**RESTRICTED ACCESS**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **DISTRIBUTION :** | **Firm** | **To** | **Ref** | **Copies** | **1st page** | **e-mail** |
|  | FCE | Xavier Christmann, Claude Redon, Adel Bassaid | 8 |  |  |  |
|  | FCE | Hamza Zetti, Lory Médas, Sabrine Bouazizi, Wail Amri, Kérima Adjadi, Mickael Pastor, Aki Saito | 10 |  |  |  |
|  | RBE | Mihai Ianos, Daniel Andris, | 2 |  |  |  |
|  |  |  |  |  |  |  |
|  | FCE | Secretary ship | 1 |  |  |  |

**SW Architecture Design & Interface Description :**

**SFR sw UNIT**

OBJECT: This document is the description of the design & interfaces for *SFR* SW unit.

SUMMARY: This document provides a high-level view of the *SFR* SW unit. The inputs of this document are provided by the software requirement. It is linked to the DAIMLER\_MMA\_SWarchitectureDesignInterfaceDescription document.

CONCLUSION: Applicable from R01.0 SW release

**THIS DOCUMENT CONTAINS HIDDEN TEXT**

EVOLUTION OF THE DOCUMENT

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Issue** | **Date** | | **Author** | | **Motive and nature of the modifications** | |
| 1 | 31/08/2016 | | C. Redon | | First release (extract from the full PP4G architecture document) | |
| 2 | 26/09/2016 | | C. Redon | | Specification of the link between the belt function cycles and the corresponding RTE data (shared between BFS and the decision algorithms). | |
| Start extended description based on mainstream document | | | | | | |
| 1.1.1.2 | 15/07/2019 | | A. Vaché | | Update traceability to match PP4G extended platform requirements IDs | |
| 1.1.1.3 | 08/08/2019 | | A. Vaché | | Solve some traceability issues highlighted by reqtify | |
| 1.1.1.4 | 18/11/2019 | | W. AMRI | | Add missing traceability. | |
| 1.1.1.5 | 26/11/2019 | | W. AMRI | | Update template information | |
| 1.1.1.6 | 24/01/2020 | | A. Vaché | | Add requirement related to missing parameter | |
| Start DAI MMA description based on extended document | | | | | | |
| 1.1.1.6.1 | | 06/01/22 | | 1. Negrea | | First revision |
| 1.1.1.6.2 | | 17/03/22 | | 1. Negrea | | Update according to SRM |
| 1.1.1.6.3 | | 18/03/22 | | 1. Negrea | | Update according to SRM - 2 |

This document contains **15** pages.

**CONTENTS**

1. Documentation 5

1.1. Upper Level Relevant Documents 5

1.2. Design interface description Documents 6

1.3. Freescale Documents 7

1.4. Tier2 Documents 8

1.5. HW Datasheet 8

1.6. Other Documents 8

1.7. Glossary And Definition 9

2. Description 10

3. Technical functions 11

3.1. To start/stop a releasing cycle after a tensioning cycle (nominal case) 11

4. Runnables 12

4.1. SFR\_runStandardFunctionRecovery 12

4.1.1. Definition 12

4.1.2. Data flow / Parameters 13

4.1.3. Called functions 15

5. MCU resources 15

**TABLE OF FIGURES**

[**Figure 2: Sfr - Data flow description of the hard releasing activation / interrupt based on vehicle signals** 12](#_Toc98419737)

# Documentation

## Upper Level Relevant Documents

This section presents all the documents needed to write the software architecture design document.

|  |  |  |  |
| --- | --- | --- | --- |
| Nb | **Document** | **Reference** | **Company** |
|  | TF-A: To Manage the power supply | /RevAS/30\_DES\_Requirements/Technical Functions/  DES\_TF\_A\_To\_Manage\_The\_Power\_Supply | RBE/FCE |
|  | TF-B: To Manage the communication | /RevAS/30\_DES\_Requirements/Technical Functions/  DES\_TF\_B\_To\_Manage\_The\_Communication | RBE/FCE |
|  | TF-C: To Secure PP ECU functioning using Pictus MCU | /RevAS/30\_DES\_Requirements/Technical Functions/  DES\_TF\_C\_To\_Secure\_PP\_ECU\_Functioning\_Pictus | RBE/FCE |
|  | TF-D: To Program MCU | /RevAS/30\_DES\_Requirements/Technical Functions/DES\_TF\_D\_To\_Program\_MCU | RBE/FCE |
|  | TF-E: To Manage Diagnostic Requests | /RevAS/30\_DES\_Requirements/Technical Functions/DES\_TF\_E\_To\_Manage\_Diagnostic\_Requests | RBE/FCE |
|  | TF-F: To Perform Measurements | /RevAS/30\_DES\_Requirements/Technical Functions/DES\_TF\_F\_To\_Perform\_Measurements | RBE/FCE |
|  | TF-G: To Drive the Motor | /RevAS/30\_DES\_Requirements/Technical Functions/DES\_TF\_G\_To\_Drive\_the\_Motor | RBE/FCE |
|  | TF-H: To Perform Autotests | /RevAS/30\_DES\_Requirements/Technical Functions/DES\_TF\_H\_To\_Perform\_Autotests | RBE/FCE |
|  | TF-I: To Manage the Failure | /RevAS/30\_DES\_Requirements/Technical Functions/DES\_TF\_I\_To\_Manage\_The\_Failure | RBE/FCE |
|  | TF-J: To Manage NVM - NVP (Non Volatile Parameters) | /RevAS/30\_DES\_Requirements/Technical Functions/DES\_TF\_J\_To\_Manage\_NVM | RBE/FCE |
|  | TF-K: To Ensure ECU Protection and Integration | /RevAS/30\_DES\_Requirements/Technical Functions/DES\_TF\_K\_To\_Ensure\_ECU\_Protection\_And\_Integration | RBE/FCE |
|  | TF-L: To Ensure ECU Integration in Environment EMC ESD | /RevAS/30\_DES\_Requirements/Technical Functions/DES\_TF\_L\_To\_Ensure\_ECU\_Integration\_In\_Environment\_EMC\_ESD | RBE/FCE |
|  | TF-M: To generate time base | /RevAS/30\_DES\_Requirements/Technical Functions/DES\_TF\_M\_To\_Generate\_Time\_Base | RBE/FCE |
|  | TF-N: To evaluate belt data | /RevAS/30\_DES\_Requirements/Technical Functions/DES\_TF\_N\_To\_Evaluate\_Belt\_Data | RBE/FCE |
|  | TF-O: To schedule the SW | /RevAS/30\_DES\_Requirements/Technical Functions/DES\_TF\_O\_To\_Run\_SW | RBE/FCE |
|  | TF-P: To handle network management | /RevAS/30\_DES\_Requirements/Technical Functions/DES\_TF\_P\_To Handle\_Network\_Management | RBE/FCE |
|  | TF-Q: To Provide Data For Expertise | /RevAS/30\_DES\_Requirements/Technical Functions/DES\_TF\_Q\_To\_Provide\_Data\_For\_Expertise | RBE/FCE |
|  | TF-R: To Decide Belt Function Execution | /RevAS/30\_DES\_Requirements/Technical Functions/DES\_TF\_R\_To\_Decide\_Belt\_Function\_Execution | RBE/FCE |
|  | TF-S: To drive the boost | /RevAS/30\_DES\_Requirements/Technical Functions/DES\_TF\_S\_To\_Drive\_Boost | RBE/FCE |
|  | TF-X: To generate time base | /RevAS/30\_DES\_Requirements/Technical Functions/DES\_TF\_M\_To\_Generate\_Time\_Base | RBE/FCE |

## Design interface description Documents

This section presents all the documents that are linked to this software architecture design document.

Note: All links are related to S:\drive, to have them functional, please mount the S:\drive on your Audi Tr6 extended platform sandbox.

|  |  |  |  |
| --- | --- | --- | --- |
| Nb | **Document** | **Reference** | **Company** |
|  | EEPROM parameters | SBE\_4G\_NVP\_layout.xls | RBE/FCE |
|  | Design Interface description of AdcIf | N/A | RBE/FCE |
|  | Design Interface Description of Auto Tests Manager | N/A | RBE/FCE |
|  | Design Interface Description of Belt Function Decision | N/A | RBE/FCE |
|  | Design Interface Description of Belt Function Execution | [BFE - Design Interface Description.docx](file:///S:\Architectures\Application\Description\Associated_Documents\BFE%20-%20Design%20Interface%20Description%20.docx) | RBE/FCE |
|  | Design Interface Description of Belt Function Selection | [BFS - Design Interface Description.docx](file:///S:\Architectures\Application\Description\Associated_Documents\BFS%20-%20Design%20Interface%20Description%20.docx) | RBE/FCE |
|  | Design Interface Description of Belt Movement Monitoring | N/A | RBE/FCE |
|  | Design Interface Description of Belt Parking Algorithm | N/A | RBE/FCE |
|  | Design Interface Description of Belt Slack Reduction | N/A | RBE/FCE |
|  | Design Interface Description of Basic Software Manager | N/A | RBE/FCE |
|  | Design Interface Description of Basic Software Manager Interface | N/A | RBE/FCE |
|  | Design Interface Description of Can Tranceiver Interface | N/A | RBE/FCE |
|  | Design Interface Description of Communication Interaction Layer | [CIL - Design Interface Description.docx](file:///S:\Architectures\Application\Description\Associated_Documents\CIL%20-%20Design%20Interface%20Description.docx) | RBE/FCE |
|  | Design Interface Description of Diagnostic Communication Manager Interface | N/A | RBE/FCE |
|  | Design Interface Description of Diagnostic Event Manager Interface | N/A | RBE/FCE |
|  | Design Interface Description of DiagOnCAN services management | [DIA - Design Interface Description.docx](file:///S:\Architectures\Application\Description\Associated_Documents\DIA%20-%20Design%20Interface%20Description.docx) | RBE/FCE |
|  | Design Interface Description of Electronic Control Unit Manager | N/A | RBE/FCE |
|  | Design Interface Description of Electronic Control Unit Manager Interface | N/A | RBE/FCE |
|  | Design Interface Description of End of life | N/A | RBE/FCE |
|  | Design Interface Description of Error Handler | N/A | RBE/FCE |
|  | Design Interface Description of Haptic Warning | N/A | RBE/FCE |
|  | Design Interface Description of Memory Integrity Control | N/A | RBE/FCE |
|  | Design Interface Description of Mode Management | [MMG - Design Interface Description.docx](file:///S:\Architectures\Application\Description\Associated_Documents\MMG%20-%20Design%20Interface%20Description.docx) | RBE/FCE |
|  | Design Interface Description of Network Management Interface | N/A | RBE/FCE |
|  | Design Interface Description of Non-Volatile Memory Interface | N/A | RBE/FCE |
|  | Design Interface Description of Non-Volatile Parameters | [NVP - Design Interface Description.docx](file:///S:\Architectures\Application\Description\Associated_Documents\NVP%20-%20Design%20Interface%20Description.docx) | RBE/FCE |
|  | Design Interface Description of Operating System Interface | N/A | RBE/FCE |
|  | Design Interface Description of Power Abstraction Layer | [PAL - Design Interface Description.docx](file:///S:\Architectures\Application\Description\Associated_Documents\PAL%20-%20Design%20Interface%20Description.docx) | RBE/FCE |
|  | Design Interface Description of Pre-Crash Master | N/A | RBE/FCE |
|  | Design Interface Description of Physical Measures Provider | [PMP - Design Interface Description.docx](file:///S:\Architectures\Application\Description\Associated_Documents\PMP%20-%20Design%20Interface%20Description.docx) | RBE/FCE |
|  | Design Interface Description of Port Interface | N/A | RBE/FCE |
|  | Design Interface Description of Pre Pre-Tensioning | [PRE - Design Interface Description.docx](file:///S:\Architectures\Application\Description\Associated_Documents\PMP%20-%20Design%20Interface%20Description.docx) | RBE/FCE |
|  | Design Interface Description of Production cycle function | N/A | RBE/FCE |
|  | Design Interface Description of Pulse Width Modulation Interface | N/A | RBE/FCE |
|  | Design Interface Description of Reset Cause Management | N/A | RBE/FCE |
|  | Design Interface Description of SBC | N/A | RBE/FCE |
|  | Design Interface Description of System Context Management | N/A | RBE/FCE |
|  | Design Interface Description of Standard Function Recovery (releasing function) | [SFR - Design Interface Description.docx](file:///S:\Architectures\Application\Description\Associated_Documents\SFR%20-%20Design%20Interface%20Description.docx) | RBE/FCE |
|  | Design Interface Description of Serial Peripheral Interface Interface | N/A | RBE/FCE |
|  | Design Interface Description of Startup | N/A | RBE/FCE |
|  | Design Interface Description of System Time Management | N/A | RBE/FCE |
|  | Design Interface Description of Vehicle Dynamics algorithm | N/A | RBE/FCE |

## Freescale Documents

This section presents all the documents that complete this software architecture design document.

|  |  |  |  |
| --- | --- | --- | --- |
| Nb | **Document** | **Reference** | **Company** |
|  | MC9S12ZVC-Family Reference Manual Preliminary  Confidential | MC9S12ZVCRM\_Rev0.06.pdf | Freescale |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

## Tier2 Documents

This section presents all the documents that complete this software architecture design document.

|  |  |  |  |
| --- | --- | --- | --- |
| Nb | **Document** | **Reference** | **Company** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

## HW Datasheet

This section presents all the documents related to the HW components that complete this software architecture design document.

|  |  |  |  |
| --- | --- | --- | --- |
| Nb | **Document** | **Reference** | **Company** |
|  | BTN8984TA datasheet | BTN8984TA\_TDS\_051 | Infineon |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

## Other Documents

This section presents all the documents that also have been needed to write this software architecture design document.

|  |  |  |  |
| --- | --- | --- | --- |
| Nb | **Document** | **Reference** | **Company** |
|  | Unified Modelling Language | 2.1.1 | OMG |
|  | MCU RFQ | [E2581849](https://plm.autoliv.int/linkto/latest/ProductDescription/E2581849/*) | FCE |
|  |  |  |  |

## Glossary And Definition

This section presents all the definitions and/or abbreviations used in this document.

*List of terms in alphabetical order:*

|  |  |
| --- | --- |
| ***Term*** | ***Meaning*** |
| ADC | Analog Digital Converter |
| AEC | Autoliv Error Code |
| API | Application Programming Interface |
| ASDM | Active Safety Domain Master |
| ASIC | Application Specific Integrated Circuit |
| ASY | Active SafetY |
| BSW | Basic SW modules |
| CAN | Controller Area Network |
| C/S | Chip Select |
| COP | Computer Operating Properly |
| eCPL | Electronic Crash Pole Locking |
| DART | Ditch - Airborne - Rough Terrain |
| DFLASH | Data FLASH |
| ECC | Error Code Correction |
| ECU | Electronic Control Unit |
| EOL | End Of Life |
| EEPROM | Electric Erasable and Programmable Read only Memory |
| HFPP | High Force Pre-Pre-Tensioning belt function |
| HF-PRE | High Force PRE pre-tensioning |
| HR | Hard Releasing |
| I/O | Input/Output |
| IMU | Inartial Measurements Unit |
| ISS | Integrated Safing System |
| LFPP | Low Force Pre-Pre-Tensioning belt function |
| MSA | Motor Start/Stop Automatic |
| MCAL | Micro-Controller Abstraction Layer |
| MCU | Micro-controller Unit |
| NMG | Mode ManaGement |
| NVM | Non Volatile Memory |
| OS | Operating System |
| PCM | Pre-Crash Master |
| PFLASH | Program FLASH |
| PIT | Periodic Interrupt Timer |
| PLL | Phase-locked loop |
| RAM | Random Access Memory |
| RCWM | Rear Collision Warning and Mitigation |
| RML | Left PP ECU |
| RMR | Right PP ECU |
| RMx | Both PP ECU |
| ROM | Read Only Memory |
| RSU | Remote Sensor Unit |
| RTE | Real Time Environment |
| RTOS | Real Time Operating System |
| SFR | Standard Function Recovery |
| SODL | Side Obstacle Detection Left |
| SPI | Serial Peripheral Interface |
| SRS | Supplementary Restraint System |
| TBC | To be confirmed |
| TBD | To be defined |
| TF | Technical Function |
| TFLASH | Test FLASH of the Pictus MCU (“one time programmable” memory) |
| W/D | Watchdog |

# Description

The SFR component is intended to request a releasing cycle to allow recovering the standard functions of the seat belt.

This component is part of the so called “belt function decision algorithm” layer.

As depicted by the figure below, the recovery of the seat belt standard functions consists in:

* Detecting tensioning cycle start
* Exctrating the releasing cycle type FROM started tensioning cycle parameters
* Requesting the releasing cycle activation (if allowed) after the tensioning cycle execution

# Technical functions

|  |  |  |  |
| --- | --- | --- | --- |
| **Requirements** | **Criteria** | **Levels/Tolerances** | **Source** |
| ARCH\_SW\_SFR\_0020 | This component shall implement the releasing cycles triggering/aborting. | SFR\_runStandardFunctionRecovery() |  |

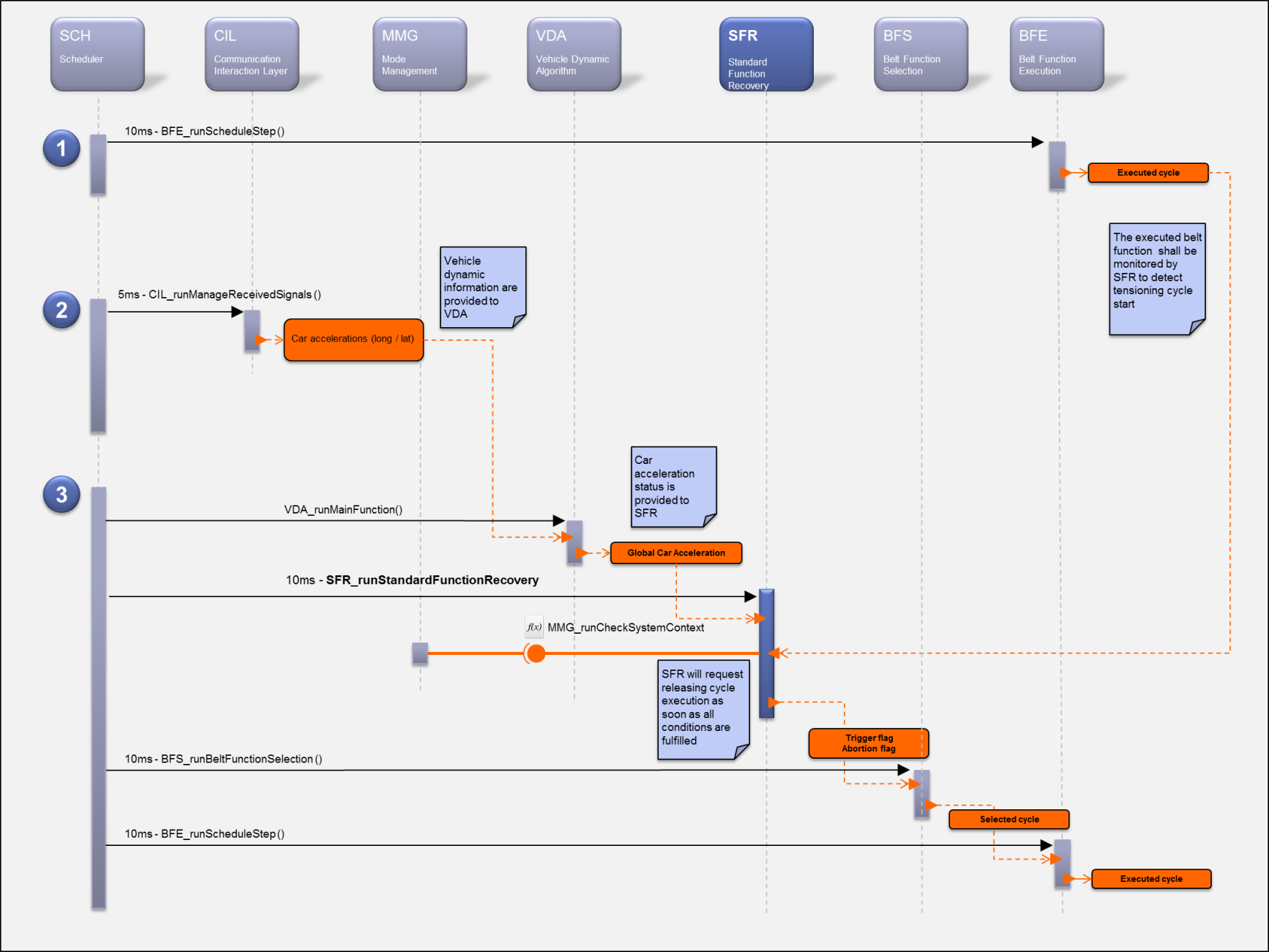
## To start/stop a releasing cycle after a tensioning cycle (nominal case)

Unlike the other electronic seat belt functions, the releasing function is internally triggered, based on the detection of the tensioning cycle start.

The releasing cycle execution request is performed in 3 steps.

1. The first step is related to the belt functions execution from which BFE provides the current executed cycle.
2. A tensioning cycle, requested by signal, is aborted : on sinal RGS\_XY\_Status Incorrect Tensioning Execution is received and a HardRelease or BackupRelease should be permormed.
3. The last execution context is the one which will call the SFR decision matrix (at this stage, all information needed by SFR are available).

If SFR detects a tensioning cycle start, it will extract the associated releasing cycle from the tensioning cycle parameters. From that point, SFR will continuously request the releasing cycle execution until its complete execution (or its abortion).



**Figure 2: Sfr - Data flow description of the hard releasing activation / interrupt based on vehicle signals**

# Runnables

## SFR\_runStandardFunctionRecovery

### Definition

|  |  |  |  |
| --- | --- | --- | --- |
| **Prototype** | | | |
| void SFR\_runStandardFunctionRecovery (void) | | | |
| **Object** | | | |
| This function shall periodically monitor the current executed cycle in order to detect the start of a releasing cycle.  In addition, this function shall also manage the anti-patina cycle.And will inform the rest of the application when antipatina is finished and if abortion/inhibion conditions are present. | | | |
| **Parameters** | | | |
| Name | Type | Direction | Description |
| NA | NA | NA | NA |
| **Returned value** | | | |
| Name | Description | | |
| NA | NA | | |
| **Dynamic aspect** | | | |
| Called every 10 ms. | | | |
| **Covered requirements** | | | |
| ARCH\_SW\_SFR\_0020 | | | |

### Data flow / Parameters

The table below specifies the input and output data related to the present runnable.

|  |  |  |  |
| --- | --- | --- | --- |
| **Requirements** | **Criteria** | **Levels/Tolerances** | **Source** |
| ARCH\_SW\_SFR\_0021 | The current executed cycle from BFE shall be an input.  This will be the **first trigger signal** for the releasing cycle management |  | ALV\_EXT\_TF\_R\_1879, ALV\_EXT\_TF\_R\_1852 |
| ARCH\_SW\_SFR\_0022 | The car acceleration low data shall be an input. |  | ALV\_EXT\_TF\_R\_1884 |
| ARCH\_SW\_SFR\_0040 | The car crash status signal from CIL shall be an input. |  | ALV\_EXT\_TF\_R\_1644 |
| ARCH\_SW\_SFR\_0023 | The cycle parameters from NVP shall be an input. |  | ALV\_EXT\_TF\_R\_1888, ALV\_EXT\_TF\_G\_36 |
| ARCH\_SW\_SFR\_0036 | HW Self protection should inhib releasing function |  |  |
| ARCH\_SW\_SFR\_0039 | Inhibition and abortion errors should be read periodically .(critical autotest, context modes and NVP) |  |  |
| ARCH\_SW\_SFR\_0036 | After a tensioning cycles is aborted or ended, a reease should be executed. |  | DAI\_EXT\_TF\_R\_2415; DAI\_EXT\_TF\_R\_2383 |
| ARCH\_SW\_SFR\_0025 | The SFR\_runStandardFunctionRecovery function shall periodically compute the **trigger** flag SFR 1 to request or not the anti-patina cycle **triggering**. |  | DAI\_EXT\_TF\_R\_2460 |
| ARCH\_SW\_SFR\_0026 | The SFR\_runStandardFunctionRecovery function shall periodically compute the **trigger** flag SFR 2 to request or not the hard releasing cycle **triggering**. |  |  |
| ARCH\_SW\_SFR\_0027 | The SFR\_runStandardFunctionRecovery function shall periodically compute the **trigger** flag SFR 3 to request or not the smooth releasing cycle **triggering**. |  | DAI\_EXT\_TF\_R\_2415 |
| ARCH\_SW\_SFR\_0028 | The SFR\_runStandardFunctionRecovery function shall periodically compute the **trigger** flag SFR 4 to request or not the backup releasing cycle **triggering**. |  |  |
| ARCH\_SW\_SFR\_0029 | The SFR\_runStandardFunctionRecovery function shall periodically compute the **interrupt** flag SFR 1 to request or not the anti-patina cycle **interrupt** |  |  |
| ARCH\_SW\_SFR\_0030 | The SFR\_runStandardFunctionRecovery function shall periodically compute the **interrupt** flag SFR 2 to request or not the hard releasing cycle **interrupt** |  |  |
| ARCH\_SW\_SFR\_0031 | The SFR\_runStandardFunctionRecovery function shall periodically compute the **interrupt** flag SFR 3 to request or not the smooth releasing cycle **interrupt** |  |  |
| ARCH\_SW\_SFR\_0032 | The SFR\_runStandardFunctionRecovery function shall periodically compute the **interrupt** flag SFR 4 to request or not the backup releasing cycle **interrupt** |  |  |
| ARCH\_SW\_SFR\_0033 | All the **trigger** flags shall be initialized to FALSE by default  . |  |  |
| ARCH\_SW\_SFR\_0034 | All the **interrupt** flags shall be initialized to FALSE by default. |  |  |
| ARCH\_SW\_SFR\_0035 | The car acceleration high timeout NVP parameter shall be an input (NVP\_u16CarAccelerationTimeout) |  |  |
| ARCH\_SW\_SFR\_0037 | This function is called every 10 ms |  |  |

### Called functions

The table below specifies the functions called by the present runnable:

|  |  |  |  |
| --- | --- | --- | --- |
| **Requirements** | **Criteria** | **Levels/Tolerances** | **Source** |
| **ARCH\_SW\_SFR\_0060** | The [MMG\_runCheckSystemContext](#_Hlk390768758) function shall be called to check the status of some modes. |  |  |
| **ARCH\_SW\_SFR\_0061** | [DIA\_runGetDiagRequestCycle](#_Hlk450720467) shall be called to check if a releasing cycle is requested by DiagOnCAN |  |  |
| **ARCH\_SW\_SFR\_0062** | [DIA\_runClearDiagRequestCycle](#_Hlk450720488) shall be called to acknowledge the releasing cycle requested by DiagOnCAN |  |  |
| **ARCH\_SW\_SFR\_0063** | [ATM\_runGetTestResult](#_Hlk450720488)  shall be called to acknowledge the result of a certain autotest |  |  |

# MCU resources

The following requirements on resource consumption objectives apply to the module/package:

|  |  |  |  |
| --- | --- | --- | --- |
| **Requirements** | **Criteria** | **Levels/Tolerances** | **Source** |
| ARCH\_SW\_SFR\_9997 | The ROM size consumed by this component shall not exceed 4.5K bytes. |  |  |
| ARCH\_SW\_SFR\_9998 | The heap size consumed by this component shall not exceed 600 bytes. |  |  |