Issue Report

License Number	Customer
CBD1701035	Nexteer Automotive (Suzhou) Co. Package: FBL Vector SLP3 - CANfbl license for the project EPS for OEMs without manufacturer specific requirements

Maintenance Expiry Date

2018-05-01

SIP Version

07.03.01

SLP	Delivery Number
FBL Vector SLP3	D00

Report Creation Date

2018-03-27

Contact

In case of questions or the need for an update of the basic software delivery, please contact Support@vector.com or your Vector contact person.

Table of Contents

1. Introduction

1.1 Resolving Issues

Reported issues are not automatically fixed with the next update delivery.
If a reported issue shall be fixed, please contact Vector agree on the issues that can be fixed with upcoming deliveries.
Please note that Vector may fix issues without explicit request.

1.2 Issue Classification

This Issue Report provides issues that have been detected since the last report. The issues have been classified to facilitate the assessment of their impact:

The chapter 'New Issues' lists issues that have been detected since the last report and which could not be excluded based on the use-case defined in the questionnaire. The issues are classified as follows:

- **Safety Related Issues:** Safety related issues have impact on the functional safety of the software module. If this issue interferes with the functional safety concept of the ECU, this module (or module configuration) must not be used for serial production in a safety-related project. The effect of the issue to the ECU functionality and functional safety has to be analyzed by the user as the software usage and its configuration is not known by Vector. The risk of change has also to be taken into account.
- **Runtime Issues without Workaround:** Runtime issues without a workaround require an update of the software delivery in case the issue affects the ECU overall functionality. The effect of an issue to the ECU functionality has to be analyzed by the customer as the software usage and its configuration is not known by Vector. The risk of change has also to be taken into account.
- **Runtime Issues with Workaround:** It is not recommended to update a delivery due to a runtime issue with a documented workaround. The effect of an issue to the ECU functionality has to be analyzed by the user as the software usage and its configuration is not known by Vector. The risk of change has also to be taken into account.
- **Not Released Functionality:** Not released functionalities (BETA) are either complete software modules or features in the software module that have not yet passed a complete development cycle (they are e.g. not or only partly tested). If a BETA issue ticket affects a complete software module, the software module must not be used for serial production. If a BETA issue ticket affects a feature in the software module, the user has to ensure that all BETA features are disabled as indicated for the serial production release of the ECU.
- **Apparent Issues:** Apparent issues are detected immediately when using the software module. If an issue does not show up while working with the software module, the ECU project is not affected by the issue. Apparent issues may or may not have workarounds.
- **Compiler Warnings:** As a service we also provide the known compiler warnings. The occurrence of a compiler warning may depend on the used software module configuration and compiler settings.

The chapter 'New Issues for Information' lists issues that are not relevant for the use-case that has been documented in the questionnaire provided to Vector. The issues may, however, be relevant for other use-cases. Additionally, issues that have been accepted or are tolerated by the OEM (as defined in the questionnaire) are reported here.

2. New Issues

2.1 Safety Relevant Issues

Safety related issues have impact on the functional safety of the software module. If this issue interferes with the functional safety concept of the ECU, this module (or module configuration) must not be used for serial production in a safety-related project.

The effect of the issue to the ECU functionality and functional safety has to be analyzed by the user as the software usage and its configuration is not known by Vector. The risk of change has also to be taken into account.

No issue to be reported.

2.2 Runtime Issues without Workaround

Runtime issues without a workaround require an update of the software delivery in case the issue affects the ECU overall functionality. The effect of an issue to the ECU functionality has to be analyzed by the customer as the software usage and its configuration is not known by Vector. The risk of change has also to be taken into account.

No issue to be reported.

2.3 Runtime Issues with Workaround

It is not recommended to update a delivery due to a runtime issue with a documented workaround. The effect of an issue to the ECU functionality has to be analyzed by the user as the software usage and its configuration is not known by Vector. The risk of change has also to be taken into account.

Index

ESCAN00097115	Buffer overflow during gap fill operation
Component@Subcomponent:	FblLib_Mem@Implementation
First affected version:	3.01.00
Fixed in versions:	

Problem Description:
What happens (symptoms):

A write to the internal buffer holding the fill pattern for the gap fill operation is outside the array bounds.
This can cause other variables to be overwritten, resulting in undefined behavior.

When system check is enabled (FBL_ENABLE_SYSTEM_CHECK) the corrupted buffer will be detected afterwards and a general error will be issued.

When does this happen:

During the gap fill operation, e.g. during a RequestTransferExit.

In which configuration does this happen:

When all of the following conditions apply:

- Gap fill is enabled (FBL_MEM_ENABLE_GAP_FILL)
- Gap fill segmentation is smaller than the memory segment size (FBL_MEM_GAP_FILL_SEGMENTATION < FBL_MEM_SEGMENT_SIZE)
Typically the gap fill segmentation is equal to the write segmentation (FBL_MEM_WRITE_SEGMENTATION).

Resolution Description:
Workaround:

Ensure the gap fill segmentation is equal to or larger than the memory segment size (FBL_MEM_GAP_FILL_SEGMENTATION >= FBL_MEM_SEGMENT_SIZE).
Typicall this can be achieve by setting the WriteSegmentation in the configuration tool to at least to the size of the greatest SegmentSize of your memory drivers.

Resolution:

The described issue is corrected by modification of all affected work-products.

2.4 Not Released Functionality

Not released functionalities (BETA) are either complete software modules or features in the software module that have not yet passed a complete development cycle (they are e.g. not or only partly tested). If a BETA issue ticket affects a complete software module, the software module must not be used for serial production. If a BETA issue ticket affects a feature in the software module, the user has to ensure that all BETA features are disabled as indicated for the serial production release of the ECU.

No issue to be reported.

2.5 Apparent Issues

Apparent issues are detected immediately when using the software module. If an issue does not show up while working with the software module, the ECU project is not affected by the issue. Apparent issues may or may not have workarounds.

Index

ESCAN00078508	[depends on derivative] Illegal flash block table configuration cause unintended block erase FblDrvFlash_Rh850Rv40His@Impl_Base
ESCAN00081436	Using FlashDriver_SetResetVector() might cause exception FblDrvFlash_Rh850Rv40His@Impl_Base
ESCAN00086590	Obsolete generated code in WrapNv_cfg.c does not compile SysService_WrapperNv@GenTool_Geny
ESCAN00090094	FblCanWakeup() does not allow to enable Can clock again FblDrvCan_Rh850RscanCrx@Implementation
ESCAN00095072	ApplFblSetModulePresence() Cannot write presence pattern to multiple memory devices with different erased values FblKbApi@Implementation
ESCAN00096436	The "divide clock frequency by 8" option of the bustiming configuration dialog must not be active if the feature "CanIsoCanFdCapable" is used. Hw__baseCpuCan@GenTool_Geny
ESCAN00097060	Compiler error: Unresolved symbol: secCrcZeroValue SysService_SecModHis@Impl_Verification
ESCAN00097741	Potential buffer overflow in flashCode buffer FblDiag_14229_Uds2@Implementation
ESCAN00098666	Negative values are not accepted in arguments FblTool_Hexeditor_Hexview@Application_Exe
ESCAN00098670	Public Key Hash is overwritten when merging VBF files FblTool_Hexeditor_Hexview@Application_Exe
ESCAN00098693	'sw_signature written to VBF-file with no content FblTool_Hexeditor_Hexview@Application_Exe

ESCAN00078508	[depends on derivative] Illegal flash block table configuration cause unintended block erase
Component@Subcomponent:	FblDrvFlash_Rh850Rv40His@Impl_Base
First affected version:	0.90.00
Fixed in versions:	

Problem Description:

What happens (symptoms):

If the code flash contains gaps where no flash exists and the user configure a flash block in this area, the flash driver will erase the next valid flash block (first block with start address bigger than the illegal configured block).

When does this happen:

Always and immediately

In which configuration does this happen:

---

all configurations, but not all derivatives

Note: The gap between user area and extended user area is not relevant. Until now, no known derivative is affected by this issue!

Resolution Description:

Workaround:

Well configured flash block table, which corresponds to the real flash block structure.

Resolution:

The described issue is corrected by modification of all affected work-products.

ESCAN00081436	Using FlashDriver_SetResetVector() might cause exception
Component@Subcomponent:	FblDrvFlash_Rh850Rv40His@Impl_Base
First affected version:	1.02.00
Fixed in versions:	

Problem Description:

What happens (symptoms):

When using FlashDriver_SetResetVector() an exception occurs.

When does this happen:

When code called from wdTriggerFct (typically FblLookForWatchdog()) is not located in RAM. This may apply e.g. to the Communication Wrapper task functions.

In which configuration does this happen:

---

if FLASH_ENABLE_SET_RESETVECTOR_API is enabled.

Resolution Description:

Workaround:

Either manually handle memDrvDeviceActive in the updater or locate any code referenced by FblLookForWatchdog() in RAM

Resolution:

None.

ESCAN00086590	Obsolete generated code in WrapNv_cfg.c does not compile
Component@Subcomponent:	SysService_WrapperNv@GenTool_Geny
First affected version:	1.00.00
Fixed in versions:	

Problem Description:

What happens (symptoms):

Obsolete generated code in WrapNv_cfg.c does not compile, file should no longer be generated.

When does this happen:

Always and immediately

In which configuration does this happen:

Any configuration

Resolution Description:

Workaround:

The C file is not needed. Do not compile this file and try to link it to your bootloader.

Resolution:

The described issue is corrected by modification of all affected work-products.

ESCAN00090094	FblCanWakeup() does not allow to enable Can clock again
Component@Subcomponent:	FblDrvCan_Rh850RscanCrx@Implementation
First affected version:	1.02.00
Fixed in versions:	

Problem Description:

What happens (symptoms):

After call to FblCanSleep and wakup call to FblCanWakeUp, no CAN communicaton is possible any more.

When does this happen:

When waking up again via FblCanWakeUp.

In which configuration does this happen:

Configurations that support Can low power mode (FBL_ENABLE_SLEEPMODE defined).

Resolution Description:

ESCAN00090094	FblCanWakeup() does not allow to enable Can clock again

Workaround:

---

1. Replace calls to FblCanWakeUp() by calls to ApplFblCanWakeUp() in user callback context.
2. Add code to ApplFblCanWakeUp() to wake up again:

```
void ApplFblCanWakeUp( void )
{
 /* Clear error flags */
 Can->ChCtrl[kFblCanChannel].EF &= FblInvert32Bit(kCanEfMask);

 /* Clear rx full pending buffers 0 - 31*/
 Can->CRBRCF[0] = 0;

 /* Set channel reset mode (currently in stop or reset mode) */
 CanLL_ModeReq_Phys(kFblCanChannel,kCanResetMode);
 while ((!CanLL_ModeCheck_Phys(kFblCanChannel,kCanResetMode)))
 {
 ;
 }

 /* Switch to operation mode (and wait till it is reached) */
 CanLL_ModeReq_Phys(kFblCanChannel,kCanOperationMode);

 while (!CanLL_ModeCheck_Phys(kFblCanChannel,kCanOperationModeCheck))
 {
 ;
 }
}
```

3. Define these macros so that they are available within ApplFblCanWakeUp():

```
 /**< Requests a on a physical channel */
#define CanLL_ModeReq_Phys(pch,mode) (Can->ChCtrl[pch].CR = ((Can->ChCtrl[pch].CR &
kCanModeMask) | (mode)))
#define CanLL_ModeCheck_Phys(pch,mode) ((Can->ChCtrl[pch].SR & kCanModeBits) == ((mode)
& kCanModeBits))
```

Resolution:

The described issue is corrected by modification of all affected work-products.

ESCAN00095072	ApplFblSetModulePresence() Cannot write presence pattern to multiple memory devices with different erased values
Component@Subcomponent:	FblKbApi@Implementation
First affected version:	1.00.00
Fixed in versions:	

Problem Description:

What happens (symptoms):

ApplFblSetModulePresence() errantly returns kFblFailed when it has written a valid presence pattern. Download will be halted.

When does this happen:

During the validation of a block of memory down loaded to secondary device type with a different erased value than primary memory

In which configuration does this happen:

FBL_ENABLE_PRESENCE_PATTERN
AND
FBL_ENABLE_MULTIPLE_MEM_DEVICES
AND
FBL_FLASH_DELETED is a different value than the deleted value of the secondary device driver.

Resolution Description:

Workaround:

ApplFblSetModulePresence() has to be adapted according to the erased code.

Resolution:

The described issue is corrected by modification of all affected work-products.

ESCAN00096436	The "divide clock frequency by 8" option of the bustiming configuration dialog must not be active if the feature "CanIsoCanFdCapable" is used.
Component@Subcomponent:	Hw__baseCpuCan@GenTool_Geny
First affected version:	2.30.00
Fixed in versions:	2.31.02, 3.00.01

Problem Description:

What happens (symptoms):

The "divide clock frequency by 8" option of the bustiming configuration dialog is active allthough the feature "CanIsoCanFdCapable" is used. This combination is not supported by the hardware and results into incorrect bustiming settings!

When does this happen:

This happens always but only under specific circumstances

In which configuration does this happen:

"CanIsoCanFdCapable" is selected

AND

"Non ISO Operation" is selected
OR
"Protocol Exception Disable" is selected

Resolution Description:

Workaround:

No workaround available.

Resolution:

The described issue is corrected by modification of all affected work-products.

ESCAN00097060	Compiler error: Unresolved symbol: secCrcZeroValue
Component@Subcomponent:	SysService_SecModHis@Impl_Verification
First affected version:	2.06.00
Fixed in versions:	2.08.01

Problem Description:

What happens (symptoms):

Global secCrcZeroValue is not available, linkage therefore fails.

When does this happen:

The error is issued by the compiler during linkage.

In which configuration does this happen:

If no CRC is present.

Resolution Description:

Workaround:

Create missing variable in fbl_ap.c "Globals" section:

```
/
**********************************************************************************

 * GLOBAL DATA

**********************************************************************************


V_MEMROM0 V_MEMROM1 SecM_CRCType V_MEMROM2 secCrcZeroValue = 0u;
```

Resolution:

The described issue is corrected by modification of all affected work-products.

ESCAN00097741	Potential buffer overflow in flashCode buffer
Component@Subcomponent:	FblDiag_14229_Uds2@Implementation
First affected version:	7.00.00
Fixed in versions:	7.01.01

Problem Description:
What happens (symptoms):

Data located behind the flashCode buffer may be overwritten.

When does this happen:

When the flash driver is initialized

In which configuration does this happen:

If configuration switch FBL_DIAG_ENABLE_FLASHDRV_ROM is set (either driver from ROM only or optional flash driver download).

Resolution Description:
Workaround:

Verify that all static flash driver images are smaller than the configured buffers. This has to be done by a manual review before the ECU software is released.

Resolution:

The described issue is corrected by modification of all affected work-products.

ESCAN00098666	Negative values are not accepted in arguments
Component@Subcomponent:	FblTool_Hexeditor_Hexview@Application_Exe
First affected version:	1.10.01
Fixed in versions:	

Problem Description:
What happens (symptoms):

A negative offset cannot be applied when merging a file through commandline

When does this happen:

When using argument values, e.g. merging a file with offset (/MT:merge.hex;-0x1000)

In which configuration does this happen:

This happens in all configurations.

Resolution Description:
Workaround:

Use two's complement instead of '-' in front of the value.

Resolution:

The described issue is corrected by modification of all affected work-products.

ESCAN00098670	Public Key Hash is overwritten when merging VBF files
Component@Subcomponent:	FblTool_Hexeditor_Hexview@Application_Exe
First affected version:	1.10.00
Fixed in versions:	

Problem Description:
What happens (symptoms):

The Public_Key_Hash is not generated when merging two VBF files.
OR
When loading a VBF file and performing some operations, then writing the VBF file back, the PUBLIC_KEY_HASH is not generated.

When does this happen:

This happens when the associated INI file does not contain a PUBLIC_KEY_HASH entry.

In which configuration does this happen:

Always when loading an existing VBF into Hexview, an output is generated and no INI file is available resp. the associated INI file doesn't contain a public key hash.

Resolution Description:
Workaround:

Use an INI for the VBF that contains a PUBLIC_KEY_HASH value.

Resolution:

The described issue is corrected by modification of all affected work-products.

ESCAN00098693	'sw_signature written to VBF-file with no content
Component@Subcomponent:	FblTool_Hexeditor_Hexview@Application_Exe
First affected version:	1.10.00
Fixed in versions:	

Problem Description:
What happens (symptoms):

The key "sw_signature" is written to VBF without key value.

When does this happen:

When insufficient information is provided through the INI-file to generate a valid signature and the VBF version allows to write signatures.

In which configuration does this happen:

Always.

Resolution Description:
Workaround:

No workaround available.

Resolution:

The described issue is corrected by modification of all affected work-products.

2.6 Compiler Warnings

As a service we also provide the known compiler warnings. The occurrence of a compiler warning may depend on the used software module configuration and compiler settings.

Index

ESCAN00069885	Compiler warning: statement is unreachable
Component@Subcomponent:	FblTp_Iso@Implementation
First affected version:	3.12.00
Fixed in versions:	

Problem Description:

What happens (symptoms):

Compiler warns for a code statement which will never be executed.

When does this happen:

The warning is issued by the compiler during compilation of the code in case the configuration is as described below.

In which configuration does this happen:

Queued Requests enabled (FBL_TP_ENABLE_QUEUED_REQUESTS)

Resolution Description:

Workaround:

No workaround available.

Resolution:

The described issue is corrected by modification of all affected work-products.

ESCAN00077761	Compiler warning: Conversion from integer to smaller pointer
Component@Subcomponent:	SysService_SecModHis@Impl_Verification
First affected version:	2.00.00
Fixed in versions:	

Problem Description:
What happens (symptoms):

Compiler warns: Conversion from integer to smaller pointer

Example for IAR compiler:
pWorkspace = (V_MEMRAM1 SEC_VERIFY_CLASS_CCC_WORKSPACE_TYPE V_MEMRAM2 V_MEMRAM3 *)pVerifyParam->currentHash.sigResultBuffer;
D:\usr\usage\Delivery\CBD14x\CBD1400332\D01\external\BSW\SecMod\Sec_Verification.c",1335
Warning[Pe1053]: conversion from integer to smaller pointer

When does this happen:

The warning is issued by the compiler during compilation of the code in case the configuration is as described below.

In which configuration does this happen:

Always.

Resolution Description:
Workaround:

No workaround available.

Resolution:

The described issue is corrected by modification of all affected work-products.

ESCAN00083332	Compiler warning: Wrong spelling of include SecM_Inc.h in SecM_Par.*
Component@Subcomponent:	SysService_SecModHis@GenTool_Geny
First affected version:	1.03.00
Fixed in versions:	

Problem Description:

What happens (symptoms):

Compiler warns for a differently spelled file name.

When does this happen:

The warning is issued by the compiler during compilation of the code in case the configuration is as described below.

In which configuration does this happen:

Any configuration that checks the case of includes.

Resolution Description:

Workaround:

If your operating system has case sensitive file names you can create a SecM_inc.h which includes a SecM_Inc.h.

Resolution:

The described issue is corrected by modification of all affected work-products.

ESCAN00087058	Compiler warning: Condition is always false
Component@Subcomponent:	FblTp_Iso@Implementation
First affected version:	2.00.00
Fixed in versions:	

Problem Description:

What happens (symptoms):

Compiler warns for "condition is always false": This may happen depending on configuration

When does this happen:

The warning is issued by the compiler during compilation of the code in case the configuration is as described below.

In which configuration does this happen:

It happens when
FBL_TP_ENABLE_CONFIRMATION_INTERRUPT
is set.

Hint:

The compiler warning is known and has been analyzed thoroughly for its impact on the code.

Resolution Description:

Workaround:

The warning can be ignored because the issue results in additional code only.

Resolution:

The described issue is corrected by modification of all affected work-products.

ESCAN00092073	Compiler warning: condition is always true
Component@Subcomponent:	SysService_SecModHis@Impl_SeedKey
First affected version:	3.01.00
Fixed in versions:	

Problem Description:

What happens (symptoms):

Compiler: Tasking 3.0r3:
c166 W549: ["../../../BSW/SecMod/Sec_SeedKey.c" 370/19] condition is always true

```
SecM_StatusType SecM_GenerateSeed( V_MEMRAM1 SecM_SeedType V_MEMRAM2 V_MEMRAM3
* seed )
{

 /* Generate pseudo random numbers */
 result = SEC_PRNG_GENERATE_RANDOM(SEC_PRNG_POOL, pRandom, SEC_WORD_TYPE_SIZE);
<-------------------- SecM_GenerateRandomLcg () returns always SECM_OK

 if (SECM_OK == result) <---------- always true
 {
 /* Generate pseudo random numbers */
 result = SEC_PRNG_GENERATE_RANDOM(SEC_PRNG_POOL, pRandom, SEC_WORD_TYPE_SIZE);
 pBaseSeed->seedY = SecM_GetInteger(SEC_WORD_TYPE_SIZE, pRandom);

 }
}
```

When does this happen:

The warning is issued by the compiler during compilation of the code in case the configuration is as described below.

In which configuration does this happen:

When utilized random number generator always succeeds and therefore always returns SECM_OK.

Resolution Description:

Workaround:

No workaround available.

Resolution:

The described issue is corrected by modification of all affected work-products.

ESCAN00092074	Compiler warning: condition is always false
Component@Subcomponent:	SysService_SecModHis@Impl_SeedKey
First affected version:	3.01.00
Fixed in versions:	

Problem Description:

What happens (symptoms):

Compiler: Tasking 3.0r3:
c166 W549: ["../../../BSW/SecMod/Sec_SeedKey.c" 221/18] condition is always false

```
#define SEC_WORD_TYPE_SIZE 4u

SecM_StatusType SecM_GenerateSeed( V_MEMRAM1 SecM_SeedType V_MEMRAM2 V_MEMRAM3
* seed )
{
result = SEC_PRNG_GENERATE_RANDOM(SEC_PRNG_POOL, pRandom, SEC_WORD_TYPE_SIZE);
<---------
}


static SecM_StatusType SecM_GenerateRandomLcg( V_MEMRAM1 SecM_ByteType V_MEMRAM2
V_MEMRAM3 * pRandom, SecM_LengthType length )
{

 byteCount = length;

 if (byteCount > SEC_WORD_TYPE_SIZE)<------------------- always false since we always pass
"SEC_WORD_TYPE_SIZE"
 {
 byteCount = SEC_WORD_TYPE_SIZE;
 }

}
```

When does this happen:

The warning is issued by the compiler during compilation of the code in case the configuration is as described below.

In which configuration does this happen:

For all configurations where LCG random number generator is used and seed length doesn't exceed size of word type (32 bit / 4 byte).

Resolution Description:

Workaround:

No workaround available.

Resolution:

The described issue is corrected by modification of all affected work-products.

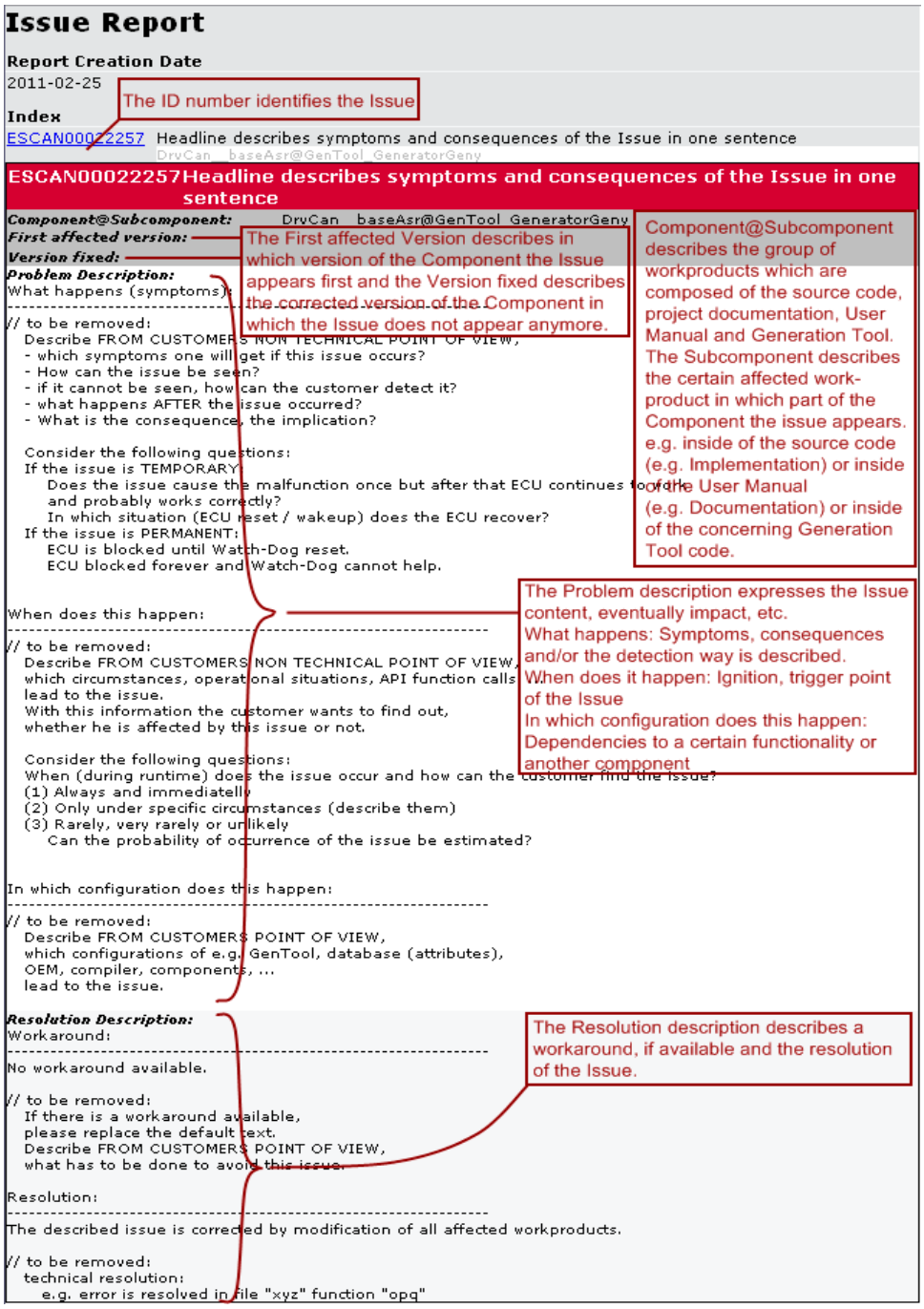
3. New Issues for Information

Issues which should not have an effect on the usage of the license as the issues are relevant for use cases other than those defined in the questionnaire. The list contains issues that have been detected since the last report.

Issues listed in this section are not relevant for the use case that has been documented in the questionnaire provided to Vector. However, the issues may be relevant for other use cases. Also issues that have been accepted or are tolerated by the OEM (as defined in the questionnaire) are reported here.

No issue to be reported.

4. Report Legend



5. 3rd Party Software Issues

This issue report does not include issues of 3rd party software. If 3rd party software was included in the SIP, the documentation of the issue reporting process is included in the SIP: .\Doc \DeliveryInformation\IssueHandling_<Name>.pdf. Please follow the given instructions.

6. Quality Management Contact

Quality Management
Productline Embedded Software (PES)

Vector Informatik GmbH
Ingersheimer Str. 24
D-70499 Stuttgart

Phone: +49 711 80670-3700
Fax: +49 711 80670-399
eMail: QualityPES@vector.com