|  |  | |  |
| --- | --- | --- | --- |
|  |  | |  |
|  |  | |  |
|  |  | |  |
|  |  | |  |
|  | Safety Requirements Specification | |  |
|  |  | |  |
|  | including  Safety Requirements Specification  System Architectural Design Specification | |  |
|  |  |
|  |  |
|  |  | |  |
| Commodities | Steering Column / Pedal Position Control Feature | |  |
| Program(s) | MY 25 U71X | |  |
| VSEM ID(s) | F004690 | |  |
| Document Version | 0.4 | |  |
| Document  Owner | Barry Maloney(bmalon24)  Angela Shubsda (ASHUBSDA),  Diana Aguilar (daguil24)  Ashish Keshri (AKESHRI) | |  |
|  |  | |  |
|  | Template Authors: | [Global FS Technical Governance Board](https://azureford.sharepoint.com/sites/GlobalFunctionalSafety/Functional%20Safety%20FAQ%20Wiki%20Page/Functional%20Safety%20Team.aspx) |  |
|  | Template Version: | 9.1 |  |
|  |  |  |  |

# Change Control

|  |  |  |  |
| --- | --- | --- | --- |
| **Version** | **Date** | **Author** | **Change / Remark** |
| 0.1 | 08/29/2021 | Namita Khurana | Initial Draft |
| 0.2 | 09/19/2021 | Ashish Keshri | * Updated Technical Safety Requirements according to FFSD02 HARA (ver. 0.7) and FFSD03 FSC (ver. 0.7) * Updated Technical Safety Requirements per discussion with Phoenix team * Added Technical Safety Requirements attributes (TSR Rationale, Safety V&V Acceptance Criteria, operation modes, draft FHT) * Updated TSR Allocation Table, Operating Modes Table, Input Section |
| 0.3 | 10/08/2021 | Ashish Keshri Namita Khurana  Manikanta Gupta | * Added TSRs for Pedal Position Control SG02 * Added TSRs for SG01 related to Single-point and latent fault handling * Combined TSRs related to Maintain Safe State/Recovery (SCPC-F-S-Req01.10, SCPC-F-S-Req01.11, SCPC-F-S-Req01.9, SCPC-F-S-Req01.11) * Updated TSRs wording per team discussion and other features TSRs related to steering and pedal position controls (e.g U71X/CDX707N Classic Memory) |
| 0.4 | 10/14/2021 | Ashish Keshri | Following modification are done according to review feedback on version 0.3 SRS:   * TSRs wording is updated related to TSR text, Verification Criteria, and Rationale * ASIL Rating is updated (ASIL B-> ASIL A) for TSRs related to latent fault handing * Section 3.6 Allocation is updated for TSR allocation to DSM and APIM\_CDC |

*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://azureford.sharepoint.com/sites/GlobalFunctionalSafety/Functional%20Safety%20FAQ%20Wiki%20Page/Functional%20Safety%20Team.aspx*](https://azureford.sharepoint.com/sites/GlobalFunctionalSafety/Functional%20Safety%20FAQ%20Wiki%20Page/Functional%20Safety%20Team.aspx)*.*

*“Template” should be removed from Cover Page in the program specific document.*

*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 8](#_Toc84574526)

[1.1 Purpose 8](#_Toc84574527)

[1.2 Input documents 8](#_Toc84574528)

[2. Input from System Design, Item Definition / Feature Document [FFSD01.1(0)] and Functional Safety Concept [FFSD03] 1](#_Toc84574529)

[2.1 Implementation Details of External Interfaces 2](#_Toc84574530)

[2.2 Constraints 1](#_Toc84574531)

[2.3 Technical Block Diagram 1](#_Toc84574532)

[2.4 Functional Overview of Elements/Components/Systems 1](#_Toc84574533)

[2.4.1 Elements/Components/Systems within System Boundary 1](#_Toc84574534)

[2.4.2 Elements/Components/Systems outside System Boundary 4](#_Toc84574535)

[2.5 Implementation Details of Internal Interfaces 1](#_Toc84574536)

[2.6 System Level Architecture (including redundancy) 1](#_Toc84574537)

[2.6.1 Safety Goal: SG01 (ASIL B) : Prevent impaired access to the steering controls 1](#_Toc84574538)

[2.6.2 Safety Goal: SG02 (ASIL B) : Prevent impaired access to the pedal controls 1](#_Toc84574539)

[3. Technical Safety Requirements Specification 2](#_Toc84574540)

[3.1 Technical Safety Requirements 2](#_Toc84574541)

[3.1.1 Requirement Derivation for SCPC-F-S-Req01.1 (Contextual Control State Determination for Steering Column Adjust Controls) 2](#_Toc84574542)

[3.1.1.1 Requirement Derivation Diagram(s) (Optional) 2](#_Toc84574543)

[3.1.1.2 Technical Safety Requirements 2](#_Toc84574544)

[3.1.2 Requirement Derivation for SCPC-F-S-Req01.2 (Provide Steering Column Tilt Position Adjustment Request) 4](#_Toc84574545)

[3.1.2.1 Requirement Derivation Diagram(s) (Optional) 4](#_Toc84574546)

[3.1.2.2 Technical Safety Requirements 4](#_Toc84574547)

[3.1.3 Requirement Derivation for SCPC-F-S-Req01.3 (Provide Steering Column Telescopic Position Adjustment Request) 8](#_Toc84574548)

[3.1.3.1 Requirement Derivation Diagram(s) (Optional) 8](#_Toc84574549)

[3.1.3.2 Technical Safety Requirements 8](#_Toc84574550)

[3.1.4 Requirement Derivation for SCPC-F-S-Req01.4 (Close Steering Column Adjust Controls) 12](#_Toc84574551)

[3.1.4.1 Requirement Derivation Diagram(s) (Optional) 12](#_Toc84574552)

[3.1.4.2 Technical Safety Requirements 12](#_Toc84574553)

[3.1.5 Requirement Derivation for SCPC-F-S-Req01.5 (Provide Steering Column Tilt Position Command) 14](#_Toc84574554)

[3.1.5.1 Requirement Derivation Diagram(s) (Optional) 14](#_Toc84574555)

[3.1.5.2 Technical Safety Requirements 14](#_Toc84574556)

[3.1.6 Requirement Derivation for SCPC-F-S-Req01.6 (Provide Steering Column Telescopic Position Command) 18](#_Toc84574557)

[3.1.6.1 Requirement Derivation Diagram(s) (Optional) 18](#_Toc84574558)

[3.1.6.2 Technical Safety Requirements 18](#_Toc84574559)

[3.1.7 Requirement Derivation for SCPC-F-S-Req01.7 (Actuate Commanded Steering Column Tilt Position) 22](#_Toc84574560)

[3.1.7.1 Requirement Derivation Diagram(s) (Optional) 22](#_Toc84574561)

[3.1.7.2 Technical Safety Requirements 22](#_Toc84574562)

[3.1.8 Requirement Derivation for SCPC-F-S-Req01.8 (Actuate Commanded Steering Column Telescopic Position) 30](#_Toc84574563)

[3.1.8.1 Requirement Derivation Diagram(s) (Optional) 30](#_Toc84574564)

[3.1.8.2 Technical Safety Requirements 30](#_Toc84574565)

[3.1.9 Requirement Derivation for SCPC-F-S-Req01.9 (Inhibit steering column tilt position adjustment) 38](#_Toc84574566)

[3.1.9.1 Requirement Derivation Diagram(s) (Optional) 38](#_Toc84574567)

[3.1.9.2 Technical Safety Requirements 38](#_Toc84574568)

[3.1.10 Requirement Derivation for SCPC-F-S-Req01.10 (Inhibit steering column telescopic position adjustment) 42](#_Toc84574569)

[3.1.10.1 Requirement Derivation Diagram(s) (Optional) 42](#_Toc84574570)

[3.1.10.2 Technical Safety Requirements 43](#_Toc84574571)

[3.1.11 Requirement Derivation for SCPC-F-S-Req02.1 (Contextual Control State Determination for Pedal Adjust Controls) 48](#_Toc84574572)

[3.1.12 Requirement Derivation for SCPC-F-S-Req02.2 (APIM\_CDC Provide Pedal Telescopic Position Adjustment Request) 50](#_Toc84574573)

[3.1.13 Requirement Derivation for SCPC-F-S-Req02.3 (Close Pedal Adjust Controls) 54](#_Toc84574574)

[3.1.14 Requirement Derivation for SCPC-F-S-Req02.4 (Provide Pedal Telescopic Position Command) 57](#_Toc84574575)

[3.1.15 Requirement Derivation for SCPC-F-S-Req02.5 (Actuate Commanded Pedal Telescopic Position) 62](#_Toc84574576)

[3.1.16 Requirement Derivation for SCPC-F-S-Req02.6 (Inhibit Pedal Telescopic Position Adjustment) and SCPC-F-S-Req02.7 (Enable Pedal Telescopic Position Adjustment) 71](#_Toc84574577)

[3.2 Timing Specification 75](#_Toc84574578)

[3.2.1 Fault Tolerant Time Interval (FTTI) Identification 75](#_Toc84574579)

[3.2.1.1 Safety Goal 02 Prevent impaired access to steering controls 75](#_Toc84574580)

[3.2.2 Fault Handling Time Specification 76](#_Toc84574581)

[3.2.2.1 Achieving the FHT for SG 02 Prevent impaired access to steering controls 76](#_Toc84574582)

[3.3 Derivation of Reduced Functionality Interval (optional) 77](#_Toc84574583)

[3.4 Operating Modes Overview (optional) 77](#_Toc84574584)

[3.5 HW Metric Requirements - Derivation and Rationale (optional) 77](#_Toc84574585)

[3.6 Allocation (optional) 77](#_Toc84574586)

[3.7 ASIL Decomposition - Derivation and Rationale (optional) 78](#_Toc84574587)

[3.8 Safety Related Parameters 78](#_Toc84574588)

[3.9 Cascading Technical Safety Requirements 80](#_Toc84574589)

[4. Requirements for Production, Operation, Service and Decommissioning 80](#_Toc84574590)

[5. Safety Analysis 80](#_Toc84574591)

[*6.* Execution and Results of Verification Review 81](#_Toc84574592)

[6.1 Verification Review 81](#_Toc84574593)

[6.1.1 Verification Review of Safety Requirements Specification 81](#_Toc84574594)

[6.1.2 Verification Review of Safety Analyses of Safety Requirements Specification (optional) 84](#_Toc84574595)

[6.2 Review Exceptions / Deviations / Findings 86](#_Toc84574596)

[6.3 Further Actions / Decisions 86](#_Toc84574597)

[7. Execution and Results of Confirmation Review 87](#_Toc84574598)

[7.1 Confirmation Review 87](#_Toc84574599)

[7.2 Review Exceptions / Deviations / Findings 88](#_Toc84574600)

[7.3 Further Actions / Decisions 88](#_Toc84574601)

[Appendix A 89](#_Toc84574602)

[A.1 Definitions, Abbreviations and Acronyms 89](#_Toc84574603)

# List of tables

[Table 1: Document Scope 8](#_Toc84574604)

[Table 2: Input 9](#_Toc84574605)

[Table 3: External Interfaces with Respect to the System Boundary 7](#_Toc84574606)

[Table 4: Elements/Components/Systems within the System Boundary 4](#_Toc84574607)

[Table 5: Relevant Systems (Elements/Components/Systems) outside System Boundary 4](#_Toc84574608)

[Table 6: System Level architecture (including redundancy) for SG01 1](#_Toc84574609)

[Table 7: Element/Component/System Technical Safety Requirements SCPC-T-S-Req01.1.1 4](#_Toc84574610)

[Table 8: Element/Component/System Technical Safety Requirements SCPC-T-S-Req01.2.1 6](#_Toc84574611)

[Table 9: Element/Component/System Technical Safety Requirements SCPC-T-S-Req01.2.2 8](#_Toc84574612)

[Table 10: Element/Component/System Technical Safety Requirements SCPC-T-S-Req01.3.1 10](#_Toc84574613)

[Table 11: Element/Component/System Technical Safety Requirements SCPC-T-S-Req01.3.2 12](#_Toc84574614)

[Table 12: Element/Component/System Technical Safety Requirements SCPC-T-S-Req01.4.1 14](#_Toc84574615)

[Table 13: Element/Component/System Technical Safety Requirements SCPC-T-S-Req01.5.1 16](#_Toc84574616)

[Table 14: Element/Component/System Technical Safety Requirements SCPC-T-S-Req01.5.2 18](#_Toc84574617)

[Table 15: Element/Component/System Technical Safety Requirements SCPC-T-S-Req01.6.1 20](#_Toc84574618)

[Table 16: Element/Component/System Technical Safety Requirements SCPC-T-S-Req01.6.2 22](#_Toc84574619)

[Table 17: Element/Component/System Technical Safety Requirements SCPC-T-S-Req01.7.1 24](#_Toc84574620)

[Table 17: Element/Component/System Technical Safety Requirements SCPC-T-S-Req01.7.2 26](#_Toc84574621)

[Table 17: Element/Component/System Technical Safety Requirements SCPC-T-S-Req01.7.3 28](#_Toc84574622)

[Table 17: Element/Component/System Technical Safety Requirements SCPC-T-S-Req01.7.4 30](#_Toc84574623)

[Table 17: Element/Component/System Technical Safety Requirements SCPC-T-S-Req01.8.1 32](#_Toc84574624)

[Table 17: Element/Component/System Technical Safety Requirements SCPC-T-S-Req01.8.2 34](#_Toc84574625)

[Table 17: Element/Component/System Technical Safety Requirements SCPC-T-S-Req01.8.3 36](#_Toc84574626)

[Table 17: Element/Component/System Technical Safety Requirements SCPC-T-S-Req01.7.4 38](#_Toc84574627)

[Table 19: Element/Component/System Technical Safety Requirements SCPC-T-S-Req01.9.1 40](#_Toc84574628)

[Table 20: Element/Component/System Technical Safety Requirements SCPC-T-S-Req01.9.2 42](#_Toc84574629)

[Table 19: Element/Component/System Technical Safety Requirements SCPC-T-S-Req01.10.1 45](#_Toc84574630)

[Table 20: Element/Component/System Technical Safety Requirements SCPC-T-S-Req01.10.2 47](#_Toc84574631)

[Table 27: Element/Component/System Technical Safety Requirements SCPC-T-S-Req02.1.1 50](#_Toc84574632)

[Table 27: Safety Mechanism Y HMT Summary 76](#_Toc84574633)

[Table 28: Safety Mechanism Y MBMT Summary 76](#_Toc84574634)

[Table 29: FTTI Summary 76](#_Toc84574635)

[Table 30: FHT Summary 77](#_Toc84574636)

[Table 31: Operating Modes 77](#_Toc84574637)

[Table 32: Allocation of Technical Safety Requirements 78](#_Toc84574638)

[Table 33: Parameter 79](#_Toc84574639)

[Table 21: Review Table 81](#_Toc84574640)

[Table 22: Checklist for Completeness of Safety Requirements Specification 84](#_Toc84574641)

[Table 23: Checklist for Correctness of qualitative, quantitative and dependent failure Analysis 86](#_Toc84574642)

[Table 24: Definitions, Abbreviations and Acronyms 89](#_Toc84574643)

# List of figures

[Figure 1 - Technical Block Diagram for U71X Steering Column and Pedal Position Control Feature 1](#_Toc84574644)

[Figure 2 - Technical Safety Requirements Derivation Diagram for SCPC-F-S-Req01.1 2](#_Toc84574645)

[Figure 2 - Technical Safety Requirements Derivation Diagram for SCPC-F-S-Req01.2 4](#_Toc84574646)

[Figure 2 - Technical Safety Requirements Derivation Diagram for SCPC-F-S-Req01.3 8](#_Toc84574647)

[Figure 2 - Technical Safety Requirements Derivation Diagram for SCPC-F-S-Req01.4 12](#_Toc84574648)

[Figure 2 - Technical Safety Requirements Derivation Diagram for SCPC-F-S-Req01.5 14](#_Toc84574649)

[Figure 2 - Technical Safety Requirements Derivation Diagram for SCPC-F-S-Req01.6 18](#_Toc84574650)

[Figure 2 - Technical Safety Requirements Derivation Diagram for SCPS-F-S-Req01.7 22](#_Toc84574651)

[Figure 2 - Technical Safety Requirements Derivation Diagram for SCPS-F-S-Req01.8 30](#_Toc84574652)

[Figure 2 - Technical Safety Requirements Derivation Diagram for SCPC-F-S-Req01.9 38](#_Toc84574653)

[Figure 2 - Technical Safety Requirements Derivation Diagram for SCPC-F-S-Req01.10 42](#_Toc84574654)

# 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 Architectural 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/systems. Elements/Components/Systems can be hardware, software or other systems.
* Other Requirements and Design Documents (= the specification tree applied within the project is used, e.g. Functional Specifications, System Specifications, Design Prerequisites, Engineering Specifications)  
  *Note: The terms Functional Specifications, System Specifications, Design Prerequisites, Engineering Specifications are not universally used within Ford*
* The Hardware Safety Requirements refine and concretize the requirements of the technical safety concept.
* The Software Safety Requirements (see are derived from the requirements of the technical safety concept and the underlying Hardware.

This Safety Requirements Specification does not cover the following aspects:

*Insert aspects not covered within this document*

|  |  |
| --- | --- |
| Aspect not covered | Assumed to be covered in |
| Functional specification of the item including SIMA, SCCM, ECG, APIM\_CDC and Display, DSM, Steering Column Motors and Sensors, Pedals Motor and Sensor | Feature Functional Specification, System / Component Functional Specification |
|  |  |

Table 1: Document Scope

## Input documents

|  |  |  |  |
| --- | --- | --- | --- |
|  | Document Name | File Name/Reference | Version |
| **FFSD / Other Input**  (Required) | FFSD01.1 Item Definition /  FFSD01.10 Feature Document | Steering Column\_Pedal Position Control Feature Document | FD0 |
| FFSD02 Hazard Analysis and Risk Assessment | FFSD02\_HazardAnalysisAndRiskAssessment\_Steering Column Position Control | 0.7 |
| FFSD03 Functional Safety Concept | FFSD03\_FunctionalSafetyConcept\_Steering Column Pedal Position Control | 0.6 |
| System Architectural Design (from an external source) | U71x Steering Column\_Pedal Position Control- BD 06-OCT- 2021 Draft |  |
| NetComSignal - SHC\_Atherton |  |
| Safety Requirements to the item from other safety relevant items (if applicable) | None |  |
| **Other Input**  (Optional) | Project Plan | FFSD01.0\_SafetyPlanGPDS\_Steering\_Column\_Position\_Control\_U71X | 1.2 |
| Functional concept | Steering Column\_Pedal Position Control Functional Specification |  |
| FunctionGroupSpec\_SHC |  |
| SW\_HMI\_Spec\_2.1 06-30-21 |  |
|  |  |
|  |  |
| Preliminary architectural assumptions | [VDOC099576-Steering Horizon Control SPSS](https://www.vsemweb.ford.com/tc/launchapp?-attach=true&-s=226TCSession&-o=GOjFhhEJx3NrTDAAAAAAAAAAAAA&servername=Production_Server) | 1.6 |
| System Design (incl. external / company / generic standards, legal, HW, SW requirements, etc.) | Allegra Tele & Rack Sensors Specification ( Alegra A33003 Specification.pdf) |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
| 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 [FFSD01.1(0)] and Functional Safety Concept [FFSD03]

## 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) |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| StewPosAdjTel\_D\_Rq | Request for adjusting steering wheel position, telescope. This signal is for Steering Horizon controller system | StewPosAdjTel\_D\_Rq | APIM | ECG | HS3-CAN | In, Out, Idle | n/a | 1sec and event based | E2E Protection |
| StewPosAdjTel\_D\_Rq | Request for adjusting steering wheel position, telescope. This signal is for Steering Horizon controller system | StewPosAdjTel\_D\_Rq | ECG | DSM | FD3-CAN | In, Out, Idle | n/a | 1sec and event based | E2E Protection |
| StewPosAdjTlt\_D\_Rq | Request for adjusting steering wheel position, tilt. This signal is for Steering Horizon controller system. | StewPosAdjTlt\_D\_Rq | APIM | ECG | HS3-CAN | Up, Down, Idle | n/a | 1sec and event based | E2E Protection |
| StewPosAdjTlt\_D\_Rq | Request for adjusting steering wheel position, tilt. This signal is for Steering Horizon controller system. | StewPosAdjTlt\_D\_Rq | ECG | DSM | FD3-CAN | Up, Down, Idle | n/a | 1sec and event based | E2E Protection |
| StewSwtchScndPos\_D\_St | Right hand steering wheel switch position status signal. This signal is for Steering Horizon controller system. | StewSwtchScndPos\_D\_St | SCCM | ECG | FD3-CAN | One, Two, Three, Four, Five, Six, Seven, Eight, Nine, Idle, Faulty | n/a | 1sec and event based | n/a |
| StewSwtchScndPos\_D\_St | Right hand steering wheel switch position status signal. This signal is for Steering Horizon controller system. | StewSwtchScndPos\_D\_St | ECG | APIM | HS3-CAN | One, Two, Three, Four, Five, Six, Seven, Eight, Nine, Idle, Faulty | n/a | 1sec and event based | n/a |
| StewSwtchScnd\_D\_Stat | Right hand steering wheel switch press status signal. This signal is for Steering Horizon controller system. | StewSwtchScnd\_D\_Stat | SCCM | ECG | FD3-CAN | Pressed, Not Pressed | n/a | 1sec and event based | n/a |
| StewSwtchScnd\_D\_Stat | Right hand steering wheel switch press status signal. This signal is for Steering Horizon controller system. | StewSwtchScnd\_D\_Stat | ECG | APIM | HS3-CAN | Pressed, Not Pressed | n/a | 1sec and event based | n/a |
| PdlAdj\_D\_Rq | Request for adjusting Pedal position, telescope. This signal is for Steering Horizon controller system | PdlAdj\_D\_Rq | APIM | ECG | HS3-CAN | In, Out, Idle | n/a | 1sec and event based | E2E Protection |
| PdlAdj\_D\_Rq | Request for adjusting pedal position, telescope. This signal is for Steering Horizon controller system | PdlAdj\_D\_Rq | ECG | DSM | MS1-CAN | In, Out, Idle | n/a | 1sec and event based | E2E Protection |

| MOTOR ADJUSTABLE STEERING COLUMN TILT (RAKE) UP | Pulse Width Modulation (PWM) signal for tilt motor fore movement | MOTOR\_TILT\_FORE | DSM | Tilt Motor | PWM | Voltage: 13.8V Nominal (16V Max),  Current: 15A Max,  PWM: ~ 50% duty cycle | n/a | n/a | n/a |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| MOTOR ADJUSTABLE STEERING COLUMN TILT (RAKE) DOWN | Pulse Width Modulation (PWM) signal for tilt motor aft movement | MOTOR\_TILT\_AFT | DSM | Tilt Motor | PWM | Voltage: 13.8V Nominal (16V Max),  Current: 15A Max,  PWM: ~ 50% duty cycle | n/a | n/a | n/a |
| MOTOR ADJUSTABLE STEERING COLUMN TELE FORE | Pulse Width Modulation (PWM) signal for tele motor fore movement | MOTOR\_TELESCOPE\_FORE | DSM | Telescopic  Motor | PWM | Voltage: 13.8V Nominal (16V Max),  Current: 15A Max,  PWM: ~ 50% duty cycle | n/a | n/a | n/a |
| MOTOR ADJUSTABLE STEERING COLUMN TELE AFT | Pulse Width Modulation (PWM) signal for tele motor aft movement | MOTOR\_TELESCOPE\_AFT | DSM | Telescopic  Motor | PWM | Voltage: 13.8V Nominal (16V Max),  Current: 15A Max,  PWM: ~ 50% duty cycle | n/a | n/a | n/a |
| MOTOR ADJUSTABLE PEDAL TELE FORE | Pulse Width Modulation (PWM) signal for pedal motor fore movement | MOTOR\_PEDAL\_FORE | DSM | Pedal Motor | PWM |  |  |  | n/a |
| MOTOR ADJUSTABLE PEDAL TELE AFT | Pulse Width Modulation (PWM) signal for pedal motor aft movement | MOTOR\_PEDAL\_AFT | DSM | Pedal Motor | PWM |  |  |  | n/a |
| TILT\_HALL\_SENSOR | SENT signal from Rake Position Sensor | TILT\_HALL\_SENSOR | Rake Sensor | DSM | SENT | See Allegra Tele & Rack Sensors Data Sheet Spec |  |  | n/a |
| TELESCOPE\_HALL\_SENSOR | SENT signal from Telescopic Position Sensor | TELESCOPE\_HALL\_SENSOR | Telescopic Sensor | DSM | SENT | See Allegra Tele & Rack Sensors Data Sheet Spec |  |  | n/a |
| PEDAL\_HALL\_SENSOR | SENT signal from Pedal Position Sensor | PEDAL\_HALL\_SENSOR | Pedal Sensor | DSM | Hardwired | See Motor Adjustment Trials for P702 ADJ ETC and Brake | | | n/a |

Table 3: External Interfaces with Respect to the System Boundary

## Constraints

1. Environmental conditions (lifetime, temperature range, humidity, vibration, shock, IP protection class, resistibility against aggressive chemicals, like motor oil, electrical requirements) are described in Specification ES7G91-3F880-FC, external document).
2. The steering column crash operation range 60mm per crash requirements and Pedal crash operation range is 47mm per crash requirements

## Technical Block Diagram

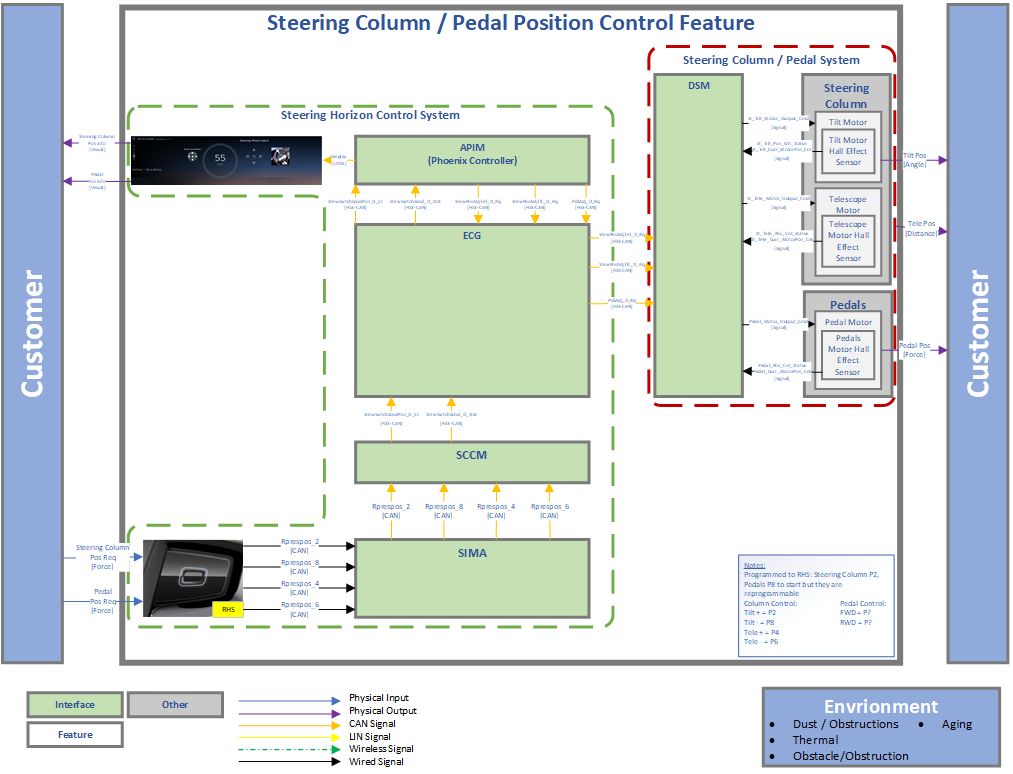
**

Figure 1 - Technical Block Diagram for U71X Steering Column and Pedal Position Control Feature

## Functional Overview of Elements/Components/Systems

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

| Element/Component/System | Description / Tasks | Reference to System Design / Detailed Specification |
| --- | --- | --- |
| SIMA | Switch Interface Module:   * Capacitive steering wheel switches. Two 3x3 matrix switch packs | This feature does not cascade any TSR to SIMA module |
| SCCM | Steering Column Control Module   * Transmits steering wheel switch position and status signals (StewSwtchScndPos\_D\_St, StewSwtchScnd\_D\_Stat) from private CAN to FD3-CAN | This feature does not cascade any TSR to SCCM module |
| ECG | Enhanced Central Gateway   * Transmits steering column tilt position request signals (StewPosAdjTlt\_D\_Rq) from HS3-CAN to FD3-CAN * Transmits steering column telescopic position request signals (StewPosAdjTel\_D\_Rq) from HS3-CAN to MS1-CAN * Transmits pedal telescopic position request signals (PdlAdj\_D\_Rq) from HS3-CAN to FD3-CAN * Transmits steering wheel switch position status and press status signals (StewSwtchScndPos\_D\_St, StewSwtchScnd\_D\_Stat) signals from FD3-CAN to HS3-CAN | This feature does not cascade any TSR to ECG module |
| APIM\_CDC and  Display | Accessory Protocol Interface Module (APIM)  Cockpit Domain Controller (CDC)  The following functions listed are relevant for Steering Column Tilt/Telescopic adjustment functionality within APIM\_CDC. Other APIM\_CDC functions are not considered here:   * Receive HS3-CAN input signals (StewSwtchScndPos\_D\_St, StewSwtchScnd\_D\_Stat) for Right hand steering wheel switch position status and press status signals * Send HS3-CAN signals (StewPosAdjTlt\_D\_Rq) for steering column tilt position adjustment * Send HS3-CAN signals (StewPosAdjTel\_D\_Rq) for steering column telescopic position adjustment * Send HS3-CAN signals (PdlAdj\_D\_Rq) for pedals telescopic position adjustment * Determine Contextual Control State for Steering Column and Pedal Adjust Controls * Timeout control for Steering Column and Pedal Adjust Controls * Safety mechanisms to detect and mitigate safety-related failures related to APIM\_CDC hardware/software resources | **SharePoint**  [Steering Horizon Control SPSS v1.6](https://azureford.sharepoint.com/sites/GlobalCockpitSystemsStrategy/DesignVault/FISI_SpecReleases/SHC/Steering%20Horizon%20Control/Ver%201.6)  **VSEM**:  [VDOC099576-Steering Horizon Control SPSS](https://www.vsemweb.ford.com/tc/launchapp?-attach=true&-s=226TCSession&-o=GOjFhhEJx3NrTDAAAAAAAAAAAAA&servername=Production_Server)  [VDOC099577-Steering Horizon Control Implementation Guide](https://www.vsemweb.ford.com/tc/launchapp?-attach=true&-s=226TCSession&-o=GeuFhhEJx3NrTDAAAAAAAAAAAAA&servername=Production_Server)  SW\_HMI\_Spec\_2.1 06-30-21.pdf |
| DSM | The following functions listed are relevant for Steering Column Tilt/Telescopic adjustment functionality within DSM. Other DSM functions are not considered here:   * Receive FD3-CAN input signals (StewPosAdjTlt\_D\_Rq) for steering column tilt position adjustment * Receive FD3-CAN input signals (StewPosAdjTel\_D\_Rq) for steering column telescopic position adjustment * Receive FD3-CAN input signals (PdlAdj\_D\_Rq) for pedal telescopic position adjustment * Receive SENT input signals from rake sensor for determination of absolute tilt position of steering column * Receive SENT input signals from angle position sensor for determination of absolute telescopic position of steering column * Receive input signals from position sensor for determination of absolute telescopic position of Pedals * Control system voltage/power to steering column rake motor * Control system voltage/power to steering column telescopic motor * Control system voltage/power to steering column pedal motor * Safety mechanisms to detect and mitigate safety-related failures related to DSM hardware/software resources | **System Hardware Architecture**  (Supplier / Gentherm)  **Functional Specification**  (Passenger Seat Module FS) |
| Rake Motor | A Rake DC Motor to bi-directionally move the steering wheel Rake | DT-L1MC-3C529-C\_C\_DT\_Report\_20210609\_000227 |
| Telescopic Motor | A Tele DC Motor to bi-directionally move the steering column | DT-L1MC-3C529-C\_C\_DT\_Report\_20210609\_000227 |
| Pedal Motor | A Pedal DC Motor to bi-directionally move the pedals | ML34-9F836-BB |
| Rake Sensor | SENT protocol packaged sensor attached to the steering column assembly send rake position | Allegra Tele & Rack Sensors Data Sheet Spec |
| Telescopic Sensor | SENT protocol packaged sensor attached to the steering column assembly send Steering Angle Tele position | Allegra Tele & Rack Sensors Data Sheet Spec |
| Pedal Sensor | Hardwired sensor attached to the pedal assembly send pedal Tele position | Motor Adjustment Trials for P702 ADJ ETC and Brake |

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

### Elements/Components/Systems outside System Boundary

| Element/Component/System | Description / Tasks |
| --- | --- |
| Steering Wheel Mechanical Assembly | Refer Steering Column FMA document |
| Pedals Mechanical Assembly | Refer Pedals FMA document |

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

## Implementation Details of Internal Interfaces

None

## System Level Architecture (including redundancy)

Refer Section 2.3 Technical Block Diagram

### Safety Goal: SG01 (ASIL B) : Prevent impaired access to the steering controls

*Insert Technical Block Diagram highlighting components that are used to satisfy this Safety Goal. Include any descriptions that will clarify how the component will be used for this Safety Goal (see Guideline).*

*Document System Level architecture for redundant components for all Safety Goals. Only necessary if redundancy is required.*

| **Affected Components/**  **Systems** | **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** |
| APIM\_CDC | None | n/a | n/a | n/a |
| DSM | None | n/a | n/a | n/a |

Table 6: System Level architecture (including redundancy) for SG01

### Safety Goal: SG02 (ASIL B) : Prevent impaired access to the pedal controls

# Technical Safety Requirements Specification

## Technical Safety Requirements

### Requirement Derivation for SCPC-F-S-Req01.1 (Contextual Control State Determination for Steering Column Adjust Controls)

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

*Derive Technical Safety Requirements from Functional Safety Requirements.*

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

Figure 2 - Technical Safety Requirements Derivation Diagram for SCPC-F-S-Req01.1

#### Technical Safety Requirements

| T-S-Req-ID: | SCPC-T-S-Req01.1.1 |
| --- | --- |
| External Reference *(optional)* |  |
| Category: | Safety Related Function |
| Version  *(only in case of category “Non-E/E requirement”)* |  |
| Author  *(only in case of category “Non-E/E requirement”)* |  |
| Safety Goal ID: | SG01: Prevent impaired access to the steering controls |
| F-S-Req ID: | SCPC-F-S-Req01.1: Contextual Control State Determination for Steering Column Adjust Controls |
| ASIL Classification:  *(in case of category “General”: if applicable, in case of category “Non-E/E Requirement”: not applicable)* | ASIL B |
| Technical Safety Requirement Title: | APIM\_CDC Determines Contextual Control State for Steering Column Adjust Controls |
| Technical Safety Requirement Text: | The APIM\_CDC shall determinecontextual control state for steering column adjust controls when right hand steering wheel switch position (StewSwtchScndPos\_D\_St) and right-hand steering wheel switch status (StewSwtchScnd\_D\_Stat) signals are received on HS3-CAN Bus according to the contextual control flows described in the SW-HMI specification (SW\_HMI\_Spec\_2.1 06-30-21.pdf). |
| Rationale: | The right-hand steering wheel switch position and switch status are needed according to the SW-HMI specification to allow APIM\_CDC to set the contextual control state for steering column adjust controls.  Any single-point fault in SIMA or SCCM would not initiate right hand steering wheel switch information (switch position and switch status) that can activate steering column adjust controls in APIM\_CDC (e.g., Open Default Controls🡪 Open Driver Adjustments Controls-> Open Column Adjust Controls). |
| Operating Mode:  *(in case of categories “General”, “Metric”, “Non-E/E Requirement”, or “User Information”: if applicable)* | Ignition On,  Accessory On |
| Safe State:  *(in case of categories “General”, “Metric”, “Non-E/E Requirement”, or “User Information”: if applicable)* | Contextual control state is not set for steering column adjust controls |
| Reduced Functionality Tolerance Time Interval:  *(if applicable;*  *in case of categories “Metric”, “Non-E/E Requirement”, “Maintain Safe State / Recovery” or “User Information”: not applicable;*  *in case of category “Reduced Functionality”: required)* |  |
| Fault Handling Time Segment:  *(in case of categories “Metric” or “Maintain Safe State / Recovery”: not applicable;*  *in case of category “General”, “Reduced Functionality”, “Non-E/E Requirement”, or “User Information”: if applicable)* | None |
| Requirement Status | Approved |
| V&V method: | Test |
| V&V acceptance criteria:  *(UNV1 / UPV1, not in case of category “Non-E/E requirement)* | System testing: APIM\_CDC sets the contextual control state for steering column adjust controls when right hand steering wheel switch position (StewSwtchScndPos\_D\_St) and switch status (StewSwtchScnd\_D\_Stat) information are received according to the contextual control flows described in the SW-HMI specification ((SW\_HMI\_Spec\_2.1 06-30-21.pdf) |
| Allocated Element(s)/Component(s)/ System(s) *(if applicable)* | APIM\_CDC |

Table 7: Element/Component/System Technical Safety Requirements SCPC-T-S-Req01.1.1

### Requirement Derivation for SCPC-F-S-Req01.2 (Provide Steering Column Tilt Position Adjustment Request)

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

*Derive Technical Safety Requirements from Functional Safety Requirements.*

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

Figure 2 - Technical Safety Requirements Derivation Diagram for SCPC-F-S-Req01.2

#### Technical Safety Requirements

| T-S-Req-ID: | SCPC-T-S-Req01.2.1 |
| --- | --- |
| External Reference *(optional)* |  |
| Category: | Safety Related Function |
| Version  *(only in case of category “Non-E/E requirement”)* |  |
| Author  *(only in case of category “Non-E/E requirement”)* |  |
| Safety Goal ID: | SG01: Prevent impaired access to the steering controls |
| F-S-Req ID: | SCPC-F-S-Req01.2: Provide Steering Column Tilt Position Adjustment Request |
| ASIL Classification:  *(in case of category “General”: if applicable, in case of category “Non-E/E Requirement”: not applicable)* | ASIL B |
| Technical Safety Requirement Title: | APIM\_CDC Provides Steering Column Tilt Position Adjustment Request |
| Technical Safety Requirement Text: | The APIM\_CDC shall provide following steering column tilt position adjustment request (StewPosAdjTlt\_D\_Rq) on HS3-CAN bus when the Contextual Control State is set for steering column adjust controls.   * StewPosAdjTlt\_D\_Rq = Tilt Up if right hand steering wheel switch position (StewSwtchScndPos\_D\_St = Tilt Up) and right-hand steering wheel switch status (StewSwtchScnd\_D\_Stat = Pressed) * StewPosAdjTlt\_D\_Rq = Tilt Down if right hand steering wheel switch position (StewSwtchScndPos\_D\_St = Tilt Down) and right-hand steering wheel switch status (StewSwtchScnd\_D\_Stat = Pressed)   In case of Contextual Control State is not equal to steering column adjust controls, APIM\_CDCshall initiate transition to a safe state within fault handling time interval.  NOTE: APIM\_CDCFault handling time interval (FHTI) = 500ms  (sum of fault detection time interval and the fault reaction time interval) |
| Rationale: | To ensure safe execution of control algorithm (controller’s decision-making process that determines the steering column tilt position adjustment request (Tilt Up / Tilt Down) |
| Operating Mode:  *(in case of categories “General”, “Metric”, “Non-E/E Requirement”, or “User Information”: if applicable)* | Ignition On,  Accessory On |
| Safe State:  *(in case of categories “General”, “Metric”, “Non-E/E Requirement”, or “User Information”: if applicable)* | Steering Column Tilt Position Adjustment Request (StewPosAdjTlt\_D\_Rq = Idle) is sent on HS3-CAN Bus |
| Reduced Functionality Tolerance Time Interval:  *(if applicable;*  *in case of categories “Metric”, “Non-E/E Requirement”, “Maintain Safe State / Recovery” or “User Information”: not applicable;*  *in case of category “Reduced Functionality”: required)* | n/a |
| Fault Handling Time Segment:  *(in case of categories “Metric” or “Maintain Safe State / Recovery”: not applicable;*  *in case of category “General”, “Reduced Functionality”, “Non-E/E Requirement”, or “User Information”: if applicable)* | 500ms |
| Requirement Status | Approved |
| V&V method: | Test |
| V&V acceptance criteria:  *(UNV1 / UPV1, not in case of category “Non-E/E requirement)* | System testing: APIM\_CDC provides steering column tilt position adjustment request signal (StewPosAdjTlt\_D\_Rq = Tilt Up or Tilt Down) when the Contextual Control State is steering column adjust controls. |
| Allocated Element(s)/Component(s)/ System(s) *(if applicable)* | APIM\_CDC |

Table 8: Element/Component/System Technical Safety Requirements SCPC-T-S-Req01.2.1

| T-S-Req-ID: | SCPC-T-S-Req01.2.2 |
| --- | --- |
| External Reference *(optional)* |  |
| Category: | Safety Related Function |
| Version  *(only in case of category “Non-E/E requirement”)* |  |
| Author  *(only in case of category “Non-E/E requirement”)* |  |
| Safety Goal ID: | SG01: Prevent impaired access to the steering controls |
| F-S-Req ID: | SCPC-F-S-Req01.2: Provide Steering Column Tilt Position Adjustment Request |
| ASIL Classification:  *(in case of category “General”: if applicable, in case of category “Non-E/E Requirement”: not applicable)* | ASIL B |
| Technical Safety Requirement Title: | Steering Column Tilt Position Adjustment Request End to End Protection |
| Technical Safety Requirement Text: | The APIM\_CDC shall send steering column tilt position adjustment request (StewPosAdjTlt\_D\_Rq) on HS3-CAN Bus with checksum (StewPosAdjTlt\_D\_Rq\_ \_No\_Cs) and counter (StewPosAdjTlt\_D\_Rq\_ \_No\_Cnt)  NOTE: APIM\_CDC should follow AUTOSAR PROFILE 1A for Checksum and Counter. |
| Rationale: | ASIL rated signals must be end-to-end protected to ensure signal integrity between the transmitter and receiver |
| Operating Mode:  *(in case of categories “General”, “Metric”, “Non-E/E Requirement”, or “User Information”: if applicable)* | Ignition On,  Accessory On |
| Safe State:  *(in case of categories “General”, “Metric”, “Non-E/E Requirement”, or “User Information”: if applicable)* | Steering column tilt position adjustment request signal (StewPosAdjTlt\_D\_Rq = Idle) is sent over HS3-CAN |
| Reduced Functionality Tolerance Time Interval:  *(if applicable;*  *in case of categories “Metric”, “Non-E/E Requirement”, “Maintain Safe State / Recovery” or “User Information”: not applicable;*  *in case of category “Reduced Functionality”: required)* | N/A |
| Fault Handling Time Segment:  *(in case of categories “Metric” or “Maintain Safe State / Recovery”: not applicable;*  *in case of category “General”, “Reduced Functionality”, “Non-E/E Requirement”, or “User Information”: if applicable)* | N/A |
| Requirement Status | Approved |
| V&V method: | Test |
| V&V acceptance criteria:  *(UNV1 / UPV1, not in case of category “Non-E/E requirement)* | System testing: APIM\_CDC transmits steering column tilt position adjustment request on HS3-CAN Bus with correct checksum (StewPosAdjTlt\_D\_Rq\_ \_No\_Cs) and counter (StewPosAdjTlt\_D\_Rq\_ \_No\_Cnt) |
| Allocated Element(s)/Component(s)/ System(s) *(if applicable)* | APIM\_CDC |

Table 9: Element/Component/System Technical Safety Requirements SCPC-T-S-Req01.2.2

### Requirement Derivation for SCPC-F-S-Req01.3 (Provide Steering Column Telescopic Position Adjustment Request)

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

*Derive Technical Safety Requirements from Functional Safety Requirements.*

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

Figure 2 - Technical Safety Requirements Derivation Diagram for SCPC-F-S-Req01.3

#### Technical Safety Requirements

| T-S-Req-ID: | SCPC-T-S-Req01.3.1 |
| --- | --- |
| External Reference *(optional)* |  |
| Category: | Safety Related Function |
| Version  *(only in case of category “Non-E/E requirement”)* |  |
| Author  *(only in case of category “Non-E/E requirement”)* |  |
| Safety Goal ID: | SG01: Prevent impaired access to the steering controls |
| F-S-Req ID: | SCPC-F-S-Req01.3: Provide Steering Column Telescopic Position Adjustment Request |
| ASIL Classification:  *(in case of category “General”: if applicable, in case of category “Non-E/E Requirement”: not applicable)* | ASIL B |
| Technical Safety Requirement Title: | APIM\_CDC Provides Steering Column Telescopic Position Adjustment Request |
| Technical Safety Requirement Text: | The APIM\_CDC shall provide following steering column tele position adjustment request signal (StewPosAdjTel\_D\_Rq) on HS3-CAN bus when the Contextual Control State is set for steering column adjust controls.   * StewPosAdjTel\_D\_Rq = Tel IN if right hand steering wheel switch position (StewSwtchScndPos\_D\_St = Tel IN) and right-hand steering wheel switch status (StewSwtchScnd\_D\_Stat = Pressed) * StewPosAdjTel\_D\_Rq = Tel OUT if right hand steering wheel switch position (StewSwtchScndPos\_D\_St = Tel OUT) and right-hand steering wheel switch status (StewSwtchScnd\_D\_Stat = Pressed)   In case of Contextual Control State is not equal to steering column adjust controls, APIM\_CDCshall initiate transition to a safe state within fault handling time interval.  NOTE: APIM\_CDCFault handling time interval (FHTI) = 500ms  (sum of fault detection time interval and the fault reaction time interval) |
| Rationale: | To ensure safe execution of control algorithm (controller’s decision-making process that determines the steering column tele position adjustment request (Tel IN / Tel OUT) |
| Operating Mode:  *(in case of categories “General”, “Metric”, “Non-E/E Requirement”, or “User Information”: if applicable)* | Ignition On,  Accessory On |
| Safe State:  *(in case of categories “General”, “Metric”, “Non-E/E Requirement”, or “User Information”: if applicable)* | Steering Column Telescopic Position Adjustment Request (StewPosAdjTel\_D\_Rq = Idle) is sent on HS3-CAN Bus |
| Reduced Functionality Tolerance Time Interval:  *(if applicable;*  *in case of categories “Metric”, “Non-E/E Requirement”, “Maintain Safe State / Recovery” or “User Information”: not applicable;*  *in case of category “Reduced Functionality”: required)* | N/A |
| Fault Handling Time Segment:  *(in case of categories “Metric” or “Maintain Safe State / Recovery”: not applicable;*  *in case of category “General”, “Reduced Functionality”, “Non-E/E Requirement”, or “User Information”: if applicable)* | 500ms |
| Requirement Status | Approved |
| V&V method: | Test |
| V&V acceptance criteria:  *(UNV1 / UPV1, not in case of category “Non-E/E requirement)* | System testing: APIM\_CDC provides steering column tele position adjustment request (StewPosAdjTel\_D\_Rq = Tel IN or Tel OUT) on HS3-CAN bus when the Contextual Control State is steering column adjust controls. |
| Allocated Element(s)/Component(s)/ System(s) *(if applicable)* | APIM\_CDC |

Table 10: Element/Component/System Technical Safety Requirements SCPC-T-S-Req01.3.1

| T-S-Req-ID: | SCPC-T-S-Req01.3.2 |
| --- | --- |
| External Reference *(optional)* |  |
| Category: | Safety Related Function |
| Version  *(only in case of category “Non-E/E requirement”)* |  |
| Author  *(only in case of category “Non-E/E requirement”)* |  |
| Safety Goal ID: | SG01: Prevent impaired access to the steering controls |
| F-S-Req ID: | SCPC-F-S-Req01.3: Provide Steering Column Telescopic Position Adjustment Request |
| ASIL Classification:  *(in case of category “General”: if applicable, in case of category “Non-E/E Requirement”: not applicable)* | ASIL B |
| Technical Safety Requirement Title: | Steering Column Telescopic Position Adjustment Request End to End Protection |
| Technical Safety Requirement Text: | The APIM\_CDC shall send steering column telescopic position adjustment request (StewPosAdjTel\_D\_Rq) on HS3-CAN Bus with checksum (StewPosAdjTel\_D\_Rq\_ \_No\_Cs) and counter (StewPosAdjTel\_D\_Rq\_ \_No\_Cnt)  NOTE: APIM\_CDC should follow AUTOSAR PROFILE 1A for Checksum and Counter. |
| Rationale: | ASIL rated signals must be end-to-end protected to ensure signal integrity between the transmitter and receiver |
| Operating Mode:  *(in case of categories “General”, “Metric”, “Non-E/E Requirement”, or “User Information”: if applicable)* | Ignition On,  Accessory On |
| Safe State:  *(in case of categories “General”, “Metric”, “Non-E/E Requirement”, or “User Information”: if applicable)* | Steering Column Telescopic Position Adjustment Request (StewPosAdjTel\_D\_Rq = Idle) is sent on HS3-CAN Bus |
| Reduced Functionality Tolerance Time Interval:  *(if applicable;*  *in case of categories “Metric”, “Non-E/E Requirement”, “Maintain Safe State / Recovery” or “User Information”: not applicable;*  *in case of category “Reduced Functionality”: required)* | N/A |
| Fault Handling Time Segment:  *(in case of categories “Metric” or “Maintain Safe State / Recovery”: not applicable;*  *in case of category “General”, “Reduced Functionality”, “Non-E/E Requirement”, or “User Information”: if applicable)* | 500ms |
| Requirement Status | Approved |
| V&V method: | Test |
| V&V acceptance criteria:  *(UNV1 / UPV1, not in case of category “Non-E/E requirement)* | System testing: APIM\_CDC transmits steering column tele position adjustment request on HS3-CAN Bus with correct checksum (StewPosAdjTel\_D\_Rq\_ \_No\_Cs) and counter (StewPosAdjTel\_D\_Rq\_ \_No\_Cnt) |
| Allocated Element(s)/Component(s)/ System(s) *(if applicable)* | APIM\_CDC |

Table 11: Element/Component/System Technical Safety Requirements SCPC-T-S-Req01.3.2

### Requirement Derivation for SCPC-F-S-Req01.4 (Close Steering Column Adjust Controls)

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

*Derive Technical Safety Requirements from Functional Safety Requirements.*

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

Figure 2 - Technical Safety Requirements Derivation Diagram for SCPC-F-S-Req01.4

#### Technical Safety Requirements

| T-S-Req-ID: | SCPC-T-S-Req01.4.1 |
| --- | --- |
| External Reference *(optional)* |  |
| Category: | Safety Related Function |
| Version  *(only in case of category “Non-E/E requirement”)* |  |
| Author  *(only in case of category “Non-E/E requirement”)* |  |
| Safety Goal ID: | SG01: Prevent impaired access to the steering controls |
| F-S-Req ID: | SCPC-F-S-Req01.4: Close Steering Column Adjust Controls |
| ASIL Classification:  *(in case of category “General”: if applicable, in case of category “Non-E/E Requirement”: not applicable)* | ASIL B |
| Technical Safety Requirement Title: | APIM\_CDC Closes Steering Column Adjust Controls |
| Technical Safety Requirement Text: | The APIM\_CDC shall close contextual control state for steering column controls when right hand steering wheel switch status (StewSwtchScnd\_D\_Stat != Pressed) is received on HS3-CAN Bus for 10 seconds  In case of contextual control state is not equal to steering column adjust controls, APIM\_CDCshall initiate transition to a safe state within fault handling time interval.  NOTE: APIM\_CDCFault handling time interval (FHTI) = 500ms  (sum of fault detection time interval and the fault reaction time interval) |
| Rationale: | Idle Timeout (inactivity timeout) is needed for steering column adjust controls to prevent unintended user input (via right hand steering wheel switch) for steering column adjustment.  Incorrect switch status (stuck at “StewSwtchScnd\_D\_Stat = Pressed”) to APIM\_CDC while using steering column adjust controls could lead to a QM hazard “steering column movement more that intended” (see FFSD02\_HazardAnalysisAndRiskAssessment\_Steering Column Position Control) |
| Operating Mode:  *(in case of categories “General”, “Metric”, “Non-E/E Requirement”, or “User Information”: if applicable)* | Ignition On,  Accessory On |
| Safe State:  *(in case of categories “General”, “Metric”, “Non-E/E Requirement”, or “User Information”: if applicable)* | Steering Column Tilt Adjustment Request (StewPosAdjTlt\_D\_Rq = Idle) is sent on HS3-CAN Bus  Steering Column Telescopic Adjustment Request (StewPosAdjTel\_D\_Rq = Idle) is sent on HS3-CAN Bus |
| Reduced Functionality Tolerance Time Interval:  *(if applicable;*  *in case of categories “Metric”, “Non-E/E Requirement”, “Maintain Safe State / Recovery” or “User Information”: not applicable;*  *in case of category “Reduced Functionality”: required)* | N/A |
| Fault Handling Time Segment:  *(in case of categories “Metric” or “Maintain Safe State / Recovery”: not applicable;*  *in case of category “General”, “Reduced Functionality”, “Non-E/E Requirement”, or “User Information”: if applicable)* | 500ms |
| Requirement Status | Approved |
| V&V method: | Test |
| V&V acceptance criteria:  *(UNV1 / UPV1, not in case of category “Non-E/E requirement)* | System testing: APIM\_CDC closes contextual control state for steering column adjust control after a 10 sec Idle timeout (No touch input to right hand steering wheel switch) |
| Allocated Element(s)/Component(s)/ System(s) *(if applicable)* | APIM\_CDC |

Table 12: Element/Component/System Technical Safety Requirements SCPC-T-S-Req01.4.1

### Requirement Derivation for SCPC-F-S-Req01.5 (Provide Steering Column Tilt Position Command)

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

*Derive Technical Safety Requirements from Functional Safety Requirements.*

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

Figure 2 - Technical Safety Requirements Derivation Diagram for SCPC-F-S-Req01.5

#### Technical Safety Requirements

| T-S-Req-ID: | SCPC-T-S-Req01.5.1 |
| --- | --- |
| External Reference *(optional)* |  |
| Category: | Safety Related Function |
| Version  *(only in case of category “Non-E/E requirement”)* |  |
| Author  *(only in case of category “Non-E/E requirement”)* |  |
| Safety Goal ID: | SG01: Prevent impaired access to the steering controls |
| F-S-Req ID: | SCPC-F-S-Req01.5 Provide Steering Column Tilt Position Command |
| ASIL Classification:  *(in case of category “General”: if applicable, in case of category “Non-E/E Requirement”: not applicable)* | ASIL B |
| Technical Safety Requirement Title: | DSM Provides Motor Power for Manual Steering Column Tilt Movement |
| Technical Safety Requirement Text: | The DSM shall provide system voltage (~12V) to the steering column tilt motor for manual steering column tilt movement (TILT\_POS\_ADJ\_RNG, TILT\_POS\_ADJ\_SPEED) only when steering column tilt position adjustment request (StewPosAdjTlt\_D\_Rq = Tilt Up or Tilt Down) is received on FD3-CAN Bus.  In case of steering column tilt position adjustment request (StewPosAdjTlt\_D\_Rq = Idle), DSM shall initiate transition to a safe state within fault handling time interval  NOTE: DSM Fault handling time interval (FHTI) = 500ms  (sum of fault detection time interval and the fault reaction time interval) |
| Rationale: | To ensure safe execution of control algorithm (controller’s decision-making process that determines the motor power for manual steering column tilt movement) |
| Operating Mode:  *(in case of categories “General”, “Metric”, “Non-E/E Requirement”, or “User Information”: if applicable)* | Ignition On,  Accessory On |
| Safe State:  *(in case of categories “General”, “Metric”, “Non-E/E Requirement”, or “User Information”: if applicable)* | Motor Power is Turned Off for Manual Steering Column Tilt Movement |
| Reduced Functionality Tolerance Time Interval:  *(if applicable;*  *in case of categories “Metric”, “Non-E/E Requirement”, “Maintain Safe State / Recovery” or “User Information”: not applicable;*  *in case of category “Reduced Functionality”: required)* | N/A |
| Fault Handling Time Segment:  *(in case of categories “Metric” or “Maintain Safe State / Recovery”: not applicable;*  *in case of category “General”, “Reduced Functionality”, “Non-E/E Requirement”, or “User Information”: if applicable)* | 500ms |
| Requirement Status | Approved |
| V&V method: | Test |
| V&V acceptance criteria:  *(UNV1 / UPV1, not in case of category “Non-E/E requirement)* | System testing: DSM provides system voltage (~12V) to the steering column tilt motor for manual steering column tilt movement when steering column tilt position adjustment request (StewPosAdjTlt\_D\_Rq= Tilt Up or Tilt Down) is received on FD3-CAN Bus |
| Allocated Element(s)/Component(s)/ System(s) *(if applicable)* | DSM |

Table 13: Element/Component/System Technical Safety Requirements SCPC-T-S-Req01.5.1

| T-S-Req-ID: | SCPC-T-S-Req01.5.2 |
| --- | --- |
| External Reference *(optional)* |  |
| Category: | External Fault Handling |
| Version  *(only in case of category “Non-E/E requirement”)* |  |
| Author  *(only in case of category “Non-E/E requirement”)* |  |
| Safety Goal ID: | SG01: Prevent impaired access to the steering controls |
| F-S-Req ID: | SCPC-F-S-Req01.5 Provide Steering Column Tilt Position Command |
| ASIL Classification:  *(in case of category “General”: if applicable, in case of category “Non-E/E Requirement”: not applicable)* | ASIL B |
| Technical Safety Requirement Title: | DSM Verifies Steering Column Tilt Adjustment Request Checksum and Counter |
| Technical Safety Requirement Text: | The DSM shall verify the checksum (StewPosAdjTlt\_D\_Rq \_No\_Cs), counter (StewPosAdjTlt\_D\_Rq \_No\_Cnt) and timeout of received steering column tilt position adjustment request on FD3-CAN Bus.  If the checksum (StewPosAdjTlt\_D\_Rq \_No\_Cs) or counter (StewPosAdjTlt\_D\_Rq \_No\_Cnt)) or timeout of received steering column tilt position adjustment request fails, DSM shall set an internal software flag to "INVALID" and transition to a safe state within fault handling time interval.  NOTE: DSM Fault handling time interval (FHTI) = 500ms  (sum of fault detection time interval and the fault reaction time interval) |
| Rationale: | ASIL rated signals must be end-to-end protected to ensure signal integrity between the transmitter and receiver |
| Operating Mode:  *(in case of categories “General”, “Metric”, “Non-E/E Requirement”, or “User Information”: if applicable)* | Ignition On,  Accessory On |
| Safe State:  *(in case of categories “General”, “Metric”, “Non-E/E Requirement”, or “User Information”: if applicable)* | Motor Power is Turned Off for Manual Steering Column Tilt Movement |
| Reduced Functionality Tolerance Time Interval:  *(if applicable;*  *in case of categories “Metric”, “Non-E/E Requirement”, “Maintain Safe State / Recovery” or “User Information”: not applicable;*  *in case of category “Reduced Functionality”: required)* | N/A |
| Fault Handling Time Segment:  *(in case of categories “Metric” or “Maintain Safe State / Recovery”: not applicable;*  *in case of category “General”, “Reduced Functionality”, “Non-E/E Requirement”, or “User Information”: if applicable)* | 500ms |
| Requirement Status | Approved |
| V&V method: | Test |
| V&V acceptance criteria:  *(UNV1 / UPV1, not in case of category “Non-E/E requirement)* | System testing: Manipulate checksum or counter of input signal. DSM must set correct replacement value during fault confirmation time. DSM must flag signal as invalid internally, after confirmation time is exceeded.  Start with sending signal in specified periodicity. Stop sending signal (simulate missed message). DSM must set correct replacement value during fault confirmation time. DSM must flag signal as invalid internally, after confirmation time is exceeded. |
| Allocated Element(s)/Component(s)/ System(s) *(if applicable)* | DSM |

Table 14: Element/Component/System Technical Safety Requirements SCPC-T-S-Req01.5.2

### Requirement Derivation for SCPC-F-S-Req01.6 (Provide Steering Column Telescopic Position Command)

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

*Derive Technical Safety Requirements from Functional Safety Requirements.*

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

Figure 2 - Technical Safety Requirements Derivation Diagram for SCPC-F-S-Req01.6

#### Technical Safety Requirements

| T-S-Req-ID: | SCPC-T-S-Req01.6.1 |
| --- | --- |
| External Reference *(optional)* |  |
| Category: | Safety Related Function |
| Version  *(only in case of category “Non-E/E requirement”)* |  |
| Author  *(only in case of category “Non-E/E requirement”)* |  |
| Safety Goal ID: | SG01: Prevent impaired access to the steering controls |
| F-S-Req ID: | SCPC-F-S-Req01.6 Provide Steering Column Telescopic Position Command |
| ASIL Classification:  *(in case of category “General”: if applicable, in case of category “Non-E/E Requirement”: not applicable)* | ASIL B |
| Technical Safety Requirement Title: | DSM Provides Motor Power for Manual Steering Column Telescopic Movement |
| Technical Safety Requirement Text: | The DSM shall provide system voltage (~12V) to the steering column telescopic motor for manual steering column tele movement (TEL\_POS\_ADJ\_RNG, TEL\_POS\_ADJ\_SPEED) only when steering column tele position adjustment request (StewPosAdjTel\_D\_Rq = Tel IN or Tel OUT) is received on FD3-CAN Bus.  In case of steering column telescopic position adjustment request (StewPosAdjTel\_D\_Rq = Idle), DSM shall initiate transition to a safe state within fault handling time interval  NOTE: DSM Fault handling time interval (FHTI) = 500ms  (sum of fault detection time interval and the fault reaction time interval) |
| Rationale: | To ensure safe execution of control algorithm (controller’s decision-making process that determines the motor power for manual steering column tele movement) |
| Operating Mode:  *(in case of categories “General”, “Metric”, “Non-E/E Requirement”, or “User Information”: if applicable)* | Ignition On,  Accessory On |
| Safe State:  *(in case of categories “General”, “Metric”, “Non-E/E Requirement”, or “User Information”: if applicable)* | Motor Power is Turned Off for Manual Steering Column Telescopic Movement |
| Reduced Functionality Tolerance Time Interval:  *(if applicable;*  *in case of categories “Metric”, “Non-E/E Requirement”, “Maintain Safe State / Recovery” or “User Information”: not applicable;*  *in case of category “Reduced Functionality”: required)* | N/A |
| Fault Handling Time Segment:  *(in case of categories “Metric” or “Maintain Safe State / Recovery”: not applicable;*  *in case of category “General”, “Reduced Functionality”, “Non-E/E Requirement”, or “User Information”: if applicable)* | 500ms |
| Requirement Status | Approved |
| V&V method: | Test |
| V&V acceptance criteria:  *(UNV1 / UPV1, not in case of category “Non-E/E requirement)* | System testing: DSM provides system voltage (~12V) to the steering column tele motor for manual steering column tele movement when steering column tele position adjustment request (StewPosAdjTel\_D\_Rq= Tel IN or Tel OUT) is received on FD3-CAN Bus |
| Allocated Element(s)/Component(s)/ System(s) *(if applicable)* | DSM |

Table 15: Element/Component/System Technical Safety Requirements SCPC-T-S-Req01.6.1

| T-S-Req-ID: | SCPC-T-S-Req01.6.2 |
| --- | --- |
| External Reference *(optional)* |  |
| Category: | Safety Related Function |
| Version  *(only in case of category “Non-E/E requirement”)* |  |
| Author  *(only in case of category “Non-E/E requirement”)* |  |
| Safety Goal ID: | SG01: Prevent impaired access to the steering controls |
| F-S-Req ID: | SCPC-F-S-Req01.6 Provide Steering Column Telescopic Position Command |
| ASIL Classification:  *(in case of category “General”: if applicable, in case of category “Non-E/E Requirement”: not applicable)* | ASIL B |
| Technical Safety Requirement Title: | DSM Verifies Steering Column Tele Adjustment Request Checksum and Counter |
| Technical Safety Requirement Text: | The DSM shall verify the checksum (StewPosAdjTel\_D\_Rq \_No\_Cs), counter (StewPosAdjTel\_D\_Rq \_No\_Cnt) and timeout of received steering column tele position adjustment request on FD3-CAN Bus according to the specified E2E protection (AUTOSAR PROFILE 1A for Checksum and Counter).  If the checksum (StewPosAdjTel\_D\_Rq \_No\_Cs) or counter (StewPosAdjTel\_D\_Rq \_No\_Cnt)) or timeout of received steering column tele position adjustment request fails, DSM shall set an internal software flag to "INVALID" and transition to a safe state within fault handling time interval.  NOTE: DSM Fault handling time interval (FHTI) = 500ms  (sum of fault detection time interval and the fault reaction time interval) |
| Rationale: | ASIL rated signals must be end-to-end protected to ensure signal integrity between the transmitter and receiver |
| Operating Mode:  *(in case of categories “General”, “Metric”, “Non-E/E Requirement”, or “User Information”: if applicable)* | Ignition On,  Accessory On |
| Safe State:  *(in case of categories “General”, “Metric”, “Non-E/E Requirement”, or “User Information”: if applicable)* | Motor Power is Turned Off for Manual Steering Column Telescopic Movement |
| Reduced Functionality Tolerance Time Interval:  *(if applicable;*  *in case of categories “Metric”, “Non-E/E Requirement”, “Maintain Safe State / Recovery” or “User Information”: not applicable;*  *in case of category “Reduced Functionality”: required)* | N/A |
| Fault Handling Time Segment:  *(in case of categories “Metric” or “Maintain Safe State / Recovery”: not applicable;*  *in case of category “General”, “Reduced Functionality”, “Non-E/E Requirement”, or “User Information”: if applicable)* | 500ms |
| Requirement Status | Approved |
| V&V method: | Test |
| V&V acceptance criteria:  *(UNV1 / UPV1, not in case of category “Non-E/E requirement)* | System testing: Manipulate checksum or counter of input signal. DSM must set correct replacement value during fault confirmation time. DSM must flag signal as invalid internally, after confirmation time is exceeded.  Start with sending signal in specified periodicity. Stop sending signal (simulate missed message). DSM must set correct replacement value during fault confirmation time. DSM must flag signal as invalid internally, after confirmation time is exceeded. |
| Allocated Element(s)/Component(s)/ System(s) *(if applicable)* | DSM |

Table 16: Element/Component/System Technical Safety Requirements SCPC-T-S-Req01.6.2

### Requirement Derivation for SCPC-F-S-Req01.7 (Actuate Commanded Steering Column Tilt Position)

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

*Derive Technical Safety Requirements from Functional Safety Requirements.*

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

Figure 2 - Technical Safety Requirements Derivation Diagram for SCPS-F-S-Req01.7

#### Technical Safety Requirements

| T-S-Req-ID: | SCPC-T-S-Req01.7.1 |
| --- | --- |
| External Reference *(optional)* |  |
| Category: | Internal Fault Handling |
| Version  *(only in case of category “Non-E/E requirement”)* |  |
| Author  *(only in case of category “Non-E/E requirement”)* |  |
| Safety Goal ID: | SG01: Prevent impaired access to the steering controls |
| F-S-Req ID: | SCPC-F-S-Req01.7 Actuate Commanded Steering Column Tilt Position |
| ASIL Classification:  *(in case of category “General”: if applicable, in case of category “Non-E/E Requirement”: not applicable)* | ASIL B |
| Technical Safety Requirement Title: | APIM\_CDC Monitors Single-Point Faults Regarding Steering Column Tilt Position Adjustment |
| Technical Safety Requirement Text: | The APIM\_CDC shall monitor the single-point faults in the APIM\_CDC hardware and software resources that responsible for steering column tilt position adjustment.  In case of any detected fault, the internal APIM\_CDC Failure flag shall be set to "INVALID" and transition to a safe state within fault handling time interval.  APIM\_CDC self-monitoring can include following checks (as applicable) to detect random hardware faults and, if appropriate, to detect systematic faults of APIM\_CDC:  - Program Sequence Checks  - RAM/ROM Checks  - Software Logic Checks  - Other Checks (If applicable) |
| Rationale: | To ensure the reliable execution of APIM\_CDC. |
| Operating Mode:  *(in case of categories “General”, “Metric”, “Non-E/E Requirement”, or “User Information”: if applicable)* | Ignition On,  Accessory On |
| Safe State:  *(in case of categories “General”, “Metric”, “Non-E/E Requirement”, or “User Information”: if applicable)* | Steering Column Tilt Adjustment Request (StewPosAdjTlt\_D\_Rq = Idle) is sent on HS3-CAN Bus |
| Reduced Functionality Tolerance Time Interval:  *(if applicable;*  *in case of categories “Metric”, “Non-E/E Requirement”, “Maintain Safe State / Recovery” or “User Information”: not applicable;*  *in case of category “Reduced Functionality”: required)* | N/A |
| Fault Handling Time Segment:  *(in case of categories “Metric” or “Maintain Safe State / Recovery”: not applicable;*  *in case of category “General”, “Reduced Functionality”, “Non-E/E Requirement”, or “User Information”: if applicable)* | 500ms |
| Requirement Status | Approved |
| V&V method: | Test  Analysis |
| V&V acceptance criteria:  *(UNV1 / UPV1, not in case of category “Non-E/E requirement)* | Fault Injection Testing. APIM\_CDC detects all single-point faults in the APIMC\_CDC itself. APIM\_CDC failure SW flag is set to "INVALID". |
| Allocated Element(s)/Component(s)/ System(s) *(if applicable)* | APIM\_CDC |

Table 17: Element/Component/System Technical Safety Requirements SCPC-T-S-Req01.7.1

| T-S-Req-ID: | SCPC-T-S-Req01.7.2 |
| --- | --- |
| External Reference *(optional)* |  |
| Category: | Internal Fault Handling |
| Version  *(only in case of category “Non-E/E requirement”)* |  |
| Author  *(only in case of category “Non-E/E requirement”)* |  |
| Safety Goal ID: | SG01: Prevent impaired access to the steering controls |
| F-S-Req ID: | SCPC-F-S-Req01.7 Actuate Commanded Steering Column Tilt Position |
| ASIL Classification:  *(in case of category “General”: if applicable, in case of category “Non-E/E Requirement”: not applicable)* | ASIL B |
| Technical Safety Requirement Title: | DSM Monitors Single-Point Faults Regarding Manual Steering Column Tilt Movement |
| Technical Safety Requirement Text: | The DSM shall monitor the single-point faults in the DSM hardware and software resources that responsible for steering column tilt movement.  In case of any detected fault, the internal DSM Failure flag shall be set to "INVALID" and transition to a safe state within fault handling time interval.  DSM self-monitoring can include following checks (as applicable) to detect random hardware faults and, if appropriate, to detect systematic faults of DSM:  - Program Sequence Checks  - RAM/ROM Checks  - Software Logic Checks  - Output "Motor signals" Checks  - H-bridge and Wiring Harness Checks  - Other Checks (If applicable) |
| Rationale: | To ensure the reliable execution of DSM. |
| Operating Mode:  *(in case of categories “General”, “Metric”, “Non-E/E Requirement”, or “User Information”: if applicable)* | Ignition On,  Accessory On |
| Safe State:  *(in case of categories “General”, “Metric”, “Non-E/E Requirement”, or “User Information”: if applicable)* | Motor Power is Turned Off for Manual Steering Column Tilt Movement |
| Reduced Functionality Tolerance Time Interval:  *(if applicable;*  *in case of categories “Metric”, “Non-E/E Requirement”, “Maintain Safe State / Recovery” or “User Information”: not applicable;*  *in case of category “Reduced Functionality”: required)* | N/A |
| Fault Handling Time Segment:  *(in case of categories “Metric” or “Maintain Safe State / Recovery”: not applicable;*  *in case of category “General”, “Reduced Functionality”, “Non-E/E Requirement”, or “User Information”: if applicable)* | 500ms |
| Requirement Status | Approved |
| V&V method: | Test  Analysis |
| V&V acceptance criteria:  *(UNV1 / UPV1, not in case of category “Non-E/E requirement)* | Fault Injection Testing. DSM detects all single-point faults in the DSM itself. DSM failure SW flag is set to "INVALID". |
| Allocated Element(s)/Component(s)/ System(s) *(if applicable)* | DSM |

Table 17: Element/Component/System Technical Safety Requirements SCPC-T-S-Req01.7.2

| T-S-Req-ID: | SCPC-T-S-Req01.7.3 |
| --- | --- |
| External Reference *(optional)* |  |
| Category: | Latent Fault Handling |
| Version  *(only in case of category “Non-E/E requirement”)* |  |
| Author  *(only in case of category “Non-E/E requirement”)* |  |
| Safety Goal ID: | SG01: Prevent impaired access to the steering controls |
| F-S-Req ID: | SCPC-F-S-Req01.7 Actuate Commanded Steering Column Tilt Position |
| ASIL Classification:  *(in case of category “General”: if applicable, in case of category “Non-E/E Requirement”: not applicable)* | ASIL A |
| Technical Safety Requirement Title: | APIM\_CDC Monitors Latent Faults Regarding Steering Column Tilt Position Adjustment |
| Technical Safety Requirement Text: | The APIM\_CDC shall monitor the latent faults in the APIM\_CDC hardware and software resources that can enable unintended steering column tilt position adjustment.  In case of any detected latent fault, the internal APIM\_CDC Failure flag shall be set to "INVALID" and transition to a safe state within fault handling time interval.  APIM\_CDC self-monitoring can include following checks (as applicable) to detect random hardware faults and, if appropriate, to detect systematic faults:  - Power-up self-checks for APIM\_CDC hardware resources  - Other Checks (If applicable) |
| Rationale: | To avoid multiple-point faults that have the potential to be latent (e.g., fault in the safety mechanism that detect/mitigate single-point fault)  The development of safety mechanisms that are implemented only to prevent dual point faults from being latent shall at least comply with ASIL A for technical safety requirements assigned ASIL B (ISO 26262-4, 6.4.2.5) |
| Operating Mode:  *(in case of categories “General”, “Metric”, “Non-E/E Requirement”, or “User Information”: if applicable)* | Ignition On,  Accessory On |
| Safe State:  *(in case of categories “General”, “Metric”, “Non-E/E Requirement”, or “User Information”: if applicable)* | Steering Column Tilt Adjustment Request (StewPosAdjTlt\_D\_Rq = Idle) is sent on HS3-CAN Bus |
| Reduced Functionality Tolerance Time Interval:  *(if applicable;*  *in case of categories “Metric”, “Non-E/E Requirement”, “Maintain Safe State / Recovery” or “User Information”: not applicable;*  *in case of category “Reduced Functionality”: required)* | N/A |
| Fault Handling Time Segment:  *(in case of categories “Metric” or “Maintain Safe State / Recovery”: not applicable;*  *in case of category “General”, “Reduced Functionality”, “Non-E/E Requirement”, or “User Information”: if applicable)* | 500ms |
| Requirement Status | Approved |
| V&V method: | Test  Analysis |
| V&V acceptance criteria:  *(UNV1 / UPV1, not in case of category “Non-E/E requirement)* | Fault Injection Testing. APIM\_CDC detects latent failures and sets the internal APIM\_CDC failure SW flag to "INVALID". |
| Allocated Element(s)/Component(s)/ System(s) *(if applicable)* | APIM\_CDC |

Table 17: Element/Component/System Technical Safety Requirements SCPC-T-S-Req01.7.3

| T-S-Req-ID: | SCPC-T-S-Req01.7.4 |
| --- | --- |
| External Reference *(optional)* |  |
| Category: | Latent Fault Handling |
| Version  *(only in case of category “Non-E/E requirement”)* |  |
| Author  *(only in case of category “Non-E/E requirement”)* |  |
| Safety Goal ID: | SG01: Prevent impaired access to the steering controls |
| F-S-Req ID: | SCPC-F-S-Req01.7 Actuate Commanded Steering Column Tilt Position |
| ASIL Classification:  *(in case of category “General”: if applicable, in case of category “Non-E/E Requirement”: not applicable)* | ASIL A |
| Technical Safety Requirement Title: | DSM Monitors Latent Faults Regarding Manual Steering Column Tilt Movement |
| Technical Safety Requirement Text: | The DSM shall monitor the latent faults in the DSM hardware and software resources that can enable unintended steering column tilt movement.  In case of any detected latent fault, the internal DSM Failure flag shall be set to "INVALID" and transition to a safe state within fault handling time interval.  DSM self-monitoring can include following checks (as applicable) to detect random hardware faults and, if appropriate, to detect systematic faults:  - Power-up self-checks for DSM hardware resources  - Other Checks (If applicable) |
| Rationale: | To avoid multiple-point faults that have the potential to be latent (e.g., fault in the safety mechanism that detect/mitigate single-point fault)  The development of safety mechanisms that are implemented only to prevent dual point faults from being latent shall at least comply with ASIL A for technical safety requirements assigned ASIL B (ISO 26262-4, 6.4.2.5) |
| Operating Mode:  *(in case of categories “General”, “Metric”, “Non-E/E Requirement”, or “User Information”: if applicable)* | Ignition On,  Accessory On |
| Safe State:  *(in case of categories “General”, “Metric”, “Non-E/E Requirement”, or “User Information”: if applicable)* | Motor Power is Turned Off for Manual Steering Column Tilt Movement |
| Reduced Functionality Tolerance Time Interval:  *(if applicable;*  *in case of categories “Metric”, “Non-E/E Requirement”, “Maintain Safe State / Recovery” or “User Information”: not applicable;*  *in case of category “Reduced Functionality”: required)* | N/A |
| Fault Handling Time Segment:  *(in case of categories “Metric” or “Maintain Safe State / Recovery”: not applicable;*  *in case of category “General”, “Reduced Functionality”, “Non-E/E Requirement”, or “User Information”: if applicable)* | 500ms |
| Requirement Status | Approved |
| V&V method: | Test  Analysis |
| V&V acceptance criteria:  *(UNV1 / UPV1, not in case of category “Non-E/E requirement)* | Fault Injection Testing. DSM detects latent faults and sets the internal DSM failure SW flag to "INVALID". |
| Allocated Element(s)/Component(s)/ System(s) *(if applicable)* | DSM |

Table 17: Element/Component/System Technical Safety Requirements SCPC-T-S-Req01.7.4

### Requirement Derivation for SCPC-F-S-Req01.8 (Actuate Commanded Steering Column Telescopic Position)

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

*Derive Technical Safety Requirements from Functional Safety Requirements.*

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

Figure 2 - Technical Safety Requirements Derivation Diagram for SCPS-F-S-Req01.8

#### Technical Safety Requirements

| T-S-Req-ID: | SCPC-T-S-Req01.8.1 |
| --- | --- |
| External Reference *(optional)* |  |
| Category: | Internal Fault Handling |
| Version  *(only in case of category “Non-E/E requirement”)* |  |
| Author  *(only in case of category “Non-E/E requirement”)* |  |
| Safety Goal ID: | SG01: Prevent impaired access to the steering controls |
| F-S-Req ID: | SCPC-F-S-Req01.8 Actuate Commanded Steering Column Telescopic Position |
| ASIL Classification:  *(in case of category “General”: if applicable, in case of category “Non-E/E Requirement”: not applicable)* | ASIL B |
| Technical Safety Requirement Title: | APIM\_CDC Monitors Single-Point Faults Regarding Steering Column Telescopic Position Adjustment |
| Technical Safety Requirement Text: | The APIM\_CDC shall monitor the single-point faults in the APIM\_CDC hardware and software resources that responsible for steering column tele position adjustment.  In case of any detected fault, the internal APIM\_CDC Failure flag shall be set to "INVALID" and transition to a safe state within fault handling time interval.  APIM\_CDC self-monitoring can include following checks (as applicable) to detect random hardware faults and, if appropriate, to detect systematic faults of APIM\_CDC :  - Program Sequence Checks  - RAM/ROM Checks  - Software Logic Checks  - Other Checks (If applicable) |
| Rationale: | To ensure the reliable execution of APIM\_CDC. |
| Operating Mode:  *(in case of categories “General”, “Metric”, “Non-E/E Requirement”, or “User Information”: if applicable)* | Ignition On,  Accessory On |
| Safe State:  *(in case of categories “General”, “Metric”, “Non-E/E Requirement”, or “User Information”: if applicable)* | Steering Column Tele Adjustment Request (StewPosAdjTel\_D\_Rq = Idle) is sent on HS3-CAN Bus |
| Reduced Functionality Tolerance Time Interval:  *(if applicable;*  *in case of categories “Metric”, “Non-E/E Requirement”, “Maintain Safe State / Recovery” or “User Information”: not applicable;*  *in case of category “Reduced Functionality”: required)* | N/A |
| Fault Handling Time Segment:  *(in case of categories “Metric” or “Maintain Safe State / Recovery”: not applicable;*  *in case of category “General”, “Reduced Functionality”, “Non-E/E Requirement”, or “User Information”: if applicable)* | 500ms |
| Requirement Status | Approved |
| V&V method: | Test  Analysis |
| V&V acceptance criteria:  *(UNV1 / UPV1, not in case of category “Non-E/E requirement)* | Fault Injection Testing. APIM\_CDC detects all single-point faults in the APIM\_CDC itself and sets the internal APIM\_CDC failure SW flag to "INVALID". |
| Allocated Element(s)/Component(s)/ System(s) *(if applicable)* | APIM\_CDC |

Table 17: Element/Component/System Technical Safety Requirements SCPC-T-S-Req01.8.1

| T-S-Req-ID: | SCPC-T-S-Req01.8.2 |
| --- | --- |
| External Reference *(optional)* |  |
| Category: | Internal Fault Handling |
| Version  *(only in case of category “Non-E/E requirement”)* |  |
| Author  *(only in case of category “Non-E/E requirement”)* |  |
| Safety Goal ID: | SG01: Prevent impaired access to the steering controls |
| F-S-Req ID: | SCPC-F-S-Req01.8 Actuate Commanded Steering Column Telescopic Position |
| ASIL Classification:  *(in case of category “General”: if applicable, in case of category “Non-E/E Requirement”: not applicable)* | ASIL B |
| Technical Safety Requirement Title: | DSM Monitors Single-Point Faults Regarding Manual Steering Column Telescopic Movement |
| Technical Safety Requirement Text: | The DSM shall monitor the single-point faults in the DSM hardware and software resources that responsible for steering column tele position adjustment.  In case of any detected fault, the internal DSM Failure flag shall be set to "INVALID" and transition to a safe state within fault handling time interval.  DSM self-monitoring can include following checks (as applicable) to detect random hardware faults and, if appropriate, to detect systematic faults of DSM :  - Program Sequence Checks  - RAM/ROM Checks  - Software Logic Checks  - Output "Motor signals" Checks  - H-bridge and Wiring Harness Checks  - Other Checks (If applicable) |
| Rationale: | To ensure the reliable execution of DSM. |
| Operating Mode:  *(in case of categories “General”, “Metric”, “Non-E/E Requirement”, or “User Information”: if applicable)* | Ignition On,  Accessory On |
| Safe State:  *(in case of categories “General”, “Metric”, “Non-E/E Requirement”, or “User Information”: if applicable)* | Motor Power is Turned Off for Manual Steering Column Telescopic Movement |
| Reduced Functionality Tolerance Time Interval:  *(if applicable;*  *in case of categories “Metric”, “Non-E/E Requirement”, “Maintain Safe State / Recovery” or “User Information”: not applicable;*  *in case of category “Reduced Functionality”: required)* | N/A |
| Fault Handling Time Segment:  *(in case of categories “Metric” or “Maintain Safe State / Recovery”: not applicable;*  *in case of category “General”, “Reduced Functionality”, “Non-E/E Requirement”, or “User Information”: if applicable)* | 500ms |
| Requirement Status | Approved |
| V&V method: | Test  Analysis |
| V&V acceptance criteria:  *(UNV1 / UPV1, not in case of category “Non-E/E requirement)* | Fault Injection Testing. DSM detects all single-point faults in the DSM itself and sets the internal DSM failure SW flag to "INVALID". |
| Allocated Element(s)/Component(s)/ System(s) *(if applicable)* | DSM |

Table 17: Element/Component/System Technical Safety Requirements SCPC-T-S-Req01.8.2

| T-S-Req-ID: | SCPC-T-S-Req01.8.3 |
| --- | --- |
| External Reference *(optional)* |  |
| Category: | Latent Fault Handling |
| Version  *(only in case of category “Non-E/E requirement”)* |  |
| Author  *(only in case of category “Non-E/E requirement”)* |  |
| Safety Goal ID: | SG01: Prevent impaired access to the steering controls |
| F-S-Req ID: | SCPC-F-S-Req01.8 Actuate Commanded Steering Column Telescopic Position |
| ASIL Classification:  *(in case of category “General”: if applicable, in case of category “Non-E/E Requirement”: not applicable)* | ASIL A |
| Technical Safety Requirement Title: | APIM\_CDC Monitors Latent Faults for Steering Column Telescopic Position Adjustment |
| Technical Safety Requirement Text: | The APIM\_CDC shall monitor the latent faults in the APIM\_CDC hardware and software resources responsible for steering column tele position adjustment.  In case of any detected latent fault, the internal APIM\_CDC Failure flag shall be set to "INVALID" and transition to a safe state within fault handling time interval.  APIM\_CDC self-monitoring can include following checks (as applicable) to detect random hardware faults and, if appropriate, to detect systematic faults:  - Power-up self-checks for APIM\_CDC hardware resources  - Other Checks (If applicable) |
| Rationale: | To avoid multiple-point faults that have the potential to be latent (e.g., fault in the safety mechanism that detect/mitigate single-point fault)  The development of safety mechanisms that are implemented only to prevent dual point faults from being latent shall at least comply with ASIL A for technical safety requirements assigned ASIL B (ISO 26262-4, 6.4.2.5) |
| Operating Mode:  *(in case of categories “General”, “Metric”, “Non-E/E Requirement”, or “User Information”: if applicable)* | Ignition On,  Accessory On |
| Safe State:  *(in case of categories “General”, “Metric”, “Non-E/E Requirement”, or “User Information”: if applicable)* | Steering Column Tele Adjustment Request (StewPosAdjTel\_D\_Rq = Idle) is sent on HS3-CAN Bus |
| Reduced Functionality Tolerance Time Interval:  *(if applicable;*  *in case of categories “Metric”, “Non-E/E Requirement”, “Maintain Safe State / Recovery” or “User Information”: not applicable;*  *in case of category “Reduced Functionality”: required)* | N/A |
| Fault Handling Time Segment:  *(in case of categories “Metric” or “Maintain Safe State / Recovery”: not applicable;*  *in case of category “General”, “Reduced Functionality”, “Non-E/E Requirement”, or “User Information”: if applicable)* | 500ms |
| Requirement Status | Approved |
| V&V method: | Test  Analysis |
| V&V acceptance criteria:  *(UNV1 / UPV1, not in case of category “Non-E/E requirement)* | Fault Injection Testing. APIM\_CDC detects latent faults and sets the internal APIM\_CDC failure SW flag to "INVALID". |
| Allocated Element(s)/Component(s)/ System(s) *(if applicable)* | APIM\_CDC |

Table 17: Element/Component/System Technical Safety Requirements SCPC-T-S-Req01.8.3

| T-S-Req-ID: | SCPC-T-S-Req01.8.4 |
| --- | --- |
| External Reference *(optional)* |  |
| Category: | Latent Fault Handling |
| Version  *(only in case of category “Non-E/E requirement”)* |  |
| Author  *(only in case of category “Non-E/E requirement”)* |  |
| Safety Goal ID: | SG01: Prevent impaired access to the steering controls |
| F-S-Req ID: | SCPC-F-S-Req01.8 Actuate Commanded Steering Column Telescopic Position |
| ASIL Classification:  *(in case of category “General”: if applicable, in case of category “Non-E/E Requirement”: not applicable)* | ASIL A |
| Technical Safety Requirement Title: | DSM Monitors Latent Faults for Manual Steering Column Telescopic Movement |
| Technical Safety Requirement Text: | The DSM shall monitor the latent faults in the DSM hardware and software resources responsible for steering column tele position adjustment.  In case of any detected latent fault, the internal DSM Failure flag shall be set to "INVALID" and transition to a safe state within fault handling time interval (TBD).  DSM self-monitoring can include following checks (as applicable) to detect random hardware faults and, if appropriate, to detect systematic faults:  - Power-up self-checks for DSM hardware resources  - Other Checks (If applicable) |
| Rationale: | To avoid multiple-point faults that have the potential to be latent (e.g., fault in the safety mechanism that detect/mitigate single-point fault).  The development of safety mechanisms that are implemented only to prevent dual point faults from being latent shall at least comply with ASIL A for technical safety requirements assigned ASIL B (ISO 26262-4, 6.4.2.5) |
| Operating Mode:  *(in case of categories “General”, “Metric”, “Non-E/E Requirement”, or “User Information”: if applicable)* | Ignition On,  Accessory On |
| Safe State:  *(in case of categories “General”, “Metric”, “Non-E/E Requirement”, or “User Information”: if applicable)* | Motor Power is Turned Off for Manual Steering Column Telescopic Movement |
| Reduced Functionality Tolerance Time Interval:  *(if applicable;*  *in case of categories “Metric”, “Non-E/E Requirement”, “Maintain Safe State / Recovery” or “User Information”: not applicable;*  *in case of category “Reduced Functionality”: required)* | N/A |
| Fault Handling Time Segment:  *(in case of categories “Metric” or “Maintain Safe State / Recovery”: not applicable;*  *in case of category “General”, “Reduced Functionality”, “Non-E/E Requirement”, or “User Information”: if applicable)* | 500ms |
| Requirement Status | Approved |
| V&V method: | Test  Analysis |
| V&V acceptance criteria:  *(UNV1 / UPV1, not in case of category “Non-E/E requirement)* | Fault Injection Testing. DSM detects all latent faults and sets the internal DSM failure SW flag to "INVALID". |
| Allocated Element(s)/Component(s)/ System(s) *(if applicable)* | DSM |

Table 17: Element/Component/System Technical Safety Requirements SCPC-T-S-Req01.7.4

### Requirement Derivation for SCPC-F-S-Req01.9 (Inhibit steering column tilt position adjustment)

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

*Derive Technical Safety Requirements from Functional Safety Requirements.*

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

Figure 2 - Technical Safety Requirements Derivation Diagram for SCPC-F-S-Req01.9

#### Technical Safety Requirements

| T-S-Req-ID: | SCPC-T-S-Req01.9.1 |
| --- | --- |
| External Reference *(optional)* |  |
| Category: | Maintain Safe State/Recovery |
| Version  *(only in case of category “Non-E/E requirement”)* |  |
| Author  *(only in case of category “Non-E/E requirement”)* |  |
| Safety Goal ID: | SG01: Prevent impaired access to the steering controls |
| F-S-Req ID: | SCPC-F-S-Req01.9 Inhibit steering column tilt position adjustment  SCPC-F-S-Req01.11 Enable steering column tilt position adjustment |
| ASIL Classification:  *(in case of category “General”: if applicable, in case of category “Non-E/E Requirement”: not applicable)* | ASIL B |
| Technical Safety Requirement Title: | APIM\_CDC Sends Steering Column Tilt Position Adjustment Request as IDLE |
| Technical Safety Requirement Text: | The APIM\_CDC shall send steering column tilt position adjustment request as idle (StewPosAdjTlt\_D\_Rq = Idle) on HS3-CAN if any of following condition is true:   * contextual control state is not equal to steering column adjust controls * a safety critical fault is detected in the APIM\_CDC itself   APIM\_CDC shall maintain the safe state until correct operation of failed APIM\_CDC resources and contextual control state for steering column adjust control are sufficiently validated  NOTE: APIM\_CDC Fault handling time interval (FHTI) = 500ms  (sum of fault detection time interval and the fault reaction time interval) |
| Rationale: | Safety mechanisms that contribute to the system achieving or maintaining the safe state of the item |
| Operating Mode:  *(in case of categories “General”, “Metric”, “Non-E/E Requirement”, or “User Information”: if applicable)* | Ignition On,  Accessory On |
| Safe State:  *(in case of categories “General”, “Metric”, “Non-E/E Requirement”, or “User Information”: if applicable)* | Steering Column Tilt Adjustment Request (StewPosAdjTlt\_D\_Rq = Idle) is sent on HS3-CAN Bus |
| Reduced Functionality Tolerance Time Interval:  *(if applicable;*  *in case of categories “Metric”, “Non-E/E Requirement”, “Maintain Safe State / Recovery” or “User Information”: not applicable;*  *in case of category “Reduced Functionality”: required)* | N/A |
| Fault Handling Time Segment:  *(in case of categories “Metric” or “Maintain Safe State / Recovery”: not applicable;*  *in case of category “General”, “Reduced Functionality”, “Non-E/E Requirement”, or “User Information”: if applicable)* | 500ms |
| Requirement Status | Approved |
| V&V method: | Test |
| V&V acceptance criteria:  *(UNV1 / UPV1, not in case of category “Non-E/E requirement)* | System testing: PIM\_CDC sends steering column tilt adjustment request as idle (StewPosAdjTlt\_D\_Rq = Idle) on HS3-CAN if any of following condition is true:   * a safety critical fault is detected in the APIM\_CDC itself * contextual control state is not equal to steering column adjust controls |
| Allocated Element(s)/Component(s)/ System(s) *(if applicable)* | APIM\_CDC |

Table 19: Element/Component/System Technical Safety Requirements SCPC-T-S-Req01.9.1

| T-S-Req-ID: | SCPC-T-S-Req01.9.2 |
| --- | --- |
| External Reference *(optional)* |  |
| Category: | Maintain Safe State/Recovery |
| Version  *(only in case of category “Non-E/E requirement”)* |  |
| Author  *(only in case of category “Non-E/E requirement”)* |  |
| Safety Goal ID: | SG01: Prevent impaired access to the steering controls |
| F-S-Req ID: | SCPC-F-S-Req01.9 Inhibit steering column tilt position adjustment  SCPC-F-S-Req01.11 (Enable steering column tilt position adjustment |
| ASIL Classification:  *(in case of category “General”: if applicable, in case of category “Non-E/E Requirement”: not applicable)* | ASIL B |
| Technical Safety Requirement Title: | DSM Inhibits Motor Power for Manual Steering Column Tilt Movement |
| Technical Safety Requirement Text: | The DSM shall switch OFF the power supply to steering column tilt motor for manual steering column tilt movement if any of following condition is true:  - steering column tilt adjustment request (StewPosAdjTlt\_D\_Rq = Idle)  OR  - steering column tilt adjustment request signal integrity (Cs, Cnt, and Periodicity) is NOT GOOD  OR  - Safety critical fault is detected in the DSM itselft  DSM shall maintain the safe state until correct operation of failed DSM hardware and software resources and steering column tilt position request are sufficiently validated  NOTE: DSM Fault handling time interval (FHTI) = 500ms  (sum of fault detection time interval and the fault reaction time interval |
| Rationale: | Safety mechanisms that contribute to the system achieving or maintaining the safe state of the item |
| Operating Mode:  *(in case of categories “General”, “Metric”, “Non-E/E Requirement”, or “User Information”: if applicable)* | Ignition On,  Accessory On |
| Safe State:  *(in case of categories “General”, “Metric”, “Non-E/E Requirement”, or “User Information”: if applicable)* | Motor Power is Turned Off for Manual Steering Column Tilt Movement |
| Reduced Functionality Tolerance Time Interval:  *(if applicable;*  *in case of categories “Metric”, “Non-E/E Requirement”, “Maintain Safe State / Recovery” or “User Information”: not applicable;*  *in case of category “Reduced Functionality”: required)* | N/A |
| Fault Handling Time Segment:  *(in case of categories “Metric” or “Maintain Safe State / Recovery”: not applicable;*  *in case of category “General”, “Reduced Functionality”, “Non-E/E Requirement”, or “User Information”: if applicable)* | 500ms |
| Requirement Status | Approved |
| V&V method: | Test |
| V&V acceptance criteria:  *(UNV1 / UPV1, not in case of category “Non-E/E requirement)* | System testing: DSM turns off power supply to steering column tilt motor for manual steering column tilt movement if any of following condition is true:  - steering column tilt adjustment request is Idle (StewPosAdjTlt\_D\_Rq = Idle  - steering column tilt adjustment request signal integrity (Cs, Cnt, and Periodicity) is NOT GOOD  - Safety critical fault is detected in the DSM hardware and software resources |
| Allocated Element(s)/Component(s)/ System(s) *(if applicable)* | DSM |

Table 20: Element/Component/System Technical Safety Requirements SCPC-T-S-Req01.9.2

### Requirement Derivation for SCPC-F-S-Req01.10 (Inhibit steering column telescopic position adjustment)

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

*Derive Technical Safety Requirements from Functional Safety Requirements.*

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

Figure 2 - Technical Safety Requirements Derivation Diagram for SCPC-F-S-Req01.10

#### Technical Safety Requirements

| T-S-Req-ID: | SCPC-T-S-Req01.10.1 |
| --- | --- |
| External Reference *(optional)* |  |
| Category: | Maintain Safe State/Recovery |
| Version  *(only in case of category “Non-E/E requirement”)* |  |
| Author  *(only in case of category “Non-E/E requirement”)* |  |
| Safety Goal ID: | SG01: Prevent impaired access to the steering controls |
| F-S-Req ID: | SCPC-F-S-Req01.10 Inhibit steering column telescopic position adjustment  SCPC-F-S-Req01.12 Enable steering column telescopic position adjustment |
| ASIL Classification:  *(in case of category “General”: if applicable, in case of category “Non-E/E Requirement”: not applicable)* | ASIL B |
| Technical Safety Requirement Title: | APIM\_CDC Sends Steering Column Telescopic Position Adjustment Request as IDLE |
| Technical Safety Requirement Text: | The APIM\_CDC shall send steering column telescopic position adjustment request as idle (StewPosAdjTel\_D\_Rq = Idle) on HS3-CAN if any of following condition is true:   * contextual control state is not equal to steering column adjust controls * a safety critical fault is detected in the APIM\_CDC itself   APIM\_CDC shall maintain the safe state until correct operation of failed APIM\_CDC resources and contextual control state for steering column adjust controls are sufficiently validated  NOTE: APIM\_CDC Fault handling time interval (FHTI) = 500ms  (sum of fault detection time interval and the fault reaction time interval) |
| Rationale: | Safety mechanisms that contribute to the system achieving or maintaining the safe state of the item |
| Operating Mode:  *(in case of categories “General”, “Metric”, “Non-E/E Requirement”, or “User Information”: if applicable)* | Ignition On,  Accessory On |
| Safe State:  *(in case of categories “General”, “Metric”, “Non-E/E Requirement”, or “User Information”: if applicable)* | Steering Column Telescopic Adjustment Request (StewPosAdjTel\_D\_Rq = Idle) is sent on HS3-CAN Bus |
| Reduced Functionality Tolerance Time Interval:  *(if applicable;*  *in case of categories “Metric”, “Non-E/E Requirement”, “Maintain Safe State / Recovery” or “User Information”: not applicable;*  *in case of category “Reduced Functionality”: required)* | N/A |
| Fault Handling Time Segment:  *(in case of categories “Metric” or “Maintain Safe State / Recovery”: not applicable;*  *in case of category “General”, “Reduced Functionality”, “Non-E/E Requirement”, or “User Information”: if applicable)* | 500ms |
| Requirement Status | Approved |
| V&V method: | Test |
| V&V acceptance criteria:  *(UNV1 / UPV1, not in case of category “Non-E/E requirement)* | System testing: APIM\_CDC sends steering column telescopic adjustment request as idle (StewPosAdjTel\_D\_Rq = Idle) over HS3-CAN if any of following condition is true:   * a safety critical fault is detected in the APIM\_CDC hardware and software resources * contextual control state is not equal to steering column adjust controls |
| Allocated Element(s)/Component(s)/ System(s) *(if applicable)* | APIM\_CDC |

Table 19: Element/Component/System Technical Safety Requirements SCPC-T-S-Req01.10.1

| T-S-Req-ID: | SCPC-T-S-Req01.10.2 |
| --- | --- |
| External Reference *(optional)* |  |
| Category: | Maintain Safe State/Recovery |
| Version  *(only in case of category “Non-E/E requirement”)* |  |
| Author  *(only in case of category “Non-E/E requirement”)* |  |
| Safety Goal ID: | SG01: Prevent impaired access to the steering controls |
| F-S-Req ID: | SCPC-F-S-Req01.10 Inhibit steering column tele position adjustment  SCPC-F-S-Req01.12 (Enable steering column telescopic position adjustment) |
| ASIL Classification:  *(in case of category “General”: if applicable, in case of category “Non-E/E Requirement”: not applicable)* | ASIL B |
| Technical Safety Requirement Title: | DSM Inhibits Motor Power for Manual Steering Column Telescopic Movement |
| Technical Safety Requirement Text: | The DSM shall switch OFF the power supply to steering column tele motor for manual steering column tele movement if any of following condition is true:  - steering column telescopic adjustment request is Idle (StewPosAdjTel\_D\_Rq = Idle)  OR  - steering column telescopic adjustment request signal integrity (Cs, Cnt, and Periodicity) is NOT GOOD  OR  - Safety critical fault is detected in the DSM hardware and software resources  DSM shall maintain the safe state until correct operation of failed DSM hardware and software resources and steering column tele position adjustment request are sufficiently validated  NOTE: DSM Fault handling time interval (FHTI) = 500ms  (sum of fault detection time interval and the fault reaction time interval) |
| Rationale: | Safety mechanisms that contribute to the system achieving or maintaining the safe state of the item. |
| Operating Mode:  *(in case of categories “General”, “Metric”, “Non-E/E Requirement”, or “User Information”: if applicable)* | Ignition On,  Accessory On |
| Safe State:  *(in case of categories “General”, “Metric”, “Non-E/E Requirement”, or “User Information”: if applicable)* | Motor Power is Turned Off for Manual Steering Column Telescopic Movement |
| Reduced Functionality Tolerance Time Interval:  *(if applicable;*  *in case of categories “Metric”, “Non-E/E Requirement”, “Maintain Safe State / Recovery” or “User Information”: not applicable;*  *in case of category “Reduced Functionality”: required)* | N/A |
| Fault Handling Time Segment:  *(in case of categories “Metric” or “Maintain Safe State / Recovery”: not applicable;*  *in case of category “General”, “Reduced Functionality”, “Non-E/E Requirement”, or “User Information”: if applicable)* | 500ms |
| Requirement Status | Approved |
| V&V method: | Test |
| V&V acceptance criteria:  *(UNV1 / UPV1, not in case of category “Non-E/E requirement)* | System testing: DSM turns off power supply to steering column tele motor for manual steering column tilt movement if any of following condition is true:  - steering column tele adjustment request is Idle (StewPosAdjTel\_D\_Rq = Idle)  - steering column tele adjustment request signal integrity (Cs, Cnt, and Periodicity) is NOT GOOD  - Safety critical fault is detected in the DSM hardware and software resources |
| Allocated Element(s)/Component(s)/ System(s) *(if applicable)* | DSM |

Table 20: Element/Component/System Technical Safety Requirements SCPC-T-S-Req01.10.2

### Requirement Derivation for SCPC-F-S-Req02.1 (Contextual Control State Determination for Pedal Adjust Controls)

| T-S-Req-ID: | SCPC-T-S-Req02.1.1 |
| --- | --- |
| External Reference *(optional)* |  |
| Category: | Safety Related Function |
| Version  *(only in case of category “Non-E/E requirement”)* |  |
| Author  *(only in case of category “Non-E/E requirement”)* |  |
| Safety Goal ID: | SG02: Prevent impaired access to the pedal controls |
| F-S-Req ID: | SCPC-F-S-Req02.1: Contextual Control State Determination for Pedal Adjust Controls |
| ASIL Classification:  *(in case of category “General”: if applicable, in case of category “Non-E/E Requirement”: not applicable)* | ASIL B |
| Technical Safety Requirement Title: | APIM\_CDC Determines Contextual Control State for Pedal Adjust Controls |
| Technical Safety Requirement Text: | The APIM\_CDC shall determine contextual control state for pedal adjust controls when right hand steering wheel switch position (StewSwtchScndPos\_D\_St) and right-hand steering wheel switch status (StewSwtchScnd\_D\_Stat) signals are received on HS3-CAN Bus according to the contextual control flows described in the SW-HMI specification (SW\_HMI\_Spec\_2.1 06-30-21.pdf) |
| Rationale: | The right-hand steering wheel switch position and switch status are needed according to the SW-HMI specification to allow APIM\_CDC to set the contextual control state for pedal adjust controls.  Any single-point fault in SIMA or SCCM would not initiate right hand steering wheel switch information (switch position and switch status) that can activate pedal adjust controls in APIM\_CDC (e.g., Open Default Controls🡪 Open Driver Adjustments Controls-> Open Pedal Adjust Controls). |
| Operating Mode:  *(in case of categories “General”, “Metric”, “Non-E/E Requirement”, or “User Information”: if applicable)* | Ignition On,  Accessory On |
| Safe State:  *(in case of categories “General”, “Metric”, “Non-E/E Requirement”, or “User Information”: if applicable)* | Contextual control state is not set for pedal adjust controls |
| Reduced Functionality Tolerance Time Interval:  *(if applicable;*  *in case of categories “Metric”, “Non-E/E Requirement”, “Maintain Safe State / Recovery” or “User Information”: not applicable;*  *in case of category “Reduced Functionality”: required)* | N/A |
| Fault Handling Time Segment:  *(in case of categories “Metric” or “Maintain Safe State / Recovery”: not applicable;*  *in case of category “General”, “Reduced Functionality”, “Non-E/E Requirement”, or “User Information”: if applicable)* | 500ms |
| Requirement Status | Approved |
| V&V method: | Test  Analysis |
| V&V acceptance criteria:  *(UNV1 / UPV1, not in case of category “Non-E/E requirement)* | System testing: APIM\_CDC sets the contextual control state for pedal adjust controls when right hand steering wheel switch position (StewSwtchScndPos\_D\_St) and right-hand steering wheel switch status (StewSwtchScnd\_D\_Stat) information are received on HS3-CAN Bus according to the contextual control flows described in the SW-HMI specification ((SW\_HMI\_Spec\_2.1 06-30-21.pdf) |
| Allocated Element(s)/Component(s)/ System(s) *(if applicable)* | APIM\_CDC |

Table 27: Element/Component/System Technical Safety Requirements SCPC-T-S-Req02.1.1

### Requirement Derivation for SCPC-F-S-Req02.2 (Provide Pedal Telescopic Position Adjustment Request)

| T-S-Req-ID: | SCPC-T-S-Req02.2.1 |
| --- | --- |
| External Reference *(optional)* |  |
| Category: | Safety Related Function |
| Version  *(only in case of category “Non-E/E requirement”)* |  |
| Author  *(only in case of category “Non-E/E requirement”)* |  |
| Safety Goal ID: | SG02: Prevent impaired access to the pedal controls |
| F-S-Req ID: | SCPC-F-S-Req02.2: Provide Pedal Telescopic Position Adjustment Request |
| ASIL Classification:  *(in case of category “General”: if applicable, in case of category “Non-E/E Requirement”: not applicable)* | ASIL B |
| Technical Safety Requirement Title: | APIM\_CDC Provide Pedal Telescopic Position Adjustment Request |
| Technical Safety Requirement Text: | The APIM\_CDC shall provide following pedal tele position adjustment request (PdlAdj\_D\_Rq) on HS3-CAN bus when the Contextual Control State is set for pedal adjust controls.  - PdlAdj\_D\_Rq = Tel IN if right hand steering wheel switch position (StewSwtchScndPos\_D\_St = Tel IN) and right-hand steering wheel switch status (StewSwtchScnd\_D\_Stat = Pressed)  - PdlAdj\_D\_Rq = Tel OUT if right hand steering wheel switch position (StewSwtchScndPos\_D\_St = Tel OUT) and right-hand steering wheel switch status (StewSwtchScnd\_D\_Stat = Pressed)  In case of Contextual Control State is not equal to pedal adjust controls, APIM\_CDC shall initiate transition to a safe state within fault handling time interval.  NOTE: APIM\_CDC Fault handling time interval (FHTI) = 500ms  (sum of fault detection time interval and the fault reaction time interval) |
| Rationale: | To ensure safe execution of control algorithm (controller’s decision-making process that determines the pedal tel position adjustment request (Tel IN / Tel OUT) |
| Operating Mode:  *(in case of categories “General”, “Metric”, “Non-E/E Requirement”, or “User Information”: if applicable)* | Ignition On,  Accessory On |
| Safe State:  *(in case of categories “General”, “Metric”, “Non-E/E Requirement”, or “User Information”: if applicable)* | Pedal telescopic position adjustment request (PdlAdj\_D\_Rq = Idle) is sent on HS3-CAN |
| Reduced Functionality Tolerance Time Interval:  *(if applicable;*  *in case of categories “Metric”, “Non-E/E Requirement”, “Maintain Safe State / Recovery” or “User Information”: not applicable;*  *in case of category “Reduced Functionality”: required)* | N/A |
| Fault Handling Time Segment:  *(in case of categories “Metric” or “Maintain Safe State / Recovery”: not applicable;*  *in case of category “General”, “Reduced Functionality”, “Non-E/E Requirement”, or “User Information”: if applicable)* | 500ms |
| Requirement Status | Approved |
| V&V method: | Test  Analysis |
| V&V acceptance criteria:  *(UNV1 / UPV1, not in case of category “Non-E/E requirement)* | System testing: APIM\_CDC provides pedal tele position adjustment request (PdlAdj\_D\_Rq = Tel IN or Tel OUT) on HS3-CAN bus when the Contextual Control State is set for pedal adjust controls. |
| Allocated Element(s)/Component(s)/ System(s) *(if applicable)* | APIM\_CDC |

Table 28: Element/Component/System Technical Safety Requirements SCPC-T-S-Req02.2.1

| T-S-Req-ID: | SCPC-T-S-Req02.2.2 |
| --- | --- |
| External Reference *(optional)* |  |
| Category: | Safety Related Function |
| Version  *(only in case of category “Non-E/E requirement”)* |  |
| Author  *(only in case of category “Non-E/E requirement”)* |  |
| Safety Goal ID: | SG02: Prevent impaired access to the pedal controls |
| F-S-Req ID: | SCPC-F-S-Req02.2: Provide Pedal Telescopic Position Adjustment Request |
| ASIL Classification:  *(in case of category “General”: if applicable, in case of category “Non-E/E Requirement”: not applicable)* | ASIL B |
| Technical Safety Requirement Title: | Pedal Telescopic Position Adjustment Request End to End Protection |
| Technical Safety Requirement Text: | The APIM\_CDC shall send pedal telescopic position adjustment request (PdlAdj\_D\_Rq) on HS3-CAN Bus with checksum (PdlAdj\_D\_Rq\_ \_No\_Cs) and counter (PdlAdj\_D\_Rq\_ \_No\_Cnt).  NOTE: APIM\_CDC should follow AUTOSAR PROFILE 1A for Checksum and Counter. |
| Rationale: | ASIL rated signals must be end-to-end protected to ensure signal integrity between the transmitter and receiver |
| Operating Mode:  *(in case of categories “General”, “Metric”, “Non-E/E Requirement”, or “User Information”: if applicable)* | Ignition On,  Accessory On |
| Safe State:  *(in case of categories “General”, “Metric”, “Non-E/E Requirement”, or “User Information”: if applicable)* | Pedal telescopic position adjustment request (PdlAdj\_D\_Rq = Idle) is sent to the DSM |
| Reduced Functionality Tolerance Time Interval:  *(if applicable;*  *in case of categories “Metric”, “Non-E/E Requirement”, “Maintain Safe State / Recovery” or “User Information”: not applicable;*  *in case of category “Reduced Functionality”: required)* | N/A |
| Fault Handling Time Segment:  *(in case of categories “Metric” or “Maintain Safe State / Recovery”: not applicable;*  *in case of category “General”, “Reduced Functionality”, “Non-E/E Requirement”, or “User Information”: if applicable)* | 500ms |
| Requirement Status | Approved |
| V&V method: | Test  Analysis |
| V&V acceptance criteria:  *(UNV1 / UPV1, not in case of category “Non-E/E requirement)* | System testing: APIM\_CDC transmits pedal telescopic position adjustment signal (PdlAdj\_D\_Rq) on HS3-CAN Bus with correct checksum and counter. |
| Allocated Element(s)/Component(s)/ System(s) *(if applicable)* | APIM\_CDC |

Table 30: Element/Component/System Technical Safety Requirements SCPC-T-S-Req02.2.2

### Requirement Derivation for SCPC-F-S-Req02.3 (Close Pedal Adjust Controls)

| T-S-Req-ID: | SCPC-T-S-Req02.3.1 |
| --- | --- |
| External Reference *(optional)* |  |
| Category: | Safety Related Function |
| Version  *(only in case of category “Non-E/E requirement”)* |  |
| Author  *(only in case of category “Non-E/E requirement”)* |  |
| Safety Goal ID: | SG02: Prevent impaired access to the pedal controls |
| F-S-Req ID: | SCPC-F-S-Req02.3: Close Pedal Adjust Controls |
| ASIL Classification:  *(in case of category “General”: if applicable, in case of category “Non-E/E Requirement”: not applicable)* | ASIL B |
| Technical Safety Requirement Title: | APIM\_CDC Closes Contextual Control for Pedal Adjust Controls |
| Technical Safety Requirement Text: | The APIM\_CDC shall close contextual control state for pedal adjust controls when right hand steering wheel switch status (StewSwtchScnd\_D\_Stat != Pressed) is received on HS3-CAN Bus for 10 seconds  In case of contextual control state is not equal to pedal adjust controls, APIM\_CDC shall initiate transition to a safe state within fault handling time interval.  NOTE: APIM\_CDC Fault handling time interval (FHTI) = 500ms  (sum of fault detection time interval and the fault reaction time interval) |
| Rationale: | Idle Timeout (inactivity timeout) is needed for steering column adjust controls to prevent unintended user input (via right hand steering wheel switch) for steering column adjustment.  Incorrect switch status (stuck at “StewSwtchScnd\_D\_Stat = Pressed”) to APIM\_CDC while using steering column adjust controls could lead to a QM hazard “steering column movement more that intended” (see FFSD02\_HazardAnalysisAndRiskAssessment\_Steering Column Position Control) |
| Operating Mode:  *(in case of categories “General”, “Metric”, “Non-E/E Requirement”, or “User Information”: if applicable)* | Ignition On,  Accessory On |
| Safe State:  *(in case of categories “General”, “Metric”, “Non-E/E Requirement”, or “User Information”: if applicable)* | Pedals telescopic position adjustment request signal (PdlAdj\_D\_Rq = Idle) are sent on HS3-CAN |
| Reduced Functionality Tolerance Time Interval:  *(if applicable;*  *in case of categories “Metric”, “Non-E/E Requirement”, “Maintain Safe State / Recovery” or “User Information”: not applicable;*  *in case of category “Reduced Functionality”: required)* | N/A |
| Fault Handling Time Segment:  *(in case of categories “Metric” or “Maintain Safe State / Recovery”: not applicable;*  *in case of category “General”, “Reduced Functionality”, “Non-E/E Requirement”, or “User Information”: if applicable)* | 500ms |
| Requirement Status | Approved |
| V&V method: | Test  Analysis |
| V&V acceptance criteria:  *(UNV1 / UPV1, not in case of category “Non-E/E requirement)* | System testing: Verify that the APIM\_CDC closes contextual control state for pedal adjust controls when release Touch is received from right hand steering wheel switch (StewSwtchScnd\_D\_Stat != Pressed) on HS3-CAN Bus for 10 seconds |
| Allocated Element(s)/Component(s)/ System(s) *(if applicable)* | APIM\_CDC |

Table 31: Element/Component/System Technical Safety Requirements SCPC-T-S-Req02.3.1

### Requirement Derivation for SCPC-F-S-Req02.4 (Provide Pedal Telescopic Position Command)

| T-S-Req-ID: | SCPC-T-S-Req02.4.1 |
| --- | --- |
| External Reference *(optional)* |  |
| Category: | Safety Related Function |
| Version  *(only in case of category “Non-E/E requirement”)* |  |
| Author  *(only in case of category “Non-E/E requirement”)* |  |
| Safety Goal ID: | SG02: Prevent impaired access to the pedal controls |
| F-S-Req ID: | SCPC-F-S-Req02.4: Provide Pedal Telescopic Position Command |
| ASIL Classification:  *(in case of category “General”: if applicable, in case of category “Non-E/E Requirement”: not applicable)* | ASIL B |
| Technical Safety Requirement Title: | DSM Provides Motor Power for Manual pedal Telescopic Movement |
| Technical Safety Requirement Text: | The DSM shall provide system voltage (~12V) to the pedal telescopic motor for manual pedal movement (PDL\_POS\_ADJ\_RNG, PDL\_POS\_ADJ\_SPEED) only when pedal tele position adjustment request (PdlAdj\_D\_Rq= Tel IN or Tel OUT) is received on FD3-CAN Bus.  In case of pedal tele position adjustment request (PdlAdj\_D\_Rq= Idle), DSM shall initiate transition to a safe state within fault handling time interval  NOTE: DSM Fault handling time interval (FHTI) = 500ms  (sum of fault detection time interval and the fault reaction time interval) |
| Rationale: | To ensure safe execution of control algorithm (controller’s decision-making process that determines the motor power for manual pedal tele movement) |
| Operating Mode:  *(in case of categories “General”, “Metric”, “Non-E/E Requirement”, or “User Information”: if applicable)* | Ignition On,  Accessory On |
| Safe State:  *(in case of categories “General”, “Metric”, “Non-E/E Requirement”, or “User Information”: if applicable)* | Motor Power is Turned Off for Manual Pedal Movement |
| Reduced Functionality Tolerance Time Interval:  *(if applicable;*  *in case of categories “Metric”, “Non-E/E Requirement”, “Maintain Safe State / Recovery” or “User Information”: not applicable;*  *in case of category “Reduced Functionality”: required)* | N/A |
| Fault Handling Time Segment:  *(in case of categories “Metric” or “Maintain Safe State / Recovery”: not applicable;*  *in case of category “General”, “Reduced Functionality”, “Non-E/E Requirement”, or “User Information”: if applicable)* | 500ms |
| Requirement Status | Approved |
| V&V method: | Test  Analysis |
| V&V acceptance criteria:  *(UNV1 / UPV1, not in case of category “Non-E/E requirement)* | System testing: DSM provides system voltage (~12V) to the pedal tele motor for manual pedal tele movement when pedal tele position adjustment request (PdlAdj\_D\_Rq = Tel IN or Tel OUT) is received on FD3-CAN Bus |
| Allocated Element(s)/Component(s)/ System(s) *(if applicable)* | DSM |

Table 32: Element/Component/System Technical Safety Requirements SCPC-T-S-Req02.4.1

| T-S-Req-ID: | SCPC-T-S-Req02.4.2 |
| --- | --- |
| External Reference *(optional)* |  |
| Category: | Safety Related Function |
| Version  *(only in case of category “Non-E/E requirement”)* |  |
| Author  *(only in case of category “Non-E/E requirement”)* |  |
| Safety Goal ID: | SG02: Prevent impaired access to the pedal controls |
| F-S-Req ID: | SCPC-F-S-Req02.4: Provide Pedal Telescopic Position Command |
| ASIL Classification:  *(in case of category “General”: if applicable, in case of category “Non-E/E Requirement”: not applicable)* | ASIL B |
| Technical Safety Requirement Title: | DSM Verifies Manual Pedal Adjustment Request Checksum and Counter |
| Technical Safety Requirement Text: | The DSM shall verify the checksum (PdlAdj\_D\_Rq \_No\_Cs), counter (PdlAdj\_D\_Rq \_No\_Cnt) and timeout of received pedal tele position adjustment request on FD3-CAN Bus according to the specified E2E protection (AUTOSAR PROFILE 1A for Checksum and Counter).  If the checksum (PdlAdj\_D\_Rq \_No\_Cs) or counter (PdlAdj\_D\_Rq \_No\_Cnt)) or timeout of received pedal tele position adjustment request fails, DSM shall set an internal software flag to "INVALID" and transition to a safe state within fault handling time interval.  NOTE: DSM Fault handling time interval (FHTI) = 500ms  (sum of fault detection time interval and the fault reaction time interval) |
| Rationale: | ASIL rated signals must be end-to-end protected to ensure signal integrity between the transmitter and receiver |
| Operating Mode:  *(in case of categories “General”, “Metric”, “Non-E/E Requirement”, or “User Information”: if applicable)* | Ignition On,  Accessory On |
| Safe State:  *(in case of categories “General”, “Metric”, “Non-E/E Requirement”, or “User Information”: if applicable)* | Motor Power is Turned Off for Manual Pedal Movement |
| Reduced Functionality Tolerance Time Interval:  *(if applicable;*  *in case of categories “Metric”, “Non-E/E Requirement”, “Maintain Safe State / Recovery” or “User Information”: not applicable;*  *in case of category “Reduced Functionality”: required)* | N/A |
| Fault Handling Time Segment:  *(in case of categories “Metric” or “Maintain Safe State / Recovery”: not applicable;*  *in case of category “General”, “Reduced Functionality”, “Non-E/E Requirement”, or “User Information”: if applicable)* | 500ms |
| Requirement Status | Approved |
| V&V method: | Test |
| V&V acceptance criteria:  *(UNV1 / UPV1, not in case of category “Non-E/E requirement)* | System testing: Manipulate checksum or counter of input signal. DSM must set correct replacement value during fault confirmation time. DSM must flag signal as invalid internally, after confirmation time is exceeded.  Start with sending signal in specified periodicity. Stop sending signal (simulate missed message). DSM must set correct replacement value during fault confirmation time. DSM must flag signal as invalid internally, after confirmation time is exceeded. |
| Allocated Element(s)/Component(s)/ System(s) *(if applicable)* | DSM |

Table 33: Element/Component/System Technical Safety Requirements SCPC-T-S-Req02.4.2

### Requirement Derivation for SCPC-F-S-Req02.5 (Actuate Commanded Pedal Telescopic Position)

| T-S-Req-ID: | SCPC-T-S-Req02.5.1 |
| --- | --- |
| External Reference *(optional)* |  |
| Category: | Internal Fault Handling |
| Version  *(only in case of category “Non-E/E requirement”)* |  |
| Author  *(only in case of category “Non-E/E requirement”)* |  |
| Safety Goal ID: | SG02: Prevent impaired access to the pedal controls |
| F-S-Req ID: | SCPC-F-S-Req02.5: Actuate Commanded Pedal Position |
| ASIL Classification:  *(in case of category “General”: if applicable, in case of category “Non-E/E Requirement”: not applicable)* | ASIL B |
| Technical Safety Requirement Title: | APIM\_CDC Monitors Single-Point Faults Regarding Pedal Telescopic Position Adjustment |
| Technical Safety Requirement Text: | The APIM\_CDC shall monitor the single-point faults in the APIM\_CDC hardware and software resources that responsible for pedal telescopic position adjustment.  In case of any detected fault, the internal APIM\_CDC Failure flag shall be set to "INVALID" and transition to a safe state within fault handling time interval.  APIM\_CDC self-monitoring can include following checks (as applicable) to detect random hardware faults and, if appropriate, to detect systematic faults of APIM\_CDC :  - Program Sequence Checks  - RAM/ROM Checks  - Software Logic Checks  - Other Checks (If applicable) |
| Rationale: | To ensure the reliable execution of APIM\_CDC. |
| Operating Mode:  *(in case of categories “General”, “Metric”, “Non-E/E Requirement”, or “User Information”: if applicable)* | Ignition On,  Accessory On |
| Safe State:  *(in case of categories “General”, “Metric”, “Non-E/E Requirement”, or “User Information”: if applicable)* | Pedal Tele Adjustment Request (PdlAdj\_D\_Rq = Idle) is sent on HS3-CAN Bus |
| Reduced Functionality Tolerance Time Interval:  *(if applicable;*  *in case of categories “Metric”, “Non-E/E Requirement”, “Maintain Safe State / Recovery” or “User Information”: not applicable;*  *in case of category “Reduced Functionality”: required)* | N/A |
| Fault Handling Time Segment:  *(in case of categories “Metric” or “Maintain Safe State / Recovery”: not applicable;*  *in case of category “General”, “Reduced Functionality”, “Non-E/E Requirement”, or “User Information”: if applicable)* | 500ms |
| Requirement Status | Approved |
| V&V method: | Test |
| V&V acceptance criteria:  *(UNV1 / UPV1, not in case of category “Non-E/E requirement)* | Fault Injection Testing. APIM\_CDC detects all single-point faults in APIM\_CDC itself and sets the internal APIM\_CDC failure SW flag to "INVALID". |
| Allocated Element(s)/Component(s)/ System(s) *(if applicable)* | APIM\_CDC |

Table 34: Element/Component/System Technical Safety Requirements SCPC-T-S-Req02.5.1

| T-S-Req-ID: | SCPC-T-S-Req02.5.2 |
| --- | --- |
| External Reference *(optional)* |  |
| Category: | Internal Fault Handling |
| Version  *(only in case of category “Non-E/E requirement”)* |  |
| Author  *(only in case of category “Non-E/E requirement”)* |  |
| Safety Goal ID: | SG02: Prevent impaired access to the pedal controls |
| F-S-Req ID: | SCPC-F-S-Req02.5: Actuate Commanded Pedal Telescopic Position |
| ASIL Classification:  *(in case of category “General”: if applicable, in case of category “Non-E/E Requirement”: not applicable)* | ASIL B |
| Technical Safety Requirement Title: | DSM Monitors Single-Point Faults Regarding Manual Pedal Movement |
| Technical Safety Requirement Text: | The DSM shall monitor the single-point faults in the DSM hardware and software resources that responsible for pedal telescopic movement.  In case of any detected fault, the internal DSM Failure flag shall be set to "INVALID" and transition to a safe state within fault handling time interval.  DSM self-monitoring can include following checks (as applicable) to detect random hardware faults and, if appropriate, to detect systematic faults of DSM :  - Program Sequence Checks  - RAM/ROM Checks  - Software Logic Checks  - Output "Motor signals" Checks  - H-bridge and Wiring Harness Checks  - Other Checks (If applicable) |
| Rationale: | To ensure the reliable execution of DSM. |
| Operating Mode:  *(in case of categories “General”, “Metric”, “Non-E/E Requirement”, or “User Information”: if applicable)* | Ignition On,  Accessory On |
| Safe State:  *(in case of categories “General”, “Metric”, “Non-E/E Requirement”, or “User Information”: if applicable)* | Motor Power is Turned Off for Manual Pedal Movement |
| Reduced Functionality Tolerance Time Interval:  *(if applicable;*  *in case of categories “Metric”, “Non-E/E Requirement”, “Maintain Safe State / Recovery” or “User Information”: not applicable;*  *in case of category “Reduced Functionality”: required)* | N/A |
| Fault Handling Time Segment:  *(in case of categories “Metric” or “Maintain Safe State / Recovery”: not applicable;*  *in case of category “General”, “Reduced Functionality”, “Non-E/E Requirement”, or “User Information”: if applicable)* | 500ms |
| Requirement Status | Approved |
| V&V method: | Test |
| V&V acceptance criteria:  *(UNV1 / UPV1, not in case of category “Non-E/E requirement)* | Fault Injection Testing. DSM detects all single-point faults in the DSM itself and sets the internal DSM failure SW flag to "INVALID". |
| Allocated Element(s)/Component(s)/ System(s) *(if applicable)* | DSM |

Table 35: Element/Component/System Technical Safety Requirements SCPC-T-S-Req02.5.2

| T-S-Req-ID: | SCPC-T-S-Req02.5.3 |
| --- | --- |
| External Reference *(optional)* |  |
| Category: | Latent Fault Handling |
| Version  *(only in case of category “Non-E/E requirement”)* |  |
| Author  *(only in case of category “Non-E/E requirement”)* |  |
| Safety Goal ID: | SG02: Prevent impaired access to the pedal controls |
| F-S-Req ID: | SCPC-F-S-Req02.5: Actuate Commanded Pedal Telescopic Position |
| ASIL Classification:  *(in case of category “General”: if applicable, in case of category “Non-E/E Requirement”: not applicable)* | ASIL A |
| Technical Safety Requirement Title: | APIM\_CDC Monitors Latent Faults Regarding Pedal Position Adjustment |
| Technical Safety Requirement Text: | The APIM\_CDC shall monitor the latent faults in the APIM\_CDC hardware and software resources that can enable unintended pedal telescopic position adjustment.  In case of any detected latent fault, the internal APIM\_CDC Failure flag shall be set to "INVALID" and transition to a safe state within fault handling time interval (TBD).  APIM\_CDC self-monitoring can include following checks (as applicable) to detect random hardware faults and, if appropriate, to detect systematic faults:  - Power-up self-checks for APIM\_CDC hardware resources  - Other Checks (If applicable) |
| Rationale: | To avoid multiple-point faults that have the potential to be latent (e.g., fault in the safety mechanism that detect/mitigate single-point fault)  The development of safety mechanisms that are implemented only to prevent dual point faults from being latent shall at least comply with ASIL A for technical safety requirements assigned ASIL B (ISO 26262-4, 6.4.2.5) |
| Operating Mode:  *(in case of categories “General”, “Metric”, “Non-E/E Requirement”, or “User Information”: if applicable)* | Ignition On,  Accessory On |
| Safe State:  *(in case of categories “General”, “Metric”, “Non-E/E Requirement”, or “User Information”: if applicable)* | Pedal Tele Adjustment Request (PdlAdj\_D\_Rq = Idle) is sent on HS3-CAN Bus |
| Reduced Functionality Tolerance Time Interval:  *(if applicable;*  *in case of categories “Metric”, “Non-E/E Requirement”, “Maintain Safe State / Recovery” or “User Information”: not applicable;*  *in case of category “Reduced Functionality”: required)* | N/A |
| Fault Handling Time Segment:  *(in case of categories “Metric” or “Maintain Safe State / Recovery”: not applicable;*  *in case of category “General”, “Reduced Functionality”, “Non-E/E Requirement”, or “User Information”: if applicable)* | 500ms |
| Requirement Status | Approved |
| V&V method: | Test |
| V&V acceptance criteria:  *(UNV1 / UPV1, not in case of category “Non-E/E requirement)* | Fault Injection Testing. APIM\_CDC detects latent faults and sets the internal APIM\_CDC failure SW flag to "INVALID". |
| Allocated Element(s)/Component(s)/ System(s) *(if applicable)* | APIM\_CDC |

Table 36: Element/Component/System Technical Safety Requirements SCPC-T-S-Req02.5.3

| T-S-Req-ID: | SCPC-T-S-Req02.5.4 |
| --- | --- |
| External Reference *(optional)* |  |
| Category: | Latent Fault Handling |
| Version  *(only in case of category “Non-E/E requirement”)* |  |
| Author  *(only in case of category “Non-E/E requirement”)* |  |
| Safety Goal ID: | SG02: Prevent impaired access to the pedal controls |
| F-S-Req ID: | SCPC-F-S-Req02.5: Actuate Commanded Pedal Telescopic Position |
| ASIL Classification:  *(in case of category “General”: if applicable, in case of category “Non-E/E Requirement”: not applicable)* | ASIL B |
| Technical Safety Requirement Title: | DSM Monitors Latent Faults Regarding Manual Pedal Movement |
| Technical Safety Requirement Text: | The DSM shall monitor the latent faults in the DSM hardware and software resources that can enable unintended pedal tele movement.  In case of any detected latent fault, the internal DSM Failure flag shall be set to "INVALID" and transition to a safe state within multiple-point fault handling time interval (TBD).  DSM self-monitoring can include following checks (as applicable) to detect random hardware faults and, if appropriate, to detect systematic faults:  - Power-up self-checks for DSM hardware resources  - Other Checks (If applicable) |
| Rationale: | To avoid multiple-point faults that have the potential to be latent (e.g., fault in the safety mechanism that detect/mitigate single-point fault)  The development of safety mechanisms that are implemented only to prevent dual point faults from being latent shall at least comply with ASIL A for technical safety requirements assigned ASIL B (ISO 26262-4, 6.4.2.5). |
| Operating Mode:  *(in case of categories “General”, “Metric”, “Non-E/E Requirement”, or “User Information”: if applicable)* | Ignition On,  Accessory On |
| Safe State:  *(in case of categories “General”, “Metric”, “Non-E/E Requirement”, or “User Information”: if applicable)* | Motor Power is Turned Off for Manual Pedal Movement |
| Reduced Functionality Tolerance Time Interval:  *(if applicable;*  *in case of categories “Metric”, “Non-E/E Requirement”, “Maintain Safe State / Recovery” or “User Information”: not applicable;*  *in case of category “Reduced Functionality”: required)* | N/A |
| Fault Handling Time Segment:  *(in case of categories “Metric” or “Maintain Safe State / Recovery”: not applicable;*  *in case of category “General”, “Reduced Functionality”, “Non-E/E Requirement”, or “User Information”: if applicable)* | 500ms |
| Requirement Status | Approved |
| V&V method: | Test |
| V&V acceptance criteria:  *(UNV1 / UPV1, not in case of category “Non-E/E requirement)* | Fault Injection Testing. DSM detects latent faults and sets the internal DSM failure SW flag to "INVALID". |
| Allocated Element(s)/Component(s)/ System(s) *(if applicable)* | DSM |

Table 37: Element/Component/System Technical Safety Requirements SCPC-T-S-Req02.5.2

### Requirement Derivation for SCPC-F-S-Req02.6 (Inhibit Pedal Telescopic Position Adjustment) and SCPC-F-S-Req02.7 (Enable Pedal Telescopic Position Adjustment)

| T-S-Req-ID: | SCPC-T-S-Req02.6.1 |
| --- | --- |
| External Reference *(optional)* |  |
| Category: | Maintain Safe state/Recovery |
| Version  *(only in case of category “Non-E/E requirement”)* |  |
| Author  *(only in case of category “Non-E/E requirement”)* |  |
| Safety Goal ID: | SG02: Prevent impaired access to the pedal controls |
| F-S-Req ID: | SCPC-F-S-Req02.6: Actuate Commanded Pedal Telescopic Position  SCPC-F-S-Req02.7 : Enable Pedal Telescopic Position Adjustment |
| ASIL Classification:  *(in case of category “General”: if applicable, in case of category “Non-E/E Requirement”: not applicable)* | ASIL B |
| Technical Safety Requirement Title: | APIM\_CDC Sends pedal Telescopic Position Adjustment Request as IDLE |
| Technical Safety Requirement Text: | The APIM\_CDC shall send pedal telescopic position adjustment request as idle (PdlAdj\_D\_Rq = Idle) on HS3-CAN if any of following condition is true:  - contextual control state is not equal to pedal adjust controls  - a safety critical fault is detected in the APIM\_CDC hardware and software resources  APIM\_CDC shall maintain the safe state until correct operation of failed APIM\_CDC resources and Contextual Control State for pedal adjust controls are sufficiently validated  NOTE: APIM\_CDC Fault handling time interval (FHTI) = 500ms  (sum of fault detection time interval and the fault reaction time interval) |
| Rationale: | Safety mechanisms that contribute to the system achieving or maintaining the safe state of the item |
| Operating Mode:  *(in case of categories “General”, “Metric”, “Non-E/E Requirement”, or “User Information”: if applicable)* | Ignition On,  Accessory On |
| Safe State:  *(in case of categories “General”, “Metric”, “Non-E/E Requirement”, or “User Information”: if applicable)* | Pedal Tel Adjustment Request (PdlAdj\_D\_Rq = Idle) is sent on HS3-CAN Bus |
| Reduced Functionality Tolerance Time Interval:  *(if applicable;*  *in case of categories “Metric”, “Non-E/E Requirement”, “Maintain Safe State / Recovery” or “User Information”: not applicable;*  *in case of category “Reduced Functionality”: required)* | N/A |
| Fault Handling Time Segment:  *(in case of categories “Metric” or “Maintain Safe State / Recovery”: not applicable;*  *in case of category “General”, “Reduced Functionality”, “Non-E/E Requirement”, or “User Information”: if applicable)* | 500ms |
| Requirement Status | Approved |
| V&V method: | Test |
| V&V acceptance criteria:  *(UNV1 / UPV1, not in case of category “Non-E/E requirement)* | System testing: APIM\_CDC sends pedal telescopic adjustment request as idle (PdlAdj\_D\_Rq = Idle) on HS3-CAN if any of following condition is true:  - a safety critical fault is detected in the APIM\_CDC hardware and software resources  - contextual control state is not equal to pedal adjust controls |
| Allocated Element(s)/Component(s)/ System(s) *(if applicable)* | APIM\_CDC |

Table 38: Element/Component/System Technical Safety Requirements SCPC-T-S-Req02.6.1

| T-S-Req-ID: | SCPC-T-S-Req02.6.2 |
| --- | --- |
| External Reference *(optional)* |  |
| Category: | Maintain Safe state/Recovery |
| Version  *(only in case of category “Non-E/E requirement”)* |  |
| Author  *(only in case of category “Non-E/E requirement”)* |  |
| Safety Goal ID: | SG02: Prevent impaired access to the pedal controls |
| F-S-Req ID: | SCPC-F-S-Req02.6: Actuate Commanded Pedal Telescopic Position  SCPC-F-S-Req02.7 : Enable Pedal Telescopic Position Adjustment |
| ASIL Classification:  *(in case of category “General”: if applicable, in case of category “Non-E/E Requirement”: not applicable)* | ASIL B |
| Technical Safety Requirement Title: | DSM Inhibits Motor Power for Manual pedal Movement |
| Technical Safety Requirement Text: | The DSM shall switch OFF the power supply to pedal motor for manual pedal movement if any of following condition is true:  - pedal telescopic adjustment request is Idle (PdlAdj\_D\_Rq = Idle)  OR  - pedal telescopic adjustment request signal integrity (Cs, Cnt, and Periodicity) is NOT GOOD  OR  - Safety critical fault is detected in the DSM hardware and software resources  DSM shall maintain the safe state until correct operation of failed DSM resources and pedal position adjustment request are sufficiently validated  NOTE: DSM Fault handling time interval (FHTI) = 500ms  (sum of fault detection time interval and the fault reaction time interval) |
| Rationale: | To transition the vehicle to a safe operating mode when failures are detected. |
| Operating Mode:  *(in case of categories “General”, “Metric”, “Non-E/E Requirement”, or “User Information”: if applicable)* | Ignition On,  Accessory On |
| Safe State:  *(in case of categories “General”, “Metric”, “Non-E/E Requirement”, or “User Information”: if applicable)* | Motor Power is Turned Off for Manual Pedal Movement |
| Reduced Functionality Tolerance Time Interval:  *(if applicable;*  *in case of categories “Metric”, “Non-E/E Requirement”, “Maintain Safe State / Recovery” or “User Information”: not applicable;*  *in case of category “Reduced Functionality”: required)* | N/A |
| Fault Handling Time Segment:  *(in case of categories “Metric” or “Maintain Safe State / Recovery”: not applicable;*  *in case of category “General”, “Reduced Functionality”, “Non-E/E Requirement”, or “User Information”: if applicable)* | 500ms |
| Requirement Status | Approved |
| V&V method: | Test |
| V&V acceptance criteria:  *(UNV1 / UPV1, not in case of category “Non-E/E requirement)* | System testing: DSM turns off power supply to pedal motor for manual pedal movement if any of following condition is true:  - pedal tele adjustment request is Idle (PdlAdj\_D\_Rq = Idle)  - pedal tele adjustment request signal integrity (Cs, Cnt, and Periodicity) is NOT GOOD  - Safety critical fault is detected in the DSM hardware and software resources |
| Allocated Element(s)/Component(s)/ System(s) *(if applicable)* | DSM |

Table 39: Element/Component/System Technical Safety Requirements SCPC-T-S-Req02.6.2

## Timing Specification

### Fault Tolerant Time Interval (FTTI) Identification

*This section to be left blank.*

#### Safety Goal 02 Prevent impaired access to steering controls

Refer FFSD03\_FunctionalSafetyConcept\_Steering Column Pedal Position Control, Section 2.1.1.2 Functional Safety Requirements

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

##### Malfunctioning Behaviour 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 27: 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 28: 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 29: FTTI Summary

### Fault Handling Time Specification

*This section to be left blank.*

#### Achieving the FHT for SG 02 Prevent impaired access to steering controls

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

Refer Section 3.1 Technical Safety Requirements

##### Malfunctioning Behaviour 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 30: FHT Summary

## Derivation of Reduced Functionality Interval (optional)

*Derive Reduced Functionality Tolerance Interval for Technical Safety Requirements from Functional Safety Requirements.*

None

## Operating Modes Overview (optional)

*Insert the operating modes used in the requirement tables in Section 3.1 into Column 2: If is helpful to relate these operating modes to the operating modes in the Functional Safety Concept [FFSD03] (Column 1). If the operating modes (or detailed ones) are in the System Design or Model provide a reference in Column 3. Insert a description of the operating mode into Column 4.*

| **Operating Mode in the Functional Safety Concept [FFSD03]**  (if applicable) | Operating Mode used in tables in Section 3.1 | **Description** |
| --- | --- | --- |
| Active and Idle | Ignition ON | Steering column tilt/telescopic and pedal position adjustment functionalities are available for users when ignition is ON and no safety critical fault is detected. If Driver is not requesting for adjustment when feature is active that is known as Idle mode. |
| Accessory ON | Steering column tilt/telescopic and pedal position adjustment functionalities are available for users when accessory is ON and no safety critical fault is detected. If Driver is not requesting for adjustment when feature is active that is known as Idle mode. |
| Inactive | Ignition ON | Steering column tilt/telescopic position adjustment functionalities are not available for users when ignition is ON and a safety critical fault is detected |
| Accessory ON | Steering column tilt/telescopic position adjustment functionalities are not available for users when accessory is ON and a safety critical fault is detected |

Table 31: Operating Modes

## HW Metric Requirements - Derivation and Rationale (optional)

Not required for ASIL B SG01 and SG02

## Allocation (optional)

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

| **Element/Component / System Name** | **Inside (I)/ Outside (O) Item Boundary** | **Technical Safety Requirement ID** | **Technical Safety Requirement ASIL** | **Element/Com-ponent/System ASIL** |
| --- | --- | --- | --- | --- |
| APIM\_CDC | I | SCPC-T-S-Req01.1.1 | B | B |
| SCPC-T-S-Req01.2.1 | B |
| SCPC-T-S-Req01.2.2 | B |
| SCPC-T-S-Req01.3.1 | B |
| SCPC-T-S-Req01.3.2 | B |
| SCPC-T-S-Req01.4.1 | B |
| SCPC-T-S-Req01.7.1 | B |
| SCPC-T-S-Req01.7.3 | A |
| SCPC-T-S-Req01.8.1 | B |
| SCPC-T-S-Req01.8.3 | A |
| SCPC-T-S-Req01.9.1 | B |
| SCPC-T-S-Req01.10.1 | B |
| SCPC-T-S-Req02.1.1 | B |
| SCPC-T-S-Req02.2.1 | B |
| SCPC-T-S-Req02.2.2 | B |
| SCPC-T-S-Req02.3.1 | B |
| SCPC-T-S-Req02.5.1 | B |
| SCPC-T-S-Req02.5.3 | A |
| SCPC-T-S-Req02.6.1 | B |
| DSM | I | SCPC-T-S-Req01.5.1 | B | B |
| SCPC-T-S-Req01.5.2 | B |
| SCPC-T-S-Req01.6.1 | B |
| SCPC-T-S-Req01.6.2 | B |
| SCPC-T-S-Req01.7.2 | B |
| SCPC-T-S-Req01.7.4 | A |
| SCPC-T-S-Req01.8.2 | B |
| SCPC-T-S-Req01.8.4 | A |
| SCPC-T-S-Req01.9.2 | B |
| SCPC-T-S-Req01.10.2 | B |
| SCPC-T-S-Req01.11.2 | B |
| SCPC-T-S-Req01.12.2 | B |
| SCPC-T-S-Req02.4.1 | B |
| SCPC-T-S-Req02.4.2 | B |
| SCPC-T-S-Req02.5.2 | B |
| SCPC-T-S-Req02.5.4 | A |
| SCPC-T-S-Req02.6.2 | B |

Table 32: Allocation of Technical Safety Requirements

## ASIL Decomposition - Derivation and Rationale (optional)

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

ASIL decomposition has not been considered for SG01 and SG02 at feature level SRS (FFSD 04 SRS)

## Safety Related Parameters

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

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

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

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Parameter name | Description | Range  Resolution  Initial Value  Unit | Rationale and/or  Constraints | Cali-brat-able | Used in Requirements  (add ID and name of requirement) |
| TILT\_POS\_ADJ\_RNG | Steering column tilt position adjustment range | +-2.8 deg |  |  | SCPC-T-S-Req01.5.1 |
| TILT\_POS\_ADJ\_SPEED | Steering column tilt position adjustment speed | 11 mm/sec  (~ 50 duty cycle) |  |  | SCPC-T-S-Req01.5.1 |
| TEL\_POS\_ADJ\_RNG | Steering column telescopic position adjustment range | 117.46 mm |  |  | SCPC-T-S-Req01.6.1 |
| TEL\_POS\_ADJ\_SPEED | Steering column telescopic position adjustment speed | 11 mm/sec  (~ 50 duty cycle) |  |  | SCPC-T-S-Req01.6.1 |
| PDL\_POS\_ADJ\_RNG | Pedal position adjustment range | ~47mm range |  |  | SCPC-T-S-Req02.4.1 |
| PDL\_POS\_ADJ\_SPEED | Pedal position adjustment speed | 8.5 mm/sec |  |  | SCPC-T-S-Req02.4.1 |

Table 33: 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).*

Link to DFMEA Steering Column\_Pedal Feature in FEDE (ID for the feature DFMEA : FNBDFMEA-00051275):  
<https://www.fedewb.ford.com/#/object-viewer?uid=SklBLsLPoPHwuB&tab=Overview>

SHC Generic DFMEA.pdf

STPA Analysis for Steering Horizon Controller and Steering/Pedal Position Controller

# Execution and Results of Verification Review

|  |  |  |
| --- | --- | --- |
| **Date of review completion** | **Reviewed Version of FFSD** | **Responsible Person for Review** |
| **2021-10-11** | **0.3** | **HDARAISE, SREKAPAL, BMALON24, MDENNI44, araza9, vsrikak1, akeshri** |

Table 21: 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://azureford.sharepoint.com/sites/GlobalFunctionalSafety/Functional%20Safety%20FAQ%20Wiki%20Page/Verification%20Review%20Process.aspx*](https://azureford.sharepoint.com/sites/GlobalFunctionalSafety/Functional%20Safety%20FAQ%20Wiki%20Page/Verification%20Review%20Process.aspx)

*Note: Verification review of FFSDs are required before moving into the next milestone in GTDS/GPDS if the document has been modified and is to be released in the current milestone.*

## 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/Systems | Yes |
|  | Implementation Details of Internal Interfaces | Yes |
|  | System Level architecture (including redundancy) | Yes |
| Technical Safety Requirements Specification  Technical Safety Requirements Derivation | All Technical Safety requirements are traceable to Functional Safety requirements  *(GPDS: UNV0/UPV0, GTDS: <AR>)* | Yes |
|  | 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/system 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/systems 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 “FFSD04 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 Production, Operation, Service and Decommissioning  *(GPDS: UNV0/UPV0, GTDS: <AR>)* | Requirements for Production, Operation, Service and Decommissioning completed | Yes |
| Technical Safety Requirements on Elements/Components/Systems  *(GPDS: UNV1/UPV1, GTDS: n/a)* | V&V acceptance criteria | Yes |

Table 22: 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)*

FFSD 06 Safety Analysis Report has not been rolled out yet.

| **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 |  |  |
| Have hardware safety requirements (categorized as Production, Operation, Service and Decommissioning) been specified for relevant safety-related special characteristics of the safety analysis? | A-D |  |  |
| **Quantitative Safety Analysis Requirements** | | | |
| Is a quantitative analysis performed to verify that the target values are defined appropriately? | (B), C, D |  | See comment |
| 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 |  | See comment |
| 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 |  | See comment |
| **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*. | A-D |  | See comment |
| 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 FFSD06.* | A-D |  | See comment |

Table 23: Checklist for Correctness of qualitative, quantitative and dependent failure Analysis

## Review Exceptions / Deviations / Findings

*Insert project-relevant Input*

No redundancy has been used at feature level SRS

No Reduced Functionality has been derived at feature level SRS

No TSR has been identified related to constraints at feature level SRS

HW Metric Requirements is not applicable for ASIL B SG

ASIL decomposition has not been applied at feature level SRS

Requirements concerning the ability to configure a system by calibration data were not identified

Requirements for Production, Operation, Service and Decommissioning were not identified

## Further Actions / Decisions

*Insert project-relevant Input*

# Execution and Results of Confirmation Review

|  |  |  |  |
| --- | --- | --- | --- |
| **Date of Review**  **Completion** | **Reviewed Version of FFSD** | **Responsible Person for Review** | **Level of Independence** |
|  |  |  |  |
|  |  |  |  |

Table 21: Confirmation review table

\*\*For ASIL C and D Features, Confirmation reviews are combined with the Functional Safety Assessment Activity. Contact Functional Safety Assessment Team to perform the Confirmation Review and Ford Functional Safety Assessment.

*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://azureford.sharepoint.com/sites/GlobalFunctionalSafety/Functional%20Safety%20FAQ%20Wiki%20Page/Confirmation%20Review%20Process.aspx*](https://azureford.sharepoint.com/sites/GlobalFunctionalSafety/Functional%20Safety%20FAQ%20Wiki%20Page/Confirmation%20Review%20Process.aspx) *x*

*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 who reports to a separate Department Manager and was not involved in creation of the work product.*

## 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? *(Optional)* |  |
| Is the Technical Safety Concept appropriate considering the Safety Analysis Report (FFSD06), to ensure confidence in the effectiveness and completeness of Technical Safety Requirements? *(Optional)* |  |
| Do the specified safety mechanisms adequately consider the failures modes of the components identified in the Safety Analysis Report (FFSD06), to ensure the safety mechanisms sufficiently  cover faults? *(Optional)* |  |
| Is the implementation of warning and degradation strategy consistent with the Functional Safety Concept (FFSD03)? *(Optional)* |  |
| ASIL decompositions:   * Are the decomposed technical safety requirements correct (e.g. attributes, parameters) and redundant? *(Optional)* * Is the required independence (no homogeneous redundancy) feasible? * Is the decomposition performed as per the FFSG 04, Section 2.4.2.8? |  |
| Have all the assumptions made in this Safety Requirements Specification been documented and are valid? *(Optional)* |  |
| Are all the Technical Safety Requirements allocated to elements of the system architectural design, to ensure coverage? |  |
| Safety Analysis | Is a qualitative Safety Analyses performed and is it appropriately described? |  |
| Is a quantitative Safety Analyses performed, is it appropriately described with guide words and is the tool described? |  |
| General | Are all sections of the template filled out appropriately, or otherwise contain a valid explanation stating why the section is not necessary? |  |

Table 22: Checklist for Safety Requirements Specification Confirmation

## Review Exceptions / Deviations / Findings

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

No redundancy has been used at feature level SRS

No Reduced Functionality has been derived at feature level SRS

No assumption has been identified at feature level SRS

HW Metric Requirements is not applicable for ASIL B SG

ASIL decomposition has not been applied at feature level SRS

Formal Safety Analysis Report (FFSD 06 ) has not been rolled out

## Further Actions / Decisions

*Describe the resulting actions*

2. Definitions, Abbreviations and Acronyms

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

|  |  |
| --- | --- |
| FFSD | Ford Functional Safety Document |
| APIM | Accessory Protocol Interface Module |
| SCCM | Steering Column Control Module |
| DSM | Driver Seat Module |
| PSM | Passenger Seat Module |
| CDC | Cockpit Domain Controller |
| FHTI | Fault Handling Time Interval |
| E2E | End to End Protection for CAN Communication |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

Table 24: Definitions, Abbreviations and Acronyms