|  |  | |  |
| --- | --- | --- | --- |
|  |  | |  |
|  |  | |  |
|  | Template | |  |
|  |  | |  |
|  | Safety Requirements Specification | |  |
|  |  | |  |
|  | including  Safety Requirements Specification  System Architectural Design Specification | |  |
|  |  |
|  |  |
|  |  | |  |
| Commodities | **Low Beam Including Manual and Auto Lamp** | |  |
| Program(s) | **Core** | |  |
| VSEM ID(s) | **F000998** | |  |
| Document Version | SRS3 | |  |
| Document  Owner | Feature Document: AMATTOS4  FuSA: LSILV152 | |  |
|  |  | |  |
|  |  | |  |
|  | 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: | 9.1 |  |
|  | SysML Report Template Version: | 9.1.0 |  |

**Change Control**

|  |  |  |  |
| --- | --- | --- | --- |
| **Version** | **Date** | **Author** | **Change / Remark** |
| SRS1 | 2021-08-26 | lsilv152 | Updated SRS |
| SRS2 | 2021-10-25 | lsilv152 | Update TSR 1.2.1.2.1; Added TSR1.2.1.2.2; Removed TSR1.2.5 and 1.2.9. |
| SRS3 | 2022-02-16 | lsilv152 | Review TSR with Lighting Team. |

*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 "FFSD04 Safety Requirement Specification".*

*To create the document, the corresponding guideline shall be used by Ford. 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 for Ford usage in the "Functional Safety Toolbox":*

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

*Format-Options*

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

# Content

[1. Introduction 6](#_Toc97621550)

[1.1 Purpose 6](#_Toc97621551)

[1.2 Input documents 6](#_Toc97621552)

[2. Input from System Design, Item Definition / Feature Document [FFSD 01.1(0)] and Functional Safety Concept [FFSD 03] 7](#_Toc97621553)

[2.1 Implementation Details of External Interfaces 7](#_Toc97621554)

[2.2 Constraints 8](#_Toc97621555)

[2.3 Technical Block Diagram 8](#_Toc97621556)

[2.4 Functional Overview of Elements/Components/Subsystems 9](#_Toc97621557)

[2.4.1 Elements/Components/Systems within System Boundary 9](#_Toc97621558)

[2.4.2 Elements/Components/Systems outside System Boundary 10](#_Toc97621559)

[2.5 Implementation Details of Internal Interfaces 11](#_Toc97621560)

[2.6 System Level Architecture (including redundancy) 12](#_Toc97621561)

[2.6.1 Safety Goal: SG01 (ASIL B) 12](#_Toc97621562)

[3. Technical Safety Requirements Specification 13](#_Toc97621563)

[3.1 Technical Safety Requirements 13](#_Toc97621564)

[3.1.1 Requirement Derivation Diagram(s) for FSR1 - Driver Inputs as request for Low Beam lamps activation 13](#_Toc97621565)

[3.1.2 Requirement Derivation Diagram(s) for TSR1.2.1.2 - Verify headlamp switch input - CAN 24](#_Toc97621566)

[3.1.3 Requirement Derivation Diagram(s) for FSR2 - Arbitration logic working properly for Low Beam activation 25](#_Toc97621567)

[3.1.4 Requirement Derivation Diagram(s) for FSR3 - Activation of light sources 51](#_Toc97621568)

[3.2 Timing Specification 57](#_Toc97621569)

[3.2.1 Fault Tolerant Time Interval (FTTI) Identification 57](#_Toc97621570)

[3.2.1.1 Safety Goal X 61](#_Toc97621571)

[3.2.2 Fault Handling Time Specification 62](#_Toc97621572)

[3.2.2.1 Achieving the FHT for SG X 62](#_Toc97621573)

[3.3 Derivation of Reduced Functionality Interval (optional) 62](#_Toc97621574)

[3.4 Operating Modes Overview (optional) 62](#_Toc97621575)

[3.5 HW Metric Requirements - Derivation and Rationale 65](#_Toc97621576)

[3.5.1 Element/Component/System contribution to the maximum probability of safety goal violation due to random hardware failures (PMHF) 65](#_Toc97621577)

[3.5.2 Single Point Faults and Latent Faults Metric 65](#_Toc97621578)

[3.6 Allocation (optional) 66](#_Toc97621579)

[3.7 ASIL Decomposition- Derivation and Rationale (optional) 67](#_Toc97621580)

[3.8 Safety Related Parameters 67](#_Toc97621581)

[3.9 Cascading Technical Safety Requirements 68](#_Toc97621582)

[4. Requirements for Production, Operation, Service and Decommissioning 68](#_Toc97621583)

[5. Safety Analysis 68](#_Toc97621584)

[*6.* Execution and Results of Verification Review 69](#_Toc97621585)

[6.1 Verification Review 69](#_Toc97621586)

[6.1.1 Verification Review of Safety Requirements Specification 70](#_Toc97621587)

[6.1.2 Verification Review of Safety Analyses of Safety Requirements Specification (optional) 73](#_Toc97621588)

[6.2 Review Exceptions / Deviations / Findings 75](#_Toc97621589)

[6.3 Further Actions / Decisions 75](#_Toc97621590)

[7. Execution and Results of Confirmation Review 76](#_Toc97621591)

[7.1 Confirmation Review 76](#_Toc97621592)

[7.2 Review Exceptions / Deviations / Findings 77](#_Toc97621593)

[7.3 Further Actions / Decisions 77](#_Toc97621594)

[Appendix A 78](#_Toc97621595)

[A.1 Definitions, Abbreviations and Acronyms 78](#_Toc97621596)

# List of tables

[Table 1: Document Scope 6](#_Toc97621597)

[Table 2: Input 6](#_Toc97621598)

[Table 3: External Interfaces with Respect to the System Boundary 7](#_Toc97621599)

[Table 4: Elements/Components/Subsystems within the System Boundary 10](#_Toc97621600)

[Table 5: Relevant Systems (Elements/Components/Subsystems) outside System Boundary 10](#_Toc97621601)

[Table 6: Implementation Details of Internal Interfaces 11](#_Toc97621602)

[Table 7: System Level architecture (including redundancy) for SG01 12](#_Toc97621603)

[Table 8: Verify validity of headlamp switch low beam request - (headlamp switch type Variant 2) 14](#_Toc97621604)

[Table 9: Verify validity of headlamp switch low beam request - 5 15](#_Toc97621605)

[Table 10: Verify validity Relative LIN E2E signal 16](#_Toc97621606)

[Table 11: Verify headlamp switch input - CAN 17](#_Toc97621607)

[Table 12: Verify headlamp switch input 18](#_Toc97621608)

[Table 13: Verify headlamp switch input (Headlamp Switch Type Variant 2) - LIN 19](#_Toc97621609)

[Table 14: Headlamp Switch (Headlamp Switch Type Variant 3) CAN E2E 20](#_Toc97621610)

[Table 15: Latch the switch input (Headlamp Switch Type 3) 21](#_Toc97621611)

[Table 16: Self Diagnosis of headlamp switch (headlamp switch type 3) 22](#_Toc97621612)

[Table 17: Debounce headlamp switch input (Headlamp Switch Type Variant 3) 23](#_Toc97621613)

[Table 18: Report Headlamp Switch Request Determination Fault 25](#_Toc97621614)

[Table 19: Verify validity of headlamp switch configuration 27](#_Toc97621615)

[Table 20: Verify validity of headlamp switch type request output 28](#_Toc97621616)

[Table 21: Verify validity of headlamp switch type request control 29](#_Toc97621617)

[Table 22: Verify validity of headlamp switch type request state 30](#_Toc97621618)

[Table 23: Verify validity of headlamp switch type request - SW2\_stat 31](#_Toc97621619)

[Table 24: Verify validity of headlamp switch type request - SW3\_stat 32](#_Toc97621620)

[Table 25: Ensure validity of headlamp request during ignition status 33](#_Toc97621621)

[Table 26: Verify the arbitrated headlamp request - 1 34](#_Toc97621622)

[Table 27: Verify the arbitrated headlamp request - 2 35](#_Toc97621623)

[Table 28: Verify the arbitrated headlamp request - 3 36](#_Toc97621624)

[Table 29: Verify the arbitrated headlamp request - 4 37](#_Toc97621625)

[Table 30: Verify validity of headlamp switch low beam request - 2 38](#_Toc97621626)

[Table 31: Verify validity of headlamp switch low beam request - 4 39](#_Toc97621627)

[Table 32: Verify validity of headlamp switch low beam request - 6 40](#_Toc97621628)

[Table 33: Verify validity of headlamp switch low beam request - 3 41](#_Toc97621629)

[Table 34: Verify validity of headlamp switch low beam request - 1 42](#_Toc97621630)

[Table 35: Verify validity of ALS faults 43](#_Toc97621631)

[Table 36: Verify validity condition from AUTOLAMP deactivation. 44](#_Toc97621632)

[Table 37: Verify vehicle speed E2E 45](#_Toc97621633)

[Table 38: Verify the output device - 2 46](#_Toc97621634)

[Table 39: Verify the output device - 1 47](#_Toc97621635)

[Table 40: Verify validity Absolute LIN E2E signal 48](#_Toc97621636)

[Table 41: Verify the arbitrated control of low beams to output device - Left 49](#_Toc97621637)

[Table 42: Verify the arbitrated control of low beams to output device - Right 50](#_Toc97621638)

[Table 43: Separate circuits output drivers 52](#_Toc97621639)

[Table 44: Separate LED driver module for left and right 53](#_Toc97621640)

[Table 45: Fault handling for headlamps 54](#_Toc97621641)

[Table 46: Operating temperature range 55](#_Toc97621642)

[Table 47: Operating Voltage range 56](#_Toc97621643)

[Table 48: LDM fail safe state 57](#_Toc97621644)

[Table 49: Fault tolerant time interval allocation to Elements/Components/Subsystems 60](#_Toc97621645)

[Table 50: Safety Mechanism Y HMT Summary 61](#_Toc97621646)

[Table 51: Safety Mechanism Y MBMT Summary 61](#_Toc97621647)

[Table 52: FTTI Summary 61](#_Toc97621648)

[Table 53: FHT Summary 62](#_Toc97621649)

[Table 54: Operating Modes 64](#_Toc97621650)

[Table 55: PMHF derivation 65](#_Toc97621651)

[Table 56: Single Point Fault Metric derivation 65](#_Toc97621652)

[Table 57: Latent Fault Metric derivation 65](#_Toc97621653)

[Table 58: Allocation of Technical Safety Requirements 67](#_Toc97621654)

[Table 59: Parameter 67](#_Toc97621655)

[Table 60: Review Table 69](#_Toc97621656)

[Table 61: Checklist for Completeness of Safety Requirements Specification 73](#_Toc97621657)

[Table 62: Review Table 76](#_Toc97621658)

[Table 63: Definitions, Abbreviations and Acronyms 78](#_Toc97621659)

# List of Figures

[Figure 1 - Technical Safety Requirements Derivation Diagram for FSR1 – Driver Inputs as request for Low Beam lamps activation 13](#_Toc97621660)

[Figure 2 - Technical Safety Requirements Derivation Diagram for FSR1(2) – Driver Inputs as request for Low Beam lamps activation 13](#_Toc97621661)

[Figure 3- Technical Safety Requirements Derivation Diagram for TSR1.2.1.2 – Verify headlamp switch input - CAN 24](#_Toc97621662)

[Figure 4 - Technical Safety Requirements Derivation Diagram for FSR2 – Arbitration logic working properly for Low Beam activation 25](#_Toc97621663)

[Figure 5 - Technical Safety Requirements Derivation Diagram for FSR2(2) – Arbitration logic working properly for Low Beam activation 26](#_Toc97621664)

[Figure 6 - Technical Safety Requirements Derivation Diagram for FSR2(3) – Arbitration logic working properly for Low Beam activation 26](#_Toc97621665)

[Figure 7 - Technical Safety Requirements Derivation Diagram for FSR3 - Activation of light sources – Activation of light sources 51](#_Toc97621666)

[Figure 8: Operating Modes Overview Diagram 63](#_Toc97621667)

# 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:

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

Table 1: Document Scope

## Input documents

|  |  |  |  |
| --- | --- | --- | --- |
|  | Document Name | File Name/Reference | Version |
| **FFSD / Other Input**  **(Required)** | FFSD01.1 Item Definition /  FFSD01.10 Feature Document | low\_beams\_fd\_rev\_02 | - |
| FFSD02 Hazard Analysis and Risk Assessment | VDOC0077096 | D |
| FFSD03 Functional Safety Concept | FFSD03 Functional Safety Concept  VDOC86357 | FSC5  B |
| System Architectural Design (from an external source) |  |  |
| Safety Requirements to the item from other safety relevant items (if applicable) |  |  |
| **Other Input**  **(Optional)** | Project Plan |  |  |
| Functional concept |  |  |
| Preliminary architectural assumptions |  |  |
| System Design (incl. external / company / generic standards, legal, HW, SW requirements, etc.) |  |  |
| Instructions for Production, Operation, Service and Decommissioning |  |  |
| Open concerns / Action items (from multiple sources) |  | - |

Table 2: Input

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

## Implementation Details of External Interfaces

| Signal name on CAN/in circuit diagram | Signal short description | Logical signal name (as used in T.-S.-Reqs) | Sender | Receiver | Information transfer type (e.g. HSCAN, analog, discrete, private CAN, Bluetooth) | Values (including unit, resolution or state encoding, if applicable) | Quality information of signal (e.g. QF or embedded) | Timing (Rate of Information Transfer) | Safety Mechanism for Information transfer (e.g. End-to-End Protection) |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  |  |  |  |

Table 3: External Interfaces with Respect to the System Boundary

## Constraints

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

No Constraints Specified on Physical elements in the SysML Model.

## Technical Block Diagram









Figure 1 - Technical Block Diagram

## Functional Overview of Elements/Components/Subsystems

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

| Element/Component/Subsystem | Description / Tasks | Reference to System Design / Detailed Specification |
| --- | --- | --- |
| Headlamp Switch | The is LIN based rotary switch (to the BCM) that has the setting of off, park, LB (headlamp) and autolamp that can be set by the user to activate the lights. This is one variant. |  |
| APIM (Accessory Protocol Interface Module) | This is the synch system that mimics the headlamp switch settings of off, park, LB (headlamp) and autolamp for the user to activate the lights. |  |
| ECG (Enhanced Central Gateway) | Gateway Module which is responsible for transitioning of messages from one Network to other. |  |
| BCM (Body Control Module) | Module which is responsible for arbitrating control of the lamps based on various functions of the vehicle |  |
| HCM (Headlamp Control Module) | This module communicates via private CAN to the headlamps and via CAN FD1 to the BCM. It acts a gateway between BCM and headlamps |  |
| LDM (LED Driver Module) | This module controls the current and voltage to the LEDs and holds the smarts for the lamps. It communicates via private CAN to the HCM. |  |
| IPC (Instrument Panel Cluster) | Display to the driver behind the Steering wheel which provides critical data required to the drive during driving conditions |  |

Table 4: Elements/Components/Subsystems within the System Boundary

### Elements/Components/Systems outside System Boundary

| Element/Component/Subsystem | Description / Tasks |
| --- | --- |
|  |  |
|  |  |

Table 5: Relevant Systems (Elements/Components/Subsystems) outside System Boundary

## Implementation Details of Internal Interfaces

| Signal name on CAN/in circuit diagram | Signal short description | Logical signal name (as used in T.-S.-Reqs) | Sender | Receiver | Information transfer type (e.g. HSCAN, analog, discrete, private CAN, Bluetooth) | Values (including unit, resolution or state encoding, if applicable) | Quality information of signal (e.g. QF or embedded) | Timing (Rate of Information Transfer) | Safety Mechanism for Information transfer (e.g. End-to-End Protection) |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  |  |  |  |

Table 6: Implementation Details of Internal Interfaces

## System Level Architecture (including redundancy)

### Safety Goal: SG01 (ASIL B)

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

Table 7: System Level architecture (including redundancy) for SG01

# Technical Safety Requirements Specification

## Technical Safety Requirements

### Requirement Derivation Diagram(s) for FSR1 - Driver Inputs as request for Low Beam lamps activation

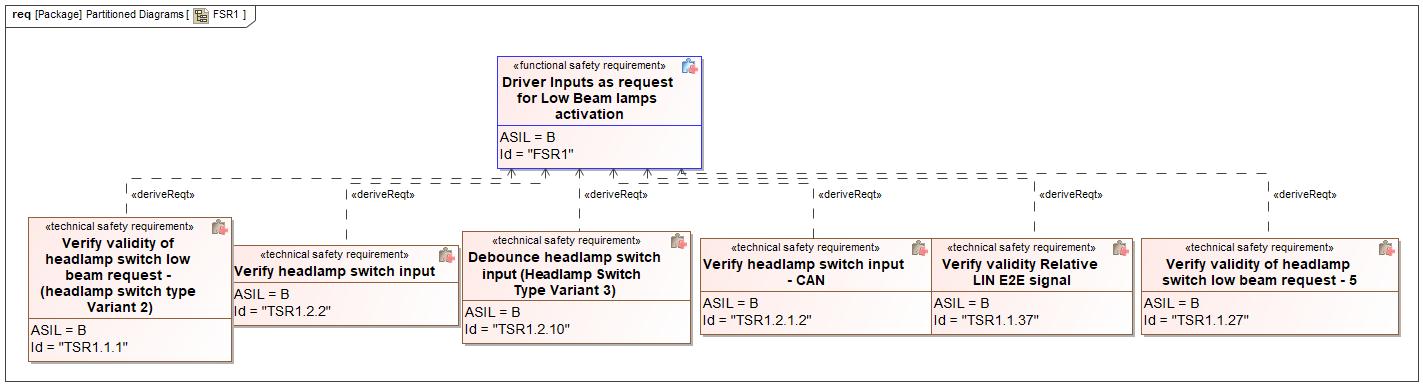


Figure 1 - Technical Safety Requirements Derivation Diagram for FSR1 – Driver Inputs as request for Low Beam lamps activation

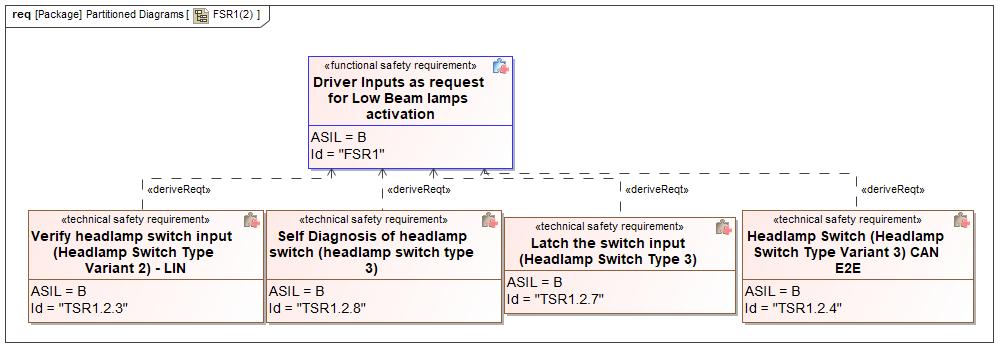


Figure 2 - Technical Safety Requirements Derivation Diagram for FSR1(2) – Driver Inputs as request for Low Beam lamps activation

| T-S-Req-ID: | TSR1.1.1 - Verify validity of headlamp switch low beam request - (headlamp switch type Variant 2) |
| --- | --- |
| External Reference |  |
| Category: | Safety Related Function |
| Safety Goal ID: | SG01 - Ensure Low Beam is not deactivated unintendedly |
| F-S-Req ID: | FSR1 - Driver Inputs as request for Low Beam lamps activation |
| ASIL Classification: | B |
| Technical Safety Requirement Title: | Verify validity of headlamp switch low beam request - (headlamp switch type Variant 2) |
| Technical Safety Requirement Text: | For a LIN relative headlamp switch (LIN REL SW1) or LIN absolute switch (LIN ABSO SW2), BCM shall receive a LIN E2E protected message from the headlamp switch. |
| Rationale: | To prevent communications errors that result in unintended deactivation request from headlamp switch input. |
| Operating Mode: | <S1> Low Beam Activated (ON) |
| Safe State: | Low Beam On (At least one side) |
| Reduced Functionality Tolerance Time Interval: |  |
| Fault Handling Time Segment: | 1000ms |
| Requirement Status | Approved |
| V&V method: | Test |
| V&V acceptance criteria: | For LIN REL SW1 confirm BCM shall receive a LIN E2E protected message from the headlamp switch. |
| Allocated Element(s)/Component(s)/ Subsystem(s) | BCM  LIN Relative Headlamp switch  LIN Absolute Headlamp switch |

Table 8: Verify validity of headlamp switch low beam request - (headlamp switch type Variant 2)

| T-S-Req-ID: | TSR1.1.27 - Verify validity of headlamp switch low beam request - 5 |
| --- | --- |
| External Reference |  |
| Category: | Safety Related Function |
| Safety Goal ID: | SG01 - Ensure Low Beam is not deactivated unintendedly |
| F-S-Req ID: | FSR1 - Driver Inputs as request for Low Beam lamps activation |
| ASIL Classification: | B |
| Technical Safety Requirement Title: | Verify validity of headlamp switch low beam request - 5 |
| Technical Safety Requirement Text: | For a HMI switch (HMI SW3), BCM shall recieve a CAN signal (HeadLghtCtl\_D\_RqMnu ) with AUTOSAR1A E2E protection from the APIM. |
| Rationale: | To prevent communications errors that result in unintended deactivation request from headlamp switch input. |
| Operating Mode: | <S1> Low Beam Activated (ON) |
| Safe State: | Low Beam On (At least one side) |
| Reduced Functionality Tolerance Time Interval: |  |
| Fault Handling Time Segment: | 1000ms |
| Requirement Status | Approved |
| V&V method: | Test |
| V&V acceptance criteria: | Confirm for HMI switch (HMI SW3), BCM shall recieve a CAN signal (HeadLghtCtl\_D\_RqMnu ) with AUTOSAR1A E2E protection from the APIM. |
| Allocated Element(s)/Component(s)/ Subsystem(s) | BCM |

Table 9: Verify validity of headlamp switch low beam request - 5

| T-S-Req-ID: | TSR1.1.37 - Verify validity Relative LIN E2E signal |
| --- | --- |
| External Reference |  |
| Category: | Safety Related Function |
| Safety Goal ID: | SG01 - Ensure Low Beam is not deactivated unintendedly |
| F-S-Req ID: | FSR1 - Driver Inputs as request for Low Beam lamps activation |
| ASIL Classification: | B |
| Technical Safety Requirement Title: | Verify validity Relative LIN E2E signal |
| Technical Safety Requirement Text: | Lin Relative Headlamps Switch shall publish Invalid in Abs\_Pos\_Stat\_LINHSM\_Asil |
| Rationale: | To prevent communications errors that result in unintended deactivation request from headlamp switch input. |
| Operating Mode: | <S1> Low Beam Activated (ON) |
| Safe State: | Low Beam On (At least one side) |
| Reduced Functionality Tolerance Time Interval: |  |
| Fault Handling Time Segment: | 1000ms |
| Requirement Status | Approved |
| V&V method: | Test |
| V&V acceptance criteria: | Lin Relative Headlamps Switch shall publish Invalid in Abs\_Pos\_Stat\_LINHSM\_Asil |
| Allocated Element(s)/Component(s)/ Subsystem(s) | LIN Relative Headlamp switch |

Table 10: Verify validity Relative LIN E2E signal

| T-S-Req-ID: | TSR1.2.1.2 - Verify headlamp switch input - CAN |
| --- | --- |
| External Reference |  |
| Category: | Safety Related Function |
| Safety Goal ID: | SG01 - Ensure Low Beam is not deactivated unintendedly |
| F-S-Req ID: | FSR1 - Driver Inputs as request for Low Beam lamps activation |
| ASIL Classification: | B |
| Technical Safety Requirement Title: | Verify headlamp switch input - CAN |
| Technical Safety Requirement Text: | Headlamp switch shall ensure that HeadLghtCtl\_D\_RqMnu signal matches the physical switch request/interaction provided by the driver |
| Rationale: | Headlamp switch Request Signal Match Physical Request/Interaction |
| Operating Mode: | <S1> Low Beam Activated (ON) |
| Safe State: | Low Beam On (At least one side) |
| Reduced Functionality Tolerance Time Interval: |  |
| Fault Handling Time Segment: | 1000ms |
| Requirement Status | Approved |
| V&V method: | Test |
| V&V acceptance criteria: | Confirm that Headlamp switch shall ensure that HeadLghtCtl\_D\_RqMnu signal matches the physical switch request/interaction provided by the driver |
| Allocated Element(s)/Component(s)/ Subsystem(s) | APIM\_CDC |

Table 11: Verify headlamp switch input - CAN

| T-S-Req-ID: | TSR1.2.2 - Verify headlamp switch input |
| --- | --- |
| External Reference |  |
| Category: | Safety Related Function |
| Safety Goal ID: | SG01 - Ensure Low Beam is not deactivated unintendedly |
| F-S-Req ID: | FSR1 - Driver Inputs as request for Low Beam lamps activation |
| ASIL Classification: | B |
| Technical Safety Requirement Title: | Verify headlamp switch input |
| Technical Safety Requirement Text: | LIN based head lamp switch shall transmit the headlamp switch position message (Encoder\_Cnt\_Dn\_LINHSM\_Asil and Encoder\_Cnt\_Up\_LINHSM\_Asil and Abs\_Pos\_Stat\_LINHSM\_Asil) with E2E protection |
| Rationale: | To prevent communications errors that result in unintended deactivation request from headlamp switch input. |
| Operating Mode: | <S1> Low Beam Activated (ON) |
| Safe State: | Low Beam On (At least one side) |
| Reduced Functionality Tolerance Time Interval: |  |
| Fault Handling Time Segment: | 1000ms |
| Requirement Status | Approved |
| V&V method: | Test |
| V&V acceptance criteria: | Confirm LIN based head lamp switch shall transmit the headlamp switch position message (Encoder\_Cnt\_Dn\_LINHSM\_Asil and Encoder\_Cnt\_Up\_LINHSM\_Asil and Abs\_Pos\_Stat\_LINHSM\_Asil) with E2E protection |
| Allocated Element(s)/Component(s)/ Subsystem(s) | Headlamp Switch |

Table 12: Verify headlamp switch input

| T-S-Req-ID: | TSR1.2.3 - Verify headlamp switch input (Headlamp Switch Type Variant 2) - LIN |
| --- | --- |
| External Reference |  |
| Category: | Safety Related Function |
| Safety Goal ID: | SG01 - Ensure Low Beam is not deactivated unintendedly |
| F-S-Req ID: | FSR1 - Driver Inputs as request for Low Beam lamps activation |
| ASIL Classification: | B |
| Technical Safety Requirement Title: | Verify headlamp switch input (Headlamp Switch Type Variant 2) - LIN |
| Technical Safety Requirement Text: | LIN based headlamp switch shall detect faults that avoiding the Low Beam on and report out and unknow or invalid status thru LIN message. |
| Rationale: | To prevent communications errors that result in unintended deactivation request from headlamp switch input. |
| Operating Mode: | <S1> Low Beam Activated (ON) |
| Safe State: | Low Beam On (At least one side) |
| Reduced Functionality Tolerance Time Interval: |  |
| Fault Handling Time Segment: | 1000ms |
| Requirement Status | Approved |
| V&V method: | Test |
| V&V acceptance criteria: | Confirm LIN abased headlamp switch detect faults and report out an unknown or invalid status thru LIN message. |
| Allocated Element(s)/Component(s)/ Subsystem(s) | LIN Absolute Headlamp switch  LIN Relative Headlamp switch |

Table 13: Verify headlamp switch input (Headlamp Switch Type Variant 2) - LIN

| T-S-Req-ID: | TSR1.2.4 - Headlamp Switch (Headlamp Switch Type Variant 3) CAN E2E |
| --- | --- |
| External Reference |  |
| Category: | Safety Related Function |
| Safety Goal ID: | SG01 - Ensure Low Beam is not deactivated unintendedly |
| F-S-Req ID: | FSR1 - Driver Inputs as request for Low Beam lamps activation |
| ASIL Classification: | B |
| Technical Safety Requirement Title: | Headlamp Switch (Headlamp Switch Type Variant 3) CAN E2E |
| Technical Safety Requirement Text: | CAN based head lamp switch (APIM) shall transmit the headlamp switch position (HeadLghtCtl\_D\_RqMnu) with AUTOSAR1A E2E based on software guide RQT-003701-023579. |
| Rationale: | To prevent communications errors that result in unintended deactivation request from headlamp switch input. |
| Operating Mode: | <S1> Low Beam Activated (ON) |
| Safe State: | Low Beam On (At least one side) |
| Reduced Functionality Tolerance Time Interval: |  |
| Fault Handling Time Segment: | 1000ms |
| Requirement Status | Approved |
| V&V method: | Test |
| V&V acceptance criteria: | Confirm that CAN based head lamp switch (APIM) shall transmit the headlamp switch position (HeadLghtCtl\_D\_RqMnu) with AUTOSAR1A E2E based on software guide RQT-003701-023579. |
| Allocated Element(s)/Component(s)/ Subsystem(s) | APIM\_CDC |

Table 14: Headlamp Switch (Headlamp Switch Type Variant 3) CAN E2E

| T-S-Req-ID: | TSR1.2.7 - Latch the switch input (Headlamp Switch Type 3) |
| --- | --- |
| External Reference |  |
| Category: | Safety Related Function |
| Safety Goal ID: | SG01 - Ensure Low Beam is not deactivated unintendedly |
| F-S-Req ID: | FSR1 - Driver Inputs as request for Low Beam lamps activation |
| ASIL Classification: | B |
| Technical Safety Requirement Title: | Latch the switch input (Headlamp Switch Type 3) |
| Technical Safety Requirement Text: | When the APIM (SYNC) sets <HeadLghtCtl\_D\_RqMnu = Headlamp/Parklamp/Autolamp/Off>, it shall latch the request until the APIM (SYNC) has transitioned to a power-down state or detects a new headlamp selection from the driver |
| Rationale: | Latch the switch input request to confirm user selection and ensure no deactivation of low beams. |
| Operating Mode: | <S1> Low Beam Activated (ON) |
| Safe State: | Low Beam On (At least one side) |
| Reduced Functionality Tolerance Time Interval: |  |
| Fault Handling Time Segment: | 1000ms |
| Requirement Status | Approved |
| V&V method: | Test |
| V&V acceptance criteria: | Confirm when the APIM (SYNC) sets <HeadLghtCtl\_D\_RqMnu = Headlamp/Parklamp/Autolamp/Off>, it shall latch the request until the APIM (SYNC) has transitioned to a power-down state or detects a new headlamp selection from the driver. |
| Allocated Element(s)/Component(s)/ Subsystem(s) | APIM\_CDC |

Table 15: Latch the switch input (Headlamp Switch Type 3)

| T-S-Req-ID: | TSR1.2.8 - Self Diagnosis of headlamp switch (headlamp switch type 3) |
| --- | --- |
| External Reference |  |
| Category: | Safety Related Function |
| Safety Goal ID: | SG01 - Ensure Low Beam is not deactivated unintendedly |
| F-S-Req ID: | FSR1 - Driver Inputs as request for Low Beam lamps activation |
| ASIL Classification: | B |
| Technical Safety Requirement Title: | Self Diagnosis of headlamp switch (headlamp switch type 3) |
| Technical Safety Requirement Text: | The APIM (SYNC) microprocessor shall execute a power-on diagnostic self-test to determine internal failures that can lead to unintended headlamp low beam deactivation request including checks for stack over/under flow and watchdog operation. |
| Rationale: | Ensure low beam is not deactivated by self diagnosis |
| Operating Mode: | <S1> Low Beam Activated (ON) |
| Safe State: | Low Beam On (At least one side) |
| Reduced Functionality Tolerance Time Interval: |  |
| Fault Handling Time Segment: | 1000ms |
| Requirement Status | Approved |
| V&V method: | Test |
| V&V acceptance criteria: | Confirm that APIM (SYNC) microprocessor execute a power-on diagnostic self-test to determine internal failures that can lead to unintended headlamp low beam deactivation request including checks for stack over/under flow and watchdog operation. |
| Allocated Element(s)/Component(s)/ Subsystem(s) | APIM\_CDC |

Table 16: Self Diagnosis of headlamp switch (headlamp switch type 3)

| T-S-Req-ID: | TSR1.2.10 - Debounce headlamp switch input (Headlamp Switch Type Variant 3) |
| --- | --- |
| External Reference |  |
| Category: | Safety Related Function |
| Safety Goal ID: | SG01 - Ensure Low Beam is not deactivated unintendedly |
| F-S-Req ID: | FSR1 - Driver Inputs as request for Low Beam lamps activation |
| ASIL Classification: | B |
| Technical Safety Requirement Title: | Debounce headlamp switch input (Headlamp Switch Type Variant 3) |
| Technical Safety Requirement Text: | For CAN based headlamp switch, The APIM (SYNC) shall detect and debounce the driver input request and set <HeadLghtCtl\_D\_RqMnu = Headlamp/Parklamp/Autolamp/Off> when it detects a driver selection request for <HL\_DEBOUNCE\_LO\_CNT> debounce cycles. |
| Rationale: | Debounce switch input to confirm user selection and ensure no deactivation of low beams. |
| Operating Mode: | <S1> Low Beam Activated (ON) |
| Safe State: | Low Beam On (At least one side) |
| Reduced Functionality Tolerance Time Interval: |  |
| Fault Handling Time Segment: | 1000ms |
| Requirement Status | Approved |
| V&V method: | Test |
| V&V acceptance criteria: | In case of AN based headlamp switch, The APIM (SYNC) detect and debounce the driver input request and set <HeadLghtCtl\_D\_RqMnu = Headlamp/Parklamp/Autolamp/Off> when it detects a driver selection request for <HL\_DEBOUNCE\_LO\_CNT> debounce cycles. Confirm the cycle. |
| Allocated Element(s)/Component(s)/ Subsystem(s) | APIM\_CDC |

Table 17: Debounce headlamp switch input (Headlamp Switch Type Variant 3)

### Requirement Derivation Diagram(s) for TSR1.2.1.2 - Verify headlamp switch input - CAN

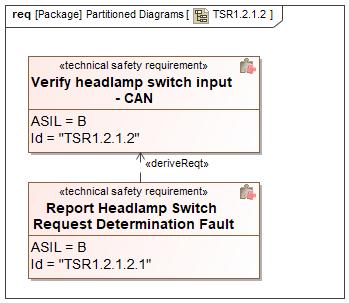


Figure 3- Technical Safety Requirements Derivation Diagram for TSR1.2.1.2 – Verify headlamp switch input - CAN

| T-S-Req-ID: | TSR1.2.1.2.1 - Report Headlamp Switch Request Determination Fault |
| --- | --- |
| External Reference |  |
| Category: | Safety Related Function |
| Safety Goal ID: | SG01 - Ensure Low Beam is not deactivated unintendedly |
| F-S-Req ID: | FSR1 - Driver Inputs as request for Low Beam lamps activation |
| ASIL Classification: | B |
| Technical Safety Requirement Title: | Report Headlamp Switch Request Determination Fault |
| Technical Safety Requirement Text: | If the value of HeadLghtCtl\_D\_RqMnu cannot be determined, then APIM\_CDC shall set signal HeadLghtCtl\_D\_RqMnu=faulted. |
| Rationale: | To prevent communications errors that result in unintended deactivation request from headlamp switch input. |
| Operating Mode: | <S1> Low Beam Activated (ON) |
| Safe State: | Low Beam On (At least one side) |
| Reduced Functionality Tolerance Time Interval: |  |
| Fault Handling Time Segment: | 1000ms |
| Requirement Status | Approved |
| V&V method: | Test |
| V&V acceptance criteria: | Confirm when the value of HeadLghtCtl\_D\_RqMnu cannot be determined, then APIM\_CDC shall set signal HeadLghtCtl\_D\_RqMnu=faulted. |
| Allocated Element(s)/Component(s)/ Subsystem(s) | APIM\_CDC |

Table 18: Report Headlamp Switch Request Determination Fault

### Requirement Derivation Diagram(s) for FSR2 - Arbitration logic working properly for Low Beam activation

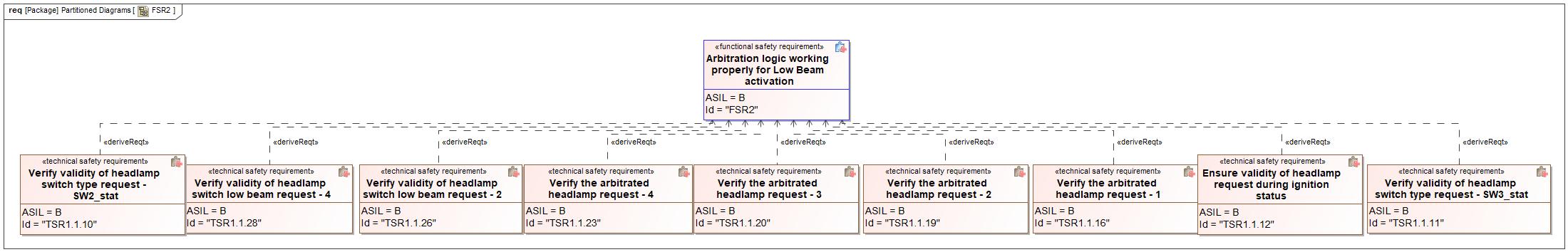


Figure 4 - Technical Safety Requirements Derivation Diagram for FSR2 – Arbitration logic working properly for Low Beam activation

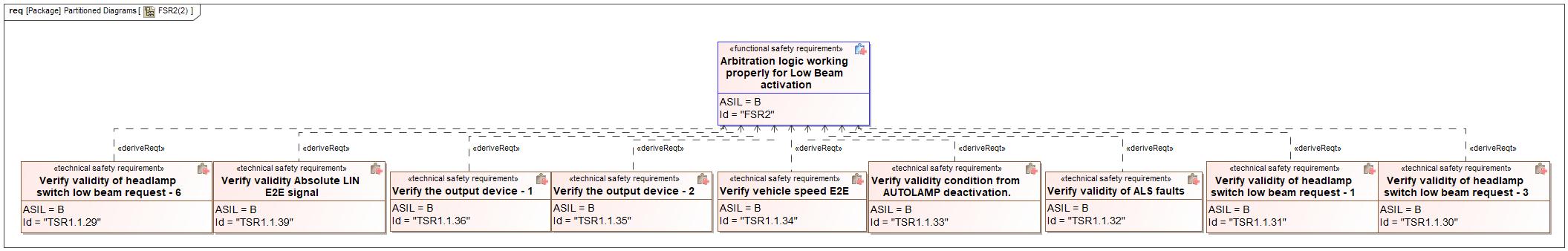


Figure 5 - Technical Safety Requirements Derivation Diagram for FSR2(2) – Arbitration logic working properly for Low Beam activation

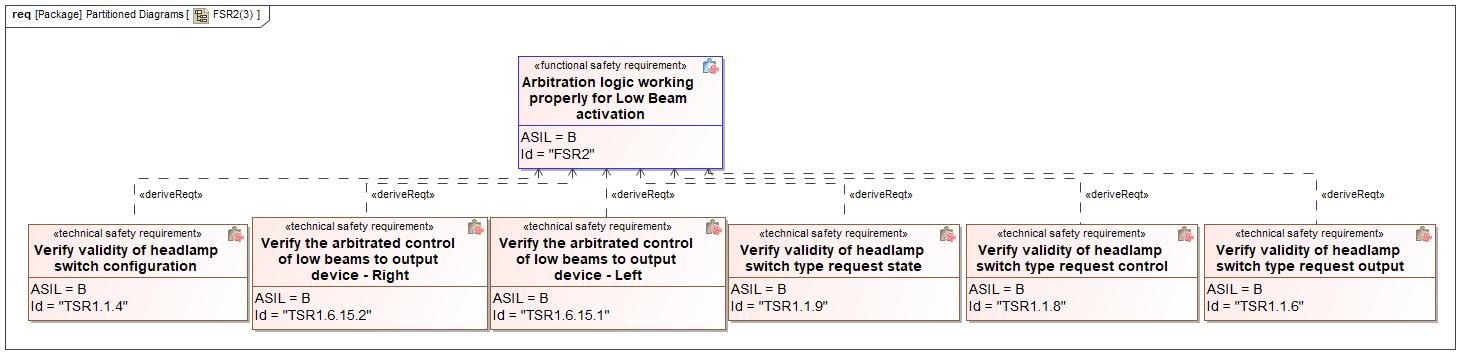


Figure 6 - Technical Safety Requirements Derivation Diagram for FSR2(3) – Arbitration logic working properly for Low Beam activation

| T-S-Req-ID: | TSR1.1.4 - Verify validity of headlamp switch configuration |
| --- | --- |
| External Reference |  |
| Category: | Safety Related Function |
| Safety Goal ID: | SG01 - Ensure Low Beam is not deactivated unintendedly |
| F-S-Req ID: | FSR2 - Arbitration logic working properly for Low Beam activation |
| ASIL Classification: | B |
| Technical Safety Requirement Title: | Verify validity of headlamp switch configuration |
| Technical Safety Requirement Text: | BCM shall have a functional safe configuration for selecting headlamp switch type (HeadlampSwitchType\_Cfg). Initial value for HeadlampSwitchType\_Cfg shall be set to NOT\_CONFIG. |
| Rationale: | To prevent communications errors that result in unintended deactivation request from headlamp switch input. |
| Operating Mode: | <S1> Low Beam Activated (ON) |
| Safe State: | Low Beam On (At least one side) |
| Reduced Functionality Tolerance Time Interval: |  |
| Fault Handling Time Segment: | 1000ms |
| Requirement Status | Approved |
| V&V method: | Test |
| V&V acceptance criteria: | When initial value for HeadlampSwitchType\_Cfg is set to NOT\_CONFIG. BCM shall have a functional safe configuration for selecting headlamp switch type (HeadlampSwitchType\_Cfg). |
| Allocated Element(s)/Component(s)/ Subsystem(s) | BCM |

Table 19: Verify validity of headlamp switch configuration

| T-S-Req-ID: | TSR1.1.6 - Verify validity of headlamp switch type request output |
| --- | --- |
| External Reference |  |
| Category: | Safety Related Function |
| Safety Goal ID: | SG01 - Ensure Low Beam is not deactivated unintendedly |
| F-S-Req ID: | FSR2 - Arbitration logic working properly for Low Beam activation |
| ASIL Classification: | B |
| Technical Safety Requirement Title: | Verify validity of headlamp switch type request output |
| Technical Safety Requirement Text: | Low Beam Controller shall provide an arbitrated headlamp switch request output (FuSa\_HLampSW\_Rqst) |
| Rationale: | To prevent communications errors that result in unintended deactivation request from headlamp switch input. |
| Operating Mode: | <S1> Low Beam Activated (ON) |
| Safe State: | Low Beam On (At least one side) |
| Reduced Functionality Tolerance Time Interval: |  |
| Fault Handling Time Segment: | 1000ms |
| Requirement Status | Approved |
| V&V method: | Test |
| V&V acceptance criteria: | Confirm that Low Beam Controller shall provide an arbitrated headlamp switch request output (FuSa\_HLampSW\_Rqst). |
| Allocated Element(s)/Component(s)/ Subsystem(s) | BCM |

Table 20: Verify validity of headlamp switch type request output

| T-S-Req-ID: | TSR1.1.8 - Verify validity of headlamp switch type request control |
| --- | --- |
| External Reference |  |
| Category: | Safety Related Function |
| Safety Goal ID: | SG01 - Ensure Low Beam is not deactivated unintendedly |
| F-S-Req ID: | FSR2 - Arbitration logic working properly for Low Beam activation |
| ASIL Classification: | B |
| Technical Safety Requirement Title: | Verify validity of headlamp switch type request control |
| Technical Safety Requirement Text: | If HeadlampSwitchType\_Cfg is NOT\_CONFIG or an invalid value , then headlamp switch request (FuSa\_HLampSW\_Rqst) shall be set to ERR. |
| Rationale: | To prevent communications errors that result in unintended deactivation request from headlamp switch input. |
| Operating Mode: | <S1> Low Beam Activated (ON) |
| Safe State: | Low Beam On (At least one side) |
| Reduced Functionality Tolerance Time Interval: |  |
| Fault Handling Time Segment: | 1000ms |
| Requirement Status | Approved |
| V&V method: | Test |
| V&V acceptance criteria: | Confirm If HeadlampSwitchType\_Cfg is NOT\_CONFIG or an invalid value , then headlamp switch request (FuSa\_HLampSW\_Rqst) shall be set to ERR. |
| Allocated Element(s)/Component(s)/ Subsystem(s) | BCM |

Table 21: Verify validity of headlamp switch type request control

| T-S-Req-ID: | TSR1.1.9 - Verify validity of headlamp switch type request state |
| --- | --- |
| External Reference |  |
| Category: | Safety Related Function |
| Safety Goal ID: | SG01 - Ensure Low Beam is not deactivated unintendedly |
| F-S-Req ID: | FSR2 - Arbitration logic working properly for Low Beam activation |
| ASIL Classification: | B |
| Technical Safety Requirement Title: | Verify validity of headlamp switch type request state |
| Technical Safety Requirement Text: | If HeadlampSwitchType\_Cfg is LIN REL SW1, then BCM shall set headlamp switch request (FuSa\_HLampSW\_Rqst) according to the state of the LIN Relative Headlamps Switch per TSR1.1.30. |
| Rationale: | To prevent communications errors that result in unintended deactivation request from headlamp switch input. |
| Operating Mode: | <S1> Low Beam Activated (ON) |
| Safe State: | Low Beam On (At least one side) |
| Reduced Functionality Tolerance Time Interval: |  |
| Fault Handling Time Segment: | 1000ms |
| Requirement Status | Approved |
| V&V method: | Test |
| V&V acceptance criteria: | Confirm that: If HeadlampSwitchType\_Cfg is LIN REL SW1, then BCM shall set headlamp switch request (FuSa\_HLampSW\_Rqst) according to the state of the LIN Relative Headlamps Switch per TSR1.1.30. |
| Allocated Element(s)/Component(s)/ Subsystem(s) | BCM |

Table 22: Verify validity of headlamp switch type request state

| T-S-Req-ID: | TSR1.1.10 - Verify validity of headlamp switch type request - SW2\_stat |
| --- | --- |
| External Reference |  |
| Category: | Safety Related Function |
| Safety Goal ID: | SG01 - Ensure Low Beam is not deactivated unintendedly |
| F-S-Req ID: | FSR2 - Arbitration logic working properly for Low Beam activation |
| ASIL Classification: | B |
| Technical Safety Requirement Title: | Verify validity of headlamp switch type request - SW2\_stat |
| Technical Safety Requirement Text: | If HeadlampSwitchType\_Cfg is LIN ABSO SW2, then BCM shall set headlamp switch request (FuSa\_HLampSW\_Rqst) according to the state of the LIN Absolute Headlamps Switch per TSR1.1.28. |
| Rationale: | To prevent communications errors that result in unintended deactivation request from headlamp switch input. |
| Operating Mode: | <S1> Low Beam Activated (ON) |
| Safe State: | Low Beam On (At least one side) |
| Reduced Functionality Tolerance Time Interval: |  |
| Fault Handling Time Segment: | 1000ms |
| Requirement Status | Approved |
| V&V method: | Test |
| V&V acceptance criteria: | Confirm If HeadlampSwitchType\_Cfg is LIN ABSO SW2, then BCM shall set headlamp switch request (FuSa\_HLampSW\_Rqst) according to the state of the LIN Absolute Headlamps Switch per TSR1.1.28. |
| Allocated Element(s)/Component(s)/ Subsystem(s) | BCM |

Table 23: Verify validity of headlamp switch type request - SW2\_stat

| T-S-Req-ID: | TSR1.1.11 - Verify validity of headlamp switch type request - SW3\_stat |
| --- | --- |
| External Reference |  |
| Category: | Safety Related Function |
| Safety Goal ID: | SG01 - Ensure Low Beam is not deactivated unintendedly |
| F-S-Req ID: | FSR2 - Arbitration logic working properly for Low Beam activation |
| ASIL Classification: | B |
| Technical Safety Requirement Title: | Verify validity of headlamp switch type request - SW3\_stat |
| Technical Safety Requirement Text: | If HeadlampSwitchType\_Cfg is HMI SW3, , then BCM shall set headlamp switch request (FuSa\_HLampSW\_Rqst) according to the state of the HMI Headlamp Switch per TSR1.1.29. |
| Rationale: | To prevent communications errors that result in unintended deactivation request from headlamp switch input. |
| Operating Mode: | <S1> Low Beam Activated (ON) |
| Safe State: | Low Beam On (At least one side) |
| Reduced Functionality Tolerance Time Interval: |  |
| Fault Handling Time Segment: | 1000ms |
| Requirement Status | Approved |
| V&V method: | Test |
| V&V acceptance criteria: | Confirm when HeadlampSwitchType\_Cfg is HMI SW3, , then BCM shall set headlamp switch request (FuSa\_HLampSW\_Rqst) according to the state of the HMI Headlamp Switch per TSR1.1.29. |
| Allocated Element(s)/Component(s)/ Subsystem(s) | BCM |

Table 24: Verify validity of headlamp switch type request - SW3\_stat

| T-S-Req-ID: | TSR1.1.12 - Ensure validity of headlamp request during ignition status |
| --- | --- |
| External Reference |  |
| Category: | Safety Related Function |
| Safety Goal ID: | SG01 - Ensure Low Beam is not deactivated unintendedly |
| F-S-Req ID: | FSR2 - Arbitration logic working properly for Low Beam activation |
| ASIL Classification: | B |
| Technical Safety Requirement Title: | Ensure validity of headlamp request during ignition status |
| Technical Safety Requirement Text: | BCM shall provide the controlling mode of the vehicle (VehOnSrc\_D\_Stat) |
| Rationale: | To prevent unintended deactivation request during different ignition states |
| Operating Mode: | <S1> Low Beam Activated (ON) |
| Safe State: | Low Beam On (At least one side) |
| Reduced Functionality Tolerance Time Interval: |  |
| Fault Handling Time Segment: | 1000ms |
| Requirement Status | Approved |
| V&V method: | Test |
| V&V acceptance criteria: | Confirm that BCM shall provide the controlling mode of the vehicle (VehOnSrc\_D\_Stat) |
| Allocated Element(s)/Component(s)/ Subsystem(s) | BCM |

Table 25: Ensure validity of headlamp request during ignition status

| T-S-Req-ID: | TSR1.1.16 - Verify the arbitrated headlamp request - 1 |
| --- | --- |
| External Reference |  |
| Category: | Safety Related Function |
| Safety Goal ID: | SG01 - Ensure Low Beam is not deactivated unintendedly |
| F-S-Req ID: | FSR2 - Arbitration logic working properly for Low Beam activation |
| ASIL Classification: | B |
| Technical Safety Requirement Title: | Verify the arbitrated headlamp request - 1 |
| Technical Safety Requirement Text: | Low Beam Controller shall provide an arbitrated headlamp request (LowBeam\_Rqst) |
| Rationale: | To prevent unintended deactivation request |
| Operating Mode: | <S1> Low Beam Activated (ON) |
| Safe State: | Low Beam On (At least one side) |
| Reduced Functionality Tolerance Time Interval: |  |
| Fault Handling Time Segment: | 1000ms |
| Requirement Status | Approved |
| V&V method: | Test |
| V&V acceptance criteria: | Confirm that Low Beam Controller provide an arbitrated headlamp request (LowBeam\_Rqst ). |
| Allocated Element(s)/Component(s)/ Subsystem(s) | BCM |

Table 26: Verify the arbitrated headlamp request - 1

| T-S-Req-ID: | TSR1.1.19 - Verify the arbitrated headlamp request - 2 |
| --- | --- |
| External Reference |  |
| Category: | Safety Related Function |
| Safety Goal ID: | SG01 - Ensure Low Beam is not deactivated unintendedly |
| F-S-Req ID: | FSR2 - Arbitration logic working properly for Low Beam activation |
| ASIL Classification: | B |
| Technical Safety Requirement Title: | Verify the arbitrated headlamp request - 2 |
| Technical Safety Requirement Text: | If the FuSa\_HLampSW\_Rqst is set to MANUAL and ExtLightVehPrecondition <> ALLOWED, then LowBeam\_Rqst shall be set to ON. |
| Rationale: | To prevent unintended deactivation request |
| Operating Mode: | <S1> Low Beam Activated (ON) |
| Safe State: | Low Beam On (At least one side) |
| Reduced Functionality Tolerance Time Interval: |  |
| Fault Handling Time Segment: | 1000ms |
| Requirement Status | Approved |
| V&V method: | Test |
| V&V acceptance criteria: | Confirm If the FuSa\_HLampSW\_Rqst is set to MANUAL and ExtLightVehPrecondition <> ALLOWED, then LowBeam\_Rqst shall be set to ON. |
| Allocated Element(s)/Component(s)/ Subsystem(s) | BCM |

Table 27: Verify the arbitrated headlamp request - 2

| T-S-Req-ID: | TSR1.1.20 - Verify the arbitrated headlamp request - 3 |
| --- | --- |
| External Reference |  |
| Category: | Safety Related Function |
| Safety Goal ID: | SG01 - Ensure Low Beam is not deactivated unintendedly |
| F-S-Req ID: | FSR2 - Arbitration logic working properly for Low Beam activation |
| ASIL Classification: | B |
| Technical Safety Requirement Title: | Verify the arbitrated headlamp request - 3 |
| Technical Safety Requirement Text: | If the FuSa\_HLampSW\_Rqst is set to ERR and ExtLightVehPrecondition <> ALLOWED, then LowBeam\_Rqst shall be set to ON. |
| Rationale: | To prevent unintended deactivation request |
| Operating Mode: | <S1> Low Beam Activated (ON) |
| Safe State: | Low Beam On (At least one side) |
| Reduced Functionality Tolerance Time Interval: |  |
| Fault Handling Time Segment: | 1000ms |
| Requirement Status | Approved |
| V&V method: | Test |
| V&V acceptance criteria: | Confirm If the FuSa\_HLampSW\_Rqst is set to ERR and ExtLightVehPrecondition <> ALLOWED, then LowBeam\_Rqst shall be set to ON. |
| Allocated Element(s)/Component(s)/ Subsystem(s) | BCM |

Table 28: Verify the arbitrated headlamp request - 3

| T-S-Req-ID: | TSR1.1.23 - Verify the arbitrated headlamp request - 4 |
| --- | --- |
| External Reference |  |
| Category: | Safety Related Function |
| Safety Goal ID: | SG01 - Ensure Low Beam is not deactivated unintendedly |
| F-S-Req ID: | FSR2 - Arbitration logic working properly for Low Beam activation |
| ASIL Classification: | B |
| Technical Safety Requirement Title: | Verify the arbitrated headlamp request - 4 |
| Technical Safety Requirement Text: | If the FuSa\_HLampSW\_Rqst is set to AUTO and ExtLightVehPrecondition <> ALLOWED and AmbientLight\_Stat <> DAY then BCM shall set LowBeam\_Rqst to ON. |
| Rationale: | To prevent unintended deactivation request |
| Operating Mode: | <S1> Low Beam Activated (ON) |
| Safe State: | Low Beam On (At least one side) |
| Reduced Functionality Tolerance Time Interval: |  |
| Fault Handling Time Segment: | 1000ms |
| Requirement Status | Approved |
| V&V method: | Test |
| V&V acceptance criteria: | Conform if the FuSa\_HLampSW\_Rqst is set to AUTO and ExtLightVehPrecondition <> ALLOWED and AmbientLight\_Stat <> DAY then BCM shall set LowBeam\_Rqst to ON. |
| Allocated Element(s)/Component(s)/ Subsystem(s) | BCM |

Table 29: Verify the arbitrated headlamp request - 4

| T-S-Req-ID: | TSR1.1.26 - Verify validity of headlamp switch low beam request - 2 |
| --- | --- |
| External Reference |  |
| Category: | Safety Related Function |
| Safety Goal ID: | SG01 - Ensure Low Beam is not deactivated unintendedly |
| F-S-Req ID: | FSR2 - Arbitration logic working properly for Low Beam activation |
| ASIL Classification: | B |
| Technical Safety Requirement Title: | Verify validity of headlamp switch low beam request - 2 |
| Technical Safety Requirement Text: | The BCM shall determine LIN Absolute headlamp switch Channel invalid and set LIN\_Abso\_HLamp\_ValidChan accordingly within 500 ms if either of the following are true:  ·abs\_pos\_stat\_LINHSM signal is not received  ·Counter and checksum are not valid |
| Rationale: | To prevent communications errors that result in unintended deactivation request from headlamp switch input. |
| Operating Mode: | <S1> Low Beam Activated (ON) |
| Safe State: | Low Beam On (At least one side) |
| Reduced Functionality Tolerance Time Interval: |  |
| Fault Handling Time Segment: | 1000ms |
| Requirement Status | Approved |
| V&V method: | Test |
| V&V acceptance criteria: | Confrm when BCM determines LIN Absolute headlamp switch Channel invalid and set LIN\_Abso\_HLamp\_ValidChan accordingly within 500 ms if either of the following are true:  ·abs\_pos\_stat\_LINHSM signal is not received  ·Counter and checksum are not valid |
| Allocated Element(s)/Component(s)/ Subsystem(s) | BCM |

Table 30: Verify validity of headlamp switch low beam request - 2

| T-S-Req-ID: | TSR1.1.28 - Verify validity of headlamp switch low beam request - 4 |
| --- | --- |
| External Reference |  |
| Category: | Safety Related Function |
| Safety Goal ID: | SG01 - Ensure Low Beam is not deactivated unintendedly |
| F-S-Req ID: | FSR2 - Arbitration logic working properly for Low Beam activation |
| ASIL Classification: | B |
| Technical Safety Requirement Title: | Verify validity of headlamp switch low beam request - 4 |
| Technical Safety Requirement Text: | For a LIN absolute headlamp Switch (LIN\_ABSO\_SW2), the BCM shall set SW2\_stat as follows:  If abs\_pos\_stat\_LINHSM=(unknown or invalid) OR LINAbso\_Hlamp\_ValidChan <> VALID  then set SW2\_stat = ERR  Else  set SW2\_stat = abs\_pos\_stat\_LINHSM |
| Rationale: | To prevent communications errors that result in unintended deactivation request from headlamp switch input. |
| Operating Mode: | <S1> Low Beam Activated (ON) |
| Safe State: | Low Beam On (At least one side) |
| Reduced Functionality Tolerance Time Interval: |  |
| Fault Handling Time Segment: | 1000ms |
| Requirement Status | Approved |
| V&V method: | Test |
| V&V acceptance criteria: | Confirm when LIN absolute headlamp Switch (LIN\_ABSO\_SW2), the BCM shall set SW2\_stat as follows:  If abs\_pos\_stat\_LINHSM=(unknown or invalid) OR LINAbso\_Hlamp\_ValidChan <> VALID  then set SW2\_stat = ERR  Else  set SW2\_stat = abs\_pos\_stat\_LINHSM |
| Allocated Element(s)/Component(s)/ Subsystem(s) | BCM |

Table 31: Verify validity of headlamp switch low beam request - 4

| T-S-Req-ID: | TSR1.1.29 - Verify validity of headlamp switch low beam request - 6 |
| --- | --- |
| External Reference |  |
| Category: | Safety Related Function |
| Safety Goal ID: | SG01 - Ensure Low Beam is not deactivated unintendedly |
| F-S-Req ID: | FSR2 - Arbitration logic working properly for Low Beam activation |
| ASIL Classification: | B |
| Technical Safety Requirement Title: | Verify validity of headlamp switch low beam request - 6 |
| Technical Safety Requirement Text: | For an HMI headlamp Switch (HMI\_SW3), the BCM shall set SW3\_stat as follows:  If HeadLghtCtl\_D\_RqMnu=(Faultly or NotUsed\_1 or NotUsed\_2)  then set SW3\_stat = ERR  If HeadLghtCtl\_D\_RqMnu=Null  then set SW3\_stat=not change  Else  set SW3\_stat = HeadLghtCtl\_D\_RqMnu |
| Rationale: | To prevent communications errors that result in unintended deactivation request from headlamp switch input. |
| Operating Mode: | <S1> Low Beam Activated (ON) |
| Safe State: | Low Beam On (At least one side) |
| Reduced Functionality Tolerance Time Interval: |  |
| Fault Handling Time Segment: | 1000ms |
| Requirement Status | Approved |
| V&V method: | Test |
| V&V acceptance criteria: | Confirm For an HMI headlamp Switch (HMI\_SW3), the BCM shall set SW3\_stat as follows:  If HeadLghtCtl\_D\_RqMnu=(Faultly or NotUsed\_1 or NotUsed\_2)  then set SW3\_stat = ERR  If HeadLghtCtl\_D\_RqMnu=Null  then set SW3\_stat=not change  Else  set SW3\_stat = HeadLghtCtl\_D\_RqMnu |
| Allocated Element(s)/Component(s)/ Subsystem(s) | BCM |

Table 32: Verify validity of headlamp switch low beam request - 6

| T-S-Req-ID: | TSR1.1.30 - Verify validity of headlamp switch low beam request - 3 |
| --- | --- |
| External Reference |  |
| Category: | Safety Related Function |
| Safety Goal ID: | SG01 - Ensure Low Beam is not deactivated unintendedly |
| F-S-Req ID: | FSR2 - Arbitration logic working properly for Low Beam activation |
| ASIL Classification: | B |
| Technical Safety Requirement Title: | Verify validity of headlamp switch low beam request - 3 |
| Technical Safety Requirement Text: | For a LIN relative headlamp Switch (LIN\_REL\_SW1), the BCM shall set SW1\_stat as follows:  1) When Encoder\_Cnt\_Up\_LINHSM increments and it is in a range 1 to 6 then SW1\_stat progresses in the following order:  OFF -> POS -> AUTO -> ON  2) When Encoder\_Cnt\_Dn\_LINHSM increments and it is in a range 1 to 6 then SW1\_stat progresses in the following order:  ON -> AUTO -> POS -> OFF)  3) If either counter is set to value 7, then set SW1\_stat to ERR |
| Rationale: | To prevent communications errors that result in unintended deactivation request from headlamp switch input. |
| Operating Mode: | <S1> Low Beam Activated (ON) |
| Safe State: | Low Beam On (At least one side) |
| Reduced Functionality Tolerance Time Interval: |  |
| Fault Handling Time Segment: | 1000ms |
| Requirement Status | Approved |
| V&V method: | Test |
| V&V acceptance criteria: | Confirm for LIN relative headlamp Switch (LIN\_REL\_SW1), the BCM shall set SW1\_stat as follows:  TBD |
| Allocated Element(s)/Component(s)/ Subsystem(s) | BCM  Headlamp Switch |

Table 33: Verify validity of headlamp switch low beam request - 3

| T-S-Req-ID: | TSR1.1.31 - Verify validity of headlamp switch low beam request - 1 |
| --- | --- |
| External Reference |  |
| Category: | Safety Related Function |
| Safety Goal ID: | SG01 - Ensure Low Beam is not deactivated unintendedly |
| F-S-Req ID: | FSR2 - Arbitration logic working properly for Low Beam activation |
| ASIL Classification: | B |
| Technical Safety Requirement Title: | Verify validity of headlamp switch low beam request - 1 |
| Technical Safety Requirement Text: | The BCM shall determine LIN Relative headlamp switch Channel invalid and set LIN\_Rel\_HLamp\_ValidChan accordingly within 500 ms if either of the following are true:  ·LIN HLamp message (Count Up LINHSM and Count Down LINHSM) is not received  ·Counter and checksum are not valid |
| Rationale: | To prevent communications errors that result in unintended deactivation request from headlamp switch input. |
| Operating Mode: | <S1> Low Beam Activated (ON) |
| Safe State: | Low Beam On (At least one side) |
| Reduced Functionality Tolerance Time Interval: |  |
| Fault Handling Time Segment: | 1000ms |
| Requirement Status | Approved |
| V&V method: | Test |
| V&V acceptance criteria: | Confirm when BCM shall determine LIN Relative headlamp switch Channel invalid and set LIN\_Rel\_HLamp\_ValidChan accordingly within 500 ms if either of the following are true:  ·LIN HLamp message (TBD signal) is not received  ·Counter and checksum are not valid |
| Allocated Element(s)/Component(s)/ Subsystem(s) | BCM |

Table 34: Verify validity of headlamp switch low beam request - 1

| T-S-Req-ID: | TSR1.1.32 - Verify validity of ALS faults |
| --- | --- |
| External Reference |  |
| Category: | Safety Related Function |
| Safety Goal ID: | SG01 - Ensure Low Beam is not deactivated unintendedly |
| F-S-Req ID: | FSR2 - Arbitration logic working properly for Low Beam activation |
| ASIL Classification: | B |
| Technical Safety Requirement Title: | Verify validity of ALS faults |
| Technical Safety Requirement Text: | BCM shall detect short battery and short ground from Ambient Light Sensor (ALS). |
| Rationale: | To prevent unintended errors that result in unintended deactivation from Ambient Light Conditions. |
| Operating Mode: | <S1> Low Beam Activated (ON) |
| Safe State: | Low Beam On (At least one side) |
| Reduced Functionality Tolerance Time Interval: |  |
| Fault Handling Time Segment: | 1000ms |
| Requirement Status | Approved |
| V&V method: | Test |
| V&V acceptance criteria: | Confirm that BCM shall detect short battery and short ground from Ambient Light Sensor (ALS). |
| Allocated Element(s)/Component(s)/ Subsystem(s) | BCM |

Table 35: Verify validity of ALS faults

| T-S-Req-ID: | TSR1.1.33 - Verify validity condition from AUTOLAMP deactivation. |
| --- | --- |
| External Reference |  |
| Category: | Safety Related Function |
| Safety Goal ID: | SG01 - Ensure Low Beam is not deactivated unintendedly |
| F-S-Req ID: | FSR2 - Arbitration logic working properly for Low Beam activation |
| ASIL Classification: | B |
| Technical Safety Requirement Title: | Verify validity condition from AUTOLAMP deactivation. |
| Technical Safety Requirement Text: | BCM shall set AmbientLight\_Stat =Day only when Ambient Light Sensor measures more than 1000Lux and no fault is detected. |
| Rationale: | To prevent reading errors that result in unintended deactivation request from Ambient Light conditions. |
| Operating Mode: | <S1> Low Beam Activated (ON) |
| Safe State: | Low Beam On (At least one side) |
| Reduced Functionality Tolerance Time Interval: |  |
| Fault Handling Time Segment: | 1000ms |
| Requirement Status | Approved |
| V&V method: | Test |
| V&V acceptance criteria: | Confirm that BCM shall set AmbientLight\_Stat =Day only when Ambient Light Sensor measures more than 1000Lux and no fault is detected. |
| Allocated Element(s)/Component(s)/ Subsystem(s) | BCM |

Table 36: Verify validity condition from AUTOLAMP deactivation.

| T-S-Req-ID: | TSR1.1.34 - Verify vehicle speed E2E |
| --- | --- |
| External Reference |  |
| Category: | Safety Related Function |
| Safety Goal ID: | SG01 - Ensure Low Beam is not deactivated unintendedly |
| F-S-Req ID: | FSR2 - Arbitration logic working properly for Low Beam activation |
| ASIL Classification: | B |
| Technical Safety Requirement Title: | Verify vehicle speed E2E |
| Technical Safety Requirement Text: | BCM shall receive vehicle speed (Veh\_V\_ActlBrk and VehVActlBrk\_D\_Qf) with FORD E2E counter and checksum. |
| Rationale: | To prevent single point light failure |
| Operating Mode: | <S1> Low Beam Activated (ON) |
| Safe State: | Low Beam On (At least one side) |
| Reduced Functionality Tolerance Time Interval: |  |
| Fault Handling Time Segment: | 1000ms |
| Requirement Status | Approved |
| V&V method: | Test |
| V&V acceptance criteria: | Confirm that BCM shall receive vehicle speed (Veh\_V\_ActlBrk and VehVActlBrk\_D\_Qf) with FORD E2E counter and checksum. |
| Allocated Element(s)/Component(s)/ Subsystem(s) | BCM |

Table 37: Verify vehicle speed E2E

| T-S-Req-ID: | TSR1.1.35 - Verify the output device - 2 |
| --- | --- |
| External Reference |  |
| Category: | Safety Related Function |
| Safety Goal ID: | SG01 - Ensure Low Beam is not deactivated unintendedly |
| F-S-Req ID: | FSR2 - Arbitration logic working properly for Low Beam activation |
| ASIL Classification: | B |
| Technical Safety Requirement Title: | Verify the output device - 2 |
| Technical Safety Requirement Text: | BCM shall set ExtLightVehPrecondition to ALLOWED when:  - (ABS\_Veh\_Speed < 5kph and ABS\_SpeedValidCahn = VALID)  OR  - (ABS\_Speed\_ValidChan <> VALID  AND  - VehOnSrc\_D\_Stat = Off | RemoteStart | OverTheAir | StolenVehicleInhibit | FleetVehicleInhibit | EsclRssd)  Else set ExtLightVehPrecondition to NOT\_ALLOWED. |
| Rationale: | To prevent unintended deactivation of the output source |
| Operating Mode: | <S1> Low Beam Activated (ON) |
| Safe State: | Low Beam On (At least one side) |
| Reduced Functionality Tolerance Time Interval: |  |
| Fault Handling Time Segment: | 1000ms |
| Requirement Status | Approved |
| V&V method: | Test |
| V&V acceptance criteria: | Confirm that BCM shall set ExtLightVehPrecondition to ALLOWED when:  - (ABS\_Veh\_Speed < 5kph and ABS\_SpeedValidCahn = VALID)  OR  - (ABS\_Speed\_ValidChan <> VALID  AND  - VehOnSrc\_D\_Stat = Off | RemoteStart | OverTheAir | StolenVehicleInhibit | FleetVehicleInhibit | EsclRssd)  Else set ExtLightVehPrecondition to NOT\_ALLOWED. |
| Allocated Element(s)/Component(s)/ Subsystem(s) | BCM |

Table 38: Verify the output device - 2

| T-S-Req-ID: | TSR1.1.36 - Verify the output device - 1 |
| --- | --- |
| External Reference |  |
| Category: | Safety Related Function |
| Safety Goal ID: | SG01 - Ensure Low Beam is not deactivated unintendedly |
| F-S-Req ID: | FSR2 - Arbitration logic working properly for Low Beam activation |
| ASIL Classification: | B |
| Technical Safety Requirement Title: | Verify the output device - 1 |
| Technical Safety Requirement Text: | The BCM shall determine Veh\_V\_ActlBrk Channel invalid and set ABS\_Speed\_ValidChan accordingly within 500 ms if either of the following are true:  ·Veh\_V\_ActlBrk message is not received  ·Counter and checksum are not valid |
| Rationale: | To prevent unintended deactivation of the output source |
| Operating Mode: | <S1> Low Beam Activated (ON) |
| Safe State: | Low Beam On (At least one side) |
| Reduced Functionality Tolerance Time Interval: |  |
| Fault Handling Time Segment: | 1000ms |
| Requirement Status | Approved |
| V&V method: | Test |
| V&V acceptance criteria: | Confirm that BCM shall determine Veh\_V\_ActlBrk Channel invalid and set ABS\_Speed\_ValidChan accordingly within 500 ms if either of the following are true:  ·Veh\_V\_ActlBrk message is not received  ·Counter and checksum are not valid |
| Allocated Element(s)/Component(s)/ Subsystem(s) | BCM |

Table 39: Verify the output device - 1

| T-S-Req-ID: | TSR1.1.39 - Verify validity Absolute LIN E2E signal |
| --- | --- |
| External Reference |  |
| Category: | Safety Related Function |
| Safety Goal ID: | SG01 - Ensure Low Beam is not deactivated unintendedly |
| F-S-Req ID: | FSR2 - Arbitration logic working properly for Low Beam activation |
| ASIL Classification: | B |
| Technical Safety Requirement Title: | Verify validity Absolute LIN E2E signal |
| Technical Safety Requirement Text: | Lin Absolute Position Headlamps Switch shall publish an invalid value (7) in Encoder\_Cnt\_Dn\_LINHSM\_Asil and Encoder\_Cnt\_Up\_LINHSM\_Asil |
| Rationale: | To prevent communications errors that result in unintended deactivation request from headlamp switch input. |
| Operating Mode: | <S1> Low Beam Activated (ON) |
| Safe State: | Low Beam On (At least one side) |
| Reduced Functionality Tolerance Time Interval: |  |
| Fault Handling Time Segment: | 1000ms |
| Requirement Status | Approved |
| V&V method: | Test |
| V&V acceptance criteria: | Confirm Lin Absolute Position Headlamps Switch shall publish an invalid value (7) in Encoder\_Cnt\_Dn\_LINHSM\_Asil and Encoder\_Cnt\_Up\_LINHSM\_Asil |
| Allocated Element(s)/Component(s)/ Subsystem(s) | LIN Absolute Headlamp switch |

Table 40: Verify validity Absolute LIN E2E signal

| T-S-Req-ID: | TSR1.6.15.1 - Verify the arbitrated control of low beams to output device - Left |
| --- | --- |
| External Reference |  |
| Category: | Safety Related Function |
| Safety Goal ID: | SG01 - Ensure Low Beam is not deactivated unintendedly |
| F-S-Req ID: | FSR2 - Arbitration logic working properly for Low Beam activation |
| ASIL Classification: | B |
| Technical Safety Requirement Title: | Verify the arbitrated control of low beams to output device - Left |
| Technical Safety Requirement Text: | When LowBeam\_Rqst is not set to OFF, BCM shall ensure voltage is applied to LF\_Low\_Beam\_Ckt as follows:  When the LF\_Low\_Beam\_Ckt power source is above 11.8 volts, BCM shall apply the minimum VRMS of 9.0 volts.  When the LF\_Low\_Beam\_Ckt power source is at or below 11.8 volts, BCM shall apply power source Voltage with maximum voltage drop of 300mVolts. |
| Rationale: | To prevent unintended deactivation of the output source |
| Operating Mode: | <S1> Low Beam Activated (ON) |
| Safe State: | Low Beam On (At least one side) |
| Reduced Functionality Tolerance Time Interval: |  |
| Fault Handling Time Segment: | 1000ms |
| Requirement Status | Approved |
| V&V method: | Test |
| V&V acceptance criteria: | Confirm when LowBeam\_Rqst is not set to OFF, BCM shall ensure voltage is applied to LF\_Low\_Beam\_Ckt as follows:  When the LF\_Low\_Beam\_Ckt power source is above 11.8 volts, BCM shall apply the minimum VRMS of 9.0 volts.  When the LF\_Low\_Beam\_Ckt power source is at or below 11.8 volts, BCM shall apply power source Voltage with maximum voltage drop of 300mVolts. |
| Allocated Element(s)/Component(s)/ Subsystem(s) | BCM |

Table 41: Verify the arbitrated control of low beams to output device - Left

| T-S-Req-ID: | TSR1.6.15.2 - Verify the arbitrated control of low beams to output device - Right |
| --- | --- |
| External Reference |  |
| Category: | Safety Related Function |
| Safety Goal ID: | SG01 - Ensure Low Beam is not deactivated unintendedly |
| F-S-Req ID: | FSR2 - Arbitration logic working properly for Low Beam activation |
| ASIL Classification: | B |
| Technical Safety Requirement Title: | Verify the arbitrated control of low beams to output device - Right |
| Technical Safety Requirement Text: | When LowBeam\_Rqst is not set to OFF, BCM shall ensure voltage is applied to RF\_Low\_Beam\_Ckt as follows:  When the RF\_Low\_Beam\_Ckt power source is above 11.8 volts, BCM shall apply the minimum VRMS of 9.0 volts.  When the RF\_Low\_Beam\_Ckt power source is at or below 11.8 volts, BCM shall apply power source Voltage with maximum voltage drop of 300mVolts. |
| Rationale: | To prevent unintended deactivation of the output source |
| Operating Mode: | <S1> Low Beam Activated (ON) |
| Safe State: | Low Beam On (At least one side) |
| Reduced Functionality Tolerance Time Interval: |  |
| Fault Handling Time Segment: | 1000ms |
| Requirement Status | Approved |
| V&V method: | Test |
| V&V acceptance criteria: | Confirm when LowBeam\_Rqst is not set to OFF, BCM shall ensure voltage is applied to RF\_Low\_Beam\_Ckt as follows:  When the RF\_Low\_Beam\_Ckt power source is above 11.8 volts, BCM shall apply the minimum VRMS of 9.0 volts.  When the RF\_Low\_Beam\_Ckt power source is at or below 11.8 volts, BCM shall apply power source Voltage with maximum voltage drop of 300mVolts. |
| Allocated Element(s)/Component(s)/ Subsystem(s) | BCM |

Table 42: Verify the arbitrated control of low beams to output device - Right

### Requirement Derivation Diagram(s) for FSR3 - Activation of light sources

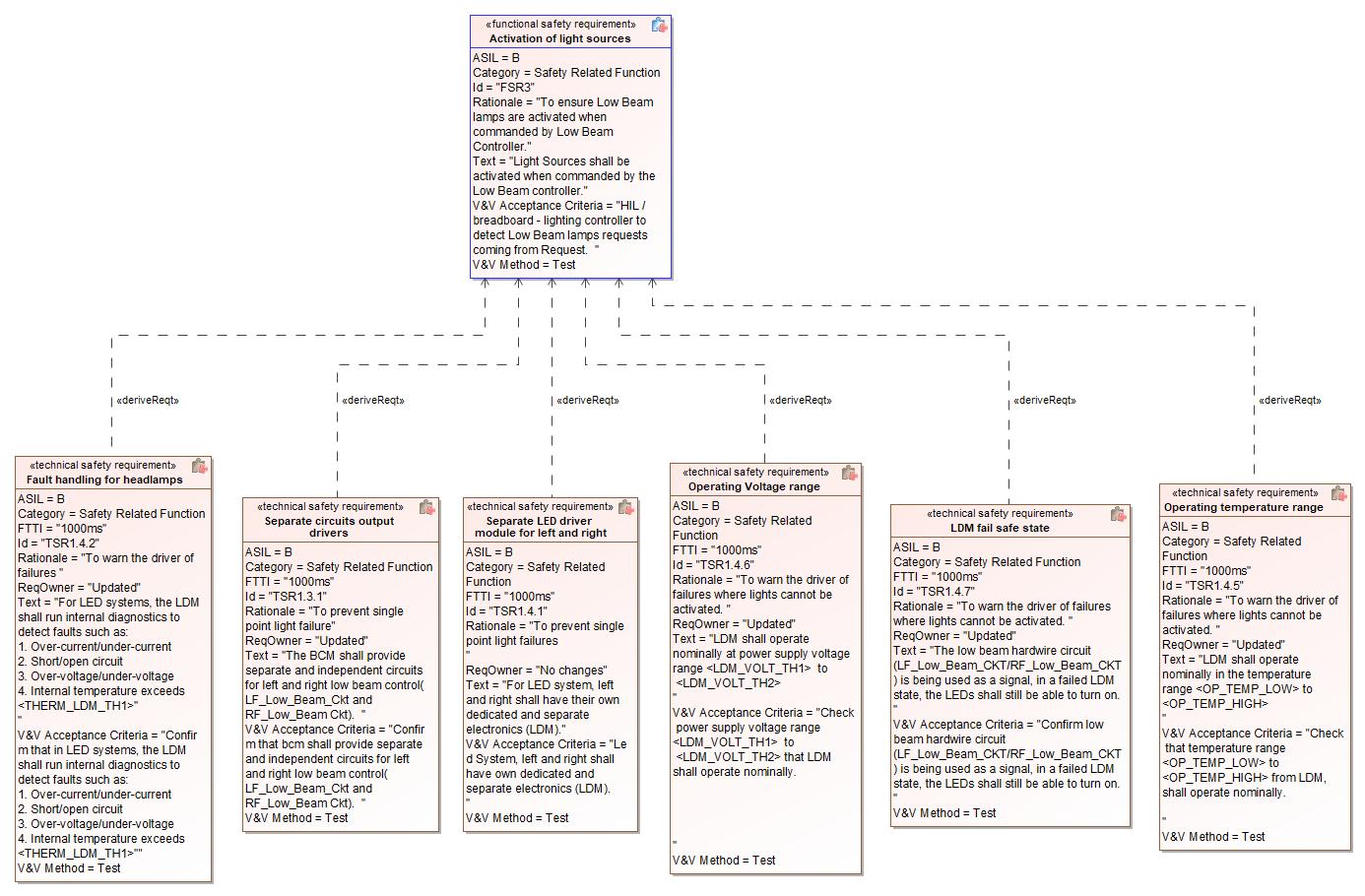


Figure 7 - Technical Safety Requirements Derivation Diagram for FSR3 - Activation of light sources – Activation of light sources

| T-S-Req-ID: | TSR1.3.1 - Separate circuits output drivers |
| --- | --- |
| External Reference |  |
| Category: | Safety Related Function |
| Safety Goal ID: | SG01 - Ensure Low Beam is not deactivated unintendedly |
| F-S-Req ID: | FSR3 - Activation of light sources |
| ASIL Classification: | B |
| Technical Safety Requirement Title: | Separate circuits output drivers |
| Technical Safety Requirement Text: | The BCM shall provide separate and independent circuits for left and right low beam control( LF\_Low\_Beam\_Ckt and RF\_Low\_Beam Ckt). |
| Rationale: | To prevent single point light failure |
| Operating Mode: | <S1> Low Beam Activated (ON) |
| Safe State: | Low Beam On (At least one side) |
| Reduced Functionality Tolerance Time Interval: |  |
| Fault Handling Time Segment: | 1000ms |
| Requirement Status | Approved |
| V&V method: | Test |
| V&V acceptance criteria: | Confirm that bcm shall provide separate and independent circuits for left and right low beam control( LF\_Low\_Beam\_Ckt and RF\_Low\_Beam Ckt). |
| Allocated Element(s)/Component(s)/ Subsystem(s) | BCM |

Table 43: Separate circuits output drivers

| T-S-Req-ID: | TSR1.4.1 - Separate LED driver module for left and right |
| --- | --- |
| External Reference |  |
| Category: | Safety Related Function |
| Safety Goal ID: | SG01 - Ensure Low Beam is not deactivated unintendedly |
| F-S-Req ID: | FSR3 - Activation of light sources |
| ASIL Classification: | B |
| Technical Safety Requirement Title: | Separate LED driver module for left and right |
| Technical Safety Requirement Text: | For LED system, left and right shall have their own dedicated and separate electronics (LDM). |
| Rationale: | To prevent single point light failures |
| Operating Mode: | <S1> Low Beam Activated (ON) |
| Safe State: | Low Beam On (At least one side) |
| Reduced Functionality Tolerance Time Interval: |  |
| Fault Handling Time Segment: | 1000ms |
| Requirement Status | Approved |
| V&V method: | Test |
| V&V acceptance criteria: | Led System, left and right shall have own dedicated and separate electronics (LDM). |
| Allocated Element(s)/Component(s)/ Subsystem(s) | Headlamps  LDM |

Table 44: Separate LED driver module for left and right

| T-S-Req-ID: | TSR1.4.2 -  Fault handling for headlamps |
| --- | --- |
| External Reference |  |
| Category: | Safety Related Function |
| Safety Goal ID: | SG01 - Ensure Low Beam is not deactivated unintendedly |
| F-S-Req ID: | FSR3 - Activation of light sources |
| ASIL Classification: | B |
| Technical Safety Requirement Title: | Fault handling for headlamps |
| Technical Safety Requirement Text: | For LED systems, the LDM shall run internal diagnostics to detect faults such as:  1. Over-current/under-current  2. Short/open circuit  3. Over-voltage/under-voltage  4. Internal temperature exceeds <THERM\_LDM\_TH1>" |
| Rationale: | To warn the driver of failures |
| Operating Mode: | <S1> Low Beam Activated (ON) |
| Safe State: | Low Beam On (At least one side) |
| Reduced Functionality Tolerance Time Interval: |  |
| Fault Handling Time Segment: | 1000ms |
| Requirement Status | Approved |
| V&V method: | Test |
| V&V acceptance criteria: | Confirm that in LED systems, the LDM shall run internal diagnostics to detect faults such as:  1. Over-current/under-current  2. Short/open circuit  3. Over-voltage/under-voltage  4. Internal temperature exceeds <THERM\_LDM\_TH1>" |
| Allocated Element(s)/Component(s)/ Subsystem(s) | LDM |

Table 45: Fault handling for headlamps

| T-S-Req-ID: | TSR1.4.5 - Operating temperature range |
| --- | --- |
| External Reference |  |
| Category: | Safety Related Function |
| Safety Goal ID: | SG01 - Ensure Low Beam is not deactivated unintendedly |
| F-S-Req ID: | FSR3 - Activation of light sources |
| ASIL Classification: | B |
| Technical Safety Requirement Title: | Operating temperature range |
| Technical Safety Requirement Text: | LDM shall operate nominally in the temperature range <OP\_TEMP\_LOW> to <OP\_TEMP\_HIGH> |
| Rationale: | To warn the driver of failures where lights cannot be activated. |
| Operating Mode: | <S1> Low Beam Activated (ON) |
| Safe State: | Low Beam On (At least one side) |
| Reduced Functionality Tolerance Time Interval: |  |
| Fault Handling Time Segment: | 1000ms |
| Requirement Status | Approved |
| V&V method: | Test |
| V&V acceptance criteria: | Check that temperature range <OP\_TEMP\_LOW> to <OP\_TEMP\_HIGH> from LDM, shall operate nominally. |
| Allocated Element(s)/Component(s)/ Subsystem(s) | Headlamps  LDM |

Table 46: Operating temperature range

| T-S-Req-ID: | TSR1.4.6 - Operating Voltage range |
| --- | --- |
| External Reference |  |
| Category: | Safety Related Function |
| Safety Goal ID: | SG01 - Ensure Low Beam is not deactivated unintendedly |
| F-S-Req ID: | FSR3 - Activation of light sources |
| ASIL Classification: | B |
| Technical Safety Requirement Title: | Operating Voltage range |
| Technical Safety Requirement Text: | LDM shall operate nominally at power supply voltage range <LDM\_VOLT\_TH1> to <LDM\_VOLT\_TH2> |
| Rationale: | To warn the driver of failures where lights cannot be activated. |
| Operating Mode: | <S1> Low Beam Activated (ON) |
| Safe State: | Low Beam On (At least one side) |
| Reduced Functionality Tolerance Time Interval: |  |
| Fault Handling Time Segment: | 1000ms |
| Requirement Status | Approved |
| V&V method: | Test |
| V&V acceptance criteria: | Check power supply voltage range <LDM\_VOLT\_TH1> to <LDM\_VOLT\_TH2> that LDM shall operate nominally. |
| Allocated Element(s)/Component(s)/ Subsystem(s) | Headlamps  LDM |

Table 47: Operating Voltage range

| T-S-Req-ID: | TSR1.4.7 - LDM fail safe state |
| --- | --- |
| External Reference |  |
| Category: | Safety Related Function |
| Safety Goal ID: | SG01 - Ensure Low Beam is not deactivated unintendedly |
| F-S-Req ID: | FSR3 - Activation of light sources |
| ASIL Classification: | B |
| Technical Safety Requirement Title: | LDM fail safe state |
| Technical Safety Requirement Text: | The low beam hardwire circuit (LF\_Low\_Beam\_CKT/RF\_Low\_Beam\_CKT) is being used as a signal, in a failed LDM state, the LEDs shall still be able to turn on. |
| Rationale: | To warn the driver of failures where lights cannot be activated. |
| Operating Mode: | <S1> Low Beam Activated (ON) |
| Safe State: | Low Beam On (At least one side) |
| Reduced Functionality Tolerance Time Interval: |  |
| Fault Handling Time Segment: | 1000ms |
| Requirement Status | Approved |
| V&V method: | Test |
| V&V acceptance criteria: | Confirm low beam hardwire circuit (LF\_Low\_Beam\_CKT/RF\_Low\_Beam\_CKT) is being used as a signal, in a failed LDM state, the LEDs shall still be able to turn on. |
| Allocated Element(s)/Component(s)/ Subsystem(s) | Headlamps  LDM |

Table 48: LDM fail safe state

## Timing Specification

### Fault Tolerant Time Interval (FTTI) Identification

*This section to be left blank.*

| **F-S-Req-ID** | Fault tolerant time interval (from Functional Safety Concept) | **Element/Component/System or Communication Channel1** | **T-S-Req-ID1** | **Fault Handling Time Interval for T-S-Req. or**  **[Time Delay of Communication Channel]**  Explanation (if necessary)  [Note (if necessary)]1 |
| --- | --- | --- | --- | --- |
| FSR1 |  | Controller | TSR1.1.1 | 1000ms |
| TSR1.1.27 | 1000ms |
| TSR1.1.30 | 1000ms |
| TSR1.1.37 | 1000ms |
| TSR1.2.1.2 | 1000ms |
| TSR1.2.1.2.1 | 1000ms |
| TSR1.2.2 | 1000ms |
| TSR1.2.3 | 1000ms |
| TSR1.2.4 | 1000ms |
| TSR1.2.7 | 1000ms |
| TSR1.2.8 | 1000ms |
| TSR1.2.10 | 1000ms |
| HMI | TSR1.1.1 | 1000ms |
| TSR1.1.27 | 1000ms |
| TSR1.1.30 | 1000ms |
| TSR1.1.37 | 1000ms |
| TSR1.2.1.2 | 1000ms |
| TSR1.2.1.2.1 | 1000ms |
| TSR1.2.2 | 1000ms |
| TSR1.2.3 | 1000ms |
| TSR1.2.4 | 1000ms |
| TSR1.2.7 | 1000ms |
| TSR1.2.8 | 1000ms |
| TSR1.2.10 | 1000ms |
| FSR2 |  | Arbitration Subsystem | TSR1.1.4 | 1000ms |
| TSR1.1.6 | 1000ms |
| TSR1.1.8 | 1000ms |
| TSR1.1.9 | 1000ms |
| TSR1.1.10 | 1000ms |
| TSR1.1.11 | 1000ms |
| TSR1.1.12 | 1000ms |
| TSR1.1.16 | 1000ms |
| TSR1.1.19 | 1000ms |
| TSR1.1.20 | 1000ms |
| TSR1.1.23 | 1000ms |
| TSR1.1.26 | 1000ms |
| TSR1.1.28 | 1000ms |
| TSR1.1.29 | 1000ms |
| TSR1.1.30 | 1000ms |
| TSR1.1.31 | 1000ms |
| TSR1.1.32 | 1000ms |
| TSR1.1.33 | 1000ms |
| TSR1.1.34 | 1000ms |
| TSR1.1.35 | 1000ms |
| TSR1.1.36 | 1000ms |
| TSR1.1.39 | 1000ms |
| TSR1.6.15.1 | 1000ms |
| TSR1.6.15.2 | 1000ms |
| Controller | TSR1.1.4 | 1000ms |
| TSR1.1.6 | 1000ms |
| TSR1.1.8 | 1000ms |
| TSR1.1.9 | 1000ms |
| TSR1.1.10 | 1000ms |
| TSR1.1.11 | 1000ms |
| TSR1.1.12 | 1000ms |
| TSR1.1.16 | 1000ms |
| TSR1.1.19 | 1000ms |
| TSR1.1.20 | 1000ms |
| TSR1.1.23 | 1000ms |
| TSR1.1.26 | 1000ms |
| TSR1.1.28 | 1000ms |
| TSR1.1.29 | 1000ms |
| TSR1.1.30 | 1000ms |
| TSR1.1.31 | 1000ms |
| TSR1.1.32 | 1000ms |
| TSR1.1.33 | 1000ms |
| TSR1.1.34 | 1000ms |
| TSR1.1.35 | 1000ms |
| TSR1.1.36 | 1000ms |
| TSR1.1.39 | 1000ms |
| TSR1.6.15.1 | 1000ms |
| TSR1.6.15.2 | 1000ms |
| Output Device | TSR1.1.4 | 1000ms |
| TSR1.1.6 | 1000ms |
| TSR1.1.8 | 1000ms |
| TSR1.1.9 | 1000ms |
| TSR1.1.10 | 1000ms |
| TSR1.1.11 | 1000ms |
| TSR1.1.12 | 1000ms |
| TSR1.1.16 | 1000ms |
| TSR1.1.19 | 1000ms |
| TSR1.1.20 | 1000ms |
| TSR1.1.23 | 1000ms |
| TSR1.1.26 | 1000ms |
| TSR1.1.28 | 1000ms |
| TSR1.1.29 | 1000ms |
| TSR1.1.30 | 1000ms |
| TSR1.1.31 | 1000ms |
| TSR1.1.32 | 1000ms |
| TSR1.1.33 | 1000ms |
| TSR1.1.34 | 1000ms |
| TSR1.1.35 | 1000ms |
| TSR1.1.36 | 1000ms |
| TSR1.1.39 | 1000ms |
| TSR1.6.15.1 | 1000ms |
| TSR1.6.15.2 | 1000ms |
| FSR3 |  | Arbitration Subsystem | TSR1.3.1 | 1000ms |
| TSR1.4.1 | 1000ms |
| TSR1.4.2 | 1000ms |
| TSR1.4.5 | 1000ms |
| TSR1.4.6 | 1000ms |
| TSR1.4.7 | 1000ms |
| Controller | TSR1.3.1 | 1000ms |
| TSR1.4.1 | 1000ms |
| TSR1.4.2 | 1000ms |
| TSR1.4.5 | 1000ms |
| TSR1.4.6 | 1000ms |
| TSR1.4.7 | 1000ms |
| Output Device | TSR1.3.1 | 1000ms |
| TSR1.4.1 | 1000ms |
| TSR1.4.2 | 1000ms |
| TSR1.4.5 | 1000ms |
| TSR1.4.6 | 1000ms |
| TSR1.4.7 | 1000ms |

Table 49: Fault tolerant time interval allocation to Elements/Components/Subsystems

#### Safety Goal X

*This section to be left blank. Repeat this section for each Safety Goal and fill out the subsections accordingly.*

##### Malfunctioning Behavior Y

*Fill out the tables below:*

HMT:

*Fill out the following table.*

|  |
| --- |
| **Safety Mechanism:** |
| *<Insert Safety Mechanism Name>* |
| **Associated Hazardous Event(s):** |
| *<Insert the Hazardous Event ID(s) from the HARA that are covered by the Safety Mechanism>* |
| **Hazard Manifestation Time (HMT):** |
| *<Insert the HMT constraint on the Safety Mechanism>* |
| **References:** |
| *<Insert a reference to the testing/simulation Data and/or studies/publications used to determine the HMT>* |
| **Explanation:** |
| *<Explain the significance of the Data, Studies or Publications used how the Hazard Manifestation Time (HMT) was determined>* |

Table 50: Safety Mechanism Y HMT Summary

MBMT:

*Fill out the following table and optionally insert a sequence (or other timing diagram/chart) below illustrating the relevant failure paths starting with the failure and ending at the physical manifestation of the malfunctioning behavior (excess torque produced, incorrect steering, lack of message, etc).*

|  |  |  |
| --- | --- | --- |
| **Safety Mechanism:** | | |
| *<Insert Safety Mechanism Name>* | | |
| **Malfunctioning Behavior Manifestation Time (MBMT):** | | |
| *<Insert the minimum MBMT across each failure cause covered by the Safety Mechanism>* | | |
| **References:** | | |
| *<Insert a reference to any timing diagrams or analysis document used to determine the MBMT or alternately insert a sequence diagram/timing analysis below this table>* | | |
| **Component** | **Failure Cause** | **Malfunctioning Behavior Manifestation Time (MBMT)** |
| *Sensor 1* | *Shorted High* | *110ms* |
| *Actuator 1* | *Stuck in Range* | *30ms* |
|  |  |  |
|  |  |  |

Table 51: Safety Mechanism Y MBMT Summary

FTTI:

*Fill out the following table based on the information provided above.*

|  |  |  |
| --- | --- | --- |
| **FTTI Name/ID** | **FTTI Value** | **Applicable Component Failure Modes** |
| *FTTI\_SG1\_MB1\_2* | *1500ms* | *Sensor 1 Shorted High* |
| *Sensor 2 Stuck in range* |
| *Actuator 1 Non functional* |
| *Controller 1 Loss of Com* |
| *FTTI\_SG2* |  |  |

Table 52: FTTI Summary

### Fault Handling Time Specification

*This section to be left blank.*

#### Achieving the FHT for SG X

*This section to be left blank. Repeat this section for each Safety Goal and fill out the subsections accordingly.*

##### Malfunctioning Behavior Y

*Repeat this section for each FTTI Identified in the preceding sections.*

###### FHT Functional Timing for FTTI X

*Add sequence/timing diagrams below starting with the failure and ending with the achievement of the safe state. Under each diagram, state the combined FHT of the sequence.*

###### Fault Handling Time Summary

*For each function involved in achieving the safe state list the contribution to the Fault Handling Time and the TSR that states the FHT requirement.*

|  |  |  |
| --- | --- | --- |
| **Atomic Function** | **Contribution to the Fault Handling Time** | **Requirement ID** |
| Diagnose Component A Failure Mode X | 50ms | TSR-00X |
| Transmit XYZ on CAB | 10ms | TSR-00Y |
| Display Message to driver | 10ms | TSR-00W |

Table 53: FHT Summary

## Derivation of Reduced Functionality Interval (optional)

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

## Operating Modes Overview (optional)



Figure 8: Operating Modes Overview Diagram

| **Operating Mode in the Functional Safety Concept [FFSD03]**  (if applicable) | Operating Mode used in tables in Section 3.1 | **Description** |
| --- | --- | --- |
|  |  |  |
|  | <S1> Low Beam Activated (ON) | At vehicle start the feature is disabled until all the enabling conditions are met. |
|  | <S2> Low Beam Deactivated (OFF) | Feature is enabled when the enabling conditions are met, and driver turn ON low beams using lamp control |
|  | <T1> Enabling Condition IGN=RUN/ACC || IGN=OFF && MLC=ON | Enable Low Beam feature when the Ignition is switched to RUN/ACC OR Ignition is OFF and MLC is switched to ON position |
|  | <T2> Disabling Condition IGN=OFF && MLC<> ON | Disable Low Beam feature when the Ignition is switched OFF AND MLC is not in ON position |
|  | <T3>Activate Low Beam | Activate Low Beam when Master Lighting Control/Reductive Control switch is ON OR if Master Lighting Control/Reductive Control Switch is in AUTO then take the input from Ambient Light,  Wiper and Rain Sensor  Trigger signal: Master Lighting Control/Reductive Switch = ON OR  Master Lighting Control/Reductive Switch = AUTO AND  Ambient Light Sensor/Reductive Switchr = DARK AND  Rain Sensor = DAY AND  Wiper Sensor = OFF OR  Master Lighting Control/Reductive Switch = AUTO AND  Ambient Light Sensor = LIGHT AND  Rain Sensor = NIGHT AND  Wiper Sensor = ON |
|  | <T4> Deactivate Low Beam | Deactivate Low Beam when Master Lighting Control is OFF OR if Master Lighting Control is in AUTO then take the input from Ambient Light,  Wiper and Rain Sensor to switch off the Low Beams  Trigger signal: Master Lighting Control Switch = OFF OR  Master Lighting Control Switch = AUTO AND  Ambient Light Sensor = LIGHT AND  Rain Sensor = DAY AND  Wiper Sensor = OFF |
|  | <T5> Activate Low Beam | Activate Low Beam when Master Lighting Control is ON OR if Master Lighting Control is in AUTO then take the input from Ambient Light,  Wiper and Rain Sensor |
|  | Disabled Feature | At vehicle start the feature is disabled until all the enabling conditions are met. |
|  | Enabled Feature | Feature is enabled when the enabling conditions are met, and driver turn ON low beams using lamp control |
|  | Low Beam On | Normal operation |
|  | Low Beam On (At least one side) | One Side Low Beam On |

Table 54: Operating Modes

## HW Metric Requirements - Derivation and Rationale

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

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

Table 55: PMHF derivation

### Single Point Faults and Latent Faults Metric

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

Table 56: Single Point Fault Metric derivation

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

Table 57: Latent Fault Metric derivation

## Allocation (optional)

| **Element/Component/System Name** | **Inside (I)/ Outside (O) Item Boundary** | **Technical Safety Requirement ID** | **Technical Safety Requirement ASIL** | **Element/Component/ System ASIL** |
| --- | --- | --- | --- | --- |
| APIM\_CDC | O | TSR1.2.1.2 | B | B |
| TSR1.2.1.2.1 | B | B |
| TSR1.2.4 | B | B |
| TSR1.2.7 | B | B |
| TSR1.2.8 | B | B |
| TSR1.2.10 | B | B |
| BCM | I | TSR1.1.1 | B | B |
| TSR1.1.4 | B | B |
| TSR1.1.6 | B | B |
| TSR1.1.8 | B | B |
| TSR1.1.9 | B | B |
| TSR1.1.10 | B | B |
| TSR1.1.11 | B | B |
| TSR1.1.12 | B | B |
| TSR1.1.16 | B | B |
| TSR1.1.19 | B | B |
| TSR1.1.20 | B | B |
| TSR1.1.23 | B | B |
| TSR1.1.26 | B | B |
| TSR1.1.27 | B | B |
| TSR1.1.28 | B | B |
| TSR1.1.29 | B | B |
| TSR1.1.30 | B | B |
| TSR1.1.31 | B | B |
| TSR1.1.32 | B | B |
| TSR1.1.33 | B | B |
| TSR1.1.34 | B | B |
| TSR1.1.35 | B | B |
| TSR1.1.36 | B | B |
| TSR1.3.1 | B | B |
| TSR1.6.15.1 | B | B |
| TSR1.6.15.2 | B | B |
| Headlamp Switch | I | TSR1.1.30 | B | B |
| TSR1.2.2 | B | B |
| Headlamps | O | TSR1.4.1 | B | B |
| TSR1.4.5 | B | B |
| TSR1.4.6 | B | B |
| TSR1.4.7 | B | B |
| LDM | I | TSR1.4.1 | B | B |
| TSR1.4.2 | B | B |
| TSR1.4.5 | B | B |
| TSR1.4.6 | B | B |
| TSR1.4.7 | B | B |
| LIN Absolute Headlamp switch | O | TSR1.1.1 | B | B |
| TSR1.1.39 | B | B |
| TSR1.2.3 | B | B |
| LIN Relative Headlamp switch | O | TSR1.1.1 | B | B |
| TSR1.1.37 | B | B |
| TSR1.2.3 | B | B |

Table 58: Allocation of Technical Safety Requirements

## ASIL Decomposition- Derivation and Rationale (optional)

ASIL Decompositions not specified.

## Safety Related Parameters

*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.*

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Parameter name | Description | Range  Resolution  Initial Value  Unit | Rationale and/or  Constraints | Cali-brat-able | Used in Requirements  (add ID and name of requirement) |

Table 59: Parameter

## Cascading Technical Safety Requirements

*The project specific document setup shall be used for exchanging requirements with the component/system provider. The guideline describes in section 2.3.3.9.x information has to be requested from the component/system provider depending on the requirement category.*

*This section of the document can be left empty or deleted.*

# Requirements for Production, Operation, Service and Decommissioning

**Production Plan:**

*Define or reference all safety related content for the production plan.* Refer (and may create) requirements for production (examples are given in FFSG, Section 11.2.1.2). These requirements will be linked in FFSD08 V&V Report to the safety analysis. This guarantees that the FMA process is applied for these requirements. Additionally, the V&V of these requirement is referenced in FFSD08 V&V Report. In the FFSD08, the requirement can be closed by referring the DFMEA.

**Owner’s Manual:**

*Define or reference all safety related content for owner’s manual an add references to related technical safety requirements.* *The persons creating the owner’s manual will contact the feature owner when the owner’s manual is created. These requirements will be linked in FFSD08 V&V Report to the safety analysis. This guarantees that the FMA process is applied for these requirements. Additionally, the V&V of these requirement is referenced in FFSD08 V&V Report. In the FFSD08, the requirement can be closed by referring the DFMEA.*

**Service Manual:**

*Define or reference all safety related content for service manual an add references to related technical safety requirements.* *The persons creating the service manual will contact the feature owner when the service manual is created. These requirements will be linked in FFSD08 V&V Report to the safety analysis. This guarantees that the FMA process is applied for these requirements. Additionally, the V&V of these requirement is referenced in FFSD08 V&V Report. In the FFSD08, the requirement can be closed by referring the DFMEA.*

**Decommissioning:**

*Define or reference all safety related content for decommissioning an add references to related technical safety requirements.* *These requirements will be linked in FFSD08 V&V Report to the safety analysis. This guarantees that the FMA process is applied for these requirements. Additionally, the V&V of these requirement is referenced in FFSD08 V&V Report. In the FFSD08, the requirement can be closed by referring the DFMEA.*

# Safety Analysis

*A Safety Analysis (e.g. FTA with comments for rationales, top-down FMEA with comments for rationales, GSN, MBSE with comments for rationales) shall be performed to:*

1. *show compliance and consistency between the Technical Safety Concept and the Functional Safety concept and the preliminary architectural assumptions.*
2. *verify the system design regarding compliance and completeness with regard to the technical safety concept.*

*Insert a reference to the Safety Analysis (e.g. Fault Tree Analysis (FTA) with comments for rationales, top-down FMEA with comments for rationales, System-Theoretic Process Analysis (STPA), Argument for Safety Requirement Derivation (ASRD) using GSN, FMEA, Structured Technical Safety Requirement Development using SysML with comments for rationales, Simulation documentation (if necessary) and Test documentation (if necessary).*

# Execution and Results of Verification Review

|  |  |  |
| --- | --- | --- |
| **Date of review completion** | **Reviewed Version of FFSD** | **Responsible Person for Review** |
| **2/16/22** | **SRS3** | **Claudio Labate**  **Rafael Oliveira** |

Table 60: 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. The Verification review shall be completed with your organization's Application Functional Safety Engineer see the* [*Verification Review Process*](https://azureford.sharepoint.com/sites/GlobalFunctionalSafety/Functional%20Safety%20FAQ%20Wiki%20Page/Verification%20Review%20Process.aspx)*.*

### Verification Review of Safety Requirements Specification

| **Completed according to the Guidelines?** | | **Yes /**  **No** |
| --- | --- | --- |
| Input from System Design, Item Definition / Feature Document, and Functional Safety Concept  *(GPDS: UNV0/UPV0, GTDS: <AR>)* | External Interfaces | Yes |
| Constraints | Yes |
| Technical Block Diagram | Yes |
| Functional Overview of Elements/Components/Subsystems | Yes |
| Implementation Details of Internal Interfaces | Yes |
| System Level architecture (including redundancy) | Yes |
| Technical Safety Requirements Specification  Technical Safety Requirements Derivation | Derivation of Technical Safety Requirements (without V&V acceptance criteria)  *(GPDS: UNV0/UPV0, GTDS: <AR>)* | Yes |
| Definition of Technical Safety Requirements V&V acceptance criteria  *(GPDS: UNV1/UPV1)* | Yes |
| Derivation of Fault Tolerant Time  *(GPDS: UNV0/UPV0, GTDS: <AR>)* | Yes |
| Derivation of Reduced Functionality (interval)  *(GPDS: UNV0/UPV0, GTDS: <AR>)* | Yes |
| Consistency between Technical Safety Requirements and Functional Safety Concept  *Note: Methods could be Safety Analyses, e.g. Fault Tree Analysis (FTA), System-Theoretic Process Analysis (STPA), Argument for Safety Requirement Derivation (ASRD) using GSN, FMEA, Structured Technical Safety Requirement Development using SysML (all with rationales), see also ISO 26262, Part 4, 7.5.8* | Yes |
| Each Technical Safety Requirement   * contains all required attributes (except “V&V acceptance criteria”)   *(GPDS: UNV0/UPV0, GTDS: <AR>)* | Yes |
| Each Technical Safety Requirement   * is simple, atomic, verifiable, necessary, achievable, and traceable   *(GPDS: UNV0/UPV0, GTDS: <AR>)* | Yes |
| Each Technical Safety Requirement   * is accepted by the element/component/subsystem provider   *Note: To accept the requirements use the current engineering process.*  *(GPDS: UNV0/UPV0, GTDS: <AR>)* | Yes |
| Constraints are transformed into requirements  *(GPDS: UNV0/UPV0, GTDS: <AR>)* | Yes |
| 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>)* | Yes |
| ASIL Decomposition (Optional)  *(GPDS: UNV0/UPV0, GTDS: <AR>)* | Yes |
| Safety Related Parameters  *(GPDS: UNV0/UPV0, GTDS: <AR>)* | Yes |
| Requirements concerning the ability to configure a system by calibration data are defined  *(GPDS: UNV0/UPV0, GTDS: <AR>)* | Yes |
| Each Technical Safety Requirement  can be verified  *(GPDS: UNV0/UPV0, GTDS: <AR>)* | Yes |
| The Technical Safety Requirements are consistent and complete regarding the System Design, including "Response to Stimuli".  *(GPDS: UNV0/UPV0, GTDS: <AR>)* | Yes |
| All Technical Safety requirements are traceable to Functional Safety requirements. *(GPDS: UNV0/UPV0, GTDS: <AR>)* | Yes |
| The set of safety requirements is externally consistent? The Technical Safety Requirements and non-Safety Requirements do not contradict. *(GPDS: UNV0/UPV0, GTDS: <AR>)* | Yes |
| There are no contradictions between Functional Safety Requirements and Technical Safety Requirements  *(GPDS: UNV0/UPV0, GTDS: <AR>)* | Yes |
| Each Technical Safety Requirement does not repeat any other Technical Safety Requirement.  *(GPDS: UNV0/UPV0, GTDS: <AR>)* | Yes |
| System Design  *(GPDS: UNV0/UPV0, GTDS: <AR>)* | 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”)* | Yes |
| … fulfils the Technical Safety Requirements  *Note: Methods could be: System design inspection, System design walkthrough, Simulation, Prototyping and vehicle tests, Safety analyses, e.g. System Level FMEA, Argument for Safety Requirement Derivation (ASRD) using GSN, Fault Tree Analysis (FTA), Structured Technical Safety Requirement Development using SysML (all with rationales), System -Theoretic Process Analysis (STPA),…* | Yes |
| … is aligned with assumptions on the Preliminary Architectural Design in the Functional Safety Concept.  *Note: Methods could be: System design inspection, System design walkthrough, Simulation, Prototyping and vehicle tests, Safety analyses, e.g. System Level FMEA, Argument for Safety Requirement Derivation (ASRD) using GSN, Fault Tree Analysis (FTA), Structured Technical Safety Requirement Development using SysML (all with rationales), System -Theoretic Process Analysis (STPA),…* | Yes |
| Timing Specification | The specified FTTI is less than or equal to the sum of the HMT and MBMT for each failure mode covered by the Safety Mechanism. See section 3.2.1.X. | Yes |
| The specified FHT is equal to the sum of the FHT segments assigned to the functions involved in achieving the safe state. This needs to be evaluated for each functional path/flow. See section 3.2.2.X | Yes |
| The total FHT for each failure is less than the specified FTTI being addressed | Yes |
| Requirements for Operation, Service and Decommissioning  *(GPDS: UNV0/UPV0, GTDS: <AR>)* | Requirements for Operation and Service completed | Yes |
| Technical Safety Requirements on Elements/Components/Subsystems  *(GPDS: UNV1/UPV1, GTDS: n/a)* | V&V acceptance criteria | Yes |

Table 61: Checklist for Completeness of Safety Requirements Specification

### Verification Review of Safety Analyses of Safety Requirements Specification (optional)

*This section shall be completed within UNV0 for UN or UPV0 for UP features.*

*Note: This section provides detailed requirements for the FFSD04 Safety Requirements Specification, section 6 (FFSD > v6.16)*

| **Checklist for Safety Analysis** | **Applicable for ASIL** | **Fulfilled (yes/no)** | **Remarks** |
| --- | --- | --- | --- |
| **Generic Safety Analysis Requirements** | | | |
| Are the Safety Analyses performed in accordance with appropriate Standards or Guidelines  Note: Minimum is FFSG06 Safety Analysis Report Guideline and Ford FMEA Handbook. | A-D |  |  |
| Are the elements of the Safety Analysis traceable to Safety Requirements (including document version of the specifications) and vice versa?  Note: Can be checked using FFSD08 Safety V&V Report. | A-D |  |  |
| Is an inductive analysis performed on system level? | A-D |  |  |
| Is a deductive analysis performed on system level? | (B), C, D |  |  |
| Do the inductive and deductive Safety Analyses include   * a systematic identification of faults or malfunctioning behaviours that could lead to the violation of safety goals or safety requirements, * the evaluation of the consequences of each identified fault, * the identification of the causes of each identified fault, and * the identification, or the support for the identification, of potential safety concept weaknesses, including the ineffectiveness of safety mechanisms in handling anomalies such as latent faults, multiple-point faults, common cause failures and cascading failures? | A-D |  |  |
| Do the inductive and deductive Safety Analyses cover   * the commodity or * the interaction of the commodities with other commodities, or * the usage of the commodity? | A-D |  |  |
| Are the results from the Safety Analyses used for deriving requirements, and are these requirements fed back into the specification documents? | A-D |  |  |
| **Quantitative Safety Analysis Requirements** | | | |
| Is a quantitative analysis performed to verify that the target values are defined appropriately? | (B), C, D |  |  |
| To avoid single point faults, is evidence of the ability of the safety mechanisms to maintain a safe state, or to switch safely into a safe state, available?  *Note: Evidence can be provided by referencing the element within the analysis to the specification of the safety mechanism.* | (B), C, D |  |  |
| To avoid latent faults, is evidence of the ability to notify to the driver, within the acceptable multiple-point fault detection interval available  *Note: Evidence can be provided by referencing the element within the analysis to the specification of the safety mechanism.* | (B), C, D |  |  |
| **Dependent Failure Analysis Requirements** | | | |
| Is an appropriate safety analysis performed to identify potential causes for dependent failures (e.g. FTA Cut Set evaluation, dependencies or cascading failures identified in the FMEA)?  *Note: The safety analysis shall investigate if the element/component/system has single events or single causes that could bypass or invalidate a required independence or freedom from interference between given elements and violate a safety requirement or a safety goal,* **Error! Reference source not found.**. | A-D |  |  |
| Are for each identified dependent failure on system level   * justification why the malfunctioning behaviour is not plausible provided or * measures for the resolution of the dependent failures defined?   *Note: This includes the evaluation of the identified potential dependent failures with rationales, operational situation, and operating modes, see* **Error! Reference source not found.** | A-D |  |  |

## Review Exceptions / Deviations / Findings

2/16/22 :

Manually updated:

- Template page;

- 1.2 Input documents;

- 2.3 Technical Block Diagram update as latest version from FD.

- 2.4.1 Elements/Components/Systems within System Boundary;

- Figure 8: Operating Modes Overview Diagram.

## Further Actions / Decisions

2/16/22 :

# Execution and Results of Confirmation Review

|  |  |  |  |
| --- | --- | --- | --- |
| **Date of review completion** | **Reviewed Version of FFSD** | **Responsible Person for Review** | **Level of Independence** |
| **3/8/22** | **SRS3** | **Claudio Labate**  **Rafael Oliveira** | **I1** |

Table 62: 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*

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

*Note: Independence should be used as follows:*

*I0:* *the confirmation measure should be performed; if no confirmation measure is performed, a rationale shall be provided; however, if the confirmation measure is performed, it shall be performed by a different person*

*I1:*  *the confirmation measure shall be performed, by a different person*

*I2:*  *the confirmation measure shall be performed, by a person from a different team, i.e. not reporting to the same direct superior (LL6)*

*I3:*  *the confirmation measure shall be performed, by a person from a different Director-level organization, i.e. independent from the department responsible for the considered work product(s) regarding management, resources and release authority (cross-domain, not from the domain taking-over the feature, e.g. Powertrain for Chassis or R&A for PD).*

## Confirmation Review

| **Compliant to ISO 26262?** | | **Yes / No** |
| --- | --- | --- |
| Technical safety concept and requirements compliance with the Functional safety requirements, considering the elements of system design. | Are all Technical Safety Requirements described needed for the implementation of the Functional Safety Requirements? | Yes |
| Is the Technical Safety Concept appropriate considering the Safety Analysis Report (FFSD 06), to ensure confidence in the effectiveness and completeness of Technical Safety Requirements? | Yes |
| Do the specified safety mechanisms adequately consider the failures modes of the components identified in the Safety Analysis Report (FFSD 06), to ensure the safety mechanisms sufficiently  cover faults? | Yes |
| Is the implementation of warning and degradation strategy consistent with the Functional Safety Concept (FFSD 03)? | Yes |
| ASIL decompositions:   * Are the decomposed technical safety requirements correct (e.g. attributes, parameters) and redundant? * Is the required independence (no homogeneous redundancy) feasible? * Is the decomposition performed as per the FFSG 04, Section 2.3.3.7? | Yes |
| Have all the assumptions made in this Safety Requirements Specification been documented and are valid? | Yes |
| Are all the Technical Safety Requirements allocated to elements of the system architectural design, to ensure coverage? | Yes |
| Safety Analysis | Is a qualitative Safety Analyses performed and is it appropriately described? | Yes |
| Is a quantitative Safety Analyses performed, is it appropriately described with guide words and is the tool described? | Yes |
| General | Are all sections of the template filled out appropriately, or otherwise contain a valid explanation stating why the section is not necessary? | Yes |

Table 22: Checklist for Safety Requirements Specification Confirmation

## Review Exceptions / Deviations / Findings

3/4/22 :

## Further Actions / Decisions

3/4/22 :

2. Definitions, Abbreviations and Acronyms

|  |  |
| --- | --- |
| HMI | Human Machine Interface |
| Low speed | Approximately 12 to 36 mph (19 to 58 kph ) |

Table 63: Definitions, Abbreviations and Acronyms