|  |  |  |  |
| --- | --- | --- | --- |
|  |  | |  |
|  |  | |  |
|  |  | |  |
|  |  | |  |
|  | Functional Safety Concept | |  |
|  |  | |  |
|  |  | |  |
|  |  | |  |
|  |  | |  |
| Commodities | Multi-Module OTA | |  |
| Program(s) | MY21 P702 | |  |
| Document Version | FSC6 | |  |
| Document  Owner | Sangeetha Sangameswaran, Brennan Hamilton,  Agish George, Olukoyejo Oyesiku | |  |
|  |  | |  |
|  |  | |  |
|  |  | |  |
|  |  | |  |
|  | Template Authors: | [Global FS Technical Governance Board](https://pd3.spt.ford.com/sites/GlobalFunctionalSafety/Functional%20Safety%20FAQ%20Wiki%20Page/Functional%20Safety%20Team.aspx) |  |
|  | Template Version: | 6.15 |  |
|  | SysML Template Version: | L |  |

# Change Control

|  |  |  |  |
| --- | --- | --- | --- |
| **Version** | **Date** | **Author** | **Change / Remark** |
| FSC1 | 2017-09-23 | ooyesik1 | R&A Functional Safety OTA Working Team: Release for Review. |
| FSC2 | 2017-10-17 | ooyesik1 | R&A Functional Safety OTA Working Team: Updates from phase 1 review |
| FSC3 | 2018-02-27 | ooyesik1 | R&A Functional Safety OTA Working Team: Ready for phase 1 release |
| FSC4 | 2018-04-18 | ooyesik1 | FSC Baseline for AR |
| FSC5 | 2018-08-29 | ooyesik1 | Updates baseline for UNV0 |
| FSC6 | 2018-09-07 | ooyesik1 | Internal Review Updates |

*Note: If this document is not stored in VSEM and marked as final, it is an intermediate document and not the final version.*

***Note:***

*This document is the Template for the Ford Functional Safety Document "FFSD 03 Functional Safety Concept".*

*To create the document, the corresponding guideline shall be used. The Template in combination with the requirements of the Guideline represents the basis for an ISO 26262 aligned document.*

*The template has the IP Classification “Proprietary”. In the footer, IP Classification “Confidential” is stated because usually the FFSD (that will be created from the template) will have IP Classification “Confidential”.*

*For all persons involved in the creation or review of a document it is recommended to read and understand all Ford Functional Safety guidelines in order to get a sufficient overview on the overall Safety Process.*

*As supporting documents, templates for meeting minutes as well as open concerns exist. These supporting documents shall be used in accordance to the Functional Safety guidelines, as required.*

*The Functional Safety Document Set is available in the "Functional Safety Toolbox":*

[*https://www.vsemweb.ford.com/tc/webclient?argument=GoH5bEVTx3NrTD&TC\_file=pse/pse.html*](https://www.vsemweb.ford.com/tc/webclient?argument=GoH5bEVTx3NrTD&TC_file=pse/pse.html)

*Format Options*

*Hints: Light grey italic formatted text. This text can be removed in the final document.*

# Content

[1. Introduction 7](#_Toc524088061)

[1.1 Purpose 7](#_Toc524088062)

[1.2 Input documents 7](#_Toc524088063)

[2. Functional Safety Concept 8](#_Toc524088064)

[Safety Architecture Concept 8](#_Toc524088065)

[2.1 Derivation of Functional Safety Requirements 8](#_Toc524088066)

[2.1.1 Safety Goal SG01 – Prevents Corruption of Existing Software 8](#_Toc524088067)

[2.1.1.1 Safety Concept 9](#_Toc524088068)

[2.1.1.2 Functional Safety Requirements 10](#_Toc524088069)

[2.1.2 Safety Goal SG02 – Prevents Flashing of Incorrect SW 50](#_Toc524088070)

[2.1.2.1 Safety Concept 51](#_Toc524088071)

[2.1.2.2 Functional Safety Requirements 51](#_Toc524088072)

[2.1.3 Safety Goal SG03 – Ensure Safe Activation 86](#_Toc524088073)

[2.1.3.1 Safety Concept 87](#_Toc524088074)

[2.1.3.2 Functional Safety Requirements 87](#_Toc524088075)

[2.1.4 Safety Goal SG04 – Ensure Safe Verification of Activation 120](#_Toc524088076)

[2.1.4.1 Safety Concept 121](#_Toc524088077)

[2.1.4.2 Functional Safety Requirements 121](#_Toc524088078)

[2.1.5 Safety Goal SG05 – Ensure Safe Rollback 134](#_Toc524088079)

[2.1.5.1 Safety Concept 134](#_Toc524088080)

[2.1.5.2 Functional Safety Requirements 134](#_Toc524088081)

[2.1.6 Safety Goal SG6 – Ensure safe erase 150](#_Toc524088082)

[2.1.6.1 Safety Concept 150](#_Toc524088083)

[2.1.6.2 Functional Safety Requirements 150](#_Toc524088084)

[2.1.7 Safety Goal SG7 – Ensure Safe Programming 152](#_Toc524088085)

[2.1.7.1 Safety Concept 153](#_Toc524088086)

[2.1.7.2 Functional Safety Requirements 153](#_Toc524088087)

[2.2 Operating Modes Overview 155](#_Toc524088088)

[2.2.1 Operating Modes Overview Diagram (optional) 155](#_Toc524088089)

[2.3 Safe State and Requirement References 155](#_Toc524088090)

[2.4 Derivation of Requirements on means, controls and user manual to ensure driver (or other persons involved) controllability 157](#_Toc524088091)

[2.5 Definition of parameters used in the Functional Safety Requirements 158](#_Toc524088092)

[2.6 ASIL Decomposition (OPTIONAL) 159](#_Toc524088093)

[2.6.1 Decomposition Functional Safety Requirement F-S-Req096 159](#_Toc524088094)

[2.7 Allocation of Functional Safety Requirements 160](#_Toc524088095)

[2.7.1 Requirements allocation 160](#_Toc524088096)

[2.7.1.1 Preconditions and goals for allocation 160](#_Toc524088097)

[2.7.1.2 Requirements allocation 160](#_Toc524088098)

[3. Execution and Results of Verification Review 162](#_Toc524088099)

[3.1 Verification Review 162](#_Toc524088100)

[3.2 Review Exceptions / Deviations / Findings 163](#_Toc524088101)

[3.3 Further Actions / Decisions 163](#_Toc524088102)

[Appendix A 164](#_Toc524088103)

[A.1 Definitions, Abbreviations and Acronyms 164](#_Toc524088104)

# List of Tables

[Table 1: Input 7](#_Toc524088105)

[Table 2: Requirement F-S-Req030 - Cloud Authenticates Software Update 18](#_Toc524088106)

[Table 3: Requirement F-S-Req031 - OTA Feature Detects Data Corruption 20](#_Toc524088107)

[Table 4: Requirement F-S-Req045 - OTA Feature Authenticates Cloud Connection 23](#_Toc524088108)

[Table 5: Requirement F-S-Req046 - OTA Feature Communicates E2E with the Cloud 25](#_Toc524088109)

[Table 6: Requirement F-S-Req052 - OTA Feature Informs the Cloud of Data Corruption 27](#_Toc524088110)

[Table 7: Requirement F-S-Req071 - OTA App Detects Data Corruption During Software Download 30](#_Toc524088111)

[Table 8: Requirement F-S-Req072 - OTA Feature Detects Data Corruption During Software Download 32](#_Toc524088112)

[Table 9: Requirement F-S-Req082 - OTA App Prevents Active Memory Erasing or Writing 34](#_Toc524088113)

[Table 10: Requirement F-S-Req084 - OTA App Informs the OTA Feature of Data Corruption 36](#_Toc524088114)

[Table 11: Requirement F-S-Req086 - OTA App Authenticates Erase And Programming Commands 39](#_Toc524088115)

[Table 12: Requirement F-S-Req087 - OTA App Executes OTA Without Affecting Basic Function 41](#_Toc524088116)

[Table 13: Requirement F-S-Req088 - Other ECU SW Prevents Active Memory Erasing or Writing 43](#_Toc524088117)

[Table 14: Requirement F-S-Req090 - Other ECU SW Executes OTA Without Affecting Basic Function 46](#_Toc524088118)

[Table 15: Requirement F-S-Req094 - Other ECU SW Executes Active Memory 48](#_Toc524088119)

[Table 16: Requirement F-S-Req095 - OTA App Detects Communication Errors 50](#_Toc524088120)

[Table 17: Requirement F-S-Req018 - Cloud Uses E2E 58](#_Toc524088121)

[Table 18: Requirement F-S-Req020 - OTA Governance Board shall review and approve the software that is to be pushed via OTA 61](#_Toc524088122)

[Table 19: Requirement F-S-Req021 - Cloud Detects Data Corruption 63](#_Toc524088123)

[Table 20: Requirement F-S-Req022 - Engineer Ensures Unique SW IDs 65](#_Toc524088124)

[Table 21: Requirement F-S-Req024 - Engineer Uploads Correct Software 67](#_Toc524088125)

[Table 22: Requirement F-S-Req033 - OTA Feature Detects Invalid Software 70](#_Toc524088126)

[Table 23: Requirement F-S-Req040 - Engineer Marks OTA and Non-OTA Software 72](#_Toc524088127)

[Table 24: Requirement F-S-Req047 - Cloud Sends Correct Software for the Target ECU 74](#_Toc524088128)

[Table 25: Requirement F-S-Req059 - Cloud and Engineers Ensure Correct Software is Flashed 77](#_Toc524088129)

[Table 26: Requirement F-S-Req081 - Other ECU SW Provides Part Number 79](#_Toc524088130)

[Table 27: Requirement F-S-Req091 - OTA App rejects Invalid Software 82](#_Toc524088131)

[Table 28: Requirement F-S-Req092 - OTA App Sends Correct Part Number 84](#_Toc524088132)

[Table 29: Requirement F-S-Req111 - Cloud and OTA Supervisor Communicates Manifest Securely 86](#_Toc524088133)

[Table 30: Requirement F-S-Req019 - Powertrain Controls Ensure Start Has Been Inhibited 93](#_Toc524088134)

[Table 31: Requirement F-S-Req042 - OTA Feature Evaluates Safe Time to Perform Activation 96](#_Toc524088135)

[Table 32: Requirement F-S-Req074 - OTA Feature Command Inhibit Start 99](#_Toc524088136)

[Table 33: Requirement F-S-Req075 - Ignition Control Module Inhibits Start Upon Command 101](#_Toc524088137)

[Table 34: Requirement F-S-Req079 - OTA App (ASIL C/D) Verify Safe Vehicle State 103](#_Toc524088138)

[Table 35: Requirement F-S-Req083 - Other ECU SW (ASIL C/D) Verify Safe Vehicle State 106](#_Toc524088139)

[Table 36: Requirement F-S-Req096 - OTA Feature, OTA App, and Other ECU SW (ASIL C/D) Ensures Safe Time To Perform Activation 108](#_Toc524088140)

[Table 37: Requirement F-S-Req097 - OTA App and Other ECU SW (ASIL C/D) Ensures Safe Time To Perform Activation 111](#_Toc524088141)

[Table 38: Requirement F-S-Req098 - Independence in Ensuring Safe Time To Perform Activation 113](#_Toc524088142)

[Table 39: Requirement F-S-Req100 - OTA Feature and Ignition Control Module Communicates E2E 115](#_Toc524088143)

[Table 40: Requirement F-S-Req101 - Ignition Control Module and Powertrain Controls Communicates E2E 118](#_Toc524088144)

[Table 41: Requirement F-S-Req103 - Iginition Control Module Rejects Start Inhibit Request if Engine is Running 120](#_Toc524088145)

[Table 42: Requirement F-S-Req077 - OTA App Authenticates ACTIVATION Commands 128](#_Toc524088146)

[Table 43: Requirement F-S-Req078 - Other ECU SW Reports ACTIVATION Readiness 130](#_Toc524088147)

[Table 44: Requirement F-S-Req080 - OTA App Communicates E2E with the OTA Feature 133](#_Toc524088148)

[Table 45: Requirement F-S-Req027 - OTA Feature Evaluates ACTIVATION Success 139](#_Toc524088149)

[Table 46: Requirement F-S-Req041 - OTA Feature Evaluates Roll Back Success 142](#_Toc524088150)

[Table 47: Requirement F-S-Req085 - Other ECU SW Performs Activation Within Time Limit 145](#_Toc524088151)

[Table 48: Requirement F-S-Req093 - OTA App Verifies Installed Software During Activation 147](#_Toc524088152)

[Table 49: Requirement F-S-Req099 - OTA Feature Commands Rollback Upon Unsuccessful Activation 150](#_Toc524088153)

[Table 50: Operating Modes Overview 155](#_Toc524088154)

[Table 51: Safe State and Functional Safety Requirement Overview 157](#_Toc524088155)

[Table 52: Parameter 158](#_Toc524088156)

[Table 53: Decomposition F-S-Req096 159](#_Toc524088157)

[Table 54: Requirements allocation 161](#_Toc524088158)

[Table 55: Review Table 162](#_Toc524088159)

[Table 56: Checklist for Completeness of Functional Safety concept 162](#_Toc524088160)

[Table 57: Definitions, Abbreviations and Acronyms 164](#_Toc524088161)

# Introduction

## Purpose

To comply with the Safety Goals of the Hazard Analysis and Risk Assessment, the Functional Safety Concept specifies the basic safety mechanisms and safety measures in the form of Functional Safety Requirements. The Functional Safety Requirements are allocated to elements in the System Architecture.

The Functional Safety Requirements shall be specified in accordance with the overall management of Safety Requirements.

## Input documents

|  |  |  |  |
| --- | --- | --- | --- |
|  | Document Name | File Name/Reference | Version |
| **FFSD** | FFSD 01.1 Item Definition /  FFSD 01.10 Feature Document |  |  |
| FFSD 02 Hazard Analysis and Risk Assessment |  |  |
| **Other Input** | Preliminary architectural assumptions |  |  |
| System Description/ Specifications/ Design |  |  |
| Open concerns / Action items (from multiple sources) |  | - |

Table 1: Input

# Functional Safety Concept

### Safety Architecture Concept

Figure 1 shows the architectural elements of the MMOTA Logical Architecture.

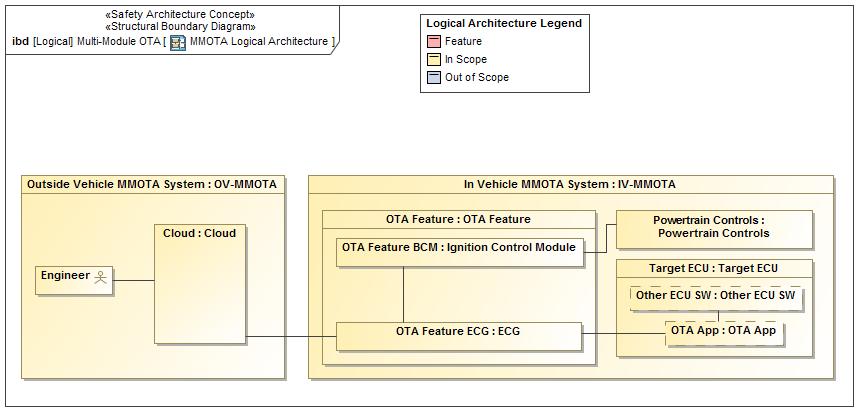


Figure 2: Block diagram of preliminary safety architecture concept (functional blocks and signals may also be used for safety purposes)

The next sections show how the Functional Safety Requirements are derived systematically from the Safety Goals.

## Derivation of Functional Safety Requirements

### Safety Goal SG01 – Prevents Corruption of Existing Software

**Name:** Prevents Corruption of Existing Software

**Purpose:**

**Text:**

Target ECU needs to protect up to their ASIL level

**ASIL:** D

#### Safety Concept

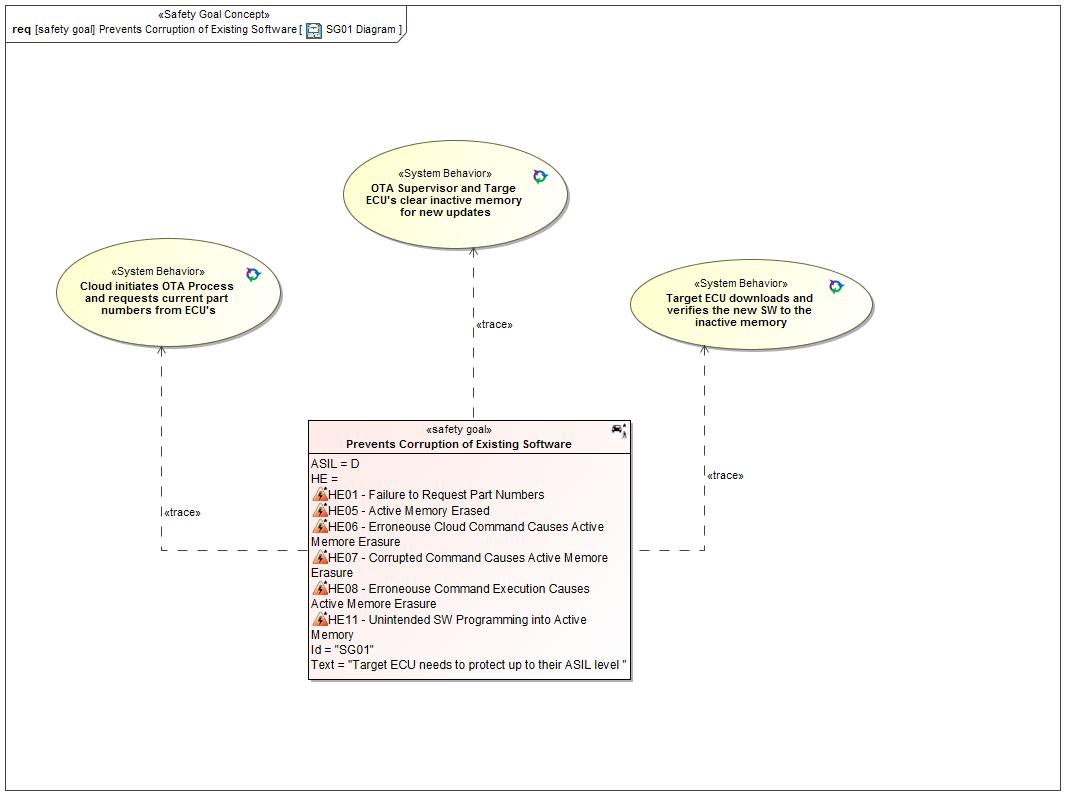


Figure 3: SG01 Diagram

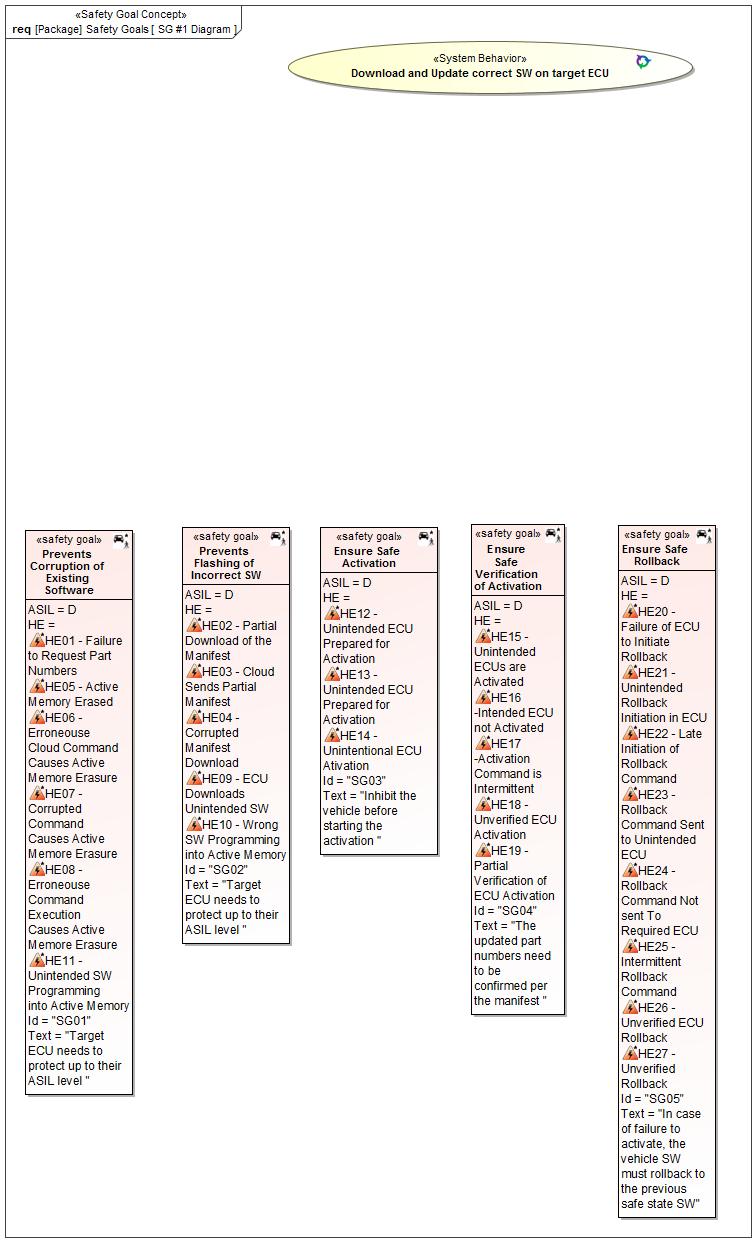


Figure 4: SG #1 Diagram

#### Functional Safety Requirements

##### Requirement Derivation Diagram(s)(Optional)

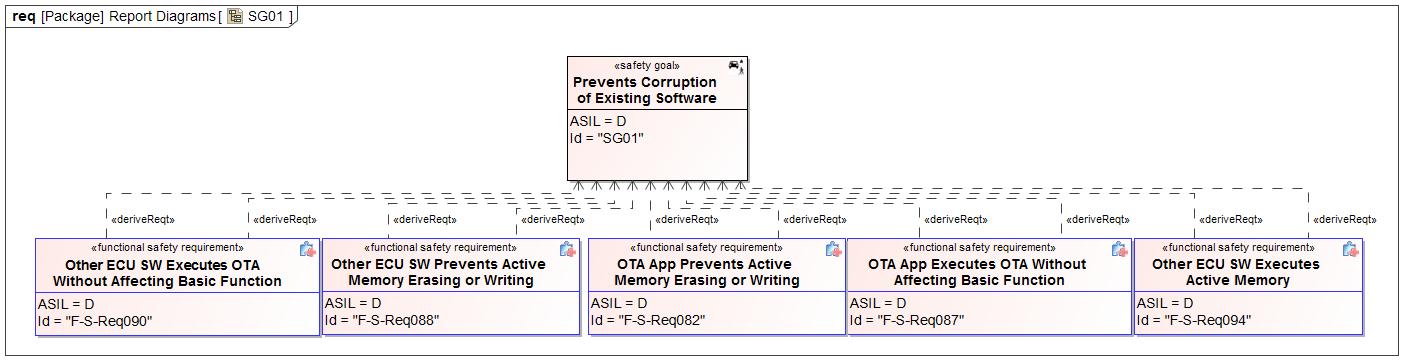


Figure 5 - Functional Safety Requirements Derivation Diagram for SG01

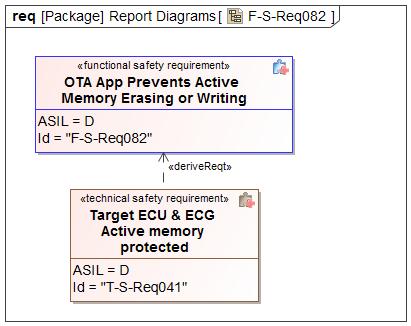


Figure 6 - Functional Safety Requirements Derivation Diagram for OTA App Prevents Active Memory Erasing or Writing

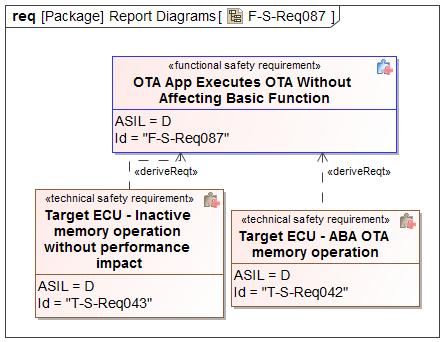


Figure 7 - Functional Safety Requirements Derivation Diagram for OTA App Executes OTA Without Affecting Basic Function

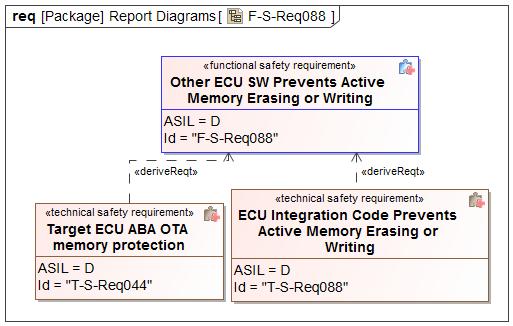


Figure 8 - Functional Safety Requirements Derivation Diagram for Other ECU SW Prevents Active Memory Erasing or Writing

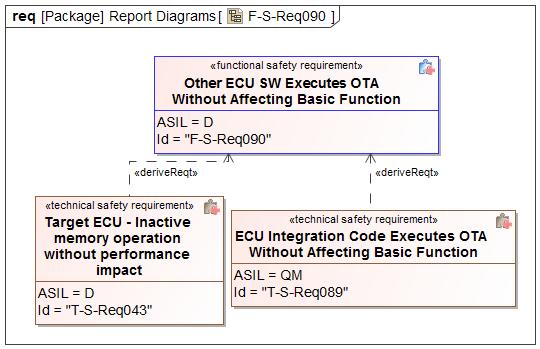


Figure 9 - Functional Safety Requirements Derivation Diagram for Other ECU SW Executes OTA Without Affecting Basic Function

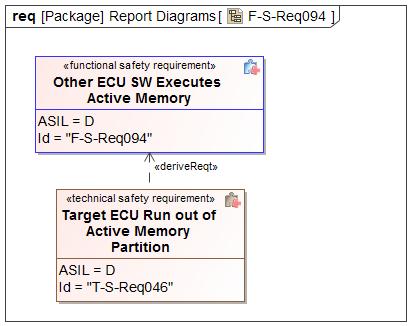


Figure 10 - Functional Safety Requirements Derivation Diagram for Other ECU SW Executes Active Memory

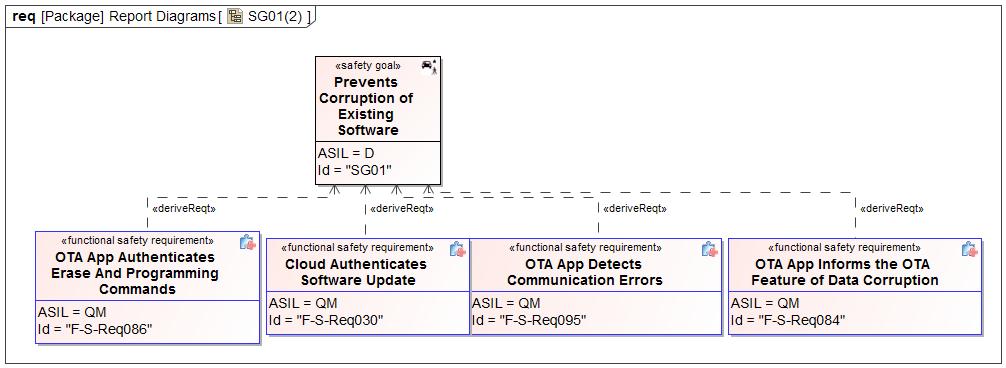


Figure 11 - Functional Safety Requirements Derivation Diagram for SG01

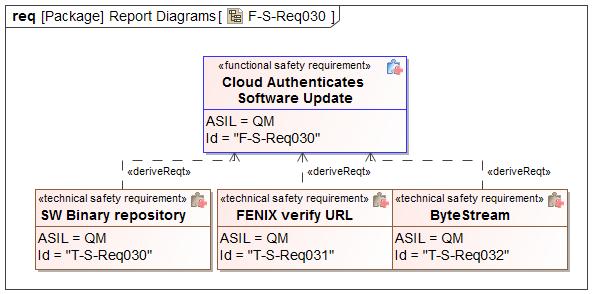


Figure 12 - Functional Safety Requirements Derivation Diagram for Cloud Authenticates Software Update

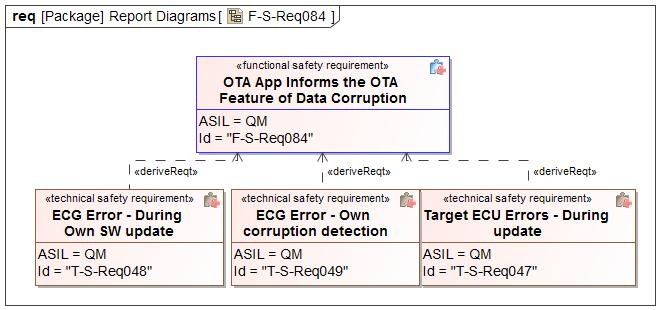


Figure 13 - Functional Safety Requirements Derivation Diagram for OTA App Informs the OTA Feature of Data Corruption

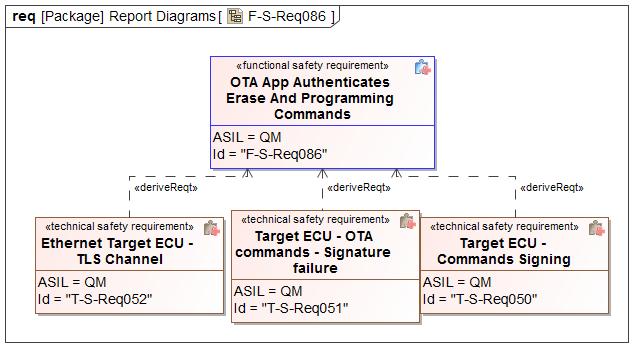


Figure 14 - Functional Safety Requirements Derivation Diagram for OTA App Authenticates Erase And Programming Commands

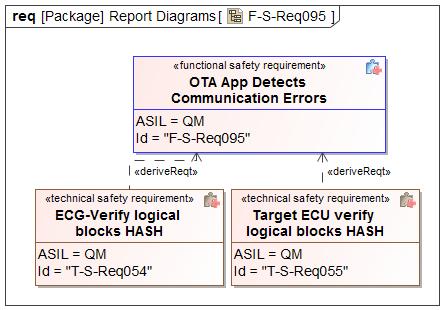


Figure 15 - Functional Safety Requirements Derivation Diagram for OTA App Detects Communication Errors

##### Functional Safety Requirements for SG01 - Prevents Corruption of Existing Software

*Insert a table for each requirement according to its category.*

|  |  |  |  |
| --- | --- | --- | --- |
| Safety Req-ID | **F-S-Req030 - Cloud Authenticates Software Update** | |  |
| Category | Safety Related Function | |  |
| Version  *only applicable in case of:*   * *Non-E/E Requirements* |  | |  |
| Author  *only applicable in case of:*  *Non-E/E Requirements* |  | |  |
| External Reference *(optional)* |  | | |
| Safety Goal Ref. | SG01 - Prevents Corruption of Existing Software  SG02 - Prevents Flashing of Incorrect SW | Operating Modes | Ignition Off  Ignition On |
| ASIL Classification:  *if applicable in case of category*   * *General*   *not applicable in case of category*   * *Non-E/E Requirement* | **ASIL Override Rationale -** ISO 26262 ASIL rating applies only to electrical and electronic automobile systems.Therefore requirements for the cloud cannot be ASIL rated.  QM | Safe State  *if applicable for:*   * *General Requirements* * *User information* * *Non-E/E Requirements* | Software Rejected |
| Functional Safety Requirement Title | Cloud Authenticates Software Update | | |
| Functional Safety Requirement  *In case of User information including:*  *- Functional Safety Requirement Text*  *- Content of Information*  *- Method for Information*  *- Timing of Information*  *- Content of printed instructions (owner’s guide/service manuals etc.)* | The Cloud shall authenticate the source of the received software. | | |
| Rationale | To prevent malicious actors from uploading corrupt/malicious software (Data corruption during software download shall be detectable). | | |
| Description of actions of the driver or other endangered persons  *if applicable in case of:*   * *Safety Related Functions* * *Reduced Functionality* * *User information*   *not applicable in case of:*   * *General Requirements* * *Maintain Safe State / Recovery* * *Non-E/E Requirements* |  | | |
| Validation Criteria for these actions  *if applicable in case of:*   * *Safety Related Functions* * *Reduced Functionality* * *User information*   *not applicable in case of:*   * *General Requirements* * *Maintain Safe State / Recovery* * *Non-E/E Requirements* |  | | |
| Fault Tolerant Time interval *if applicable)* | N/A | | |
| Reduced Functionality interval *(if applicable)* |  | | |
| Functional Redundancies (e.g. fault tolerance)  *(if applicable)* |  | | |
| Requirement Status |  | | |
| V&V method | System test | | |
| V&V acceptance criteria  *not applicable in case of:*   * *Non-E/E Requirements* | It should not be possible for an unauthorized person to upload software to the cloud | | |
| V&V ID  *only applicable in case of:*   * *Non-E/E Requirements* |  | | |
| V&V Version  *only applicable in case of:*  *Non-E/E Requirements* |  | | |
| V&V Author  *only applicable in case of:*   * *Non-E/E Requirements* |  | | |
| V&V Status  *only applicable in case of:*   * *Non-E/E Requirements* |  | | |

Table 2: Requirement F-S-Req030 - Cloud Authenticates Software Update

|  |  |  |  |
| --- | --- | --- | --- |
| Safety Req-ID | **F-S-Req031 - OTA Feature Detects Data Corruption** | |  |
| Category | Safety Related Function | |  |
| Version  *only applicable in case of:*   * *Non-E/E Requirements* |  | |  |
| Author  *only applicable in case of:*  *Non-E/E Requirements* |  | |  |
| External Reference *(optional)* |  | | |
| Safety Goal Ref. | SG01 - Prevents Corruption of Existing Software  SG04 - Ensure Safe Verification of Activation | Operating Modes | Ignition On |
| ASIL Classification:  *if applicable in case of category*   * *General*   *not applicable in case of category*   * *Non-E/E Requirement* | **ASIL Override Rationale -** Failure to detect data corruption during download would not lead to a violation of the safety goal since the software is not used immediately. The software is validated before being activated.  QM | Safe State  *if applicable for:*   * *General Requirements* * *User information* * *Non-E/E Requirements* | Software Rejected |
| Functional Safety Requirement Title | OTA Feature Detects Data Corruption | | |
| Functional Safety Requirement  *In case of User information including:*  *- Functional Safety Requirement Text*  *- Content of Information*  *- Method for Information*  *- Timing of Information*  *- Content of printed instructions (owner’s guide/service manuals etc.)* | The OTA Feature shall detect data corruption errors in the downloaded software. | | |
| Rationale | The system needs to be able to detect common communication faults like data corruption, missing messages, messages arriving out of order etc. | | |
| Description of actions of the driver or other endangered persons  *if applicable in case of:*   * *Safety Related Functions* * *Reduced Functionality* * *User information*   *not applicable in case of:*   * *General Requirements* * *Maintain Safe State / Recovery* * *Non-E/E Requirements* |  | | |
| Validation Criteria for these actions  *if applicable in case of:*   * *Safety Related Functions* * *Reduced Functionality* * *User information*   *not applicable in case of:*   * *General Requirements* * *Maintain Safe State / Recovery* * *Non-E/E Requirements* |  | | |
| Fault Tolerant Time interval *if applicable)* | N/A | | |
| Reduced Functionality interval *(if applicable)* |  | | |
| Functional Redundancies (e.g. fault tolerance)  *(if applicable)* |  | | |
| Requirement Status |  | | |
| V&V method | Vehicle test | | |
| V&V acceptance criteria  *not applicable in case of:*   * *Non-E/E Requirements* | The OTA Feature detects data corruption errors in the downloaded software | | |
| V&V ID  *only applicable in case of:*   * *Non-E/E Requirements* |  | | |
| V&V Version  *only applicable in case of:*  *Non-E/E Requirements* |  | | |
| V&V Author  *only applicable in case of:*   * *Non-E/E Requirements* |  | | |
| V&V Status  *only applicable in case of:*   * *Non-E/E Requirements* |  | | |

Table 3: Requirement F-S-Req031 - OTA Feature Detects Data Corruption

|  |  |  |  |
| --- | --- | --- | --- |
| Safety Req-ID | **F-S-Req045 - OTA Feature Authenticates Cloud Connection** | |  |
| Category | Safety Related Function | |  |
| Version  *only applicable in case of:*   * *Non-E/E Requirements* |  | |  |
| Author  *only applicable in case of:*  *Non-E/E Requirements* |  | |  |
| External Reference *(optional)* |  | | |
| Safety Goal Ref. | SG04 - Ensure Safe Verification of Activation | Operating Modes | Ignition On |
| ASIL Classification:  *if applicable in case of category*   * *General*   *not applicable in case of category*   * *Non-E/E Requirement* | **ASIL Override Rationale -** ISO 26262 ASIL rating applies only to electrical and electronic automobile systems. Therefore requirements for the cloud cannot be ASIL rated.  QM | Safe State  *if applicable for:*   * *General Requirements* * *User information* * *Non-E/E Requirements* | Command rejected |
| Functional Safety Requirement Title | OTA Feature Authenticates Cloud Connection | | |
| Functional Safety Requirement  *In case of User information including:*  *- Functional Safety Requirement Text*  *- Content of Information*  *- Method for Information*  *- Timing of Information*  *- Content of printed instructions (owner’s guide/service manuals etc.)* | The OTA Feature shall authenticate the connection with the Cloud. | | |
| Rationale | To prevent malicious actors from attempting an MMOTA. | | |
| Description of actions of the driver or other endangered persons  *if applicable in case of:*   * *Safety Related Functions* * *Reduced Functionality* * *User information*   *not applicable in case of:*   * *General Requirements* * *Maintain Safe State / Recovery* * *Non-E/E Requirements* |  | | |
| Validation Criteria for these actions  *if applicable in case of:*   * *Safety Related Functions* * *Reduced Functionality* * *User information*   *not applicable in case of:*   * *General Requirements* * *Maintain Safe State / Recovery* * *Non-E/E Requirements* |  | | |
| Fault Tolerant Time interval *if applicable)* | N/A | | |
| Reduced Functionality interval *(if applicable)* |  | | |
| Functional Redundancies (e.g. fault tolerance)  *(if applicable)* |  | | |
| Requirement Status |  | | |
| V&V method | Vehicle test | | |
| V&V acceptance criteria  *not applicable in case of:*   * *Non-E/E Requirements* | The OTA Feature authenticates the connection with the Cloud | | |
| V&V ID  *only applicable in case of:*   * *Non-E/E Requirements* |  | | |
| V&V Version  *only applicable in case of:*  *Non-E/E Requirements* |  | | |
| V&V Author  *only applicable in case of:*   * *Non-E/E Requirements* |  | | |
| V&V Status  *only applicable in case of:*   * *Non-E/E Requirements* |  | | |

Table 4: Requirement F-S-Req045 - OTA Feature Authenticates Cloud Connection

|  |  |  |  |
| --- | --- | --- | --- |
| Safety Req-ID | **F-S-Req046 - OTA Feature Communicates E2E with the Cloud** | |  |
| Category | Safety Related Function | |  |
| Version  *only applicable in case of:*   * *Non-E/E Requirements* |  | |  |
| Author  *only applicable in case of:*  *Non-E/E Requirements* |  | |  |
| External Reference *(optional)* |  | | |
| Safety Goal Ref. | SG04 - Ensure Safe Verification of Activation | Operating Modes | Ignition On |
| ASIL Classification:  *if applicable in case of category*   * *General*   *not applicable in case of category*   * *Non-E/E Requirement* | **ASIL Override Rationale -** ISO 26262 ASIL rating applies only to electrical and electronic automobile systems. Therefore requirements for the cloud cannot be ASIL rated.  QM | Safe State  *if applicable for:*   * *General Requirements* * *User information* * *Non-E/E Requirements* | N/A |
| Functional Safety Requirement Title | OTA Feature Communicates E2E with the Cloud | | |
| Functional Safety Requirement  *In case of User information including:*  *- Functional Safety Requirement Text*  *- Content of Information*  *- Method for Information*  *- Timing of Information*  *- Content of printed instructions (owner’s guide/service manuals etc.)* | The OTA Feature shall communicate with the cloud over an end-to-end protected communication path. | | |
| Rationale | The OTA Feature should be able to detect common communication faults like data corruption, missing messages, messages arriving out of order etc. | | |
| Description of actions of the driver or other endangered persons  *if applicable in case of:*   * *Safety Related Functions* * *Reduced Functionality* * *User information*   *not applicable in case of:*   * *General Requirements* * *Maintain Safe State / Recovery* * *Non-E/E Requirements* |  | | |
| Validation Criteria for these actions  *if applicable in case of:*   * *Safety Related Functions* * *Reduced Functionality* * *User information*   *not applicable in case of:*   * *General Requirements* * *Maintain Safe State / Recovery* * *Non-E/E Requirements* |  | | |
| Fault Tolerant Time interval *if applicable)* | N/A | | |
| Reduced Functionality interval *(if applicable)* |  | | |
| Functional Redundancies (e.g. fault tolerance)  *(if applicable)* |  | | |
| Requirement Status |  | | |
| V&V method | Vehicle test | | |
| V&V acceptance criteria  *not applicable in case of:*   * *Non-E/E Requirements* | Rejection of corrupted data by the OTA Feature | | |
| V&V ID  *only applicable in case of:*   * *Non-E/E Requirements* |  | | |
| V&V Version  *only applicable in case of:*  *Non-E/E Requirements* |  | | |
| V&V Author  *only applicable in case of:*   * *Non-E/E Requirements* |  | | |
| V&V Status  *only applicable in case of:*   * *Non-E/E Requirements* |  | | |

Table 5: Requirement F-S-Req046 - OTA Feature Communicates E2E with the Cloud

|  |  |  |  |
| --- | --- | --- | --- |
| Safety Req-ID | **F-S-Req052 - OTA Feature Informs the Cloud of Data Corruption** | |  |
| Category | Safety Related Function | |  |
| Version  *only applicable in case of:*   * *Non-E/E Requirements* |  | |  |
| Author  *only applicable in case of:*  *Non-E/E Requirements* |  | |  |
| External Reference *(optional)* |  | | |
| Safety Goal Ref. | SG04 - Ensure Safe Verification of Activation | Operating Modes | Ignition On |
| ASIL Classification:  *if applicable in case of category*   * *General*   *not applicable in case of category*   * *Non-E/E Requirement* | **ASIL Override Rationale -** Failure to inform the cloud would not result in the violation of the safety goal.  QM | Safe State  *if applicable for:*   * *General Requirements* * *User information* * *Non-E/E Requirements* | N/A |
| Functional Safety Requirement Title | OTA Feature Informs the Cloud of Data Corruption | | |
| Functional Safety Requirement  *In case of User information including:*  *- Functional Safety Requirement Text*  *- Content of Information*  *- Method for Information*  *- Timing of Information*  *- Content of printed instructions (owner’s guide/service manuals etc.)* | The OTA feature shall inform the cloud of any data corruption detected during downstream transmission and storage. | | |
| Rationale | To prevent a malfunction of the MMOTA feature from causing the highest level hazard in the target ECU. | | |
| Description of actions of the driver or other endangered persons  *if applicable in case of:*   * *Safety Related Functions* * *Reduced Functionality* * *User information*   *not applicable in case of:*   * *General Requirements* * *Maintain Safe State / Recovery* * *Non-E/E Requirements* |  | | |
| Validation Criteria for these actions  *if applicable in case of:*   * *Safety Related Functions* * *Reduced Functionality* * *User information*   *not applicable in case of:*   * *General Requirements* * *Maintain Safe State / Recovery* * *Non-E/E Requirements* |  | | |
| Fault Tolerant Time interval *if applicable)* | N/A | | |
| Reduced Functionality interval *(if applicable)* |  | | |
| Functional Redundancies (e.g. fault tolerance)  *(if applicable)* |  | | |
| Requirement Status |  | | |
| V&V method | Vehicle test | | |
| V&V acceptance criteria  *not applicable in case of:*   * *Non-E/E Requirements* | Verify the OTA feature informs the the cloud of any data corruption detected during downstream transmission and storage. | | |
| V&V ID  *only applicable in case of:*   * *Non-E/E Requirements* |  | | |
| V&V Version  *only applicable in case of:*  *Non-E/E Requirements* |  | | |
| V&V Author  *only applicable in case of:*   * *Non-E/E Requirements* |  | | |
| V&V Status  *only applicable in case of:*   * *Non-E/E Requirements* |  | | |

Table 6: Requirement F-S-Req052 - OTA Feature Informs the Cloud of Data Corruption

|  |  |  |  |
| --- | --- | --- | --- |
| Safety Req-ID | **F-S-Req071 - OTA App Detects Data Corruption During Software Download** | |  |
| Category | Safety Related Function | |  |
| Version  *only applicable in case of:*   * *Non-E/E Requirements* |  | |  |
| Author  *only applicable in case of:*  *Non-E/E Requirements* |  | |  |
| External Reference *(optional)* |  | | |
| Safety Goal Ref. |  | Operating Modes | Ignition On |
| ASIL Classification:  *if applicable in case of category*   * *General*   *not applicable in case of category*   * *Non-E/E Requirement* | **ASIL Override Rationale -** For A/B swap, the downloading of the software is in the inactive memory bank and should not affect the normal functioning of the vehicle nor affect the safe mechanisms in the module.  QM | Safe State  *if applicable for:*   * *General Requirements* * *User information* * *Non-E/E Requirements* | Software Rejected |
| Functional Safety Requirement Title | OTA App Detects Data Corruption During Software Download | | |
| Functional Safety Requirement  *In case of User information including:*  *- Functional Safety Requirement Text*  *- Content of Information*  *- Method for Information*  *- Timing of Information*  *- Content of printed instructions (owner’s guide/service manuals etc.)* | The OTA App in the Target ECU shall detect data corruption during software download. | | |
| Rationale | To prevent a malfunction of the MMOTA feature from causing the highest level hazard in the target ECU. | | |
| Description of actions of the driver or other endangered persons  *if applicable in case of:*   * *Safety Related Functions* * *Reduced Functionality* * *User information*   *not applicable in case of:*   * *General Requirements* * *Maintain Safe State / Recovery* * *Non-E/E Requirements* |  | | |
| Validation Criteria for these actions  *if applicable in case of:*   * *Safety Related Functions* * *Reduced Functionality* * *User information*   *not applicable in case of:*   * *General Requirements* * *Maintain Safe State / Recovery* * *Non-E/E Requirements* |  | | |
| Fault Tolerant Time interval *if applicable)* | N/A | | |
| Reduced Functionality interval *(if applicable)* |  | | |
| Functional Redundancies (e.g. fault tolerance)  *(if applicable)* |  | | |
| Requirement Status |  | | |
| V&V method | Vehicle test | | |
| V&V acceptance criteria  *not applicable in case of:*   * *Non-E/E Requirements* | The OTA App in the Target ECU detects data corruption during software download | | |
| V&V ID  *only applicable in case of:*   * *Non-E/E Requirements* |  | | |
| V&V Version  *only applicable in case of:*  *Non-E/E Requirements* |  | | |
| V&V Author  *only applicable in case of:*   * *Non-E/E Requirements* |  | | |
| V&V Status  *only applicable in case of:*   * *Non-E/E Requirements* |  | | |

Table 7: Requirement F-S-Req071 - OTA App Detects Data Corruption During Software Download

|  |  |  |  |
| --- | --- | --- | --- |
| Safety Req-ID | **F-S-Req072 - OTA Feature Detects Data Corruption During Software Download** | |  |
| Category | Safety Related Function | |  |
| Version  *only applicable in case of:*   * *Non-E/E Requirements* |  | |  |
| Author  *only applicable in case of:*  *Non-E/E Requirements* |  | |  |
| External Reference *(optional)* |  | | |
| Safety Goal Ref. |  | Operating Modes | Ignition On |
| ASIL Classification:  *if applicable in case of category*   * *General*   *not applicable in case of category*   * *Non-E/E Requirement* | **ASIL Override Rationale -** For A/B swap, the downloading of the software is in the inactive memory bank and should not affect the normal functioning of the vehicle nor affect the safe mechanisms in the module.  QM | Safe State  *if applicable for:*   * *General Requirements* * *User information* * *Non-E/E Requirements* | Software Rejected |
| Functional Safety Requirement Title | OTA Feature Detects Data Corruption During Software Download | | |
| Functional Safety Requirement  *In case of User information including:*  *- Functional Safety Requirement Text*  *- Content of Information*  *- Method for Information*  *- Timing of Information*  *- Content of printed instructions (owner’s guide/service manuals etc.)* | The IV-MMOTA shall detect data corruption during software download. | | |
| Rationale | To prevent a malfunction of the MMOTA feature from causing the highest level hazard in the target ECU. | | |
| Description of actions of the driver or other endangered persons  *if applicable in case of:*   * *Safety Related Functions* * *Reduced Functionality* * *User information*   *not applicable in case of:*   * *General Requirements* * *Maintain Safe State / Recovery* * *Non-E/E Requirements* |  | | |
| Validation Criteria for these actions  *if applicable in case of:*   * *Safety Related Functions* * *Reduced Functionality* * *User information*   *not applicable in case of:*   * *General Requirements* * *Maintain Safe State / Recovery* * *Non-E/E Requirements* |  | | |
| Fault Tolerant Time interval *if applicable)* | N/A | | |
| Reduced Functionality interval *(if applicable)* |  | | |
| Functional Redundancies (e.g. fault tolerance)  *(if applicable)* |  | | |
| Requirement Status |  | | |
| V&V method | Vehicle test | | |
| V&V acceptance criteria  *not applicable in case of:*   * *Non-E/E Requirements* | The IV-MMOTA detects data corruption during software download | | |
| V&V ID  *only applicable in case of:*   * *Non-E/E Requirements* |  | | |
| V&V Version  *only applicable in case of:*  *Non-E/E Requirements* |  | | |
| V&V Author  *only applicable in case of:*   * *Non-E/E Requirements* |  | | |
| V&V Status  *only applicable in case of:*   * *Non-E/E Requirements* |  | | |

Table 8: Requirement F-S-Req072 - OTA Feature Detects Data Corruption During Software Download

|  |  |  |  |
| --- | --- | --- | --- |
| Safety Req-ID | **F-S-Req082 - OTA App Prevents Active Memory Erasing or Writing** | |  |
| Category | Safety Related Function | |  |
| Version  *only applicable in case of:*   * *Non-E/E Requirements* |  | |  |
| Author  *only applicable in case of:*  *Non-E/E Requirements* |  | |  |
| External Reference *(optional)* |  | | |
| Safety Goal Ref. | SG01 - Prevents Corruption of Existing Software | Operating Modes | Ignition On |
| ASIL Classification:  *if applicable in case of category*   * *General*   *not applicable in case of category*   * *Non-E/E Requirement* | D | Safe State  *if applicable for:*   * *General Requirements* * *User information* * *Non-E/E Requirements* | Software Rejected |
| Functional Safety Requirement Title | OTA App Prevents Active Memory Erasing or Writing | | |
| Functional Safety Requirement  *In case of User information including:*  *- Functional Safety Requirement Text*  *- Content of Information*  *- Method for Information*  *- Timing of Information*  *- Content of printed instructions (owner’s guide/service manuals etc.)* | The OTA App in the Target ECU shall not attempt writing or erasing memory sections containing the "active software". | | |
| Rationale | To avoid disrupting current software functions the OTA App should avoid memory sections containing the "active software" inclusive of program and data while an OTA is in progress). | | |
| Description of actions of the driver or other endangered persons  *if applicable in case of:*   * *Safety Related Functions* * *Reduced Functionality* * *User information*   *not applicable in case of:*   * *General Requirements* * *Maintain Safe State / Recovery* * *Non-E/E Requirements* |  | | |
| Validation Criteria for these actions  *if applicable in case of:*   * *Safety Related Functions* * *Reduced Functionality* * *User information*   *not applicable in case of:*   * *General Requirements* * *Maintain Safe State / Recovery* * *Non-E/E Requirements* |  | | |
| Fault Tolerant Time interval *if applicable)* | 1 second | | |
| Reduced Functionality interval *(if applicable)* |  | | |
| Functional Redundancies (e.g. fault tolerance)  *(if applicable)* |  | | |
| Requirement Status |  | | |
| V&V method | Vehicle test | | |
| V&V acceptance criteria  *not applicable in case of:*   * *Non-E/E Requirements* | Review if by design the OTA App can ever write into the active memory section Check via a test switch if an attempt by OTA App to write into an active memory address(fault) is prevented. | | |
| V&V ID  *only applicable in case of:*   * *Non-E/E Requirements* |  | | |
| V&V Version  *only applicable in case of:*  *Non-E/E Requirements* |  | | |
| V&V Author  *only applicable in case of:*   * *Non-E/E Requirements* |  | | |
| V&V Status  *only applicable in case of:*   * *Non-E/E Requirements* |  | | |

Table 9: Requirement F-S-Req082 - OTA App Prevents Active Memory Erasing or Writing

|  |  |  |  |
| --- | --- | --- | --- |
| Safety Req-ID | **F-S-Req084 - OTA App Informs the OTA Feature of Data Corruption** | |  |
| Category | Safety Related Function | |  |
| Version  *only applicable in case of:*   * *Non-E/E Requirements* |  | |  |
| Author  *only applicable in case of:*  *Non-E/E Requirements* |  | |  |
| External Reference *(optional)* |  | | |
| Safety Goal Ref. | SG01 - Prevents Corruption of Existing Software | Operating Modes | Ignition On |
| ASIL Classification:  *if applicable in case of category*   * *General*   *not applicable in case of category*   * *Non-E/E Requirement* | **ASIL Override Rationale -** Failure to inform the OTA feature of data corruption would not lead to a violation of the safety goal.  QM | Safe State  *if applicable for:*   * *General Requirements* * *User information* * *Non-E/E Requirements* | Software Rejected |
| Functional Safety Requirement Title | OTA App Informs the OTA Feature of Data Corruption | | |
| Functional Safety Requirement  *In case of User information including:*  *- Functional Safety Requirement Text*  *- Content of Information*  *- Method for Information*  *- Timing of Information*  *- Content of printed instructions (owner’s guide/service manuals etc.)* | The OTA App in the Target ECU shall inform the OTA feature (ECG) of any errors detected during software update. | | |
| Rationale | To prevent a malfunction of the MMOTA feature from causing the highest level hazard in the OTA App. | | |
| Description of actions of the driver or other endangered persons  *if applicable in case of:*   * *Safety Related Functions* * *Reduced Functionality* * *User information*   *not applicable in case of:*   * *General Requirements* * *Maintain Safe State / Recovery* * *Non-E/E Requirements* |  | | |
| Validation Criteria for these actions  *if applicable in case of:*   * *Safety Related Functions* * *Reduced Functionality* * *User information*   *not applicable in case of:*   * *General Requirements* * *Maintain Safe State / Recovery* * *Non-E/E Requirements* |  | | |
| Fault Tolerant Time interval *if applicable)* | N/A | | |
| Reduced Functionality interval *(if applicable)* |  | | |
| Functional Redundancies (e.g. fault tolerance)  *(if applicable)* |  | | |
| Requirement Status |  | | |
| V&V method | Vehicle test | | |
| V&V acceptance criteria  *not applicable in case of:*   * *Non-E/E Requirements* | Verify the OTA App informs the OTA feature and inturn the cloud of any data corruption detected during downstream transmission and storage. | | |
| V&V ID  *only applicable in case of:*   * *Non-E/E Requirements* |  | | |
| V&V Version  *only applicable in case of:*  *Non-E/E Requirements* |  | | |
| V&V Author  *only applicable in case of:*   * *Non-E/E Requirements* |  | | |
| V&V Status  *only applicable in case of:*   * *Non-E/E Requirements* |  | | |

Table 10: Requirement F-S-Req084 - OTA App Informs the OTA Feature of Data Corruption

|  |  |  |  |
| --- | --- | --- | --- |
| Safety Req-ID | **F-S-Req086 - OTA App Authenticates Erase And Programming Commands** | |  |
| Category | Safety Related Function | |  |
| Version  *only applicable in case of:*   * *Non-E/E Requirements* |  | |  |
| Author  *only applicable in case of:*  *Non-E/E Requirements* |  | |  |
| External Reference *(optional)* |  | | |
| Safety Goal Ref. | SG01 - Prevents Corruption of Existing Software | Operating Modes | Ignition On |
| ASIL Classification:  *if applicable in case of category*   * *General*   *not applicable in case of category*   * *Non-E/E Requirement* | **ASIL Override Rationale -** Failure to authenticate the activation command would not violate the safety goal since security authentication is independent from the safety validations.  QM | Safe State  *if applicable for:*   * *General Requirements* * *User information* * *Non-E/E Requirements* | Command rejected |
| Functional Safety Requirement Title | OTA App Authenticates Erase And Programming Commands | | |
| Functional Safety Requirement  *In case of User information including:*  *- Functional Safety Requirement Text*  *- Content of Information*  *- Method for Information*  *- Timing of Information*  *- Content of printed instructions (owner’s guide/service manuals etc.)* | The OTA App in the Target ECU shall authenticate all erase and program secured commands coming from the OTA Feature (ECG). | | |
| Rationale | To prevent malicious actors from intruding the CAN network and attempting a SW reflash. A wrong SW reflash can overwrite active memory, cause incompatible software or trigger an ACTIVATION leading to the highest rated malfunction of the OTA ECU. | | |
| Description of actions of the driver or other endangered persons  *if applicable in case of:*   * *Safety Related Functions* * *Reduced Functionality* * *User information*   *not applicable in case of:*   * *General Requirements* * *Maintain Safe State / Recovery* * *Non-E/E Requirements* |  | | |
| Validation Criteria for these actions  *if applicable in case of:*   * *Safety Related Functions* * *Reduced Functionality* * *User information*   *not applicable in case of:*   * *General Requirements* * *Maintain Safe State / Recovery* * *Non-E/E Requirements* |  | | |
| Fault Tolerant Time interval *if applicable)* | N/A | | |
| Reduced Functionality interval *(if applicable)* |  | | |
| Functional Redundancies (e.g. fault tolerance)  *(if applicable)* |  | | |
| Requirement Status |  | | |
| V&V method | Vehicle test | | |
| V&V acceptance criteria  *not applicable in case of:*   * *Non-E/E Requirements* | OTA App rejects non authentic/malicious erase or program commands that are injected onto the CAN bus using an external tool | | |
| V&V ID  *only applicable in case of:*   * *Non-E/E Requirements* |  | | |
| V&V Version  *only applicable in case of:*  *Non-E/E Requirements* |  | | |
| V&V Author  *only applicable in case of:*   * *Non-E/E Requirements* |  | | |
| V&V Status  *only applicable in case of:*   * *Non-E/E Requirements* |  | | |

Table 11: Requirement F-S-Req086 - OTA App Authenticates Erase And Programming Commands

|  |  |  |  |
| --- | --- | --- | --- |
| Safety Req-ID | **F-S-Req087 - OTA App Executes OTA Without Affecting Basic Function** | |  |
| Category | Safety Related Function | |  |
| Version  *only applicable in case of:*   * *Non-E/E Requirements* |  | |  |
| Author  *only applicable in case of:*  *Non-E/E Requirements* |  | |  |
| External Reference *(optional)* |  | | |
| Safety Goal Ref. | SG01 - Prevents Corruption of Existing Software | Operating Modes | Ignition On |
| ASIL Classification:  *if applicable in case of category*   * *General*   *not applicable in case of category*   * *Non-E/E Requirement* | D | Safe State  *if applicable for:*   * *General Requirements* * *User information* * *Non-E/E Requirements* | Software Rejected |
| Functional Safety Requirement Title | OTA App Executes OTA Without Affecting Basic Function | | |
| Functional Safety Requirement  *In case of User information including:*  *- Functional Safety Requirement Text*  *- Content of Information*  *- Method for Information*  *- Timing of Information*  *- Content of printed instructions (owner’s guide/service manuals etc.)* | The OTA App in the Target ECU shall initiate and continue flash programming without significantly affecting execution of current software including any peripheral communication. | | |
| Rationale | To avoid disrupting normal existing current software functions. For example flash when idle and ensure OTA is pre-emptible. | | |
| Description of actions of the driver or other endangered persons  *if applicable in case of:*   * *Safety Related Functions* * *Reduced Functionality* * *User information*   *not applicable in case of:*   * *General Requirements* * *Maintain Safe State / Recovery* * *Non-E/E Requirements* |  | | |
| Validation Criteria for these actions  *if applicable in case of:*   * *Safety Related Functions* * *Reduced Functionality* * *User information*   *not applicable in case of:*   * *General Requirements* * *Maintain Safe State / Recovery* * *Non-E/E Requirements* |  | | |
| Fault Tolerant Time interval *if applicable)* | 1 second | | |
| Reduced Functionality interval *(if applicable)* |  | | |
| Functional Redundancies (e.g. fault tolerance)  *(if applicable)* |  | | |
| Requirement Status |  | | |
| V&V method | Vehicle test | | |
| V&V acceptance criteria  *not applicable in case of:*   * *Non-E/E Requirements* | Perform a scheduler analysis (at a particular operating point) and then measure it again with MMOTA active.  Check for scheduler behaviour for safety software and other functionalities when MMOTA is running versus when it is not. Check for jitters or delays in the scheduling and execution of currnt SW. Is MMOTA premptible by the current SW. MMOTA should not progress or execute when the CPU load is close to maximum. | | |
| V&V ID  *only applicable in case of:*   * *Non-E/E Requirements* |  | | |
| V&V Version  *only applicable in case of:*  *Non-E/E Requirements* |  | | |
| V&V Author  *only applicable in case of:*   * *Non-E/E Requirements* |  | | |
| V&V Status  *only applicable in case of:*   * *Non-E/E Requirements* |  | | |

Table 12: Requirement F-S-Req087 - OTA App Executes OTA Without Affecting Basic Function

|  |  |  |  |
| --- | --- | --- | --- |
| Safety Req-ID | **F-S-Req088 - Other ECU SW Prevents Active Memory Erasing or Writing** | |  |
| Category | Safety Related Function | |  |
| Version  *only applicable in case of:*   * *Non-E/E Requirements* |  | |  |
| Author  *only applicable in case of:*  *Non-E/E Requirements* |  | |  |
| External Reference *(optional)* |  | | |
| Safety Goal Ref. | SG01 - Prevents Corruption of Existing Software | Operating Modes | Ignition On |
| ASIL Classification:  *if applicable in case of category*   * *General*   *not applicable in case of category*   * *Non-E/E Requirement* | D | Safe State  *if applicable for:*   * *General Requirements* * *User information* * *Non-E/E Requirements* | Software Rejected |
| Functional Safety Requirement Title | Other ECU SW Prevents Active Memory Erasing or Writing | | |
| Functional Safety Requirement  *In case of User information including:*  *- Functional Safety Requirement Text*  *- Content of Information*  *- Method for Information*  *- Timing of Information*  *- Content of printed instructions (owner’s guide/service manuals etc.)* | The Other ECU SW shall prevent writing or erasing memory sections containing the "active software". | | |
| Rationale | To avoid disrupting current software functions the OTA App should avoid memory sections containing the "active software" inclusive of program and data while an OTA is in progress). | | |
| Description of actions of the driver or other endangered persons  *if applicable in case of:*   * *Safety Related Functions* * *Reduced Functionality* * *User information*   *not applicable in case of:*   * *General Requirements* * *Maintain Safe State / Recovery* * *Non-E/E Requirements* |  | | |
| Validation Criteria for these actions  *if applicable in case of:*   * *Safety Related Functions* * *Reduced Functionality* * *User information*   *not applicable in case of:*   * *General Requirements* * *Maintain Safe State / Recovery* * *Non-E/E Requirements* |  | | |
| Fault Tolerant Time interval *if applicable)* | 1 second | | |
| Reduced Functionality interval *(if applicable)* |  | | |
| Functional Redundancies (e.g. fault tolerance)  *(if applicable)* |  | | |
| Requirement Status |  | | |
| V&V method | Vehicle test | | |
| V&V acceptance criteria  *not applicable in case of:*   * *Non-E/E Requirements* | Review if by design the OTA App can ever write into the active memory section Check via a test switch if an attempt by OTA App to write into an active memory address(fault) is prevented. | | |
| V&V ID  *only applicable in case of:*   * *Non-E/E Requirements* |  | | |
| V&V Version  *only applicable in case of:*  *Non-E/E Requirements* |  | | |
| V&V Author  *only applicable in case of:*   * *Non-E/E Requirements* |  | | |
| V&V Status  *only applicable in case of:*   * *Non-E/E Requirements* |  | | |

Table 13: Requirement F-S-Req088 - Other ECU SW Prevents Active Memory Erasing or Writing

|  |  |  |  |
| --- | --- | --- | --- |
| Safety Req-ID | **F-S-Req090 - Other ECU SW Executes OTA Without Affecting Basic Function** | |  |
| Category | Safety Related Function | |  |
| Version  *only applicable in case of:*   * *Non-E/E Requirements* |  | |  |
| Author  *only applicable in case of:*  *Non-E/E Requirements* |  | |  |
| External Reference *(optional)* |  | | |
| Safety Goal Ref. | SG01 - Prevents Corruption of Existing Software | Operating Modes | Ignition On |
| ASIL Classification:  *if applicable in case of category*   * *General*   *not applicable in case of category*   * *Non-E/E Requirement* | D | Safe State  *if applicable for:*   * *General Requirements* * *User information* * *Non-E/E Requirements* | Software Rejected |
| Functional Safety Requirement Title | Other ECU SW Executes OTA Without Affecting Basic Function | | |
| Functional Safety Requirement  *In case of User information including:*  *- Functional Safety Requirement Text*  *- Content of Information*  *- Method for Information*  *- Timing of Information*  *- Content of printed instructions (owner’s guide/service manuals etc.)* | The Other ECU SW shall execute OTA commands without affecting execution of current software including any peripheral communication (e.g. flash when idle and ensure OTA is pre-emptible). | | |
| Rationale | To avoid disrupting normal existing current software functions. | | |
| Description of actions of the driver or other endangered persons  *if applicable in case of:*   * *Safety Related Functions* * *Reduced Functionality* * *User information*   *not applicable in case of:*   * *General Requirements* * *Maintain Safe State / Recovery* * *Non-E/E Requirements* |  | | |
| Validation Criteria for these actions  *if applicable in case of:*   * *Safety Related Functions* * *Reduced Functionality* * *User information*   *not applicable in case of:*   * *General Requirements* * *Maintain Safe State / Recovery* * *Non-E/E Requirements* |  | | |
| Fault Tolerant Time interval *if applicable)* | 1 second | | |
| Reduced Functionality interval *(if applicable)* |  | | |
| Functional Redundancies (e.g. fault tolerance)  *(if applicable)* |  | | |
| Requirement Status |  | | |
| V&V method | Vehicle test | | |
| V&V acceptance criteria  *not applicable in case of:*   * *Non-E/E Requirements* | Perform a scheduler analysis (at a particular operating point) and then measure it again with MMOTA active.  Check for scheduler behaviour for safety software and other functionalities when MMOTA is running versus when it is not. Check for jitters or delays in the scheduling and execution of currnt SW. Is MMOTA premptible by the current SW. MMOTA should not progress or execute when the CPU load is close to maximum. | | |
| V&V ID  *only applicable in case of:*   * *Non-E/E Requirements* |  | | |
| V&V Version  *only applicable in case of:*  *Non-E/E Requirements* |  | | |
| V&V Author  *only applicable in case of:*   * *Non-E/E Requirements* |  | | |
| V&V Status  *only applicable in case of:*   * *Non-E/E Requirements* |  | | |

Table 14: Requirement F-S-Req090 - Other ECU SW Executes OTA Without Affecting Basic Function

|  |  |  |  |
| --- | --- | --- | --- |
| Safety Req-ID | **F-S-Req094 - Other ECU SW Executes Active Memory** | |  |
| Category | Safety Related Function | |  |
| Version  *only applicable in case of:*   * *Non-E/E Requirements* |  | |  |
| Author  *only applicable in case of:*  *Non-E/E Requirements* |  | |  |
| External Reference *(optional)* |  | | |
| Safety Goal Ref. | SG01 - Prevents Corruption of Existing Software | Operating Modes | Ignition On |
| ASIL Classification:  *if applicable in case of category*   * *General*   *not applicable in case of category*   * *Non-E/E Requirement* | D | Safe State  *if applicable for:*   * *General Requirements* * *User information* * *Non-E/E Requirements* | Target ECU not running |
| Functional Safety Requirement Title | Other ECU SW Executes Active Memory | | |
| Functional Safety Requirement  *In case of User information including:*  *- Functional Safety Requirement Text*  *- Content of Information*  *- Method for Information*  *- Timing of Information*  *- Content of printed instructions (owner’s guide/service manuals etc.)* | The Other ECU SW shall only execute software from the active memory partition. | | |
| Rationale | To avoid disrupting current software functions. | | |
| Description of actions of the driver or other endangered persons  *if applicable in case of:*   * *Safety Related Functions* * *Reduced Functionality* * *User information*   *not applicable in case of:*   * *General Requirements* * *Maintain Safe State / Recovery* * *Non-E/E Requirements* |  | | |
| Validation Criteria for these actions  *if applicable in case of:*   * *Safety Related Functions* * *Reduced Functionality* * *User information*   *not applicable in case of:*   * *General Requirements* * *Maintain Safe State / Recovery* * *Non-E/E Requirements* |  | | |
| Fault Tolerant Time interval *if applicable)* | 1 second | | |
| Reduced Functionality interval *(if applicable)* |  | | |
| Functional Redundancies (e.g. fault tolerance)  *(if applicable)* |  | | |
| Requirement Status |  | | |
| V&V method | Vehicle test | | |
| V&V acceptance criteria  *not applicable in case of:*   * *Non-E/E Requirements* | Review if by design the CPU can ever execute from the non active memory section Check via a test switch if an attempt to execute from inactive memory address(fault) is prevented. | | |
| V&V ID  *only applicable in case of:*   * *Non-E/E Requirements* |  | | |
| V&V Version  *only applicable in case of:*  *Non-E/E Requirements* |  | | |
| V&V Author  *only applicable in case of:*   * *Non-E/E Requirements* |  | | |
| V&V Status  *only applicable in case of:*   * *Non-E/E Requirements* |  | | |

Table 15: Requirement F-S-Req094 - Other ECU SW Executes Active Memory

|  |  |  |  |
| --- | --- | --- | --- |
| Safety Req-ID | **F-S-Req095 - OTA App Detects Communication Errors** | |  |
| Category | Safety Related Function | |  |
| Version  *only applicable in case of:*   * *Non-E/E Requirements* |  | |  |
| Author  *only applicable in case of:*  *Non-E/E Requirements* |  | |  |
| External Reference *(optional)* |  | | |
| Safety Goal Ref. | SG01 - Prevents Corruption of Existing Software | Operating Modes | Ignition On |
| ASIL Classification:  *if applicable in case of category*   * *General*   *not applicable in case of category*   * *Non-E/E Requirement* | **ASIL Override Rationale -** For A/B swap, the downloading of the software is in the inactive memory bank and should not affect the normal functioning of the module. Therefore failure to detect errors during software download would not violate the safety goal, especially since the software is validated right before activation.  QM | Safe State  *if applicable for:*   * *General Requirements* * *User information* * *Non-E/E Requirements* | Software Rejected |
| Functional Safety Requirement Title | OTA App Detects Communication Errors | | |
| Functional Safety Requirement  *In case of User information including:*  *- Functional Safety Requirement Text*  *- Content of Information*  *- Method for Information*  *- Timing of Information*  *- Content of printed instructions (owner’s guide/service manuals etc.)* | The OTA App in the Target ECU shall detect data corruption that may happen during communication between the OTA Feature and itself. | | |
| Rationale | So the OTA App shall be able to detect communication faults like data corruption, missing messages, messages out of sequence etc. | | |
| Description of actions of the driver or other endangered persons  *if applicable in case of:*   * *Safety Related Functions* * *Reduced Functionality* * *User information*   *not applicable in case of:*   * *General Requirements* * *Maintain Safe State / Recovery* * *Non-E/E Requirements* |  | | |
| Validation Criteria for these actions  *if applicable in case of:*   * *Safety Related Functions* * *Reduced Functionality* * *User information*   *not applicable in case of:*   * *General Requirements* * *Maintain Safe State / Recovery* * *Non-E/E Requirements* |  | | |
| Fault Tolerant Time interval *if applicable)* | N/A | | |
| Reduced Functionality interval *(if applicable)* |  | | |
| Functional Redundancies (e.g. fault tolerance)  *(if applicable)* |  | | |
| Requirement Status |  | | |
| V&V method | Vehicle test | | |
| V&V acceptance criteria  *not applicable in case of:*   * *Non-E/E Requirements* | Check if a corrupted software block from the OTA Feature is rejected by the OTA App | | |
| V&V ID  *only applicable in case of:*   * *Non-E/E Requirements* |  | | |
| V&V Version  *only applicable in case of:*  *Non-E/E Requirements* |  | | |
| V&V Author  *only applicable in case of:*   * *Non-E/E Requirements* |  | | |
| V&V Status  *only applicable in case of:*   * *Non-E/E Requirements* |  | | |

Table 16: Requirement F-S-Req095 - OTA App Detects Communication Errors

### Safety Goal SG02 – Prevents Flashing of Incorrect SW

**Name:** Prevents Flashing of Incorrect SW

**Purpose:**

**Text:**

Target ECU needs to protect up to their ASIL level

**ASIL:** D

#### Safety Concept

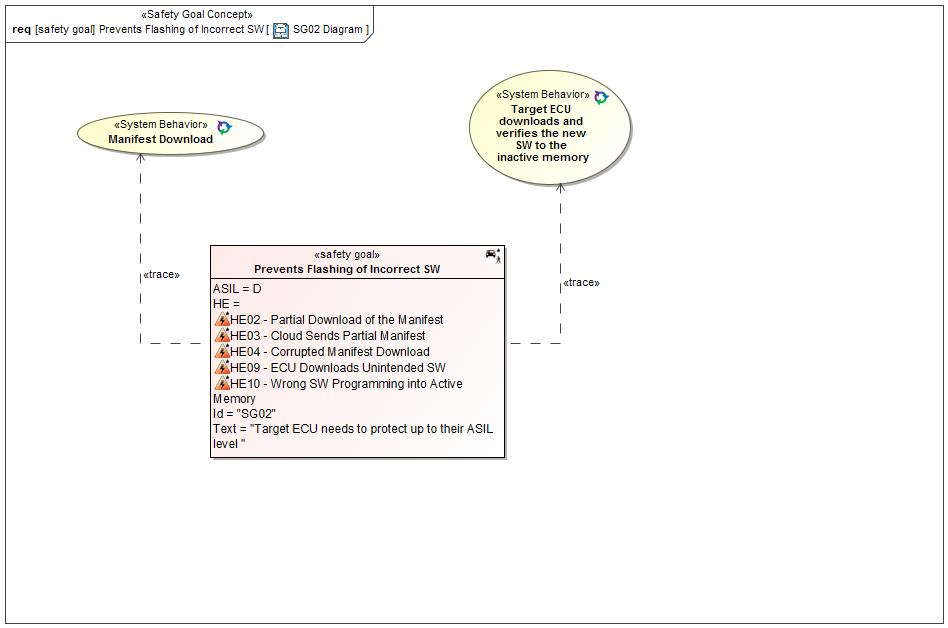


Figure 16: SG02 Diagram

#### Functional Safety Requirements

##### Requirement Derivation Diagram(s)(Optional)

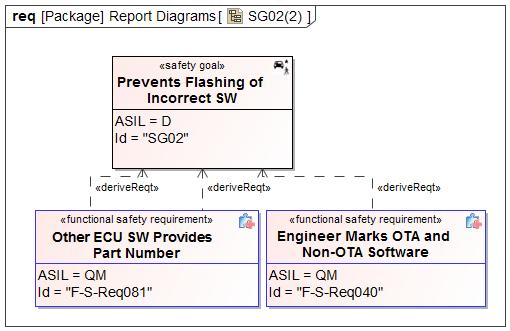


Figure 17 - Functional Safety Requirements Derivation Diagram for SG02

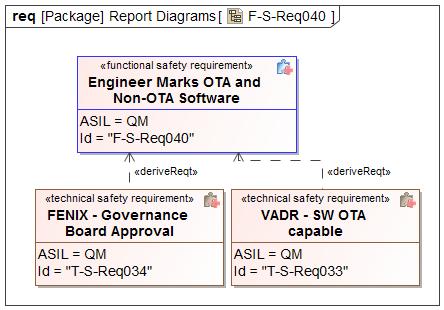


Figure 18 - Functional Safety Requirements Derivation Diagram for Engineer Marks OTA and Non-OTA Software

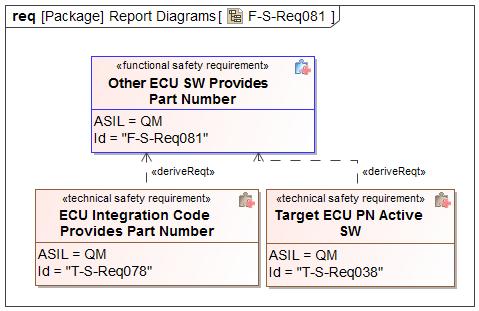


Figure 19 - Functional Safety Requirements Derivation Diagram for Other ECU SW Provides Part Number

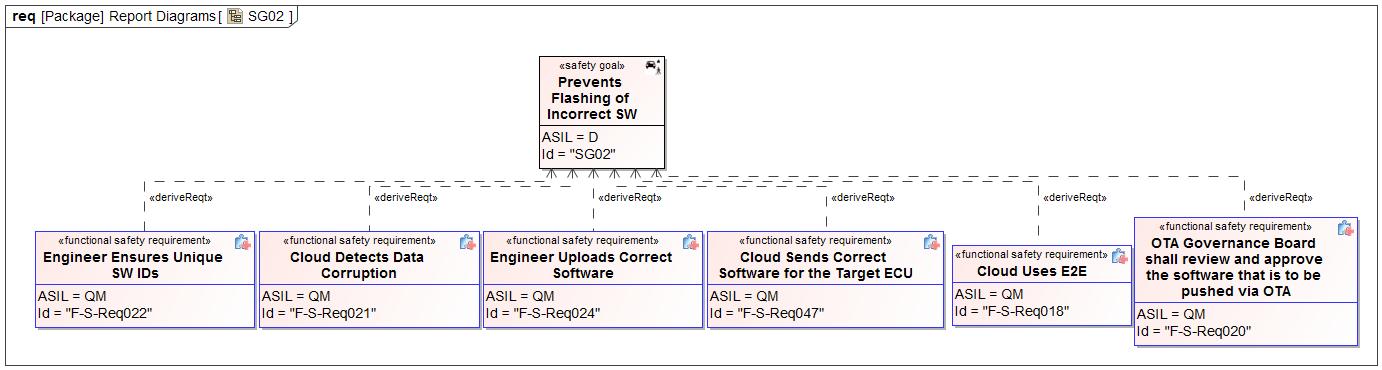


Figure 20 - Functional Safety Requirements Derivation Diagram for SG02

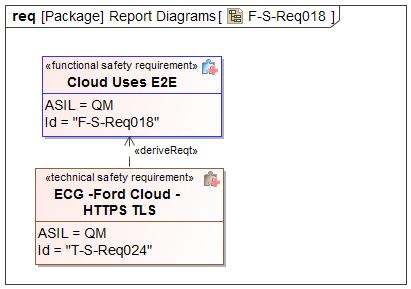


Figure 21 - Functional Safety Requirements Derivation Diagram for Cloud Uses E2E

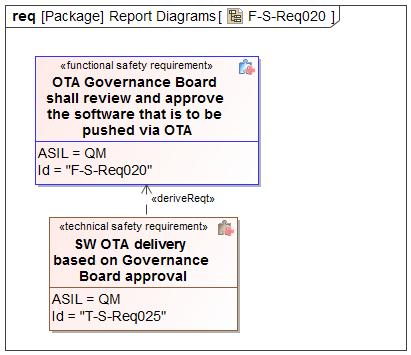


Figure 22 - Functional Safety Requirements Derivation Diagram for OTA Governance Board shall review and approve the software that is to be pushed via OTA

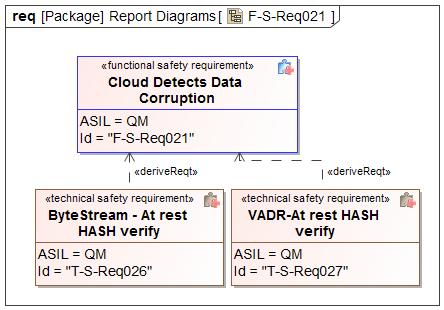


Figure 23 - Functional Safety Requirements Derivation Diagram for Cloud Detects Data Corruption

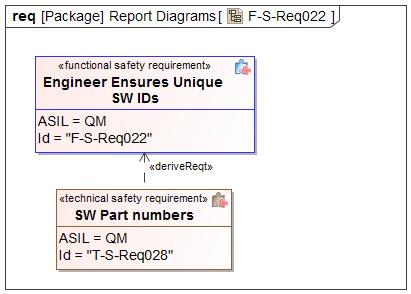


Figure 24 - Functional Safety Requirements Derivation Diagram for Engineer Ensures Unique SW IDs

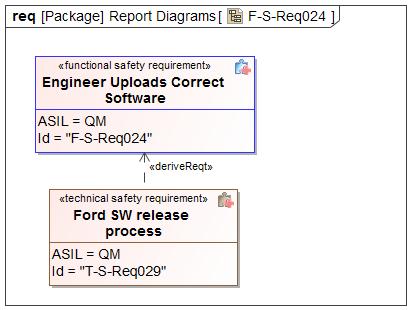


Figure 25 - Functional Safety Requirements Derivation Diagram for Engineer Uploads Correct Software

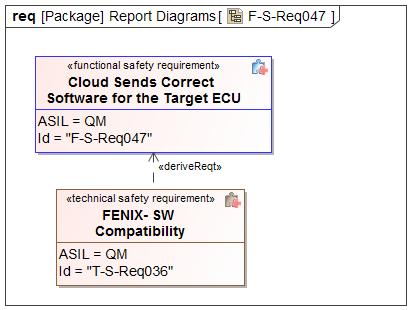


Figure 26 - Functional Safety Requirements Derivation Diagram for Cloud Sends Correct Software for the Target ECU

##### Functional Safety Requirements for SG02 - Prevents Flashing of Incorrect SW

*Insert a table for each requirement according to its category.*

|  |  |  |  |
| --- | --- | --- | --- |
| Safety Req-ID | **F-S-Req018 - Cloud Uses E2E** | |  |
| Category | Safety Related Function | |  |
| Version  *only applicable in case of:*   * *Non-E/E Requirements* |  | |  |
| Author  *only applicable in case of:*  *Non-E/E Requirements* |  | |  |
| External Reference *(optional)* |  | | |
| Safety Goal Ref. | SG02 - Prevents Flashing of Incorrect SW | Operating Modes | Ignition Off  Ignition On |
| ASIL Classification:  *if applicable in case of category*   * *General*   *not applicable in case of category*   * *Non-E/E Requirement* | **ASIL Override Rationale -** ISO 26262 ASIL rating applies only to electrical and electronic automobile systems.Therefore requirements for the cloud cannot be ASIL rated.  QM | Safe State  *if applicable for:*   * *General Requirements* * *User information* * *Non-E/E Requirements* | N/A |
| Functional Safety Requirement Title | Cloud Uses E2E | | |
| Functional Safety Requirement  *In case of User information including:*  *- Functional Safety Requirement Text*  *- Content of Information*  *- Method for Information*  *- Timing of Information*  *- Content of printed instructions (owner’s guide/service manuals etc.)* | The Cloud shall communicate with the OTA Feature over an end-to-end protected communication path. | | |
| Rationale | The system needs to be able to detect common communication faults like data corruption, missing messages, messages arriving out of order etc. The ASIL needs to be the equivalent of D as the ACTIVATION signal can be corrupted after it is sent from the Cloud and is therefore needs to be detected as it is a single point fault. | | |
| Description of actions of the driver or other endangered persons  *if applicable in case of:*   * *Safety Related Functions* * *Reduced Functionality* * *User information*   *not applicable in case of:*   * *General Requirements* * *Maintain Safe State / Recovery* * *Non-E/E Requirements* |  | | |
| Validation Criteria for these actions  *if applicable in case of:*   * *Safety Related Functions* * *Reduced Functionality* * *User information*   *not applicable in case of:*   * *General Requirements* * *Maintain Safe State / Recovery* * *Non-E/E Requirements* |  | | |
| Fault Tolerant Time interval *if applicable)* | N/A | | |
| Reduced Functionality interval *(if applicable)* |  | | |
| Functional Redundancies (e.g. fault tolerance)  *(if applicable)* |  | | |
| Requirement Status |  | | |
| V&V method | System test | | |
| V&V acceptance criteria  *not applicable in case of:*   * *Non-E/E Requirements* | Verify the cloud uses E2E criteria | | |
| V&V ID  *only applicable in case of:*   * *Non-E/E Requirements* |  | | |
| V&V Version  *only applicable in case of:*  *Non-E/E Requirements* |  | | |
| V&V Author  *only applicable in case of:*   * *Non-E/E Requirements* |  | | |
| V&V Status  *only applicable in case of:*   * *Non-E/E Requirements* |  | | |

Table 17: Requirement F-S-Req018 - Cloud Uses E2E

|  |  |  |  |
| --- | --- | --- | --- |
| Safety Req-ID | **F-S-Req020 - OTA Governance Board shall review and approve the software that is to be pushed via OTA** | |  |
| Category | Safety Related Function | |  |
| Version  *only applicable in case of:*   * *Non-E/E Requirements* |  | |  |
| Author  *only applicable in case of:*  *Non-E/E Requirements* |  | |  |
| External Reference *(optional)* |  | | |
| Safety Goal Ref. | SG02 - Prevents Flashing of Incorrect SW | Operating Modes | Ignition Off  Ignition On |
| ASIL Classification:  *if applicable in case of category*   * *General*   *not applicable in case of category*   * *Non-E/E Requirement* | **ASIL Override Rationale -** ISO 26262 ASIL rating applies only to electrical and electronic automobile systems.Therefore requirements for people cannot be ASIL rated.  QM | Safe State  *if applicable for:*   * *General Requirements* * *User information* * *Non-E/E Requirements* | N/A |
| Functional Safety Requirement Title | OTA Governance Board shall review and approve the software that is to be pushed via OTA | | |
| Functional Safety Requirement  *In case of User information including:*  *- Functional Safety Requirement Text*  *- Content of Information*  *- Method for Information*  *- Timing of Information*  *- Content of printed instructions (owner’s guide/service manuals etc.)* | OTA Governance Board shall review and approve the software that is to be pushed via OTA | | |
| Rationale | To ensure the correct SW is downloaded and switched over to (Prevent flashing of incorrect software). The Cloud determines the correct SW parts to upgrade to based on the part number list. | | |
| Description of actions of the driver or other endangered persons  *if applicable in case of:*   * *Safety Related Functions* * *Reduced Functionality* * *User information*   *not applicable in case of:*   * *General Requirements* * *Maintain Safe State / Recovery* * *Non-E/E Requirements* |  | | |
| Validation Criteria for these actions  *if applicable in case of:*   * *Safety Related Functions* * *Reduced Functionality* * *User information*   *not applicable in case of:*   * *General Requirements* * *Maintain Safe State / Recovery* * *Non-E/E Requirements* |  | | |
| Fault Tolerant Time interval *if applicable)* | N/A | | |
| Reduced Functionality interval *(if applicable)* |  | | |
| Functional Redundancies (e.g. fault tolerance)  *(if applicable)* |  | | |
| Requirement Status |  | | |
| V&V method | System test | | |
| V&V acceptance criteria  *not applicable in case of:*   * *Non-E/E Requirements* | Check if the Cloud rejects a corrupted part number list | | |
| V&V ID  *only applicable in case of:*   * *Non-E/E Requirements* |  | | |
| V&V Version  *only applicable in case of:*  *Non-E/E Requirements* |  | | |
| V&V Author  *only applicable in case of:*   * *Non-E/E Requirements* |  | | |
| V&V Status  *only applicable in case of:*   * *Non-E/E Requirements* |  | | |

Table 18: Requirement F-S-Req020 - OTA Governance Board shall review and approve the software that is to be pushed via OTA

|  |  |  |  |
| --- | --- | --- | --- |
| Safety Req-ID | **F-S-Req021 - Cloud Detects Data Corruption** | |  |
| Category | Safety Related Function | |  |
| Version  *only applicable in case of:*   * *Non-E/E Requirements* |  | |  |
| Author  *only applicable in case of:*  *Non-E/E Requirements* |  | |  |
| External Reference *(optional)* |  | | |
| Safety Goal Ref. | SG02 - Prevents Flashing of Incorrect SW | Operating Modes | Ignition Off  Ignition On |
| ASIL Classification:  *if applicable in case of category*   * *General*   *not applicable in case of category*   * *Non-E/E Requirement* | **ASIL Override Rationale -** ISO 26262 ASIL rating applies only to electrical and electronic automobile systems.Therefore requirements for the cloud cannot be ASIL rated.  QM | Safe State  *if applicable for:*   * *General Requirements* * *User information* * *Non-E/E Requirements* | Software Rejected |
| Functional Safety Requirement Title | Cloud Detects Data Corruption | | |
| Functional Safety Requirement  *In case of User information including:*  *- Functional Safety Requirement Text*  *- Content of Information*  *- Method for Information*  *- Timing of Information*  *- Content of printed instructions (owner’s guide/service manuals etc.)* | The Cloud shall detect data corruption during reception and storage of software from Ford. | | |
| Rationale | To prevent data corruption that may happen during upload or while storage from cascading downstream (Data corruption during software download shall be detectable). | | |
| Description of actions of the driver or other endangered persons  *if applicable in case of:*   * *Safety Related Functions* * *Reduced Functionality* * *User information*   *not applicable in case of:*   * *General Requirements* * *Maintain Safe State / Recovery* * *Non-E/E Requirements* |  | | |
| Validation Criteria for these actions  *if applicable in case of:*   * *Safety Related Functions* * *Reduced Functionality* * *User information*   *not applicable in case of:*   * *General Requirements* * *Maintain Safe State / Recovery* * *Non-E/E Requirements* |  | | |
| Fault Tolerant Time interval *if applicable)* | N/A | | |
| Reduced Functionality interval *(if applicable)* |  | | |
| Functional Redundancies (e.g. fault tolerance)  *(if applicable)* |  | | |
| Requirement Status |  | | |
| V&V method | System test | | |
| V&V acceptance criteria  *not applicable in case of:*   * *Non-E/E Requirements* | Cloud software should be able to flag that software is corrupted | | |
| V&V ID  *only applicable in case of:*   * *Non-E/E Requirements* |  | | |
| V&V Version  *only applicable in case of:*  *Non-E/E Requirements* |  | | |
| V&V Author  *only applicable in case of:*   * *Non-E/E Requirements* |  | | |
| V&V Status  *only applicable in case of:*   * *Non-E/E Requirements* |  | | |

Table 19: Requirement F-S-Req021 - Cloud Detects Data Corruption

|  |  |  |  |
| --- | --- | --- | --- |
| Safety Req-ID | **F-S-Req022 - Engineer Ensures Unique SW IDs** | |  |
| Category | Safety Related Function | |  |
| Version  *only applicable in case of:*   * *Non-E/E Requirements* |  | |  |
| Author  *only applicable in case of:*  *Non-E/E Requirements* |  | |  |
| External Reference *(optional)* |  | | |
| Safety Goal Ref. | SG02 - Prevents Flashing of Incorrect SW | Operating Modes | Ignition Off  Ignition On |
| ASIL Classification:  *if applicable in case of category*   * *General*   *not applicable in case of category*   * *Non-E/E Requirement* | **ASIL Override Rationale -** ISO 26262 ASIL rating applies only to electrical and electronic automobile systems.Therefore requirements for people cannot be ASIL rated.  QM | Safe State  *if applicable for:*   * *General Requirements* * *User information* * *Non-E/E Requirements* | N/A |
| Functional Safety Requirement Title | Engineer Ensures Unique SW IDs | | |
| Functional Safety Requirement  *In case of User information including:*  *- Functional Safety Requirement Text*  *- Content of Information*  *- Method for Information*  *- Timing of Information*  *- Content of printed instructions (owner’s guide/service manuals etc.)* | The D&R engineer shall ensure each unique OTA SW version has a unique identifier. | | |
| Rationale | To ensure the correct SW is downloaded (Prevent flashing of incorrect software). | | |
| Description of actions of the driver or other endangered persons  *if applicable in case of:*   * *Safety Related Functions* * *Reduced Functionality* * *User information*   *not applicable in case of:*   * *General Requirements* * *Maintain Safe State / Recovery* * *Non-E/E Requirements* |  | | |
| Validation Criteria for these actions  *if applicable in case of:*   * *Safety Related Functions* * *Reduced Functionality* * *User information*   *not applicable in case of:*   * *General Requirements* * *Maintain Safe State / Recovery* * *Non-E/E Requirements* |  | | |
| Fault Tolerant Time interval *if applicable)* | N/A | | |
| Reduced Functionality interval *(if applicable)* |  | | |
| Functional Redundancies (e.g. fault tolerance)  *(if applicable)* |  | | |
| Requirement Status |  | | |
| V&V method | Peer review | | |
| V&V acceptance criteria  *not applicable in case of:*   * *Non-E/E Requirements* | Verify the process steps involved in the release of new software to the cloud. | | |
| V&V ID  *only applicable in case of:*   * *Non-E/E Requirements* |  | | |
| V&V Version  *only applicable in case of:*  *Non-E/E Requirements* |  | | |
| V&V Author  *only applicable in case of:*   * *Non-E/E Requirements* |  | | |
| V&V Status  *only applicable in case of:*   * *Non-E/E Requirements* |  | | |

Table 20: Requirement F-S-Req022 - Engineer Ensures Unique SW IDs

|  |  |  |  |
| --- | --- | --- | --- |
| Safety Req-ID | **F-S-Req024 - Engineer Uploads Correct Software** | |  |
| Category | Safety Related Function | |  |
| Version  *only applicable in case of:*   * *Non-E/E Requirements* |  | |  |
| Author  *only applicable in case of:*  *Non-E/E Requirements* |  | |  |
| External Reference *(optional)* |  | | |
| Safety Goal Ref. | SG02 - Prevents Flashing of Incorrect SW | Operating Modes | Ignition Off  Ignition On |
| ASIL Classification:  *if applicable in case of category*   * *General*   *not applicable in case of category*   * *Non-E/E Requirement* | **ASIL Override Rationale -** ISO 26262 ASIL rating applies only to electrical and electronic automobile systems.Therefore requirements for people cannot be ASIL rated.  QM | Safe State  *if applicable for:*   * *General Requirements* * *User information* * *Non-E/E Requirements* | N/A |
| Functional Safety Requirement Title | Engineer Uploads Correct Software | | |
| Functional Safety Requirement  *In case of User information including:*  *- Functional Safety Requirement Text*  *- Content of Information*  *- Method for Information*  *- Timing of Information*  *- Content of printed instructions (owner’s guide/service manuals etc.)* | The D&R engineer shall release the correct version(s) of software onto the cloud. | | |
| Rationale | To ensure the correct SW is downloaded (Prevent flashing of incorrect software). | | |
| Description of actions of the driver or other endangered persons  *if applicable in case of:*   * *Safety Related Functions* * *Reduced Functionality* * *User information*   *not applicable in case of:*   * *General Requirements* * *Maintain Safe State / Recovery* * *Non-E/E Requirements* |  | | |
| Validation Criteria for these actions  *if applicable in case of:*   * *Safety Related Functions* * *Reduced Functionality* * *User information*   *not applicable in case of:*   * *General Requirements* * *Maintain Safe State / Recovery* * *Non-E/E Requirements* |  | | |
| Fault Tolerant Time interval *if applicable)* | N/A | | |
| Reduced Functionality interval *(if applicable)* |  | | |
| Functional Redundancies (e.g. fault tolerance)  *(if applicable)* |  | | |
| Requirement Status |  | | |
| V&V method | Peer review | | |
| V&V acceptance criteria  *not applicable in case of:*   * *Non-E/E Requirements* | Verify the process steps involved in the release of new software to the cloud. If required do a PFMEA to identify weaknesses. | | |
| V&V ID  *only applicable in case of:*   * *Non-E/E Requirements* |  | | |
| V&V Version  *only applicable in case of:*  *Non-E/E Requirements* |  | | |
| V&V Author  *only applicable in case of:*   * *Non-E/E Requirements* |  | | |
| V&V Status  *only applicable in case of:*   * *Non-E/E Requirements* |  | | |

Table 21: Requirement F-S-Req024 - Engineer Uploads Correct Software

Please see the Functional Safety Requirement table for [Cloud Authenticates Software Update](#_4ca51e01184a59be985def8aa360adf7) displayed under the Safety Goal SG01.

Please see the Functional Safety Requirement table for [OTA Feature Detects Data Corruption](#_76f74d3d6f97e104e86d7f82f8a1ddf2) displayed under the Safety Goal SG01.

|  |  |  |  |
| --- | --- | --- | --- |
| Safety Req-ID | **F-S-Req033 - OTA Feature Detects Invalid Software** | |  |
| Category | Safety Related Function | |  |
| Version  *only applicable in case of:*   * *Non-E/E Requirements* |  | |  |
| Author  *only applicable in case of:*  *Non-E/E Requirements* |  | |  |
| External Reference *(optional)* |  | | |
| Safety Goal Ref. | SG02 - Prevents Flashing of Incorrect SW  SG04 - Ensure Safe Verification of Activation | Operating Modes | Ignition On |
| ASIL Classification:  *if applicable in case of category*   * *General*   *not applicable in case of category*   * *Non-E/E Requirement* | **ASIL Override Rationale -** Failure to detect invalid software during download would not lead to a violation of the safety goal since the software is not used immediately but placed in inactive memory. The software is validated before being activated.  QM | Safe State  *if applicable for:*   * *General Requirements* * *User information* * *Non-E/E Requirements* | Software Rejected |
| Functional Safety Requirement Title | OTA Feature Detects Invalid Software | | |
| Functional Safety Requirement  *In case of User information including:*  *- Functional Safety Requirement Text*  *- Content of Information*  *- Method for Information*  *- Timing of Information*  *- Content of printed instructions (owner’s guide/service manuals etc.)* | The OTA Feature shall detect incorrect software. | | |
| Rationale | To be able to detect invalid software downloads in order to prevent malfunctions due to erroneous software. | | |
| Description of actions of the driver or other endangered persons  *if applicable in case of:*   * *Safety Related Functions* * *Reduced Functionality* * *User information*   *not applicable in case of:*   * *General Requirements* * *Maintain Safe State / Recovery* * *Non-E/E Requirements* |  | | |
| Validation Criteria for these actions  *if applicable in case of:*   * *Safety Related Functions* * *Reduced Functionality* * *User information*   *not applicable in case of:*   * *General Requirements* * *Maintain Safe State / Recovery* * *Non-E/E Requirements* |  | | |
| Fault Tolerant Time interval *if applicable)* | N/A | | |
| Reduced Functionality interval *(if applicable)* |  | | |
| Functional Redundancies (e.g. fault tolerance)  *(if applicable)* |  | | |
| Requirement Status |  | | |
| V&V method | Vehicle test | | |
| V&V acceptance criteria  *not applicable in case of:*   * *Non-E/E Requirements* | The OTA Feature detects incorrect software. | | |
| V&V ID  *only applicable in case of:*   * *Non-E/E Requirements* |  | | |
| V&V Version  *only applicable in case of:*  *Non-E/E Requirements* |  | | |
| V&V Author  *only applicable in case of:*   * *Non-E/E Requirements* |  | | |
| V&V Status  *only applicable in case of:*   * *Non-E/E Requirements* |  | | |

Table 22: Requirement F-S-Req033 - OTA Feature Detects Invalid Software

|  |  |  |  |
| --- | --- | --- | --- |
| Safety Req-ID | **F-S-Req040 - Engineer Marks OTA and Non-OTA Software** | |  |
| Category | Safety Related Function | |  |
| Version  *only applicable in case of:*   * *Non-E/E Requirements* |  | |  |
| Author  *only applicable in case of:*  *Non-E/E Requirements* |  | |  |
| External Reference *(optional)* |  | | |
| Safety Goal Ref. | SG02 - Prevents Flashing of Incorrect SW | Operating Modes | Ignition Off  Ignition On |
| ASIL Classification:  *if applicable in case of category*   * *General*   *not applicable in case of category*   * *Non-E/E Requirement* | **ASIL Override Rationale -** ISO 26262 ASIL rating applies only to electrical and electronic automobile systems.Therefore requirements for people cannot be ASIL rated.  QM | Safe State  *if applicable for:*   * *General Requirements* * *User information* * *Non-E/E Requirements* | N/A |
| Functional Safety Requirement Title | Engineer Marks OTA and Non-OTA Software | | |
| Functional Safety Requirement  *In case of User information including:*  *- Functional Safety Requirement Text*  *- Content of Information*  *- Method for Information*  *- Timing of Information*  *- Content of printed instructions (owner’s guide/service manuals etc.)* | The D&R engineer shall mark non OTA compatible SW parts as ”non-compatible” in the cloud. | | |
| Rationale | OTA non compatible software should not be sent for a reflash. To ensure the correct SW is downloaded (Prevent flashing of incorrect software). | | |
| Description of actions of the driver or other endangered persons  *if applicable in case of:*   * *Safety Related Functions* * *Reduced Functionality* * *User information*   *not applicable in case of:*   * *General Requirements* * *Maintain Safe State / Recovery* * *Non-E/E Requirements* |  | | |
| Validation Criteria for these actions  *if applicable in case of:*   * *Safety Related Functions* * *Reduced Functionality* * *User information*   *not applicable in case of:*   * *General Requirements* * *Maintain Safe State / Recovery* * *Non-E/E Requirements* |  | | |
| Fault Tolerant Time interval *if applicable)* | N/A | | |
| Reduced Functionality interval *(if applicable)* |  | | |
| Functional Redundancies (e.g. fault tolerance)  *(if applicable)* |  | | |
| Requirement Status |  | | |
| V&V method | Peer review | | |
| V&V acceptance criteria  *not applicable in case of:*   * *Non-E/E Requirements* | Verify the process steps involved in the release of new software to the cloud. If required do a PFMEA to identify weaknesses. | | |
| V&V ID  *only applicable in case of:*   * *Non-E/E Requirements* |  | | |
| V&V Version  *only applicable in case of:*  *Non-E/E Requirements* |  | | |
| V&V Author  *only applicable in case of:*   * *Non-E/E Requirements* |  | | |
| V&V Status  *only applicable in case of:*   * *Non-E/E Requirements* |  | | |

Table 23: Requirement F-S-Req040 - Engineer Marks OTA and Non-OTA Software

Please see the Functional Safety Requirement table for [OTA Feature Authenticates Cloud Connection](#_efd36d91e07c56151380e9b74df9ad0a) displayed under the Safety Goal SG01.

Please see the Functional Safety Requirement table for [OTA Feature Communicates E2E with the Cloud](#_a458b919ab42ff23acd4fea432087958) displayed under the Safety Goal SG01.

|  |  |  |  |
| --- | --- | --- | --- |
| Safety Req-ID | **F-S-Req047 - Cloud Sends Correct Software for the Target ECU** | |  |
| Category | Safety Related Function | |  |
| Version  *only applicable in case of:*   * *Non-E/E Requirements* |  | |  |
| Author  *only applicable in case of:*  *Non-E/E Requirements* |  | |  |
| External Reference *(optional)* |  | | |
| Safety Goal Ref. | SG02 - Prevents Flashing of Incorrect SW | Operating Modes | Ignition Off  Ignition On |
| ASIL Classification:  *if applicable in case of category*   * *General*   *not applicable in case of category*   * *Non-E/E Requirement* | **ASIL Override Rationale -** ISO 26262 ASIL rating applies only to electrical and electronic automobile systems. Therefore requirements for the cloud cannot be ASIL rated.  QM | Safe State  *if applicable for:*   * *General Requirements* * *User information* * *Non-E/E Requirements* | N/A |
| Functional Safety Requirement Title | Cloud Sends Correct Software for the Target ECU | | |
| Functional Safety Requirement  *In case of User information including:*  *- Functional Safety Requirement Text*  *- Content of Information*  *- Method for Information*  *- Timing of Information*  *- Content of printed instructions (owner’s guide/service manuals etc.)* | The Cloud shall send the correct software for each respective ECU to the OTA Feature. | | |
| Rationale | To ensure the correct SW part is downloaded (Prevent flashing of incorrect software). | | |
| Description of actions of the driver or other endangered persons  *if applicable in case of:*   * *Safety Related Functions* * *Reduced Functionality* * *User information*   *not applicable in case of:*   * *General Requirements* * *Maintain Safe State / Recovery* * *Non-E/E Requirements* |  | | |
| Validation Criteria for these actions  *if applicable in case of:*   * *Safety Related Functions* * *Reduced Functionality* * *User information*   *not applicable in case of:*   * *General Requirements* * *Maintain Safe State / Recovery* * *Non-E/E Requirements* |  | | |
| Fault Tolerant Time interval *if applicable)* | N/A | | |
| Reduced Functionality interval *(if applicable)* |  | | |
| Functional Redundancies (e.g. fault tolerance)  *(if applicable)* |  | | |
| Requirement Status |  | | |
| V&V method | System test | | |
| V&V acceptance criteria  *not applicable in case of:*   * *Non-E/E Requirements* | The SW part sent by the Cloud for a target ECU should be a valid SW part for the reflash ( e.g AB or BA send for AA) | | |
| V&V ID  *only applicable in case of:*   * *Non-E/E Requirements* |  | | |
| V&V Version  *only applicable in case of:*  *Non-E/E Requirements* |  | | |
| V&V Author  *only applicable in case of:*   * *Non-E/E Requirements* |  | | |
| V&V Status  *only applicable in case of:*   * *Non-E/E Requirements* |  | | |

Table 24: Requirement F-S-Req047 - Cloud Sends Correct Software for the Target ECU

Please see the Functional Safety Requirement table for [OTA Feature Informs the Cloud of Data Corruption](#_d1f561bf9e8a4063ad777e30bc18134f) displayed under the Safety Goal SG01.

|  |  |  |  |
| --- | --- | --- | --- |
| Safety Req-ID | **F-S-Req059 - Cloud and Engineers Ensure Correct Software is Flashed** | |  |
| Category | Safety Related Function | |  |
| Version  *only applicable in case of:*   * *Non-E/E Requirements* |  | |  |
| Author  *only applicable in case of:*  *Non-E/E Requirements* |  | |  |
| External Reference *(optional)* |  | | |
| Safety Goal Ref. |  | Operating Modes | Ignition Off  Ignition On |
| ASIL Classification:  *if applicable in case of category*   * *General*   *not applicable in case of category*   * *Non-E/E Requirement* | **ASIL Override Rationale -** ISO 26262 ASIL rating applies only to electrical and electronic automobile systems.Therefore the cloud and engineers cannot get ASIL rated requirements.  QM | Safe State  *if applicable for:*   * *General Requirements* * *User information* * *Non-E/E Requirements* | Software Rejected |
| Functional Safety Requirement Title | Cloud and Engineers Ensure Correct Software is Flashed | | |
| Functional Safety Requirement  *In case of User information including:*  *- Functional Safety Requirement Text*  *- Content of Information*  *- Method for Information*  *- Timing of Information*  *- Content of printed instructions (owner’s guide/service manuals etc.)* | The Cloud and Engineers shall ensure correct software is flashed. | | |
| Rationale | To prevent a malfunction of the MMOTA feature from causing the highest level hazard in the target ECU. | | |
| Description of actions of the driver or other endangered persons  *if applicable in case of:*   * *Safety Related Functions* * *Reduced Functionality* * *User information*   *not applicable in case of:*   * *General Requirements* * *Maintain Safe State / Recovery* * *Non-E/E Requirements* |  | | |
| Validation Criteria for these actions  *if applicable in case of:*   * *Safety Related Functions* * *Reduced Functionality* * *User information*   *not applicable in case of:*   * *General Requirements* * *Maintain Safe State / Recovery* * *Non-E/E Requirements* |  | | |
| Fault Tolerant Time interval *if applicable)* | N/A | | |
| Reduced Functionality interval *(if applicable)* |  | | |
| Functional Redundancies (e.g. fault tolerance)  *(if applicable)* |  | | |
| Requirement Status |  | | |
| V&V method | System test | | |
| V&V acceptance criteria  *not applicable in case of:*   * *Non-E/E Requirements* | The Cloud and Engineers ensure correct software is flashed | | |
| V&V ID  *only applicable in case of:*   * *Non-E/E Requirements* |  | | |
| V&V Version  *only applicable in case of:*  *Non-E/E Requirements* |  | | |
| V&V Author  *only applicable in case of:*   * *Non-E/E Requirements* |  | | |
| V&V Status  *only applicable in case of:*   * *Non-E/E Requirements* |  | | |

Table 25: Requirement F-S-Req059 - Cloud and Engineers Ensure Correct Software is Flashed

Please see the Functional Safety Requirement table for [OTA App Detects Data Corruption During Software Download](#_0344dfc0fe65adce2f0ab2d4179cd7f1) displayed under the Safety Goal SG01.

Please see the Functional Safety Requirement table for [OTA Feature Detects Data Corruption During Software Download](#_469e6e08115ee3fecea46961210e32dd) displayed under the Safety Goal SG01.

|  |  |  |  |
| --- | --- | --- | --- |
| Safety Req-ID | **F-S-Req081 - Other ECU SW Provides Part Number** | |  |
| Category | Safety Related Function | |  |
| Version  *only applicable in case of:*   * *Non-E/E Requirements* |  | |  |
| Author  *only applicable in case of:*  *Non-E/E Requirements* |  | |  |
| External Reference *(optional)* |  | | |
| Safety Goal Ref. | SG02 - Prevents Flashing of Incorrect SW | Operating Modes | Ignition On |
| ASIL Classification:  *if applicable in case of category*   * *General*   *not applicable in case of category*   * *Non-E/E Requirement* | **ASIL Override Rationale -** A failure to send the part number would not violate the safety goal of the module since the process would not get to the activation state  QM | Safe State  *if applicable for:*   * *General Requirements* * *User information* * *Non-E/E Requirements* | New software not activated |
| Functional Safety Requirement Title | Other ECU SW Provides Part Number | | |
| Functional Safety Requirement  *In case of User information including:*  *- Functional Safety Requirement Text*  *- Content of Information*  *- Method for Information*  *- Timing of Information*  *- Content of printed instructions (owner’s guide/service manuals etc.)* | Upon request from the OTA App in the Target ECU, the Other ECU SW shall provide the correct part number. | | |
| Rationale | To ensure the Other ECU SW does not sent wrong part numbers. | | |
| Description of actions of the driver or other endangered persons  *if applicable in case of:*   * *Safety Related Functions* * *Reduced Functionality* * *User information*   *not applicable in case of:*   * *General Requirements* * *Maintain Safe State / Recovery* * *Non-E/E Requirements* |  | | |
| Validation Criteria for these actions  *if applicable in case of:*   * *Safety Related Functions* * *Reduced Functionality* * *User information*   *not applicable in case of:*   * *General Requirements* * *Maintain Safe State / Recovery* * *Non-E/E Requirements* |  | | |
| Fault Tolerant Time interval *if applicable)* | N/A | | |
| Reduced Functionality interval *(if applicable)* |  | | |
| Functional Redundancies (e.g. fault tolerance)  *(if applicable)* |  | | |
| Requirement Status |  | | |
| V&V method | Vehicle test | | |
| V&V acceptance criteria  *not applicable in case of:*   * *Non-E/E Requirements* | Check if the correct part number is being sent | | |
| V&V ID  *only applicable in case of:*   * *Non-E/E Requirements* |  | | |
| V&V Version  *only applicable in case of:*  *Non-E/E Requirements* |  | | |
| V&V Author  *only applicable in case of:*   * *Non-E/E Requirements* |  | | |
| V&V Status  *only applicable in case of:*   * *Non-E/E Requirements* |  | | |

Table 26: Requirement F-S-Req081 - Other ECU SW Provides Part Number

Please see the Functional Safety Requirement table for [OTA App Prevents Active Memory Erasing or Writing](#_0ad92bdb6a99e3d10ce1dc0d0a77e60a) displayed under the Safety Goal SG01.

Please see the Functional Safety Requirement table for [OTA App Informs the OTA Feature of Data Corruption](#_360bdf0d5ab05912ccfeafc1f7b16cad) displayed under the Safety Goal SG01.

Please see the Functional Safety Requirement table for [OTA App Authenticates Erase And Programming Commands](#_e63467aecb84419c92184c8c6805edc0) displayed under the Safety Goal SG01.

Please see the Functional Safety Requirement table for [OTA App Executes OTA Without Affecting Basic Function](#_27bc942123bd1574d78bbd287b70358c) displayed under the Safety Goal SG01.

Please see the Functional Safety Requirement table for [Other ECU SW Prevents Active Memory Erasing or Writing](#_2fad9e75d48a85a9587e37c286f61f5d) displayed under the Safety Goal SG01.

Please see the Functional Safety Requirement table for [Other ECU SW Executes OTA Without Affecting Basic Function](#_25f65ce1928c94d70c987c03951c4b4e) displayed under the Safety Goal SG01.

|  |  |  |  |
| --- | --- | --- | --- |
| Safety Req-ID | **F-S-Req091 - OTA App rejects Invalid Software** | |  |
| Category | Safety Related Function | |  |
| Version  *only applicable in case of:*   * *Non-E/E Requirements* |  | |  |
| Author  *only applicable in case of:*  *Non-E/E Requirements* |  | |  |
| External Reference *(optional)* |  | | |
| Safety Goal Ref. | SG02 - Prevents Flashing of Incorrect SW  SG04 - Ensure Safe Verification of Activation | Operating Modes | Ignition On |
| ASIL Classification:  *if applicable in case of category*   * *General*   *not applicable in case of category*   * *Non-E/E Requirement* | **ASIL Override Rationale -** For A/B swap, the downloading of the software is in the inactive memory bank and should not affect the normal functioning of the module. Therefore failure to reject the invalid software would not violate the safety goal especially since the software is validated right before activation.  QM | Safe State  *if applicable for:*   * *General Requirements* * *User information* * *Non-E/E Requirements* | Software Rejected |
| Functional Safety Requirement Title | OTA App rejects Invalid Software | | |
| Functional Safety Requirement  *In case of User information including:*  *- Functional Safety Requirement Text*  *- Content of Information*  *- Method for Information*  *- Timing of Information*  *- Content of printed instructions (owner’s guide/service manuals etc.)* | The OTA App in the Target ECU shall reject software that is not meant for the Target ECU. | | |
| Rationale | To be able to detect invalid software downloads in order to prevent malfunctions due to erroneous software. | | |
| Description of actions of the driver or other endangered persons  *if applicable in case of:*   * *Safety Related Functions* * *Reduced Functionality* * *User information*   *not applicable in case of:*   * *General Requirements* * *Maintain Safe State / Recovery* * *Non-E/E Requirements* |  | | |
| Validation Criteria for these actions  *if applicable in case of:*   * *Safety Related Functions* * *Reduced Functionality* * *User information*   *not applicable in case of:*   * *General Requirements* * *Maintain Safe State / Recovery* * *Non-E/E Requirements* |  | | |
| Fault Tolerant Time interval *if applicable)* | N/A | | |
| Reduced Functionality interval *(if applicable)* |  | | |
| Functional Redundancies (e.g. fault tolerance)  *(if applicable)* |  | | |
| Requirement Status |  | | |
| V&V method | Vehicle test | | |
| V&V acceptance criteria  *not applicable in case of:*   * *Non-E/E Requirements* | The OTA App shall rejects software that is not meant for the Target ECU | | |
| V&V ID  *only applicable in case of:*   * *Non-E/E Requirements* |  | | |
| V&V Version  *only applicable in case of:*  *Non-E/E Requirements* |  | | |
| V&V Author  *only applicable in case of:*   * *Non-E/E Requirements* |  | | |
| V&V Status  *only applicable in case of:*   * *Non-E/E Requirements* |  | | |

Table 27: Requirement F-S-Req091 - OTA App rejects Invalid Software

|  |  |  |  |
| --- | --- | --- | --- |
| Safety Req-ID | **F-S-Req092 - OTA App Sends Correct Part Number** | |  |
| Category | Safety Related Function | |  |
| Version  *only applicable in case of:*   * *Non-E/E Requirements* |  | |  |
| Author  *only applicable in case of:*  *Non-E/E Requirements* |  | |  |
| External Reference *(optional)* |  | | |
| Safety Goal Ref. | SG02 - Prevents Flashing of Incorrect SW  SG04 - Ensure Safe Verification of Activation | Operating Modes | Ignition On |
| ASIL Classification:  *if applicable in case of category*   * *General*   *not applicable in case of category*   * *Non-E/E Requirement* | **ASIL Override Rationale -** Failure to send the part number would not violate the safety goal especially since activation process would not begin without the right part numbers and the module would remain in its current safe software.  QM | Safe State  *if applicable for:*   * *General Requirements* * *User information* * *Non-E/E Requirements* | New software not activated |
| Functional Safety Requirement Title | OTA App Sends Correct Part Number | | |
| Functional Safety Requirement  *In case of User information including:*  *- Functional Safety Requirement Text*  *- Content of Information*  *- Method for Information*  *- Timing of Information*  *- Content of printed instructions (owner’s guide/service manuals etc.)* | The OTA App in the Target ECU shall send the correct part number to the OTA Feature upon request from the OTA Feature. | | |
| Rationale | To ensure the OTA App does not sent wrong part numbers. | | |
| Description of actions of the driver or other endangered persons  *if applicable in case of:*   * *Safety Related Functions* * *Reduced Functionality* * *User information*   *not applicable in case of:*   * *General Requirements* * *Maintain Safe State / Recovery* * *Non-E/E Requirements* |  | | |
| Validation Criteria for these actions  *if applicable in case of:*   * *Safety Related Functions* * *Reduced Functionality* * *User information*   *not applicable in case of:*   * *General Requirements* * *Maintain Safe State / Recovery* * *Non-E/E Requirements* |  | | |
| Fault Tolerant Time interval *if applicable)* | N/A | | |
| Reduced Functionality interval *(if applicable)* |  | | |
| Functional Redundancies (e.g. fault tolerance)  *(if applicable)* |  | | |
| Requirement Status |  | | |
| V&V method | Vehicle test | | |
| V&V acceptance criteria  *not applicable in case of:*   * *Non-E/E Requirements* | Check if the correct part number is being sent | | |
| V&V ID  *only applicable in case of:*   * *Non-E/E Requirements* |  | | |
| V&V Version  *only applicable in case of:*  *Non-E/E Requirements* |  | | |
| V&V Author  *only applicable in case of:*   * *Non-E/E Requirements* |  | | |
| V&V Status  *only applicable in case of:*   * *Non-E/E Requirements* |  | | |

Table 28: Requirement F-S-Req092 - OTA App Sends Correct Part Number

Please see the Functional Safety Requirement table for [Other ECU SW Executes Active Memory](#_b8e39606250fba93cad1eea6e2003901) displayed under the Safety Goal SG01.

Please see the Functional Safety Requirement table for [OTA App Detects Communication Errors](#_9532234d56f31920200b2f5b2b4c28c4) displayed under the Safety Goal SG01.

|  |  |  |  |
| --- | --- | --- | --- |
| Safety Req-ID | **F-S-Req111 - Cloud and OTA Supervisor Communicates Manifest Securely** | |  |
| Category | Safety Related Function | |  |
| Version  *only applicable in case of:*   * *Non-E/E Requirements* |  | |  |
| Author  *only applicable in case of:*  *Non-E/E Requirements* |  | |  |
| External Reference *(optional)* |  | | |
| Safety Goal Ref. |  | Operating Modes | Ignition On |
| ASIL Classification:  *if applicable in case of category*   * *General*   *not applicable in case of category*   * *Non-E/E Requirement* | **ASIL Override Rationale -** ISO 26262 ASIL rating applies only to electrical and electronic automobile systems. Therefore requirements for the cloud cannot be ASIL rated.  QM | Safe State  *if applicable for:*   * *General Requirements* * *User information* * *Non-E/E Requirements* | N/A |
| Functional Safety Requirement Title | Cloud and OTA Supervisor Communicates Manifest Securely | | |
| Functional Safety Requirement  *In case of User information including:*  *- Functional Safety Requirement Text*  *- Content of Information*  *- Method for Information*  *- Timing of Information*  *- Content of printed instructions (owner’s guide/service manuals etc.)* | The Cloud and OTA Feature shall ensure the OTA Manifest is securely transmitted to the vehicle | | |
| Rationale |  | | |
| Description of actions of the driver or other endangered persons  *if applicable in case of:*   * *Safety Related Functions* * *Reduced Functionality* * *User information*   *not applicable in case of:*   * *General Requirements* * *Maintain Safe State / Recovery* * *Non-E/E Requirements* |  | | |
| Validation Criteria for these actions  *if applicable in case of:*   * *Safety Related Functions* * *Reduced Functionality* * *User information*   *not applicable in case of:*   * *General Requirements* * *Maintain Safe State / Recovery* * *Non-E/E Requirements* |  | | |
| Fault Tolerant Time interval *if applicable)* |  | | |
| Reduced Functionality interval *(if applicable)* |  | | |
| Functional Redundancies (e.g. fault tolerance)  *(if applicable)* |  | | |
| Requirement Status |  | | |
| V&V method | Vehicle test | | |
| V&V acceptance criteria  *not applicable in case of:*   * *Non-E/E Requirements* | OTA Manifest is securely transmitted to the vehicle | | |
| V&V ID  *only applicable in case of:*   * *Non-E/E Requirements* |  | | |
| V&V Version  *only applicable in case of:*  *Non-E/E Requirements* |  | | |
| V&V Author  *only applicable in case of:*   * *Non-E/E Requirements* |  | | |
| V&V Status  *only applicable in case of:*   * *Non-E/E Requirements* |  | | |

Table 29: Requirement F-S-Req111 - Cloud and OTA Supervisor Communicates Manifest Securely

### Safety Goal SG03 – Ensure Safe Activation

**Name:** Ensure Safe Activation

**Purpose:**

**Text:**

Inhibit the vehicle before starting the activation

**ASIL:** D

#### Safety Concept

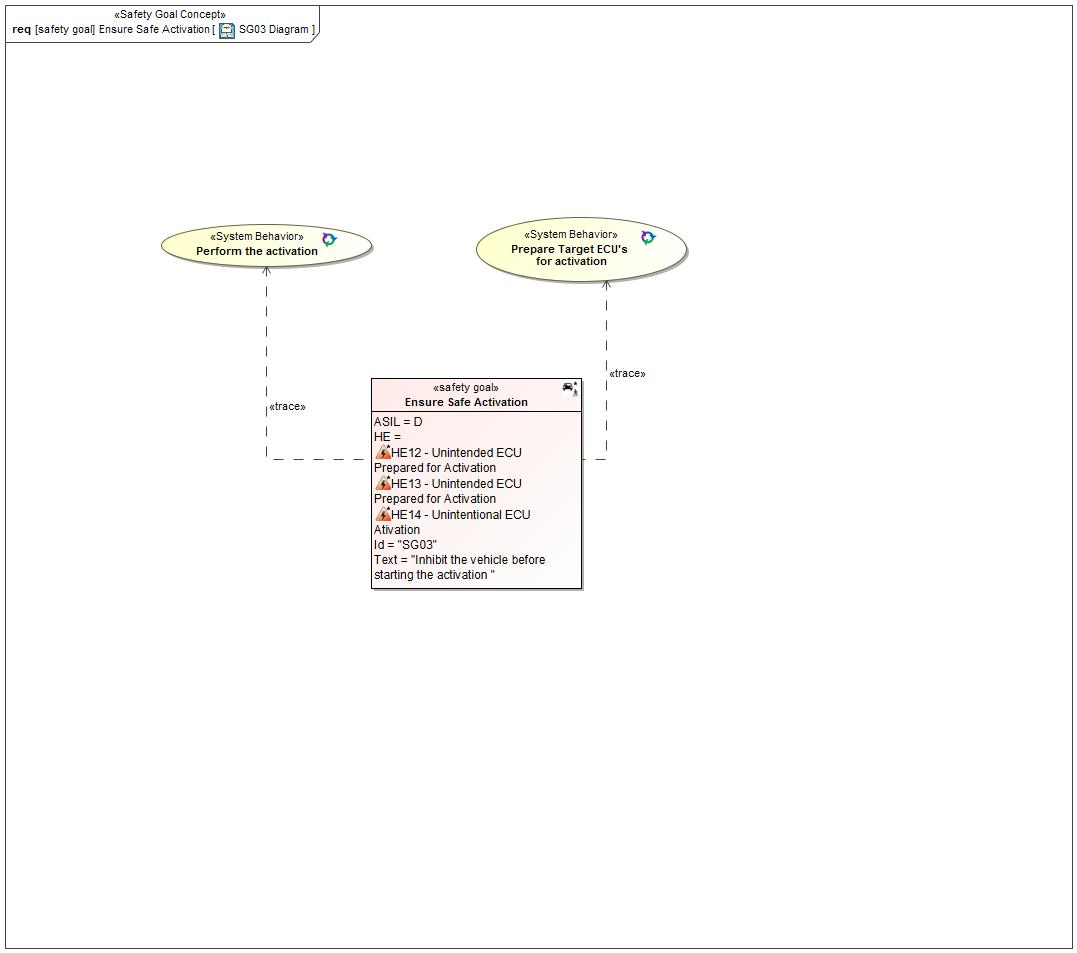


Figure 27: SG03 Diagram

#### Functional Safety Requirements

##### Requirement Derivation Diagram(s)(Optional)

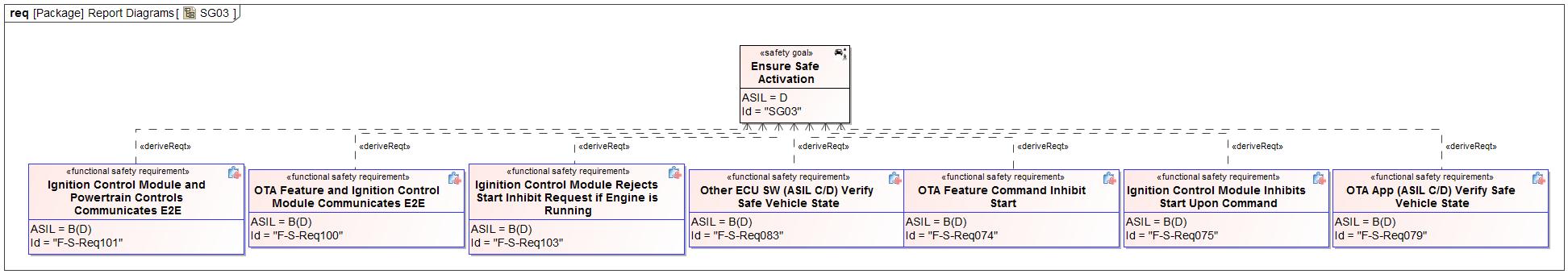


Figure 28 - Functional Safety Requirements Derivation Diagram for SG03

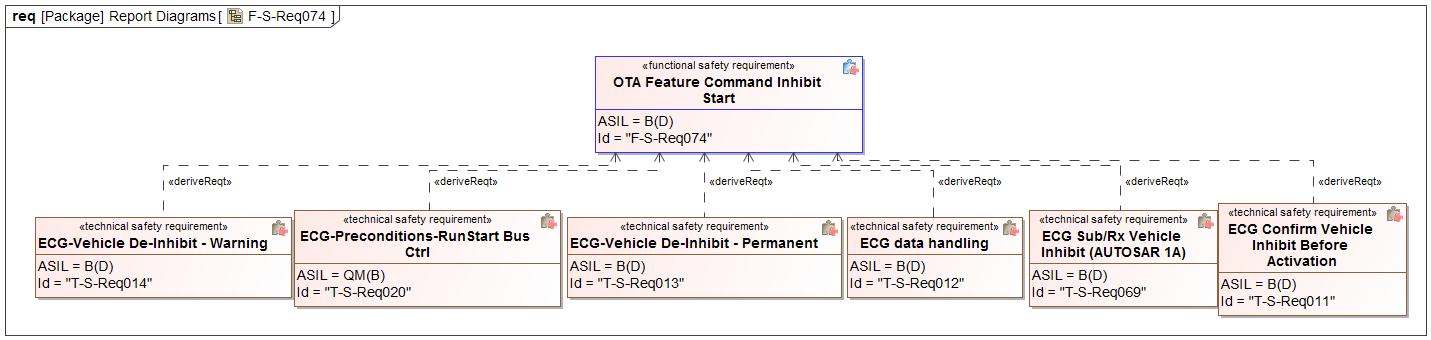


Figure 29 - Functional Safety Requirements Derivation Diagram for OTA Feature Command Inhibit Start

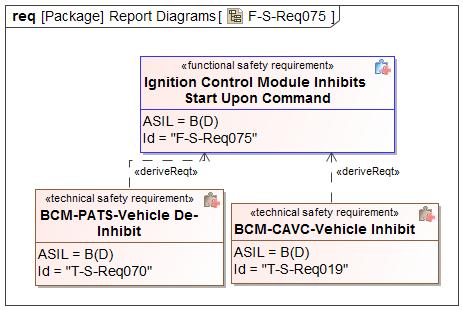


Figure 30 - Functional Safety Requirements Derivation Diagram for Ignition Control Module Inhibits Start Upon Command

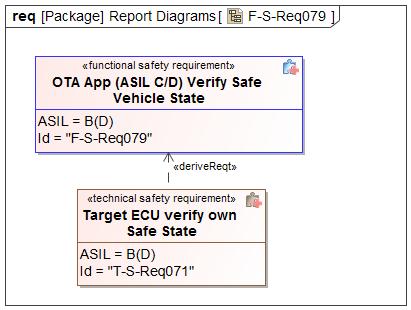


Figure 31 - Functional Safety Requirements Derivation Diagram for OTA App (ASIL C/D) Verify Safe Vehicle State

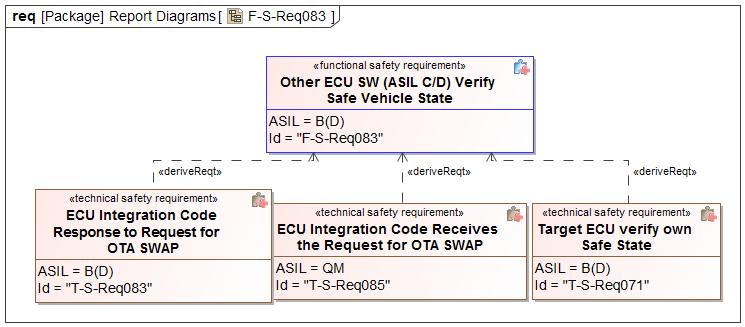


Figure 32 - Functional Safety Requirements Derivation Diagram for Other ECU SW (ASIL C/D) Verify Safe Vehicle State

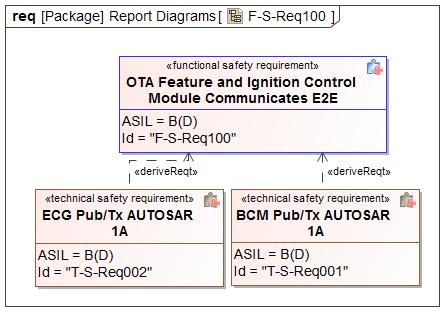


Figure 33 - Functional Safety Requirements Derivation Diagram for OTA Feature and Ignition Control Module Communicates E2E

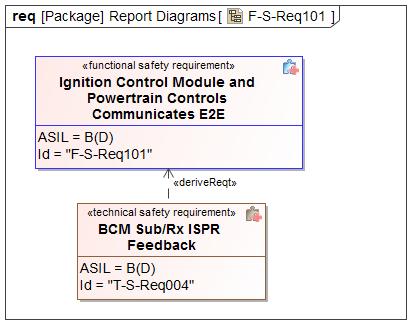


Figure 34 - Functional Safety Requirements Derivation Diagram for Ignition Control Module and Powertrain Controls Communicates E2E

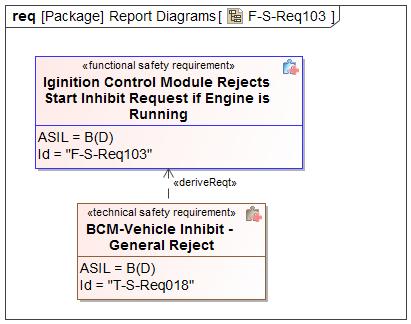


Figure 35 - Functional Safety Requirements Derivation Diagram for Iginition Control Module Rejects Start Inhibit Request if Engine is Running

##### Functional Safety Requirements for SG03 - Ensure Safe Activation

*Insert a table for each requirement according to its category.*

Please see the Functional Safety Requirement table for [Cloud Uses E2E](#_bfa5782f5133ad7e3479f6f556a349ef) displayed under the Safety Goal SG02.

|  |  |  |  |
| --- | --- | --- | --- |
| Safety Req-ID | **F-S-Req019 - Powertrain Controls Ensure Start Has Been Inhibited** | |  |
| Category | Safety Related Function | |  |
| Version  *only applicable in case of:*   * *Non-E/E Requirements* |  | |  |
| Author  *only applicable in case of:*  *Non-E/E Requirements* |  | |  |
| External Reference *(optional)* |  | | |
| Safety Goal Ref. | SG03 - Ensure Safe Activation | Operating Modes | Ignition On |
| ASIL Classification:  *if applicable in case of category*   * *General*   *not applicable in case of category*   * *Non-E/E Requirement* | **ASIL Override Rationale -** The Powertrain Controls help determine when the car is in a safe state to swap by inhibiting vehicle start, it has a lower ASIL rating because it is not solely responsible for determining when the ECU modules are safe to swap.  B(D) | Safe State  *if applicable for:*   * *General Requirements* * *User information* * *Non-E/E Requirements* | New software not activated |
| Functional Safety Requirement Title | Powertrain Controls Ensure Start Has Been Inhibited | | |
| Functional Safety Requirement  *In case of User information including:*  *- Functional Safety Requirement Text*  *- Content of Information*  *- Method for Information*  *- Timing of Information*  *- Content of printed instructions (owner’s guide/service manuals etc.)* | Upon request from the Ignition control module, the powertrain controls shall ensure the vehicle startup has been inhibited. | | |
| Rationale | Since every target ECU will not be able to detect the vehicle safe state, and there needs to be a more central way to ensure the vehicle is in a safe state to perform ACTIVATION. The start inihibit command would come from the OTA feature via the Ignition Control Module to the Powertrain Controls. | | |
| Description of actions of the driver or other endangered persons  *if applicable in case of:*   * *Safety Related Functions* * *Reduced Functionality* * *User information*   *not applicable in case of:*   * *General Requirements* * *Maintain Safe State / Recovery* * *Non-E/E Requirements* |  | | |
| Validation Criteria for these actions  *if applicable in case of:*   * *Safety Related Functions* * *Reduced Functionality* * *User information*   *not applicable in case of:*   * *General Requirements* * *Maintain Safe State / Recovery* * *Non-E/E Requirements* |  | | |
| Fault Tolerant Time interval *if applicable)* | 1 second | | |
| Reduced Functionality interval *(if applicable)* |  | | |
| Functional Redundancies (e.g. fault tolerance)  *(if applicable)* |  | | |
| Requirement Status |  | | |
| V&V method | Vehicle test | | |
| V&V acceptance criteria  *not applicable in case of:*   * *Non-E/E Requirements* | Check if powertrain controls ensure that torque cannot be applied to the vehicle when vehicle start is inhibited. | | |
| V&V ID  *only applicable in case of:*   * *Non-E/E Requirements* |  | | |
| V&V Version  *only applicable in case of:*  *Non-E/E Requirements* |  | | |
| V&V Author  *only applicable in case of:*   * *Non-E/E Requirements* |  | | |
| V&V Status  *only applicable in case of:*   * *Non-E/E Requirements* |  | | |

Table 30: Requirement F-S-Req019 - Powertrain Controls Ensure Start Has Been Inhibited

Please see the Functional Safety Requirement table for [OTA Governance Board shall review and approve the software that is to be pushed via OTA](#_5e9c9f6ae103b356824b6a2fea307a77) displayed under the Safety Goal SG02.

Please see the Functional Safety Requirement table for [Cloud Detects Data Corruption](#_c2b07e9d4169c67352344389f6bd163a) displayed under the Safety Goal SG02.

Please see the Functional Safety Requirement table for [Engineer Ensures Unique SW IDs](#_797e4f7cb4952f9289177ae847795e8f) displayed under the Safety Goal SG02.

Please see the Functional Safety Requirement table for [Engineer Uploads Correct Software](#_40547e13ba8870d835f2297ac78bbfe0) displayed under the Safety Goal SG02.

Please see the Functional Safety Requirement table for [Cloud Authenticates Software Update](#_4ca51e01184a59be985def8aa360adf7) displayed under the Safety Goal SG01.

Please see the Functional Safety Requirement table for [OTA Feature Detects Data Corruption](#_76f74d3d6f97e104e86d7f82f8a1ddf2) displayed under the Safety Goal SG01.

Please see the Functional Safety Requirement table for [OTA Feature Detects Invalid Software](#_126b516cfa2b0c927e018d1ef3a934c0) displayed under the Safety Goal SG02.

Please see the Functional Safety Requirement table for [Engineer Marks OTA and Non-OTA Software](#_70bc1df474703c72e5cd3a5a8243e41e) displayed under the Safety Goal SG02.

|  |  |  |  |
| --- | --- | --- | --- |
| Safety Req-ID | **F-S-Req042 - OTA Feature Evaluates Safe Time to Perform Activation** | |  |
| Category | Safety Related Function | |  |
| Version  *only applicable in case of:*   * *Non-E/E Requirements* |  | |  |
| Author  *only applicable in case of:*  *Non-E/E Requirements* |  | |  |
| External Reference *(optional)* |  | | |
| Safety Goal Ref. |  | Operating Modes | Ignition On |
| ASIL Classification:  *if applicable in case of category*   * *General*   *not applicable in case of category*   * *Non-E/E Requirement* | **ASIL Override Rationale -** Ensuring safe state to perform activation is independently shared between the OTA feature and the ASIL C/D modules.  B(D) | Safe State  *if applicable for:*   * *General Requirements* * *User information* * *Non-E/E Requirements* | New software not activated |
| Functional Safety Requirement Title | OTA Feature Evaluates Safe Time to Perform Activation | | |
| Functional Safety Requirement  *In case of User information including:*  *- Functional Safety Requirement Text*  *- Content of Information*  *- Method for Information*  *- Timing of Information*  *- Content of printed instructions (owner’s guide/service manuals etc.)* | The OTA Feature shall correctly determine when to send the "ACTIVATION" signal to the target ECU(s). | | |
| Rationale | To ensure that the OTA Feature sends the ACTIVATION signal at the right point of time Examples – - After the ignition is switched off and vehicle is stationary;  - Same ignition cycle (key on-off) after reception of the ACTIVATION authorization; - Never send an ACTIVATION signal without the authorization of the cloud; - Every target ECU will not be able to detect the vehicle state and hence this would need to be able to be done by the OTA Feature itself. | | |
| Description of actions of the driver or other endangered persons  *if applicable in case of:*   * *Safety Related Functions* * *Reduced Functionality* * *User information*   *not applicable in case of:*   * *General Requirements* * *Maintain Safe State / Recovery* * *Non-E/E Requirements* |  | | |
| Validation Criteria for these actions  *if applicable in case of:*   * *Safety Related Functions* * *Reduced Functionality* * *User information*   *not applicable in case of:*   * *General Requirements* * *Maintain Safe State / Recovery* * *Non-E/E Requirements* |  | | |
| Fault Tolerant Time interval *if applicable)* | 1 second | | |
| Reduced Functionality interval *(if applicable)* |  | | |
| Functional Redundancies (e.g. fault tolerance)  *(if applicable)* |  | | |
| Requirement Status |  | | |
| V&V method | Vehicle test | | |
| V&V acceptance criteria  *not applicable in case of:*   * *Non-E/E Requirements* | Verify the OTA Feature correctly determines when to send the "ACTIVATION" signal to the target ECU(s). | | |
| V&V ID  *only applicable in case of:*   * *Non-E/E Requirements* |  | | |
| V&V Version  *only applicable in case of:*  *Non-E/E Requirements* |  | | |
| V&V Author  *only applicable in case of:*   * *Non-E/E Requirements* |  | | |
| V&V Status  *only applicable in case of:*   * *Non-E/E Requirements* |  | | |

Table 31: Requirement F-S-Req042 - OTA Feature Evaluates Safe Time to Perform Activation

Please see the Functional Safety Requirement table for [OTA Feature Authenticates Cloud Connection](#_efd36d91e07c56151380e9b74df9ad0a) displayed under the Safety Goal SG01.

Please see the Functional Safety Requirement table for [OTA Feature Communicates E2E with the Cloud](#_a458b919ab42ff23acd4fea432087958) displayed under the Safety Goal SG01.

Please see the Functional Safety Requirement table for [Cloud Sends Correct Software for the Target ECU](#_f7354c219e6ca75d905bf27442e7fbdb) displayed under the Safety Goal SG02.

Please see the Functional Safety Requirement table for [OTA Feature Informs the Cloud of Data Corruption](#_d1f561bf9e8a4063ad777e30bc18134f) displayed under the Safety Goal SG01.

Please see the Functional Safety Requirement table for [Cloud and Engineers Ensure Correct Software is Flashed](#_1a52ed0580e4fe18b0253a01c3f1947f) displayed under the Safety Goal SG02.

Please see the Functional Safety Requirement table for [OTA App Detects Data Corruption During Software Download](#_0344dfc0fe65adce2f0ab2d4179cd7f1) displayed under the Safety Goal SG01.

Please see the Functional Safety Requirement table for [OTA Feature Detects Data Corruption During Software Download](#_469e6e08115ee3fecea46961210e32dd) displayed under the Safety Goal SG01.

|  |  |  |  |
| --- | --- | --- | --- |
| Safety Req-ID | **F-S-Req074 - OTA Feature Command Inhibit Start** | |  |
| Category | Safety Related Function | |  |
| Version  *only applicable in case of:*   * *Non-E/E Requirements* |  | |  |
| Author  *only applicable in case of:*  *Non-E/E Requirements* |  | |  |
| External Reference *(optional)* |  | | |
| Safety Goal Ref. | SG03 - Ensure Safe Activation | Operating Modes | Ignition On |
| ASIL Classification:  *if applicable in case of category*   * *General*   *not applicable in case of category*   * *Non-E/E Requirement* | **ASIL Override Rationale -** Ensuring safe state to perform activation is independently shared between the OTA feature and the ASIL C/D modules.  B(D) | Safe State  *if applicable for:*   * *General Requirements* * *User information* * *Non-E/E Requirements* | New software not activated |
| Functional Safety Requirement Title | OTA Feature Command Inhibit Start | | |
| Functional Safety Requirement  *In case of User information including:*  *- Functional Safety Requirement Text*  *- Content of Information*  *- Method for Information*  *- Timing of Information*  *- Content of printed instructions (owner’s guide/service manuals etc.)* | The OTA feature shall command the ignition control module to “inhibit start” before issuing the ACTIVATION command to the target ECU’s and shall remove the inhibit after a successful ACTIVATION or rollback has been confirmed. | | |
| Rationale | To ensure the vehicle is in a safe state to perform the ACTIVATION. | | |
| Description of actions of the driver or other endangered persons  *if applicable in case of:*   * *Safety Related Functions* * *Reduced Functionality* * *User information*   *not applicable in case of:*   * *General Requirements* * *Maintain Safe State / Recovery* * *Non-E/E Requirements* |  | | |
| Validation Criteria for these actions  *if applicable in case of:*   * *Safety Related Functions* * *Reduced Functionality* * *User information*   *not applicable in case of:*   * *General Requirements* * *Maintain Safe State / Recovery* * *Non-E/E Requirements* |  | | |
| Fault Tolerant Time interval *if applicable)* | ACTIVATION\_TIMEOUT | | |
| Reduced Functionality interval *(if applicable)* |  | | |
| Functional Redundancies (e.g. fault tolerance)  *(if applicable)* |  | | |
| Requirement Status |  | | |
| V&V method | Vehicle test | | |
| V&V acceptance criteria  *not applicable in case of:*   * *Non-E/E Requirements* | The OTA featurel commands the ignition control module to “inhibit start” before issuing the ACTIVATION command to the target ECU’s and removes the inhibit after a successful ACTIVATION or rollback has been confirmed. | | |
| V&V ID  *only applicable in case of:*   * *Non-E/E Requirements* |  | | |
| V&V Version  *only applicable in case of:*  *Non-E/E Requirements* |  | | |
| V&V Author  *only applicable in case of:*   * *Non-E/E Requirements* |  | | |
| V&V Status  *only applicable in case of:*   * *Non-E/E Requirements* |  | | |

Table 32: Requirement F-S-Req074 - OTA Feature Command Inhibit Start

|  |  |  |  |
| --- | --- | --- | --- |
| Safety Req-ID | **F-S-Req075 - Ignition Control Module Inhibits Start Upon Command** | |  |
| Category | Safety Related Function | |  |
| Version  *only applicable in case of:*   * *Non-E/E Requirements* |  | |  |
| Author  *only applicable in case of:*  *Non-E/E Requirements* |  | |  |
| External Reference *(optional)* |  | | |
| Safety Goal Ref. | SG03 - Ensure Safe Activation | Operating Modes | Ignition On |
| ASIL Classification:  *if applicable in case of category*   * *General*   *not applicable in case of category*   * *Non-E/E Requirement* | **ASIL Override Rationale -** The ignition control module helps to report when the car is in a safe state to swap but it is not solely responsible for determining when to swap. Ensuring safe state to perform activation is independently shared between the OTA feature and the ASIL C/D modules.  B(D) | Safe State  *if applicable for:*   * *General Requirements* * *User information* * *Non-E/E Requirements* | New software not activated |
| Functional Safety Requirement Title | Ignition Control Module Inhibits Start Upon Command | | |
| Functional Safety Requirement  *In case of User information including:*  *- Functional Safety Requirement Text*  *- Content of Information*  *- Method for Information*  *- Timing of Information*  *- Content of printed instructions (owner’s guide/service manuals etc.)* | The "Ignition control module" shall “inhibit start” when commanded by the OTA manager and continue to do so until the OTA manager commands it to remove the inhibit. | | |
| Rationale | To ensure the vehicle is in a safe state to perform the ACTIVATION. | | |
| Description of actions of the driver or other endangered persons  *if applicable in case of:*   * *Safety Related Functions* * *Reduced Functionality* * *User information*   *not applicable in case of:*   * *General Requirements* * *Maintain Safe State / Recovery* * *Non-E/E Requirements* |  | | |
| Validation Criteria for these actions  *if applicable in case of:*   * *Safety Related Functions* * *Reduced Functionality* * *User information*   *not applicable in case of:*   * *General Requirements* * *Maintain Safe State / Recovery* * *Non-E/E Requirements* |  | | |
| Fault Tolerant Time interval *if applicable)* | 1 second | | |
| Reduced Functionality interval *(if applicable)* |  | | |
| Functional Redundancies (e.g. fault tolerance)  *(if applicable)* |  | | |
| Requirement Status |  | | |
| V&V method | Vehicle test | | |
| V&V acceptance criteria  *not applicable in case of:*   * *Non-E/E Requirements* | The "Ignition control module" inhibits start when commanded by the OTA manager and continue to do so until the OTA manager commands it to remove the inhibit. | | |
| V&V ID  *only applicable in case of:*   * *Non-E/E Requirements* |  | | |
| V&V Version  *only applicable in case of:*  *Non-E/E Requirements* |  | | |
| V&V Author  *only applicable in case of:*   * *Non-E/E Requirements* |  | | |
| V&V Status  *only applicable in case of:*   * *Non-E/E Requirements* |  | | |

Table 33: Requirement F-S-Req075 - Ignition Control Module Inhibits Start Upon Command

|  |  |  |  |
| --- | --- | --- | --- |
| Safety Req-ID | **F-S-Req079 - OTA App (ASIL C/D) Verify Safe Vehicle State** | |  |
| Category | Safety Related Function | |  |
| Version  *only applicable in case of:*   * *Non-E/E Requirements* |  | |  |
| Author  *only applicable in case of:*  *Non-E/E Requirements* |  | |  |
| External Reference *(optional)* |  | | |
| Safety Goal Ref. | SG03 - Ensure Safe Activation | Operating Modes | Ignition On |
| ASIL Classification:  *if applicable in case of category*   * *General*   *not applicable in case of category*   * *Non-E/E Requirement* | **ASIL Override Rationale -** Ensuring safe state to perform activation is independently shared between the OTA feature and the ASIL C/D modules.  B(D) | Safe State  *if applicable for:*   * *General Requirements* * *User information* * *Non-E/E Requirements* | New software not activated |
| Functional Safety Requirement Title | OTA App (ASIL C/D) Verify Safe Vehicle State | | |
| Functional Safety Requirement  *In case of User information including:*  *- Functional Safety Requirement Text*  *- Content of Information*  *- Method for Information*  *- Timing of Information*  *- Content of printed instructions (owner’s guide/service manuals etc.)* | The OTA app in each ASIL C or ASIL D module shall receive confirmation from the "Other ECU SW" that the module is in a safe state to activate the new software. | | |
| Rationale | To prevent switchover at an unsafe time. | | |
| Description of actions of the driver or other endangered persons  *if applicable in case of:*   * *Safety Related Functions* * *Reduced Functionality* * *User information*   *not applicable in case of:*   * *General Requirements* * *Maintain Safe State / Recovery* * *Non-E/E Requirements* |  | | |
| Validation Criteria for these actions  *if applicable in case of:*   * *Safety Related Functions* * *Reduced Functionality* * *User information*   *not applicable in case of:*   * *General Requirements* * *Maintain Safe State / Recovery* * *Non-E/E Requirements* |  | | |
| Fault Tolerant Time interval *if applicable)* | 1 second | | |
| Reduced Functionality interval *(if applicable)* |  | | |
| Functional Redundancies (e.g. fault tolerance)  *(if applicable)* |  | | |
| Requirement Status |  | | |
| V&V method | Vehicle test | | |
| V&V acceptance criteria  *not applicable in case of:*   * *Non-E/E Requirements* | The OTA app in each ASIL C or ASIL D module confirms the module is in a safe state to activate the new software from the "Other ECU SW". | | |
| V&V ID  *only applicable in case of:*   * *Non-E/E Requirements* |  | | |
| V&V Version  *only applicable in case of:*  *Non-E/E Requirements* |  | | |
| V&V Author  *only applicable in case of:*   * *Non-E/E Requirements* |  | | |
| V&V Status  *only applicable in case of:*   * *Non-E/E Requirements* |  | | |

Table 34: Requirement F-S-Req079 - OTA App (ASIL C/D) Verify Safe Vehicle State

Please see the Functional Safety Requirement table for [Other ECU SW Provides Part Number](#_b17a109130a284464de3daf7f51ef258) displayed under the Safety Goal SG02.

Please see the Functional Safety Requirement table for [OTA App Prevents Active Memory Erasing or Writing](#_0ad92bdb6a99e3d10ce1dc0d0a77e60a) displayed under the Safety Goal SG01.

|  |  |  |  |
| --- | --- | --- | --- |
| Safety Req-ID | **F-S-Req083 - Other ECU SW (ASIL C/D) Verify Safe Vehicle State** | |  |
| Category | Safety Related Function | |  |
| Version  *only applicable in case of:*   * *Non-E/E Requirements* |  | |  |
| Author  *only applicable in case of:*  *Non-E/E Requirements* |  | |  |
| External Reference *(optional)* |  | | |
| Safety Goal Ref. | SG03 - Ensure Safe Activation | Operating Modes | Ignition On |
| ASIL Classification:  *if applicable in case of category*   * *General*   *not applicable in case of category*   * *Non-E/E Requirement* | **ASIL Override Rationale -** Ensuring safe state to perform activation is independently shared between the OTA feature and the ASIL C/D modules.  B(D) | Safe State  *if applicable for:*   * *General Requirements* * *User information* * *Non-E/E Requirements* | New software not activated |
| Functional Safety Requirement Title | Other ECU SW (ASIL C/D) Verify Safe Vehicle State | | |
| Functional Safety Requirement  *In case of User information including:*  *- Functional Safety Requirement Text*  *- Content of Information*  *- Method for Information*  *- Timing of Information*  *- Content of printed instructions (owner’s guide/service manuals etc.)* | In each ASIL C or ASIL D module, upon request by the OTA App, the other ECU SW shall independently verify they are in a safe state to activate the new software. | | |
| Rationale | To prevent switchover at an unsafe time. For ASIL QM to ASIL B, the start inhibit is enough to verify the vehicle safe state. The higher ASIL rated modules would have to perform independent safe state verification. | | |
| Description of actions of the driver or other endangered persons  *if applicable in case of:*   * *Safety Related Functions* * *Reduced Functionality* * *User information*   *not applicable in case of:*   * *General Requirements* * *Maintain Safe State / Recovery* * *Non-E/E Requirements* |  | | |
| Validation Criteria for these actions  *if applicable in case of:*   * *Safety Related Functions* * *Reduced Functionality* * *User information*   *not applicable in case of:*   * *General Requirements* * *Maintain Safe State / Recovery* * *Non-E/E Requirements* |  | | |
| Fault Tolerant Time interval *if applicable)* | 1 second | | |
| Reduced Functionality interval *(if applicable)* |  | | |
| Functional Redundancies (e.g. fault tolerance)  *(if applicable)* |  | | |
| Requirement Status |  | | |
| V&V method | Vehicle test | | |
| V&V acceptance criteria  *not applicable in case of:*   * *Non-E/E Requirements* | Each ASIL C or ASIL D module verifies they are in a safe vehicle state to activate the new software | | |
| V&V ID  *only applicable in case of:*   * *Non-E/E Requirements* |  | | |
| V&V Version  *only applicable in case of:*  *Non-E/E Requirements* |  | | |
| V&V Author  *only applicable in case of:*   * *Non-E/E Requirements* |  | | |
| V&V Status  *only applicable in case of:*   * *Non-E/E Requirements* |  | | |

Table 35: Requirement F-S-Req083 - Other ECU SW (ASIL C/D) Verify Safe Vehicle State

Please see the Functional Safety Requirement table for [OTA App Informs the OTA Feature of Data Corruption](#_360bdf0d5ab05912ccfeafc1f7b16cad) displayed under the Safety Goal SG01.

Please see the Functional Safety Requirement table for [OTA App Authenticates Erase And Programming Commands](#_e63467aecb84419c92184c8c6805edc0) displayed under the Safety Goal SG01.

Please see the Functional Safety Requirement table for [OTA App Executes OTA Without Affecting Basic Function](#_27bc942123bd1574d78bbd287b70358c) displayed under the Safety Goal SG01.

Please see the Functional Safety Requirement table for [Other ECU SW Prevents Active Memory Erasing or Writing](#_2fad9e75d48a85a9587e37c286f61f5d) displayed under the Safety Goal SG01.

Please see the Functional Safety Requirement table for [Other ECU SW Executes OTA Without Affecting Basic Function](#_25f65ce1928c94d70c987c03951c4b4e) displayed under the Safety Goal SG01.

Please see the Functional Safety Requirement table for [OTA App rejects Invalid Software](#_9ef6d483a829a79f7882c26ec92e1d8f) displayed under the Safety Goal SG02.

Please see the Functional Safety Requirement table for [OTA App Sends Correct Part Number](#_22c4e180014b476d89e62ab131101f2f) displayed under the Safety Goal SG02.

Please see the Functional Safety Requirement table for [Other ECU SW Executes Active Memory](#_b8e39606250fba93cad1eea6e2003901) displayed under the Safety Goal SG01.

Please see the Functional Safety Requirement table for [OTA App Detects Communication Errors](#_9532234d56f31920200b2f5b2b4c28c4) displayed under the Safety Goal SG01.

|  |  |  |  |
| --- | --- | --- | --- |
| Safety Req-ID | **F-S-Req096 - OTA Feature, OTA App, and Other ECU SW (ASIL C/D) Ensures Safe Time To Perform Activation** | |  |
| Category | Safety Related Function | |  |
| Version  *only applicable in case of:*   * *Non-E/E Requirements* |  | |  |
| Author  *only applicable in case of:*  *Non-E/E Requirements* |  | |  |
| External Reference *(optional)* |  | | |
| Safety Goal Ref. |  | Operating Modes | Ignition On |
| ASIL Classification:  *if applicable in case of category*   * *General*   *not applicable in case of category*   * *Non-E/E Requirement* | D | Safe State  *if applicable for:*   * *General Requirements* * *User information* * *Non-E/E Requirements* | Target ECU not running |
| Functional Safety Requirement Title | OTA Feature, OTA App, and Other ECU SW (ASIL C/D) Ensures Safe Time To Perform Activation | | |
| Functional Safety Requirement  *In case of User information including:*  *- Functional Safety Requirement Text*  *- Content of Information*  *- Method for Information*  *- Timing of Information*  *- Content of printed instructions (owner’s guide/service manuals etc.)* | The OTA Feature, OTA App, and Other ECU SW (in ASIL C/D ECU) shall ensure a safe time to perform activation. | | |
| Rationale | To prevent a malfunction of the MMOTA feature from causing the highest level hazard in the target ECU. | | |
| Description of actions of the driver or other endangered persons  *if applicable in case of:*   * *Safety Related Functions* * *Reduced Functionality* * *User information*   *not applicable in case of:*   * *General Requirements* * *Maintain Safe State / Recovery* * *Non-E/E Requirements* |  | | |
| Validation Criteria for these actions  *if applicable in case of:*   * *Safety Related Functions* * *Reduced Functionality* * *User information*   *not applicable in case of:*   * *General Requirements* * *Maintain Safe State / Recovery* * *Non-E/E Requirements* |  | | |
| Fault Tolerant Time interval *if applicable)* | 1 second | | |
| Reduced Functionality interval *(if applicable)* |  | | |
| Functional Redundancies (e.g. fault tolerance)  *(if applicable)* |  | | |
| Requirement Status |  | | |
| V&V method | Vehicle test | | |
| V&V acceptance criteria  *not applicable in case of:*   * *Non-E/E Requirements* | The OTA Feature, OTA App, and Other ECU SW (ASIL C/D) ensures a safe time to perform activation. | | |
| V&V ID  *only applicable in case of:*   * *Non-E/E Requirements* |  | | |
| V&V Version  *only applicable in case of:*  *Non-E/E Requirements* |  | | |
| V&V Author  *only applicable in case of:*   * *Non-E/E Requirements* |  | | |
| V&V Status  *only applicable in case of:*   * *Non-E/E Requirements* |  | | |

Table 36: Requirement F-S-Req096 - OTA Feature, OTA App, and Other ECU SW (ASIL C/D) Ensures Safe Time To Perform Activation

|  |  |  |  |
| --- | --- | --- | --- |
| Safety Req-ID | **F-S-Req097 - OTA App and Other ECU SW (ASIL C/D) Ensures Safe Time To Perform Activation** | |  |
| Category | Safety Related Function | |  |
| Version  *only applicable in case of:*   * *Non-E/E Requirements* |  | |  |
| Author  *only applicable in case of:*  *Non-E/E Requirements* |  | |  |
| External Reference *(optional)* |  | | |
| Safety Goal Ref. |  | Operating Modes | Ignition On |
| ASIL Classification:  *if applicable in case of category*   * *General*   *not applicable in case of category*   * *Non-E/E Requirement* | **ASIL Override Rationale -** Ensuring safe state to perform activation is independently shared between the OTA feature and the ASIL C/D modules.  B(D) | Safe State  *if applicable for:*   * *General Requirements* * *User information* * *Non-E/E Requirements* | Target ECU not running |
| Functional Safety Requirement Title | OTA App and Other ECU SW (ASIL C/D) Ensures Safe Time To Perform Activation | | |
| Functional Safety Requirement  *In case of User information including:*  *- Functional Safety Requirement Text*  *- Content of Information*  *- Method for Information*  *- Timing of Information*  *- Content of printed instructions (owner’s guide/service manuals etc.)* | In each ASIL C or ASIL D module, the OTA App and Other ECU SW shall ensure the vehicle is secured to perform OTA activation. | | |
| Rationale | To prevent a malfunction of the MMOTA feature from causing the highest level hazard in the target ECU. | | |
| Description of actions of the driver or other endangered persons  *if applicable in case of:*   * *Safety Related Functions* * *Reduced Functionality* * *User information*   *not applicable in case of:*   * *General Requirements* * *Maintain Safe State / Recovery* * *Non-E/E Requirements* |  | | |
| Validation Criteria for these actions  *if applicable in case of:*   * *Safety Related Functions* * *Reduced Functionality* * *User information*   *not applicable in case of:*   * *General Requirements* * *Maintain Safe State / Recovery* * *Non-E/E Requirements* |  | | |
| Fault Tolerant Time interval *if applicable)* | 1 second | | |
| Reduced Functionality interval *(if applicable)* |  | | |
| Functional Redundancies (e.g. fault tolerance)  *(if applicable)* |  | | |
| Requirement Status |  | | |
| V&V method | Vehicle test | | |
| V&V acceptance criteria  *not applicable in case of:*   * *Non-E/E Requirements* | The OTA App and Other ECU SW ensure a safe time to perform activation. | | |
| V&V ID  *only applicable in case of:*   * *Non-E/E Requirements* |  | | |
| V&V Version  *only applicable in case of:*  *Non-E/E Requirements* |  | | |
| V&V Author  *only applicable in case of:*   * *Non-E/E Requirements* |  | | |
| V&V Status  *only applicable in case of:*   * *Non-E/E Requirements* |  | | |

Table 37: Requirement F-S-Req097 - OTA App and Other ECU SW (ASIL C/D) Ensures Safe Time To Perform Activation

|  |  |  |  |
| --- | --- | --- | --- |
| Safety Req-ID | **F-S-Req098 - Independence in Ensuring Safe Time To Perform Activation** | |  |
| Category | Safety Related Function | |  |
| Version  *only applicable in case of:*   * *Non-E/E Requirements* |  | |  |
| Author  *only applicable in case of:*  *Non-E/E Requirements* |  | |  |
| External Reference *(optional)* |  | | |
| Safety Goal Ref. |  | Operating Modes | Ignition On |
| ASIL Classification:  *if applicable in case of category*   * *General*   *not applicable in case of category*   * *Non-E/E Requirement* | D | Safe State  *if applicable for:*   * *General Requirements* * *User information* * *Non-E/E Requirements* | Target ECU not running |
| Functional Safety Requirement Title | Independence in Ensuring Safe Time To Perform Activation | | |
| Functional Safety Requirement  *In case of User information including:*  *- Functional Safety Requirement Text*  *- Content of Information*  *- Method for Information*  *- Timing of Information*  *- Content of printed instructions (owner’s guide/service manuals etc.)* | The OTA Feature and the Target ECU shall be sufficiently independent in ensuring the vehicle is secured to perform OTA Activation | | |
| Rationale | To prevent a malfunction of the MMOTA feature from causing the highest level hazard in the target ECU. | | |
| Description of actions of the driver or other endangered persons  *if applicable in case of:*   * *Safety Related Functions* * *Reduced Functionality* * *User information*   *not applicable in case of:*   * *General Requirements* * *Maintain Safe State / Recovery* * *Non-E/E Requirements* |  | | |
| Validation Criteria for these actions  *if applicable in case of:*   * *Safety Related Functions* * *Reduced Functionality* * *User information*   *not applicable in case of:*   * *General Requirements* * *Maintain Safe State / Recovery* * *Non-E/E Requirements* |  | | |
| Fault Tolerant Time interval *if applicable)* | 1 second | | |
| Reduced Functionality interval *(if applicable)* |  | | |
| Functional Redundancies (e.g. fault tolerance)  *(if applicable)* |  | | |
| Requirement Status |  | | |
| V&V method | Vehicle test | | |
| V&V acceptance criteria  *not applicable in case of:*   * *Non-E/E Requirements* | The OTA Feature and the Target ECU are sufficiently independent in ensuring the vehicle is secured to perform OTA Activation. | | |
| V&V ID  *only applicable in case of:*   * *Non-E/E Requirements* |  | | |
| V&V Version  *only applicable in case of:*  *Non-E/E Requirements* |  | | |
| V&V Author  *only applicable in case of:*   * *Non-E/E Requirements* |  | | |
| V&V Status  *only applicable in case of:*   * *Non-E/E Requirements* |  | | |

Table 38: Requirement F-S-Req098 - Independence in Ensuring Safe Time To Perform Activation

|  |  |  |  |
| --- | --- | --- | --- |
| Safety Req-ID | **F-S-Req100 - OTA Feature and Ignition Control Module Communicates E2E** | |  |
| Category | Safety Related Function | |  |
| Version  *only applicable in case of:*   * *Non-E/E Requirements* |  | |  |
| Author  *only applicable in case of:*  *Non-E/E Requirements* |  | |  |
| External Reference *(optional)* |  | | |
| Safety Goal Ref. | SG03 - Ensure Safe Activation | Operating Modes | Ignition On |
| ASIL Classification:  *if applicable in case of category*   * *General*   *not applicable in case of category*   * *Non-E/E Requirement* | **ASIL Override Rationale -** Ensuring safe state to perform activation is independently shared between the OTA feature and the ASIL C/D modules.  B(D) | Safe State  *if applicable for:*   * *General Requirements* * *User information* * *Non-E/E Requirements* | Software Rejected |
| Functional Safety Requirement Title | OTA Feature and Ignition Control Module Communicates E2E | | |
| Functional Safety Requirement  *In case of User information including:*  *- Functional Safety Requirement Text*  *- Content of Information*  *- Method for Information*  *- Timing of Information*  *- Content of printed instructions (owner’s guide/service manuals etc.)* | For OTA safety critical messages, the OTA Feature and Ignition Control Module shall communicate with each other over an end-to-end protected communication path. | | |
| Rationale | To detect data error during communication via the CAN bus. | | |
| Description of actions of the driver or other endangered persons  *if applicable in case of:*   * *Safety Related Functions* * *Reduced Functionality* * *User information*   *not applicable in case of:*   * *General Requirements* * *Maintain Safe State / Recovery* * *Non-E/E Requirements* |  | | |
| Validation Criteria for these actions  *if applicable in case of:*   * *Safety Related Functions* * *Reduced Functionality* * *User information*   *not applicable in case of:*   * *General Requirements* * *Maintain Safe State / Recovery* * *Non-E/E Requirements* |  | | |
| Fault Tolerant Time interval *if applicable)* | 1 second | | |
| Reduced Functionality interval *(if applicable)* |  | | |
| Functional Redundancies (e.g. fault tolerance)  *(if applicable)* |  | | |
| Requirement Status |  | | |
| V&V method | Vehicle test | | |
| V&V acceptance criteria  *not applicable in case of:*   * *Non-E/E Requirements* | The Ignition Control Module should communicate end-to-end with the OTA Feature. | | |
| V&V ID  *only applicable in case of:*   * *Non-E/E Requirements* |  | | |
| V&V Version  *only applicable in case of:*  *Non-E/E Requirements* |  | | |
| V&V Author  *only applicable in case of:*   * *Non-E/E Requirements* |  | | |
| V&V Status  *only applicable in case of:*   * *Non-E/E Requirements* |  | | |

Table 39: Requirement F-S-Req100 - OTA Feature and Ignition Control Module Communicates E2E

|  |  |  |  |
| --- | --- | --- | --- |
| Safety Req-ID | **F-S-Req101 - Ignition Control Module and Powertrain Controls Communicates E2E** | |  |
| Category | Safety Related Function | |  |
| Version  *only applicable in case of:*   * *Non-E/E Requirements* |  | |  |
| Author  *only applicable in case of:*  *Non-E/E Requirements* |  | |  |
| External Reference *(optional)* |  | | |
| Safety Goal Ref. | SG03 - Ensure Safe Activation | Operating Modes | Ignition On |
| ASIL Classification:  *if applicable in case of category*   * *General*   *not applicable in case of category*   * *Non-E/E Requirement* | **ASIL Override Rationale -** Ensuring safe state to perform activation is independently shared between the OTA feature and the ASIL C/D modules.  B(D) | Safe State  *if applicable for:*   * *General Requirements* * *User information* * *Non-E/E Requirements* | New software not activated |
| Functional Safety Requirement Title | Ignition Control Module and Powertrain Controls Communicates E2E | | |
| Functional Safety Requirement  *In case of User information including:*  *- Functional Safety Requirement Text*  *- Content of Information*  *- Method for Information*  *- Timing of Information*  *- Content of printed instructions (owner’s guide/service manuals etc.)* | For OTA safety critical messages, the Ignition Control Module and Powertrain Controls shall communicate with each other over an end-to-end protected communication path. | | |
| Rationale | To detect data error during communication via the CAN bus. | | |
| Description of actions of the driver or other endangered persons  *if applicable in case of:*   * *Safety Related Functions* * *Reduced Functionality* * *User information*   *not applicable in case of:*   * *General Requirements* * *Maintain Safe State / Recovery* * *Non-E/E Requirements* |  | | |
| Validation Criteria for these actions  *if applicable in case of:*   * *Safety Related Functions* * *Reduced Functionality* * *User information*   *not applicable in case of:*   * *General Requirements* * *Maintain Safe State / Recovery* * *Non-E/E Requirements* |  | | |
| Fault Tolerant Time interval *if applicable)* | 1 second | | |
| Reduced Functionality interval *(if applicable)* |  | | |
| Functional Redundancies (e.g. fault tolerance)  *(if applicable)* |  | | |
| Requirement Status |  | | |
| V&V method | Vehicle test | | |
| V&V acceptance criteria  *not applicable in case of:*   * *Non-E/E Requirements* | The Ignition Control Module should communicate end-to-end with the Powertrain Controls. | | |
| V&V ID  *only applicable in case of:*   * *Non-E/E Requirements* |  | | |
| V&V Version  *only applicable in case of:*  *Non-E/E Requirements* |  | | |
| V&V Author  *only applicable in case of:*   * *Non-E/E Requirements* |  | | |
| V&V Status  *only applicable in case of:*   * *Non-E/E Requirements* |  | | |

Table 40: Requirement F-S-Req101 - Ignition Control Module and Powertrain Controls Communicates E2E

|  |  |  |  |
| --- | --- | --- | --- |
| Safety Req-ID | **F-S-Req103 - Iginition Control Module Rejects Start Inhibit Request if Engine is Running** | |  |
| Category | Safety Related Function | |  |
| Version  *only applicable in case of:*   * *Non-E/E Requirements* |  | |  |
| Author  *only applicable in case of:*  *Non-E/E Requirements* |  | |  |
| External Reference *(optional)* |  | | |
| Safety Goal Ref. | SG03 - Ensure Safe Activation | Operating Modes | Ignition On |
| ASIL Classification:  *if applicable in case of category*   * *General*   *not applicable in case of category*   * *Non-E/E Requirement* | **ASIL Override Rationale -** Ensuring safe state to perform activation is independently shared between the OTA feature and the ASIL C/D modules.  B(D) | Safe State  *if applicable for:*   * *General Requirements* * *User information* * *Non-E/E Requirements* | New software not activated |
| Functional Safety Requirement Title | Iginition Control Module Rejects Start Inhibit Request if Engine is Running | | |
| Functional Safety Requirement  *In case of User information including:*  *- Functional Safety Requirement Text*  *- Content of Information*  *- Method for Information*  *- Timing of Information*  *- Content of printed instructions (owner’s guide/service manuals etc.)* | The Ignition Control Module shall reject a start inhibit request from the OTA feature if powertrain controls indicates the engine is running. | | |
| Rationale | To avoid unintended shutdown of the engine the Ignition Control Module checks the engine run status prior to commanding start inhibit for OTA. | | |
| Description of actions of the driver or other endangered persons  *if applicable in case of:*   * *Safety Related Functions* * *Reduced Functionality* * *User information*   *not applicable in case of:*   * *General Requirements* * *Maintain Safe State / Recovery* * *Non-E/E Requirements* |  | | |
| Validation Criteria for these actions  *if applicable in case of:*   * *Safety Related Functions* * *Reduced Functionality* * *User information*   *not applicable in case of:*   * *General Requirements* * *Maintain Safe State / Recovery* * *Non-E/E Requirements* |  | | |
| Fault Tolerant Time interval *if applicable)* | 1 second | | |
| Reduced Functionality interval *(if applicable)* |  | | |
| Functional Redundancies (e.g. fault tolerance)  *(if applicable)* |  | | |
| Requirement Status |  | | |
| V&V method | Vehicle test | | |
| V&V acceptance criteria  *not applicable in case of:*   * *Non-E/E Requirements* | Ignition Control Module Rejects Start Inhibit Request if Engine is Running. | | |
| V&V ID  *only applicable in case of:*   * *Non-E/E Requirements* |  | | |
| V&V Version  *only applicable in case of:*  *Non-E/E Requirements* |  | | |
| V&V Author  *only applicable in case of:*   * *Non-E/E Requirements* |  | | |
| V&V Status  *only applicable in case of:*   * *Non-E/E Requirements* |  | | |

Table 41: Requirement F-S-Req103 - Iginition Control Module Rejects Start Inhibit Request if Engine is Running

Please see the Functional Safety Requirement table for [Cloud and OTA Supervisor Communicates Manifest Securely](#_a8d1156cba0e2c7ecfd20c5c41ac21f9) displayed under the Safety Goal SG02.

### Safety Goal SG04 – Ensure Safe Verification of Activation

**Name:** Ensure Safe Verification of Activation

**Purpose:**

**Text:**

The updated part numbers need to be confirmed per the manifest

**ASIL:** D

#### Safety Concept

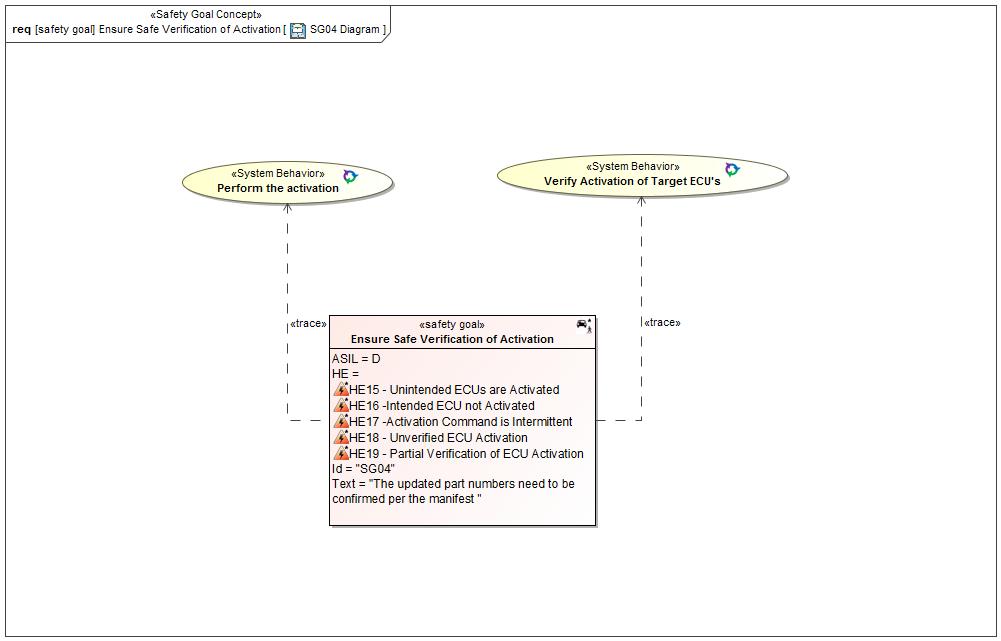


Figure 36: SG04 Diagram

#### Functional Safety Requirements

##### Requirement Derivation Diagram(s)(Optional)

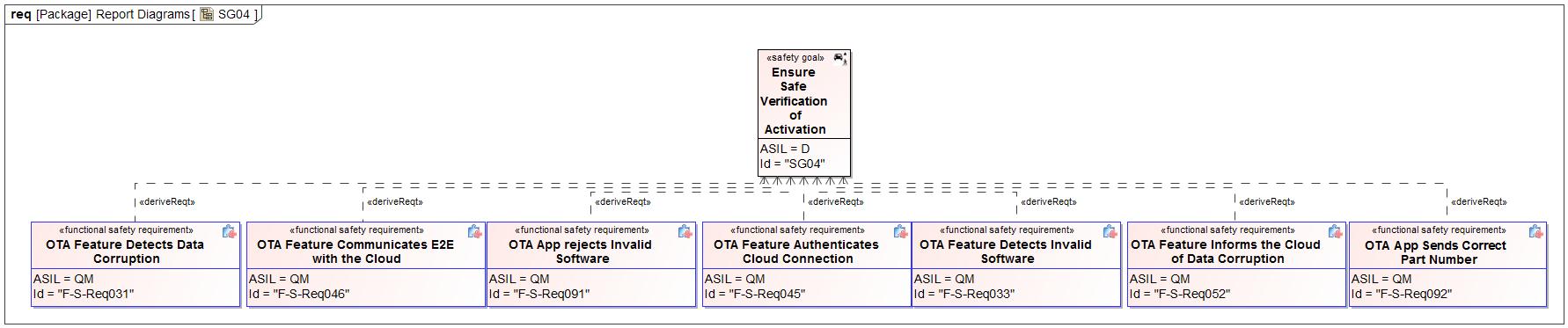


Figure 37 - Functional Safety Requirements Derivation Diagram for SG04

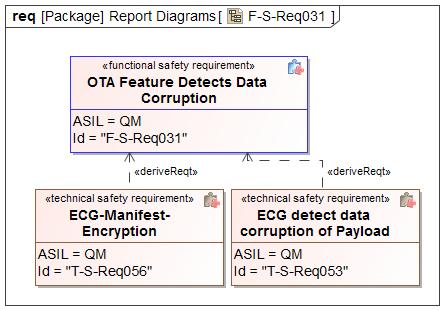


Figure 38 - Functional Safety Requirements Derivation Diagram for OTA Feature Detects Data Corruption

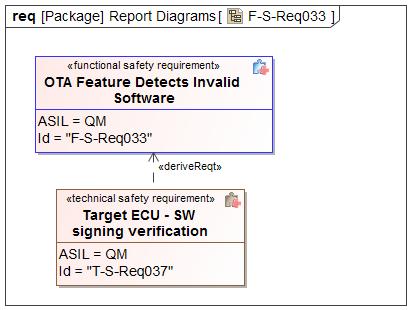


Figure 39 - Functional Safety Requirements Derivation Diagram for OTA Feature Detects Invalid Software

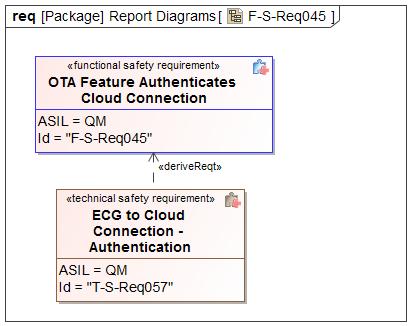


Figure 40 - Functional Safety Requirements Derivation Diagram for OTA Feature Authenticates Cloud Connection

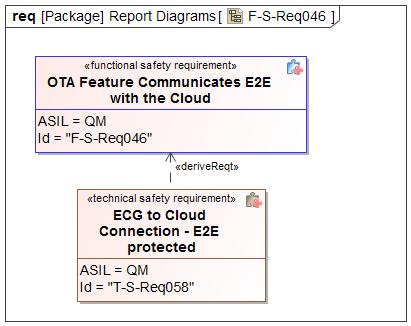


Figure 41 - Functional Safety Requirements Derivation Diagram for OTA Feature Communicates E2E with the Cloud

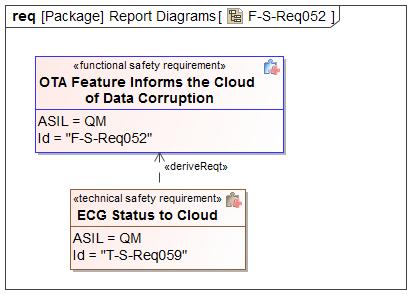


Figure 42 - Functional Safety Requirements Derivation Diagram for OTA Feature Informs the Cloud of Data Corruption

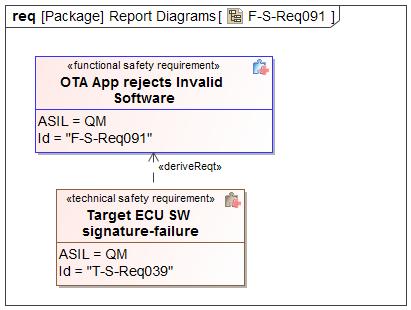


Figure 43 - Functional Safety Requirements Derivation Diagram for OTA App rejects Invalid Software

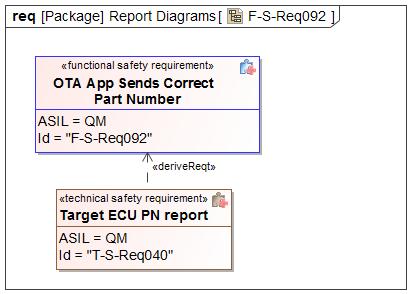


Figure 44 - Functional Safety Requirements Derivation Diagram for OTA App Sends Correct Part Number

##### Functional Safety Requirements for SG04 - Ensure Safe Verification of Activation

*Insert a table for each requirement according to its category.*

Please see the Functional Safety Requirement table for [Cloud Uses E2E](#_bfa5782f5133ad7e3479f6f556a349ef) displayed under the Safety Goal SG02.

Please see the Functional Safety Requirement table for [Powertrain Controls Ensure Start Has Been Inhibited](#_a042b56c4b399229727b05adb279e516) displayed under the Safety Goal SG03.

Please see the Functional Safety Requirement table for [OTA Governance Board shall review and approve the software that is to be pushed via OTA](#_5e9c9f6ae103b356824b6a2fea307a77) displayed under the Safety Goal SG02.

Please see the Functional Safety Requirement table for [Cloud Detects Data Corruption](#_c2b07e9d4169c67352344389f6bd163a) displayed under the Safety Goal SG02.

Please see the Functional Safety Requirement table for [Engineer Ensures Unique SW IDs](#_797e4f7cb4952f9289177ae847795e8f) displayed under the Safety Goal SG02.

Please see the Functional Safety Requirement table for [Engineer Uploads Correct Software](#_40547e13ba8870d835f2297ac78bbfe0) displayed under the Safety Goal SG02.

Please see the Functional Safety Requirement table for [Cloud Authenticates Software Update](#_4ca51e01184a59be985def8aa360adf7) displayed under the Safety Goal SG01.

Please see the Functional Safety Requirement table for [OTA Feature Detects Data Corruption](#_76f74d3d6f97e104e86d7f82f8a1ddf2) displayed under the Safety Goal SG01.

Please see the Functional Safety Requirement table for [OTA Feature Detects Invalid Software](#_126b516cfa2b0c927e018d1ef3a934c0) displayed under the Safety Goal SG02.

Please see the Functional Safety Requirement table for [Engineer Marks OTA and Non-OTA Software](#_70bc1df474703c72e5cd3a5a8243e41e) displayed under the Safety Goal SG02.

Please see the Functional Safety Requirement table for [OTA Feature Evaluates Safe Time to Perform Activation](#_284a84c3da72aeb284cdbf591676dc19) displayed under the Safety Goal SG03.

Please see the Functional Safety Requirement table for [OTA Feature Authenticates Cloud Connection](#_efd36d91e07c56151380e9b74df9ad0a) displayed under the Safety Goal SG01.

Please see the Functional Safety Requirement table for [OTA Feature Communicates E2E with the Cloud](#_a458b919ab42ff23acd4fea432087958) displayed under the Safety Goal SG01.

Please see the Functional Safety Requirement table for [Cloud Sends Correct Software for the Target ECU](#_f7354c219e6ca75d905bf27442e7fbdb) displayed under the Safety Goal SG02.

Please see the Functional Safety Requirement table for [OTA Feature Informs the Cloud of Data Corruption](#_d1f561bf9e8a4063ad777e30bc18134f) displayed under the Safety Goal SG01.

Please see the Functional Safety Requirement table for [Cloud and Engineers Ensure Correct Software is Flashed](#_1a52ed0580e4fe18b0253a01c3f1947f) displayed under the Safety Goal SG02.

Please see the Functional Safety Requirement table for [OTA App Detects Data Corruption During Software Download](#_0344dfc0fe65adce2f0ab2d4179cd7f1) displayed under the Safety Goal SG01.

Please see the Functional Safety Requirement table for [OTA Feature Detects Data Corruption During Software Download](#_469e6e08115ee3fecea46961210e32dd) displayed under the Safety Goal SG01.

Please see the Functional Safety Requirement table for [OTA Feature Command Inhibit Start](#_5eed06eafb01869c08654d163c8fee95) displayed under the Safety Goal SG03.

Please see the Functional Safety Requirement table for [Ignition Control Module Inhibits Start Upon Command](#_0791b33efcfd7cbd90196f9a3bd445f6) displayed under the Safety Goal SG03.

|  |  |  |  |
| --- | --- | --- | --- |
| Safety Req-ID | **F-S-Req077 - OTA App Authenticates ACTIVATION Commands** | |  |
| Category | Safety Related Function | |  |
| Version  *only applicable in case of:*   * *Non-E/E Requirements* |  | |  |
| Author  *only applicable in case of:*  *Non-E/E Requirements* |  | |  |
| External Reference *(optional)* |  | | |
| Safety Goal Ref. | SG04 - Ensure Safe Verification of Activation | Operating Modes | Ignition On |
| ASIL Classification:  *if applicable in case of category*   * *General*   *not applicable in case of category*   * *Non-E/E Requirement* | **ASIL Override Rationale -** Failure to authenticate the activation command would not violate the safety goal since security authentication is independent from the safety authentication.  QM | Safe State  *if applicable for:*   * *General Requirements* * *User information* * *Non-E/E Requirements* | Command rejected |
| Functional Safety Requirement Title | OTA App Authenticates ACTIVATION Commands | | |
| Functional Safety Requirement  *In case of User information including:*  *- Functional Safety Requirement Text*  *- Content of Information*  *- Method for Information*  *- Timing of Information*  *- Content of printed instructions (owner’s guide/service manuals etc.)* | The OTA App in the Target ECU shall authenticate the "ACTIVATION" signal on reception from the OTA Feature (ECG). | | |
| Rationale | To ensure that the OTA App processes the ACTIVATION signal only if they are from legitimate sources. To prevent improper ACTIVATION. | | |
| Description of actions of the driver or other endangered persons  *if applicable in case of:*   * *Safety Related Functions* * *Reduced Functionality* * *User information*   *not applicable in case of:*   * *General Requirements* * *Maintain Safe State / Recovery* * *Non-E/E Requirements* |  | | |
| Validation Criteria for these actions  *if applicable in case of:*   * *Safety Related Functions* * *Reduced Functionality* * *User information*   *not applicable in case of:*   * *General Requirements* * *Maintain Safe State / Recovery* * *Non-E/E Requirements* |  | | |
| Fault Tolerant Time interval *if applicable)* | N/A | | |
| Reduced Functionality interval *(if applicable)* |  | | |
| Functional Redundancies (e.g. fault tolerance)  *(if applicable)* |  | | |
| Requirement Status |  | | |
| V&V method | Vehicle test | | |
| V&V acceptance criteria  *not applicable in case of:*   * *Non-E/E Requirements* | Check for authentication Check for possibilities for breaking the implemented authentication system | | |
| V&V ID  *only applicable in case of:*   * *Non-E/E Requirements* |  | | |
| V&V Version  *only applicable in case of:*  *Non-E/E Requirements* |  | | |
| V&V Author  *only applicable in case of:*   * *Non-E/E Requirements* |  | | |
| V&V Status  *only applicable in case of:*   * *Non-E/E Requirements* |  | | |

Table 42: Requirement F-S-Req077 - OTA App Authenticates ACTIVATION Commands

|  |  |  |  |
| --- | --- | --- | --- |
| Safety Req-ID | **F-S-Req078 - Other ECU SW Reports ACTIVATION Readiness** | |  |
| Category | Safety Related Function | |  |
| Version  *only applicable in case of:*   * *Non-E/E Requirements* |  | |  |
| Author  *only applicable in case of:*  *Non-E/E Requirements* |  | |  |
| External Reference *(optional)* |  | | |
| Safety Goal Ref. | SG04 - Ensure Safe Verification of Activation | Operating Modes | Ignition On |
| ASIL Classification:  *if applicable in case of category*   * *General*   *not applicable in case of category*   * *Non-E/E Requirement* | **ASIL Override Rationale -** A failure to meet the activation time limit would not violate the safety goal of the module. It is upon the OTA Feature to determine the overall success or failure of the multi-module ACTIVATION and act accordingly.  QM | Safe State  *if applicable for:*   * *General Requirements* * *User information* * *Non-E/E Requirements* | N/A |
| Functional Safety Requirement Title | Other ECU SW Reports ACTIVATION Readiness | | |
| Functional Safety Requirement  *In case of User information including:*  *- Functional Safety Requirement Text*  *- Content of Information*  *- Method for Information*  *- Timing of Information*  *- Content of printed instructions (owner’s guide/service manuals etc.)* | Upon request via the OTA App in the Target ECU, the Other ECU SW shall report their readiness to perform the ACTIVATION function. | | |
| Rationale | To be able to know that Other ECU SW’s have really completed flashing and consider themselves ready to do a ACTIVATION. | | |
| Description of actions of the driver or other endangered persons  *if applicable in case of:*   * *Safety Related Functions* * *Reduced Functionality* * *User information*   *not applicable in case of:*   * *General Requirements* * *Maintain Safe State / Recovery* * *Non-E/E Requirements* |  | | |
| Validation Criteria for these actions  *if applicable in case of:*   * *Safety Related Functions* * *Reduced Functionality* * *User information*   *not applicable in case of:*   * *General Requirements* * *Maintain Safe State / Recovery* * *Non-E/E Requirements* |  | | |
| Fault Tolerant Time interval *if applicable)* | N/A | | |
| Reduced Functionality interval *(if applicable)* |  | | |
| Functional Redundancies (e.g. fault tolerance)  *(if applicable)* |  | | |
| Requirement Status |  | | |
| V&V method | Vehicle test | | |
| V&V acceptance criteria  *not applicable in case of:*   * *Non-E/E Requirements* | Check if Other ECU SW(s) coomunicate readiness | | |
| V&V ID  *only applicable in case of:*   * *Non-E/E Requirements* |  | | |
| V&V Version  *only applicable in case of:*  *Non-E/E Requirements* |  | | |
| V&V Author  *only applicable in case of:*   * *Non-E/E Requirements* |  | | |
| V&V Status  *only applicable in case of:*   * *Non-E/E Requirements* |  | | |

Table 43: Requirement F-S-Req078 - Other ECU SW Reports ACTIVATION Readiness

Please see the Functional Safety Requirement table for [OTA App (ASIL C/D) Verify Safe Vehicle State](#_bffab8356c3ab9f101860ca95b9bbf59) displayed under the Safety Goal SG03.

|  |  |  |  |
| --- | --- | --- | --- |
| Safety Req-ID | **F-S-Req080 - OTA App Communicates E2E with the OTA Feature** | |  |
| Category | Safety Related Function | |  |
| Version  *only applicable in case of:*   * *Non-E/E Requirements* |  | |  |
| Author  *only applicable in case of:*  *Non-E/E Requirements* |  | |  |
| External Reference *(optional)* |  | | |
| Safety Goal Ref. | SG04 - Ensure Safe Verification of Activation | Operating Modes | Ignition On |
| ASIL Classification:  *if applicable in case of category*   * *General*   *not applicable in case of category*   * *Non-E/E Requirement* | **ASIL Override Rationale -** Most CAN communication between the OTA App and OTA feature presents no ASIL rated violations. The exceptional ASIL rated communication are covered by separate addiitonal requirements.  QM | Safe State  *if applicable for:*   * *General Requirements* * *User information* * *Non-E/E Requirements* | Command rejected |
| Functional Safety Requirement Title | OTA App Communicates E2E with the OTA Feature | | |
| Functional Safety Requirement  *In case of User information including:*  *- Functional Safety Requirement Text*  *- Content of Information*  *- Method for Information*  *- Timing of Information*  *- Content of printed instructions (owner’s guide/service manuals etc.)* | The OTA App in the Target ECU shall communicate with the OTA Feature over an end-to-end protected communication path. | | |
| Rationale | To prevent malicious actors from uploading software over the CAN network. | | |
| Description of actions of the driver or other endangered persons  *if applicable in case of:*   * *Safety Related Functions* * *Reduced Functionality* * *User information*   *not applicable in case of:*   * *General Requirements* * *Maintain Safe State / Recovery* * *Non-E/E Requirements* |  | | |
| Validation Criteria for these actions  *if applicable in case of:*   * *Safety Related Functions* * *Reduced Functionality* * *User information*   *not applicable in case of:*   * *General Requirements* * *Maintain Safe State / Recovery* * *Non-E/E Requirements* |  | | |
| Fault Tolerant Time interval *if applicable)* | N/A | | |
| Reduced Functionality interval *(if applicable)* |  | | |
| Functional Redundancies (e.g. fault tolerance)  *(if applicable)* |  | | |
| Requirement Status |  | | |
| V&V method | Vehicle test | | |
| V&V acceptance criteria  *not applicable in case of:*   * *Non-E/E Requirements* | The OTA App should be able to detect data corruption on the CAN bus | | |
| V&V ID  *only applicable in case of:*   * *Non-E/E Requirements* |  | | |
| V&V Version  *only applicable in case of:*  *Non-E/E Requirements* |  | | |
| V&V Author  *only applicable in case of:*   * *Non-E/E Requirements* |  | | |
| V&V Status  *only applicable in case of:*   * *Non-E/E Requirements* |  | | |

Table 44: Requirement F-S-Req080 - OTA App Communicates E2E with the OTA Feature

Please see the Functional Safety Requirement table for [Other ECU SW Provides Part Number](#_b17a109130a284464de3daf7f51ef258) displayed under the Safety Goal SG02.

Please see the Functional Safety Requirement table for [OTA App Prevents Active Memory Erasing or Writing](#_0ad92bdb6a99e3d10ce1dc0d0a77e60a) displayed under the Safety Goal SG01.

Please see the Functional Safety Requirement table for [Other ECU SW (ASIL C/D) Verify Safe Vehicle State](#_e1a5e6e842346be1b123f9d1bb141c29) displayed under the Safety Goal SG03.

Please see the Functional Safety Requirement table for [OTA App Informs the OTA Feature of Data Corruption](#_360bdf0d5ab05912ccfeafc1f7b16cad) displayed under the Safety Goal SG01.

Please see the Functional Safety Requirement table for [OTA App Authenticates Erase And Programming Commands](#_e63467aecb84419c92184c8c6805edc0) displayed under the Safety Goal SG01.

Please see the Functional Safety Requirement table for [OTA App Executes OTA Without Affecting Basic Function](#_27bc942123bd1574d78bbd287b70358c) displayed under the Safety Goal SG01.

Please see the Functional Safety Requirement table for [Other ECU SW Prevents Active Memory Erasing or Writing](#_2fad9e75d48a85a9587e37c286f61f5d) displayed under the Safety Goal SG01.

Please see the Functional Safety Requirement table for [Other ECU SW Executes OTA Without Affecting Basic Function](#_25f65ce1928c94d70c987c03951c4b4e) displayed under the Safety Goal SG01.

Please see the Functional Safety Requirement table for [OTA App rejects Invalid Software](#_9ef6d483a829a79f7882c26ec92e1d8f) displayed under the Safety Goal SG02.

Please see the Functional Safety Requirement table for [OTA App Sends Correct Part Number](#_22c4e180014b476d89e62ab131101f2f) displayed under the Safety Goal SG02.

Please see the Functional Safety Requirement table for [Other ECU SW Executes Active Memory](#_b8e39606250fba93cad1eea6e2003901) displayed under the Safety Goal SG01.

Please see the Functional Safety Requirement table for [OTA App Detects Communication Errors](#_9532234d56f31920200b2f5b2b4c28c4) displayed under the Safety Goal SG01.

Please see the Functional Safety Requirement table for [OTA Feature, OTA App, and Other ECU SW (ASIL C/D) Ensures Safe Time To Perform Activation](#_444a9bf5ba12d221e2c7050a8a404d6f) displayed under the Safety Goal SG03.

Please see the Functional Safety Requirement table for [OTA App and Other ECU SW (ASIL C/D) Ensures Safe Time To Perform Activation](#_70a16b42350a59de17383add9750f77e) displayed under the Safety Goal SG03.

Please see the Functional Safety Requirement table for [Independence in Ensuring Safe Time To Perform Activation](#_b60f124bff43593f89fa16de6dc08746) displayed under the Safety Goal SG03.

Please see the Functional Safety Requirement table for [OTA Feature and Ignition Control Module Communicates E2E](#_497b586208652b7bf3ecf9888364076e) displayed under the Safety Goal SG03.

Please see the Functional Safety Requirement table for [Ignition Control Module and Powertrain Controls Communicates E2E](#_6727b3fe41799c0eb954c97221e9193c) displayed under the Safety Goal SG03.

Please see the Functional Safety Requirement table for [Iginition Control Module Rejects Start Inhibit Request if Engine is Running](#_3fff402ec2f9eb6e2da7fec3b6571401) displayed under the Safety Goal SG03.

Please see the Functional Safety Requirement table for [Cloud and OTA Supervisor Communicates Manifest Securely](#_a8d1156cba0e2c7ecfd20c5c41ac21f9) displayed under the Safety Goal SG02.

### Safety Goal SG05 – Ensure Safe Rollback

**Name:** Ensure Safe Rollback

**Purpose:**

**Text:**

In case of failure to activate, the vehicle SW must rollback to the previous safe state SW

**ASIL:** D

#### Safety Concept

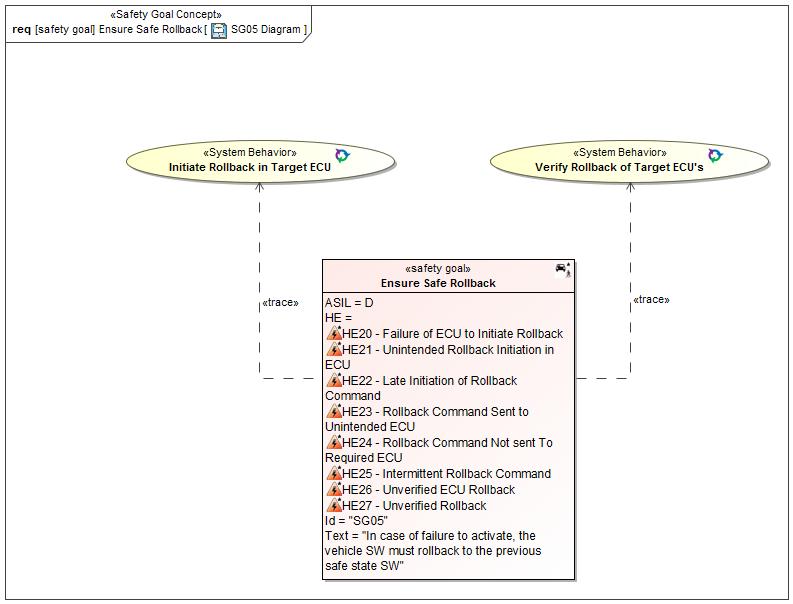


Figure 45: SG05 Diagram

#### Functional Safety Requirements

##### Requirement Derivation Diagram(s)(Optional)

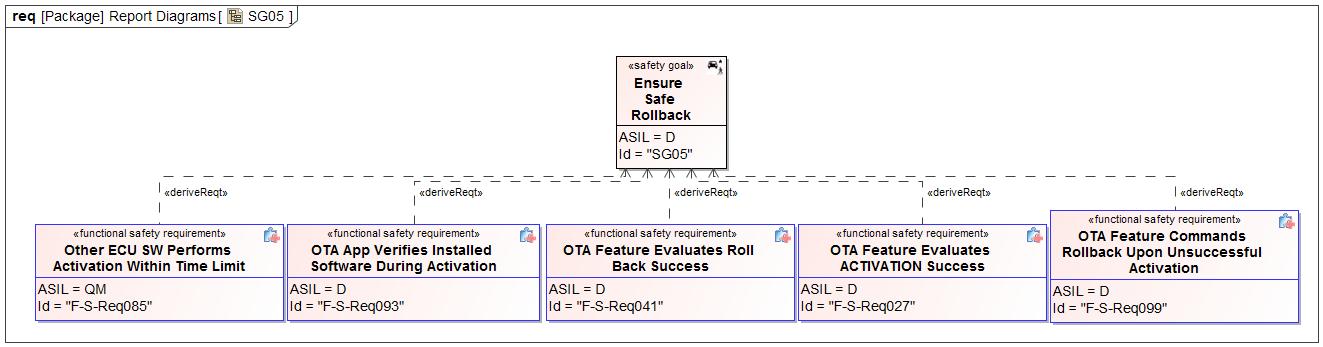


Figure 46 - Functional Safety Requirements Derivation Diagram for SG05

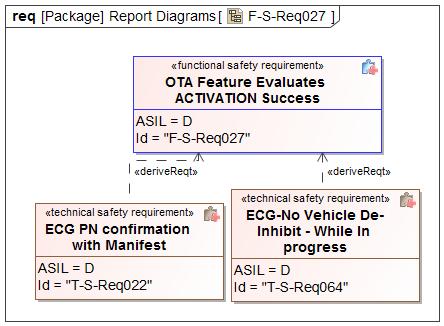


Figure 47 - Functional Safety Requirements Derivation Diagram for OTA Feature Evaluates ACTIVATION Success

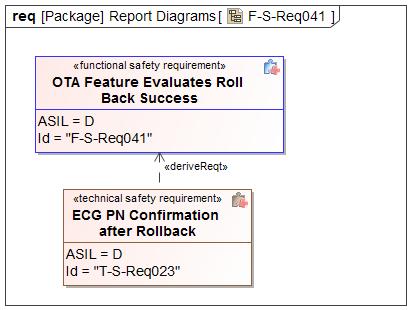


Figure 48 - Functional Safety Requirements Derivation Diagram for OTA Feature Evaluates Roll Back Success

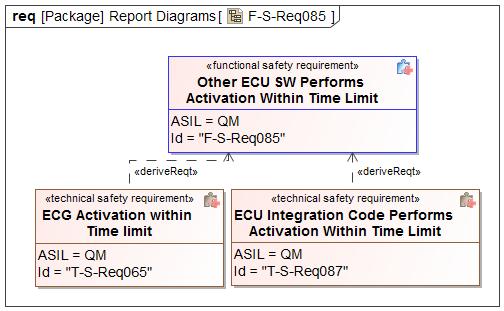


Figure 49 - Functional Safety Requirements Derivation Diagram for Other ECU SW Performs Activation Within Time Limit

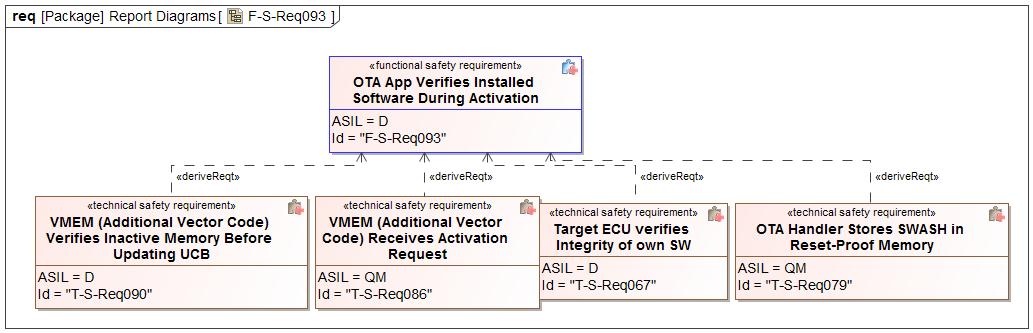


Figure 50 - Functional Safety Requirements Derivation Diagram for OTA App Verifies Installed Software During Activation

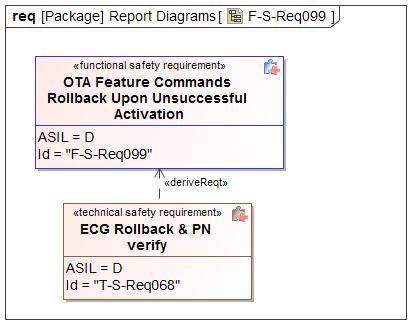


Figure 51 - Functional Safety Requirements Derivation Diagram for OTA Feature Commands Rollback Upon Unsuccessful Activation

##### Functional Safety Requirements for SG05 - Ensure Safe Rollback

*Insert a table for each requirement according to its category.*

Please see the Functional Safety Requirement table for [Cloud Uses E2E](#_bfa5782f5133ad7e3479f6f556a349ef) displayed under the Safety Goal SG02.

Please see the Functional Safety Requirement table for [Powertrain Controls Ensure Start Has Been Inhibited](#_a042b56c4b399229727b05adb279e516) displayed under the Safety Goal SG03.

Please see the Functional Safety Requirement table for [OTA Governance Board shall review and approve the software that is to be pushed via OTA](#_5e9c9f6ae103b356824b6a2fea307a77) displayed under the Safety Goal SG02.

Please see the Functional Safety Requirement table for [Cloud Detects Data Corruption](#_c2b07e9d4169c67352344389f6bd163a) displayed under the Safety Goal SG02.

Please see the Functional Safety Requirement table for [Engineer Ensures Unique SW IDs](#_797e4f7cb4952f9289177ae847795e8f) displayed under the Safety Goal SG02.

Please see the Functional Safety Requirement table for [Engineer Uploads Correct Software](#_40547e13ba8870d835f2297ac78bbfe0) displayed under the Safety Goal SG02.

|  |  |  |  |
| --- | --- | --- | --- |
| Safety Req-ID | **F-S-Req027 - OTA Feature Evaluates ACTIVATION Success** | |  |
| Category | Safety Related Function | |  |
| Version  *only applicable in case of:*   * *Non-E/E Requirements* |  | |  |
| Author  *only applicable in case of:*  *Non-E/E Requirements* |  | |  |
| External Reference *(optional)* |  | | |
| Safety Goal Ref. | SG05 - Ensure Safe Rollback | Operating Modes | Ignition On |
| ASIL Classification:  *if applicable in case of category*   * *General*   *not applicable in case of category*   * *Non-E/E Requirement* | D | Safe State  *if applicable for:*   * *General Requirements* * *User information* * *Non-E/E Requirements* | Rollback initiated |
| Functional Safety Requirement Title | OTA Feature Evaluates ACTIVATION Success | | |
| Functional Safety Requirement  *In case of User information including:*  *- Functional Safety Requirement Text*  *- Content of Information*  *- Method for Information*  *- Timing of Information*  *- Content of printed instructions (owner’s guide/service manuals etc.)* | Before the next ignition cycle, the OTA Feature shall evaluate if all the relevant target ECU’s have performed ACTIVATION successfully by verifying all relevant Target ECUs are on the correct software version. | | |
| Rationale | To ensure that the target ECU performed ACTIVATION within the time window. | | |
| Description of actions of the driver or other endangered persons  *if applicable in case of:*   * *Safety Related Functions* * *Reduced Functionality* * *User information*   *not applicable in case of:*   * *General Requirements* * *Maintain Safe State / Recovery* * *Non-E/E Requirements* |  | | |
| Validation Criteria for these actions  *if applicable in case of:*   * *Safety Related Functions* * *Reduced Functionality* * *User information*   *not applicable in case of:*   * *General Requirements* * *Maintain Safe State / Recovery* * *Non-E/E Requirements* |  | | |
| Fault Tolerant Time interval *if applicable)* | ACTIVATION\_TIMEOUT | | |
| Reduced Functionality interval *(if applicable)* |  | | |
| Functional Redundancies (e.g. fault tolerance)  *(if applicable)* |  | | |
| Requirement Status |  | | |
| V&V method | Vehicle test | | |
| V&V acceptance criteria  *not applicable in case of:*   * *Non-E/E Requirements* | Verify the OTA Feature evaluates if all the relevant target ECU’s have performed ACTIVATION successfully before the next ignition cycle | | |
| V&V ID  *only applicable in case of:*   * *Non-E/E Requirements* |  | | |
| V&V Version  *only applicable in case of:*  *Non-E/E Requirements* |  | | |
| V&V Author  *only applicable in case of:*   * *Non-E/E Requirements* |  | | |
| V&V Status  *only applicable in case of:*   * *Non-E/E Requirements* |  | | |

Table 45: Requirement F-S-Req027 - OTA Feature Evaluates ACTIVATION Success

Please see the Functional Safety Requirement table for [Cloud Authenticates Software Update](#_4ca51e01184a59be985def8aa360adf7) displayed under the Safety Goal SG01.

Please see the Functional Safety Requirement table for [OTA Feature Detects Data Corruption](#_76f74d3d6f97e104e86d7f82f8a1ddf2) displayed under the Safety Goal SG01.

Please see the Functional Safety Requirement table for [OTA Feature Detects Invalid Software](#_126b516cfa2b0c927e018d1ef3a934c0) displayed under the Safety Goal SG02.

Please see the Functional Safety Requirement table for [Engineer Marks OTA and Non-OTA Software](#_70bc1df474703c72e5cd3a5a8243e41e) displayed under the Safety Goal SG02.

|  |  |  |  |
| --- | --- | --- | --- |
| Safety Req-ID | **F-S-Req041 - OTA Feature Evaluates Roll Back Success** | |  |
| Category | Safety Related Function | |  |
| Version  *only applicable in case of:*   * *Non-E/E Requirements* |  | |  |
| Author  *only applicable in case of:*  *Non-E/E Requirements* |  | |  |
| External Reference *(optional)* |  | | |
| Safety Goal Ref. | SG05 - Ensure Safe Rollback | Operating Modes | Ignition On |
| ASIL Classification:  *if applicable in case of category*   * *General*   *not applicable in case of category*   * *Non-E/E Requirement* | D | Safe State  *if applicable for:*   * *General Requirements* * *User information* * *Non-E/E Requirements* | Permanent Vehicle Inhibit |
| Functional Safety Requirement Title | OTA Feature Evaluates Roll Back Success | | |
| Functional Safety Requirement  *In case of User information including:*  *- Functional Safety Requirement Text*  *- Content of Information*  *- Method for Information*  *- Timing of Information*  *- Content of printed instructions (owner’s guide/service manuals etc.)* | During the rollback process, the OTA Feature shall evaluate if all the relevant target ECU’s have performed rollback successfully by verifying all relevant Target ECUs are on the previous software version. | | |
| Rationale | To ensure that the target ECU(s) really reversed ACTIVATION back to the original SW after a failed ACTIVATION attempt. | | |
| Description of actions of the driver or other endangered persons  *if applicable in case of:*   * *Safety Related Functions* * *Reduced Functionality* * *User information*   *not applicable in case of:*   * *General Requirements* * *Maintain Safe State / Recovery* * *Non-E/E Requirements* |  | | |
| Validation Criteria for these actions  *if applicable in case of:*   * *Safety Related Functions* * *Reduced Functionality* * *User information*   *not applicable in case of:*   * *General Requirements* * *Maintain Safe State / Recovery* * *Non-E/E Requirements* |  | | |
| Fault Tolerant Time interval *if applicable)* | ACTIVATION\_TIMEOUT | | |
| Reduced Functionality interval *(if applicable)* |  | | |
| Functional Redundancies (e.g. fault tolerance)  *(if applicable)* |  | | |
| Requirement Status |  | | |
| V&V method | Vehicle test | | |
| V&V acceptance criteria  *not applicable in case of:*   * *Non-E/E Requirements* | Verify the OTA Feature evaluates if the roll back was successful before the next ignition cycle. | | |
| V&V ID  *only applicable in case of:*   * *Non-E/E Requirements* |  | | |
| V&V Version  *only applicable in case of:*  *Non-E/E Requirements* |  | | |
| V&V Author  *only applicable in case of:*   * *Non-E/E Requirements* |  | | |
| V&V Status  *only applicable in case of:*   * *Non-E/E Requirements* |  | | |

Table 46: Requirement F-S-Req041 - OTA Feature Evaluates Roll Back Success

Please see the Functional Safety Requirement table for [OTA Feature Evaluates Safe Time to Perform Activation](#_284a84c3da72aeb284cdbf591676dc19) displayed under the Safety Goal SG03.

Please see the Functional Safety Requirement table for [OTA Feature Authenticates Cloud Connection](#_efd36d91e07c56151380e9b74df9ad0a) displayed under the Safety Goal SG01.

Please see the Functional Safety Requirement table for [OTA Feature Communicates E2E with the Cloud](#_a458b919ab42ff23acd4fea432087958) displayed under the Safety Goal SG01.

Please see the Functional Safety Requirement table for [Cloud Sends Correct Software for the Target ECU](#_f7354c219e6ca75d905bf27442e7fbdb) displayed under the Safety Goal SG02.

Please see the Functional Safety Requirement table for [OTA Feature Informs the Cloud of Data Corruption](#_d1f561bf9e8a4063ad777e30bc18134f) displayed under the Safety Goal SG01.

Please see the Functional Safety Requirement table for [Cloud and Engineers Ensure Correct Software is Flashed](#_1a52ed0580e4fe18b0253a01c3f1947f) displayed under the Safety Goal SG02.

Please see the Functional Safety Requirement table for [OTA App Detects Data Corruption During Software Download](#_0344dfc0fe65adce2f0ab2d4179cd7f1) displayed under the Safety Goal SG01.

Please see the Functional Safety Requirement table for [OTA Feature Detects Data Corruption During Software Download](#_469e6e08115ee3fecea46961210e32dd) displayed under the Safety Goal SG01.

Please see the Functional Safety Requirement table for [OTA Feature Command Inhibit Start](#_5eed06eafb01869c08654d163c8fee95) displayed under the Safety Goal SG03.

Please see the Functional Safety Requirement table for [Ignition Control Module Inhibits Start Upon Command](#_0791b33efcfd7cbd90196f9a3bd445f6) displayed under the Safety Goal SG03.

Please see the Functional Safety Requirement table for [OTA App Authenticates ACTIVATION Commands](#_7ea836717de6dfa23917304f2a2fbd4c) displayed under the Safety Goal SG04.

Please see the Functional Safety Requirement table for [Other ECU SW Reports ACTIVATION Readiness](#_6ba42446e78d1e5b0768c39bf56d7af4) displayed under the Safety Goal SG04.

Please see the Functional Safety Requirement table for [OTA App (ASIL C/D) Verify Safe Vehicle State](#_bffab8356c3ab9f101860ca95b9bbf59) displayed under the Safety Goal SG03.

Please see the Functional Safety Requirement table for [OTA App Communicates E2E with the OTA Feature](#_5ba720b2aad75d21e8a3bb978613a346) displayed under the Safety Goal SG04.

Please see the Functional Safety Requirement table for [Other ECU SW Provides Part Number](#_b17a109130a284464de3daf7f51ef258) displayed under the Safety Goal SG02.

Please see the Functional Safety Requirement table for [OTA App Prevents Active Memory Erasing or Writing](#_0ad92bdb6a99e3d10ce1dc0d0a77e60a) displayed under the Safety Goal SG01.

Please see the Functional Safety Requirement table for [Other ECU SW (ASIL C/D) Verify Safe Vehicle State](#_e1a5e6e842346be1b123f9d1bb141c29) displayed under the Safety Goal SG03.

Please see the Functional Safety Requirement table for [OTA App Informs the OTA Feature of Data Corruption](#_360bdf0d5ab05912ccfeafc1f7b16cad) displayed under the Safety Goal SG01.

|  |  |  |  |
| --- | --- | --- | --- |
| Safety Req-ID | **F-S-Req085 - Other ECU SW Performs Activation Within Time Limit** | |  |
| Category | Safety Related Function | |  |
| Version  *only applicable in case of:*   * *Non-E/E Requirements* |  | |  |
| Author  *only applicable in case of:*  *Non-E/E Requirements* |  | |  |
| External Reference *(optional)* |  | | |
| Safety Goal Ref. | SG05 - Ensure Safe Rollback | Operating Modes | Ignition On |
| ASIL Classification:  *if applicable in case of category*   * *General*   *not applicable in case of category*   * *Non-E/E Requirement* | **ASIL Override Rationale -** A failure to meet the activation time limit would not violate the safety goal of the module. It is upon the OTA Feature to determine the overall success or failure of the multi-module ACTIVATION and act accordingly.  QM | Safe State  *if applicable for:*   * *General Requirements* * *User information* * *Non-E/E Requirements* | Permanent Vehicle Inhibit |
| Functional Safety Requirement Title | Other ECU SW Performs Activation Within Time Limit | | |
| Functional Safety Requirement  *In case of User information including:*  *- Functional Safety Requirement Text*  *- Content of Information*  *- Method for Information*  *- Timing of Information*  *- Content of printed instructions (owner’s guide/service manuals etc.)* | The Other ECU SW shall perform ACTIVATION within a deterministic time “ACTIVATION\_TIMEOUT” after it receives the correct "ACTIVATION" command via the OTA App. | | |
| Rationale | To ensure that the Other ECU SW switches active memory within a pre-definable time and also so as to make it possible for the OTA Feature to verify this after that time window elapses. | | |
| Description of actions of the driver or other endangered persons  *if applicable in case of:*   * *Safety Related Functions* * *Reduced Functionality* * *User information*   *not applicable in case of:*   * *General Requirements* * *Maintain Safe State / Recovery* * *Non-E/E Requirements* |  | | |
| Validation Criteria for these actions  *if applicable in case of:*   * *Safety Related Functions* * *Reduced Functionality* * *User information*   *not applicable in case of:*   * *General Requirements* * *Maintain Safe State / Recovery* * *Non-E/E Requirements* |  | | |
| Fault Tolerant Time interval *if applicable)* | N/A | | |
| Reduced Functionality interval *(if applicable)* |  | | |
| Functional Redundancies (e.g. fault tolerance)  *(if applicable)* |  | | |
| Requirement Status |  | | |
| V&V method | Vehicle test | | |
| V&V acceptance criteria  *not applicable in case of:*   * *Non-E/E Requirements* | Verify the Other ECU SW ensures switching over execution to the newly flashed software within a deterministic time ACTIVATION\_TIMEOUT after it receives the ACTIVATION signal from the OTA Feature | | |
| V&V ID  *only applicable in case of:*   * *Non-E/E Requirements* |  | | |
| V&V Version  *only applicable in case of:*  *Non-E/E Requirements* |  | | |
| V&V Author  *only applicable in case of:*   * *Non-E/E Requirements* |  | | |
| V&V Status  *only applicable in case of:*   * *Non-E/E Requirements* |  | | |

Table 47: Requirement F-S-Req085 - Other ECU SW Performs Activation Within Time Limit

Please see the Functional Safety Requirement table for [OTA App Authenticates Erase And Programming Commands](#_e63467aecb84419c92184c8c6805edc0) displayed under the Safety Goal SG01.

Please see the Functional Safety Requirement table for [OTA App Executes OTA Without Affecting Basic Function](#_27bc942123bd1574d78bbd287b70358c) displayed under the Safety Goal SG01.

Please see the Functional Safety Requirement table for [Other ECU SW Prevents Active Memory Erasing or Writing](#_2fad9e75d48a85a9587e37c286f61f5d) displayed under the Safety Goal SG01.

Please see the Functional Safety Requirement table for [Other ECU SW Executes OTA Without Affecting Basic Function](#_25f65ce1928c94d70c987c03951c4b4e) displayed under the Safety Goal SG01.

Please see the Functional Safety Requirement table for [OTA App rejects Invalid Software](#_9ef6d483a829a79f7882c26ec92e1d8f) displayed under the Safety Goal SG02.

Please see the Functional Safety Requirement table for [OTA App Sends Correct Part Number](#_22c4e180014b476d89e62ab131101f2f) displayed under the Safety Goal SG02.

|  |  |  |  |
| --- | --- | --- | --- |
| Safety Req-ID | **F-S-Req093 - OTA App Verifies Installed Software During Activation** | |  |
| Category | Safety Related Function | |  |
| Version  *only applicable in case of:*   * *Non-E/E Requirements* |  | |  |
| Author  *only applicable in case of:*  *Non-E/E Requirements* |  | |  |
| External Reference *(optional)* |  | | |
| Safety Goal Ref. | SG05 - Ensure Safe Rollback | Operating Modes | Ignition On |
| ASIL Classification:  *if applicable in case of category*   * *General*   *not applicable in case of category*   * *Non-E/E Requirement* | D | Safe State  *if applicable for:*   * *General Requirements* * *User information* * *Non-E/E Requirements* | Software Rejected |
| Functional Safety Requirement Title | OTA App Verifies Installed Software During Activation | | |
| Functional Safety Requirement  *In case of User information including:*  *- Functional Safety Requirement Text*  *- Content of Information*  *- Method for Information*  *- Timing of Information*  *- Content of printed instructions (owner’s guide/service manuals etc.)* | The OTA App in the Target ECU shall verify the integrity of the newly flashed software as part of the ACTIVATION process. | | |
| Rationale | To ensure that the SW that is re-flashed has not got tampered or corrupted due to any reason. To ensure the module can switch to a valid software. | | |
| Description of actions of the driver or other endangered persons  *if applicable in case of:*   * *Safety Related Functions* * *Reduced Functionality* * *User information*   *not applicable in case of:*   * *General Requirements* * *Maintain Safe State / Recovery* * *Non-E/E Requirements* |  | | |
| Validation Criteria for these actions  *if applicable in case of:*   * *Safety Related Functions* * *Reduced Functionality* * *User information*   *not applicable in case of:*   * *General Requirements* * *Maintain Safe State / Recovery* * *Non-E/E Requirements* |  | | |
| Fault Tolerant Time interval *if applicable)* | 1 second | | |
| Reduced Functionality interval *(if applicable)* |  | | |
| Functional Redundancies (e.g. fault tolerance)  *(if applicable)* |  | | |
| Requirement Status |  | | |
| V&V method | Vehicle test | | |
| V&V acceptance criteria  *not applicable in case of:*   * *Non-E/E Requirements* | Check if the OTA App can reject corrupted software | | |
| V&V ID  *only applicable in case of:*   * *Non-E/E Requirements* |  | | |
| V&V Version  *only applicable in case of:*  *Non-E/E Requirements* |  | | |
| V&V Author  *only applicable in case of:*   * *Non-E/E Requirements* |  | | |
| V&V Status  *only applicable in case of:*   * *Non-E/E Requirements* |  | | |

Table 48: Requirement F-S-Req093 - OTA App Verifies Installed Software During Activation

Please see the Functional Safety Requirement table for [Other ECU SW Executes Active Memory](#_b8e39606250fba93cad1eea6e2003901) displayed under the Safety Goal SG01.

Please see the Functional Safety Requirement table for [OTA App Detects Communication Errors](#_9532234d56f31920200b2f5b2b4c28c4) displayed under the Safety Goal SG01.

Please see the Functional Safety Requirement table for [OTA Feature, OTA App, and Other ECU SW (ASIL C/D) Ensures Safe Time To Perform Activation](#_444a9bf5ba12d221e2c7050a8a404d6f) displayed under the Safety Goal SG03.

Please see the Functional Safety Requirement table for [OTA App and Other ECU SW (ASIL C/D) Ensures Safe Time To Perform Activation](#_70a16b42350a59de17383add9750f77e) displayed under the Safety Goal SG03.

Please see the Functional Safety Requirement table for [Independence in Ensuring Safe Time To Perform Activation](#_b60f124bff43593f89fa16de6dc08746) displayed under the Safety Goal SG03.

|  |  |  |  |
| --- | --- | --- | --- |
| Safety Req-ID | **F-S-Req099 - OTA Feature Commands Rollback Upon Unsuccessful Activation** | |  |
| Category | Safety Related Function | |  |
| Version  *only applicable in case of:*   * *Non-E/E Requirements* |  | |  |
| Author  *only applicable in case of:*  *Non-E/E Requirements* |  | |  |
| External Reference *(optional)* |  | | |
| Safety Goal Ref. | SG05 - Ensure Safe Rollback | Operating Modes | Ignition On |
| ASIL Classification:  *if applicable in case of category*   * *General*   *not applicable in case of category*   * *Non-E/E Requirement* | D | Safe State  *if applicable for:*   * *General Requirements* * *User information* * *Non-E/E Requirements* | New software not activated  Permanent Vehicle Inhibit |
| Functional Safety Requirement Title | OTA Feature Commands Rollback Upon Unsuccessful Activation | | |
| Functional Safety Requirement  *In case of User information including:*  *- Functional Safety Requirement Text*  *- Content of Information*  *- Method for Information*  *- Timing of Information*  *- Content of printed instructions (owner’s guide/service manuals etc.)* | In the event of an unsuccessful ACTIVATION, the OTA feature shall command roll back of the relevant target ECUs. | | |
| Rationale | To ensure that the target ECU(s) really reversed ACTIVATION back to the original SW after a failed ACTIVATION attempt. | | |
| Description of actions of the driver or other endangered persons  *if applicable in case of:*   * *Safety Related Functions* * *Reduced Functionality* * *User information*   *not applicable in case of:*   * *General Requirements* * *Maintain Safe State / Recovery* * *Non-E/E Requirements* |  | | |
| Validation Criteria for these actions  *if applicable in case of:*   * *Safety Related Functions* * *Reduced Functionality* * *User information*   *not applicable in case of:*   * *General Requirements* * *Maintain Safe State / Recovery* * *Non-E/E Requirements* |  | | |
| Fault Tolerant Time interval *if applicable)* | ACTIVATION\_TIMEOUT | | |
| Reduced Functionality interval *(if applicable)* |  | | |
| Functional Redundancies (e.g. fault tolerance)  *(if applicable)* |  | | |
| Requirement Status |  | | |
| V&V method | Vehicle test | | |
| V&V acceptance criteria  *not applicable in case of:*   * *Non-E/E Requirements* | Verify the OTA Feature commands rollback upon unsuccessful activation | | |
| V&V ID  *only applicable in case of:*   * *Non-E/E Requirements* |  | | |
| V&V Version  *only applicable in case of:*  *Non-E/E Requirements* |  | | |
| V&V Author  *only applicable in case of:*   * *Non-E/E Requirements* |  | | |
| V&V Status  *only applicable in case of:*   * *Non-E/E Requirements* |  | | |

Table 49: Requirement F-S-Req099 - OTA Feature Commands Rollback Upon Unsuccessful Activation

Please see the Functional Safety Requirement table for [OTA Feature and Ignition Control Module Communicates E2E](#_497b586208652b7bf3ecf9888364076e) displayed under the Safety Goal SG03.

Please see the Functional Safety Requirement table for [Ignition Control Module and Powertrain Controls Communicates E2E](#_6727b3fe41799c0eb954c97221e9193c) displayed under the Safety Goal SG03.

Please see the Functional Safety Requirement table for [Iginition Control Module Rejects Start Inhibit Request if Engine is Running](#_3fff402ec2f9eb6e2da7fec3b6571401) displayed under the Safety Goal SG03.

Please see the Functional Safety Requirement table for [Cloud and OTA Supervisor Communicates Manifest Securely](#_a8d1156cba0e2c7ecfd20c5c41ac21f9) displayed under the Safety Goal SG02.

### Safety Goal SG6 – Ensure safe erase

**Name:** Ensure safe erase

**Purpose:**

**Text:** Inhibit the vehicle before starting the E/R

**ASIL:** D

#### Safety Concept

#### Functional Safety Requirements

##### Functional Safety Requirements for SG6 - Ensure safe erase

*Insert a table for each requirement according to its category.*

Please see the Functional Safety Requirement table for [Cloud Uses E2E](#_bfa5782f5133ad7e3479f6f556a349ef) displayed under the Safety Goal SG02.

Please see the Functional Safety Requirement table for [Powertrain Controls Ensure Start Has Been Inhibited](#_a042b56c4b399229727b05adb279e516) displayed under the Safety Goal SG03.

Please see the Functional Safety Requirement table for [OTA Governance Board shall review and approve the software that is to be pushed via OTA](#_5e9c9f6ae103b356824b6a2fea307a77) displayed under the Safety Goal SG02.

Please see the Functional Safety Requirement table for [Cloud Detects Data Corruption](#_c2b07e9d4169c67352344389f6bd163a) displayed under the Safety Goal SG02.

Please see the Functional Safety Requirement table for [Engineer Ensures Unique SW IDs](#_797e4f7cb4952f9289177ae847795e8f) displayed under the Safety Goal SG02.

Please see the Functional Safety Requirement table for [Engineer Uploads Correct Software](#_40547e13ba8870d835f2297ac78bbfe0) displayed under the Safety Goal SG02.

Please see the Functional Safety Requirement table for [OTA Feature Evaluates ACTIVATION Success](#_1201bf93c6e74892cfce3184f741b328) displayed under the Safety Goal SG05.

Please see the Functional Safety Requirement table for [Cloud Authenticates Software Update](#_4ca51e01184a59be985def8aa360adf7) displayed under the Safety Goal SG01.

Please see the Functional Safety Requirement table for [OTA Feature Detects Data Corruption](#_76f74d3d6f97e104e86d7f82f8a1ddf2) displayed under the Safety Goal SG01.

Please see the Functional Safety Requirement table for [OTA Feature Detects Invalid Software](#_126b516cfa2b0c927e018d1ef3a934c0) displayed under the Safety Goal SG02.

Please see the Functional Safety Requirement table for [Engineer Marks OTA and Non-OTA Software](#_70bc1df474703c72e5cd3a5a8243e41e) displayed under the Safety Goal SG02.

Please see the Functional Safety Requirement table for [OTA Feature Evaluates Roll Back Success](#_c33c8cb17cda4f7b44af29220b7aff23) displayed under the Safety Goal SG05.

Please see the Functional Safety Requirement table for [OTA Feature Evaluates Safe Time to Perform Activation](#_284a84c3da72aeb284cdbf591676dc19) displayed under the Safety Goal SG03.

Please see the Functional Safety Requirement table for [OTA Feature Authenticates Cloud Connection](#_efd36d91e07c56151380e9b74df9ad0a) displayed under the Safety Goal SG01.

Please see the Functional Safety Requirement table for [OTA Feature Communicates E2E with the Cloud](#_a458b919ab42ff23acd4fea432087958) displayed under the Safety Goal SG01.

Please see the Functional Safety Requirement table for [Cloud Sends Correct Software for the Target ECU](#_f7354c219e6ca75d905bf27442e7fbdb) displayed under the Safety Goal SG02.

Please see the Functional Safety Requirement table for [OTA Feature Informs the Cloud of Data Corruption](#_d1f561bf9e8a4063ad777e30bc18134f) displayed under the Safety Goal SG01.

Please see the Functional Safety Requirement table for [Cloud and Engineers Ensure Correct Software is Flashed](#_1a52ed0580e4fe18b0253a01c3f1947f) displayed under the Safety Goal SG02.

Please see the Functional Safety Requirement table for [OTA App Detects Data Corruption During Software Download](#_0344dfc0fe65adce2f0ab2d4179cd7f1) displayed under the Safety Goal SG01.

Please see the Functional Safety Requirement table for [OTA Feature Detects Data Corruption During Software Download](#_469e6e08115ee3fecea46961210e32dd) displayed under the Safety Goal SG01.

Please see the Functional Safety Requirement table for [OTA Feature Command Inhibit Start](#_5eed06eafb01869c08654d163c8fee95) displayed under the Safety Goal SG03.

Please see the Functional Safety Requirement table for [Ignition Control Module Inhibits Start Upon Command](#_0791b33efcfd7cbd90196f9a3bd445f6) displayed under the Safety Goal SG03.

Please see the Functional Safety Requirement table for [OTA App Authenticates ACTIVATION Commands](#_7ea836717de6dfa23917304f2a2fbd4c) displayed under the Safety Goal SG04.

Please see the Functional Safety Requirement table for [Other ECU SW Reports ACTIVATION Readiness](#_6ba42446e78d1e5b0768c39bf56d7af4) displayed under the Safety Goal SG04.

Please see the Functional Safety Requirement table for [OTA App (ASIL C/D) Verify Safe Vehicle State](#_bffab8356c3ab9f101860ca95b9bbf59) displayed under the Safety Goal SG03.

Please see the Functional Safety Requirement table for [OTA App Communicates E2E with the OTA Feature](#_5ba720b2aad75d21e8a3bb978613a346) displayed under the Safety Goal SG04.

Please see the Functional Safety Requirement table for [Other ECU SW Provides Part Number](#_b17a109130a284464de3daf7f51ef258) displayed under the Safety Goal SG02.

Please see the Functional Safety Requirement table for [OTA App Prevents Active Memory Erasing or Writing](#_0ad92bdb6a99e3d10ce1dc0d0a77e60a) displayed under the Safety Goal SG01.

Please see the Functional Safety Requirement table for [Other ECU SW (ASIL C/D) Verify Safe Vehicle State](#_e1a5e6e842346be1b123f9d1bb141c29) displayed under the Safety Goal SG03.

Please see the Functional Safety Requirement table for [OTA App Informs the OTA Feature of Data Corruption](#_360bdf0d5ab05912ccfeafc1f7b16cad) displayed under the Safety Goal SG01.

Please see the Functional Safety Requirement table for [Other ECU SW Performs Activation Within Time Limit](#_b4423e010a63ca1ce4754c5248514a5d) displayed under the Safety Goal SG05.

Please see the Functional Safety Requirement table for [OTA App Authenticates Erase And Programming Commands](#_e63467aecb84419c92184c8c6805edc0) displayed under the Safety Goal SG01.

Please see the Functional Safety Requirement table for [OTA App Executes OTA Without Affecting Basic Function](#_27bc942123bd1574d78bbd287b70358c) displayed under the Safety Goal SG01.

Please see the Functional Safety Requirement table for [Other ECU SW Prevents Active Memory Erasing or Writing](#_2fad9e75d48a85a9587e37c286f61f5d) displayed under the Safety Goal SG01.

Please see the Functional Safety Requirement table for [Other ECU SW Executes OTA Without Affecting Basic Function](#_25f65ce1928c94d70c987c03951c4b4e) displayed under the Safety Goal SG01.

Please see the Functional Safety Requirement table for [OTA App rejects Invalid Software](#_9ef6d483a829a79f7882c26ec92e1d8f) displayed under the Safety Goal SG02.

Please see the Functional Safety Requirement table for [OTA App Sends Correct Part Number](#_22c4e180014b476d89e62ab131101f2f) displayed under the Safety Goal SG02.

Please see the Functional Safety Requirement table for [OTA App Verifies Installed Software During Activation](#_5818e1f53582763e569a9d1a996e2acf) displayed under the Safety Goal SG05.

Please see the Functional Safety Requirement table for [Other ECU SW Executes Active Memory](#_b8e39606250fba93cad1eea6e2003901) displayed under the Safety Goal SG01.

Please see the Functional Safety Requirement table for [OTA App Detects Communication Errors](#_9532234d56f31920200b2f5b2b4c28c4) displayed under the Safety Goal SG01.

Please see the Functional Safety Requirement table for [OTA Feature, OTA App, and Other ECU SW (ASIL C/D) Ensures Safe Time To Perform Activation](#_444a9bf5ba12d221e2c7050a8a404d6f) displayed under the Safety Goal SG03.

Please see the Functional Safety Requirement table for [OTA App and Other ECU SW (ASIL C/D) Ensures Safe Time To Perform Activation](#_70a16b42350a59de17383add9750f77e) displayed under the Safety Goal SG03.

Please see the Functional Safety Requirement table for [Independence in Ensuring Safe Time To Perform Activation](#_b60f124bff43593f89fa16de6dc08746) displayed under the Safety Goal SG03.

Please see the Functional Safety Requirement table for [OTA Feature Commands Rollback Upon Unsuccessful Activation](#_0760a1bf3d86bb51b7ea9fc76ca0084d) displayed under the Safety Goal SG05.

Please see the Functional Safety Requirement table for [OTA Feature and Ignition Control Module Communicates E2E](#_497b586208652b7bf3ecf9888364076e) displayed under the Safety Goal SG03.

Please see the Functional Safety Requirement table for [Ignition Control Module and Powertrain Controls Communicates E2E](#_6727b3fe41799c0eb954c97221e9193c) displayed under the Safety Goal SG03.

Please see the Functional Safety Requirement table for [Iginition Control Module Rejects Start Inhibit Request if Engine is Running](#_3fff402ec2f9eb6e2da7fec3b6571401) displayed under the Safety Goal SG03.

Please see the Functional Safety Requirement table for [Cloud and OTA Supervisor Communicates Manifest Securely](#_a8d1156cba0e2c7ecfd20c5c41ac21f9) displayed under the Safety Goal SG02.

### Safety Goal SG7 – Ensure Safe Programming

**Name:** Ensure Safe Programming

**Purpose:**

**Text:** Inhibit the vehicle before starting the E/R

**ASIL:** D

#### Safety Concept

#### Functional Safety Requirements

##### Functional Safety Requirements for SG7 - Ensure Safe Programming

*Insert a table for each requirement according to its category.*

Please see the Functional Safety Requirement table for [Cloud Uses E2E](#_bfa5782f5133ad7e3479f6f556a349ef) displayed under the Safety Goal SG02.

Please see the Functional Safety Requirement table for [Powertrain Controls Ensure Start Has Been Inhibited](#_a042b56c4b399229727b05adb279e516) displayed under the Safety Goal SG03.

Please see the Functional Safety Requirement table for [OTA Governance Board shall review and approve the software that is to be pushed via OTA](#_5e9c9f6ae103b356824b6a2fea307a77) displayed under the Safety Goal SG02.

Please see the Functional Safety Requirement table for [Cloud Detects Data Corruption](#_c2b07e9d4169c67352344389f6bd163a) displayed under the Safety Goal SG02.

Please see the Functional Safety Requirement table for [Engineer Ensures Unique SW IDs](#_797e4f7cb4952f9289177ae847795e8f) displayed under the Safety Goal SG02.

Please see the Functional Safety Requirement table for [Engineer Uploads Correct Software](#_40547e13ba8870d835f2297ac78bbfe0) displayed under the Safety Goal SG02.

Please see the Functional Safety Requirement table for [OTA Feature Evaluates ACTIVATION Success](#_1201bf93c6e74892cfce3184f741b328) displayed under the Safety Goal SG05.

Please see the Functional Safety Requirement table for [Cloud Authenticates Software Update](#_4ca51e01184a59be985def8aa360adf7) displayed under the Safety Goal SG01.

Please see the Functional Safety Requirement table for [OTA Feature Detects Data Corruption](#_76f74d3d6f97e104e86d7f82f8a1ddf2) displayed under the Safety Goal SG01.

Please see the Functional Safety Requirement table for [OTA Feature Detects Invalid Software](#_126b516cfa2b0c927e018d1ef3a934c0) displayed under the Safety Goal SG02.

Please see the Functional Safety Requirement table for [Engineer Marks OTA and Non-OTA Software](#_70bc1df474703c72e5cd3a5a8243e41e) displayed under the Safety Goal SG02.

Please see the Functional Safety Requirement table for [OTA Feature Evaluates Roll Back Success](#_c33c8cb17cda4f7b44af29220b7aff23) displayed under the Safety Goal SG05.

Please see the Functional Safety Requirement table for [OTA Feature Evaluates Safe Time to Perform Activation](#_284a84c3da72aeb284cdbf591676dc19) displayed under the Safety Goal SG03.

Please see the Functional Safety Requirement table for [OTA Feature Authenticates Cloud Connection](#_efd36d91e07c56151380e9b74df9ad0a) displayed under the Safety Goal SG01.

Please see the Functional Safety Requirement table for [OTA Feature Communicates E2E with the Cloud](#_a458b919ab42ff23acd4fea432087958) displayed under the Safety Goal SG01.

Please see the Functional Safety Requirement table for [Cloud Sends Correct Software for the Target ECU](#_f7354c219e6ca75d905bf27442e7fbdb) displayed under the Safety Goal SG02.

Please see the Functional Safety Requirement table for [OTA Feature Informs the Cloud of Data Corruption](#_d1f561bf9e8a4063ad777e30bc18134f) displayed under the Safety Goal SG01.

Please see the Functional Safety Requirement table for [Cloud and Engineers Ensure Correct Software is Flashed](#_1a52ed0580e4fe18b0253a01c3f1947f) displayed under the Safety Goal SG02.

Please see the Functional Safety Requirement table for [OTA App Detects Data Corruption During Software Download](#_0344dfc0fe65adce2f0ab2d4179cd7f1) displayed under the Safety Goal SG01.

Please see the Functional Safety Requirement table for [OTA Feature Detects Data Corruption During Software Download](#_469e6e08115ee3fecea46961210e32dd) displayed under the Safety Goal SG01.

Please see the Functional Safety Requirement table for [OTA Feature Command Inhibit Start](#_5eed06eafb01869c08654d163c8fee95) displayed under the Safety Goal SG03.

Please see the Functional Safety Requirement table for [Ignition Control Module Inhibits Start Upon Command](#_0791b33efcfd7cbd90196f9a3bd445f6) displayed under the Safety Goal SG03.

Please see the Functional Safety Requirement table for [OTA App Authenticates ACTIVATION Commands](#_7ea836717de6dfa23917304f2a2fbd4c) displayed under the Safety Goal SG04.

Please see the Functional Safety Requirement table for [Other ECU SW Reports ACTIVATION Readiness](#_6ba42446e78d1e5b0768c39bf56d7af4) displayed under the Safety Goal SG04.

Please see the Functional Safety Requirement table for [OTA App (ASIL C/D) Verify Safe Vehicle State](#_bffab8356c3ab9f101860ca95b9bbf59) displayed under the Safety Goal SG03.

Please see the Functional Safety Requirement table for [OTA App Communicates E2E with the OTA Feature](#_5ba720b2aad75d21e8a3bb978613a346) displayed under the Safety Goal SG04.

Please see the Functional Safety Requirement table for [Other ECU SW Provides Part Number](#_b17a109130a284464de3daf7f51ef258) displayed under the Safety Goal SG02.

Please see the Functional Safety Requirement table for [OTA App Prevents Active Memory Erasing or Writing](#_0ad92bdb6a99e3d10ce1dc0d0a77e60a) displayed under the Safety Goal SG01.

Please see the Functional Safety Requirement table for [Other ECU SW (ASIL C/D) Verify Safe Vehicle State](#_e1a5e6e842346be1b123f9d1bb141c29) displayed under the Safety Goal SG03.

Please see the Functional Safety Requirement table for [OTA App Informs the OTA Feature of Data Corruption](#_360bdf0d5ab05912ccfeafc1f7b16cad) displayed under the Safety Goal SG01.

Please see the Functional Safety Requirement table for [Other ECU SW Performs Activation Within Time Limit](#_b4423e010a63ca1ce4754c5248514a5d) displayed under the Safety Goal SG05.

Please see the Functional Safety Requirement table for [OTA App Authenticates Erase And Programming Commands](#_e63467aecb84419c92184c8c6805edc0) displayed under the Safety Goal SG01.

Please see the Functional Safety Requirement table for [OTA App Executes OTA Without Affecting Basic Function](#_27bc942123bd1574d78bbd287b70358c) displayed under the Safety Goal SG01.

Please see the Functional Safety Requirement table for [Other ECU SW Prevents Active Memory Erasing or Writing](#_2fad9e75d48a85a9587e37c286f61f5d) displayed under the Safety Goal SG01.

Please see the Functional Safety Requirement table for [Other ECU SW Executes OTA Without Affecting Basic Function](#_25f65ce1928c94d70c987c03951c4b4e) displayed under the Safety Goal SG01.

Please see the Functional Safety Requirement table for [OTA App rejects Invalid Software](#_9ef6d483a829a79f7882c26ec92e1d8f) displayed under the Safety Goal SG02.

Please see the Functional Safety Requirement table for [OTA App Sends Correct Part Number](#_22c4e180014b476d89e62ab131101f2f) displayed under the Safety Goal SG02.

Please see the Functional Safety Requirement table for [OTA App Verifies Installed Software During Activation](#_5818e1f53582763e569a9d1a996e2acf) displayed under the Safety Goal SG05.

Please see the Functional Safety Requirement table for [Other ECU SW Executes Active Memory](#_b8e39606250fba93cad1eea6e2003901) displayed under the Safety Goal SG01.

Please see the Functional Safety Requirement table for [OTA App Detects Communication Errors](#_9532234d56f31920200b2f5b2b4c28c4) displayed under the Safety Goal SG01.

Please see the Functional Safety Requirement table for [OTA Feature, OTA App, and Other ECU SW (ASIL C/D) Ensures Safe Time To Perform Activation](#_444a9bf5ba12d221e2c7050a8a404d6f) displayed under the Safety Goal SG03.

Please see the Functional Safety Requirement table for [OTA App and Other ECU SW (ASIL C/D) Ensures Safe Time To Perform Activation](#_70a16b42350a59de17383add9750f77e) displayed under the Safety Goal SG03.

Please see the Functional Safety Requirement table for [Independence in Ensuring Safe Time To Perform Activation](#_b60f124bff43593f89fa16de6dc08746) displayed under the Safety Goal SG03.

Please see the Functional Safety Requirement table for [OTA Feature Commands Rollback Upon Unsuccessful Activation](#_0760a1bf3d86bb51b7ea9fc76ca0084d) displayed under the Safety Goal SG05.

Please see the Functional Safety Requirement table for [OTA Feature and Ignition Control Module Communicates E2E](#_497b586208652b7bf3ecf9888364076e) displayed under the Safety Goal SG03.

Please see the Functional Safety Requirement table for [Ignition Control Module and Powertrain Controls Communicates E2E](#_6727b3fe41799c0eb954c97221e9193c) displayed under the Safety Goal SG03.

Please see the Functional Safety Requirement table for [Iginition Control Module Rejects Start Inhibit Request if Engine is Running](#_3fff402ec2f9eb6e2da7fec3b6571401) displayed under the Safety Goal SG03.

Please see the Functional Safety Requirement table for [Cloud and OTA Supervisor Communicates Manifest Securely](#_a8d1156cba0e2c7ecfd20c5c41ac21f9) displayed under the Safety Goal SG02.

## Operating Modes Overview

*Insert Name of Operating Mode, an explanation including a short summary of the safety aspect and a reference to the document describing the Operating Mode in detail. Only operating modes having a safety aspect (e.g. the functional safety requirement depend on the operating mode) should be listed in the following table. The Operation Modes include the Safe States.*

|  |  |  |
| --- | --- | --- |
| Operating Mode | Explanation (including short summary of safety aspect) | Reference |
| Ignition Off | Driver has switched off the ignition |  |
| Ignition On | Driver has switched on the ignition |  |

Table 50: Operating Modes Overview

### Operating Modes Overview Diagram (optional)

*Insert a diagram depicting the Operating Modes (e.g., SysML diagram) if no diagram is in the documents referenced in Section 2.2. Otherwise, put in “n/a” instead of the diagram.*

**Error! Reference source not found.** shows the Operating Modes Overview Diagram.

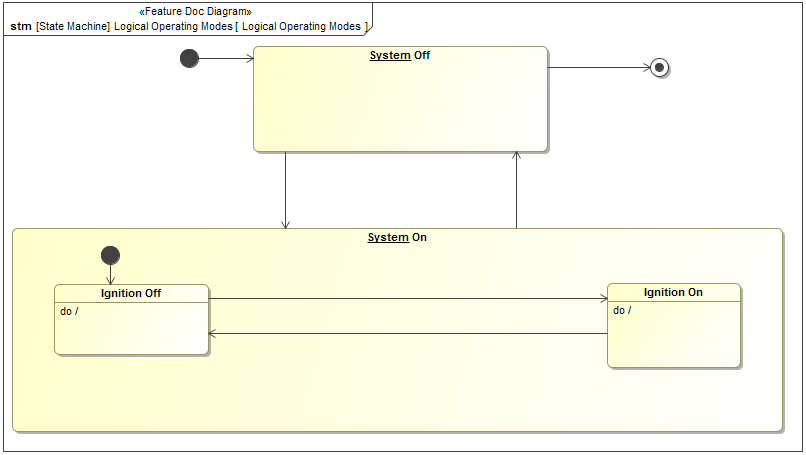


Figure 52: Operating Modes Overview Diagram

## Safe State and Requirement References

*To provide an overview, insert references to Safety Goals, the corresponding Safe States, reference to the Strategy, and reference to related Functional Safety Requirements (e.g., transition to safe state, user information and recovery to normal mode).*

Safe States related to Safety Goals not specified.

| **Functional Safety Requirement ID** | **Functional Safety Requirement Title** | **ASIL** | **Safe State** |
| --- | --- | --- | --- |
| F-S-Req018 | Cloud Uses E2E | QM | N/A |
| F-S-Req019 | Powertrain Controls Ensure Start Has Been Inhibited | B(D) | New software not activated |
| F-S-Req020 | OTA Governance Board shall review and approve the software that is to be pushed via OTA | QM | N/A |
| F-S-Req021 | Cloud Detects Data Corruption | QM | Software Rejected |
| F-S-Req022 | Engineer Ensures Unique SW IDs | QM | N/A |
| F-S-Req024 | Engineer Uploads Correct Software | QM | N/A |
| F-S-Req027 | OTA Feature Evaluates ACTIVATION Success | D | Rollback initiated |
| F-S-Req030 | Cloud Authenticates Software Update | QM | Software Rejected |
| F-S-Req031 | OTA Feature Detects Data Corruption | QM | Software Rejected |
| F-S-Req033 | OTA Feature Detects Invalid Software | QM | Software Rejected |
| F-S-Req040 | Engineer Marks OTA and Non-OTA Software | QM | N/A |
| F-S-Req041 | OTA Feature Evaluates Roll Back Success | D | Permanent Vehicle Inhibit |
| F-S-Req042 | OTA Feature Evaluates Safe Time to Perform Activation | B(D) | New software not activated |
| F-S-Req045 | OTA Feature Authenticates Cloud Connection | QM | Command rejected |
| F-S-Req046 | OTA Feature Communicates E2E with the Cloud | QM | N/A |
| F-S-Req047 | Cloud Sends Correct Software for the Target ECU | QM | N/A |
| F-S-Req052 | OTA Feature Informs the Cloud of Data Corruption | QM | N/A |
| F-S-Req059 | Cloud and Engineers Ensure Correct Software is Flashed | QM | Software Rejected |
| F-S-Req071 | OTA App Detects Data Corruption During Software Download | QM | Software Rejected |
| F-S-Req072 | OTA Feature Detects Data Corruption During Software Download | QM | Software Rejected |
| F-S-Req074 | OTA Feature Command Inhibit Start | B(D) | New software not activated |
| F-S-Req075 | Ignition Control Module Inhibits Start Upon Command | B(D) | New software not activated |
| F-S-Req077 | OTA App Authenticates ACTIVATION Commands | QM | Command rejected |
| F-S-Req078 | Other ECU SW Reports ACTIVATION Readiness | QM | N/A |
| F-S-Req079 | OTA App (ASIL C/D) Verify Safe Vehicle State | B(D) | New software not activated |
| F-S-Req080 | OTA App Communicates E2E with the OTA Feature | QM | Command rejected |
| F-S-Req081 | Other ECU SW Provides Part Number | QM | New software not activated |
| F-S-Req082 | OTA App Prevents Active Memory Erasing or Writing | D | Software Rejected |
| F-S-Req083 | Other ECU SW (ASIL C/D) Verify Safe Vehicle State | B(D) | New software not activated |
| F-S-Req084 | OTA App Informs the OTA Feature of Data Corruption | QM | Software Rejected |
| F-S-Req085 | Other ECU SW Performs Activation Within Time Limit | QM | Permanent Vehicle Inhibit |
| F-S-Req086 | OTA App Authenticates Erase And Programming Commands | QM | Command rejected |
| F-S-Req087 | OTA App Executes OTA Without Affecting Basic Function | D | Software Rejected |
| F-S-Req088 | Other ECU SW Prevents Active Memory Erasing or Writing | D | Software Rejected |
| F-S-Req090 | Other ECU SW Executes OTA Without Affecting Basic Function | D | Software Rejected |
| F-S-Req091 | OTA App rejects Invalid Software | QM | Software Rejected |
| F-S-Req092 | OTA App Sends Correct Part Number | QM | New software not activated |
| F-S-Req093 | OTA App Verifies Installed Software During Activation | D | Software Rejected |
| F-S-Req094 | Other ECU SW Executes Active Memory | D | Target ECU not running |
| F-S-Req095 | OTA App Detects Communication Errors | QM | Software Rejected |
| F-S-Req096 | OTA Feature, OTA App, and Other ECU SW (ASIL C/D) Ensures Safe Time To Perform Activation | D | Target ECU not running |
| F-S-Req097 | OTA App and Other ECU SW (ASIL C/D) Ensures Safe Time To Perform Activation | B(D) | Target ECU not running |
| F-S-Req098 | Independence in Ensuring Safe Time To Perform Activation | D | Target ECU not running |
| F-S-Req099 | OTA Feature Commands Rollback Upon Unsuccessful Activation | D | New software not activated  Permanent Vehicle Inhibit |
| F-S-Req100 | OTA Feature and Ignition Control Module Communicates E2E | B(D) | Software Rejected |
| F-S-Req101 | Ignition Control Module and Powertrain Controls Communicates E2E | B(D) | New software not activated |
| F-S-Req103 | Iginition Control Module Rejects Start Inhibit Request if Engine is Running | B(D) | New software not activated |
| F-S-Req111 | Cloud and OTA Supervisor Communicates Manifest Securely | QM | N/A |

Table 51: Safe State and Functional Safety Requirement Overview

*Note: General Requirements, Reduced Functionality Safety Requirement, User Information Functional Safety Requirement, and Recovery Functional Safety Requirement are not covered by this table.*

Neither User Information Functional Safety Requirements nor Maintain Safe State/Recovery Functional Safety Requirements specified.

## Derivation of Requirements on means, controls and user manual to ensure driver (or other persons involved) controllability

*Insert the assumptions from the controllability rationale in document "FFSD 02 Hazard Analysis* *and Risk Assessment”.*

*Describe the driver actions necessary to control the situation.*

*Describe adequate means and controls to realize driver controllability and validation activity for controllability assumptions.*

*If applicable, add a reference to the Functional Safety Requirements defining the necessary means and controls with ID and title. If applicable, add an additional line the content of printed instructions (owner’s guide/ service manuals etc.).*

No Assumptions specified.

Safety Goal with Fault Tolerant Time Interval not specified.

## Definition of parameters used in the Functional Safety Requirements

*Insert parameter name with description in brackets, a preliminary value and / or a range, and the constraints for the value range* *as well as a rationale or reference to a document containing the rationale for the constraints.*

*Note: This section includes preliminary definition of the parameters for the development of the Safety Concept. The refined parameters are documented in the appropriate document as authoritative source of information for the implementation, e.g. in the Safety Requirement Specification, SW Requirements, documentation for performance tuning etc.*

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| ID | Parameter name  (Description) | Used in Reqs. | Preliminary Value and/or Range | Constraints | Rationale |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

Table 52: Parameter

## ASIL Decomposition (OPTIONAL)

### Decomposition Functional Safety Requirement F-S-Req096

Independence in Ensuring Safe Time To Perform Activation

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Initial Safety Reqirement | | Functional Safety Requirement F-S-Req096 | | |
| Decomposition Rationale |  | | | |
| **Method for Decomposition** | |  | D 🡺 C(D) + A(D) | |
| X | D 🡺 B(D) + B(D) | |
|  | D 🡺 D(D) + QM(D) | |
|  | C 🡺 B(C) + A(C) | |
|  | C 🡺 C(C) + QM(C) | |
|  | B 🡺 A(B) + A(B) | |
|  | B 🡺 B(B) + QM(B) | |
|  | A 🡺 A(A) + QM(A) | |
| Functional Safety Requirement 1 after Decomposition | | Req.-ID | | F-S-Req042 |
| ASIL | | B(D) |
| Req. Title | | OTA Feature Evaluates Safe Time to Perform Activation |
| Rationale | | To ensure that the OTA Feature sends the ACTIVATION signal at the right point of time Examples – - After the ignition is switched off and vehicle is stationary;  - Same ignition cycle (key on-off) after reception of the ACTIVATION authorization; - Never send an ACTIVATION signal without the authorization of the cloud; - Every target ECU will not be able to detect the vehicle state and hence this would need to be able to be done by the OTA Feature itself. |
| Functional Safety Requirement 2 after Decomposition | | Req.-ID | | F-S-Req097  #sorter.humanSort([com.nomagic.uml2.ext.magicdraw.classes.mdkernel.impl.ClassImpl@17c99b98, com.nomagic.uml2.ext.magicdraw.classes.mdkernel.impl.ClassImpl@908e366], ‘Id’).get(1).Id) |
| ASIL | | B(D) |
| Req. Title | | OTA App and Other ECU SW (ASIL C/D) Ensures Safe Time To Perform Activation |
| Rationale | | To prevent a malfunction of the MMOTA feature from causing the highest level hazard in the target ECU. |
| Functional Safety Requirement for Independence | | Req.-ID | | F-S-Req098 |
| ASIL | | D |
| Req. Title | | Independence in Ensuring Safe Time To Perform Activation |
| Rationale | | To prevent a malfunction of the MMOTA feature from causing the highest level hazard in the target ECU. |

Table 53: Decomposition F-S-Req096

## Allocation of Functional Safety Requirements

*Note:* ***Error! Reference source not found.*** *illustrates the architectural elements available for requirement allocation*

### Requirements allocation

#### Preconditions and goals for allocation

*Insert a description of the preconditions and goals for allocation.*

*Not supported by MagicDraw report generation.*

#### Requirements allocation

*Insert name of elements/subsystems/components, Functional Safety Requirements, ASILs and allocate requirements to elements/subsystems/components by inserting ‘X’.*

*The authoritative source for the Functional Safety Requirements is section 2.1.1.2 of this document. The documentation of Functional Safety Requirements in this chapter (complete or summarised) is for information only.*

The requirements from section 2.5 are allocated as follows:

The requirements from section 2.5 are allocated as follows:

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **<Feature Abbreviation>-F-S-Req.ID** | **Requirement Title** | **ASIL** | **Subsystem/Component** | | | | | | | | | |
| **Cloud** | **IV-MMOTA** | **Ignition Control Module** | **Multi-Module OTA** | **OTA App** | **OTA Feature** | **OV-MMOTA** | **Other ECU SW** | **Powertrain Controls** | **Target ECU** |
| F-S-Req018 | Cloud Uses E2E | QM | X |  |  |  |  |  | X |  |  |  |
| F-S-Req019 | Powertrain Controls Ensure Start Has Been Inhibited | B(D) |  |  |  |  |  |  |  |  | X |  |
| F-S-Req020 | OTA Governance Board shall review and approve the software that is to be pushed via OTA | QM | X |  |  |  |  |  | X |  |  |  |
| F-S-Req021 | Cloud Detects Data Corruption | QM | X |  |  |  |  |  | X |  |  |  |
| F-S-Req022 | Engineer Ensures Unique SW IDs | QM |  |  |  | X |  |  | X |  |  |  |
| F-S-Req024 | Engineer Uploads Correct Software | QM |  |  |  | X |  |  | X |  |  |  |
| F-S-Req027 | OTA Feature Evaluates ACTIVATION Success | D |  | X |  |  |  | X |  |  |  |  |
| F-S-Req030 | Cloud Authenticates Software Update | QM | X |  |  |  |  |  | X |  |  |  |
| F-S-Req031 | OTA Feature Detects Data Corruption | QM |  | X |  |  |  | X |  |  |  |  |
| F-S-Req033 | OTA Feature Detects Invalid Software | QM |  | X |  |  |  | X |  |  |  |  |
| F-S-Req040 | Engineer Marks OTA and Non-OTA Software | QM |  |  |  | X |  |  | X |  |  |  |
| F-S-Req041 | OTA Feature Evaluates Roll Back Success | D |  | X |  |  |  | X |  |  |  |  |
| F-S-Req042 | OTA Feature Evaluates Safe Time to Perform Activation | B(D) |  | X |  |  |  | X |  |  |  |  |
| F-S-Req045 | OTA Feature Authenticates Cloud Connection | QM |  | X |  |  |  | X |  |  |  |  |
| F-S-Req046 | OTA Feature Communicates E2E with the Cloud | QM |  | X |  |  |  | X |  |  |  |  |
| F-S-Req047 | Cloud Sends Correct Software for the Target ECU | QM | X |  |  |  |  |  | X |  |  |  |
| F-S-Req052 | OTA Feature Informs the Cloud of Data Corruption | QM |  | X |  |  |  | X |  |  |  |  |
| F-S-Req059 | Cloud and Engineers Ensure Correct Software is Flashed | QM | X |  |  |  |  |  | X |  |  |  |
| F-S-Req071 | OTA App Detects Data Corruption During Software Download | QM |  | X |  |  | X |  |  |  |  | X |
| F-S-Req072 | OTA Feature Detects Data Corruption During Software Download | QM |  | X |  |  |  | X |  |  |  |  |
| F-S-Req074 | OTA Feature Command Inhibit Start | B(D) |  | X |  |  |  | X |  |  |  |  |
| F-S-Req075 | Ignition Control Module Inhibits Start Upon Command | B(D) |  |  | X |  |  |  |  |  |  |  |
| F-S-Req077 | OTA App Authenticates ACTIVATION Commands | QM |  | X |  |  | X |  |  |  |  | X |
| F-S-Req078 | Other ECU SW Reports ACTIVATION Readiness | QM |  | X |  |  |  |  |  | X |  | X |
| F-S-Req079 | OTA App (ASIL C/D) Verify Safe Vehicle State | B(D) |  | X |  |  | X |  |  |  |  | X |
| F-S-Req080 | OTA App Communicates E2E with the OTA Feature | QM |  | X |  |  | X |  |  |  |  | X |
| F-S-Req081 | Other ECU SW Provides Part Number | QM |  | X |  |  |  |  |  | X |  | X |
| F-S-Req082 | OTA App Prevents Active Memory Erasing or Writing | D |  | X |  |  | X |  |  |  |  | X |
| F-S-Req083 | Other ECU SW (ASIL C/D) Verify Safe Vehicle State | B(D) |  | X |  |  |  |  |  | X |  | X |
| F-S-Req084 | OTA App Informs the OTA Feature of Data Corruption | QM |  | X |  |  | X |  |  |  |  | X |
| F-S-Req085 | Other ECU SW Performs Activation Within Time Limit | QM |  | X |  |  |  |  |  | X |  | X |
| F-S-Req086 | OTA App Authenticates Erase And Programming Commands | QM |  | X |  |  | X |  |  |  |  | X |
| F-S-Req087 | OTA App Executes OTA Without Affecting Basic Function | D |  | X |  |  | X |  |  |  |  | X |
| F-S-Req088 | Other ECU SW Prevents Active Memory Erasing or Writing | D |  | X |  |  |  |  |  | X |  | X |
| F-S-Req090 | Other ECU SW Executes OTA Without Affecting Basic Function | D |  | X |  |  |  |  |  | X |  | X |
| F-S-Req091 | OTA App rejects Invalid Software | QM |  | X |  |  | X |  |  |  |  | X |
| F-S-Req092 | OTA App Sends Correct Part Number | QM |  | X |  |  | X |  |  |  |  | X |
| F-S-Req093 | OTA App Verifies Installed Software During Activation | D |  | X |  |  | X |  |  |  |  | X |
| F-S-Req094 | Other ECU SW Executes Active Memory | D |  | X |  |  |  |  |  | X |  | X |
| F-S-Req095 | OTA App Detects Communication Errors | QM |  | X |  |  | X |  |  |  |  | X |
| F-S-Req096 | OTA Feature, OTA App, and Other ECU SW (ASIL C/D) Ensures Safe Time To Perform Activation | D |  |  |  | X |  |  |  |  |  |  |
| F-S-Req097 | OTA App and Other ECU SW (ASIL C/D) Ensures Safe Time To Perform Activation | B(D) |  | X |  |  | X |  |  | X |  | X |
| F-S-Req098 | Independence in Ensuring Safe Time To Perform Activation | D |  | X |  |  |  |  |  |  |  |  |
| F-S-Req099 | OTA Feature Commands Rollback Upon Unsuccessful Activation | D |  | X |  |  |  | X |  |  |  |  |
| F-S-Req100 | OTA Feature and Ignition Control Module Communicates E2E | B(D) |  | X | X |  |  | X |  |  |  |  |
| F-S-Req101 | Ignition Control Module and Powertrain Controls Communicates E2E | B(D) |  |  | X |  |  |  |  |  |  |  |
| F-S-Req103 | Iginition Control Module Rejects Start Inhibit Request if Engine is Running | B(D) |  |  | X |  |  |  |  |  |  |  |
| **HIGHEST ASIL** | | D | QM | D | B(D) | D | D | D | QM | D | B(D) | D |

Table 54: Requirements allocation

**Error! Reference source not found.** shows the highest ASIL for each element/component/subsystem/interface graphically.

*Remark: Block diagram is optional*

# Execution and Results of Verification Review

|  |  |
| --- | --- |
| **Date of review completion** | **Responsible Person for Review** |

Table 55: Review Table

*Note: For more information on how to complete the verification review, and the key stakeholders to invite, please visit the Functional Safety Wiki page and browse the 'Verification Review Process' link: https://pd3.spt.ford.com/sites/GlobalFunctionalSafety/Functional%20Safety%20FAQ%20Wiki%20Page/Home.aspx*

## Verification Review

*Evaluate this document according to the line items and document the status of appropriate completion.The responsible persons for the verification review shall have had a ISO 26262 training and*

*be a domain expert, such as someone from the working team or technical experts on the technology.*

|  |  |  |
| --- | --- | --- |
| **Completed according to the Guidelines?** | | **Yes / No** |
| Safety Goals |  |  |
| Assumptions |  |  |
|  | If the Functional Safety Requirement refers to a user manual entry or a driver action, Relevant input for the user manual are identified and documented |  |
| Argumentation for Safety Goal achievement |  |  |
| Safe State and Requirements Overview |  |  |
| Operating Modes Overview |  |  |
| Assumptions on actions of driver or other persons to ensure Controllability according to HARA |  |  |
| Functional Safety Requirements | Contains all required attributes |  |
|  | Are simple, verifiable, necessary, achievable, and traceable |  |
|  | The Fault Tolerant Time Intervals in the Functional Safety Concept and in the Hazard Analysis and Risk Assessment are consistent.  *Note:* ***Error! Reference source not found.*** *can support the review.* |  |
|  | Fit to the existing information (e.g. electrical architecture, safety capability of ECU's, influence of parameters) |  |
|  | Can be realized (confirmation from responsible parties) |  |
|  | Can be verified |  |
| Parameter values for Functional Safety Requirements | The identified parameters for the Functional Safety Requirement are complete. |  |
| Allocation of Functional Safety Requirements |  |  |
| ASIL Decomposition (Optional) |  |  |

Table 56: Checklist for Completeness of Functional Safety concept

## Review Exceptions / Deviations / Findings

*In case of exceptions, deviation or findings, please describe the concerns.*

## Further Actions / Decisions

*Describe what the resulting actions are.*

2. Definitions, Abbreviations and Acronyms

*Insert Definitions, Abbreviations and Acronyms used in this document, maybe reference to separate list. Commonly used abbreviations (e.g., ECU) should be left out.*

|  |  |
| --- | --- |
| ACTIVATION\_TIMEOUT | The time limit for which the Target ECU must switch execution from the current active memory to the inactive memory. As of September 19th, 2017 it is 2 minutes. |
| CAN | Controller Area Network |
| E2E | (aka end-to-end protected communication path) involves using techniques like checksum, rolling counters and CRC’s to ensure communication faults like data corruption, messages coming out of sequence etc.. can be detected. |
| ECU | Electronic Control Unit (In context of E/E systems, component is usually used for an ECU) |
| Ignition Control Module | For example BCM |
| IV-MMOTA | In-Vehicle components of the Multi Module OTA system |
| MMOTA | Multi Module OTA |
| OTA | Over the Air |
| OTA App | OTA Application Software within the target ECU |
| Other ECU SW | Other ECU SW represents other internal ECU components that are separate from the OTA App. It refers to components like the ECU application software, the Bootloader, Supplier Basic Software, etc |
| OV-MMOTA | Outside Vehicle components of the Multi Module OTA system, i.e. the components needed for OTA to work that do not reside in the vehicle like the Cloud |
| Safe State | Operating mode of an item without an unreasonable level of risk Example: intended operating mode, degraded operating mode or switched-off modes |
| Software Rejected | Software Rejected means that the newly downloaded software is not activated and the Target ECU remains on its previous software. |
| System | A network of interdependent components that work together to accomplish the aim of the system.  Note: Aim of an E/E System is usually a function or feature. |
| Vehicle | The overall Vehicle System, including all functions, features, material and information provided to the end User by the vehicle manufacturer as the result of a purchase. |

Table 57: Definitions, Abbreviations and Acronyms