the Operating Software, the FBL obtains the Tester Id from a structure called the CAN Initialization Table. For details on starting the FBL from the Operating Software, please refer to Chapter 5.

#### 4.12 **[#oem\_ref]** – Label Reference File

Several structures are shared between the Operating Software and the FBL:

- > Module File-Headers, to read out part numbers, DLS, etc. (Application header address is configured in GENy.
- > And generated to fbl\_cfg.h)
- > Application Vector Table (if no vector base register),
- > The address of the Application Vector Table must be known to the FBL when it is compiled. The link address of the structure MUST be the same in both the bootloader and Operating Software. Additional details regarding the Application Vector Table may be found in section 4.5.
- > SBA ticket (received in Application, read in boot)
- > Crypto lib / Public key (in case of validating SBA ticket in appl)



## 5 Adapting the Operating Software

Typically, the Operating Software is initially developed as a stand-alone program, independent of the bootloader environment. To download the Operating S/W with the FBL, several changes need to be made.

For the following, many references are made to your 'Makefile' and 'Linker Directives'. You should interpret these as references to the tools in your development environment that control which files are compiled into the Operating System, how they are compiled, and where in memory the compiled objects are located. In many instances, the Integrated Development Environment (IDE) supplied by your compiler vendor is used to manage how the software is built.

There are four files that are shared between the Operating Software and the Flash Bootloader: `fbl_def.h`, `v_def.h`, `v_cfg.h`, and `fbl_cfg.h`. You should add the paths to folders containing these files to the file-search (include) path list in your Makefile. You must recompile both the FBL and your Operating Software when you reconfigure your bootloader since `fbl_cfg.h` is a generated (using GENy) file.

### STEP 1: **ADAPT START-UP CODE**

When the ECU is powered-up, register initialization, memory configuration, etc, will be handled by the startup code of the bootloader. If you have modified the startup code provided by the compiler-vendor to perform any hardware-specific I/O or register initialization, the modifications should be copied to the startup code of the FBL. Keep in mind that many ECUs contain registers that may be written only once.

### STEP 2: **CHANGE MAPPING CHECK INTERRUPT VECTOR TABLE**

Move or replace the Interrupt Vector Table in use by the Operating Software. It has to be located in Add the Interrupt Service Routines for the Operating Software to the application vector table, found in `app/vect.c`. Add `applvect.c` to the Makefile/Link-list for the Operating Software (set the start address to the same location as that used by the FBL).

### STEP 3: **[#oem\_trans] – ADD DIAGNOSTICS TO INVOKE BOOTLOADER**

When a session control (service 10 02) is received, the Operating S/W should initialize the structure defined by `tCanInitTable` and invoke the bootloader. The following table describes the fields found in the structure:

Name	Description
<code>TpTargetAddress</code> (1 byte/vuint8)	Tester Id. Required to continue communication by Fbl
<code>extendedInfo</code> (4 byte/tFblAddress)	Generic parameter, currently unused. May be used to e.g. reference address to further parameters or single additional parameter.

Table 5-1 Parameters passed to FBL by Operating Software



An example of the table initialization and FBL call may be found inside the DemoApp project we deliver (usually `fbl_jmpToFbl.c`).

Once the table has been initialized, the FBL may be started by invoking the macro `CallFblStart()`. The Operating S/W should not send a positive-response to the download request (the response will be sent by the FBL).

Because the Fbl may need to check the SBA ticket upon starting up, you should send a Request-Correctly-Received; Response-Pending (RCR-RP) message before jumping to the boot.

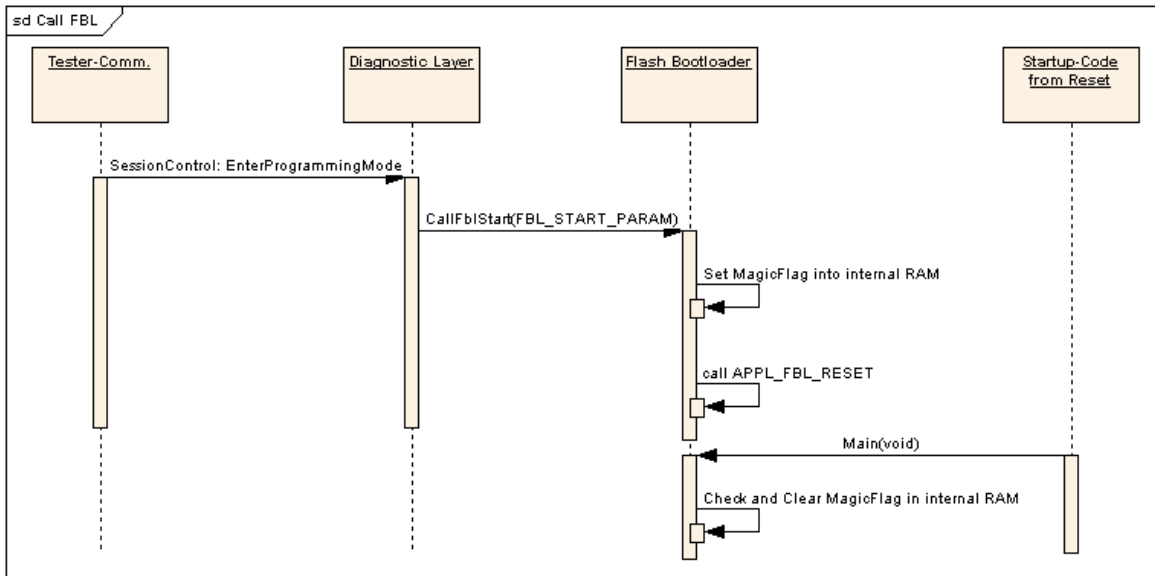


Figure 5-1 Standard transition from application to bootloader



### Caution

In most cases, the FBL will ultimately be started by forcing the ECU to reset (depends on your implementation of `ApplFblReset()`).

If your ECU is not started via a reset, you must be careful that all register (such memory-mapping or timing) settings are consistent with the power-on settings required to run the FBL.

In addition, if a reset is not employed, you should be careful to avoid starting the FBL from an interrupt service routine (such as a transmit confirmation callback for the RCR-RP message).

## STEP 4: RESERVE SPACE FOR FBL AND PRESENCE-PATTERN(S)

The Makefile/Linker directives should be modified to reserve space in flash for the bootloader and presence patterns. These areas must not be used by the Operating Software.

If a map file is available after re-compiling the Operating Software, you may want to verify that the addresses of the code and constant-data sections are within the bounds set in `fbl_apfb.c::FlashBlock`. The download will not succeed unless all sections mapped to flash memory fit within the regions defined in the

flash block table. Adjust the Makefile/Linker directives of the Operating Software as needed.

**STEP 5: BUILD CALIBRATION DATA MODULES (optional)**

This step is only necessary if the FBL was configured to require modules in addition to the Operating Software. There are several ways of creating the data modules – it is up to you to decide upon the most appropriate action. Headers for calibration files are generated together with the application header script.

**STEP 6: ADD THE FILE-Containers**

Check our Technical reference [6] to see how this is done.

## 6 Device Driver

### 6.1 General Information

The device-driver is responsible for erasing and writing data to non-volatile memory. This program is stored in the ECU flash memory and copied to RAM before downloading any other module. Most deliveries will include one device-driver capable of programming your ECU's internal flash-memory. The FBL will transfer the driver to a RAM array called `flashCode[]`. The size of the array, defined by the configuration tool, GENy, must be large enough to contain the driver.

Each device-driver is compiled as an independent program, although it does not contain ECU-startup code, nor a “main” entry point. Access to the routines should be performed by a set of high-level API functions defined by the FBL Memory Input/Output component (`fbl_mio`). See also section 6.2. The low-level API of the device-driver module is based on the HIS flash programming standard (see reference [5]).

The device-driver is compiled as either relocatable or non-relocatable code, depending on the hardware and development environment. Relocatable code is more flexible in that the code can be executed from anywhere in the memory space of the ECU; non-relocatable code has to be compiled to run from a specific RAM address: the starting address of `flashCode[]`.

If your driver supports relocatable code, the macro `FLASHCODE_RELOCATABLE` will be defined in `flashdrv.h`. In this case, the “starting” address of the driver link-file may be set to zero, since the FBL will relocate the downloaded code to `flashCode[]`.

If your driver does not support relocatable code, the “starting” address of the driver's link-file must correspond to the starting address of the `flashCode[]` array in the FBL. The FBL will reject the driver if the addresses do not match. In most cases, you should examine the address assigned to the link-section named “FLASHDRV” in the FBL, and use the same address in the link-section named “SIGNATURE” in the driver. Note that the section names will vary depending on the abilities of your development environment.

A script is provided to convert flash driver hex files into a C-array that can be compiled and linked with the bootloader.

### 6.2 High-Level Device-Driver Functions

All accesses to non-volatile memory should be performed via the bootloader's Memory-I/O component. The API redirects your request to the appropriate device-driver interface. The component is capable of reading from any device at any time, even if the device-driver has not been downloaded. However, the erase and write functions should not be called until the device-driver has been downloaded (macro `GetMemDriverInitialized()` ).

When the FBL has been configured to support multiple devices, some API functions require that you define and set a variable named `memSegment`. The variable should be set to the index of the flash-block table record that corresponds to the address of memory that you are accessing. The routine `FblMemSegmentNrGet()` may be used to obtain the correct index.

### 6.2.1 MemDriver\_InitSync

Prototype	
<code>IO_ErrorType MemDriver_InitSync( void *address )</code>	
Parameter	
address	Usage depends on the device-driver (in most cases, the parameter is not used, so NULL should be passed). See also your Hardware Technical-Reference documentation.
Return code	
IO_E_OK	Indicates that the device-driver(s) were successfully initialized. Any other value indicates that one or more drivers were not initialized. This is not necessarily an error condition. For example, when configured for multiple devices, the return value will indicate that only the device supported by the most recently downloaded driver is initialized.
Functional Description	
<code>MemDriver_InitSync()</code> is used to initialize all available device-drivers. The bootloader will call this function after downloading a device-driver.	
Particularities and Limitations	
<ul style="list-style-type: none"><li>&gt; An initialization routine must be called before invoking the driver-interface functions <code>GetMemDriverReady()</code>, <code>MemDriver_RwriteSync()</code>, <code>MemDriverDevice_RwriteSync()</code>, <code>MemDriver_VerifySync()</code>, or <code>MemDriverDevice_VerifySync()</code>. Note that <code>MemDriver_RreadSync()</code> and <code>MemDriverDevice_RreadSync()</code> may be called at anytime without initialization.</li><li>&gt; This function may take a considerable amount of time to complete. See also the limitations for <code>MemDriver_ReraseSync()</code>.</li></ul>	

Table 6-1 MemDriver\_InitSync

### 6.2.2 MemDriver\_ReraseSync

Prototype	
<code>IO_ErrorType MemDriver_REraseSync (</code> <code>                                  IO_SizeType eraseLength,</code> <code>                                  IO_PositionType eraseAddress</code> <code>)</code>	
Parameter	
eraseLength	Number of bytes to be erased. The <code>eraseAddress + eraseLength</code> should be aligned to the end of an erase-sector.
eraseAddress	Starting address of the region to be erased. The address must be aligned to the start of a sector-boundary.
Return code	
IO_E_OK	Indicates that the region was successfully erased. Any other value represents a device-specific error code.
Functional Description	
<code>MemDriver_ReraseSync()</code> is used to erase one or more sectors of non-volatile memory.	

### Particularities and Limitations

- > The function `MemDriver_InitSync()` must be called before using these functions.
- > Before calling these functions, you should call `GetMemDriverReady()` to determine that the device-driver has been downloaded and initialized.
- > When multiple-devices are supported by the FBL (`FBL_ENABLE_MULTIPLE_MEM_DEVICES`), you must set a local variable named `memSegment` before calling `MemDriver_ReraseSync()`. For example:  
`memSegment = FblMemSegmentNrGet(eraseAddress);`
- > These functions may take a considerable amount of time to complete. Maintenance of the watchdog-timer and P2Timer is handled inside delivered drivers. For you own drivers added please poll for `FblRealTimeSupport()` in a cycle <1ms.

Table 6-2 MemDriver\_ReraseSync

## 6.2.3 MemDriver\_RreadSync

### Prototype

```
IO_ErrorType MemDriver_RReadSync (
    unsigned char* readBuffer,
    IO_SizeType readLength,
    IO_PositionType readAddress
)
```

### Parameter

readBuffer	Pointer to RAM buffer where the retrieved data will be copied to.
readLength	Number of bytes to obtain.
readAddress	Starting (logical) address of memory to read.

### Return code

IO_E_OK	Indicates that the region was successfully obtained. Any other value represents a device-specific error code.
---------	--

### Functional Description

Use these functions to read data from non-volatile memory into RAM.

### Particularities and Limitations

- > When multiple-devices are supported by the FBL (`FBL_ENABLE_MULTIPLE_MEM_DEVICES`), you must set a local variable named `memSegment` before calling `MemDriver_RreadSync()`. For example:  
`memSegment = FblMemSegmentNrGet(readAddress);`
- > These functions may take a considerable amount of time to complete. See also the limitations for `MemDriver_ReraseSync()`.
- > These functions may be called at any time without regard to whether or not the device-driver has been downloaded or initialized.

Table 6-3 MemDriver\_RreadSync

## 6.2.4 MemDriver\_RwriteSync

Prototype	
<pre>IO_ErrorType MemDriver_RWriteSync (     unsigned char* writeBuffer,     IO_SizeType writeLength,     IO_PositionType writeAddress )</pre>	
Parameter	
writeBuffer	Pointer to the source of data that is to be written to non-volatile memory. Many device-drivers require that the pointer is aligned to a specific (e.g. longword) boundary.
writeLength	Number of bytes to be written. The value must be a multiple of the devices write-segment size (See MemDriver_SegmentSize()).
writeAddress	Starting address (logical) where the data will be written to. The address must be aligned to a segment boundary (i.e. The value should be a multiple of the write-segment size).
Return code	
IO_E_OK	Indicates that the region was successfully written. Any other value represents a device-specific error code.
Functional Description	
Use these functions to write data to non-volatile memory.	
Particularities and Limitations	
<ul style="list-style-type: none"><li>&gt; The function MemDriver_InitSync() must be called before using these functions.</li><li>&gt; Before calling these functions, you should call GetMemDriverReady() to determine that the device-driver has been downloaded and initialized.</li><li>&gt; When multiple-devices are supported by the FBL (FBL_ENABLE_MULTIPLE_MEM_DEVICES), you must set a local variable named memSegment before calling MemDriver_RwriteSync(). For example: memSegment = FblMemSegmentNrGet(writeAddress);</li><li>&gt; These functions may take a considerable amount of time to complete. See also the limitations for MemDriver_ReraseSync().</li></ul>	

Table 6-4 MemDriver\_RwriteSync

## 6.2.5 MemDriver\_VerifySync

Prototype	
<pre>IO_ErrorType MemDriver_VerifySync( void *address )</pre>	
Parameter	
address	Starting address of the sector to be verified. NULL may be passed to verify all sectors that have been modified (erased or written) since the initialization of the driver, or since the last call to this function.  Note that on some systems, a (void *) cannot reach all addresses on the system. In this case, NULL must be passed as the argument. See also your Hardware Technical Reference.

Return code	
IO_E_OK	Indicates that the region was successfully verified. Any other value represents a device-specific error code.
Functional Description	
Use these function to verify the data written to non-volatile memory. This is required by some devices to ensure data-retention time.	
Particularities and Limitations	
<ul style="list-style-type: none"> <li>&gt; The function <code>MemDriver_InitSync()</code> must be called before using these functions.</li> <li>&gt; Before calling these functions, you should call <code>GetMemDriverReady()</code> to determine that the device-driver has been downloaded and initialized.</li> <li>&gt; When multiple-devices are supported by the FBL (<code>FBL_ENABLE_MULTIPLE_MEM_DEVICES</code>), you must set a local variable named <code>memSegment</code> before calling <code>MemDriver_RwriteSync()</code>. For example:  <code>memSegment = FblMemSegmentNrGet(writeAddress);</code></li> <li>&gt; These functions may take a considerable amount of time to complete. See also the limitations for <code>MemDriver_ReraseSync()</code>.</li> </ul>	

Table 6-5 MemDriver\_VerifySync

## 7 Using the Flash Tool for GM

vFlash is a Download Tool provided by Vector to be used for all OEM flash processes supported. It is a PC (Microsoft Windows <sup>™</sup>) based application that can transfer your Operating Software and other data modules to your ECU via the Flash Bootloader. The vFlash tool has to be purchased separately. The delivery includes a template for the GM use case that needs to be installed to be able to use vFlash with this bootloader.

### 7.1 Preparing the File-Header

Every module downloaded via the bootloader is required to have a File-Container. The container identifies the type of data, where the data should be stored, and so on. The format and contents of the header varies depending on the type of module

We recommend using our provided scripts to generate the required header information. A description of how to create the file containers using HexView can be found in [6].

### 7.2 Configuring vFlash

vFlash has several tabs that must be configured for your system.

#### 7.2.1 vFlash Communication Tab

The vFlash communication allows you to configure communication parameters (see screenshot below).



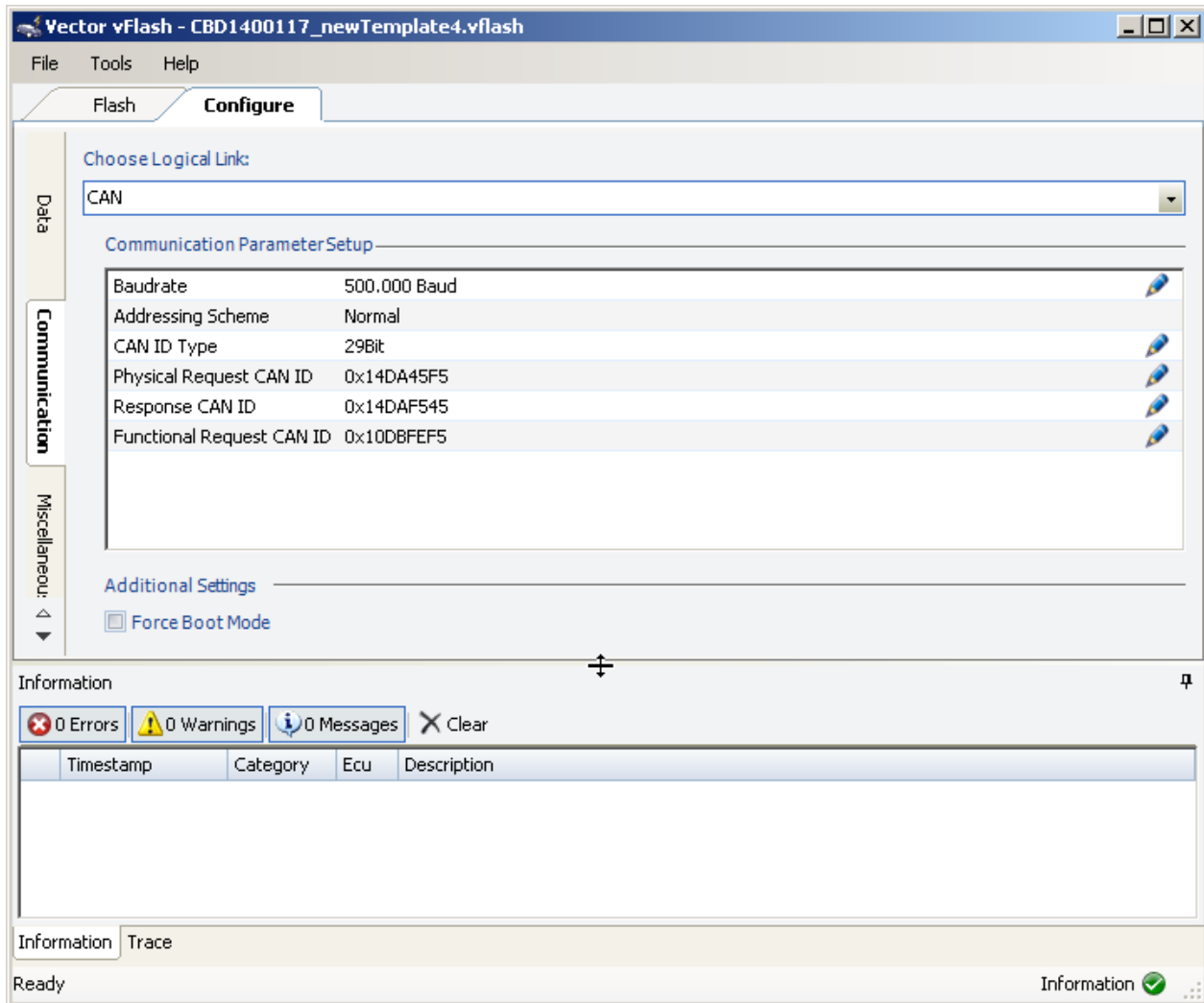


Figure 7-1 Example vFlash Communication Configuration Dialogue

Parameter	Configuration
Communication link	Only CAN is supported.
Baudrate	Baudrate of the bus that vFlash is connected to.
Address Scheme	Only Normal is supported for this bootloader.
CAN ID BusType	Length of CAN IDs used. Only 29Bit is supported currently in vFlash. The 11bit request mode is not supported by the tool (the Fbl supports it).
Physical Request CAN ID	The physical reception ID of the ECU.
Response CAN ID	The physical response ID of the ECU.
Function Request CAN ID	The functional (broadcast) ID of all ECUs on the bus.
Force Boot Mode	Vector development feature, see 3.4.1. Not available in vFlash tool before 1 <sup>st</sup> Q 2015. The required ping message (31 01 F5 1B) need to be sent manually to the Bootloader if the feature is to be used.

Table 7-1 Parameter description of the communication tab in vFlash

## 7.2.2 vFlash Miscellaneous Tab

The vFlash miscellaneous tab allows you to configure additional options of vFlash.

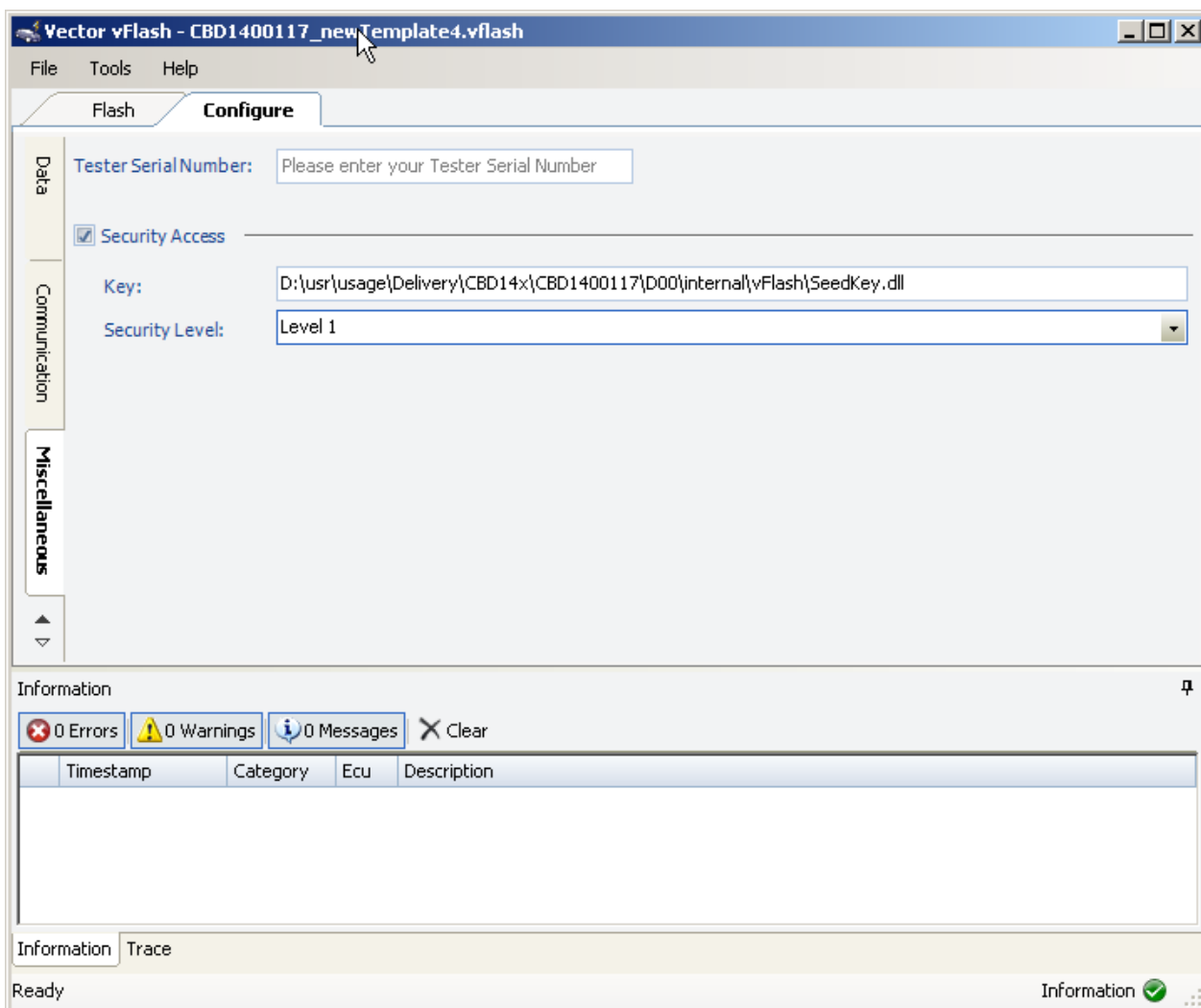


Figure 7-2 Example vFlash Miscellaneous Configuration dialog

Parameter	Configuration
Tester Serial Number	Not relevant for this bootloader.
Security Access	When enabled, vFlash will send the security access requests.
Key	DLL used to calculate the key from the seed received. You may create your own dll to allow security access with your application (in Bootloader Security access is always unlocked upon \$27 \$01). A project to to that can be found in the .\FlashTool folder.
Security Level	Always Level 1 for this bootloader.

Table 7-2 Parameter description of the miscellaneous tab in vFlash

## 7.2.3 vFlash Data Tab

The vFlash data tab allows you to configure the modules to be downloaded to the ECU. The modules will be downloaded in the order specified.

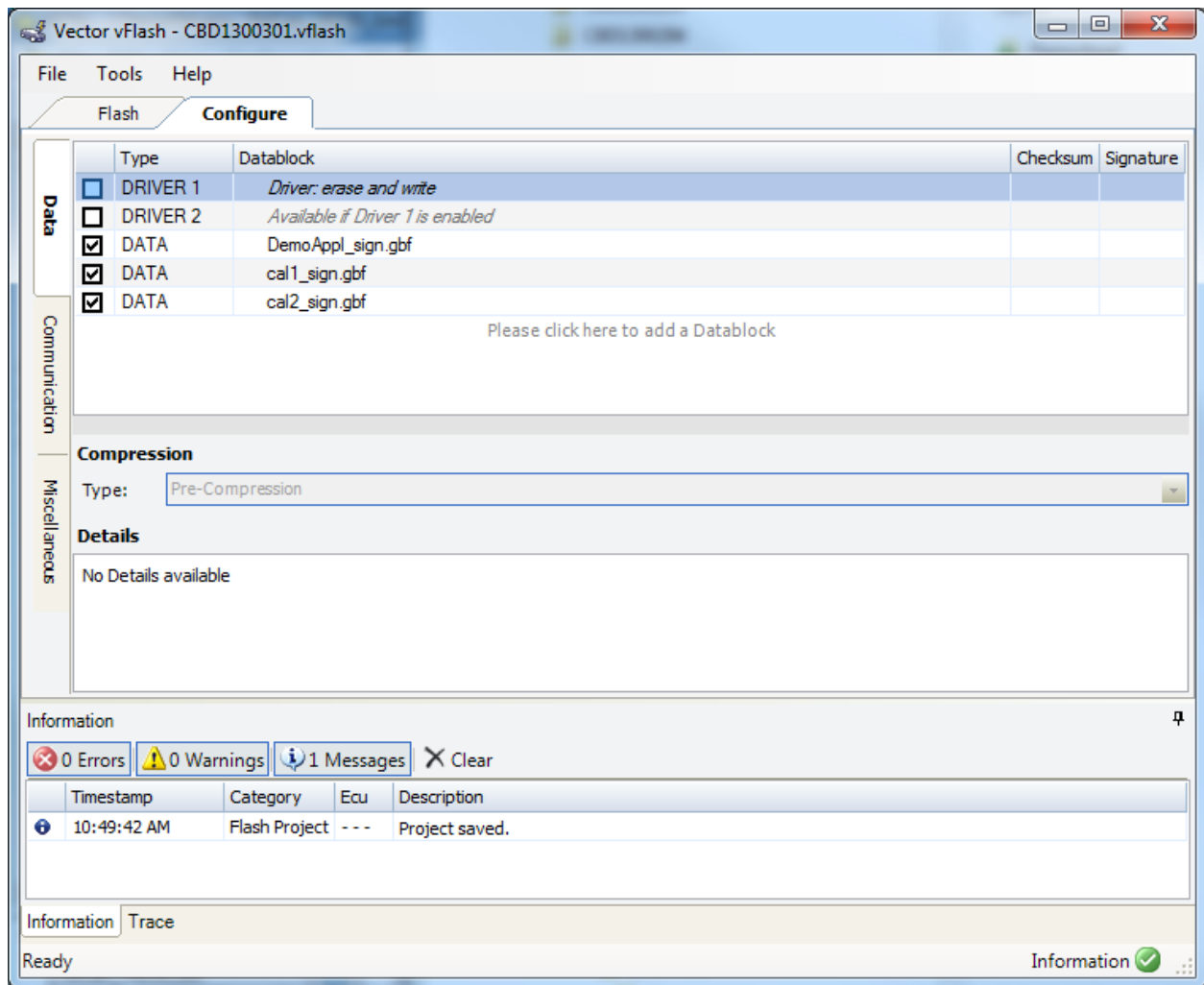


Figure 7-3 Example vFlash Data Configuration Dialogue



**Note**

Do not configure DRIVER1/DRIVER2. It is not required for this use case

### 7.3 Starting the flash sequence with vFlash

To start the flash process, click the 'Flash' button in the upper right of the Flash tab in vFlash. The result of the flashing session will be displayed in the windows below.

## 8 Miscellaneous

### 8.1 [#oem\_multi] – Multiple-Identity-Modules

For more general information about this see the UserManual\_FlashBootloader in the chapter **Multiple ECU Support**.

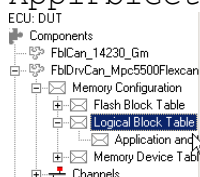
Multiple Identity Modules (MIM) support is enabled when multiple nodes are selected in the configuration tool (GENy) (see Section 3.2). When enabled, you must add code to the FBL to determine the identity of the module, and select the appropriate CAN identifiers.

The FBL calls the function `ApplFblCanParamInit()` to obtain this information. You must implement this function to initialize the FBL's structures appropriately. Please refer to the description of `ApplFblCanParamInit()` for details.

### 8.2 Multiple Processor Support

For multiple processor support, please configure the `FblCan_14230_Gm->GM Modules configuration->(Multiple application modules support)` option.

You will have to add entry(s) for your additional application + calibration areas. Please note that you will have to configure `Header Address` and `Presence Pattern Address` configuration describing application header start and validity info location. These items are returned inside the callbacks `ApplFblGetModuleHeaderAddress()` and `ApplFblGetBaseModulePPRegion()`.



Name	Block Index	Disposability	Start Address	End Address	Header Address	Presence Pattern Address	Verification RAM	Verification ROM	Description
Application and Calibration Area1	0x1*	mandatory	0x10000	0x80fff	0x10000	0x80fff0	FblHdPipelinedVerityIntegrity*	FblHdVerityIntegrity*	

Figure 8-1 Multi-Processor logical block table configuration

Attributes:

- > **Block Index:** Please configure Block Index attribute for the required Partition ID (OpSw1 0x01, OpSw2 0x11, OpSw3 0x21, OpSw4 0x31).
- > **Other Attributes:** Compare Logical Block Table configuration.

Multi-processor solutions typically use a communication protocol to allow flashing of a slave ECU from a master ECU. The physical layer will typically be CAN/LIN/SPI. The required protocols are not part of the standard delivery. Please contact us to discuss possible solutions.

### 8.3 PEC error code and Debug-Status

Many diagnostics services provide very limited information regarding the cause of an error (for example, "General Programming Failure"). Gm specifies the pec error code to hold more detailed information. In Project state "Integration", more detailed information may be obtained from the ECU sending a dedicated DID. When enabled by your configuration (Project State "Integration"), the FBL will respond to a Read-Data-By-Identifier request with

Data-Identifier (DID) CF00. The response contains information regarding the cause of the most recent negative response. In any case the Fbl will answer with some extended information on GM specified DIDs F0F1 (PEC error code) and F0F2 (Boot Initialization status). These include already helpful information. The vFlash template will query both pec error code and debug status information. F0F1 and F0F2 are GM demanded DIDs, which are preimplemented by the Fbl.

The Read-Data-By-Identifier request for DID CF00 for debugging status returns the following information additionally (see also the description of `ApplFblInitErrStatus()`):

Byte	Description
0	PCI: Least-significant 4 bits indicates number of bytes in message frame.
1	Positive Response ID: \$62
2-3	Data Identifier: \$CF 00
4	Service ID of last failed request ( <code>errStatLastServiceId</code> )
5	Failure Reason ( <code>errStatErrorCode</code> ) Possible values are defined in <code>fbl_diag.h</code> : See macros <code>kDiagErr&lt;fault&gt;</code> .
6-8	Optional: most-significant three bytes of error address ( <code>errStatAddress</code> ). Alternatively, if <code>errorStatErrorCode</code> indicate a Transport-Protocol error ( <code>kDiagErrTPFailed</code> ), a single byte value is supplied returning the TP error code ( <code>errStatTpError</code> ). In this case, the next field (file-name) starts at byte 6.
9-n	Zero-terminated string of ASCII characters identifying name of the file in which error was detected.
n-end	Line-number in file that detected error (number-of-bytes is ECU specific).

Table 8-1 Response for debug-status request

The information regarding a failure is stored via the functions `FblErrDebugStatus()` and `FblErrDebugDriver()`, as well as the macros `FblErrStatSetSid`, `FblErrStatSetState`, `FblErrStatSetFlashDrvError`, and `FblStatSetError`.

Please see `fbl_diag.h` for more information on the error status codes.

**Note**

You can retrieve additional error information reading the Programming Error Code (see section 12.6 of [2]).

## 8.4 [#oem\_time] – Stay-In-Boot mode

For more general information about this see the UserManual\_FlashBootloader in the chapter **Validation OK – Application faulty**.

A common feature of Vector bootloaders is the ability to stay in the bootloader even if the Operating Software is ready to run (`ApplFblIsValidApp()` returns `kApplValid`). For production, GM requires you to disable this feature. However, it may be very helpful during development.

For example, you download an Operating Software module that contains an issue that causes the ECU to reset. The result is that you will be unable to replace the module, since the FBL will start the Operating Software, which then resets. This starts the FBL, which starts the Operating System again, over and over. In this situation, there is no means to start a download.

To escape this situation, the Stay-In-Boot feature inserts a small delay between the time the ECU is reset, and the time the FBL starts the Operating Software. If a “ping” message is received during this delay, the FBL will stay in its main loop instead of starting the Operating Software. Once the FBL is executing its main loop, a new module may be downloaded normally.

To enable this feature, you must configure the Stay-In-Boot feature in the `FblDrvCan_<Hw>` component.

When enabled, the FBL will respond to a Routine Control (\$31) service request containing the Routine of **F5 IB**. This message must be sent using a physically-addressed CAN-Id. The message must be sent less-than 12 milliseconds after resetting the ECU. The default delay time may be set by uncommenting the `FBL_START_DELAY` defined above, and replacing ‘12’ with the desired delay time in milliseconds.

## 8.5 User-Callable Support Functions

The following documents commonly used functions in the FBL that may be invoked from callback functions.

### 8.5.1 FblStart

**Prototype**

```
void FblStart( tCanInitTable *pCanInitTable )  
void CallFblStart( tCanInitTable *pCanInitTable )
```

**Parameter**

pCanInitTable	Pointer to CAN Initialization table in Operating S/W memory. NULL may be passed if Operating S/W has directly initialized the FBL initialization table.
---------------	---

Return code	
-	-
Functional Description	
<p><code>FblStart()</code> is normally called indirectly to start the bootloader. The Operating Software should invoke <code>CallFblStart()</code> upon receipt of the Programming Session (service \$10 02) request. The macro will lookup the address of <code>FblStart()</code> and transfer control to the FBL.</p> <p><code>FblStart()</code> will copy the <code>CanInitTable</code> containing the Tester Address from memory in the Operating Software to memory controlled by the FBL. Next, the function will set the array <code>FblStartMagicFlags[]</code> to indicate that the FBL is being started by the Operating Software. Finally, the function will call <code>ApplFblReset()</code> to reset the ECU and start the FBL. See also section 2.3.2</p>	
Particularities and Limitations	
<ul style="list-style-type: none"> <li>&gt; The download-tool will expect a response to the Programming Session Request within <math>P2_{CE}</math> milliseconds. Since the FBL always may need to calculate the SBA ticket signature during startup (can take several seconds), the application shall always send a response pending prior to call the Fbl. The RCR-RP response will direct the download-tool to wait an additional 5000ms for the final response.</li> <li>&gt; <code>FblStart()</code> does not maintain the watchdog timer. Care should be taken to ensure that the watchdog timer does not expire before the time to reset the ECU. To avoid this, the Operating Software should call <code>FblStart()</code> immediately after resetting the watchdog timer to make the maximum time available to the FBL.</li> </ul>	

Table 8-2 FblStart

## 8.5.2 FblReadMem

Prototype	
<code>tFblLength FblReadProm(tFblAddress address, vuInt8* buffer, tFblLength length)</code>	
Parameter	
address	Logical address of memory to read.
Buffer	Pointer to RAM where the values from source memory will be saved at.
Length	Number of bytes to copy from source memory.
Return code	
Read length	If memory was successfully read.
Functional Description	
<p>The function copies the contents of memory starting at the specified logical address to the specified destination using the appropriate device-driver (via <code>MemDriver_RreadSync()</code>). Logical addresses are defined by the Flash-Block table found in <code>fbl_apfb.c</code>.</p> <p>If the source address does not correspond to an entry in the Flash-Block table, the routine will treat the address as a physical address; the data will be copied in a manner similar to a call to <code>memcpy()</code>.</p> <p>While copying data, <code>FblRealTimeSupport()</code> or <code>FblLookForWatchdog()</code> may be called to support response-pending messages and watchdog handing</p>	

### Particularities and Limitations

- > The address-range of physical memory should not overlap the address-range of logical memory (logical memory is defined by the Flash-Block table).

Table 8-3 FblReadMem

## 8.5.3 GetDiagInProgress

### Prototype

Boolean **GetDiagBufferLocked**( void )

### Parameter

-	-
---	---

### Return code

False	If the FBL is not currently processing a diagnostics request.
True	If the FBL is currently processing a diagnostics request.

### Functional Description

This macro will indicate if a request is being processed.

### Particularities and Limitations

- > -

Table 8-4 GetDiagInProgress

## 8.5.4 FblRealTimeSupport

### Prototype

vuint8 **FblRealTimeSupport**( void )

### Parameter

-	-
---	---

### Return code

FBL_NO_TRIGGER	Indicates that the watchdog timer was not reset during this call.
FBL_WD_TRIGGERED	Indicates that the watchdog timer was reset during this call.

### Functional Description

This function maintains operations that must occur in real-time:

1. The watchdog timer is updated as needed (See `FblLookForWatchdog()`).
2. The response-pending message is sent as needed (See `DiagExRCRResponsePending()`).

The function must be called at least once per millisecond.

### Particularities and Limitations

- > This function should usually be called rather than `FblLookForWatchdog()`, as P2 timing handling is included if required.

Table 8-5 GetDiagInProgress



### 8.5.5 FblLookForWatchdog

Prototype	
vuint8 V_API_NEAR <b>FblLookForWatchdog</b> ( void )	
Parameter	
-	-
Return code	
FBL_NO_TRIGGER	Indicates that the watchdog timer was not reset during this call.
FBL_WD_TRIGGERED	Indicates that the watchdog timer was reset during this call.
Functional Description	
<p>This function manages the hardware-specific and P2 (response-pending) timers. The function must be invoked at least once per millisecond.</p> <p>The function also checks the hardware timer to determine if it is time to reset the watchdog timer. If true, the function will invoke <code>ApplFblWDTrigger()</code> to reset the watchdog timer.</p>	
Particularities and Limitations	
<ul style="list-style-type: none"><li>&gt; No action is taken unless the hardware timer is running (the timer is started by <code>FblTimerInit()</code>).</li><li>&gt; No action is taken unless the watchdog handler has been initialized (via <code>FblInitWatchdog()</code>).</li><li>&gt; Watchdog support is provided only if enabled in the FBL configuration (<code>fbl_cfg.h</code> contains <code>FBL_WATCHDOG_ON</code>).</li><li>&gt; Note that to support watchdog handling while writing or erasing non-volatile memory, this function and <code>ApplFblWDTrigger()</code> are normally executed from RAM (most types of flash cannot be read while an erase or write operation is in progress). See also section 4.8.</li></ul>	

Table 8-6 FblLookForWatchdog

### 8.5.6 DiagExRCRResponsePending

Prototype	
void <b>DiagExRCRResponsePending</b> ( vuint8 forceSend )	
Parameter	
forceSend	<code>kNotForceSendResponsePending</code> Response-Pending message will be sent only if it is time to do so (P2 timer is less-than 10 milliseconds).  <code>kForceSendResponsePending</code> Response-Pending message will be sent unconditionally.
Return code	
-	-
Functional Description	
<p>The function will send a Request-Received-Correctly-Response-Pending message when the response-pending (P2) timer is near or at zero. Once the message has been queued for transmission, the P2 timer will be reset (5000 milliseconds if download is not in progress, 30000 milliseconds if a download is in progress).</p>	

**Particularities and Limitations**

- > This function should be called only if the FBL is handling a diagnostic request. See also `FblRealTimeSupport()` and `GetDiagInProgress()`.

Table 8-7 DiagExRCRRResponsePending

**8.5.7 FblMemSegmentNrGet****Prototype**

```
vsint16 FblMemSegmentNrGet( FBL_ADDR_TYPE address )
```

**Parameter**

address	Logical address of memory to map to Flash-Block table
---------	---

**Return code**

-1	Indicates that the Flash-Block table does not contain an entry corresponding to the requested address.
0 – (kNrOfMemDrv-1)	Index of Flash-Block table entry corresponding to the requested address.

**Functional Description**

This function is used to search the Flash-Block table (`fbl_apfb.c::FlashBlock[]`) for an entry that corresponds to a specified address.

This may be used, for example, to find address-boundaries for erase operations, or to help determine where a module's presence-pattern may go.

**Particularities and Limitations**

- > The Memory-I/O functions (`MemDriver_ReraseSync()`, `MemDriver_RreadSync()`, `MemDriver_RwriteSync()`, `MemDriver_VerifySync()`, and `MemDriver_SegmentSize()`) require a variable named `memSegment` to contain the block-table index to be set before being called if configured to support multiple-modules (`fbl_cfg.h` contains `FBL_ENABLE_MULTIPLE_MODULES`). This function may be used to obtain the index.

Table 8-8 FblMemSegmentNrGet

**8.5.8 GetFbl<XXX>Version****Prototype**

```
vuint8 GetFblMainVersion( void )  
vuint8 GetFblSubVersion( void )  
vuint8 GetFblReleaseVersion( void )
```

**Parameter**

-	-
---	---

**Return code**

-	FBL version information (0x00 – 0xFF)
---	---------------------------------------

Functional Description
<p>These macros return the version identifiers from the bootloader's File-Header. The version information is composed of three parts, a main-version, sub-version, and release-version.</p> <p>The values are associated with the macros in fbl_diag.h named FBLOEM_GM_VERSION and FBLOEM_GM_RELEASE_VERSION</p>
Particularities and Limitations
<p>&gt; These macros may be invoked from your Operating Software implementation (see fbl_def.h).</p>

Table 8-9 GetFbl<XXX>Version

### 8.5.9 GetFblDCID<X>

Prototype	
vuint8 <b>GetFblDCID0</b> ( void )	
vuint8 <b>GetFblDCID1</b> ( void )	
Parameter	
-	-
Return code	
-	Data-Compatibility-Identifier (0x00 – 0xFF)
Functional Description	
<p>These macros return the Data-Compatibility-Identifier values from the bootloader's File-Header (see references [1] and [2]).</p> <p><code>GetFblDCID0()</code> returns the most-significant byte while <code>GetFblDCID1()</code> returns the least-significant byte.</p>	
Particularities and Limitations	
<ul style="list-style-type: none"><li>&gt; The range of <code>GetFblDCID0()</code> is restricted to 0x80 – 0xFF, while <code>GetFblDCID1()</code> may return any value in the range of 0x00 – 0xFF.</li><li>&gt; These macros may be invoked from your Operating Software implementation (see <code>fbl_def.h</code>).</li></ul>	

Table 8-10 GetFblDCID<X>

### 8.5.10 GetFblSWMI<X>

Prototype	
<pre>vuint8 <b>GetFblSWMI</b>( vuint8 index ) vuint8 <b>GetFblSWMI0</b>( void ) vuint8 <b>GetFblSWMI1</b>( void ) vuint8 <b>GetFblSWMI2</b>( void ) vuint8 <b>GetFblSWMI3</b>( void )</pre>	
Parameter	
index	Index into the SWMI array (typically 0 – 3, but may be up to 15).
Return code	
-	Software-Module-Identifier (0x00 – 0xFF)

Functional Description
These macros return the Software-Module-Identifier values from the bootloader's File-Header (see references [1] and [2]). <code>GetFblSWMI0()</code> returns the most-significant byte, while <code>GetFblSWMI3()</code> returns the least-significant byte.
Particularities and Limitations
> Reference [2] constrains the SWMI field contain a 4-byte integer representing the FBL Part-Number. > These macros may be invoked from your Operating Software implementation (see <code>fbl_def.h</code> ).

Table 8-11 GetFblSWMI&lt;X&gt;

### 8.5.11 GetFblDLS<X>

Prototype
<code>vuint8 GetFblDLS0 ( void )</code> <code>vuint8 GetFblDLS1 ( void )</code>
Parameter
-
Return code
- Design-Level-Suffix, also known as Alpha-Code (0x00 – 0xFF)
Functional Description
These macros return the Design-Level-Suffix values from the bootloader's File-Header (see references [1] and [2]). <code>GetFblDLS0()</code> returns the most-significant byte, while <code>GetFblDLS1()</code> returns the least-significant byte.
Particularities and Limitations
> These macros may be invoked from your Operating Software implementation (see <code>fbl_def.h</code> ).

Table 8-12 GetFblDLS&lt;X&gt;

### 8.5.12 GetFblEcuNameAddr

Prototype
<code>vuint8 * GetFblEcuNameAddr ( void )</code>
Parameter
-
Return code
- Address of the array containing the ECU Name
Functional Description
-
Particularities and Limitations
> These macros may be invoked from your Operating Software implementation (see <code>fbl_def.h</code> ).

Table 8-13 GetFblEcuNameAddr

### 8.5.13 GetFblSubjNameAddr

Prototype	
vuint8 * <b>GetFblSubjNameAddr</b> ( void )	
Parameter	
-	-
Return code	
-	Address of the array containing the ECU Subject Name
Functional Description	
-	
Particularities and Limitations	
> These macros may be invoked from your Operating Software implementation (see fbl_def.h).	

Table 8-14 GetFblSubjNameAddr

### 8.5.14 GetFblEculdAddr

Prototype	
vuint8 * <b>GetFblEcuIdAddr</b> ( void )	
Parameter	
-	-
Return code	
-	Address of the array containing the ECU ID
Functional Description	
-	
Particularities and Limitations	
> These macros may be invoked from your Operating Software implementation (see fbl_def.h).	

Table 8-15 GetFblEculdAddr

### 8.5.15 GetFblMode

Prototype	
vuint8 <b>GetFblMode</b> ( void )	
Parameter	
-	-
Return code	
START_FROM_APPL	Indicates that the FBL was started by request of the Operating Software as a result of receiving a Request-Download (service \$34) request.

START_FROM_RESET	Indicates that the FBL has been started via a power-on reset.
APPL_CORRUPT	Reserved for future use.
STAY_IN_FLASHER	Set when application is valid and Stay-In-Boot feature is enabled. Indicates that FBL is waiting for “ping” message.
FBL_START_WITH_RESP	Reserved for future use.
FBL_START_WITH_PING	Indicates a Stay-in-Boot ping message has been received. The Diagnostics-Layer will set the security-access-delay-timer to zero and send a response.
<b>Functional Description</b>	
<p>This macro returns information about the current bootloader state. The returned value is a bit-mask; multiple bits may be set. You should perform a bitwise-AND to determine if the bootloader is in a particular state. For example:</p> <pre>if ((GetFblMode() &amp; START_FROM_RESET) != (vuint8)0) {     /* Starting from reset (not from Operating Software) */ }</pre>	
<b>Particularities and Limitations</b>	
> None	

Table 8-16 GetFblMode

## 8.6 Low Power Mode in the bootloader

There are 3 basic configurations for the FBL sleep mode. They are as follows:

- > Integrated sleep mode enabled
- > Integrated sleep mode enabled with wakeup interrupt
- > Integrated sleep mode handling disabled

Each of the configurations are detailed below

.

### 8.6.1 Integrated sleep mode enabled

The Ecu wakes up on CAN-message reception (*FblCanSleep()*, *FblCanWakeUp* are called from *App\FblEnterStopMode()* as shown in our example.

Only configurable if CAN-cell supports low power mode/wakeup on CAN-message reception.

Adapt *App\FblSleepModeAllowed()* to return *kFblOk* if conditions are correct to go to sleep. If a user-specific reason exists to not go to sleep, then return *kFblFailed*.

### 8.6.2 Integrated sleep mode enabled with wakeup interrupt

8.6.1 Integrated sleep mode enabled above applies, with the difference that a real interrupt has to be generated for the given controller to wake up on CAN-message reception.

The tag `FBL_ENABLE_WAKEUP_INT` must additionally be defined ( via GENy-preconfig file ). This configuration should only be used if a non-interrupt based configuration is not possible for a given controller.

This configuration requires modification to the vector tables and callbacks. Be sure the required measures to again wakeup the CAN-cell are handled. See the Note on “Using wake up Interrupt” comment below for further configuration aspects and potential problems that may come along.

Upon wake up interrupt *App/FblCanWakeUp()* will be called.

### 8.6.3 Integrated Sleep mode handling disabled

This is the configuration to use if a user-specific low power mode / wake-up mechanism other than CAN-message reception is to be used (e.g. when a transceivers that allows turning of the ECU power is used.)

You may adapt *App/FblSleepModeAllowed()* to return `kFblFailed` if no low power mode shall be used at all .



#### Using Wakup Interrupt

**Using a wakeup interrupt is not recommended as long as there are other possibilities for waking up again without interrupt.**

Interrupts should be globally enabled inside *App/FblEnterStopMode()* if Can Wakeup interrupt is to be used. CAN Wakeup interrupt is enabled in *FblCanSleep()*. All other peripheral interrupts except the CAN Wakeup interrupt should stay masked ( disabled ).

A sleep mode implementation using a wakeup interrupt should only be used before any application is ever programmed if the wakeup interrupt is called from reprogrammable memory ( this usually can only be avoided if there is a configurable vector table base address register ). This is to avoid enabling interrupts while there potentially is a corrupted application vector table.

The function *App/FblSleepModeAllowed()* should call the function *FblCheckBootVectTableIsValid()* to verify that it returns true ( no application was ever programmed ).

There is a potential deadlock problem when enabling global interrupts if the wakeup interrupt is served before the controller itself goes to low power mode: If the controller goes to low power mode after the CAN cell woke up, the ECU may not be able to wake up any more without externally resetting it. It must be verified if this is applicable for any given controller.

## 8.7 Example / hints to prepare containers for Ecus programmed with Fbl and Application

If you send your Ecu to the field you may prepare the files to be programmed to your ECU as follows

- > Add the presence pattern information to the end of the last block touched the same way the bootloader writes the information for each module. This depends on the controllers

minimum write size. Check in a debugger for the correct location and extract the pattern + mask information to a hexfile (e.g. insert in hexview). Verify that the application is started when the container including the patterns is programmed.

- > Merge the bootloader and all modules with presence patterns to a single file, fill the gaps with the fill pattern configured in the bootloader to fulfill the “unused bytes” requirement, compare section 7.5 in reference [2].

The same configuration can be used to load bootloader and application together to a debugger in order to debug application during development without having to program the application via CAN – this may be desirable during development.

## 8.8 Security Requirements

The bootloader is required to support two security services in order to keep malicious or unauthorized content out of the ECU [2]. See [2] for detailed descriptions of the required security handling.

- > Authentication: To ensure the content is genuine as authorized and released by GM [2].
  - > This is established through the digital signature and signer info.
- > Integrity: To ensure the content cannot be modified (intentionally or unintentionally) without being detected [2].
  - > This is established through the message digest.

The bootloader is also required to support two additional security features.

- > Application Software – Not Before Identifier (App-NBID)
- > Security Key – Not Before Identifier (Key-NBID)



### Note

Refer to [6] for information on creating plain and signed headers.

### 8.8.1 Digital Signature

The digital signature is included as a parameter of the signed header. This applies to both application and calibration modules. The digital signature is used to check that the content of the remaining parameters of the signed header are correct (e.g. authorizes the module with this signed header can be programmed to flash). The bootloader uses the public key stored in the signer info to validate the digital signature.

The digital signature needs to be updated each time a module is updated (e.g. application is modified and re-compiled). The private key must be known to update the digital signature.



During development, Vector provides an example public/private key combination that can be used to generate the digital signature. This process is described in [6].

During production, the private key is only known to GM and therefore only GM can generate the digital signature. In this instance, GM is provided with modules that contain only the plain header. GM then 'signs' these files by adding the signed header.

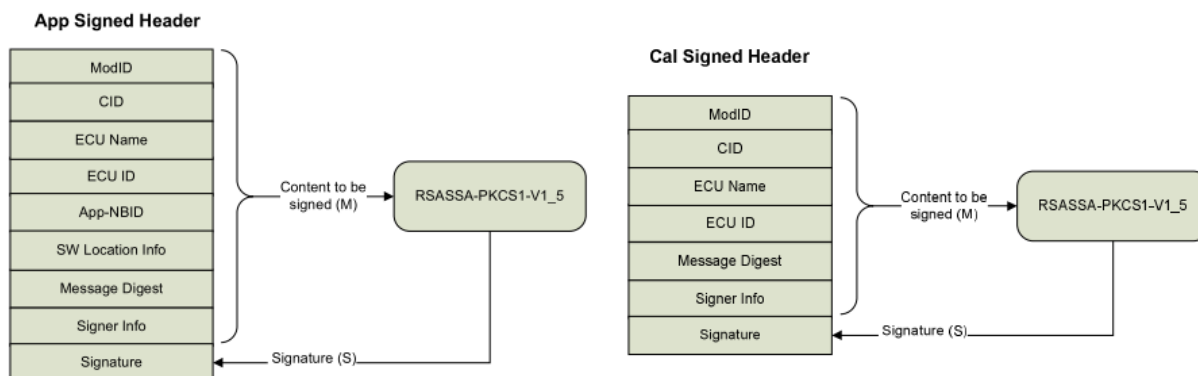


Figure 8-2 Application and Calibration signed header structures and signature calculation. "Signature" represents the digital signature

### 8.8.2 Signature-Bypass Authorization (SBA) ticket

The SBA ticket allows a way to skip the digital signature and message digest checks. The SBA ticket is a module that consists only of the Signature-Bypass Authorization Header. This can be downloaded to the ECU and stored into the ECU NVM. The download need to happen in application via a WriteDataByIdentifier DID.

During bootloader initialization, the SBA ticket will be read from NVM via the user function AppIFbINVMReadSBATicket. If a valid SBA ticket is found, the bootloader will set the Signature Bypass Indicator flag with this state. Upon receiving download of an application or calibration module, the bootloader will skip the digital signature and message digest verification. Therefore, it is possible to download modules without having the correct digital signature or message digest.

The use of an SBA ticket can be useful while debugging an issue on a production ready ECU. In this case, an SBA ticket can be downloaded to the ECU to allow it to skip the digital signature and message digest checks. Now modifications can be made to the module (application or calibration) without the need for the module to be 'signed' (e.g. the module does not need to be sent to GM for signing each time an update is made).

The delivery contains an SBA ticket valid for the Demo configuration using Demo values for ECU ID, Subject name and ECU name. It is signed using the provided demo-key and can be used for testing during development.

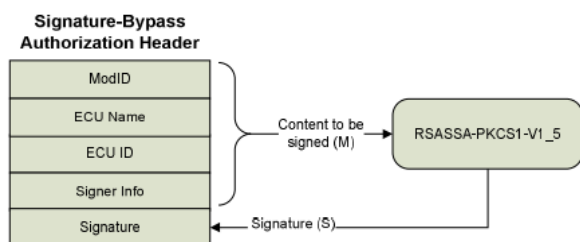


Figure 8-3 Signature-Bypass Authorization Header structure and signature calculation.

Implementations not necessarily require NVM memory in place. Please contact us in case of questions.



**Note**

An SBA ticket is only valid for a specific ECU ID and therefore can only unlock one unique ECU. Compare 8.8.7 on ECU ID.

### 8.8.3 Message Digest

The message digest is included as a parameter of the signed header. This applies to both application and calibration modules. The message digest is used to check that the content of a module that is programmed to flash memory has not been altered (intentionally or unintentionally). The message digest is calculated using the hash algorithm SHA256.

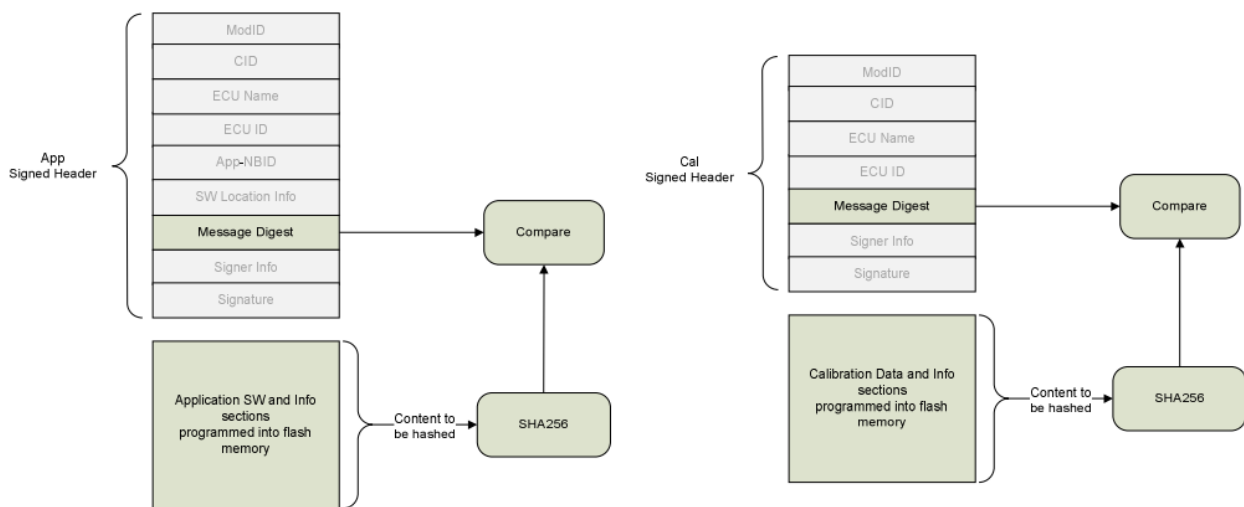


Figure 8-4 Application and Calibration Message Digest

#### 8.8.3.1 Pipelined Verification

The bootloader implements what is known as pipelined verification. Pipelined verification is when the bootloader actively calculates the hash on the programmed data while the bootloader is still downloading data. Each time a packet of data is transferred and programmed to the ECU the bootloader will calculate the hash of that packet while also receiving the next packet of data. This decreases the download time by significantly reducing the time to complete the hash calculation and message digest check at the end of programming.

#### 8.8.3.2 Optional Integrity Word Check

In addition to the message digest check, the bootloader can also perform an integrity word check. The integrity word is stored inside the plain header and contains a checksum based on a wordsum with a 2s complement of the data that is programmed to flash. The bootloader will perform this check if the macro `FBL_ENABLE_VERIFY_INTEGRITY_WORD` is set. This is set by defining the macro in a user config file.



### Caution

It is only recommended to use the integrity word check during development. This is because the integrity word check is not pipelined (like the message digest check). This means that the bootloader will need to re-read all of the data programmed to flash to perform the integrity word check. This eliminates the advantages of the pipelined verification used to calculate the message digest.

## 8.8.4 Signer Info

The signer info is included as a parameter of the signed header. This applies to both application and calibration modules. This is a certificate like structure used to validate the public key that is used as part of the digital signature. The signer info contains the root signature. The bootloader uses the public key stored in the bootloader ROM to validate the root signature (e.g. authorizes that this signer info can be used to validate the digital signature).

The signer info (including the root signature) does not need to be updated each time a module is updated. The signer info is only updated upon GM's discretion. The same signer info can be used as long as GM allows.

During development, Vector provides an example signer info block. The example signer info block contains the example public key that is used to validate the digital signature. It can be used for creating signed modules using ageing the Demo\_key.

During production, the signer info will be provided by GM as part of the received signed containers.

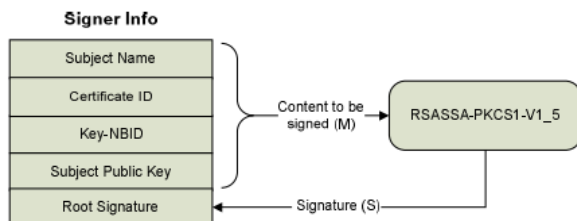


Figure 8-5 Signer Info Structure and signature calculation

## 8.8.5 Application Software – Not Before Identifier (App-NBID)

The app-NBID is a security parameter that is primarily used to prevent roll back to previous application software version [2].

The app –NBID must be stored non volatile. The initial value is generally defined to be 0x0000. Upon downloading an application module, the app –NBID stored in the application header is compared to the app –NBID stored in the bootloader. If the app –NBID in the application header is less than the app –NBID stored in the Fbl, then the module is rejected. If the app –NBID in the header is greater than the app –NBID stored in Fbl, then the NVM is updated with the new app –NBID. Checking and updating of app-NBID is bypassed with valid loaded SBAT.

**Note**

The bootloader uses the call-back functions `ApplFbINVMReadAppNBID` and `ApplFbINVMWriteAppNBID` to read and write the App-NBID. These functions are described in section 5.3 Module Validation Callbacks.

### 8.8.6 Security Key – Not Before Identifier (Key-NBID)

The Key-NBID is a security parameter that is primarily used to prevent use of a previous key [2].

The Key-NBID must be stored non volatile. The initial value is defined to be 0x0000. Upon downloading an application or calibration module, the key-NBID stored in the signer info of the header is compared to the key-NBID stored in the bootloader. If the key-NBID in the header is less than the key-NBID stored in NVM then the key (and also the module) is rejected. If the key-NBID in the header is greater than the key-NBID stored in NVM then the NVM is updated with the new key-NBID. Checking and updating of key-NBID does still happen with valid loaded SBAT.

**Note**

The bootloader uses the call-back functions `ApplFbINVMReadKeyNBID` and `ApplFbINVMWriteKeyNBID` to read and write the key-NBID. These functions are described in section 5.3 Module Validation Callbacks.

### 8.8.7 ECU ID

Gm asks you to implement a mechanism to provide a unique ECU ID per each specific ECU part. This property is crucial to maintain the security of your ECU. This is because the SBAT ticket

The layout of the required ECU ID element is outlined in your received GM specification. The bootloader provides a callback to read the ECU ID (`ApplFbINVMReadECUID`), which you need to implement according to your ECU ID storage concept. Vector does not propose any storage concept, or mechanism to provide unique numbering for each specific ECU. Depending on the used NVM solution, ECU-ID reading is either defaulted by reading from `FblHeader.ECUID` element or by reading from `NvWrapper`. Please exchange this dummy implementation.

**ECU ID**

In any case you have to choose your own strategy to implement unique ECU ID per single ECU part and remove our example implementation.

## 8.9 Programming of Unused Flash Space / Gap Fill

If gap fill is enabled in GENy (see section 4.4.2) then the bootloader will automatically call a pre-built function (FblHdrFillGaps) to fill the unused memory space. This function is designed to cover all cases and is therefore bulky and slow. It is recommended that the user disable the gap fill function in GENy and implement a custom gap fill function in simple cases. This can be done using the function ApplFblFillGaps (see section 5.3). For example, if there is only one fill region then this information can be embedded into a module (i.e. start and end address of the fill region). ApplFblFillGaps can then be implemented to simply fill this one region.

## 8.10 Partition Erase Status

Since the version 1.0 of [2] GM demands to check Partitions to be already erased before erasure. The motivation for that is to save update time. This feature is supported with FblSecHdr (fbl\_hdr.c/.h) module versions > 02.05.00.

Our implementation will initialize all partitions to “not erased” state upon reset (kFlashNotErased) within main() -> FblPreInit() ->..-> FblHdrInitPowerOn() and track erasure and programming events to the data structure logBlockPartErasedStates in order to avoid superfluous erasure (e.g. when calibration partition is downloaded after application). Erased state information is lost over reset and reinitialized after reset.

### 8.10.1 Configuration

The default configuration allows tracking of each application partitions and up to 3 associated calibration partitions (per application). The value can be modified via the macro HDR\_MAX\_TRACKED\_ERASED\_STATE\_PARTIONS (default is 4: 1 appl + 3 cal partitions).

If you want to keep the erased state information over reset, you can write information from the logBlockPartErasedStates data structure to NVM before reset within ApplFblReset() and restore the information in ApplFblStartup() (kStartupPostInit event) which is called after the above mentioned initial initialization.

**Caution**

If you intend to store partition erased state information in NVM, please check information provided by your HW-supplier. Sometimes recommendations/enforcements are given to erase directly prior to erasure.

A implementation alternative for you would be to read erased states from NVM only for production once at the beginning of an ECUs lifecycle where certain partitions are known to be erased.

## 9 Limitations

See below limitations of your FBL package

### 9.1 CG3532 ECU Security Requirements

- > The Bootloader only supports a Bootloader relevant subset of the CG3532 (defined by GM).
- > CG3532 requires the ECU to dynamically check stack bounds. This is considered hardware and configuration specific and the delivered bootloader components do not meet this requirement. It is required for the user to consider this requirement. This could be e.g. done by defining the maximum stack usage allowed somewhere during Initialization and checking the limit is adhered to regularly in a cyclically called task (ApplFblTask/ApplFblWdTrigger)

## 10 Glossary and Abbreviations

Term	Description
Address-Region	Block of consecutive data bytes. All addresses within the block contain data, there are no gaps.
API	Application Program Interface Defines the public methods within a software component that may be accessed by an application to perform certain programming tasks.
App-NBID	Application software - Not Before Identifier. A security parameter that is primarily used to selectively prevent roll back to previous application software version.
ARLE	Adaptive Run Length Encoding compression algorithm
ASCII	American Standard Code for Information Interchange Defines the numeric representation of the English alphabet, plus several special and non-printable characters.
CAN	Controller Area Network
CPU	Central Processing Unit
CS	Check-Sum Refers to module checksum field of File-Header defined by GM.
DCID	Data Compatibility Identifier This field is also referred to as the BCID (Bootloader Compatibility Identifier), and as the CCID (Calibration Compatibility Identifier).
DLL	Data Link Layer Provides software interface to the CAN hardware (also known as the CAN driver).
DLS	Design Level Suffix Refers to module revision code in File-Header defined by GM.
DPS	Development Programming System. PC based Download Tool created by General Motors.
ECU	Electronic Control Unit
EEPROM	Electrically Erasable Programmable Read-Only Memory EEPROM is a type of non-volatile memory. This type of memory is similar to flash memory, but may be erased and written one byte at a time.
FBL	Flash Bootloader. The FBL is a software application independent of the Operating Software. It is responsible for downloading and programming the Operating Software and/or related data modules into an ECU. The FBL is usually in protected memory, where it cannot be erased.
Flash-Driver	File containing the algorithms used to erase and write to flash memory. GM's specifications refer to the driver as the <i>Programming Routines</i> .
Download Tool	Any Hardware/Software system capable to connecting to the CAN bus for the purpose of reprogramming the Operating Software and/or Calibration



	or other data of an ECU. For example, Vector's <i>vFlash</i> and GM's <i>DPS</i> programs.
File-Header	Refers to file header defined by GM. All downloadable modules require a header. See GB6002
GBF	Generic Binary File GBF files cannot be read using text editors. The provided hexview tool can do this instead. The GBF file type is compatible for use with GM's DPS tool (within an SPS archive file).
GM	General Motors
HIS	Hersteller Initiative Software Refers to an effort made by a group of manufacturers to standardize aspects of software development. The FBL bases the low-level Memory I/O (e.g. the Flash Driver) APIs on this work. For additional information, see reference [5].
ISO	International Organization for Standardization
ISR	Interrupt Service Routine. Any software intended to be executed immediately upon receipt of an asynchronous event, thus interrupting whatever task the ECU was performing at the time of the event. In general, special restrictions apply to the actions an ISR may take.
KBPS	Kilo-Bits per Second Transfer rate of data across the CAN bus. Also known as the <i>Baud Rate</i> .
Key-NBID	Security key – Not Before Identifier. A security parameter that is primarily used to prevent use of a previous key.
MID	Module-ID Refers to module identification field of File-Header defined by GM.
MIM	Multiple-Identity-Module. Some ECUs running common Operating Software may be used for multiple purposes within the vehicle. For example, the same ECU might be used in all doors. Such modules must configure themselves at startup to use unique diagnostic-identifiers and CAN ids.
Module	Any data file that may be transferred to an ECU via the Bootloader Software.
NBID	Not Before Identifier. For details on the concept refer to GB6002
NVM	Non Volatile Memory. A memory location that keeps its content permanently.
OEM	Original Equipment Manufacturer
Operating Software	This is the application program responsible for implementing the tasks that an ECU should perform. It is also known as the Application, Application Software, Operational Software, Operating System, and Opcode.
PCI	Protocol-Control-Information Defines the type of message being exchanged by the Transport-Protocol layer.
PEC	Programming Error Code. A 2 byte RAM location used to store specific error code related to a failed programming step during the

	programming session.
PLL	Phase Locked Loop Electronic circuit used to maintain accuracy in an ECU's clock and timing hardware.
PMA	Product Memory Address Refers to the starting address of an Address Region within the Fbl.
PSI	Programmed State Indicator Mechanism to determine if a logical partition is programmed with valid content. Interchangeable with presence pattern in this document.
RAM	Random Access Memory
RCR-RP	A special type of negative response indicating Request Correctly Received, Response Pending.
ROM	Read Only Memory
SBA	Signature-Bypass Authorization ticket. A data file that the bootloader rely on to determine whether to set or clear the SBI flag.
SBI	Signature-Bypass Indicator flag. A flag which indicates whether signature and message digest verification shall be enforced or not.
Sector-Size	The number of bytes that are erased when an erase command is issued to a non-volatile device. This number must be a power of two (e.g. 64, 128, 256, etc). The sectors on a non-volatile device are not necessarily all the same size. Many devices allow multiple sectors to be erased with a single command.
Segment-Size	The number of bytes that must be written when a write command is issued to a non-volatile device. Most devices allow a multiple of the segment-size to be specified in write commands. The segment-size is expected to be the same for all sectors on a device. The FBL expects the value to be a power of two.
SIP	Software Integration Package Refers to all files contained in the delivery of Vector Software.
SPS	Service Programming System
SWMI	Software Module Identification Refers to module part-number field in File-Header defined by GM.
TP	Transport Protocol
Utility file	A file that contains the programming instructions for an ECU that is capable of being programmed via SPS.
WDBI	Write Data By Identifier

## 11 Contact

Visit our website for more information on

- > News
- > Products
- > Demo software
- > Support
- > Training data
- > Addresses

**[www.vector.com](http://www.vector.com)**