|  |  | |  |
| --- | --- | --- | --- |
|  |  | |  |
|  |  | |  |
|  | #findFSRVV($element)  #findFSRVV($element)  #findFSRVV($element)  #findFSRVV($element)  #findFSRVV($element)  #findFSRVV($element)  #findFSRVV($element)  #findFSRVV($element)  #findFSRVV($element)  #findFSRVV($element)  #findFSRVV($element)  #findFSRVV($element)  #findFSRVV($element)  #findFSRVV($element)  #findFSRVV($element)  #findFSRVV($element)  #findFSRVV($element)  #findFSRVV($element)  #findFSRVV($element)  #findFSRVV($element)  #findFSRVV($element)  #findFSRVV($element)  #findFSRVV($element)  #findFSRVV($element)  #findFSRVV($element)  #findFSRVV($element)  #findFSRVV($element)  #findFSRVV($element)  #findFSRVV($element)  #findFSRVV($element)  #findFSRVV($element)  #findFSRVV($element)  #findFSRVV($element)  #findFSRVV($element)  #findFSRVV($element)  #findFSRVV($element)  #findFSRVV($element)  #findFSRVV($element)  #findFSRVV($element)  #findFSRVV($element)  #findFSRVV($element)  #findFSRVV($element)  #findFSRVV($element)  #findFSRVV($element)  #findFSRVV($element)  #findFSRVV($element)  #findFSRVV($element)  #findFSRVV($element)  #findFSRVV($element)  #findFSRVV($element)  #findFSRVV($element)  #findFSRVV($element)  #findFSRVV($element)  #findFSRVV($element)  #findFSRVV($element)  #findFSRVV($element)  #findFSRVV($element)  #findFSRVV($element)  #findFSRVV($element)  #findFSRVV($element)  #findFSRVV($element)  #findFSRVV($element)  #findFSRVV($element)  #findFSRVV($element)  #findFSRVV($element)  #findFSRVV($element)  #findFSRVV($element)  #findFSRVV($element)  #findFSRVV($element)  #findFSRVV($element)  #findFSRVV($element)  #findFSRVV($element)  #findFSRVV($element) | |  |
|  |  | |  |
|  | Safety Requirements Specification | |  |
|  |  | |  |
|  | including  Technical Safety Requirements Specification  Technical Safety Concept  System Design Specification | |  |
|  |  |
|  |  |
|  |  | |  |
| Commodities | Multi-Module OTA | |  |
| Program(s) | MY21 P702 | |  |
| Document Version | SRS2 | |  |
| 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: | 6.14 |  |
|  | SysML Report Template Version: | K |  |
|  |  |  |  |

# Change Control

|  |  |  |  |
| --- | --- | --- | --- |
| **Version** | **Date** | **Author** | **Change / Remark** |
| SRS1 | 2018-08-29 | ooyesik1 | Updates baseline for UNV0 |
| SRS2 | 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 04 Safety Requirement Specification".*

*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 Functional Safety guidelines in order to get a sufficient overview about the overall Safety Process.*

*As supporting documents, a template for meeting minutes and a template for 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>

*Format-Options*

*Light gray italic formatted text parts are hints. This text can be removed in the final document.*

# Content

[1. Introduction 9](#_Toc524090123)

[1.1 Purpose 9](#_Toc524090124)

[1.2 Input documents 9](#_Toc524090125)

[1.3 Definitions, Abbreviations and Acronyms 9](#_Toc524090126)

[2. Input from System Design, Item Definition / Feature Document [FFSD 01.1(0)] and Functional Safety Concept [FFSD 03] 12](#_Toc524090127)

[2.1 Implementation Details of External Interfaces 12](#_Toc524090128)

[2.2 Constraints 12](#_Toc524090129)

[2.3 Technical Block Diagram 12](#_Toc524090130)

[2.4 Functional Overview of Elements/Components/Subsystems 13](#_Toc524090131)

[2.4.1 Elements/Components/Subsystems within System Boundary 13](#_Toc524090132)

[2.4.2 Elements/Components/Subsystems outside System Boundary 13](#_Toc524090133)

[2.5 Implementation Details of Internal Interfaces 13](#_Toc524090134)

[2.6 System Level Architecture (including redundancy) 14](#_Toc524090135)

[2.6.1 Safety Goal: SGxx (ASIL X) 14](#_Toc524090136)

[2.6.2 Safety Goal: SGxx (ASIL X) 14](#_Toc524090137)

[3. Technical Safety Requirements Specification 15](#_Toc524090138)

[3.1 Technical Safety Requirements 15](#_Toc524090139)

[3.1.1 Requirement Derivation Diagram(s) for F-S-Req111 - Cloud and OTA Supervisor Communicates Manifest Securely 15](#_Toc524090140)

[3.1.1.1 Requirement Derivation Diagram(s) (Optional) 15](#_Toc524090141)

[3.1.1.2 Technical Safety Requirements for F-S-Req111 - Cloud and OTA Supervisor Communicates Manifest Securely 15](#_Toc524090142)

[3.1.2 Requirement Derivation Diagram(s) for F-S-Req030 - Cloud Authenticates Software Update 17](#_Toc524090143)

[3.1.2.1 Requirement Derivation Diagram(s) (Optional) 17](#_Toc524090144)

[3.1.2.2 Technical Safety Requirements for F-S-Req030 - Cloud Authenticates Software Update 17](#_Toc524090145)

[3.1.3 Requirement Derivation Diagram(s) for F-S-Req021 - Cloud Detects Data Corruption 23](#_Toc524090146)

[3.1.3.1 Requirement Derivation Diagram(s) (Optional) 23](#_Toc524090147)

[3.1.3.2 Technical Safety Requirements for F-S-Req021 - Cloud Detects Data Corruption 23](#_Toc524090148)

[3.1.4 Requirement Derivation Diagram(s) for F-S-Req047 - Cloud Sends Correct Software for the Target ECU 27](#_Toc524090149)

[3.1.4.1 Requirement Derivation Diagram(s) (Optional) 27](#_Toc524090150)

[3.1.4.2 Technical Safety Requirements for F-S-Req047 - Cloud Sends Correct Software for the Target ECU 27](#_Toc524090151)

[3.1.5 Requirement Derivation Diagram(s) for F-S-Req018 - Cloud Uses E2E 29](#_Toc524090152)

[3.1.5.1 Requirement Derivation Diagram(s) (Optional) 29](#_Toc524090153)

[3.1.5.2 Technical Safety Requirements for F-S-Req018 - Cloud Uses E2E 29](#_Toc524090154)

[3.1.6 Requirement Derivation Diagram(s) for F-S-Req022 - Engineer Ensures Unique SW IDs 31](#_Toc524090155)

[3.1.6.1 Requirement Derivation Diagram(s) (Optional) 31](#_Toc524090156)

[3.1.6.2 Technical Safety Requirements for F-S-Req022 - Engineer Ensures Unique SW IDs 31](#_Toc524090157)

[3.1.7 Requirement Derivation Diagram(s) for F-S-Req040 - Engineer Marks OTA and Non-OTA Software 33](#_Toc524090158)

[3.1.7.1 Requirement Derivation Diagram(s) (Optional) 33](#_Toc524090159)

[3.1.7.2 Technical Safety Requirements for F-S-Req040 - Engineer Marks OTA and Non-OTA Software 33](#_Toc524090160)

[3.1.8 Requirement Derivation Diagram(s) for F-S-Req024 - Engineer Uploads Correct Software 37](#_Toc524090161)

[3.1.8.1 Requirement Derivation Diagram(s) (Optional) 37](#_Toc524090162)

[3.1.8.2 Technical Safety Requirements for F-S-Req024 - Engineer Uploads Correct Software 37](#_Toc524090163)

[3.1.9 Requirement Derivation Diagram(s) for F-S-Req103 - Iginition Control Module Rejects Start Inhibit Request if Engine is Running 39](#_Toc524090164)

[3.1.9.1 Requirement Derivation Diagram(s) (Optional) 39](#_Toc524090165)

[3.1.9.2 Technical Safety Requirements for F-S-Req103 - Iginition Control Module Rejects Start Inhibit Request if Engine is Running 39](#_Toc524090166)

[3.1.10 Requirement Derivation Diagram(s) for F-S-Req101 - Ignition Control Module and Powertrain Controls Communicates E2E 41](#_Toc524090167)

[3.1.10.1 Requirement Derivation Diagram(s) (Optional) 41](#_Toc524090168)

[3.1.10.2 Technical Safety Requirements for F-S-Req101 - Ignition Control Module and Powertrain Controls Communicates E2E 41](#_Toc524090169)

[3.1.11 Requirement Derivation Diagram(s) for F-S-Req075 - Ignition Control Module Inhibits Start Upon Command 43](#_Toc524090170)

[3.1.11.1 Requirement Derivation Diagram(s) (Optional) 43](#_Toc524090171)

[3.1.11.2 Technical Safety Requirements for F-S-Req075 - Ignition Control Module Inhibits Start Upon Command 43](#_Toc524090172)

[3.1.12 Requirement Derivation Diagram(s) for F-S-Req086 - OTA App Authenticates Erase And Programming Commands 47](#_Toc524090173)

[3.1.12.1 Requirement Derivation Diagram(s) (Optional) 47](#_Toc524090174)

[3.1.12.2 Technical Safety Requirements for F-S-Req086 - OTA App Authenticates Erase And Programming Commands 47](#_Toc524090175)

[3.1.13 Requirement Derivation Diagram(s) for F-S-Req095 - OTA App Detects Communication Errors 53](#_Toc524090176)

[3.1.13.1 Requirement Derivation Diagram(s) (Optional) 53](#_Toc524090177)

[3.1.13.2 Technical Safety Requirements for F-S-Req095 - OTA App Detects Communication Errors 53](#_Toc524090178)

[3.1.14 Requirement Derivation Diagram(s) for F-S-Req087 - OTA App Executes OTA Without Affecting Basic Function 57](#_Toc524090179)

[3.1.14.1 Requirement Derivation Diagram(s) (Optional) 57](#_Toc524090180)

[3.1.14.2 Technical Safety Requirements for F-S-Req087 - OTA App Executes OTA Without Affecting Basic Function 57](#_Toc524090181)

[3.1.15 Requirement Derivation Diagram(s) for F-S-Req084 - OTA App Informs the OTA Feature of Data Corruption 61](#_Toc524090182)

[3.1.15.1 Requirement Derivation Diagram(s) (Optional) 61](#_Toc524090183)

[3.1.15.2 Technical Safety Requirements for F-S-Req084 - OTA App Informs the OTA Feature of Data Corruption 61](#_Toc524090184)

[3.1.16 Requirement Derivation Diagram(s) for F-S-Req082 - OTA App Prevents Active Memory Erasing or Writing 67](#_Toc524090185)

[3.1.16.1 Requirement Derivation Diagram(s) (Optional) 67](#_Toc524090186)

[3.1.16.2 Technical Safety Requirements for F-S-Req082 - OTA App Prevents Active Memory Erasing or Writing 67](#_Toc524090187)

[3.1.17 Requirement Derivation Diagram(s) for F-S-Req091 - OTA App rejects Invalid Software 69](#_Toc524090188)

[3.1.17.1 Requirement Derivation Diagram(s) (Optional) 69](#_Toc524090189)

[3.1.17.2 Technical Safety Requirements for F-S-Req091 - OTA App rejects Invalid Software 69](#_Toc524090190)

[3.1.18 Requirement Derivation Diagram(s) for F-S-Req092 - OTA App Sends Correct Part Number 71](#_Toc524090191)

[3.1.18.1 Requirement Derivation Diagram(s) (Optional) 71](#_Toc524090192)

[3.1.18.2 Technical Safety Requirements for F-S-Req092 - OTA App Sends Correct Part Number 71](#_Toc524090193)

[3.1.19 Requirement Derivation Diagram(s) for F-S-Req093 - OTA App Verifies Installed Software During Activation 73](#_Toc524090194)

[3.1.19.1 Requirement Derivation Diagram(s) (Optional) 73](#_Toc524090195)

[3.1.19.2 Technical Safety Requirements for F-S-Req093 - OTA App Verifies Installed Software During Activation 73](#_Toc524090196)

[3.1.20 Requirement Derivation Diagram(s) for F-S-Req100 - OTA Feature and Ignition Control Module Communicates E2E 81](#_Toc524090197)

[3.1.20.1 Requirement Derivation Diagram(s) (Optional) 81](#_Toc524090198)

[3.1.20.2 Technical Safety Requirements for F-S-Req100 - OTA Feature and Ignition Control Module Communicates E2E 81](#_Toc524090199)

[3.1.21 Requirement Derivation Diagram(s) for F-S-Req045 - OTA Feature Authenticates Cloud Connection 85](#_Toc524090200)

[3.1.21.1 Requirement Derivation Diagram(s) (Optional) 85](#_Toc524090201)

[3.1.21.2 Technical Safety Requirements for F-S-Req045 - OTA Feature Authenticates Cloud Connection 85](#_Toc524090202)

[3.1.22 Requirement Derivation Diagram(s) for F-S-Req074 - OTA Feature Command Inhibit Start 87](#_Toc524090203)

[3.1.22.1 Requirement Derivation Diagram(s) (Optional) 87](#_Toc524090204)

[3.1.22.2 Technical Safety Requirements for F-S-Req074 - OTA Feature Command Inhibit Start 87](#_Toc524090205)

[3.1.23 Requirement Derivation Diagram(s) for F-S-Req099 - OTA Feature Commands Rollback Upon Unsuccessful Activation 99](#_Toc524090206)

[3.1.23.1 Requirement Derivation Diagram(s) (Optional) 99](#_Toc524090207)

[3.1.23.2 Technical Safety Requirements for F-S-Req099 - OTA Feature Commands Rollback Upon Unsuccessful Activation 99](#_Toc524090208)

[3.1.24 Requirement Derivation Diagram(s) for F-S-Req046 - OTA Feature Communicates E2E with the Cloud 101](#_Toc524090209)

[3.1.24.1 Requirement Derivation Diagram(s) (Optional) 101](#_Toc524090210)

[3.1.24.2 Technical Safety Requirements for F-S-Req046 - OTA Feature Communicates E2E with the Cloud 101](#_Toc524090211)

[3.1.25 Requirement Derivation Diagram(s) for F-S-Req031 - OTA Feature Detects Data Corruption 103](#_Toc524090212)

[3.1.25.1 Requirement Derivation Diagram(s) (Optional) 103](#_Toc524090213)

[3.1.25.2 Technical Safety Requirements for F-S-Req031 - OTA Feature Detects Data Corruption 103](#_Toc524090214)

[3.1.26 Requirement Derivation Diagram(s) for F-S-Req033 - OTA Feature Detects Invalid Software 107](#_Toc524090215)

[3.1.26.1 Requirement Derivation Diagram(s) (Optional) 107](#_Toc524090216)

[3.1.26.2 Technical Safety Requirements for F-S-Req033 - OTA Feature Detects Invalid Software 107](#_Toc524090217)

[3.1.27 Requirement Derivation Diagram(s) for F-S-Req027 - OTA Feature Evaluates ACTIVATION Success 109](#_Toc524090218)

[3.1.27.1 Requirement Derivation Diagram(s) (Optional) 109](#_Toc524090219)

[3.1.27.2 Technical Safety Requirements for F-S-Req027 - OTA Feature Evaluates ACTIVATION Success 109](#_Toc524090220)

[3.1.28 Requirement Derivation Diagram(s) for F-S-Req041 - OTA Feature Evaluates Roll Back Success 113](#_Toc524090221)

[3.1.28.1 Requirement Derivation Diagram(s) (Optional) 113](#_Toc524090222)

[3.1.28.2 Technical Safety Requirements for F-S-Req041 - OTA Feature Evaluates Roll Back Success 113](#_Toc524090223)

[3.1.29 Requirement Derivation Diagram(s) for F-S-Req052 - OTA Feature Informs the Cloud of Data Corruption 115](#_Toc524090224)

[3.1.29.1 Requirement Derivation Diagram(s) (Optional) 115](#_Toc524090225)

[3.1.29.2 Technical Safety Requirements for F-S-Req052 - OTA Feature Informs the Cloud of Data Corruption 115](#_Toc524090226)

[3.1.30 Requirement Derivation Diagram(s) for F-S-Req020 - OTA Governance Board shall review and approve the software that is to be pushed via OTA 117](#_Toc524090227)

[3.1.30.1 Requirement Derivation Diagram(s) (Optional) 117](#_Toc524090228)

[3.1.30.2 Technical Safety Requirements for F-S-Req020 - OTA Governance Board shall review and approve the software that is to be pushed via OTA 117](#_Toc524090229)

[3.1.31 Requirement Derivation Diagram(s) for F-S-Req083 - Other ECU SW (ASIL C/D) Verify Safe Vehicle State 119](#_Toc524090230)

[3.1.31.1 Requirement Derivation Diagram(s) (Optional) 119](#_Toc524090231)

[3.1.31.2 Technical Safety Requirements for F-S-Req083 - Other ECU SW (ASIL C/D) Verify Safe Vehicle State 119](#_Toc524090232)

[3.1.32 Requirement Derivation Diagram(s) for F-S-Req094 - Other ECU SW Executes Active Memory 125](#_Toc524090233)

[3.1.32.1 Requirement Derivation Diagram(s) (Optional) 125](#_Toc524090234)

[3.1.32.2 Technical Safety Requirements for F-S-Req094 - Other ECU SW Executes Active Memory 125](#_Toc524090235)

[3.1.33 Requirement Derivation Diagram(s) for F-S-Req090 - Other ECU SW Executes OTA Without Affecting Basic Function 127](#_Toc524090236)

[3.1.33.1 Requirement Derivation Diagram(s) (Optional) 127](#_Toc524090237)

[3.1.33.2 Technical Safety Requirements for F-S-Req090 - Other ECU SW Executes OTA Without Affecting Basic Function 127](#_Toc524090238)

[3.1.34 Requirement Derivation Diagram(s) for F-S-Req085 - Other ECU SW Performs Activation Within Time Limit 129](#_Toc524090239)

[3.1.34.1 Requirement Derivation Diagram(s) (Optional) 129](#_Toc524090240)

[3.1.34.2 Technical Safety Requirements for F-S-Req085 - Other ECU SW Performs Activation Within Time Limit 129](#_Toc524090241)

[3.1.35 Requirement Derivation Diagram(s) for F-S-Req088 - Other ECU SW Prevents Active Memory Erasing or Writing 133](#_Toc524090242)

[3.1.35.1 Requirement Derivation Diagram(s) (Optional) 133](#_Toc524090243)

[3.1.35.2 Technical Safety Requirements for F-S-Req088 - Other ECU SW Prevents Active Memory Erasing or Writing 133](#_Toc524090244)

[3.1.36 Requirement Derivation Diagram(s) for F-S-Req081 - Other ECU SW Provides Part Number 137](#_Toc524090245)

[3.1.36.1 Requirement Derivation Diagram(s) (Optional) 137](#_Toc524090246)

[3.1.36.2 Technical Safety Requirements for F-S-Req081 - Other ECU SW Provides Part Number 137](#_Toc524090247)

[3.1.37 Requirement Derivation Diagram(s) for F-S-Req078 - Other ECU SW Reports ACTIVATION Readiness 141](#_Toc524090248)

[3.1.37.1 Requirement Derivation Diagram(s) (Optional) 141](#_Toc524090249)

[3.1.37.2 Technical Safety Requirements for F-S-Req078 - Other ECU SW Reports ACTIVATION Readiness 141](#_Toc524090250)

[3.2 Derivation of Fault Tolerant Time 143](#_Toc524090251)

[3.3 Derivation of Reduced Functionality (interval) (optional) 144](#_Toc524090252)

[3.4 HW Metric Requirements - Derivation and Rationale 145](#_Toc524090253)

[3.4.1.1 Element/Component/Subsystem contribution to the maximum probability of safety goal violation due to random hardware failures (PMHF) 145](#_Toc524090254)

[3.4.2 Single Point Faults and Latent Faults Metric 145](#_Toc524090255)

[3.5 Allocation 145](#_Toc524090256)

[3.6 ASIL Decomposition Requirements - Derivation and Rationale (optional) 145](#_Toc524090257)

[3.6.1 Safety Related Parameters 146](#_Toc524090258)

[3.7 Requirements concerning the ability to configure a system by calibration data 146](#_Toc524090259)

[3.8 Cascading Technical Safety Requirements 147](#_Toc524090260)

[3.8.1 Element/Subsystem/Component architecture (including redundancy) 147](#_Toc524090261)

[3.8.2 Internal Fault Handling 147](#_Toc524090262)

[3.8.3 Latent Fault Handling 147](#_Toc524090263)

[3.9 Reference to description of other functions of the system 147](#_Toc524090264)

[4. System Design 148](#_Toc524090265)

[5. Requirements for Production, Operation, Service and Decommissioning 148](#_Toc524090266)

[*6.* Execution and Results of Verification Review 149](#_Toc524090267)

[6.1 Verification Review 149](#_Toc524090268)

[6.2 Review Exceptions / Deviations / Findings 151](#_Toc524090269)

[6.3 Further Actions / Decisions 151](#_Toc524090270)

# List of tables

[Table 1: Document Scope 9](#_Toc524090271)

[Table 2: Input 9](#_Toc524090272)

[Table 3: Definitions, Abbreviations and Acronyms 11](#_Toc524090273)

[Table 4: Relevant Systems (Elements/Components/Subsystems) outside System Boundary 13](#_Toc524090274)

[Table 5: System Level architecture (including redundancy) for SG01 14](#_Toc524090275)

[Table 6: ECG receive Encrypted Manifest 17](#_Toc524090276)

[Table 7: SW Binary repository 19](#_Toc524090277)

[Table 8: FENIX verify URL 21](#_Toc524090278)

[Table 9: ByteStream 23](#_Toc524090279)

[Table 10: ByteStream - At rest HASH verify 25](#_Toc524090280)

[Table 11: VADR-At rest HASH verify 27](#_Toc524090281)

[Table 12: FENIX- SW Compatibility 29](#_Toc524090282)

[Table 13: ECG -Ford Cloud - HTTPS TLS 31](#_Toc524090283)

[Table 14: SW Part numbers 33](#_Toc524090284)

[Table 15: VADR - SW OTA capable 35](#_Toc524090285)

[Table 16: FENIX - Governance Board Approval 37](#_Toc524090286)

[Table 17: Ford SW release process 39](#_Toc524090287)

[Table 18: BCM-Vehicle Inhibit - General Reject 41](#_Toc524090288)

[Table 19: BCM Sub/Rx ISPR Feedback 43](#_Toc524090289)

[Table 20: BCM-CAVC-Vehicle Inhibit 45](#_Toc524090290)

[Table 21: BCM-PATS-Vehicle De-Inhibit 47](#_Toc524090291)

[Table 22: Target ECU - Commands Signing 49](#_Toc524090292)

[Table 23: Target ECU - OTA commands - Signature failure 51](#_Toc524090293)

[Table 24: Ethernet Target ECU - TLS Channel 53](#_Toc524090294)

[Table 25: ECG-Verify logical blocks HASH 55](#_Toc524090295)

[Table 26: Target ECU verify logical blocks HASH 57](#_Toc524090296)

[Table 27: Target ECU - ABA OTA memory operation 59](#_Toc524090297)

[Table 28: Target ECU - Inactive memory operation without performance impact 61](#_Toc524090298)

[Table 29: Target ECU Errors - During update 63](#_Toc524090299)

[Table 30: ECG Error - During Own SW update 65](#_Toc524090300)

[Table 31: ECG Error - Own corruption detection 67](#_Toc524090301)

[Table 32: Target ECU & ECG Active memory protected 69](#_Toc524090302)

[Table 33: Target ECU SW signature-failure 71](#_Toc524090303)

[Table 34: Target ECU PN report 73](#_Toc524090304)

[Table 35: Target ECU verifies Integrity of own SW 75](#_Toc524090305)

[Table 36: OTA Handler Stores SWASH in Reset-Proof Memory 77](#_Toc524090306)

[Table 37: VMEM (Additional Vector Code) Receives Activation Request 79](#_Toc524090307)

[Table 38: VMEM (Additional Vector Code) Verifies Inactive Memory Before Updating UCB 81](#_Toc524090308)

[Table 39: BCM Pub/Tx AUTOSAR 1A 83](#_Toc524090309)

[Table 40: ECG Pub/Tx AUTOSAR 1A 85](#_Toc524090310)

[Table 41: ECG to Cloud Connection - Authentication 87](#_Toc524090311)

[Table 42: ECG Confirm Vehicle Inhibit Before Activation 89](#_Toc524090312)

[Table 43: ECG data handling 91](#_Toc524090313)

[Table 44: ECG-Vehicle De-Inhibit - Permanent 93](#_Toc524090314)

[Table 45: ECG-Vehicle De-Inhibit - Warning 95](#_Toc524090315)

[Table 46: ECG-Preconditions-RunStart Bus Ctrl 97](#_Toc524090316)

[Table 47: ECG Sub/Rx Vehicle Inhibit (AUTOSAR 1A) 99](#_Toc524090317)

[Table 48: ECG Rollback & PN verify 101](#_Toc524090318)

[Table 49: ECG to Cloud Connection - E2E protected 103](#_Toc524090319)

[Table 50: ECG detect data corruption of Payload 105](#_Toc524090320)

[Table 51: ECG-Manifest-Encryption 107](#_Toc524090321)

[Table 52: Target ECU - SW signing verification 109](#_Toc524090322)

[Table 53: ECG PN confirmation with Manifest 111](#_Toc524090323)

[Table 54: ECG-No Vehicle De-Inhibit - While In progress 113](#_Toc524090324)

[Table 55: ECG PN Confirmation after Rollback 115](#_Toc524090325)

[Table 56: ECG Status to Cloud 117](#_Toc524090326)

[Table 57: SW OTA delivery based on Governance Board approval 119](#_Toc524090327)

[Table 58: Target ECU verify own Safe State 121](#_Toc524090328)

[Table 59: ECU Integration Code Response to Request for OTA SWAP 123](#_Toc524090329)

[Table 60: ECU Integration Code Receives the Request for OTA SWAP 125](#_Toc524090330)

[Table 61: Target ECU Run out of Active Memory Partition 127](#_Toc524090331)

[Table 62: ECU Integration Code Executes OTA Without Affecting Basic Function 129](#_Toc524090332)

[Table 63: ECG Activation within Time limit 131](#_Toc524090333)

[Table 64: ECU Integration Code Performs Activation Within Time Limit 133](#_Toc524090334)

[Table 65: Target ECU ABA OTA memory protection 135](#_Toc524090335)

[Table 66: ECU Integration Code Prevents Active Memory Erasing or Writing 137](#_Toc524090336)

[Table 67: Target ECU PN Active SW 139](#_Toc524090337)

[Table 68: ECU Integration Code Provides Part Number 141](#_Toc524090338)

[Table 69: ECU Integration Code Reports ACTIVATION Readiness 143](#_Toc524090339)

[Table 70: Fault tolerant time interval allocation to Elements/Components/Subsystems 144](#_Toc524090340)

[Table 71: PMHF derivation 145](#_Toc524090341)

[Table 72: Single Point Fault Metric derivation 145](#_Toc524090342)

[Table 73: Latent Fault Metric derivation 145](#_Toc524090343)

[Table 74: Parameter 146](#_Toc524090344)

[Table 75: Elements/Components/Subsystems Design References 148](#_Toc524090345)

[Table 76: Review Table 149](#_Toc524090346)

[Table 77: Checklist for Completeness of Safety Requirements Specification 151](#_Toc524090347)

# Introduction

## Purpose

The purpose of this Safety Requirements Specification is to document the Technical Safety Concept, Technical Safety Requirements, Requirements for Operation, Service and Decommissioning, and the System Design Specification.

During the safety lifecycle, safety requirements are specified and detailed in a hierarchical structure.

Several levels of Safety Requirements exist:

* The Technical Safety Concept specifies the basic disposition of Functional Safety requirements on system architecture in terms of conceptual safety requirements. It cascades the top-level safety requirements down to the system, including all affected ECU's, sensors, actuators etc. The system architecture comprises elements/components/subsystems. Elements/Components/Subsystems can be hardware, software or other systems.
* Other Requirements and Design Documents (= the specification tree applied within the project is used, e.g. Functional Specifications, System Specifications, Design Prerequisites, Engineering Specifications)  
  *Note: The terms Functional Specifications, System Specifications, Design Prerequisites, Engineering Specifications are not universally used within Ford*
* The Hardware Safety Requirements refine and concretize the requirements of the technical safety concept.
* The Software Safety Requirements (see are derived from the requirements of the technical safety concept and the underlying Hardware.

This Safety Requirements Specification does not cover the following aspects:

*Insert aspects not covered within this document*

|  |  |
| --- | --- |
| Aspect not covered | Assumed to be covered in |
|  |  |

Table 1: Document Scope

## Input documents

|  |  |  |  |
| --- | --- | --- | --- |
|  | Document Name | File Name/Reference | Version |
| **FFSD** | FFSD01.1 Item Definition /  FFSD01.10 Feature Document |  |  |
| FFSD02 Hazard Analysis and Risk Assessment |  |  |
| FFSD03 Functional Safety Concept |  |  |
| **Other Input** | Project Plan |  |  |
| Functional concept |  |  |
| Preliminary architectural assumptions |  |  |
| System Design (incl. external / company / generic standards, legal, HW, SW requirements, etc.) |  |  |
| Open concerns / Action items (from multiple sources) |  | - |

Table 2: Input

## Definitions, Abbreviations and Acronyms

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

|  |  |
| --- | --- |
| Action Validation Criteria | Validation criteria for these actions |
| 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. |
| ADAS | Active Driver Assist System |
| AN1 | ASIL Note 1: The ASIL rating of the Safety goal depends on the highest ASIL rating of the ECUs within scope. From a target ECU's perspective, the ASIL rating depends on its highest level malfunction. For this document we are assuming ASIL D ECUs are within scope. |
| AN2 | ASIL Note 2: The ASIL rating of the FSR requirements depends on the target ECU within scope. The ASIL rating depends on the worst hazardous event associated with the ECU's malfunction. For this document we are assuming ASIL D ECUs are within scope. |
| AN3 | ASIL Note 3: The ASIL rating of the FSR requirements depends on the target ECU within scope. The ASIL rating depends on the worst hazardous event associated with the ECU's malfunction. For this document we are using an ASIL C ECU as an example for the Target ECU FSRs. |
| CAN | Controller Area Network |
| Component | One part of a greater System. A Component may itself be a System. Note: In context of E/E systems, component is usually used for an ECU |
| DCM | Diagnostic Communication Manager |
| DIA | Development Interface Agreement |
| DIL | Dealer Interrogator Log |
| Driver Actions or Others | Description of driver actions or other people |
| 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. |
| ECG | Enhanced Central Gateway |
| ECU | Electronic Control Unit (In context of E/E systems, component is usually used for an ECU) |
| End-to-end protected communication path | End-to-end protection 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. |
| Fault Tolerant Time Interval | Time-span in which a fault or faults can be present in a system before a hazardous event occurs |
| FFSD | Ford Functional Safety Document |
| FNOS | Ford Network Operating System |
| FOTP | Firmware Over The Air |
| FTCP | Ford Telematics Communication Protocol (Vehicle to Cloud) |
| FTTI | Fault Tolerance Time Interval |
| Functional Redundancies | Functional redundancy - fault tolerance |
| GiVIS | Global in-Vehicle Information System |
| HARA | Hazard Analysis and Risk Assessment |
| High speed | Approximately more than 52 mph (83 kph) |
| HSM | Hardware Security Module |
| Ignition Control Module | For example BCM |
| IV-MMOTA | In-Vehicle components of the Multi Module OTA system |
| IVS | In-Vehicle Software |
| IVSU | In-Vehicle Software Update |
| Low speed | Approximately 12 to 36 mph (19 to 58 kph ) |
| Medium speed | Approximately 36 mph to 52 mph (58 to 83 kph) |
| MMOTA | Multi Module OTA |
| NG SDN | Next Generation Service Delivery Network |
| ODL | Optimized DID List shall be it. |
| 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 |
| OVTP | On Vehicle Telematics Protocol (TCU to all modules) |
| PBL | Primary Boot Loader |
| PCM | Powertrain Control Module |
| Reduced Functionality | Degraded functionality from the state in which a fault occurred until the transition to a safe state is achieved as defined in the warning and degradation concept ISO 26262 uses the term "emergency operation" for the reduced functionality. |
| Reduced Functionality Interval | Specified time-span that reduced functionality is needed to support the warning and degradation concept ISO 26262 uses the term "emergency operation interval" for the reduced functionality interval. |
| RFI | Reduced Functionality Interval |
| Safe State | Operating mode of an item without an unreasonable level of risk Example: intended operating mode, degraded operating mode or switched-off modes |
| SDLC | Smart Data Link Connector |
| Software Rejected | Software Rejected means that the newly downloaded software is not activated and the Target ECU remains on its previous software. |
| SWASH | Software Hash |
| 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. |
| TCU | Telematics Control Unit |
| term | A representation of a Concept expressed in Natural Language. In the vocabulary of a Domain of Discourse a term enables common understanding of domain concepts. |
| term glossary | A term glossary is a table of agreed upon definitions for terms used in project development that may provide clarity or avoid confusion to stakeholders. |
| TLA | Three Letter Acronym |
| UCB | Unchanging Control Block |
| 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. |
| Very Low Speed | Approximately 0 to 12 mph (0 to 19 kph) |

Table 3: Definitions, Abbreviations and Acronyms

# Input from System Design, Item Definition / Feature Document [FFSD 01.1(0)] and Functional Safety Concept [FFSD 03]

## Implementation Details of External Interfaces

*Describe the external Interfaces, such as communication and user interfaces. Insert references to external documents if possible.*

External Interfaces not specified.

## Constraints

*Provide constraints, e.g. environmental conditions or functional constraints*

No Constraints Specified

## Technical Block Diagram

*Insert figure here or add a reference to an existing figure.*

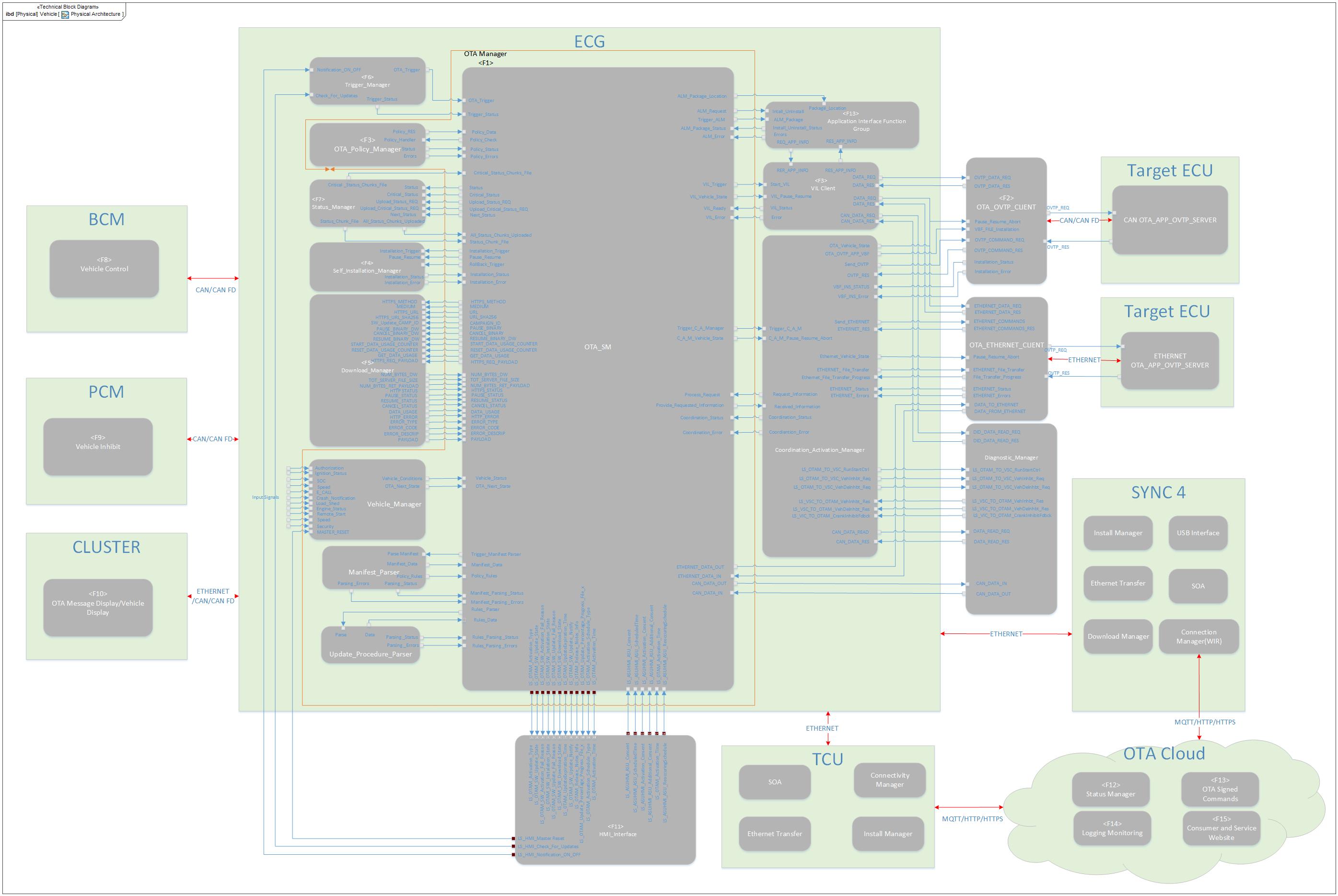


Figure 1 - Technical Block Diagram

*Physical Architecture*

*Insert description here or add a reference to an existing description.*

## Functional Overview of Elements/Components/Subsystems

### Elements/Components/**Subsystems within System Boundary**

*Insert all Elements/Components/Subsystems within System Boundary and a description.*

No Elements/Components/Subsystems within the System Boundary specified.

*Insert reference to specifications with details.*

Details are described in Specifications XXXX.

*Not supported by MagicDraw report generation.*

### Elements/Components/Subsystems outside System Boundary

*Insert all Elements/Components/Subsystems outside System Boundary and a description.*

| Element/Component/Subsystem | Description / Tasks |
| --- | --- |
| Actuator A |  |
| ECU A |  |
| ECU B |  |
| ECU C |  |
| Feature A Physical |  |
| Feature software A |  |
| physical1 |  |
| physical2 |  |
| Sensor A |  |
| Sensor B |  |
| Sensor C |  |
| Software A |  |
| Software B |  |
| Software C |  |
| System C HW1 |  |
| Vehicle |  |
| Vehicle (Physical) |  |

Table 4: Relevant Systems (Elements/Components/Subsystems) outside System Boundary

## Implementation Details of Internal Interfaces

*Insert all description of the implementation details of internal interfaces or appropriate references.*

|  |  |  |
| --- | --- | --- |
| **#** | **Signal** | **Purpose** |
| 1 | OtaActv\_D\_Stat | Inform ECUs of what OTA activity (if any) is taking place to allow for any special security needs, or functional behavior (e.g., prepare for an entry to bootloader). |
| 2 | VehOnCtl\_D\_Stat | BCM broadcasts commanded state of the Run/Start bus so ECG can verify it is being requested on.  Note: BCM sometimes needs to latch R/S for periods of time (e.g., force off for 5 seconds) |
| 3 | VehOn\_D\_RqCld | Request Run/Start bus off/on for OTA when needed.  Uses NULL when OTA does not desire R/S control |
| 4 | VehStrtInhbt\_D\_Stat | Allow ECG to know that BCM is confirming vehicle is currently inhibited due to cloud initiated (e.g., NOT if inhibited due to ESCL, ISPR off, etc.) |
| 5 | PtIgnSwtch\_D\_Stat | Allow BCM to know that PCM does not have ISPR powered and can therefore due Inhibitt |
| 6 | VehOnSrc\_D\_Stat & VehOnSrc2\_D\_Stat | Allow ECUs on the vehicle to recognize who is in control of the Run/Start bus (note it does not mean R/S is on if someone is in control) |
| 7 | CrnkInhbt\_B\_Stat | Request Inhibit from BCM to ECG (leveraging existing ESCL inhibit) |
| 8 | CloudVehCtlData\_Tp\_Rq | Cloud signed event based TP request from ECG -> BCM to securely request vehicle inhibit |
| 9 | CloudVehCtlData\_Tp\_Res | BCM -> ECG response to ack or nack the cloud signed event based TP request |
| 10 | VehStrtInhbt\_D\_Dsply (EP 1000ms) | State encoded value set different OTA messages |
| 11 | VehStrtInhbt\_T\_Dsply (EP 1000ms) | Current remaining length of time vehicle may be inhibited for display to driver |

## System Level Architecture (including redundancy)

*Insert System Level architecture (including redundancy) for all Safety Goals.*

### Safety Goal: SGxx (ASIL X)

| **Affected Elements/Components/**  **Subsystems** | **HW Architecture,**  **including redundancy on system level** | **If redundancy is used:** | | | |
| --- | --- | --- | --- | --- | --- |
| **Rational for redundancy used is suitable** | **Type of redundancy** | **Diverse or homogeneous redundancy** | **Measures for handling potential dependent failures** |
|  |  |  |  |  |  |

Table 5: System Level architecture (including redundancy) for SG01

### Safety Goal: SGxx (ASIL X)

…

# Technical Safety Requirements Specification

## Technical Safety Requirements

### Requirement Derivation Diagram(s) for F-S-Req111 - Cloud and OTA Supervisor Communicates Manifest Securely

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

*Derive Technical Safety Requirements from Functional Safety Requirements.*

*Insert ‘Requirements Derivation Diagram/Tree’ or GSN here. Several diagrams may be required depending upon the size of the Item.*

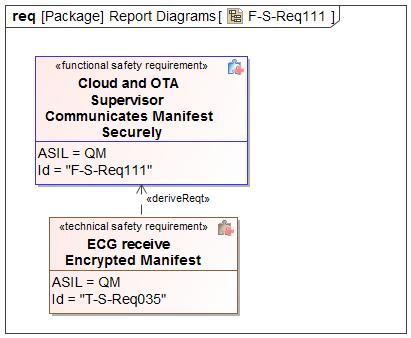


Figure 2 - Technical Safety Requirements Derivation Diagram for F-S-Req111

#### Technical Safety Requirements for F-S-Req111 - Cloud and OTA Supervisor Communicates Manifest Securely

*Describe Technical Safety Requirements from Functional Safety Requirements using Table 6 for each Technical Safety Requirement.*

| T-S-Req-ID: | T-S-Req035 - ECG receive Encrypted Manifest |
| --- | --- |
| External Reference *(optional)* |  |
| Category: | Safety Related Function |
| Safety Goal: | SG02 - Prevents Flashing of Incorrect SW |
| F-S-Req Ref.: | F-S-Req111 - Cloud and OTA Supervisor Communicates Manifest Securely |
| ASIL Classification:  *(in case of category “General”: if applicable, in case of category “Non-E/E Requirement”: not applicable)* | QM |
| Technical Safety Requirement Title: | ECG receive Encrypted Manifest |
| Technical Safety Requirement Text: | ECG shall download an encrypted Manifest (thru SYNCP) from the cloud to ensure that the URL used for downloading files has not been compromised |
| Rationale: |  |
| Safe State:  *(in case of categories “General”, “Metric”, “Non-E/E Requirement”, or “User Information”: if applicable)* | Normal |
| Reduced Functionality and Interval:  *(if applicable;*  *in case of categories “Metric”, “Non-E/E Requirement”, “Maintain Safe State / Recovery” or “User Information”: not applicable;*  *in case of category “Reduced Functionality”: required)* |  |
| Fault tolerant time interval:  *(in case of categories “Metric” or “Maintain Safe State / Recovery”: not applicable;*  *in case of category “General”, “Reduced Functionality”, “Non-E/E Requirement”, or “User Information”: if applicable)* |  |
| Requirement Status |  |
| V&V method: | System test |
| V&V acceptance criteria:  *(UNV1 / UPV1, not in case of category “Non-E/E requirement)* |  |
| Allocated Element(s)/Component(s)/ Subsystem(s) *(if applicable)* |  |

Table 6: ECG receive Encrypted Manifest

### Requirement Derivation Diagram(s) for F-S-Req030 - Cloud Authenticates Software Update

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

*Derive Technical Safety Requirements from Functional Safety Requirements.*

*Insert ‘Requirements Derivation Diagram/Tree’ or GSN here. Several diagrams may be required depending upon the size of the Item.*

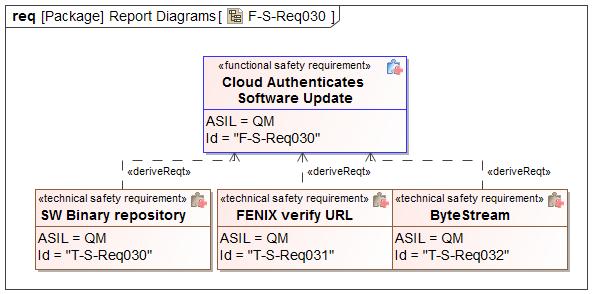


Figure 3 - Technical Safety Requirements Derivation Diagram for F-S-Req030

#### Technical Safety Requirements for F-S-Req030 - Cloud Authenticates Software Update

*Describe Technical Safety Requirements from Functional Safety Requirements using Table 6 for each Technical Safety Requirement.*

| T-S-Req-ID: | T-S-Req030 - SW Binary repository |
| --- | --- |
| External Reference *(optional)* |  |
| Category: | Safety Related Function |
| Safety Goal: | SG01 - Prevents Corruption of Existing Software  SG02 - Prevents Flashing of Incorrect SW |
| F-S-Req Ref.: | F-S-Req030 - Cloud Authenticates Software Update |
| ASIL Classification:  *(in case of category “General”: if applicable, in case of category “Non-E/E Requirement”: not applicable)* | QM |
| Technical Safety Requirement Title: | SW Binary repository |
| Technical Safety Requirement Text: | VADR shall verify that the software ingested is from a secure Ford System and the correct security tokens have been exchanged. |
| Rationale: |  |
| Safe State:  *(in case of categories “General”, “Metric”, “Non-E/E Requirement”, or “User Information”: if applicable)* | Module Safe State |
| Reduced Functionality and Interval:  *(if applicable;*  *in case of categories “Metric”, “Non-E/E Requirement”, “Maintain Safe State / Recovery” or “User Information”: not applicable;*  *in case of category “Reduced Functionality”: required)* |  |
| Fault tolerant time interval:  *(in case of categories “Metric” or “Maintain Safe State / Recovery”: not applicable;*  *in case of category “General”, “Reduced Functionality”, “Non-E/E Requirement”, or “User Information”: if applicable)* |  |
| Requirement Status |  |
| V&V method: | System test |
| V&V acceptance criteria:  *(UNV1 / UPV1, not in case of category “Non-E/E requirement)* |  |
| Allocated Element(s)/Component(s)/ Subsystem(s) *(if applicable)* |  |

Table 7: SW Binary repository

| T-S-Req-ID: | T-S-Req031 - FENIX verify URL |
| --- | --- |
| External Reference *(optional)* |  |
| Category: | Safety Related Function |
| Safety Goal: | SG01 - Prevents Corruption of Existing Software  SG02 - Prevents Flashing of Incorrect SW |
| F-S-Req Ref.: | F-S-Req030 - Cloud Authenticates Software Update |
| ASIL Classification:  *(in case of category “General”: if applicable, in case of category “Non-E/E Requirement”: not applicable)* | QM |
| Technical Safety Requirement Title: | FENIX verify URL |
| Technical Safety Requirement Text: | FENIX shall verify that the software URL provided in the Manifest is from a secured and approved Ford System and the appropriate security tokens have been exchanged |
| Rationale: |  |
| Safe State:  *(in case of categories “General”, “Metric”, “Non-E/E Requirement”, or “User Information”: if applicable)* | Normal |
| Reduced Functionality and Interval:  *(if applicable;*  *in case of categories “Metric”, “Non-E/E Requirement”, “Maintain Safe State / Recovery” or “User Information”: not applicable;*  *in case of category “Reduced Functionality”: required)* |  |
| Fault tolerant time interval:  *(in case of categories “Metric” or “Maintain Safe State / Recovery”: not applicable;*  *in case of category “General”, “Reduced Functionality”, “Non-E/E Requirement”, or “User Information”: if applicable)* |  |
| Requirement Status |  |
| V&V method: | System test |
| V&V acceptance criteria:  *(UNV1 / UPV1, not in case of category “Non-E/E requirement)* |  |
| Allocated Element(s)/Component(s)/ Subsystem(s) *(if applicable)* |  |

Table 8: FENIX verify URL

| T-S-Req-ID: | T-S-Req032 - ByteStream |
| --- | --- |
| External Reference *(optional)* |  |
| Category: | Safety Related Function |
| Safety Goal: | SG01 - Prevents Corruption of Existing Software  SG02 - Prevents Flashing of Incorrect SW |
| F-S-Req Ref.: | F-S-Req030 - Cloud Authenticates Software Update |
| ASIL Classification:  *(in case of category “General”: if applicable, in case of category “Non-E/E Requirement”: not applicable)* | QM |
| Technical Safety Requirement Title: | ByteStream |
| Technical Safety Requirement Text: | ByteStream shall verify that SW files at rest are not corrupted by verifying the HASH |
| Rationale: |  |
| Safe State:  *(in case of categories “General”, “Metric”, “Non-E/E Requirement”, or “User Information”: if applicable)* | Module Safe State |
| Reduced Functionality and Interval:  *(if applicable;*  *in case of categories “Metric”, “Non-E/E Requirement”, “Maintain Safe State / Recovery” or “User Information”: not applicable;*  *in case of category “Reduced Functionality”: required)* |  |
| Fault tolerant time interval:  *(in case of categories “Metric” or “Maintain Safe State / Recovery”: not applicable;*  *in case of category “General”, “Reduced Functionality”, “Non-E/E Requirement”, or “User Information”: if applicable)* |  |
| Requirement Status |  |
| V&V method: | System test |
| V&V acceptance criteria:  *(UNV1 / UPV1, not in case of category “Non-E/E requirement)* |  |
| Allocated Element(s)/Component(s)/ Subsystem(s) *(if applicable)* |  |

Table 9: ByteStream

### Requirement Derivation Diagram(s) for F-S-Req021 - Cloud Detects Data Corruption

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

*Derive Technical Safety Requirements from Functional Safety Requirements.*

*Insert ‘Requirements Derivation Diagram/Tree’ or GSN here. Several diagrams may be required depending upon the size of the Item.*

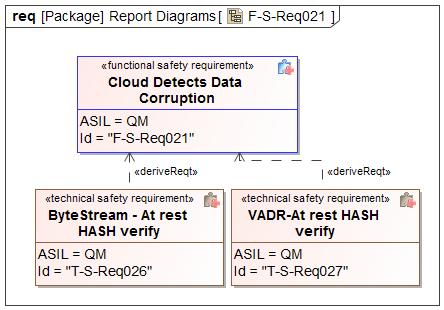


Figure 4 - Technical Safety Requirements Derivation Diagram for F-S-Req021

#### Technical Safety Requirements for F-S-Req021 - Cloud Detects Data Corruption

*Describe Technical Safety Requirements from Functional Safety Requirements using Table 6 for each Technical Safety Requirement.*

| T-S-Req-ID: | T-S-Req026 - ByteStream - At rest HASH verify |
| --- | --- |
| External Reference *(optional)* |  |
| Category: | Safety Related Function |
| Safety Goal: | SG02 - Prevents Flashing of Incorrect SW |
| F-S-Req Ref.: | F-S-Req021 - Cloud Detects Data Corruption |
| ASIL Classification:  *(in case of category “General”: if applicable, in case of category “Non-E/E Requirement”: not applicable)* | QM |
| Technical Safety Requirement Title: | ByteStream - At rest HASH verify |
| Technical Safety Requirement Text: | ByteStream shall verify that SW files at rest are not corrupted by verifying the HASH |
| Rationale: |  |
| Safe State:  *(in case of categories “General”, “Metric”, “Non-E/E Requirement”, or “User Information”: if applicable)* | Module Safe State |
| Reduced Functionality and Interval:  *(if applicable;*  *in case of categories “Metric”, “Non-E/E Requirement”, “Maintain Safe State / Recovery” or “User Information”: not applicable;*  *in case of category “Reduced Functionality”: required)* |  |
| Fault tolerant time interval:  *(in case of categories “Metric” or “Maintain Safe State / Recovery”: not applicable;*  *in case of category “General”, “Reduced Functionality”, “Non-E/E Requirement”, or “User Information”: if applicable)* |  |
| Requirement Status |  |
| V&V method: | System test |
| V&V acceptance criteria:  *(UNV1 / UPV1, not in case of category “Non-E/E requirement)* |  |
| Allocated Element(s)/Component(s)/ Subsystem(s) *(if applicable)* |  |

Table 10: ByteStream - At rest HASH verify

| T-S-Req-ID: | T-S-Req027 - VADR-At rest HASH verify |
| --- | --- |
| External Reference *(optional)* |  |
| Category: | Safety Related Function |
| Safety Goal: | SG02 - Prevents Flashing of Incorrect SW |
| F-S-Req Ref.: | F-S-Req021 - Cloud Detects Data Corruption |
| ASIL Classification:  *(in case of category “General”: if applicable, in case of category “Non-E/E Requirement”: not applicable)* | QM |
| Technical Safety Requirement Title: | VADR-At rest HASH verify |
| Technical Safety Requirement Text: | VADR shall verify that released software is not corrupted by verifying the HASH |
| Rationale: |  |
| Safe State:  *(in case of categories “General”, “Metric”, “Non-E/E Requirement”, or “User Information”: if applicable)* | Module Safe State |
| Reduced Functionality and Interval:  *(if applicable;*  *in case of categories “Metric”, “Non-E/E Requirement”, “Maintain Safe State / Recovery” or “User Information”: not applicable;*  *in case of category “Reduced Functionality”: required)* |  |
| Fault tolerant time interval:  *(in case of categories “Metric” or “Maintain Safe State / Recovery”: not applicable;*  *in case of category “General”, “Reduced Functionality”, “Non-E/E Requirement”, or “User Information”: if applicable)* |  |
| Requirement Status |  |
| V&V method: | System test |
| V&V acceptance criteria:  *(UNV1 / UPV1, not in case of category “Non-E/E requirement)* |  |
| Allocated Element(s)/Component(s)/ Subsystem(s) *(if applicable)* |  |

Table 11: VADR-At rest HASH verify

### Requirement Derivation Diagram(s) for F-S-Req047 - Cloud Sends Correct Software for the Target ECU

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

*Derive Technical Safety Requirements from Functional Safety Requirements.*

*Insert ‘Requirements Derivation Diagram/Tree’ or GSN here. Several diagrams may be required depending upon the size of the Item.*

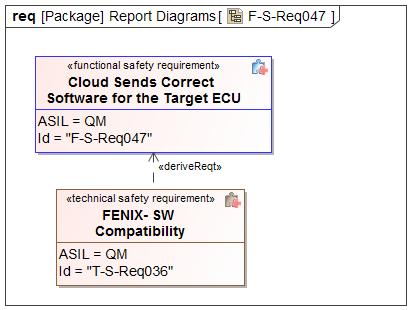


Figure 5 - Technical Safety Requirements Derivation Diagram for F-S-Req047

#### Technical Safety Requirements for F-S-Req047 - Cloud Sends Correct Software for the Target ECU

*Describe Technical Safety Requirements from Functional Safety Requirements using Table 6 for each Technical Safety Requirement.*

| T-S-Req-ID: | T-S-Req036 - FENIX- SW Compatibility |
| --- | --- |
| External Reference *(optional)* |  |
| Category: | Safety Related Function |
| Safety Goal: | SG02 - Prevents Flashing of Incorrect SW |
| F-S-Req Ref.: | F-S-Req047 - Cloud Sends Correct Software for the Target ECU |
| ASIL Classification:  *(in case of category “General”: if applicable, in case of category “Non-E/E Requirement”: not applicable)* | QM |
| Technical Safety Requirement Title: | FENIX- SW Compatibility |
| Technical Safety Requirement Text: | FENIX shall verify that the software provided in the manifest is compatible with the software version that the ECU has reported via the interrogator file |
| Rationale: |  |
| Safe State:  *(in case of categories “General”, “Metric”, “Non-E/E Requirement”, or “User Information”: if applicable)* | Normal |
| Reduced Functionality and Interval:  *(if applicable;*  *in case of categories “Metric”, “Non-E/E Requirement”, “Maintain Safe State / Recovery” or “User Information”: not applicable;*  *in case of category “Reduced Functionality”: required)* |  |
| Fault tolerant time interval:  *(in case of categories “Metric” or “Maintain Safe State / Recovery”: not applicable;*  *in case of category “General”, “Reduced Functionality”, “Non-E/E Requirement”, or “User Information”: if applicable)* |  |
| Requirement Status |  |
| V&V method: | System test |
| V&V acceptance criteria:  *(UNV1 / UPV1, not in case of category “Non-E/E requirement)* |  |
| Allocated Element(s)/Component(s)/ Subsystem(s) *(if applicable)* |  |

Table 12: FENIX- SW Compatibility

### Requirement Derivation Diagram(s) for F-S-Req018 - Cloud Uses E2E

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

*Derive Technical Safety Requirements from Functional Safety Requirements.*

*Insert ‘Requirements Derivation Diagram/Tree’ or GSN here. Several diagrams may be required depending upon the size of the Item.*

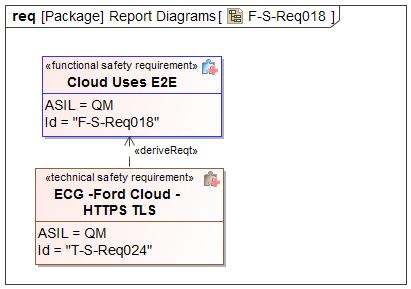


Figure 6 - Technical Safety Requirements Derivation Diagram for F-S-Req018

#### Technical Safety Requirements for F-S-Req018 - Cloud Uses E2E

*Describe Technical Safety Requirements from Functional Safety Requirements using Table 6 for each Technical Safety Requirement.*

| T-S-Req-ID: | T-S-Req024 - ECG -Ford Cloud - HTTPS TLS |
| --- | --- |
| External Reference *(optional)* |  |
| Category: | Safety Related Function |
| Safety Goal: | SG02 - Prevents Flashing of Incorrect SW |
| F-S-Req Ref.: | F-S-Req018 - Cloud Uses E2E |
| ASIL Classification:  *(in case of category “General”: if applicable, in case of category “Non-E/E Requirement”: not applicable)* | QM |
| Technical Safety Requirement Title: | ECG -Ford Cloud - HTTPS TLS |
| Technical Safety Requirement Text: | Ford Cloud to ECG shall be across TLS channel using HTTPs and SYNCP encryption |
| Rationale: |  |
| Safe State:  *(in case of categories “General”, “Metric”, “Non-E/E Requirement”, or “User Information”: if applicable)* | Normal |
| Reduced Functionality and Interval:  *(if applicable;*  *in case of categories “Metric”, “Non-E/E Requirement”, “Maintain Safe State / Recovery” or “User Information”: not applicable;*  *in case of category “Reduced Functionality”: required)* |  |
| Fault tolerant time interval:  *(in case of categories “Metric” or “Maintain Safe State / Recovery”: not applicable;*  *in case of category “General”, “Reduced Functionality”, “Non-E/E Requirement”, or “User Information”: if applicable)* |  |
| Requirement Status |  |
| V&V method: | System test |
| V&V acceptance criteria:  *(UNV1 / UPV1, not in case of category “Non-E/E requirement)* |  |
| Allocated Element(s)/Component(s)/ Subsystem(s) *(if applicable)* |  |

Table 13: ECG -Ford Cloud - HTTPS TLS

### Requirement Derivation Diagram(s) for F-S-Req022 - Engineer Ensures Unique SW IDs

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

*Derive Technical Safety Requirements from Functional Safety Requirements.*

*Insert ‘Requirements Derivation Diagram/Tree’ or GSN here. Several diagrams may be required depending upon the size of the Item.*

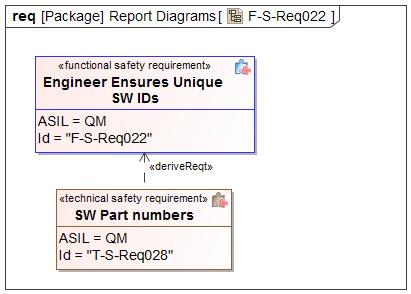


Figure 7 - Technical Safety Requirements Derivation Diagram for F-S-Req022

#### Technical Safety Requirements for F-S-Req022 - Engineer Ensures Unique SW IDs

*Describe Technical Safety Requirements from Functional Safety Requirements using Table 6 for each Technical Safety Requirement.*

| T-S-Req-ID: | T-S-Req028 - SW Part numbers |
| --- | --- |
| External Reference *(optional)* |  |
| Category: | Safety Related Function |
| Safety Goal: | SG02 - Prevents Flashing of Incorrect SW |
| F-S-Req Ref.: | F-S-Req022 - Engineer Ensures Unique SW IDs |
| ASIL Classification:  *(in case of category “General”: if applicable, in case of category “Non-E/E Requirement”: not applicable)* | QM |
| Technical Safety Requirement Title: | SW Part numbers |
| Technical Safety Requirement Text: | Released software shall follow the Ford FAP03-145 for Part numbers |
| Rationale: |  |
| Safe State:  *(in case of categories “General”, “Metric”, “Non-E/E Requirement”, or “User Information”: if applicable)* | Module Safe State |
| Reduced Functionality and Interval:  *(if applicable;*  *in case of categories “Metric”, “Non-E/E Requirement”, “Maintain Safe State / Recovery” or “User Information”: not applicable;*  *in case of category “Reduced Functionality”: required)* |  |
| Fault tolerant time interval:  *(in case of categories “Metric” or “Maintain Safe State / Recovery”: not applicable;*  *in case of category “General”, “Reduced Functionality”, “Non-E/E Requirement”, or “User Information”: if applicable)* |  |
| Requirement Status |  |
| V&V method: | System test |
| V&V acceptance criteria:  *(UNV1 / UPV1, not in case of category “Non-E/E requirement)* |  |
| Allocated Element(s)/Component(s)/ Subsystem(s) *(if applicable)* |  |

Table 14: SW Part numbers

### Requirement Derivation Diagram(s) for F-S-Req040 - Engineer Marks OTA and Non-OTA Software

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

*Derive Technical Safety Requirements from Functional Safety Requirements.*

*Insert ‘Requirements Derivation Diagram/Tree’ or GSN here. Several diagrams may be required depending upon the size of the Item.*

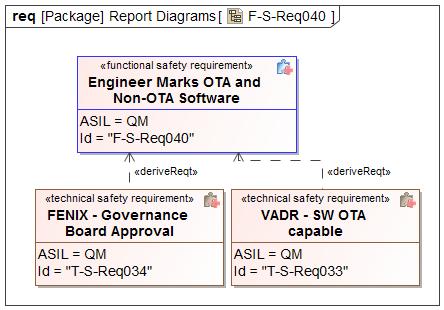


Figure 8 - Technical Safety Requirements Derivation Diagram for F-S-Req040

#### Technical Safety Requirements for F-S-Req040 - Engineer Marks OTA and Non-OTA Software

*Describe Technical Safety Requirements from Functional Safety Requirements using Table 6 for each Technical Safety Requirement.*

| T-S-Req-ID: | T-S-Req033 - VADR - SW OTA capable |
| --- | --- |
| External Reference *(optional)* |  |
| Category: | Safety Related Function |
| Safety Goal: | SG02 - Prevents Flashing of Incorrect SW |
| F-S-Req Ref.: | F-S-Req040 - Engineer Marks OTA and Non-OTA Software |
| ASIL Classification:  *(in case of category “General”: if applicable, in case of category “Non-E/E Requirement”: not applicable)* | QM |
| Technical Safety Requirement Title: | VADR - SW OTA capable |
| Technical Safety Requirement Text: | The software released in VADR shall be flagged that it is OTA Capable |
| Rationale: |  |
| Safe State:  *(in case of categories “General”, “Metric”, “Non-E/E Requirement”, or “User Information”: if applicable)* | Module Safe State |
| Reduced Functionality and Interval:  *(if applicable;*  *in case of categories “Metric”, “Non-E/E Requirement”, “Maintain Safe State / Recovery” or “User Information”: not applicable;*  *in case of category “Reduced Functionality”: required)* |  |
| Fault tolerant time interval:  *(in case of categories “Metric” or “Maintain Safe State / Recovery”: not applicable;*  *in case of category “General”, “Reduced Functionality”, “Non-E/E Requirement”, or “User Information”: if applicable)* |  |
| Requirement Status |  |
| V&V method: | System test |
| V&V acceptance criteria:  *(UNV1 / UPV1, not in case of category “Non-E/E requirement)* |  |
| Allocated Element(s)/Component(s)/ Subsystem(s) *(if applicable)* |  |

Table 15: VADR - SW OTA capable

| T-S-Req-ID: | T-S-Req034 - FENIX - Governance Board Approval |
| --- | --- |
| External Reference *(optional)* |  |
| Category: | Safety Related Function |
| Safety Goal: | SG02 - Prevents Flashing of Incorrect SW |
| F-S-Req Ref.: | F-S-Req040 - Engineer Marks OTA and Non-OTA Software |
| ASIL Classification:  *(in case of category “General”: if applicable, in case of category “Non-E/E Requirement”: not applicable)* | QM |
| Technical Safety Requirement Title: | FENIX - Governance Board Approval |
| Technical Safety Requirement Text: | FENIX shall have a specific OTA campaign that must be verifeid by the OTA Governance Board |
| Rationale: |  |
| Safe State:  *(in case of categories “General”, “Metric”, “Non-E/E Requirement”, or “User Information”: if applicable)* | Normal |
| Reduced Functionality and Interval:  *(if applicable;*  *in case of categories “Metric”, “Non-E/E Requirement”, “Maintain Safe State / Recovery” or “User Information”: not applicable;*  *in case of category “Reduced Functionality”: required)* |  |
| Fault tolerant time interval:  *(in case of categories “Metric” or “Maintain Safe State / Recovery”: not applicable;*  *in case of category “General”, “Reduced Functionality”, “Non-E/E Requirement”, or “User Information”: if applicable)* |  |
| Requirement Status |  |
| V&V method: | System test |
| V&V acceptance criteria:  *(UNV1 / UPV1, not in case of category “Non-E/E requirement)* |  |
| Allocated Element(s)/Component(s)/ Subsystem(s) *(if applicable)* |  |

Table 16: FENIX - Governance Board Approval

### Requirement Derivation Diagram(s) for F-S-Req024 - Engineer Uploads Correct Software

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

*Derive Technical Safety Requirements from Functional Safety Requirements.*

*Insert ‘Requirements Derivation Diagram/Tree’ or GSN here. Several diagrams may be required depending upon the size of the Item.*

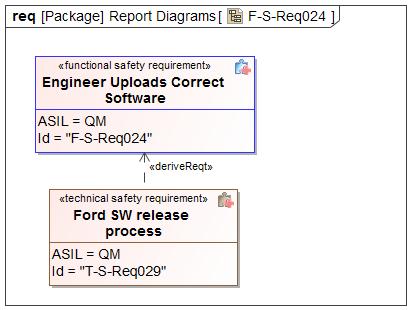


Figure 9 - Technical Safety Requirements Derivation Diagram for F-S-Req024

#### Technical Safety Requirements for F-S-Req024 - Engineer Uploads Correct Software

*Describe Technical Safety Requirements from Functional Safety Requirements using Table 6 for each Technical Safety Requirement.*

| T-S-Req-ID: | T-S-Req029 - Ford SW release process |
| --- | --- |
| External Reference *(optional)* |  |
| Category: | Safety Related Function |
| Safety Goal: | SG02 - Prevents Flashing of Incorrect SW |
| F-S-Req Ref.: | F-S-Req024 - Engineer Uploads Correct Software |
| ASIL Classification:  *(in case of category “General”: if applicable, in case of category “Non-E/E Requirement”: not applicable)* | QM |
| Technical Safety Requirement Title: | Ford SW release process |
| Technical Safety Requirement Text: | Software shall be verified and follow the Ford SW Release Process |
| Rationale: |  |
| Safe State:  *(in case of categories “General”, “Metric”, “Non-E/E Requirement”, or “User Information”: if applicable)* | Normal |
| Reduced Functionality and Interval:  *(if applicable;*  *in case of categories “Metric”, “Non-E/E Requirement”, “Maintain Safe State / Recovery” or “User Information”: not applicable;*  *in case of category “Reduced Functionality”: required)* |  |
| Fault tolerant time interval:  *(in case of categories “Metric” or “Maintain Safe State / Recovery”: not applicable;*  *in case of category “General”, “Reduced Functionality”, “Non-E/E Requirement”, or “User Information”: if applicable)* |  |
| Requirement Status |  |
| V&V method: | System test |
| V&V acceptance criteria:  *(UNV1 / UPV1, not in case of category “Non-E/E requirement)* |  |
| Allocated Element(s)/Component(s)/ Subsystem(s) *(if applicable)* |  |

Table 17: Ford SW release process

### Requirement Derivation Diagram(s) for F-S-Req103 - Iginition Control Module Rejects Start Inhibit Request if Engine is Running

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

*Derive Technical Safety Requirements from Functional Safety Requirements.*

*Insert ‘Requirements Derivation Diagram/Tree’ or GSN here. Several diagrams may be required depending upon the size of the Item.*

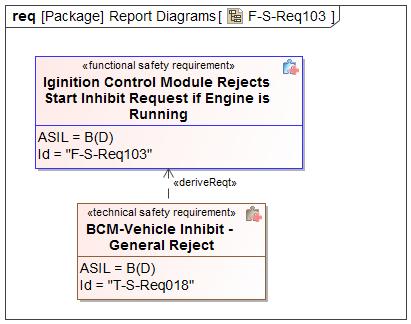


Figure 10 - Technical Safety Requirements Derivation Diagram for F-S-Req103

#### Technical Safety Requirements for F-S-Req103 - Iginition Control Module Rejects Start Inhibit Request if Engine is Running

*Describe Technical Safety Requirements from Functional Safety Requirements using Table 6 for each Technical Safety Requirement.*

| T-S-Req-ID: | T-S-Req018 - BCM-Vehicle Inhibit - General Reject |
| --- | --- |
| External Reference *(optional)* |  |
| Category: | Safety Related Function |
| Safety Goal: | SG03 - Ensure Safe Activation |
| F-S-Req Ref.: | F-S-Req103 - Iginition Control Module Rejects Start Inhibit Request if Engine is Running |
| ASIL Classification:  *(in case of category “General”: if applicable, in case of category “Non-E/E Requirement”: not applicable)* | B(D) |
| Technical Safety Requirement Title: | BCM-Vehicle Inhibit - General Reject |
| Technical Safety Requirement Text: | Although all validation check passed,  IF VSCM (BCM) any internal exception detected  OR  VSCM (BCM) transitioned run/start bus control from OTA to be in control of the customer, VSCM (BCM) shall send Negative response. |
| Rationale: |  |
| Safe State:  *(in case of categories “General”, “Metric”, “Non-E/E Requirement”, or “User Information”: if applicable)* | Module Safe State |
| Reduced Functionality and Interval:  *(if applicable;*  *in case of categories “Metric”, “Non-E/E Requirement”, “Maintain Safe State / Recovery” or “User Information”: not applicable;*  *in case of category “Reduced Functionality”: required)* |  |
| Fault tolerant time interval:  *(in case of categories “Metric” or “Maintain Safe State / Recovery”: not applicable;*  *in case of category “General”, “Reduced Functionality”, “Non-E/E Requirement”, or “User Information”: if applicable)* |  |
| Requirement Status |  |
| V&V method: | System test |
| V&V acceptance criteria:  *(UNV1 / UPV1, not in case of category “Non-E/E requirement)* |  |
| Allocated Element(s)/Component(s)/ Subsystem(s) *(if applicable)* |  |

Table 18: BCM-Vehicle Inhibit - General Reject

### Requirement Derivation Diagram(s) for F-S-Req101 - Ignition Control Module and Powertrain Controls Communicates E2E

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

*Derive Technical Safety Requirements from Functional Safety Requirements.*

*Insert ‘Requirements Derivation Diagram/Tree’ or GSN here. Several diagrams may be required depending upon the size of the Item.*

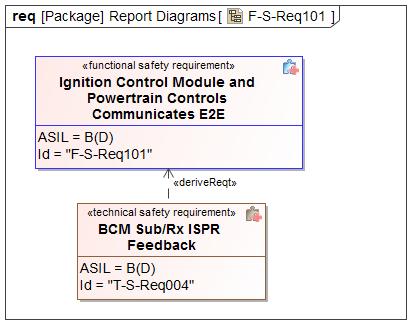


Figure 11 - Technical Safety Requirements Derivation Diagram for F-S-Req101

#### Technical Safety Requirements for F-S-Req101 - Ignition Control Module and Powertrain Controls Communicates E2E

*Describe Technical Safety Requirements from Functional Safety Requirements using Table 6 for each Technical Safety Requirement.*

| T-S-Req-ID: | T-S-Req004 - BCM Sub/Rx ISPR Feedback |
| --- | --- |
| External Reference *(optional)* |  |
| Category: | Safety Related Function |
| Safety Goal: | SG03 - Ensure Safe Activation |
| F-S-Req Ref.: | F-S-Req101 - Ignition Control Module and Powertrain Controls Communicates E2E |
| ASIL Classification:  *(in case of category “General”: if applicable, in case of category “Non-E/E Requirement”: not applicable)* | B(D) |
| Technical Safety Requirement Title: | BCM Sub/Rx ISPR Feedback |
| Technical Safety Requirement Text: | The BCMs reception of “PtIgnSwtch\_D\_Stat” (ISPR Feedback Status) from the PCM shall be E2E protected with the specified protection measures for data corruption: PtIgnSwtch\_No\_Cnt - Counter PtIgnSwtch\_No\_Cs - CRC Counter increment Periodicity: 20 ms Message transmission Periodicity: 100 ms FP |
| Rationale: |  |
| Safe State:  *(in case of categories “General”, “Metric”, “Non-E/E Requirement”, or “User Information”: if applicable)* | Module Safe State |
| Reduced Functionality and Interval:  *(if applicable;*  *in case of categories “Metric”, “Non-E/E Requirement”, “Maintain Safe State / Recovery” or “User Information”: not applicable;*  *in case of category “Reduced Functionality”: required)* |  |
| Fault tolerant time interval:  *(in case of categories “Metric” or “Maintain Safe State / Recovery”: not applicable;*  *in case of category “General”, “Reduced Functionality”, “Non-E/E Requirement”, or “User Information”: if applicable)* |  |
| Requirement Status |  |
| V&V method: | System test |
| V&V acceptance criteria:  *(UNV1 / UPV1, not in case of category “Non-E/E requirement)* |  |
| Allocated Element(s)/Component(s)/ Subsystem(s) *(if applicable)* |  |

Table 19: BCM Sub/Rx ISPR Feedback

### Requirement Derivation Diagram(s) for F-S-Req075 - Ignition Control Module Inhibits Start Upon Command

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

*Derive Technical Safety Requirements from Functional Safety Requirements.*

*Insert ‘Requirements Derivation Diagram/Tree’ or GSN here. Several diagrams may be required depending upon the size of the Item.*

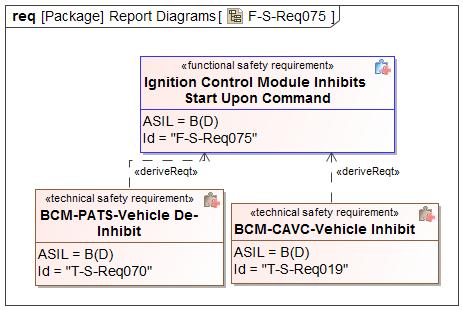


Figure 12 - Technical Safety Requirements Derivation Diagram for F-S-Req075

#### Technical Safety Requirements for F-S-Req075 - Ignition Control Module Inhibits Start Upon Command

*Describe Technical Safety Requirements from Functional Safety Requirements using Table 6 for each Technical Safety Requirement.*

| T-S-Req-ID: | T-S-Req019 - BCM-CAVC-Vehicle Inhibit |
| --- | --- |
| External Reference *(optional)* |  |
| Category: | Safety Related Function |
| Safety Goal: | SG03 - Ensure Safe Activation |
| F-S-Req Ref.: | F-S-Req075 - Ignition Control Module Inhibits Start Upon Command |
| ASIL Classification:  *(in case of category “General”: if applicable, in case of category “Non-E/E Requirement”: not applicable)* | B(D) |
| Technical Safety Requirement Title: | BCM-CAVC-Vehicle Inhibit |
| Technical Safety Requirement Text: | The BCM shall Inhibit Vehicle start, based on Cloud Authorized Vehicle Control Command (CloudVehCtlData\_Tp\_Rq – Vehicle Inhibit rq). |
| Rationale: |  |
| Safe State:  *(in case of categories “General”, “Metric”, “Non-E/E Requirement”, or “User Information”: if applicable)* | Module Safe State |
| Reduced Functionality and Interval:  *(if applicable;*  *in case of categories “Metric”, “Non-E/E Requirement”, “Maintain Safe State / Recovery” or “User Information”: not applicable;*  *in case of category “Reduced Functionality”: required)* |  |
| Fault tolerant time interval:  *(in case of categories “Metric” or “Maintain Safe State / Recovery”: not applicable;*  *in case of category “General”, “Reduced Functionality”, “Non-E/E Requirement”, or “User Information”: if applicable)* |  |
| Requirement Status |  |
| V&V method: | System test |
| V&V acceptance criteria:  *(UNV1 / UPV1, not in case of category “Non-E/E requirement)* |  |
| Allocated Element(s)/Component(s)/ Subsystem(s) *(if applicable)* |  |

Table 20: BCM-CAVC-Vehicle Inhibit

| T-S-Req-ID: | T-S-Req070 - BCM-PATS-Vehicle De-Inhibit |
| --- | --- |
| External Reference *(optional)* |  |
| Category: | Safety Related Function |
| Safety Goal: | SG03 - Ensure Safe Activation |
| F-S-Req Ref.: | F-S-Req075 - Ignition Control Module Inhibits Start Upon Command |
| ASIL Classification:  *(in case of category “General”: if applicable, in case of category “Non-E/E Requirement”: not applicable)* | B(D) |
| Technical Safety Requirement Title: | BCM-PATS-Vehicle De-Inhibit |
| Technical Safety Requirement Text: | The BCM shall remove the cloud inhibit request based on E2E protected CAVC command or PATs coded security routine, if BCM has already inhibited due to cloud request, |
| Rationale: |  |
| Safe State:  *(in case of categories “General”, “Metric”, “Non-E/E Requirement”, or “User Information”: if applicable)* | Module Safe State |
| Reduced Functionality and Interval:  *(if applicable;*  *in case of categories “Metric”, “Non-E/E Requirement”, “Maintain Safe State / Recovery” or “User Information”: not applicable;*  *in case of category “Reduced Functionality”: required)* |  |
| Fault tolerant time interval:  *(in case of categories “Metric” or “Maintain Safe State / Recovery”: not applicable;*  *in case of category “General”, “Reduced Functionality”, “Non-E/E Requirement”, or “User Information”: if applicable)* |  |
| Requirement Status |  |
| V&V method: | System test |
| V&V acceptance criteria:  *(UNV1 / UPV1, not in case of category “Non-E/E requirement)* |  |
| Allocated Element(s)/Component(s)/ Subsystem(s) *(if applicable)* |  |

Table 21: BCM-PATS-Vehicle De-Inhibit

### Requirement Derivation Diagram(s) for F-S-Req086 - OTA App Authenticates Erase And Programming Commands

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

*Derive Technical Safety Requirements from Functional Safety Requirements.*

*Insert ‘Requirements Derivation Diagram/Tree’ or GSN here. Several diagrams may be required depending upon the size of the Item.*

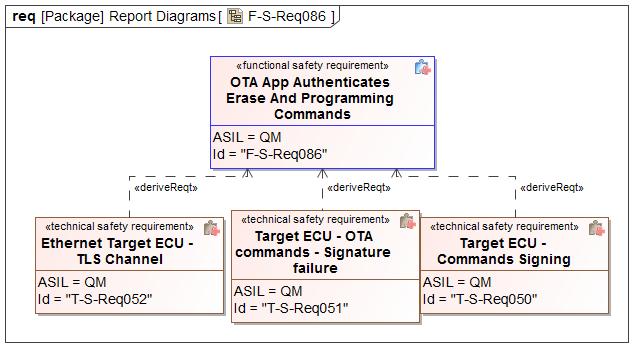


Figure 13 - Technical Safety Requirements Derivation Diagram for F-S-Req086

#### Technical Safety Requirements for F-S-Req086 - OTA App Authenticates Erase And Programming Commands

*Describe Technical Safety Requirements from Functional Safety Requirements using Table 6 for each Technical Safety Requirement.*

| T-S-Req-ID: | T-S-Req050 - Target ECU - Commands Signing |
| --- | --- |
| External Reference *(optional)* |  |
| Category: | Safety Related Function |
| Safety Goal: | SG01 - Prevents Corruption of Existing Software |
| F-S-Req Ref.: | F-S-Req086 - OTA App Authenticates Erase And Programming Commands |
| ASIL Classification:  *(in case of category “General”: if applicable, in case of category “Non-E/E Requirement”: not applicable)* | QM |
| Technical Safety Requirement Title: | Target ECU - Commands Signing |
| Technical Safety Requirement Text: | OTA Signed commands are signed with public-Private key pair stored in each Target ECU |
| Rationale: |  |
| Safe State:  *(in case of categories “General”, “Metric”, “Non-E/E Requirement”, or “User Information”: if applicable)* | Module Safe State |
| Reduced Functionality and Interval:  *(if applicable;*  *in case of categories “Metric”, “Non-E/E Requirement”, “Maintain Safe State / Recovery” or “User Information”: not applicable;*  *in case of category “Reduced Functionality”: required)* |  |
| Fault tolerant time interval:  *(in case of categories “Metric” or “Maintain Safe State / Recovery”: not applicable;*  *in case of category “General”, “Reduced Functionality”, “Non-E/E Requirement”, or “User Information”: if applicable)* |  |
| Requirement Status |  |
| V&V method: | System test |
| V&V acceptance criteria:  *(UNV1 / UPV1, not in case of category “Non-E/E requirement)* |  |
| Allocated Element(s)/Component(s)/ Subsystem(s) *(if applicable)* |  |

Table 22: Target ECU - Commands Signing

| T-S-Req-ID: | T-S-Req051 - Target ECU - OTA commands - Signature failure |
| --- | --- |
| External Reference *(optional)* |  |
| Category: | Safety Related Function |
| Safety Goal: | SG01 - Prevents Corruption of Existing Software |
| F-S-Req Ref.: | F-S-Req086 - OTA App Authenticates Erase And Programming Commands |
| ASIL Classification:  *(in case of category “General”: if applicable, in case of category “Non-E/E Requirement”: not applicable)* | QM |
| Technical Safety Requirement Title: | Target ECU - OTA commands - Signature failure |
| Technical Safety Requirement Text: | The OTA command signatures shall be verified prior to the execution. If signature fails, then the ECU shall respond to the ECG with a negative response |
| Rationale: |  |
| Safe State:  *(in case of categories “General”, “Metric”, “Non-E/E Requirement”, or “User Information”: if applicable)* | Module Safe State |
| Reduced Functionality and Interval:  *(if applicable;*  *in case of categories “Metric”, “Non-E/E Requirement”, “Maintain Safe State / Recovery” or “User Information”: not applicable;*  *in case of category “Reduced Functionality”: required)* |  |
| Fault tolerant time interval:  *(in case of categories “Metric” or “Maintain Safe State / Recovery”: not applicable;*  *in case of category “General”, “Reduced Functionality”, “Non-E/E Requirement”, or “User Information”: if applicable)* |  |
| Requirement Status |  |
| V&V method: | System test |
| V&V acceptance criteria:  *(UNV1 / UPV1, not in case of category “Non-E/E requirement)* |  |
| Allocated Element(s)/Component(s)/ Subsystem(s) *(if applicable)* |  |

Table 23: Target ECU - OTA commands - Signature failure

| T-S-Req-ID: | T-S-Req052 - Ethernet Target ECU - TLS Channel |
| --- | --- |
| External Reference *(optional)* |  |
| Category: | Safety Related Function |
| Safety Goal: | SG01 - Prevents Corruption of Existing Software |
| F-S-Req Ref.: | F-S-Req086 - OTA App Authenticates Erase And Programming Commands |
| ASIL Classification:  *(in case of category “General”: if applicable, in case of category “Non-E/E Requirement”: not applicable)* | QM |
| Technical Safety Requirement Title: | Ethernet Target ECU - TLS Channel |
| Technical Safety Requirement Text: | Ethernet ECUs shall only accept the OTA Command/Trigger on a secure TLS channel |
| Rationale: |  |
| Safe State:  *(in case of categories “General”, “Metric”, “Non-E/E Requirement”, or “User Information”: if applicable)* | Module Safe State |
| Reduced Functionality and Interval:  *(if applicable;*  *in case of categories “Metric”, “Non-E/E Requirement”, “Maintain Safe State / Recovery” or “User Information”: not applicable;*  *in case of category “Reduced Functionality”: required)* |  |
| Fault tolerant time interval:  *(in case of categories “Metric” or “Maintain Safe State / Recovery”: not applicable;*  *in case of category “General”, “Reduced Functionality”, “Non-E/E Requirement”, or “User Information”: if applicable)* |  |
| Requirement Status |  |
| V&V method: | System test |
| V&V acceptance criteria:  *(UNV1 / UPV1, not in case of category “Non-E/E requirement)* |  |
| Allocated Element(s)/Component(s)/ Subsystem(s) *(if applicable)* |  |

Table 24: Ethernet Target ECU - TLS Channel

### Requirement Derivation Diagram(s) for F-S-Req095 - OTA App Detects Communication Errors

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

*Derive Technical Safety Requirements from Functional Safety Requirements.*

*Insert ‘Requirements Derivation Diagram/Tree’ or GSN here. Several diagrams may be required depending upon the size of the Item.*

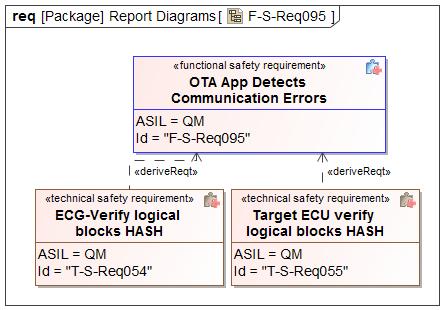


Figure 14 - Technical Safety Requirements Derivation Diagram for F-S-Req095

#### Technical Safety Requirements for F-S-Req095 - OTA App Detects Communication Errors

*Describe Technical Safety Requirements from Functional Safety Requirements using Table 6 for each Technical Safety Requirement.*

| T-S-Req-ID: | T-S-Req054 - ECG-Verify logical blocks HASH |
| --- | --- |
| External Reference *(optional)* |  |
| Category: | Safety Related Function |
| Safety Goal: | SG01 - Prevents Corruption of Existing Software |
| F-S-Req Ref.: | F-S-Req095 - OTA App Detects Communication Errors |
| ASIL Classification:  *(in case of category “General”: if applicable, in case of category “Non-E/E Requirement”: not applicable)* | QM |
| Technical Safety Requirement Title: | ECG-Verify logical blocks HASH |
| Technical Safety Requirement Text: | ECG vehicle micro shall verify the hash of each logical block transmitted via internal IPC from consumer micro |
| Rationale: |  |
| Safe State:  *(in case of categories “General”, “Metric”, “Non-E/E Requirement”, or “User Information”: if applicable)* | Module Safe State |
| Reduced Functionality and Interval:  *(if applicable;*  *in case of categories “Metric”, “Non-E/E Requirement”, “Maintain Safe State / Recovery” or “User Information”: not applicable;*  *in case of category “Reduced Functionality”: required)* |  |
| Fault tolerant time interval:  *(in case of categories “Metric” or “Maintain Safe State / Recovery”: not applicable;*  *in case of category “General”, “Reduced Functionality”, “Non-E/E Requirement”, or “User Information”: if applicable)* |  |
| Requirement Status |  |
| V&V method: | System test |
| V&V acceptance criteria:  *(UNV1 / UPV1, not in case of category “Non-E/E requirement)* |  |
| Allocated Element(s)/Component(s)/ Subsystem(s) *(if applicable)* |  |

Table 25: ECG-Verify logical blocks HASH

| T-S-Req-ID: | T-S-Req055 - Target ECU verify logical blocks HASH |
| --- | --- |
| External Reference *(optional)* |  |
| Category: | Safety Related Function |
| Safety Goal: | SG01 - Prevents Corruption of Existing Software |
| F-S-Req Ref.: | F-S-Req095 - OTA App Detects Communication Errors |
| ASIL Classification:  *(in case of category “General”: if applicable, in case of category “Non-E/E Requirement”: not applicable)* | QM |
| Technical Safety Requirement Title: | Target ECU verify logical blocks HASH |
| Technical Safety Requirement Text: | OTA Application shall verify the hash of each logical block transmitted via CAN or Ethernet |
| Rationale: |  |
| Safe State:  *(in case of categories “General”, “Metric”, “Non-E/E Requirement”, or “User Information”: if applicable)* | Module Safe State |
| Reduced Functionality and Interval:  *(if applicable;*  *in case of categories “Metric”, “Non-E/E Requirement”, “Maintain Safe State / Recovery” or “User Information”: not applicable;*  *in case of category “Reduced Functionality”: required)* |  |
| Fault tolerant time interval:  *(in case of categories “Metric” or “Maintain Safe State / Recovery”: not applicable;*  *in case of category “General”, “Reduced Functionality”, “Non-E/E Requirement”, or “User Information”: if applicable)* |  |
| Requirement Status |  |
| V&V method: | System test |
| V&V acceptance criteria:  *(UNV1 / UPV1, not in case of category “Non-E/E requirement)* |  |
| Allocated Element(s)/Component(s)/ Subsystem(s) *(if applicable)* |  |

Table 26: Target ECU verify logical blocks HASH

### Requirement Derivation Diagram(s) for F-S-Req087 - OTA App Executes OTA Without Affecting Basic Function

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

*Derive Technical Safety Requirements from Functional Safety Requirements.*

*Insert ‘Requirements Derivation Diagram/Tree’ or GSN here. Several diagrams may be required depending upon the size of the Item.*

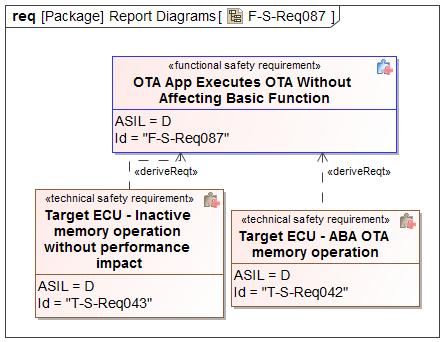


Figure 15 - Technical Safety Requirements Derivation Diagram for F-S-Req087

#### Technical Safety Requirements for F-S-Req087 - OTA App Executes OTA Without Affecting Basic Function

*Describe Technical Safety Requirements from Functional Safety Requirements using Table 6 for each Technical Safety Requirement.*

| T-S-Req-ID: | T-S-Req042 - Target ECU - ABA OTA memory operation |
| --- | --- |
| External Reference *(optional)* |  |
| Category: | Safety Related Function |
| Safety Goal: | SG01 - Prevents Corruption of Existing Software |
| F-S-Req Ref.: | F-S-Req087 - OTA App Executes OTA Without Affecting Basic Function |
| ASIL Classification:  *(in case of category “General”: if applicable, in case of category “Non-E/E Requirement”: not applicable)* | D |
| Technical Safety Requirement Title: | Target ECU - ABA OTA memory operation |
| Technical Safety Requirement Text: | ECUs that use A/B/A OTA, shall enter a safe mode (similar to a bootloader mode) prior to erasing internal memory and writing the new SW into the bootable partition. |
| Rationale: |  |
| Safe State:  *(in case of categories “General”, “Metric”, “Non-E/E Requirement”, or “User Information”: if applicable)* | Module Safe State |
| Reduced Functionality and Interval:  *(if applicable;*  *in case of categories “Metric”, “Non-E/E Requirement”, “Maintain Safe State / Recovery” or “User Information”: not applicable;*  *in case of category “Reduced Functionality”: required)* |  |
| Fault tolerant time interval:  *(in case of categories “Metric” or “Maintain Safe State / Recovery”: not applicable;*  *in case of category “General”, “Reduced Functionality”, “Non-E/E Requirement”, or “User Information”: if applicable)* |  |
| Requirement Status |  |
| V&V method: | System test |
| V&V acceptance criteria:  *(UNV1 / UPV1, not in case of category “Non-E/E requirement)* |  |
| Allocated Element(s)/Component(s)/ Subsystem(s) *(if applicable)* |  |

Table 27: Target ECU - ABA OTA memory operation

| T-S-Req-ID: | T-S-Req043 - Target ECU - Inactive memory operation without performance impact |
| --- | --- |
| External Reference *(optional)* |  |
| Category: | Safety Related Function |
| Safety Goal: | SG01 - Prevents Corruption of Existing Software |
| F-S-Req Ref.: | F-S-Req087 - OTA App Executes OTA Without Affecting Basic Function |
| ASIL Classification:  *(in case of category “General”: if applicable, in case of category “Non-E/E Requirement”: not applicable)* | D |
| Technical Safety Requirement Title: | Target ECU - Inactive memory operation without performance impact |
| Technical Safety Requirement Text: | ECUs that use A/B OTA shall program the new software in the non-active memory without impacting ECU resources or impacting any functionality. |
| Rationale: |  |
| Safe State:  *(in case of categories “General”, “Metric”, “Non-E/E Requirement”, or “User Information”: if applicable)* | Module Safe State |
| Reduced Functionality and Interval:  *(if applicable;*  *in case of categories “Metric”, “Non-E/E Requirement”, “Maintain Safe State / Recovery” or “User Information”: not applicable;*  *in case of category “Reduced Functionality”: required)* |  |
| Fault tolerant time interval:  *(in case of categories “Metric” or “Maintain Safe State / Recovery”: not applicable;*  *in case of category “General”, “Reduced Functionality”, “Non-E/E Requirement”, or “User Information”: if applicable)* |  |
| Requirement Status |  |
| V&V method: | System test |
| V&V acceptance criteria:  *(UNV1 / UPV1, not in case of category “Non-E/E requirement)* |  |
| Allocated Element(s)/Component(s)/ Subsystem(s) *(if applicable)* |  |

Table 28: Target ECU - Inactive memory operation without performance impact

### Requirement Derivation Diagram(s) for F-S-Req084 - OTA App Informs the OTA Feature of Data Corruption

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

*Derive Technical Safety Requirements from Functional Safety Requirements.*

*Insert ‘Requirements Derivation Diagram/Tree’ or GSN here. Several diagrams may be required depending upon the size of the Item.*

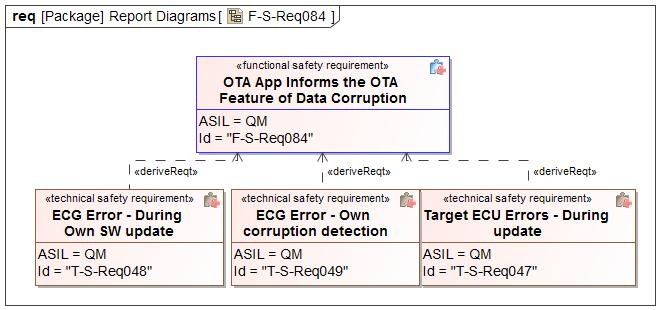


Figure 16 - Technical Safety Requirements Derivation Diagram for F-S-Req084

#### Technical Safety Requirements for F-S-Req084 - OTA App Informs the OTA Feature of Data Corruption

*Describe Technical Safety Requirements from Functional Safety Requirements using Table 6 for each Technical Safety Requirement.*

| T-S-Req-ID: | T-S-Req047 - Target ECU Errors - During update |
| --- | --- |
| External Reference *(optional)* |  |
| Category: | Safety Related Function |
| Safety Goal: | SG01 - Prevents Corruption of Existing Software |
| F-S-Req Ref.: | F-S-Req084 - OTA App Informs the OTA Feature of Data Corruption |
| ASIL Classification:  *(in case of category “General”: if applicable, in case of category “Non-E/E Requirement”: not applicable)* | QM |
| Technical Safety Requirement Title: | Target ECU Errors - During update |
| Technical Safety Requirement Text: | OTA Application shall respond with 0x72 GeneralProgrammingFailure when erasing or programming fails |
| Rationale: |  |
| Safe State:  *(in case of categories “General”, “Metric”, “Non-E/E Requirement”, or “User Information”: if applicable)* | Module Safe State |
| Reduced Functionality and Interval:  *(if applicable;*  *in case of categories “Metric”, “Non-E/E Requirement”, “Maintain Safe State / Recovery” or “User Information”: not applicable;*  *in case of category “Reduced Functionality”: required)* |  |
| Fault tolerant time interval:  *(in case of categories “Metric” or “Maintain Safe State / Recovery”: not applicable;*  *in case of category “General”, “Reduced Functionality”, “Non-E/E Requirement”, or “User Information”: if applicable)* |  |
| Requirement Status |  |
| V&V method: | System test |
| V&V acceptance criteria:  *(UNV1 / UPV1, not in case of category “Non-E/E requirement)* |  |
| Allocated Element(s)/Component(s)/ Subsystem(s) *(if applicable)* |  |

Table 29: Target ECU Errors - During update

| T-S-Req-ID: | T-S-Req048 - ECG Error - During Own SW update |
| --- | --- |
| External Reference *(optional)* |  |
| Category: | Safety Related Function |
| Safety Goal: | SG01 - Prevents Corruption of Existing Software |
| F-S-Req Ref.: | F-S-Req084 - OTA App Informs the OTA Feature of Data Corruption |
| ASIL Classification:  *(in case of category “General”: if applicable, in case of category “Non-E/E Requirement”: not applicable)* | QM |
| Technical Safety Requirement Title: | ECG Error - During Own SW update |
| Technical Safety Requirement Text: | ECG shall identify any failures with erasing or programming its own software and report it thru a DTC and Cloud Status |
| Rationale: |  |
| Safe State:  *(in case of categories “General”, “Metric”, “Non-E/E Requirement”, or “User Information”: if applicable)* | Module Safe State |
| Reduced Functionality and Interval:  *(if applicable;*  *in case of categories “Metric”, “Non-E/E Requirement”, “Maintain Safe State / Recovery” or “User Information”: not applicable;*  *in case of category “Reduced Functionality”: required)* |  |
| Fault tolerant time interval:  *(in case of categories “Metric” or “Maintain Safe State / Recovery”: not applicable;*  *in case of category “General”, “Reduced Functionality”, “Non-E/E Requirement”, or “User Information”: if applicable)* |  |
| Requirement Status |  |
| V&V method: | System test |
| V&V acceptance criteria:  *(UNV1 / UPV1, not in case of category “Non-E/E requirement)* |  |
| Allocated Element(s)/Component(s)/ Subsystem(s) *(if applicable)* |  |

Table 30: ECG Error - During Own SW update

| T-S-Req-ID: | T-S-Req049 - ECG Error - Own corruption detection |
| --- | --- |
| External Reference *(optional)* |  |
| Category: | Safety Related Function |
| Safety Goal: | SG01 - Prevents Corruption of Existing Software |
| F-S-Req Ref.: | F-S-Req084 - OTA App Informs the OTA Feature of Data Corruption |
| ASIL Classification:  *(in case of category “General”: if applicable, in case of category “Non-E/E Requirement”: not applicable)* | QM |
| Technical Safety Requirement Title: | ECG Error - Own corruption detection |
| Technical Safety Requirement Text: | ECG shall verify that its software is not corrupted prior to starting the installation, If corruption is detected, then it should report to the Ford Cloud. |
| Rationale: |  |
| Safe State:  *(in case of categories “General”, “Metric”, “Non-E/E Requirement”, or “User Information”: if applicable)* | Module Safe State |
| Reduced Functionality and Interval:  *(if applicable;*  *in case of categories “Metric”, “Non-E/E Requirement”, “Maintain Safe State / Recovery” or “User Information”: not applicable;*  *in case of category “Reduced Functionality”: required)* |  |
| Fault tolerant time interval:  *(in case of categories “Metric” or “Maintain Safe State / Recovery”: not applicable;*  *in case of category “General”, “Reduced Functionality”, “Non-E/E Requirement”, or “User Information”: if applicable)* |  |
| Requirement Status |  |
| V&V method: | System test |
| V&V acceptance criteria:  *(UNV1 / UPV1, not in case of category “Non-E/E requirement)* |  |
| Allocated Element(s)/Component(s)/ Subsystem(s) *(if applicable)* |  |

Table 31: ECG Error - Own corruption detection

### Requirement Derivation Diagram(s) for F-S-Req082 - OTA App Prevents Active Memory Erasing or Writing

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

*Derive Technical Safety Requirements from Functional Safety Requirements.*

*Insert ‘Requirements Derivation Diagram/Tree’ or GSN here. Several diagrams may be required depending upon the size of the Item.*

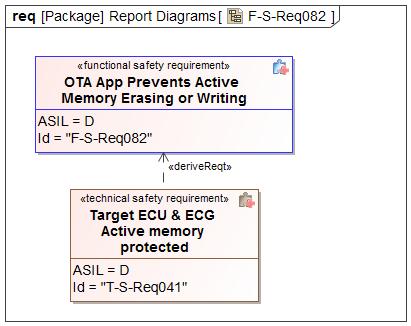


Figure 17 - Technical Safety Requirements Derivation Diagram for F-S-Req082

#### Technical Safety Requirements for F-S-Req082 - OTA App Prevents Active Memory Erasing or Writing

*Describe Technical Safety Requirements from Functional Safety Requirements using Table 6 for each Technical Safety Requirement.*

| T-S-Req-ID: | T-S-Req041 - Target ECU & ECG Active memory protected |
| --- | --- |
| External Reference *(optional)* |  |
| Category: | Safety Related Function |
| Safety Goal: | SG01 - Prevents Corruption of Existing Software |
| F-S-Req Ref.: | F-S-Req082 - OTA App Prevents Active Memory Erasing or Writing |
| ASIL Classification:  *(in case of category “General”: if applicable, in case of category “Non-E/E Requirement”: not applicable)* | D |
| Technical Safety Requirement Title: | Target ECU & ECG Active memory protected |
| Technical Safety Requirement Text: | During AB OTA update, All modules shall not program or erase active memory. |
| Rationale: |  |
| Safe State:  *(in case of categories “General”, “Metric”, “Non-E/E Requirement”, or “User Information”: if applicable)* | Module Safe State |
| Reduced Functionality and Interval:  *(if applicable;*  *in case of categories “Metric”, “Non-E/E Requirement”, “Maintain Safe State / Recovery” or “User Information”: not applicable;*  *in case of category “Reduced Functionality”: required)* |  |
| Fault tolerant time interval:  *(in case of categories “Metric” or “Maintain Safe State / Recovery”: not applicable;*  *in case of category “General”, “Reduced Functionality”, “Non-E/E Requirement”, or “User Information”: if applicable)* |  |
| Requirement Status |  |
| V&V method: | System test |
| V&V acceptance criteria:  *(UNV1 / UPV1, not in case of category “Non-E/E requirement)* |  |
| Allocated Element(s)/Component(s)/ Subsystem(s) *(if applicable)* |  |

Table 32: Target ECU & ECG Active memory protected

### Requirement Derivation Diagram(s) for F-S-Req091 - OTA App rejects Invalid Software

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

*Derive Technical Safety Requirements from Functional Safety Requirements.*

*Insert ‘Requirements Derivation Diagram/Tree’ or GSN here. Several diagrams may be required depending upon the size of the Item.*

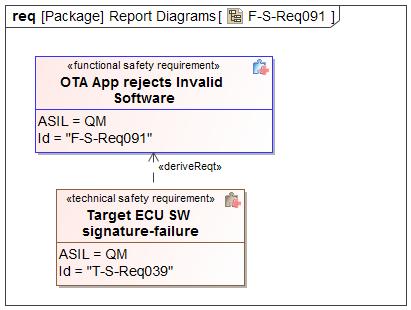


Figure 18 - Technical Safety Requirements Derivation Diagram for F-S-Req091

#### Technical Safety Requirements for F-S-Req091 - OTA App rejects Invalid Software

*Describe Technical Safety Requirements from Functional Safety Requirements using Table 6 for each Technical Safety Requirement.*

| T-S-Req-ID: | T-S-Req039 - Target ECU SW signature-failure |
| --- | --- |
| External Reference *(optional)* |  |
| Category: | Safety Related Function |
| Safety Goal: | SG04 - Ensure Safe Verification of Activation  SG02 - Prevents Flashing of Incorrect SW |
| F-S-Req Ref.: | F-S-Req091 - OTA App rejects Invalid Software |
| ASIL Classification:  *(in case of category “General”: if applicable, in case of category “Non-E/E Requirement”: not applicable)* | QM |
| Technical Safety Requirement Title: | Target ECU SW signature-failure |
| Technical Safety Requirement Text: | OTA Application shall not install software that fails the software signature |
| Rationale: |  |
| Safe State:  *(in case of categories “General”, “Metric”, “Non-E/E Requirement”, or “User Information”: if applicable)* | Module Safe State |
| Reduced Functionality and Interval:  *(if applicable;*  *in case of categories “Metric”, “Non-E/E Requirement”, “Maintain Safe State / Recovery” or “User Information”: not applicable;*  *in case of category “Reduced Functionality”: required)* |  |
| Fault tolerant time interval:  *(in case of categories “Metric” or “Maintain Safe State / Recovery”: not applicable;*  *in case of category “General”, “Reduced Functionality”, “Non-E/E Requirement”, or “User Information”: if applicable)* |  |
| Requirement Status |  |
| V&V method: | System test |
| V&V acceptance criteria:  *(UNV1 / UPV1, not in case of category “Non-E/E requirement)* |  |
| Allocated Element(s)/Component(s)/ Subsystem(s) *(if applicable)* |  |

Table 33: Target ECU SW signature-failure

### Requirement Derivation Diagram(s) for F-S-Req092 - OTA App Sends Correct Part Number

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

*Derive Technical Safety Requirements from Functional Safety Requirements.*

*Insert ‘Requirements Derivation Diagram/Tree’ or GSN here. Several diagrams may be required depending upon the size of the Item.*

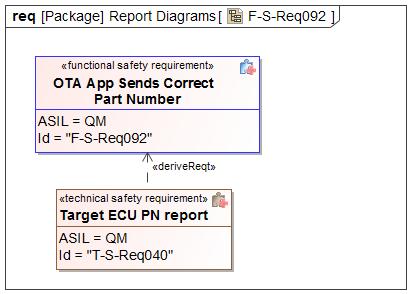


Figure 19 - Technical Safety Requirements Derivation Diagram for F-S-Req092

#### Technical Safety Requirements for F-S-Req092 - OTA App Sends Correct Part Number

*Describe Technical Safety Requirements from Functional Safety Requirements using Table 6 for each Technical Safety Requirement.*

| T-S-Req-ID: | T-S-Req040 - Target ECU PN report |
| --- | --- |
| External Reference *(optional)* |  |
| Category: | Safety Related Function |
| Safety Goal: | SG04 - Ensure Safe Verification of Activation  SG02 - Prevents Flashing of Incorrect SW |
| F-S-Req Ref.: | F-S-Req092 - OTA App Sends Correct Part Number |
| ASIL Classification:  *(in case of category “General”: if applicable, in case of category “Non-E/E Requirement”: not applicable)* | QM |
| Technical Safety Requirement Title: | Target ECU PN report |
| Technical Safety Requirement Text: | OTA Application shall provide active software part numbers to the ECG upon diagnostic request |
| Rationale: |  |
| Safe State:  *(in case of categories “General”, “Metric”, “Non-E/E Requirement”, or “User Information”: if applicable)* | Module Safe State |
| Reduced Functionality and Interval:  *(if applicable;*  *in case of categories “Metric”, “Non-E/E Requirement”, “Maintain Safe State / Recovery” or “User Information”: not applicable;*  *in case of category “Reduced Functionality”: required)* |  |
| Fault tolerant time interval:  *(in case of categories “Metric” or “Maintain Safe State / Recovery”: not applicable;*  *in case of category “General”, “Reduced Functionality”, “Non-E/E Requirement”, or “User Information”: if applicable)* |  |
| Requirement Status |  |
| V&V method: | System test |
| V&V acceptance criteria:  *(UNV1 / UPV1, not in case of category “Non-E/E requirement)* |  |
| Allocated Element(s)/Component(s)/ Subsystem(s) *(if applicable)* |  |

Table 34: Target ECU PN report

### Requirement Derivation Diagram(s) for F-S-Req093 - OTA App Verifies Installed Software During Activation

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

*Derive Technical Safety Requirements from Functional Safety Requirements.*

*Insert ‘Requirements Derivation Diagram/Tree’ or GSN here. Several diagrams may be required depending upon the size of the Item.*

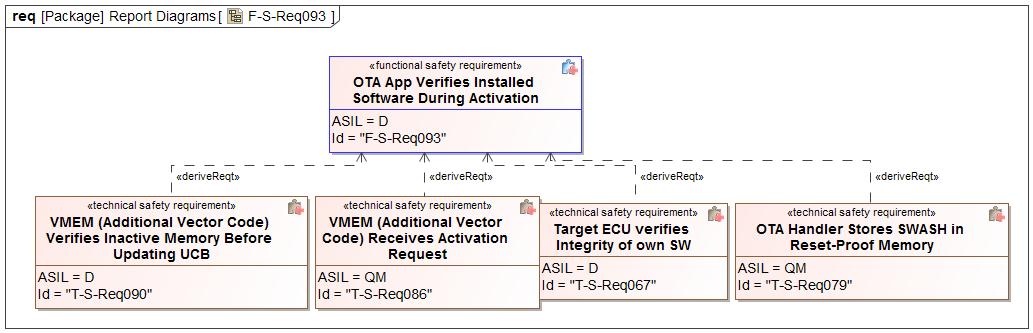


Figure 20 - Technical Safety Requirements Derivation Diagram for F-S-Req093

#### Technical Safety Requirements for F-S-Req093 - OTA App Verifies Installed Software During Activation

*Describe Technical Safety Requirements from Functional Safety Requirements using Table 6 for each Technical Safety Requirement.*

| T-S-Req-ID: | T-S-Req067 - Target ECU verifies Integrity of own SW |
| --- | --- |
| External Reference *(optional)* |  |
| Category: | Safety Related Function |
| Safety Goal: | SG05 - Ensure Safe Rollback |
| F-S-Req Ref.: | F-S-Req093 - OTA App Verifies Installed Software During Activation |
| ASIL Classification:  *(in case of category “General”: if applicable, in case of category “Non-E/E Requirement”: not applicable)* | D |
| Technical Safety Requirement Title: | Target ECU verifies Integrity of own SW |
| Technical Safety Requirement Text: | After a reflash, All Target modules shall verify the integrity of its own software. |
| Rationale: |  |
| Safe State:  *(in case of categories “General”, “Metric”, “Non-E/E Requirement”, or “User Information”: if applicable)* | Module Safe State |
| Reduced Functionality and Interval:  *(if applicable;*  *in case of categories “Metric”, “Non-E/E Requirement”, “Maintain Safe State / Recovery” or “User Information”: not applicable;*  *in case of category “Reduced Functionality”: required)* |  |
| Fault tolerant time interval:  *(in case of categories “Metric” or “Maintain Safe State / Recovery”: not applicable;*  *in case of category “General”, “Reduced Functionality”, “Non-E/E Requirement”, or “User Information”: if applicable)* |  |
| Requirement Status |  |
| V&V method: | System test |
| V&V acceptance criteria:  *(UNV1 / UPV1, not in case of category “Non-E/E requirement)* |  |
| Allocated Element(s)/Component(s)/ Subsystem(s) *(if applicable)* |  |

Table 35: Target ECU verifies Integrity of own SW

| T-S-Req-ID: | T-S-Req079 - OTA Handler Stores SWASH in Reset-Proof Memory |
| --- | --- |
| External Reference *(optional)* |  |
| Category: | Safety Related Function |
| Safety Goal: | SG05 - Ensure Safe Rollback |
| F-S-Req Ref.: | F-S-Req093 - OTA App Verifies Installed Software During Activation |
| ASIL Classification:  *(in case of category “General”: if applicable, in case of category “Non-E/E Requirement”: not applicable)* | **ASIL Override Rationale -** Failure to store or retrieve the Expected SWASH would not lead to a violation of the safety goal.  QM |
| Technical Safety Requirement Title: | OTA Handler Stores SWASH in Reset-Proof Memory |
| Technical Safety Requirement Text: | The OTA handler shall store the SWASH in a memory portion that is not erased due to a module reset. |
| Rationale: | The OTA handler provides the expected SWASH to the Vector PBL in order to verify the inactive memory. It provides the SWASH by storing it in a reset-proof memory region. |
| Safe State:  *(in case of categories “General”, “Metric”, “Non-E/E Requirement”, or “User Information”: if applicable)* | Normal |
| Reduced Functionality and Interval:  *(if applicable;*  *in case of categories “Metric”, “Non-E/E Requirement”, “Maintain Safe State / Recovery” or “User Information”: not applicable;*  *in case of category “Reduced Functionality”: required)* |  |
| Fault tolerant time interval:  *(in case of categories “Metric” or “Maintain Safe State / Recovery”: not applicable;*  *in case of category “General”, “Reduced Functionality”, “Non-E/E Requirement”, or “User Information”: if applicable)* | - |
| Requirement Status |  |
| V&V method: | System test |
| V&V acceptance criteria:  *(UNV1 / UPV1, not in case of category “Non-E/E requirement)* | The OTA handler stores SWASH in reset-proof memory. |
| Allocated Element(s)/Component(s)/ Subsystem(s) *(if applicable)* |  |

Table 36: OTA Handler Stores SWASH in Reset-Proof Memory

| T-S-Req-ID: | T-S-Req086 - VMEM (Additional Vector Code) Receives Activation Request |
| --- | --- |
| External Reference *(optional)* |  |
| Category: | Safety Related Function |
| Safety Goal: | SG05 - Ensure Safe Rollback |
| F-S-Req Ref.: | F-S-Req093 - OTA App Verifies Installed Software During Activation |
| ASIL Classification:  *(in case of category “General”: if applicable, in case of category “Non-E/E Requirement”: not applicable)* | **ASIL Override Rationale -** Failure to recieve the Activation Request command would not lead to a violation of the safety goal  QM |
| Technical Safety Requirement Title: | VMEM (Additional Vector Code) Receives Activation Request |
| Technical Safety Requirement Text: | The VMEM (Additional Vector Code) shall receive activation request from the ECU Integration Code. |
| Rationale: | To avoid switching to corrupted software, the VMEM (Additional Vector Code) compares its calculated software hash of the new software to the expected hash. |
| Safe State:  *(in case of categories “General”, “Metric”, “Non-E/E Requirement”, or “User Information”: if applicable)* | Normal |
| Reduced Functionality and Interval:  *(if applicable;*  *in case of categories “Metric”, “Non-E/E Requirement”, “Maintain Safe State / Recovery” or “User Information”: not applicable;*  *in case of category “Reduced Functionality”: required)* |  |
| Fault tolerant time interval:  *(in case of categories “Metric” or “Maintain Safe State / Recovery”: not applicable;*  *in case of category “General”, “Reduced Functionality”, “Non-E/E Requirement”, or “User Information”: if applicable)* | - |
| Requirement Status |  |
| V&V method: | System test |
| V&V acceptance criteria:  *(UNV1 / UPV1, not in case of category “Non-E/E requirement)* | VMEM (Additional Vector Code) receives activation request. |
| Allocated Element(s)/Component(s)/ Subsystem(s) *(if applicable)* |  |

Table 37: VMEM (Additional Vector Code) Receives Activation Request

| T-S-Req-ID: | T-S-Req090 - VMEM (Additional Vector Code) Verifies Inactive Memory Before Updating UCB |
| --- | --- |
| External Reference *(optional)* |  |
| Category: | Safety Related Function |
| Safety Goal: | SG05 - Ensure Safe Rollback |
| F-S-Req Ref.: | F-S-Req093 - OTA App Verifies Installed Software During Activation |
| ASIL Classification:  *(in case of category “General”: if applicable, in case of category “Non-E/E Requirement”: not applicable)* | D |
| Technical Safety Requirement Title: | VMEM (Additional Vector Code) Verifies Inactive Memory Before Updating UCB |
| Technical Safety Requirement Text: | Before switching to new software, the VMEM (Additional Vector Code) shall verify the new software by checking the expected SWASH against the calculated SWASH. |
| Rationale: | To avoid switching to corrupted software, the VMEM (Additional Vector Code) compares its calculated software hash of the new software to the expected hash. |
| Safe State:  *(in case of categories “General”, “Metric”, “Non-E/E Requirement”, or “User Information”: if applicable)* | Module Safe State |
| Reduced Functionality and Interval:  *(if applicable;*  *in case of categories “Metric”, “Non-E/E Requirement”, “Maintain Safe State / Recovery” or “User Information”: not applicable;*  *in case of category “Reduced Functionality”: required)* |  |
| Fault tolerant time interval:  *(in case of categories “Metric” or “Maintain Safe State / Recovery”: not applicable;*  *in case of category “General”, “Reduced Functionality”, “Non-E/E Requirement”, or “User Information”: if applicable)* | 1 Second |
| Requirement Status |  |
| V&V method: | System test |
| V&V acceptance criteria:  *(UNV1 / UPV1, not in case of category “Non-E/E requirement)* | VMEM (Additional Vector Code) verifies new software by comparing expected and calculated SWASH. |
| Allocated Element(s)/Component(s)/ Subsystem(s) *(if applicable)* |  |

Table 38: VMEM (Additional Vector Code) Verifies Inactive Memory Before Updating UCB

### Requirement Derivation Diagram(s) for F-S-Req100 - OTA Feature and Ignition Control Module Communicates E2E

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

*Derive Technical Safety Requirements from Functional Safety Requirements.*

*Insert ‘Requirements Derivation Diagram/Tree’ or GSN here. Several diagrams may be required depending upon the size of the Item.*

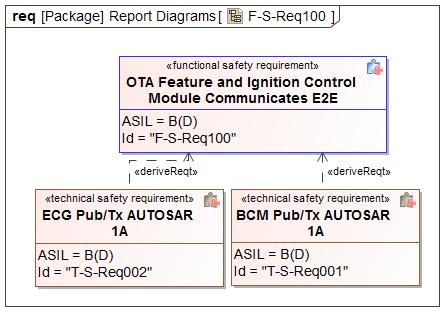


Figure 21 - Technical Safety Requirements Derivation Diagram for F-S-Req100

#### Technical Safety Requirements for F-S-Req100 - OTA Feature and Ignition Control Module Communicates E2E

*Describe Technical Safety Requirements from Functional Safety Requirements using Table 6 for each Technical Safety Requirement.*

| T-S-Req-ID: | T-S-Req001 - BCM Pub/Tx AUTOSAR 1A |
| --- | --- |
| External Reference *(optional)* |  |
| Category: | Safety Related Function |
| Safety Goal: | SG03 - Ensure Safe Activation |
| F-S-Req Ref.: | F-S-Req100 - OTA Feature and Ignition Control Module Communicates E2E |
| ASIL Classification:  *(in case of category “General”: if applicable, in case of category “Non-E/E Requirement”: not applicable)* | B(D) |
| Technical Safety Requirement Title: | BCM Pub/Tx AUTOSAR 1A |
| Technical Safety Requirement Text: | BCM transmission of the “VehStrtInhbt\_D\_Stat shall be E2E protected with the specified protection measures for data corruption: CrnkInhbt\_No\_Crc - CRC based on Polynomial 0x1D of CRC-8-SAE J1850 is specified for Profile 1. byte0 of msg 0x3A4 CrnkInhbt2\_No\_Cnt - - 4 bits, Implements a Counter mechanism that is incremented every Send request and explicitly sent. - When the counter reaches the value 14 (0xE), then it shall restart with 0 for the next send request. Data ID - 0x03A4 (Message ID is 0x3A4). Data elements: Big Endian byte1 to byte7 of msg 0x3A4. ECG shall following AUTOSAR 1A. |
| Rationale: |  |
| Safe State:  *(in case of categories “General”, “Metric”, “Non-E/E Requirement”, or “User Information”: if applicable)* | Module Safe State |
| Reduced Functionality and Interval:  *(if applicable;*  *in case of categories “Metric”, “Non-E/E Requirement”, “Maintain Safe State / Recovery” or “User Information”: not applicable;*  *in case of category “Reduced Functionality”: required)* |  |
| Fault tolerant time interval:  *(in case of categories “Metric” or “Maintain Safe State / Recovery”: not applicable;*  *in case of category “General”, “Reduced Functionality”, “Non-E/E Requirement”, or “User Information”: if applicable)* |  |
| Requirement Status |  |
| V&V method: | System test |
| V&V acceptance criteria:  *(UNV1 / UPV1, not in case of category “Non-E/E requirement)* |  |
| Allocated Element(s)/Component(s)/ Subsystem(s) *(if applicable)* |  |

Table 39: BCM Pub/Tx AUTOSAR 1A

| T-S-Req-ID: | T-S-Req002 - ECG Pub/Tx AUTOSAR 1A |
| --- | --- |
| External Reference *(optional)* |  |
| Category: | Safety Related Function |
| Safety Goal: | SG03 - Ensure Safe Activation |
| F-S-Req Ref.: | F-S-Req100 - OTA Feature and Ignition Control Module Communicates E2E |
| ASIL Classification:  *(in case of category “General”: if applicable, in case of category “Non-E/E Requirement”: not applicable)* | B(D) |
| Technical Safety Requirement Title: | ECG Pub/Tx AUTOSAR 1A |
| Technical Safety Requirement Text: | ECG Transmission of the “VehOn\_D\_RqCld shall be E2E protected with the specified protection measures for data corruption: VehOnDRqCld\_No\_Cs - CRC based on Polynomial 0x1D of CRC-8-SAE J1850 is specified for Profile 1. byte0 of msg 0x375 VehOnDRqCld\_No\_Cnt - - 4 bits, Implements a Counter mechanism that is incremented every Send request and explicitly sent. - When the counter reaches the value 14 (0xE), then it shall restart with 0 for the next send request. Data ID - 0x0375 (Message ID is 0x375). Data elements: Big Endian byte1 to byte7 of msg 0x375. ECG shall following AUTOSAR 1A. |
| Rationale: |  |
| Safe State:  *(in case of categories “General”, “Metric”, “Non-E/E Requirement”, or “User Information”: if applicable)* | Module Safe State |
| Reduced Functionality and Interval:  *(if applicable;*  *in case of categories “Metric”, “Non-E/E Requirement”, “Maintain Safe State / Recovery” or “User Information”: not applicable;*  *in case of category “Reduced Functionality”: required)* |  |
| Fault tolerant time interval:  *(in case of categories “Metric” or “Maintain Safe State / Recovery”: not applicable;*  *in case of category “General”, “Reduced Functionality”, “Non-E/E Requirement”, or “User Information”: if applicable)* |  |
| Requirement Status |  |
| V&V method: | System test |
| V&V acceptance criteria:  *(UNV1 / UPV1, not in case of category “Non-E/E requirement)* |  |
| Allocated Element(s)/Component(s)/ Subsystem(s) *(if applicable)* |  |

Table 40: ECG Pub/Tx AUTOSAR 1A

### Requirement Derivation Diagram(s) for F-S-Req045 - OTA Feature Authenticates Cloud Connection

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

*Derive Technical Safety Requirements from Functional Safety Requirements.*

*Insert ‘Requirements Derivation Diagram/Tree’ or GSN here. Several diagrams may be required depending upon the size of the Item.*

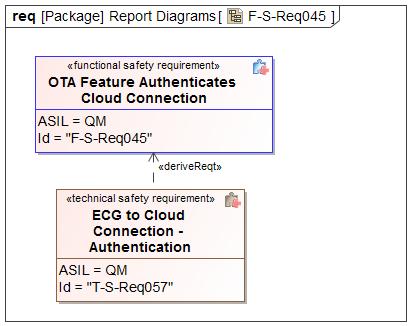


Figure 22 - Technical Safety Requirements Derivation Diagram for F-S-Req045

#### Technical Safety Requirements for F-S-Req045 - OTA Feature Authenticates Cloud Connection

*Describe Technical Safety Requirements from Functional Safety Requirements using Table 6 for each Technical Safety Requirement.*

| T-S-Req-ID: | T-S-Req057 - ECG to Cloud Connection - Authentication |
| --- | --- |
| External Reference *(optional)* |  |
| Category: | Safety Related Function |
| Safety Goal: | SG04 - Ensure Safe Verification of Activation  SG01 - Prevents Corruption of Existing Software |
| F-S-Req Ref.: | F-S-Req045 - OTA Feature Authenticates Cloud Connection |
| ASIL Classification:  *(in case of category “General”: if applicable, in case of category “Non-E/E Requirement”: not applicable)* | QM |
| Technical Safety Requirement Title: | ECG to Cloud Connection - Authentication |
| Technical Safety Requirement Text: | ECG to Cloud shall be a TLS connection |
| Rationale: |  |
| Safe State:  *(in case of categories “General”, “Metric”, “Non-E/E Requirement”, or “User Information”: if applicable)* | Normal |
| Reduced Functionality and Interval:  *(if applicable;*  *in case of categories “Metric”, “Non-E/E Requirement”, “Maintain Safe State / Recovery” or “User Information”: not applicable;*  *in case of category “Reduced Functionality”: required)* |  |
| Fault tolerant time interval:  *(in case of categories “Metric” or “Maintain Safe State / Recovery”: not applicable;*  *in case of category “General”, “Reduced Functionality”, “Non-E/E Requirement”, or “User Information”: if applicable)* |  |
| Requirement Status |  |
| V&V method: | System test |
| V&V acceptance criteria:  *(UNV1 / UPV1, not in case of category “Non-E/E requirement)* |  |
| Allocated Element(s)/Component(s)/ Subsystem(s) *(if applicable)* |  |

Table 41: ECG to Cloud Connection - Authentication

### Requirement Derivation Diagram(s) for F-S-Req074 - OTA Feature Command Inhibit Start

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

*Derive Technical Safety Requirements from Functional Safety Requirements.*

*Insert ‘Requirements Derivation Diagram/Tree’ or GSN here. Several diagrams may be required depending upon the size of the Item.*

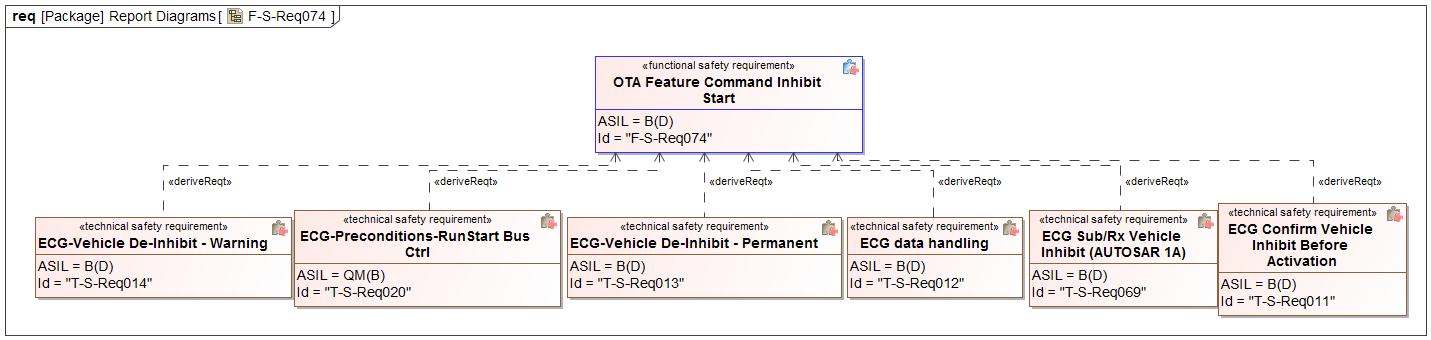


Figure 23 - Technical Safety Requirements Derivation Diagram for F-S-Req074

#### Technical Safety Requirements for F-S-Req074 - OTA Feature Command Inhibit Start

*Describe Technical Safety Requirements from Functional Safety Requirements using Table 6 for each Technical Safety Requirement.*

| T-S-Req-ID: | T-S-Req011 - ECG Confirm Vehicle Inhibit Before Activation |
| --- | --- |
| External Reference *(optional)* |  |
| Category: | Safety Related Function |
| Safety Goal: | SG03 - Ensure Safe Activation |
| F-S-Req Ref.: | F-S-Req074 - OTA Feature Command Inhibit Start |
| ASIL Classification:  *(in case of category “General”: if applicable, in case of category “Non-E/E Requirement”: not applicable)* | B(D) |
| Technical Safety Requirement Title: | ECG Confirm Vehicle Inhibit Before Activation |
| Technical Safety Requirement Text: | ECG shall receive VehStrtInhbt\_D\_Stat from BCM confirming the vehicle is inhibited due to CAVC command, before sending Authorize activation (OVTP) signal to Target ECUs. |
| Rationale: |  |
| Safe State:  *(in case of categories “General”, “Metric”, “Non-E/E Requirement”, or “User Information”: if applicable)* | Module Safe State |
| Reduced Functionality and Interval:  *(if applicable;*  *in case of categories “Metric”, “Non-E/E Requirement”, “Maintain Safe State / Recovery” or “User Information”: not applicable;*  *in case of category “Reduced Functionality”: required)* |  |
| Fault tolerant time interval:  *(in case of categories “Metric” or “Maintain Safe State / Recovery”: not applicable;*  *in case of category “General”, “Reduced Functionality”, “Non-E/E Requirement”, or “User Information”: if applicable)* |  |
| Requirement Status |  |
| V&V method: | System test |
| V&V acceptance criteria:  *(UNV1 / UPV1, not in case of category “Non-E/E requirement)* |  |
| Allocated Element(s)/Component(s)/ Subsystem(s) *(if applicable)* |  |

Table 42: ECG Confirm Vehicle Inhibit Before Activation

| T-S-Req-ID: | T-S-Req012 - ECG data handling |
| --- | --- |
| External Reference *(optional)* |  |
| Category: | Safety Related Function |
| Safety Goal: | SG03 - Ensure Safe Activation |
| F-S-Req Ref.: | F-S-Req074 - OTA Feature Command Inhibit Start |
| ASIL Classification:  *(in case of category “General”: if applicable, in case of category “Non-E/E Requirement”: not applicable)* | B(D) |
| Technical Safety Requirement Title: | ECG data handling |
| Technical Safety Requirement Text: | ECG shall verify following information  1. Vehicle Inhibit Type Flag 2. part numbers  3. CAVC commands. 4. SW update de-inhibit handling in case of failure activation:  a. Warning (De-Inibit with Degraded functionality)  b. Permanent Inhibit.(ECG shall NOT send De-inhibit) |
| Rationale: |  |
| Safe State:  *(in case of categories “General”, “Metric”, “Non-E/E Requirement”, or “User Information”: if applicable)* | Module Safe State |
| Reduced Functionality and Interval:  *(if applicable;*  *in case of categories “Metric”, “Non-E/E Requirement”, “Maintain Safe State / Recovery” or “User Information”: not applicable;*  *in case of category “Reduced Functionality”: required)* |  |
| Fault tolerant time interval:  *(in case of categories “Metric” or “Maintain Safe State / Recovery”: not applicable;*  *in case of category “General”, “Reduced Functionality”, “Non-E/E Requirement”, or “User Information”: if applicable)* |  |
| Requirement Status |  |
| V&V method: | System test |
| V&V acceptance criteria:  *(UNV1 / UPV1, not in case of category “Non-E/E requirement)* |  |
| Allocated Element(s)/Component(s)/ Subsystem(s) *(if applicable)* |  |

Table 43: ECG data handling

| T-S-Req-ID: | T-S-Req013 - ECG-Vehicle De-Inhibit - Permanent |
| --- | --- |
| External Reference *(optional)* |  |
| Category: | Safety Related Function |
| Safety Goal: | SG03 - Ensure Safe Activation |
| F-S-Req Ref.: | F-S-Req074 - OTA Feature Command Inhibit Start |
| ASIL Classification:  *(in case of category “General”: if applicable, in case of category “Non-E/E Requirement”: not applicable)* | B(D) |
| Technical Safety Requirement Title: | ECG-Vehicle De-Inhibit - Permanent |
| Technical Safety Requirement Text: | In Case of Permanent Inhibit Activation type, if ECG determines both Activation failure and Rollback failures, ECG shall not send Vehicle De-Inhibit Command to BCM (LS\_OTAM\_TO\_VSC\_VehDeInhbt\_Req). |
| Rationale: |  |
| Safe State:  *(in case of categories “General”, “Metric”, “Non-E/E Requirement”, or “User Information”: if applicable)* | Module Safe State |
| Reduced Functionality and Interval:  *(if applicable;*  *in case of categories “Metric”, “Non-E/E Requirement”, “Maintain Safe State / Recovery” or “User Information”: not applicable;*  *in case of category “Reduced Functionality”: required)* |  |
| Fault tolerant time interval:  *(in case of categories “Metric” or “Maintain Safe State / Recovery”: not applicable;*  *in case of category “General”, “Reduced Functionality”, “Non-E/E Requirement”, or “User Information”: if applicable)* |  |
| Requirement Status |  |
| V&V method: | System test |
| V&V acceptance criteria:  *(UNV1 / UPV1, not in case of category “Non-E/E requirement)* |  |
| Allocated Element(s)/Component(s)/ Subsystem(s) *(if applicable)* |  |

Table 44: ECG-Vehicle De-Inhibit - Permanent

| T-S-Req-ID: | T-S-Req014 - ECG-Vehicle De-Inhibit - Warning |
| --- | --- |
| External Reference *(optional)* |  |
| Category: | Safety Related Function |
| Safety Goal: | SG03 - Ensure Safe Activation |
| F-S-Req Ref.: | F-S-Req074 - OTA Feature Command Inhibit Start |
| ASIL Classification:  *(in case of category “General”: if applicable, in case of category “Non-E/E Requirement”: not applicable)* | B(D) |
| Technical Safety Requirement Title: | ECG-Vehicle De-Inhibit - Warning |
| Technical Safety Requirement Text: | In case of warning Activation type, if ECG Activation failure and Rollback failures occur, ECG shall send Vehicle De-Inhibit Command to BCM (LS\_OTAM\_TO\_VSC\_VehDeInhbt\_Req). |
| Rationale: |  |
| Safe State:  *(in case of categories “General”, “Metric”, “Non-E/E Requirement”, or “User Information”: if applicable)* | Module Safe State |
| Reduced Functionality and Interval:  *(if applicable;*  *in case of categories “Metric”, “Non-E/E Requirement”, “Maintain Safe State / Recovery” or “User Information”: not applicable;*  *in case of category “Reduced Functionality”: required)* |  |
| Fault tolerant time interval:  *(in case of categories “Metric” or “Maintain Safe State / Recovery”: not applicable;*  *in case of category “General”, “Reduced Functionality”, “Non-E/E Requirement”, or “User Information”: if applicable)* |  |
| Requirement Status |  |
| V&V method: | System test |
| V&V acceptance criteria:  *(UNV1 / UPV1, not in case of category “Non-E/E requirement)* |  |
| Allocated Element(s)/Component(s)/ Subsystem(s) *(if applicable)* |  |

Table 45: ECG-Vehicle De-Inhibit - Warning

| T-S-Req-ID: | T-S-Req020 - ECG-Preconditions-RunStart Bus Ctrl |
| --- | --- |
| External Reference *(optional)* |  |
| Category: | Safety Related Function |
| Safety Goal: | SG03 - Ensure Safe Activation |
| F-S-Req Ref.: | F-S-Req074 - OTA Feature Command Inhibit Start |
| ASIL Classification:  *(in case of category “General”: if applicable, in case of category “Non-E/E Requirement”: not applicable)* | **ASIL Override Rationale -** Preconditions are not Safety related  QM(B) |
| Technical Safety Requirement Title: | ECG-Preconditions-RunStart Bus Ctrl |
| Technical Safety Requirement Text: | ECG shall check preconditions required to send R/S Bus Control request to BCM.  If (VehOnSrc\_D\_Stat == “Off” AND Ignition Status = OFF) - OR (BCM Network Asleep AND Last Known received Ignition Status = OFF) |
| Rationale: |  |
| Safe State:  *(in case of categories “General”, “Metric”, “Non-E/E Requirement”, or “User Information”: if applicable)* | Module Safe State |
| Reduced Functionality and Interval:  *(if applicable;*  *in case of categories “Metric”, “Non-E/E Requirement”, “Maintain Safe State / Recovery” or “User Information”: not applicable;*  *in case of category “Reduced Functionality”: required)* |  |
| Fault tolerant time interval:  *(in case of categories “Metric” or “Maintain Safe State / Recovery”: not applicable;*  *in case of category “General”, “Reduced Functionality”, “Non-E/E Requirement”, or “User Information”: if applicable)* |  |
| Requirement Status |  |
| V&V method: | System test |
| V&V acceptance criteria:  *(UNV1 / UPV1, not in case of category “Non-E/E requirement)* |  |
| Allocated Element(s)/Component(s)/ Subsystem(s) *(if applicable)* |  |

Table 46: ECG-Preconditions-RunStart Bus Ctrl

| T-S-Req-ID: | T-S-Req069 - ECG Sub/Rx Vehicle Inhibit (AUTOSAR 1A) |
| --- | --- |
| External Reference *(optional)* |  |
| Category: | Safety Related Function |
| Safety Goal: | SG03 - Ensure Safe Activation |
| F-S-Req Ref.: | F-S-Req074 - OTA Feature Command Inhibit Start |
| ASIL Classification:  *(in case of category “General”: if applicable, in case of category “Non-E/E Requirement”: not applicable)* | B(D) |
| Technical Safety Requirement Title: | ECG Sub/Rx Vehicle Inhibit (AUTOSAR 1A) |
| Technical Safety Requirement Text: | ECG reception of the “VehStrtInhbt\_D\_Stat shall be E2E protected with the specified protection measures for data corruption: CrnkInhbt\_No\_Crc - CRC based on Polynomial 0x1D of CRC-8-SAE J1850 is specified for Profile 1. byte0 of msg 0x3A4 CrnkInhbt2\_No\_Cnt - - 4 bits, Implements a Counter mechanism that is incremented every Send request and explicitly sent. - When the counter reaches the value 14 (0xE), then it shall restart with 0 for the next send request. Data ID - 0x03A4 (Message ID is 0x3A4). Data elements: Big Endian byte1 to byte7 of msg 0x3A4. ECG shall following AUTOSAR 1A. |
| Rationale: |  |
| Safe State:  *(in case of categories “General”, “Metric”, “Non-E/E Requirement”, or “User Information”: if applicable)* | Module Safe State |
| Reduced Functionality and Interval:  *(if applicable;*  *in case of categories “Metric”, “Non-E/E Requirement”, “Maintain Safe State / Recovery” or “User Information”: not applicable;*  *in case of category “Reduced Functionality”: required)* |  |
| Fault tolerant time interval:  *(in case of categories “Metric” or “Maintain Safe State / Recovery”: not applicable;*  *in case of category “General”, “Reduced Functionality”, “Non-E/E Requirement”, or “User Information”: if applicable)* |  |
| Requirement Status |  |
| V&V method: | System test |
| V&V acceptance criteria:  *(UNV1 / UPV1, not in case of category “Non-E/E requirement)* |  |
| Allocated Element(s)/Component(s)/ Subsystem(s) *(if applicable)* |  |

Table 47: ECG Sub/Rx Vehicle Inhibit (AUTOSAR 1A)

### Requirement Derivation Diagram(s) for F-S-Req099 - OTA Feature Commands Rollback Upon Unsuccessful Activation

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

*Derive Technical Safety Requirements from Functional Safety Requirements.*

*Insert ‘Requirements Derivation Diagram/Tree’ or GSN here. Several diagrams may be required depending upon the size of the Item.*

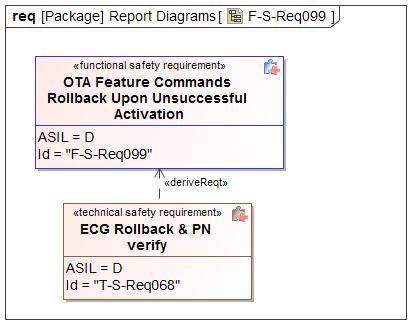


Figure 24 - Technical Safety Requirements Derivation Diagram for F-S-Req099

#### Technical Safety Requirements for F-S-Req099 - OTA Feature Commands Rollback Upon Unsuccessful Activation

*Describe Technical Safety Requirements from Functional Safety Requirements using Table 6 for each Technical Safety Requirement.*

| T-S-Req-ID: | T-S-Req068 - ECG Rollback & PN verify |
| --- | --- |
| External Reference *(optional)* |  |
| Category: | Safety Related Function |
| Safety Goal: | SG05 - Ensure Safe Rollback |
| F-S-Req Ref.: | F-S-Req099 - OTA Feature Commands Rollback Upon Unsuccessful Activation |
| ASIL Classification:  *(in case of category “General”: if applicable, in case of category “Non-E/E Requirement”: not applicable)* | D |
| Technical Safety Requirement Title: | ECG Rollback & PN verify |
| Technical Safety Requirement Text: | Covered in T-S-Req022 andT-S-Req023 |
| Rationale: |  |
| Safe State:  *(in case of categories “General”, “Metric”, “Non-E/E Requirement”, or “User Information”: if applicable)* | Module Safe State |
| Reduced Functionality and Interval:  *(if applicable;*  *in case of categories “Metric”, “Non-E/E Requirement”, “Maintain Safe State / Recovery” or “User Information”: not applicable;*  *in case of category “Reduced Functionality”: required)* |  |
| Fault tolerant time interval:  *(in case of categories “Metric” or “Maintain Safe State / Recovery”: not applicable;*  *in case of category “General”, “Reduced Functionality”, “Non-E/E Requirement”, or “User Information”: if applicable)* |  |
| Requirement Status |  |
| V&V method: | System test |
| V&V acceptance criteria:  *(UNV1 / UPV1, not in case of category “Non-E/E requirement)* |  |
| Allocated Element(s)/Component(s)/ Subsystem(s) *(if applicable)* |  |

Table 48: ECG Rollback & PN verify

### Requirement Derivation Diagram(s) for F-S-Req046 - OTA Feature Communicates E2E with the Cloud

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

*Derive Technical Safety Requirements from Functional Safety Requirements.*

*Insert ‘Requirements Derivation Diagram/Tree’ or GSN here. Several diagrams may be required depending upon the size of the Item.*

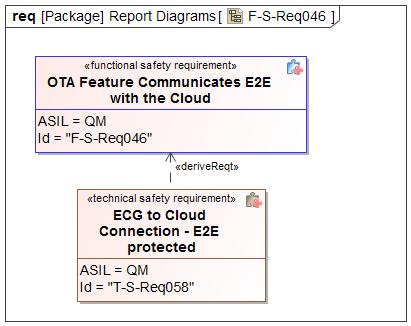


Figure 25 - Technical Safety Requirements Derivation Diagram for F-S-Req046

#### Technical Safety Requirements for F-S-Req046 - OTA Feature Communicates E2E with the Cloud

*Describe Technical Safety Requirements from Functional Safety Requirements using Table 6 for each Technical Safety Requirement.*

| T-S-Req-ID: | T-S-Req058 - ECG to Cloud Connection - E2E protected |
| --- | --- |
| External Reference *(optional)* |  |
| Category: | Safety Related Function |
| Safety Goal: | SG04 - Ensure Safe Verification of Activation  SG01 - Prevents Corruption of Existing Software |
| F-S-Req Ref.: | F-S-Req046 - OTA Feature Communicates E2E with the Cloud |
| ASIL Classification:  *(in case of category “General”: if applicable, in case of category “Non-E/E Requirement”: not applicable)* | QM |
| Technical Safety Requirement Title: | ECG to Cloud Connection - E2E protected |
| Technical Safety Requirement Text: | HTTPS channel shall be used to download the manifest and SYNCP encryption of all the payloads exchanged with the cloud |
| Rationale: |  |
| Safe State:  *(in case of categories “General”, “Metric”, “Non-E/E Requirement”, or “User Information”: if applicable)* | Normal |
| Reduced Functionality and Interval:  *(if applicable;*  *in case of categories “Metric”, “Non-E/E Requirement”, “Maintain Safe State / Recovery” or “User Information”: not applicable;*  *in case of category “Reduced Functionality”: required)* |  |
| Fault tolerant time interval:  *(in case of categories “Metric” or “Maintain Safe State / Recovery”: not applicable;*  *in case of category “General”, “Reduced Functionality”, “Non-E/E Requirement”, or “User Information”: if applicable)* |  |
| Requirement Status |  |
| V&V method: | System test |
| V&V acceptance criteria:  *(UNV1 / UPV1, not in case of category “Non-E/E requirement)* |  |
| Allocated Element(s)/Component(s)/ Subsystem(s) *(if applicable)* |  |

Table 49: ECG to Cloud Connection - E2E protected

### Requirement Derivation Diagram(s) for F-S-Req031 - OTA Feature Detects Data Corruption

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

*Derive Technical Safety Requirements from Functional Safety Requirements.*

*Insert ‘Requirements Derivation Diagram/Tree’ or GSN here. Several diagrams may be required depending upon the size of the Item.*

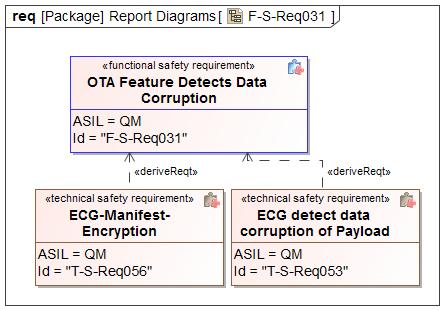


Figure 26 - Technical Safety Requirements Derivation Diagram for F-S-Req031

#### Technical Safety Requirements for F-S-Req031 - OTA Feature Detects Data Corruption

*Describe Technical Safety Requirements from Functional Safety Requirements using Table 6 for each Technical Safety Requirement.*

| T-S-Req-ID: | T-S-Req053 - ECG detect data corruption of Payload |
| --- | --- |
| External Reference *(optional)* |  |
| Category: | Safety Related Function |
| Safety Goal: | SG04 - Ensure Safe Verification of Activation  SG01 - Prevents Corruption of Existing Software |
| F-S-Req Ref.: | F-S-Req031 - OTA Feature Detects Data Corruption |
| ASIL Classification:  *(in case of category “General”: if applicable, in case of category “Non-E/E Requirement”: not applicable)* | QM |
| Technical Safety Requirement Title: | ECG detect data corruption of Payload |
| Technical Safety Requirement Text: | ECG shall verify the encryption of the payload received from the cloud by checking the Hashes and SYNCP encryption. |
| Rationale: |  |
| Safe State:  *(in case of categories “General”, “Metric”, “Non-E/E Requirement”, or “User Information”: if applicable)* | Normal |
| Reduced Functionality and Interval:  *(if applicable;*  *in case of categories “Metric”, “Non-E/E Requirement”, “Maintain Safe State / Recovery” or “User Information”: not applicable;*  *in case of category “Reduced Functionality”: required)* |  |
| Fault tolerant time interval:  *(in case of categories “Metric” or “Maintain Safe State / Recovery”: not applicable;*  *in case of category “General”, “Reduced Functionality”, “Non-E/E Requirement”, or “User Information”: if applicable)* |  |
| Requirement Status |  |
| V&V method: | System test |
| V&V acceptance criteria:  *(UNV1 / UPV1, not in case of category “Non-E/E requirement)* |  |
| Allocated Element(s)/Component(s)/ Subsystem(s) *(if applicable)* |  |

Table 50: ECG detect data corruption of Payload

| T-S-Req-ID: | T-S-Req056 - ECG-Manifest-Encryption |
| --- | --- |
| External Reference *(optional)* |  |
| Category: | Safety Related Function |
| Safety Goal: | SG04 - Ensure Safe Verification of Activation  SG01 - Prevents Corruption of Existing Software |
| F-S-Req Ref.: | F-S-Req031 - OTA Feature Detects Data Corruption |
| ASIL Classification:  *(in case of category “General”: if applicable, in case of category “Non-E/E Requirement”: not applicable)* | QM |
| Technical Safety Requirement Title: | ECG-Manifest-Encryption |
| Technical Safety Requirement Text: | The encrypted OTA Manifest shall have an HASH for each software file and shall be utilized by the ECG to verify that the file downloaded from the cloud was not corrupted. |
| Rationale: |  |
| Safe State:  *(in case of categories “General”, “Metric”, “Non-E/E Requirement”, or “User Information”: if applicable)* | Module Safe State |
| Reduced Functionality and Interval:  *(if applicable;*  *in case of categories “Metric”, “Non-E/E Requirement”, “Maintain Safe State / Recovery” or “User Information”: not applicable;*  *in case of category “Reduced Functionality”: required)* |  |
| Fault tolerant time interval:  *(in case of categories “Metric” or “Maintain Safe State / Recovery”: not applicable;*  *in case of category “General”, “Reduced Functionality”, “Non-E/E Requirement”, or “User Information”: if applicable)* |  |
| Requirement Status |  |
| V&V method: | System test |
| V&V acceptance criteria:  *(UNV1 / UPV1, not in case of category “Non-E/E requirement)* |  |
| Allocated Element(s)/Component(s)/ Subsystem(s) *(if applicable)* |  |

Table 51: ECG-Manifest-Encryption

### Requirement Derivation Diagram(s) for F-S-Req033 - OTA Feature Detects Invalid Software

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

*Derive Technical Safety Requirements from Functional Safety Requirements.*

*Insert ‘Requirements Derivation Diagram/Tree’ or GSN here. Several diagrams may be required depending upon the size of the Item.*

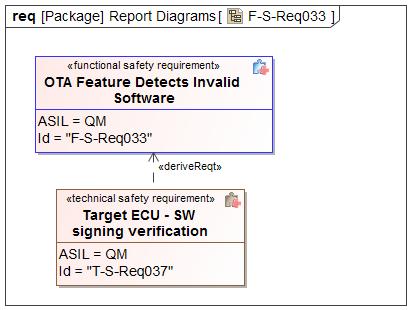


Figure 27 - Technical Safety Requirements Derivation Diagram for F-S-Req033

#### Technical Safety Requirements for F-S-Req033 - OTA Feature Detects Invalid Software

*Describe Technical Safety Requirements from Functional Safety Requirements using Table 6 for each Technical Safety Requirement.*

| T-S-Req-ID: | T-S-Req037 - Target ECU - SW signing verification |
| --- | --- |
| External Reference *(optional)* |  |
| Category: | Safety Related Function |
| Safety Goal: | SG04 - Ensure Safe Verification of Activation  SG02 - Prevents Flashing of Incorrect SW |
| F-S-Req Ref.: | F-S-Req033 - OTA Feature Detects Invalid Software |
| ASIL Classification:  *(in case of category “General”: if applicable, in case of category “Non-E/E Requirement”: not applicable)* | QM |
| Technical Safety Requirement Title: | Target ECU - SW signing verification |
| Technical Safety Requirement Text: | OTA Application in each ECU shall verify the software signature prior to installation |
| Rationale: |  |
| Safe State:  *(in case of categories “General”, “Metric”, “Non-E/E Requirement”, or “User Information”: if applicable)* | Module Safe State |
| Reduced Functionality and Interval:  *(if applicable;*  *in case of categories “Metric”, “Non-E/E Requirement”, “Maintain Safe State / Recovery” or “User Information”: not applicable;*  *in case of category “Reduced Functionality”: required)* |  |
| Fault tolerant time interval:  *(in case of categories “Metric” or “Maintain Safe State / Recovery”: not applicable;*  *in case of category “General”, “Reduced Functionality”, “Non-E/E Requirement”, or “User Information”: if applicable)* |  |
| Requirement Status |  |
| V&V method: | System test |
| V&V acceptance criteria:  *(UNV1 / UPV1, not in case of category “Non-E/E requirement)* |  |
| Allocated Element(s)/Component(s)/ Subsystem(s) *(if applicable)* |  |

Table 52: Target ECU - SW signing verification

### Requirement Derivation Diagram(s) for F-S-Req027 - OTA Feature Evaluates ACTIVATION Success

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

*Derive Technical Safety Requirements from Functional Safety Requirements.*

*Insert ‘Requirements Derivation Diagram/Tree’ or GSN here. Several diagrams may be required depending upon the size of the Item.*

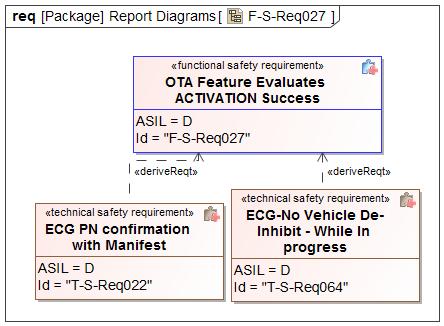


Figure 28 - Technical Safety Requirements Derivation Diagram for F-S-Req027

#### Technical Safety Requirements for F-S-Req027 - OTA Feature Evaluates ACTIVATION Success

*Describe Technical Safety Requirements from Functional Safety Requirements using Table 6 for each Technical Safety Requirement.*

| T-S-Req-ID: | T-S-Req022 - ECG PN confirmation with Manifest |
| --- | --- |
| External Reference *(optional)* |  |
| Category: | Safety Related Function |
| Safety Goal: | SG05 - Ensure Safe Rollback |
| F-S-Req Ref.: | F-S-Req027 - OTA Feature Evaluates ACTIVATION Success |
| ASIL Classification:  *(in case of category “General”: if applicable, in case of category “Non-E/E Requirement”: not applicable)* | D |
| Technical Safety Requirement Title: | ECG PN confirmation with Manifest |
| Technical Safety Requirement Text: | ECG shall read and compare the Part numbers of Target ECUs with the part numbers received in Manifest and Confirm Target ECU's successful activation. |
| Rationale: |  |
| Safe State:  *(in case of categories “General”, “Metric”, “Non-E/E Requirement”, or “User Information”: if applicable)* | Module Safe State |
| Reduced Functionality and Interval:  *(if applicable;*  *in case of categories “Metric”, “Non-E/E Requirement”, “Maintain Safe State / Recovery” or “User Information”: not applicable;*  *in case of category “Reduced Functionality”: required)* |  |
| Fault tolerant time interval:  *(in case of categories “Metric” or “Maintain Safe State / Recovery”: not applicable;*  *in case of category “General”, “Reduced Functionality”, “Non-E/E Requirement”, or “User Information”: if applicable)* |  |
| Requirement Status |  |
| V&V method: | System test |
| V&V acceptance criteria:  *(UNV1 / UPV1, not in case of category “Non-E/E requirement)* |  |
| Allocated Element(s)/Component(s)/ Subsystem(s) *(if applicable)* |  |

Table 53: ECG PN confirmation with Manifest

| T-S-Req-ID: | T-S-Req064 - ECG-No Vehicle De-Inhibit - While In progress |
| --- | --- |
| External Reference *(optional)* |  |
| Category: | Safety Related Function |
| Safety Goal: | SG05 - Ensure Safe Rollback |
| F-S-Req Ref.: | F-S-Req027 - OTA Feature Evaluates ACTIVATION Success |
| ASIL Classification:  *(in case of category “General”: if applicable, in case of category “Non-E/E Requirement”: not applicable)* | D |
| Technical Safety Requirement Title: | ECG-No Vehicle De-Inhibit - While In progress |
| Technical Safety Requirement Text: | "If a SW update requires Vehicle Inhibit, provided ECG receives "Vehicle Inhibit" and "Vehicle De-Inhibit" commands along with manifest. ECG shall not send "Vehicle De-Inhibit" while activation of one or more ECU is in progress." |
| Rationale: |  |
| Safe State:  *(in case of categories “General”, “Metric”, “Non-E/E Requirement”, or “User Information”: if applicable)* | Module Safe State |
| Reduced Functionality and Interval:  *(if applicable;*  *in case of categories “Metric”, “Non-E/E Requirement”, “Maintain Safe State / Recovery” or “User Information”: not applicable;*  *in case of category “Reduced Functionality”: required)* |  |
| Fault tolerant time interval:  *(in case of categories “Metric” or “Maintain Safe State / Recovery”: not applicable;*  *in case of category “General”, “Reduced Functionality”, “Non-E/E Requirement”, or “User Information”: if applicable)* |  |
| Requirement Status |  |
| V&V method: | System test |
| V&V acceptance criteria:  *(UNV1 / UPV1, not in case of category “Non-E/E requirement)* |  |
| Allocated Element(s)/Component(s)/ Subsystem(s) *(if applicable)* |  |

Table 54: ECG-No Vehicle De-Inhibit - While In progress

### Requirement Derivation Diagram(s) for F-S-Req041 - OTA Feature Evaluates Roll Back Success

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

*Derive Technical Safety Requirements from Functional Safety Requirements.*

*Insert ‘Requirements Derivation Diagram/Tree’ or GSN here. Several diagrams may be required depending upon the size of the Item.*

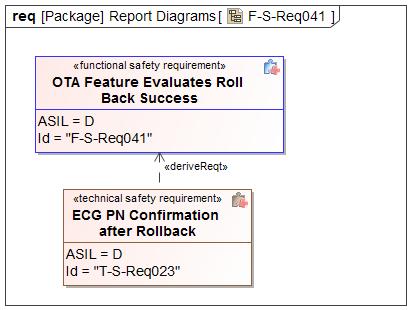


Figure 29 - Technical Safety Requirements Derivation Diagram for F-S-Req041

#### Technical Safety Requirements for F-S-Req041 - OTA Feature Evaluates Roll Back Success

*Describe Technical Safety Requirements from Functional Safety Requirements using Table 6 for each Technical Safety Requirement.*

| T-S-Req-ID: | T-S-Req023 - ECG PN Confirmation after Rollback |
| --- | --- |
| External Reference *(optional)* |  |
| Category: | Safety Related Function |
| Safety Goal: | SG05 - Ensure Safe Rollback |
| F-S-Req Ref.: | F-S-Req041 - OTA Feature Evaluates Roll Back Success |
| ASIL Classification:  *(in case of category “General”: if applicable, in case of category “Non-E/E Requirement”: not applicable)* | D |
| Technical Safety Requirement Title: | ECG PN Confirmation after Rollback |
| Technical Safety Requirement Text: | ECG shall read part numbers after a positive response to the Rollback command and compare the Part numbers of Target ECUs with the part numbers received in Manifest and Confirm Target ECU's successful rollback. |
| Rationale: |  |
| Safe State:  *(in case of categories “General”, “Metric”, “Non-E/E Requirement”, or “User Information”: if applicable)* | Module Safe State |
| Reduced Functionality and Interval:  *(if applicable;*  *in case of categories “Metric”, “Non-E/E Requirement”, “Maintain Safe State / Recovery” or “User Information”: not applicable;*  *in case of category “Reduced Functionality”: required)* |  |
| Fault tolerant time interval:  *(in case of categories “Metric” or “Maintain Safe State / Recovery”: not applicable;*  *in case of category “General”, “Reduced Functionality”, “Non-E/E Requirement”, or “User Information”: if applicable)* |  |
| Requirement Status |  |
| V&V method: | System test |
| V&V acceptance criteria:  *(UNV1 / UPV1, not in case of category “Non-E/E requirement)* |  |
| Allocated Element(s)/Component(s)/ Subsystem(s) *(if applicable)* |  |

Table 55: ECG PN Confirmation after Rollback

### Requirement Derivation Diagram(s) for F-S-Req052 - OTA Feature Informs the Cloud of Data Corruption

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

*Derive Technical Safety Requirements from Functional Safety Requirements.*

*Insert ‘Requirements Derivation Diagram/Tree’ or GSN here. Several diagrams may be required depending upon the size of the Item.*

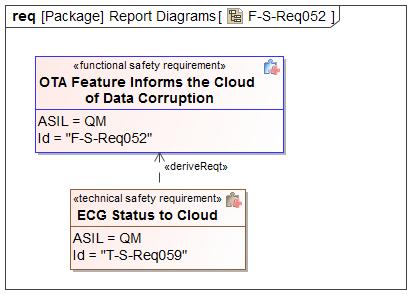


Figure 30 - Technical Safety Requirements Derivation Diagram for F-S-Req052

#### Technical Safety Requirements for F-S-Req052 - OTA Feature Informs the Cloud of Data Corruption

*Describe Technical Safety Requirements from Functional Safety Requirements using Table 6 for each Technical Safety Requirement.*

| T-S-Req-ID: | T-S-Req059 - ECG Status to Cloud |
| --- | --- |
| External Reference *(optional)* |  |
| Category: | Safety Related Function |
| Safety Goal: | SG04 - Ensure Safe Verification of Activation  SG01 - Prevents Corruption of Existing Software |
| F-S-Req Ref.: | F-S-Req052 - OTA Feature Informs the Cloud of Data Corruption |
| ASIL Classification:  *(in case of category “General”: if applicable, in case of category “Non-E/E Requirement”: not applicable)* | QM |
| Technical Safety Requirement Title: | ECG Status to Cloud |
| Technical Safety Requirement Text: | ECG Status Manager shall report corruption or other errors to the cloud thru a SYNCP JSON payload |
| Rationale: |  |
| Safe State:  *(in case of categories “General”, “Metric”, “Non-E/E Requirement”, or “User Information”: if applicable)* | Normal |
| Reduced Functionality and Interval:  *(if applicable;*  *in case of categories “Metric”, “Non-E/E Requirement”, “Maintain Safe State / Recovery” or “User Information”: not applicable;*  *in case of category “Reduced Functionality”: required)* |  |
| Fault tolerant time interval:  *(in case of categories “Metric” or “Maintain Safe State / Recovery”: not applicable;*  *in case of category “General”, “Reduced Functionality”, “Non-E/E Requirement”, or “User Information”: if applicable)* |  |
| Requirement Status |  |
| V&V method: | System test |
| V&V acceptance criteria:  *(UNV1 / UPV1, not in case of category “Non-E/E requirement)* |  |
| Allocated Element(s)/Component(s)/ Subsystem(s) *(if applicable)* |  |

Table 56: ECG Status to Cloud

### Requirement Derivation Diagram(s) for F-S-Req020 - OTA Governance Board shall review and approve the software that is to be pushed via OTA

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

*Derive Technical Safety Requirements from Functional Safety Requirements.*

*Insert ‘Requirements Derivation Diagram/Tree’ or GSN here. Several diagrams may be required depending upon the size of the Item.*

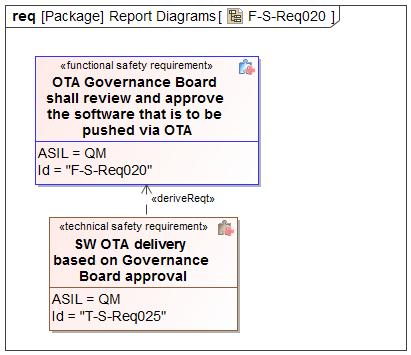


Figure 31 - Technical Safety Requirements Derivation Diagram for F-S-Req020

#### Technical Safety Requirements for F-S-Req020 - OTA Governance Board shall review and approve the software that is to be pushed via OTA

*Describe Technical Safety Requirements from Functional Safety Requirements using Table 6 for each Technical Safety Requirement.*

| T-S-Req-ID: | T-S-Req025 - SW OTA delivery based on Governance Board approval |
| --- | --- |
| External Reference *(optional)* |  |
| Category: | Safety Related Function |
| Safety Goal: | SG02 - Prevents Flashing of Incorrect SW |
| F-S-Req Ref.: | F-S-Req020 - OTA Governance Board shall review and approve the software that is to be pushed via OTA |
| ASIL Classification:  *(in case of category “General”: if applicable, in case of category “Non-E/E Requirement”: not applicable)* | **ASIL Override Rationale -** It is achieved by Cloud and Manual process  QM |
| Technical Safety Requirement Title: | SW OTA delivery based on Governance Board approval |
| Technical Safety Requirement Text: | After SW has been uploaded to FENIX, it shall hold the SW in a wait state until it has been reviewed and approved by the Governance Board. |
| Rationale: |  |
| Safe State:  *(in case of categories “General”, “Metric”, “Non-E/E Requirement”, or “User Information”: if applicable)* | Module Safe State |
| Reduced Functionality and Interval:  *(if applicable;*  *in case of categories “Metric”, “Non-E/E Requirement”, “Maintain Safe State / Recovery” or “User Information”: not applicable;*  *in case of category “Reduced Functionality”: required)* |  |
| Fault tolerant time interval:  *(in case of categories “Metric” or “Maintain Safe State / Recovery”: not applicable;*  *in case of category “General”, “Reduced Functionality”, “Non-E/E Requirement”, or “User Information”: if applicable)* |  |
| Requirement Status |  |
| V&V method: | System test |
| V&V acceptance criteria:  *(UNV1 / UPV1, not in case of category “Non-E/E requirement)* |  |
| Allocated Element(s)/Component(s)/ Subsystem(s) *(if applicable)* |  |

Table 57: SW OTA delivery based on Governance Board approval

### Requirement Derivation Diagram(s) for F-S-Req083 - Other ECU SW (ASIL C/D) Verify Safe Vehicle State

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

*Derive Technical Safety Requirements from Functional Safety Requirements.*

*Insert ‘Requirements Derivation Diagram/Tree’ or GSN here. Several diagrams may be required depending upon the size of the Item.*

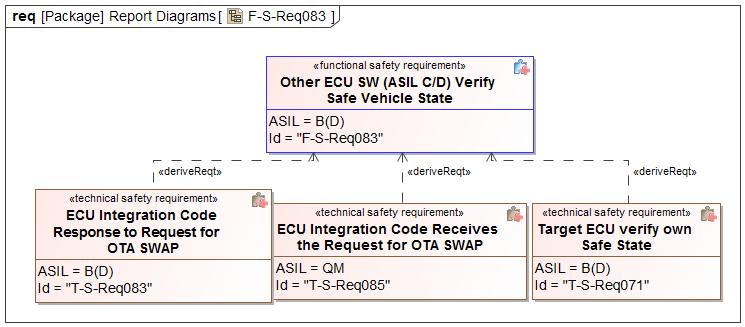


Figure 32 - Technical Safety Requirements Derivation Diagram for F-S-Req083

#### Technical Safety Requirements for F-S-Req083 - Other ECU SW (ASIL C/D) Verify Safe Vehicle State

*Describe Technical Safety Requirements from Functional Safety Requirements using Table 6 for each Technical Safety Requirement.*

| T-S-Req-ID: | T-S-Req071 - Target ECU verify own Safe State |
| --- | --- |
| External Reference *(optional)* |  |
| Category: | Safety Related Function |
| Safety Goal: | SG03 - Ensure Safe Activation |
| F-S-Req Ref.: | F-S-Req083 - Other ECU SW (ASIL C/D) Verify Safe Vehicle State |
| ASIL Classification:  *(in case of category “General”: if applicable, in case of category “Non-E/E Requirement”: not applicable)* | B(D) |
| Technical Safety Requirement Title: | Target ECU verify own Safe State |
| Technical Safety Requirement Text: | ASIL C/D rated Target ECUs shall verify their own safe state prior to activation, independent of the vehicle inhibit signals. |
| Rationale: |  |
| Safe State:  *(in case of categories “General”, “Metric”, “Non-E/E Requirement”, or “User Information”: if applicable)* | Module Safe State |
| Reduced Functionality and Interval:  *(if applicable;*  *in case of categories “Metric”, “Non-E/E Requirement”, “Maintain Safe State / Recovery” or “User Information”: not applicable;*  *in case of category “Reduced Functionality”: required)* |  |
| Fault tolerant time interval:  *(in case of categories “Metric” or “Maintain Safe State / Recovery”: not applicable;*  *in case of category “General”, “Reduced Functionality”, “Non-E/E Requirement”, or “User Information”: if applicable)* |  |
| Requirement Status |  |
| V&V method: | System test |
| V&V acceptance criteria:  *(UNV1 / UPV1, not in case of category “Non-E/E requirement)* |  |
| Allocated Element(s)/Component(s)/ Subsystem(s) *(if applicable)* |  |

Table 58: Target ECU verify own Safe State

| T-S-Req-ID: | T-S-Req083 - ECU Integration Code Response to Request for OTA SWAP |
| --- | --- |
| External Reference *(optional)* |  |
| Category: | Safety Related Function |
| Safety Goal: | SG03 - Ensure Safe Activation |
| F-S-Req Ref.: | F-S-Req083 - Other ECU SW (ASIL C/D) Verify Safe Vehicle State |
| ASIL Classification:  *(in case of category “General”: if applicable, in case of category “Non-E/E Requirement”: not applicable)* | B(D) |
| Technical Safety Requirement Title: | ECU Integration Code Response to Request for OTA SWAP |
| Technical Safety Requirement Text: | Upon receiving a Request for OTA SWAP, the ECU Integration Code shall verify module conditions before requesting activation from the VMEM (Additional Vector Code). |
| Rationale: | Since the OTA App cannot check the module status by itself, it relies on the ECU Integration Code to check the module is secured for OTA activation. |
| Safe State:  *(in case of categories “General”, “Metric”, “Non-E/E Requirement”, or “User Information”: if applicable)* | Module Safe State |
| Reduced Functionality and Interval:  *(if applicable;*  *in case of categories “Metric”, “Non-E/E Requirement”, “Maintain Safe State / Recovery” or “User Information”: not applicable;*  *in case of category “Reduced Functionality”: required)* |  |
| Fault tolerant time interval:  *(in case of categories “Metric” or “Maintain Safe State / Recovery”: not applicable;*  *in case of category “General”, “Reduced Functionality”, “Non-E/E Requirement”, or “User Information”: if applicable)* | 1 Second |
| Requirement Status |  |
| V&V method: | System test |
| V&V acceptance criteria:  *(UNV1 / UPV1, not in case of category “Non-E/E requirement)* | The ECU Integration Code verifies module conditions before requesting activation from the VMEM (Additional Vector Code). |
| Allocated Element(s)/Component(s)/ Subsystem(s) *(if applicable)* |  |

Table 59: ECU Integration Code Response to Request for OTA SWAP

| T-S-Req-ID: | T-S-Req085 - ECU Integration Code Receives the Request for OTA SWAP |
| --- | --- |
| External Reference *(optional)* |  |
| Category: | Safety Related Function |
| Safety Goal: | SG03 - Ensure Safe Activation |
| F-S-Req Ref.: | F-S-Req083 - Other ECU SW (ASIL C/D) Verify Safe Vehicle State |
| ASIL Classification:  *(in case of category “General”: if applicable, in case of category “Non-E/E Requirement”: not applicable)* | **ASIL Override Rationale -** Failure to recieve the OTA SWAP command would not lead to a violation of the safety goal  QM |
| Technical Safety Requirement Title: | ECU Integration Code Receives the Request for OTA SWAP |
| Technical Safety Requirement Text: | The ECU Integration Code shall receive the Request for OTA SWAP from the OTA Handler. |
| Rationale: | To prevent switchover at an unsafe time. For ASIL QM to ASIL B, the crank inhibit is enough to verify the vehicle safe state. The higher ASIL rated modules would have to perform independent safe state verification. |
| Safe State:  *(in case of categories “General”, “Metric”, “Non-E/E Requirement”, or “User Information”: if applicable)* | Normal |
| Reduced Functionality and Interval:  *(if applicable;*  *in case of categories “Metric”, “Non-E/E Requirement”, “Maintain Safe State / Recovery” or “User Information”: not applicable;*  *in case of category “Reduced Functionality”: required)* |  |
| Fault tolerant time interval:  *(in case of categories “Metric” or “Maintain Safe State / Recovery”: not applicable;*  *in case of category “General”, “Reduced Functionality”, “Non-E/E Requirement”, or “User Information”: if applicable)* | - |
| Requirement Status |  |
| V&V method: | System test |
| V&V acceptance criteria:  *(UNV1 / UPV1, not in case of category “Non-E/E requirement)* | ECU Integration Code receives the Request for OTA SWAP. |
| Allocated Element(s)/Component(s)/ Subsystem(s) *(if applicable)* |  |

Table 60: ECU Integration Code Receives the Request for OTA SWAP

### Requirement Derivation Diagram(s) for F-S-Req094 - Other ECU SW Executes Active Memory

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

*Derive Technical Safety Requirements from Functional Safety Requirements.*

*Insert ‘Requirements Derivation Diagram/Tree’ or GSN here. Several diagrams may be required depending upon the size of the Item.*

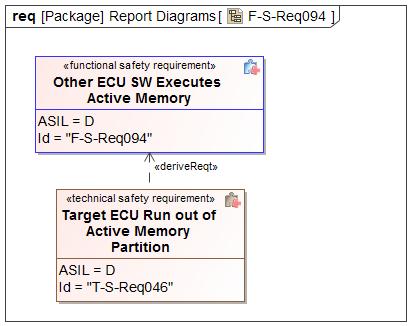


Figure 33 - Technical Safety Requirements Derivation Diagram for F-S-Req094

#### Technical Safety Requirements for F-S-Req094 - Other ECU SW Executes Active Memory

*Describe Technical Safety Requirements from Functional Safety Requirements using Table 6 for each Technical Safety Requirement.*

| T-S-Req-ID: | T-S-Req046 - Target ECU Run out of Active Memory Partition |
| --- | --- |
| External Reference *(optional)* |  |
| Category: | Safety Related Function |
| Safety Goal: | SG01 - Prevents Corruption of Existing Software |
| F-S-Req Ref.: | F-S-Req094 - Other ECU SW Executes Active Memory |
| ASIL Classification:  *(in case of category “General”: if applicable, in case of category “Non-E/E Requirement”: not applicable)* | D |
| Technical Safety Requirement Title: | Target ECU Run out of Active Memory Partition |
| Technical Safety Requirement Text: | During Activation, All modules shall execute from new Active Memory partition. |
| Rationale: |  |
| Safe State:  *(in case of categories “General”, “Metric”, “Non-E/E Requirement”, or “User Information”: if applicable)* | Module Safe State |
| Reduced Functionality and Interval:  *(if applicable;*  *in case of categories “Metric”, “Non-E/E Requirement”, “Maintain Safe State / Recovery” or “User Information”: not applicable;*  *in case of category “Reduced Functionality”: required)* |  |
| Fault tolerant time interval:  *(in case of categories “Metric” or “Maintain Safe State / Recovery”: not applicable;*  *in case of category “General”, “Reduced Functionality”, “Non-E/E Requirement”, or “User Information”: if applicable)* |  |
| Requirement Status |  |
| V&V method: | System test |
| V&V acceptance criteria:  *(UNV1 / UPV1, not in case of category “Non-E/E requirement)* |  |
| Allocated Element(s)/Component(s)/ Subsystem(s) *(if applicable)* |  |

Table 61: Target ECU Run out of Active Memory Partition

### Requirement Derivation Diagram(s) for F-S-Req090 - Other ECU SW Executes OTA Without Affecting Basic Function

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

*Derive Technical Safety Requirements from Functional Safety Requirements.*

*Insert ‘Requirements Derivation Diagram/Tree’ or GSN here. Several diagrams may be required depending upon the size of the Item.*

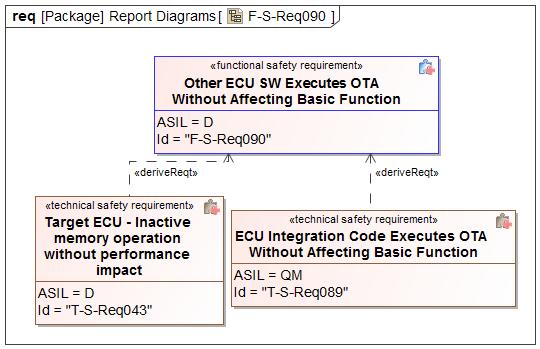


Figure 34 - Technical Safety Requirements Derivation Diagram for F-S-Req090

#### Technical Safety Requirements for F-S-Req090 - Other ECU SW Executes OTA Without Affecting Basic Function

*Describe Technical Safety Requirements from Functional Safety Requirements using Table 6 for each Technical Safety Requirement.*

Please see the Technical Safety Requirement table for [T-S-Req043](#_ef001077f89eb670b62410a6f7500699) displayed under the Functional Safety Requirement F-S-Req087.

| T-S-Req-ID: | T-S-Req089 - ECU Integration Code Executes OTA Without Affecting Basic Function |
| --- | --- |
| External Reference *(optional)* |  |
| Category: | Safety Related Function |
| Safety Goal: | SG01 - Prevents Corruption of Existing Software |
| F-S-Req Ref.: | F-S-Req090 - Other ECU SW Executes OTA Without Affecting Basic Function |
| ASIL Classification:  *(in case of category “General”: if applicable, in case of category “Non-E/E Requirement”: not applicable)* | **ASIL Override Rationale -** Based on the lower priority of the OTA protocol, and the designed partitioning of module resources; it is not realistically possible for OTA execution to violate our safety goal.  QM |
| Technical Safety Requirement Title: | ECU Integration Code Executes OTA Without Affecting Basic Function |
| Technical Safety Requirement Text: | The ECU Integration Code shall execute OTA commands without affecting execution of current software including any peripheral communication. |
| Rationale: | To avoid disrupting normal existing current software functions. (e.g. flash when idle and ensure OTA is pre-emptible). |
| Safe State:  *(in case of categories “General”, “Metric”, “Non-E/E Requirement”, or “User Information”: if applicable)* | Normal |
| Reduced Functionality and Interval:  *(if applicable;*  *in case of categories “Metric”, “Non-E/E Requirement”, “Maintain Safe State / Recovery” or “User Information”: not applicable;*  *in case of category “Reduced Functionality”: required)* |  |
| Fault tolerant time interval:  *(in case of categories “Metric” or “Maintain Safe State / Recovery”: not applicable;*  *in case of category “General”, “Reduced Functionality”, “Non-E/E Requirement”, or “User Information”: if applicable)* | - |
| Requirement Status |  |
| V&V method: | System test |
| V&V acceptance criteria:  *(UNV1 / UPV1, not in case of category “Non-E/E requirement)* | 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 current SW. Check that MMOTA is pre-emptible by the current SW. MMOTA should not progress or execute when the CPU load is close to maximum. |
| Allocated Element(s)/Component(s)/ Subsystem(s) *(if applicable)* |  |

Table 62: ECU Integration Code Executes OTA Without Affecting Basic Function

### Requirement Derivation Diagram(s) for F-S-Req085 - Other ECU SW Performs Activation Within Time Limit

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

*Derive Technical Safety Requirements from Functional Safety Requirements.*

*Insert ‘Requirements Derivation Diagram/Tree’ or GSN here. Several diagrams may be required depending upon the size of the Item.*

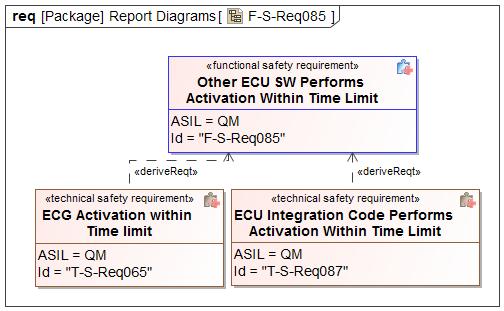


Figure 35 - Technical Safety Requirements Derivation Diagram for F-S-Req085

#### Technical Safety Requirements for F-S-Req085 - Other ECU SW Performs Activation Within Time Limit

*Describe Technical Safety Requirements from Functional Safety Requirements using Table 6 for each Technical Safety Requirement.*

| T-S-Req-ID: | T-S-Req065 - ECG Activation within Time limit |
| --- | --- |
| External Reference *(optional)* |  |
| Category: | Safety Related Function |
| Safety Goal: | SG05 - Ensure Safe Rollback |
| F-S-Req Ref.: | F-S-Req085 - Other ECU SW Performs Activation Within Time Limit |
| ASIL Classification:  *(in case of category “General”: if applicable, in case of category “Non-E/E Requirement”: not applicable)* | QM |
| Technical Safety Requirement Title: | ECG Activation within Time limit |
| Technical Safety Requirement Text: | ECUs shall not take more than 90s to activate and respond with the part numbers. |
| Rationale: |  |
| Safe State:  *(in case of categories “General”, “Metric”, “Non-E/E Requirement”, or “User Information”: if applicable)* | Module Safe State |
| Reduced Functionality and Interval:  *(if applicable;*  *in case of categories “Metric”, “Non-E/E Requirement”, “Maintain Safe State / Recovery” or “User Information”: not applicable;*  *in case of category “Reduced Functionality”: required)* |  |
| Fault tolerant time interval:  *(in case of categories “Metric” or “Maintain Safe State / Recovery”: not applicable;*  *in case of category “General”, “Reduced Functionality”, “Non-E/E Requirement”, or “User Information”: if applicable)* |  |
| Requirement Status |  |
| V&V method: | System test |
| V&V acceptance criteria:  *(UNV1 / UPV1, not in case of category “Non-E/E requirement)* |  |
| Allocated Element(s)/Component(s)/ Subsystem(s) *(if applicable)* |  |

Table 63: ECG Activation within Time limit

| T-S-Req-ID: | T-S-Req087 - ECU Integration Code Performs Activation Within Time Limit |
| --- | --- |
| External Reference *(optional)* |  |
| Category: | Safety Related Function |
| Safety Goal: | SG05 - Ensure Safe Rollback |
| F-S-Req Ref.: | F-S-Req085 - Other ECU SW Performs Activation Within Time Limit |
| ASIL Classification:  *(in case of category “General”: if applicable, in case of category “Non-E/E Requirement”: not applicable)* | **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 |
| Technical Safety Requirement Title: | ECU Integration Code Performs Activation Within Time Limit |
| Technical Safety Requirement Text: | The ECU Integration Code shall perform ACTIVATION within a deterministic time, “ACTIVATION\_TIMEOUT”, after it receives the correct "ACTIVATION" command via the OTA Handler. |
| Rationale: | To ensure that the ECU Integration Code performs activation within a pre-definable time and also so as to make it possible for the OTA Feature to verify ACTIVATION after that time window elapses. |
| Safe State:  *(in case of categories “General”, “Metric”, “Non-E/E Requirement”, or “User Information”: if applicable)* | Normal |
| Reduced Functionality and Interval:  *(if applicable;*  *in case of categories “Metric”, “Non-E/E Requirement”, “Maintain Safe State / Recovery” or “User Information”: not applicable;*  *in case of category “Reduced Functionality”: required)* |  |
| Fault tolerant time interval:  *(in case of categories “Metric” or “Maintain Safe State / Recovery”: not applicable;*  *in case of category “General”, “Reduced Functionality”, “Non-E/E Requirement”, or “User Information”: if applicable)* | - |
| Requirement Status |  |
| V&V method: | System test |
| V&V acceptance criteria:  *(UNV1 / UPV1, not in case of category “Non-E/E requirement)* | Verify the ECU Integration Code 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 |
| Allocated Element(s)/Component(s)/ Subsystem(s) *(if applicable)* |  |

Table 64: ECU Integration Code Performs Activation Within Time Limit

### Requirement Derivation Diagram(s) for F-S-Req088 - Other ECU SW Prevents Active Memory Erasing or Writing

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

*Derive Technical Safety Requirements from Functional Safety Requirements.*

*Insert ‘Requirements Derivation Diagram/Tree’ or GSN here. Several diagrams may be required depending upon the size of the Item.*

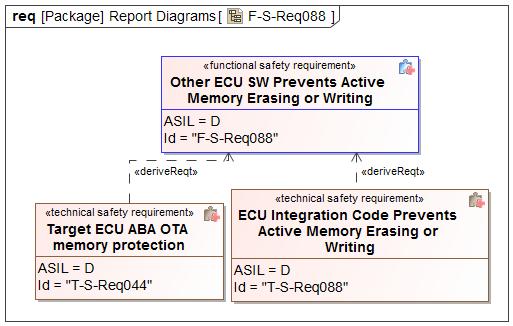


Figure 36 - Technical Safety Requirements Derivation Diagram for F-S-Req088

#### Technical Safety Requirements for F-S-Req088 - Other ECU SW Prevents Active Memory Erasing or Writing

*Describe Technical Safety Requirements from Functional Safety Requirements using Table 6 for each Technical Safety Requirement.*

| T-S-Req-ID: | T-S-Req044 - Target ECU ABA OTA memory protection |
| --- | --- |
| External Reference *(optional)* |  |
| Category: | Safety Related Function |
| Safety Goal: | SG01 - Prevents Corruption of Existing Software |
| F-S-Req Ref.: | F-S-Req088 - Other ECU SW Prevents Active Memory Erasing or Writing |
| ASIL Classification:  *(in case of category “General”: if applicable, in case of category “Non-E/E Requirement”: not applicable)* | D |
| Technical Safety Requirement Title: | Target ECU ABA OTA memory protection |
| Technical Safety Requirement Text: | For ECUs that use A/B/A OTA the Primary Bootloader shall not make any calls to write or erase into active memory of the OS while the OS is running, except for authorized activation and/or rollback. |
| Rationale: |  |
| Safe State:  *(in case of categories “General”, “Metric”, “Non-E/E Requirement”, or “User Information”: if applicable)* | Module Safe State |
| Reduced Functionality and Interval:  *(if applicable;*  *in case of categories “Metric”, “Non-E/E Requirement”, “Maintain Safe State / Recovery” or “User Information”: not applicable;*  *in case of category “Reduced Functionality”: required)* |  |
| Fault tolerant time interval:  *(in case of categories “Metric” or “Maintain Safe State / Recovery”: not applicable;*  *in case of category “General”, “Reduced Functionality”, “Non-E/E Requirement”, or “User Information”: if applicable)* |  |
| Requirement Status |  |
| V&V method: | System test |
| V&V acceptance criteria:  *(UNV1 / UPV1, not in case of category “Non-E/E requirement)* |  |
| Allocated Element(s)/Component(s)/ Subsystem(s) *(if applicable)* |  |

Table 65: Target ECU ABA OTA memory protection

| T-S-Req-ID: | T-S-Req088 - ECU Integration Code Prevents Active Memory Erasing or Writing |
| --- | --- |
| External Reference *(optional)* |  |
| Category: | Safety Related Function |
| Safety Goal: | SG01 - Prevents Corruption of Existing Software |
| F-S-Req Ref.: | F-S-Req088 - Other ECU SW Prevents Active Memory Erasing or Writing |
| ASIL Classification:  *(in case of category “General”: if applicable, in case of category “Non-E/E Requirement”: not applicable)* | D |
| Technical Safety Requirement Title: | ECU Integration Code Prevents Active Memory Erasing or Writing |
| Technical Safety Requirement Text: | The ECU Integration Code shall prevent writing or erasing memory sections containing the "active software". |
| Rationale: | To avoid disrupting higher priority ECU functions (like safety critical functions), the Integration code ignores OTA App commands affecting active software |
| Safe State:  *(in case of categories “General”, “Metric”, “Non-E/E Requirement”, or “User Information”: if applicable)* | Module Safe State |
| Reduced Functionality and Interval:  *(if applicable;*  *in case of categories “Metric”, “Non-E/E Requirement”, “Maintain Safe State / Recovery” or “User Information”: not applicable;*  *in case of category “Reduced Functionality”: required)* |  |
| Fault tolerant time interval:  *(in case of categories “Metric” or “Maintain Safe State / Recovery”: not applicable;*  *in case of category “General”, “Reduced Functionality”, “Non-E/E Requirement”, or “User Information”: if applicable)* | 1 Second |
| Requirement Status |  |
| V&V method: | System test |
| V&V acceptance criteria:  *(UNV1 / UPV1, not in case of category “Non-E/E requirement)* | 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. |
| Allocated Element(s)/Component(s)/ Subsystem(s) *(if applicable)* |  |

Table 66: ECU Integration Code Prevents Active Memory Erasing or Writing

### Requirement Derivation Diagram(s) for F-S-Req081 - Other ECU SW Provides Part Number

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

*Derive Technical Safety Requirements from Functional Safety Requirements.*

*Insert ‘Requirements Derivation Diagram/Tree’ or GSN here. Several diagrams may be required depending upon the size of the Item.*

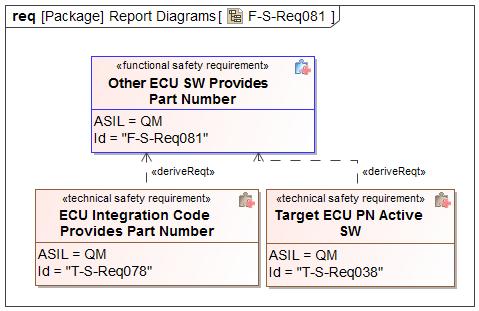


Figure 37 - Technical Safety Requirements Derivation Diagram for F-S-Req081

#### Technical Safety Requirements for F-S-Req081 - Other ECU SW Provides Part Number

*Describe Technical Safety Requirements from Functional Safety Requirements using Table 6 for each Technical Safety Requirement.*

| T-S-Req-ID: | T-S-Req038 - Target ECU PN Active SW |
| --- | --- |
| External Reference *(optional)* |  |
| Category: | Safety Related Function |
| Safety Goal: | SG02 - Prevents Flashing of Incorrect SW |
| F-S-Req Ref.: | F-S-Req081 - Other ECU SW Provides Part Number |
| ASIL Classification:  *(in case of category “General”: if applicable, in case of category “Non-E/E Requirement”: not applicable)* | QM |
| Technical Safety Requirement Title: | Target ECU PN Active SW |
| Technical Safety Requirement Text: | Each ECU shall provide part numbers of the active software to the ECG |
| Rationale: |  |
| Safe State:  *(in case of categories “General”, “Metric”, “Non-E/E Requirement”, or “User Information”: if applicable)* | Module Safe State |
| Reduced Functionality and Interval:  *(if applicable;*  *in case of categories “Metric”, “Non-E/E Requirement”, “Maintain Safe State / Recovery” or “User Information”: not applicable;*  *in case of category “Reduced Functionality”: required)* |  |
| Fault tolerant time interval:  *(in case of categories “Metric” or “Maintain Safe State / Recovery”: not applicable;*  *in case of category “General”, “Reduced Functionality”, “Non-E/E Requirement”, or “User Information”: if applicable)* |  |
| Requirement Status |  |
| V&V method: | System test |
| V&V acceptance criteria:  *(UNV1 / UPV1, not in case of category “Non-E/E requirement)* |  |
| Allocated Element(s)/Component(s)/ Subsystem(s) *(if applicable)* |  |

Table 67: Target ECU PN Active SW

| T-S-Req-ID: | T-S-Req078 - ECU Integration Code Provides Part Number |
| --- | --- |
| External Reference *(optional)* |  |
| Category: | Safety Related Function |
| Safety Goal: | SG02 - Prevents Flashing of Incorrect SW |
| F-S-Req Ref.: | F-S-Req081 - Other ECU SW Provides Part Number |
| ASIL Classification:  *(in case of category “General”: if applicable, in case of category “Non-E/E Requirement”: not applicable)* | **ASIL Override Rationale -** A failure to send the part number would not violate the safety goal of the module.  QM |
| Technical Safety Requirement Title: | ECU Integration Code Provides Part Number |
| Technical Safety Requirement Text: | Upon request from the OTA Handler in the Target ECU, the ECU Integration Code shall provide the correct part number. |
| Rationale: | To ensure proper software distribution and validation with the correct part numbers |
| Safe State:  *(in case of categories “General”, “Metric”, “Non-E/E Requirement”, or “User Information”: if applicable)* | Normal |
| Reduced Functionality and Interval:  *(if applicable;*  *in case of categories “Metric”, “Non-E/E Requirement”, “Maintain Safe State / Recovery” or “User Information”: not applicable;*  *in case of category “Reduced Functionality”: required)* |  |
| Fault tolerant time interval:  *(in case of categories “Metric” or “Maintain Safe State / Recovery”: not applicable;*  *in case of category “General”, “Reduced Functionality”, “Non-E/E Requirement”, or “User Information”: if applicable)* | - |
| Requirement Status |  |
| V&V method: | System test |
| V&V acceptance criteria:  *(UNV1 / UPV1, not in case of category “Non-E/E requirement)* | Check if the correct part number is being sent |
| Allocated Element(s)/Component(s)/ Subsystem(s) *(if applicable)* |  |

Table 68: ECU Integration Code Provides Part Number

### Requirement Derivation Diagram(s) for F-S-Req078 - Other ECU SW Reports ACTIVATION Readiness

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

*Derive Technical Safety Requirements from Functional Safety Requirements.*

*Insert ‘Requirements Derivation Diagram/Tree’ or GSN here. Several diagrams may be required depending upon the size of the Item.*

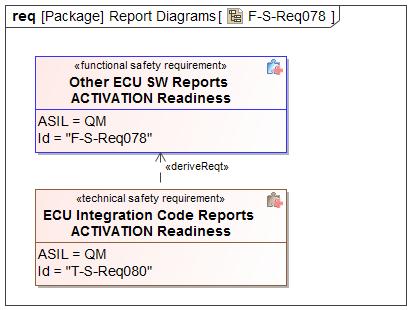


Figure 38 - Technical Safety Requirements Derivation Diagram for F-S-Req078

#### Technical Safety Requirements for F-S-Req078 - Other ECU SW Reports ACTIVATION Readiness

*Describe Technical Safety Requirements from Functional Safety Requirements using Table 6 for each Technical Safety Requirement.*

| T-S-Req-ID: | T-S-Req080 - ECU Integration Code Reports ACTIVATION Readiness |
| --- | --- |
| External Reference *(optional)* |  |
| Category: | Safety Related Function |
| Safety Goal: | SG04 - Ensure Safe Verification of Activation |
| F-S-Req Ref.: | F-S-Req078 - Other ECU SW Reports ACTIVATION Readiness |
| ASIL Classification:  *(in case of category “General”: if applicable, in case of category “Non-E/E Requirement”: not applicable)* | **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 |
| Technical Safety Requirement Title: | ECU Integration Code Reports ACTIVATION Readiness |
| Technical Safety Requirement Text: | Upon request via the OTA Handler in the Target ECU, the ECU Integration Code shall report their readiness to perform the ACTIVATION function. |
| Rationale: | To ensure proper coordination and scheduling of the activation |
| Safe State:  *(in case of categories “General”, “Metric”, “Non-E/E Requirement”, or “User Information”: if applicable)* | Normal |
| Reduced Functionality and Interval:  *(if applicable;*  *in case of categories “Metric”, “Non-E/E Requirement”, “Maintain Safe State / Recovery” or “User Information”: not applicable;*  *in case of category “Reduced Functionality”: required)* |  |
| Fault tolerant time interval:  *(in case of categories “Metric” or “Maintain Safe State / Recovery”: not applicable;*  *in case of category “General”, “Reduced Functionality”, “Non-E/E Requirement”, or “User Information”: if applicable)* | - |
| Requirement Status |  |
| V&V method: | System test |
| V&V acceptance criteria:  *(UNV1 / UPV1, not in case of category “Non-E/E requirement)* | Check if ECU Integration Code coomunicate readiness |
| Allocated Element(s)/Component(s)/ Subsystem(s) *(if applicable)* |  |

Table 69: ECU Integration Code Reports ACTIVATION Readiness

## Derivation of Fault Tolerant Time

*Derive Fault Tolerant Time for Technical Safety Requirements from Functional Safety Requirements.*

| **F-S-Req-ID** | Fault tolerant time interval (from Functional Safety Concept) | **Component/ Subsystem or [Communication Channel]1** | **T-S-Req-ID1** | **Fault tolerant time interval for T-S-Req. or**  **[Time Delay of Communication Channel]**  Explanation (if necessary)  [Note (if necessary)]1 |
| --- | --- | --- | --- | --- |
| F-S-Req078 | N/A | IV-MMOTA | T-S-Req080 | - |
| Other ECU SW | T-S-Req080 | - |
| Target ECU | T-S-Req080 | - |
| F-S-Req081 | N/A | IV-MMOTA | T-S-Req078 | - |
| Other ECU SW | T-S-Req078 | - |
| Target ECU | T-S-Req078 | - |
| F-S-Req083 | 1 second | IV-MMOTA | T-S-Req083 | 1 Second |
| T-S-Req085 | - |
| Other ECU SW | T-S-Req083 | 1 Second |
| T-S-Req085 | - |
| Target ECU | T-S-Req083 | 1 Second |
| T-S-Req085 | - |
| F-S-Req085 | N/A | IV-MMOTA | T-S-Req087 | - |
| Other ECU SW | T-S-Req087 | - |
| Target ECU | T-S-Req087 | - |
| F-S-Req088 | 1 second | IV-MMOTA | T-S-Req088 | 1 Second |
| Other ECU SW | T-S-Req088 | 1 Second |
| Target ECU | T-S-Req088 | 1 Second |
| F-S-Req090 | 1 second | IV-MMOTA | T-S-Req089 | - |
| Other ECU SW | T-S-Req089 | - |
| Target ECU | T-S-Req089 | - |
| F-S-Req093 | 1 second | IV-MMOTA | T-S-Req079 | - |
| T-S-Req086 | - |
| T-S-Req090 | 1 Second |
| OTA App | T-S-Req079 | - |
| T-S-Req086 | - |
| T-S-Req090 | 1 Second |
| Target ECU | T-S-Req079 | - |
| T-S-Req086 | - |
| T-S-Req090 | 1 Second |

Table 70: Fault tolerant time interval allocation to Elements/Components/Subsystems

## Derivation of Reduced Functionality (interval) (optional)

*Derive Reduced Functionality (interval) for Technical Safety Requirements from Functional Safety Requirements.*

No Functional Safety Requirement and no Technical Safety Requirement with Reduced Functionality Interval specified.

## HW Metric Requirements - Derivation and Rationale

#### Element/Component/Subsystem contribution to the maximum probability of safety goal violation due to random hardware failures (PMHF)

*Assign component contribution to the maximum probability of safety goal violation due to random hardware failures (PMHF).*

| **Safety Goal** | ASIL | **Safety Goal PMHF** | **Element/ Component/ Subsystem** | **Component PMHF** | **T-S-Req.- ID**  **Category: Metric** | **T-S-Req.-IDs**  **Category:**  **Safety Related Function** |
| --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  |
|  |  |  |  |
|  |  |  |  |  |  |  |

Table 71: PMHF derivation

*Give rationale for assigned PMHF portions.*

### Single Point Faults and Latent Faults Metric

*Assign Single Point Fault Metric target values and Latent Faults Metric target values to components.*

| **Safety Goal** | ASIL | **Safety Goal SPF** | **Element/ Component/ Subsystem** | **Component Fault Detection Coverage** | **T-S-Req.-IDs**  **Category: Metric** | **T-S-Req.-IDs**  **Category:  Fault Detection or**  **Safety Related Function** |
| --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  |
|  |  |  |  |
|  |  |  |  |  | | |

Table 72: Single Point Fault Metric derivation

| **Safety Goal** | ASIL | **Safety Goal LFM** | **Element/ Component/ Subsystem** | **Component Fault Detection Coverage** | **T-S-Req.-IDs**  **Category: Metric** | **T-S-Req.-IDs**  **Category:  Latent Fault Detection** |
| --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  |
|  |  |  |  |
|  |  |  |  |  |  |  |

Table 73: Latent Fault Metric derivation

*Give rationale for SPF and LFM values.*

## Allocation

*Document the allocation of Technical Safety Requirements if helpful.*

Technical Safety Requirement Components not specified.

## ASIL Decomposition Requirements - Derivation and Rationale (optional)

*If ASIL decomposition is applied, describe the decomposition in this section*

ASIL Decompositions not specified.

### Safety Related Parameters

*List the all parameters used in the Safety Requirements Specification.*

*This could be new parameters introduced in the Safety Requirements Specification, or parameters already introduced in the Functional Safety Concept and reused in the Safety Requirements Specification. For the second ones, add/update constraints, if necessary.*

*Note: The refined parameters can be documented in other documents as authoritative source of information for the implementation, e.g. in the, SW Requirements, documentation for performance tuning etc.*

| **ÎD** | **Parameter name**  **(Description)** | **Used in Reqs** | **Preliminary Value or Range** | **Constraints**  (for preliminary Value) |
| --- | --- | --- | --- | --- |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

Table 74: Parameter

## Requirements concerning the ability to configure a system by calibration data

*Describe System configuration requirements.*

## Cascading Technical Safety Requirements

*The project specific document setup shall be used for exchanging requirements with the component/subsystem provider. This section describes information has to be requested from the component/subsystem provider depending on the requirement category.*

### Element/Subsystem/Component architecture (including redundancy)

The element/component/subsystem provider shall define the architecture / redundancy concept including:

* a description of the architecture / redundancy concept
* a rationale why the redundancy used is suitable
* the type of redundancy, e.g. information redundancy, time redundancy, hardware redundancy or software redundancy
* a statement if Diverse or Homogeneous redundancy is used

*Note: Diverse redundancy is useful for mitigating risk from a systematic cause. Homogenous redundancy is useful for mitigating risk from random faults.*

* description of measures for handling potential dependent failures

*Note: The analysis has to be conducted according to ISO°26262-9, Clause 6 "Analysis of dependent failures".*

This information shall be made available for review purposes to Ford.

The document “FFSD07 Supplier Assessment Report” includes a reference to the relevant document.

### Internal Fault Handling

For all Technical Safety Requirements in this category, the element/component/subsystem provider shall define:

* Measures related to the detection of faults in the element/component/subsystem itself
* Details on internal fault reaction

If latent fault handling is described in this section, for these requirements the element/component/subsystem provider shall also define:

* Avoidance of latent faults
* Multiple Point Fault Detection Interval

This information shall be made available for review purposes to Ford.

The document “FFSD07 Supplier Assessment Report” includes a reference to the relevant document.

### Latent Fault Handling

For all Technical Safety Requirements in this category, the element/component/subsystem provider shall define:

* Measures related to the detection and indication of faults in the element/component/subsystem itself
* Avoidance of latent faults
* Multiple Point Fault Detection Interval
* Details on fault reaction

This information shall be made available for review purposes to Ford.

**The document “FFSD07 Supplier Assessment Report” includes a reference to the relevant document.**

## Reference to description of other functions of the system

*If other functions in addition to those Technical Safety Requirements specified in sections 3.8 and following are performed by the system or by elements, these functions shall be referenced.*

*Example: Other requirements coming from ECE rules, FMVSS or company platform strategies.*

# System Design

| **Element/Component/Subsystem** | **References to the other Requirements and Design Documents** |
| --- | --- |
|  |  |
|  |  |

Table 75: Elements/Components/Subsystems Design References

# Requirements for Production, Operation, Service and Decommissioning

**Production Plan:**

*Define or reference all safety related content for the production plan.*

**Owner’s Manual:**

*Define or reference all safety related content for owner’s manual an add references to related technical safety requirements.*

**Service Manual:**

*Define or reference all safety related content for service manual an add references to related technical safety requirements.*

**Decommissioning:**

*Define or reference all safety related content for decommissioning an add references to related technical safety requirements.*

# Execution and Results of Verification Review

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

Table 76: 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 appropriately?** | | **Yes /**  **No** |
| --- | --- | --- |
| Input from System Design, Item Definition / Feature Document, and Functional Safety Concept  *(GPDS: UNV0/UPV0, GTDS: <AR>)* | External Interfaces |  |
|  | Constraints |  |
|  | Technical Block Diagram |  |
|  | Functional Overview of Elements/Components/Subsystems |  |
|  | Implementation Details of Internal Interfaces |  |
|  | System Level architecture (including redundancy) |  |
| Technical Safety Requirements Specification  Technical Safety Requirements Derivation | Derivation of Technical Safety Requirements (without V&V acceptance criteria)  *(GPDS: UNV0/UPV0, GTDS: <AR>)* |  |
| Definition of Technical Safety Requirements V&V acceptance criteria  *(GPDS: UNV1/UPV1)* |  |
| Derivation of Fault Tolerant Time  *(GPDS: UNV0/UPV0, GTDS: <AR>)* |  |
| Derivation of Reduced Functionality (interval)  *(GPDS: UNV0/UPV0, GTDS: <AR>)* |  |
| Each Technical Safety Requirement   * contains all required attributes (except “V&V acceptance criteria”)   *(GPDS: UNV0/UPV0, GTDS: <AR>)* |  |
| Each Technical Safety Requirement   * is simple, atomic, verifiable, necessary, achievable, and traceable   *(GPDS: UNV0/UPV0, GTDS: <AR>)* |  |
| Each Technical Safety Requirement   * is accepted by the element/component/subsystem provider   *(GPDS: UNV0/UPV0, GTDS: <AR>)* |  |
| Constraints are transformed into requirements  *(GPDS: UNV0/UPV0, GTDS: <AR>)* |  |
| HW Metric Requirements - Derivation and Rationale   * the metric values assigned to the elements/components/subsystems fulfil the Safety Goal metric requirements.   *(GPDS: UNV0/UPV0, GTDS: <AR>)* |  |
| ASIL Decomposition (Optional)  *(GPDS: UNV0/UPV0, GTDS: <AR>)* |  |
| Safety Related Parameters  *(GPDS: UNV0/UPV0, GTDS: <AR>)* |  |
| Requirements concerning the ability to configure a system by calibration data are defined  *(GPDS: UNV0/UPV0, GTDS: <AR>)* |  |
| Each Technical Safety Requirement  can be verified  *(GPDS: UNV0/UPV0, GTDS: <AR>)* |  |
| The Technical Safety Requirements are consistent and complete regarding the System Design, including "Response to Stimuli".  *(GPDS: UNV0/UPV0, GTDS: <AR>)* |  |
| Technical Safety Requirements necessary for the achievement of the Functional Safety Requirement are generated and documented.  *(GPDS: UNV0/UPV0, GTDS: <AR>)* |  |
| Description of other functions of the system  *(GPDS: UNV0/UPV0, GTDS: <AR>)* |  |  |
| System Design  *(GPDS: UNV0/UPV0, GTDS: <AR>)* | Technical Safety Requirements included in the system design specification(s).  Aligned with Technical Safety Requirements  System Design developed in accordance with requirements related to:   * System architectural design constraints * Avoidance of systematic faults * Usage of well-trusted design principles * Measures for control of random hardware failures during operation * Allocation to hardware and software * Hardware-Software Interface Specification   *(see guideline for “FFSD 04 Safety Requirements Specification”)* |  |
| Requirements for Operation, Service and Decommissioning  *(GPDS: UNV0/UPV0, GTDS: <AR>)* | Requirements for Operation and Service completed |  |
| Technical Safety Requirements on Elements/Components/Subsystems  *(GPDS: UNV0/UPV0, GTDS: <AR>)* | V&V acceptance criteria |  |

Table 77: Checklist for Completeness of Safety Requirements Specification

## Review Exceptions / Deviations / Findings

*Insert project-relevant Input*

## Further Actions / Decisions

*Insert project-relevant Input*