Steer-by-Wire Control System

Safety Specification

Synapse Automotive Steering Safety Concept (ISO 26262)

Elena Rostova
Lead Systems Safety Engineer
e.rostova@nexa.example.com

Jonathan Hayes, PE
Director of Automotive Engineering
j.hayes@vertex.example.com

Date: August 2, 2026
Document Ref: NEXA-SBW-2026-ASIL-D
Version: v1.2.0
System: Synapse Steer-by-Wire (SbW) Core

Abstract

This document presents the functional and technical safety specification for the **Synapse Steer-by-Wire (SbW)** system developed by **Nexa Automotive Controls** and **Vertex Systems** for the **Meridian EV** platform. Formulated in compliance with the road vehicle functional safety standard **ISO 26262:2018**, this specification documents the Hazard Analysis and Risk Assessment (HARA), defining three Automotive Safety Integrity Level D (ASIL D) Safety Goals: preventing unintended self-steering torque, avoiding complete loss of steering assistance, and preventing mechanical steering rack lockups. Functional Safety Requirements (FSRs) are derived and allocated to the Hand Wheel Actuator (HWA) and Road Wheel Actuator (RWA) subsystems. Furthermore, the Technical Safety Concept (TSC) describes a dual-channel fail-operational system architecture, verified using a real-time Hardware-in-the-Loop (HIL) testing environment. Diagnostic coverage metrics and fault tolerant time intervals (FTTI) are detailed alongside system schematics and verification test matrices, proving compliance with ISO 26262.

Contents

List of Tables

List of Figures

1 Introduction

The deployment of steer-by-wire (SbW) technology is a pivotal advancement in modern electric and autonomous vehicles, facilitating weight reduction, design flexibility, and seamless integration with advanced driver assistance systems (ADAS) [2]. However, because SbW systems eliminate the physical mechanical steering column connecting the steering wheel to the steering rack, the integrity of the electrical control system is critical for vehicle control.

This document defines the functional and technical safety specification for the **Synapse Steer-by-Wire (SbW)** system developed by **Nexa Automotive Controls** in partnership with **Vertex Systems**. The target application is the **Meridian EV** platform, an electric vehicle featuring high automation capabilities. This specification is designed to satisfy the requirements of the international standard for road vehicle functional safety, **ISO 26262:2018** [1].

1.1 System Scope and Boundary

The Synapse SbW system consists of two primary physical sub-assemblies:

1. **Hand Wheel Actuator (HWA):** Contains torque and angle sensors to capture the driver's steering intent and a feedback motor to simulate road forces and provide steering feel.
2. **Road Wheel Actuator (RWA):** Comprises redundant electric motors, steering rack position sensors, and microcontrollers to physically actuate the steering linkages.

The boundary of this safety specification covers the dual-channel communication bus (FlexRay), the HWA/RWA microcontrollers, the torque/position sensors, and the actuation power electronics.

1.2 Document Objectives

The objectives of this safety specification are:

- To document the Hazard Analysis and Risk Assessment (HARA) and establish Safety Goals (SGs).
- To specify the Functional Safety Requirements (FSRs) allocated to the HWA and RWA.
- To define the Technical Safety Concept (TSC), including fault detection mechanisms, fail-operational strategies, and degraded modes of operation.
- To outline the verification and validation (V&V) milestones for system integration.

1.3 Target Audience

This document is intended for systems safety engineers, hardware architects, embedded software developers, and safety assessors responsible for validating the functional safety of the steering control loop.

2 Hazard Analysis and Risk Assessment

A systematic Hazard Analysis and Risk Assessment (HARA) was performed in accordance with ISO 26262-3:2018 [1] to identify potential hazardous events resulting from malfunctions in the steer-by-wire system. Each identified hazard is analyzed across various operational situations, evaluating Severity (S), Probability of Exposure (E), and Controllability (C).

2.1 Risk Classification Parameters

The hazard classification is conducted using the standard rating levels defined below:

- **Severity (S):** Rated from $S0$ (no injury) to $S3$ (life-threatening or fatal injuries).
- **Exposure (E):** Rated from $E0$ (incredibly unlikely) to $E4$ (high probability, everyday driving).
- **Controllability (C):** Rated from $C0$ (easy to control) to $C3$ (difficult to control or uncontrollable by an average driver).

The combination of these parameters determines the Automotive Safety Integrity Level (ASIL), ranging from ASIL A (lowest) to ASIL D (highest). If a hazard does not require safety measures under ISO 26262, it is classified as Quality Management (QM).

2.2 Hazard Identification and ASIL Determination

Table 1 details the hazards evaluated for the Synapse SbW control loop. The worst-case operational situations are selected to determine the safety requirements.

Table 1: Hazard Analysis and Risk Assessment (HARA) for Steer-by-Wire control loop.

ID	Hazard Description	Operational Situation	S	E	C	ASIL
HZ_01	Unintended self-steering (spurious torque output)	Highway driving at high speed ($>$ 100 km/h)	S3	E4	C3	ASIL D
HZ_02	Sudden, complete loss of steering assistance	Sharp cornering on mountain roads	S3	E4	C3	ASIL D
HZ_03	Mechanical lock-up of the RWA steering rack	Normal city driving with pedestrians nearby	S3	E4	C3	ASIL D
HZ_04	Incorrect feedback torque generated at HWA	Normal highway driving (spurious vibrations)	S1	E4	C1	QM
HZ_05	Delayed response of road wheels to driver input	Overtaking maneuver on a two-lane road	S3	E3	C3	ASIL C

2.3 Safety Goals (SGs)

Based on the identified hazards, the following Safety Goals (SGs) are established for the steering system. These goals represent the top-level safety requirements that must be met to avoid the hazards.

Safety Goal 1 (SG_01): Prevent Unintended Self-Steering

Safety Integrity Level:	ASIL D
Safe State:	Disable affected actuator channel, initiate standby channel, notify driver.
FTTI:	50 ms (Fault Tolerant Time Interval)

Safety Goal 2 (SG_02): Prevent Complete Loss of Steering Assistance

Safety Integrity Level:	ASIL D
Safe State:	Transition to degraded mode (50% power assist), signal visual warning.
FTTI:	100 ms

Safety Goal 3 (SG_03): Prevent Physical Steering Lock

Safety Integrity Level:	ASIL D
Safe State:	Mechanically decouple faulty channel, maintain main steering path.
FTTI:	15 ms (Immediate response required)

3 Functional Safety Requirements

The top-level Safety Goals are refined into Functional Safety Requirements (FSRs), which define the safety-related functions and diagnostic constraints for the steer-by-wire subsystems. These requirements are allocated to the Hand Wheel Actuator (HWA), the Road Wheel Actuator (RWA), and the communication bus.

3.1 FSR Refinement Strategy

To achieve the high reliability required for ASIL D targets, a multi-tier redundancy and diagnostic concept is employed:

- **Dual-Channel Sensory Paths:** Sensor inputs are acquired via independent physical channels with diverse sensing principles (e.g., optical and magnetic).
- **Diagnostic Coverage (DC):** Must exceed 99% for ASIL D paths within the Fault Tolerant Time Interval (FTTI) [3].
- **Logical Execution Checks:** Microcontrollers must execute software safety functions on dual-core lockstep hardware with hardware-enforced memory protection units (MPUs).

3.2 Functional Safety Requirements Allocation

Table 2 maps the FSRs to the respective subsystems, establishing the compliance trace matrix.

Table 2: Functional Safety Requirements (FSR) Allocation Matrix.

Req ID	Requirement Description	Allocation	Safety Goal	ASIL
FSR_HWA_01	HWA shall monitor driver torque inputs using dual-channel diverse sensors with diagnostic coverage $> 99\%$.	HWA Sensors	SG_01	ASIL D
FSR_HWA_02	HWA controller shall disable feedback motor torque if spurious movement is detected in the steering wheel.	HWA Actuator	SG_01	ASIL D
FSR_RWA_01	RWA shall monitor rotor position and torque from both motor channels to cross-validate operational outputs.	RWA Controller	SG_01, SG_02	ASIL D
FSR_RWA_02	RWA shall perform diagnostic self-tests on power electronics bridges during system startup and every key cycle.	RWA Inverter	SG_02	ASIL D
FSR_RWA_03	RWA shall mechanically isolate a jammed motor winding via an automatic coil-decoupling relay.	RWA Actuator	SG_03	ASIL D
FSR_COM_01	Communication between HWA and RWA shall use a dual-channel FlexRay bus with active CRC and frame counters.	FlexRay Bus	SG_01, SG_02	ASIL D

3.3 Technical Safety Requirements (TSRs)

Functional safety requirements are further translated into Technical Safety Requirements (TSRs) to guide the hardware and software design:

1. **TSR_HW_01:** The torque sensor signals shall be transmitted via Sentinel-bus protocol

with a 16-bit Cyclic Redundancy Check (CRC).

2. **TSR_SW_01:** Software executing on the safety microcontrollers shall implement a three-layer monitoring architecture:
   - Layer 1: Functional control path (torque control).
   - Layer 2: Independent monitoring path (cross-checking torque limits).
   - Layer 3: Processor self-tests, hardware watchdogs, and memory testing.
3. **TSR_HW_02:** The steering motor shall be a dual-wind permanent magnet synchronous motor (PMSM) with isolated power electronics bridges to ensure full drive capability if one winding fails.

4 Technical Safety Concept and System Architecture

The Synapse SbW system implements a fail-operational architecture designed to tolerate single-point hardware and software faults without compromising primary steering control. To satisfy the ASIL D requirements, both physical power paths and electrical signaling paths are fully redundant and galvanically isolated.

4.1 Redundant System Architecture

The system layout features two independent control channels that operate in parallel. Under nominal conditions, both channels contribute equally to active steering and cross-monitor each other. If one channel detects a critical fault, it disables itself and isolates its winding, while the standby channel immediately assumes 100% steering control.

Figure 1 displays the logical block diagram of the technical safety concept.

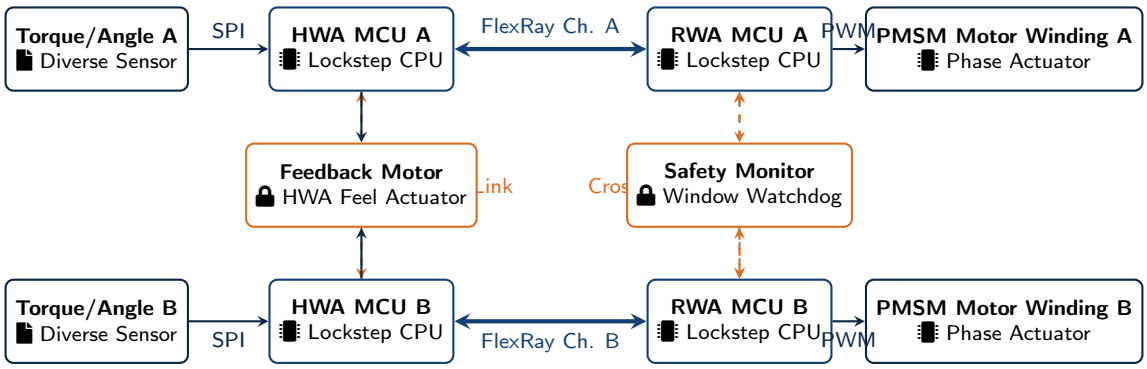

Figure 1: Steer-by-Wire fail-operational architecture schematic showing dual-channel signal pathways.

4.2 Cross-Channel Monitoring and Diagnostic Concept

To ensure instant fault containment, the microcontrollers exchange status bytes and control signals over a high-speed local serial link. The main diagnostics checked include:

- **E2E Communication Safeguards:** Data packets on the FlexRay bus include sequence numbers and a 16-bit CRC to detect signal loss, corruption, or delays.
- **Plausibility Check of Sensor Input:** The torque values from Sensor A and Sensor B are compared. If the variance exceeds 5% for more than 4 ms, a sensor fault state is declared.
- **Power Stage Diagnostics:** Gate driver diagnostic signals are checked continuously to verify proper execution of inverter switching patterns.

4.3 Transition to Safe State

If a diagnostic error is flagged, the system executes the safe state transition matrix described in Table 3.

Table 3: Safe State Transition Matrix for Steer-by-Wire Control Channels.

Diagnostic Failure Trigger	Active State	Next Safe State	Degraded Functionality
Single torque sensor channel open-circuit	Nominal Dual-Ch.	Single-Channel Mode	Full steering power assist; yellow dashboard warning lit.
FlexRay Channel A communication timeout	Nominal Dual-Ch.	Single-Channel Bus	Full power assist using FlexRay Channel B; steering response unchanged.
RWA Inverter Phase Short-Circuit (Channel A)	Nominal Dual-Ch.	Degraded Backup Mode	Channel A isolated; Channel B drives steering with 50% power assist.
Double-channel sensor failure (Dual loss)	Nominal Dual-Ch.	Safe Shutdown State	Steering assist disabled; physical steering rack locked in neutral position.

5 Verification and Validation Concept

Compliance with ISO 26262 ASIL D demands rigorous verification and validation (V&V) procedures across all stages of system development. The Synapse SbW safety concept is validated through a combination of simulation, laboratory testing, and vehicle-level verification.

5.1 V&V Testing Methodologies

The validation plan employs three distinct testing paradigms:

1. **Software-in-the-Loop (SIL):** Automated regression testing of the control and safety algorithms in a simulated vehicle dynamics environment.
2. **Hardware-in-the-Loop (HIL):** Testing the physical HWA and RWA ECUs in a real-time lab setup where hydraulic actuators simulate physical tire-road interactions.
3. **Vehicle-level Track Testing:** Functional verification on proving grounds to evaluate driver controllability and system response under degraded modes.

5.2 Fault Injection Testing on HIL Test Bench

Fault injection testing is a critical validation method used to prove that the system transitions to the designated safe state within the FTTI limit when a malfunction occurs. Table 4 lists the key fault injection scenarios executed during test bench verification.

Table 4: Key fault injection scenarios and safety responses.

Test ID	Fault Simulated	Expected Safe Response	Safety Goal	FTTI Target
FIT_HWA_01	Spurious voltage offset on Torque Sensor Channel A	Control switches to Channel B; driver torque continues without interruption.	SG_01	50 ms
FIT_RWA_02	Phase loss on Motor Winding A inverter bridge	HSI isolates Channel A; steering continues using Channel B with half-power.	SG_02	100 ms
FIT_COM_03	High electromagnetic noise on FlexRay Channel A	System rejects corrupted frames and switches to Channel B.	SG_01, SG_02	50 ms
FIT_SYS_04	Microcontroller lockup (forced watchdog timeout)	Safety monitor isolates the faulty MCU; standby MCU takes control.	SG_01, SG_02	100 ms

5.3 Safety Case Milestones and Audits

A formal safety case is prepared compile safety evidence that all SGs are met. The safety development lifecycle is audited at key milestones by external certifiers:

- **Milestone 1 (Gate 1):** Concept Phase Audit — Focuses on the HARA, Safety Goals, and Functional Safety Concept.
- **Milestone 2 (Gate 2):** System Design Review — Audits the technical safety concept and schematic designs.

- **Milestone 3 (Gate 3):** Safety Case Verification — Reviews the compilation of testing logs, diagnostic coverage analysis, and HIL reports.

Elena Rostova
Lead Systems Safety Engineer
Nexa Automotive Controls
e.rostova@nexa.example.com

Jonathan Hayes, PE
Director of Automotive Engineering
Vertex Systems
j.hayes@vertex.example.com

References

[1] International Organization for Standardization. *ISO 26262:2018 Road vehicles — Functional safety*. ISO, Geneva, Switzerland, 2018.

[2] Meridian Safety Engineering Group. Reference architecture for fail-operational steer-by-wire control loops under iso 26262 asil d. *Journal of Automotive Safety and Reliability*, 12(3):145–162, 2024.

[3] David J. Smith and Kenneth G. L. Simpson. *Functional Safety: A Straightforward Guide to Applying ISO 26262 and IEC 61508*. Routledge, London, UK, 2020.