OpenVVVF

HAZARD ANALYSIS & RISK ASSESSMENT

HARA Core

> Platform hazard analysis, safety goals, and functional safety requirements for the dual-MCU control module; fault-injection validation is defined in OV-TEST-FAULT-INJECTION.

1. Introduction

1.1. Document Set - Core Platform and Application Profiles

The OpenVVVF HARA is published as a **document set** rather than a single document:

Document	ID	Role
OpenVVVF HARA - Core Platform (this document)	OV-SAF-HARA-CORE	Defines the c
OpenVVVF HARA - Motorcycle Application Profile	OV-SAF-HARA-PROF-MOTO	Assigns moto

Additional application profiles (passenger car, rail, industrial/dynamometer) are planned as future documents in the same format. This Core document shall not contain application-specific risk ratings; profile documents shall not restate platform content, and shall declare the Core document version against which they were assessed.

Rationale for the split: the malfunctioning behaviors of a 3-phase traction inverter are platform properties, but the *risk* they create (severity, exposure, controllability, harmed parties, applicable standard) is an application property. A single S/E/C table cannot honestly cover a motorcycle, a car, a train, and a dynamometer; a layered document set can.

1.2. Compliance Statement

THIS IS NOT AN ISO 26262 COMPLIANCE CLAIM

This document
APPLIES ISO 26262:2018 METHODOLOGY
(Part 3: Concept Phase) to identify hazards, assess risk via Severity/Exposure/Controllability classification, and derive Safety Goals with ASIL ratings. For non-road-vehicle application profiles, the equivalent domain standard is referenced for vocabulary and safe-function mapping only (IEC 61800-5-2 for industrial drives; EN 50126/50128/50129 for rail). This is a **best-effort** application of functional safety engineering practice within an open-source project. Full compliance with these standards is not achievable for the project itself: the manufacturer data required for a complete safety case (safety manuals, FMEDAs, certified software libraries) is generally available only under NDA and at costs incompatible with an open-source effort, and the required test facilities (environmental, EMC) are not available. The goal is that this design and its documentation serve as a **starting point that is ready for full compliance work**: the architecture, analyses, and test plan are structured so that a party with access to the required data and facilities can carry the design through complete compliance testing without redesign. The following must be understood clearly:

- **ASIL RATINGS ARE TARGETS**

  derived from the HARA process. They represent the assessed risk level of identified hazardous events, **not a claim that the design has been verified or certified to meet those ASILs**.

- **THE SYSTEM DESCRIBED IS NOT ISO 26262 COMPLIANT**

  , nor compliant with IEC 61508, IEC 61800-5-2, or the EN 5012x railway series. Full compliance would require: complete product development per the applicable standard's product-development parts, hardware architectural metrics (e.g., SPFM ≥ 90% for ASIL B, ≥ 97% for ASIL D; LFM ≥ 60% for ASIL B, ≥ 80% for ASIL D), dependent failure analysis (DFA), software tool qualification, verification and validation testing (including fault injection), configuration management, change control, and independent safety assessment. **None of these have been completed.**

- The hardware implements a
  DUAL-MCU ARCHITECTURE

  : STM32H723ZG main MCU + STM32G474RCTx safety coprocessor. The coprocessor provides independent ADC monitoring of all safety-critical signals, 1oo2 gate drive power kill, challenge/response watchdog, independent CAN bus snooping, and bidirectional NRST. This makes **ASIL D achievable for SG-01 and SG-13 via ASIL B(D) + ASIL B(D) decomposition**.

- The gate driver ICs (onsemi NCV57100) are
  AUTOMOTIVE-QUALIFIED (AEC-Q100)

but are **not ISO 26262 safety elements**. No safety manual, FMEDA, or ASIL claim is available from the manufacturer. Internal protections (DESAT, anti-shoot-through, UVLO) provide hardware-level risk reduction but cannot be claimed as ASIL-rated safety mechanisms without additional justification.

- **SOFTWARE TEST LIBRARY (STL) LIMITATION:**

  This project uses ST's publicly available X-CUBE-CLASSB library (IEC 60730-1 Class B certified). The ISO 26262-certified Class D STL (X-CUBE-STL) requires an NDA and is not available for open-source use. The following ASIL process gaps result: no FMEDA/SPFM/LFM metrics derived for this hardware configuration; no ISO 26262 software tool qualification (compiler, static analysis); no fault injection testing campaign with coverage evidence; no independent safety assessment. ASIL decomposition using the Class B STL is a design and educational exercise only.

- The firmware is **ARCHITECTURALLY COMPLETE**. Field-Oriented Control (FOC) is implemented. Safety mechanisms (tractive effort plausibility checking, immediate safe-state transition, boot CRC, challenge/response watchdog) are specified in this document; their implementation status is tracked in Sections 8 and 11.

- This HARA and its accompanying Fault Injection Test Plan are **LIVING DESIGN-INPUT DOCUMENTS**

  intended to guide development and establish a safety engineering baseline. They do not constitute a product safety case, compliance certification, or warranty of fitness for any purpose.

This is an **OPEN-SOURCE TRACTION INVERTER** project. The documentation is published in the interest of transparency. Users bear full responsibility for evaluating the suitability of this design for their specific application, risk tolerance, and applicable regulatory requirements.

1.3. Scope

This document presents the Hazard Analysis and Risk Assessment (HARA) and Fault Injection Test Plan for the **OpenVVVF control module**: a combined traction inverter control unit and Vehicle Control Unit (VCU) designed to drive 3-phase PMSM traction motors from a DC link bus supply. The core platform is application-agnostic and may drive any compatible DC link supply and 3-phase traction motor. Application-specific operational situations, hazard analysis, and ASIL assignments are defined in separate application profile documents (see §1.1).

The DC link may be supplied by any compatible DC source (for example, a traction battery pack with a Battery Management System); no specific DC source is assumed. The analysis covers the control module and its interfaces to external systems that affect safety.

The scope includes all hardware and software within the control module: the STM32H723ZG main MCU, the STM32G474RCTx safety coprocessor, six NCV57100 gate drivers, 3-phase IGBT power stage, current/voltage/temperature sensing, HV interlock loop (HVIL) digital input, tractive effort control input processing, motor control algorithm, CAN communication, inter-MCU challenge/response watchdog, and fault handling. The Safety Coprocessor is **part of the current design** and provides independent monitoring, 1oo2 gate drive power kill, and ASIL B(D) decomposition.

Out of scope: The traction motor itself (external product), the rotor position sensor/encoder (part of the external motor), the Battery Management System (BMS), the IO board and its associated power supplies (including the Cincon DC/DC converter on the IO side - excluded from this analysis), the charger, and the vehicle display - these are external CAN nodes or external equipment interfaced by the VCU but not designed or manufactured by this project. The CAN protocol definitions in this document are the VCU-side interface only.

> **ASIL DECOMPOSITION VIA DUAL MCU**
>
> This design implements
> **ASIL B(D) DECOMPOSITION**
> through two independent MCUs: the STM32H723ZG (main processor) and the STM32G474RCTx (safety coprocessor). Each MCU independently monitors all safety-critical signals. Either MCU can trigger safe state entry. The 1oo2 gate drive power kill (GATE_DRIVE_PWR1_ENABLE from main, GATE_DRIVE_PWR2_ENABLE from coprocessor) provides an independent supply shutdown path. Target ASIL D is achievable for SG-01 and SG-13 via ASIL B(D) + ASIL B(D) decomposition.

1.4. Reference Standards

Standard	Title
ISO 26262-1:2018	*Road vehicles - Functional Safety - Part 1: Vocabulary*
ISO 26262-3:2018	*Part 3: Concept phase*
ISO 26262-4:2018	*Part 4: Product development at the system level*
ISO 26262-5:2018	*Part 5: Product development at the hardware level*
ISO 26262-8:2018	*Part 8: Supporting processes*
ISO 26262-9:2018	*Part 9: ASIL-oriented and safety-oriented analyses*
ISO 6469-3:2018	*Electrically propelled road vehicles - Safety specifications - Part 3: Electrical safe*
IEC 61800-5-2:2016	*Adjustable speed electrical power drive systems - Part 5-2: Safety requirements -*
IEC 61508	*Functional safety of E/E/PE safety-related systems*
EN 50155	*Railway applications - Electronic equipment used on rolling stock*

2. Item Definition

2.1. System Boundaries

Table 1 - System Boundary Inclusions and Exclusions

Category	Description
In Scope	Combined traction inverter control module / VCU PCB, six onsemi NCV57100 is
Interfaced (external)	DC link source (any compatible DC supply; a source management node such as
Out of Scope	DC source internals (including BMS cell protection where a battery is used), HV

2.2. Architecture Overview

The control module is a combined unit that performs both motor control (inverter) and vehicle-level control (VCU) functions. The architecture comprises the primary control path, the hardware protection layer, an independent safety monitor, rail supervision, and the safe state actuation layer.

Table 2 - External Interfaces

Interface	Connected System
DC link	DC source (any compatible supply)
3-phase AC via NCV57100 x6	PMSM traction motor
CAN1 (heartbeat 5 s)	DC source management node (e.g., BMS, if present)
CAN2 (heartbeat 1 s)	IO board (brake, kickstand, signals)
CAN2	ABS module, display, charger
Analog (dual pot + limit switch)	Tractive effort control input
Sin/Cos analog / Hall effect	Traction motor encoder
External DC/DC (IO side)	12 V onboard power rail
FLT (OR'd, active low)	Six NCV57100 fault outputs

Primary control path - STM32H723ZG main MCU. 550 MHz Cortex-M7, ECC RAM, brown-out detect, internal watchdog. Software functions: FOC motor control, tractive effort command processing, sensor acquisition and plausibility checking, fault detection and handling, CAN communication (FDCAN1 + FDCAN2), safe state management, gate drive power kill (Path 2a). Coprocessor interface: inter-MCU UART, timer sync line, bidirectional NRST. Storage: CY15B102Q-SXET 256 KB FRAM (SPI) for fault logs, configuration, hour meter, odometer; hardware write-protect pin.

Hardware protection layer - six NCV57100 gate drivers (AEC-Q100). Each device provides local hardware protection for its IGBT: DESAT short-circuit detection (<2 us), complementary anti-shoot-through inputs, UVLO, active Miller clamp, soft turn-off, and gate active pull-down. These protections operate independently of either MCU and provide the first line of defense against power stage faults. All six FLT outputs are OR'd together and fed to both MCUs. ASIL credit for these protections is addressed in Section 2.7.

Independent safety monitor - STM32G474RCTx safety coprocessor. 170 MHz Cortex-M4+FPU, 8 MHz crystal, shared +3.3 V rail (dedicated RD7-12S033R DC/DC converter), independent oscillator. Independent ADC access to all 4 current sense signals (phase U/V/W + DC link) + reference, both

IGBT temperature sensors, the DC link capacitor temperature sensor, motor temperature, and all encoder signals (Hall U/V/W, Sin/Cos). Independent gate drive monitoring: GATE_DRIVE_FAULT (OR'd FLT), GATE_DRIVE_READY, GATE_DRIVE_RESET, GATE_DRIVE_PWR1_FB, GATE_DRIVE_PWR2_FB, and all 6 PWM outputs (PH_U/V/W_HIGH/LOW). Independent CAN: FDCAN2 + FDCAN3 - can snoop both CAN buses to cross-check torque commands and node heartbeats. Inter-MCU communication: dedicated UART + timer sync line + bidirectional NRST cross-reset. 1oo2 gate drive power kill: GATE_DRIVE_PWR2_ENABLE (coprocessor) in logical-OR with GATE_DRIVE_PWR1_ENABLE (main); either MCU deasserting its enable kills all six gate drive supplies, each with independent feedback. Challenge/response watchdog: the coprocessor issues a challenge; the main MCU must respond within the window - failure leads to NRST on the main MCU and SSO. Safe state authority: the coprocessor can independently trigger SSO via gate drive power kill, gate drive RESET, or main MCU NRST.

Rail supervisor - TPS389006-Q1 6-channel window supervisor. Monitors the +3.3 V, +5 V, +12 V, and sensor +5 V rails plus both gate-drive power feedbacks (GATE_DRIVE_PWR1_FB, GATE_DRIVE_PWR2_FB). Window thresholds are I2C-configured by the main MCU at boot. On any out-of-window rail fault - including brownout of the +3.3 V rail shared by both MCUs - its NIRQ output asserts the shared GATE_DRIVER_FAULT line, which is monitored by both MCUs (the same net that carries the OR'd gate-driver FLT). The device is TI Functional Safety-Compliant and supports designs up to SIL 3 / ASIL D per TI. The boot-time I2C threshold configuration is a dependency to be covered by the pending DFA (LIMIT-08).

Safe state actuation layer - six redundant SSO pathways.

- **Path 1 (hardware, <100 ns):** TIM1 break input (TIM1_BKIN) → hardware clears MOE, all PWM outputs disabled. Triggered by OR'd gate driver FLT (DESAT/UVLO) or software fault. Independent of both CPU states after trigger.
- **Path 2a (active, ~10 us):** Main MCU → GATE_DRIVE_PWR1_ENABLE low → all six Murata MGJ2D121509MPC-R7 supplies shut down → NCV57100 UVLO → active pull-down → SSO. Feedback via GATE_DRIVE_PWR1_FB.
- **Path 2b (active, ~10 us):** Coprocessor → GATE_DRIVE_PWR2_ENABLE low → same supply shutdown. Independent of Path 2a. Feedback via GATE_DRIVE_PWR2_FB. Either Path 2a or 2b alone achieves SSO (1oo2). The ~10 us figures are actuation-only; time-to-SSO on the power-kill paths additionally depends on gate-bias rail decay to the NCV57100 UVLO threshold and is under characterization.
- **Path 3 (hardware, passive):** Loss of shared 3.3 V rail → NCV57100 VDD lost → internal active pull-down → SSO. Automatic, no software intervention.
- **Path 4 (active, <1 us):** Either MCU → DRIVER_RESET asserted → all NCV57100 RESET inputs → outputs immediately disabled (hard turn-off via OUTL active pull-down; on the NCV57100, soft turn-off exists only on the DESAT path) → SSO. Both MCUs share the RESET line (either can assert). The TPS389006-Q1 rail supervisor is an additional fault source on this pathway: on any monitored-rail fault, including brownout of the +3.3 V rail shared by both MCUs,

it asserts the shared GATE_DRIVER_FAULT line, signaling both MCUs to assert DRIVER_RESET.

- **Path 5 (active, ~100 ms):** Coprocessor challenge/response watchdog failure → coprocessor asserts main MCU NRST → system reset → SSO during boot. Main MCU WDT timeout as backup.
- **Path 6 (active, <10 us):** Coprocessor detects critical fault independently → asserts GATE_DRIVE_PWR2_ENABLE low + GATE_DRIVE_RESET → SSO without relying on the main MCU.

2.3. Safe State Philosophy - Immediate SSO, No Software Ramp-Down

DESIGN DECISION (V5.0): FAULT RESPONSE SHALL BE IMMEDIATE TRANSITION TO SIX-SWITCH-OPEN (SSO). SOFTWARE-CONTROLLED TORQUE RAMP-DOWN ON FAULT IS EXPLICITLY REJECTED.

In IEC 61800-5-2 vocabulary, this design implements **SAFE TORQUE OFF (STO)** as its sole fault response, and deliberately does **not** implement SS1 (controlled deceleration followed by STO). The rationale is as follows:

1. **A CONTROLLED RAMP REQUIRES A TRUSTWORTHY CONTROLLER.**

   A ramp-down on fault detection is executed by the same system whose integrity has just been compromised. If the fault is a lying current sensor, a corrupted tractive effort calculation, or a misbehaving MCU, the "controlled" ramp is closed around untrusted data. Worst case, the ramp-down code is itself where the fault lives. Continued torque production from a faulted controller is unbounded; abrupt torque loss is bounded and, in most operational situations, recoverable by the operator. Moreover, SSO is freewheel: at loss of drive the machine produces no braking torque either, so the torque-free state is dynamically gentle at the drive boundary. Vehicle-level consequences of abrupt torque loss are assessed in the applicable profile document.

2. **HARDWARE ALREADY FORCES SSO.**

   DESAT on the NCV57100 disables the phase within <2 us regardless of software intent; TIM1_BKIN disables all PWM within <100 ns. Any software ramp-down would apply only to the subset of faults that do not assert a hardware path - i.e., precisely the faults where software integrity is most in doubt.

3. **THE BASE-IMAGE / GENERATED-CODE TRUST MODEL REQUIRES A MINIMAL SAFETY KERNEL.**

   Application and control code on this platform is intended to be user-generated via node-based code generation (Section 2.6). A torque-ramping state machine in the base safety image would add safety-critical states, timing edge cases (new fault arriving mid-ramp, regen-to-motoring zero-crossing during ramp), and verification burden. Immediate SSO removes that class of edge-case defects entirely.

4. **RESIDUAL RISK IS OWNED, NOT HIDDEN.**

   The consequence of this decision is that every fault produces an immediate torque step to zero, which is the H-03/H-03a hazardous event. This is an **accepted residual risk**, documented in Section 2.3 and the applicable profile document. The primary risk-reduction mechanism for loss-of-traction hazards under this philosophy is **detection speed** (fault-to-SSO latency), not torque shaping.

Note: the NCV57100 **SOFT TURN-OFF ON THE DESAT PATH**

> is retained. It is a microsecond-scale di/dt/overvoltage protection inside the gate driver and is unrelated to software torque ramping.

2.4. Mitigation Strategy

The following table explains how each hazard class is mitigated by the architecture, which mechanisms cover which failure modes, and where the known limitations are.

Table 3 - Hazard Mitigation Strategy

Hazard Category	Failure Mode	Mi
Unintended tractive effort (H-01, H-15)	Throttle sensor fault (open, short, drift)	Du
Unintended tractive effort (H-01, H-15)	Software error in tractive effort calculation	To
Unintended tractive effort (H-01, H-15)	MCU latch-up / runaway	Wi
Loss of tractive effort (H-03, H-03a)	Fault-triggered safe state entry	Im
Loss of tractive effort (H-03, H-03a)	External system loss (CAN)	CA
Over-torque (H-06)	Excessive tractive effort command	So
Over-torque (H-06)	Short-circuit / shoot-through	NC
Over-temperature (H-07)	IGBT thermal runaway	2 I
Encoder loss (H-08)	Loss of rotor position feedback	En
DC link overvoltage (H-10)	Regen-induced bus rise	Isc
HV isolation (H-09)	HV exposure via isolation loss or open interlock	HV
Safe state failure (H-13, H-14)	Cannot reach SSO; latched tractive effort	Six
Gate driver fault (H-16, H-17)	DESAT/UVLO not detected; PWM deadtime violation	OF

> **HOW TO READ THIS TABLE:**
> Each row maps a hazard category to the specific failure modes that could cause it, the mitigation mechanisms in the current architecture that address those failure modes, and the known limitations of those mitigations. The left column is the **what could go wrong**; the middle column is the **how we prevent or detect it**; the right column is the **why this might not be enough**. The limitations are addressed in Section 9 (Gap Analysis).

2.5. Technical Parameters

Table 4 - Key Technical Parameters (Core Platform)

Parameter	Value / Range
Traction motor type	3-phase PMSM, FOC controlled
DC link voltage / phase current	Set by the attached power stage; the control module itse
DC link source	Any compatible DC source
Main MCU	STM32H723ZG, 550 MHz Cortex-M7, ECC RAM, FDCA
Safety coprocessor	STM32G474RCTx, 170 MHz Cortex-M4+FPU, 3x FDCA
Gate driver	onsemi NCV57100 x6 (AEC-Q100)
Isolation	>5 kV_{rms} (reinforced) per channel
Power stage	External to the control module; 3-phase 2-level IGBT bri
Fail-safe default	Six-switch-open (SSO) via NCV57100 active pull-down
Safe function mapping (industrial vocabulary)	SSO ≙ STO per IEC 61800-5-2; SS1 deliberately not im
Gate kill paths	Six redundant SSO pathways (TIM1_BKIN, 1oo2 gate-d
FLT outputs	All six NCV57100 FLT OR'd to fault input read by both M
Regenerative braking	Application-dependent (see profile documents)

Application-specific parameters (vehicle mass, speed, controllability assumptions) are defined in the applicable profile document, not in this core table.

2.6. Application Software Trust Model - Node-Based Code Generation

The OpenVVVF platform is intended to support user-defined control, modulation, and application-layer logic produced by a **node-based code generation tool**, running on top of a **base safety-tested firmware image**. The following trust model applies and is a platform assumption for all safety claims in this document:

> **GENERATED CODE IS AN UNTRUSTED ELEMENT.**
>
> 1. All safety mechanisms defined in this document - input plausibility and discrepancy checking (FSR-01, FSR-02), rate limiting (FSR-03), torque limiting (FSR-07), temperature voting (FSR-08), encoder-loss detection (FSR-09), HVIL and DC link supervision (FSR-10, FSR-11, FSR-21), watchdog and challenge/response (FSR-15), POST (FSR-16), boot CRC (FSR-19), ECC handling (FSR-20), and all six SSO actuation pathways - **SHALL RESIDE IN THE BASE FIRMWARE IMAGE AND SHALL BE INDEPENDENT OF, AND NOT MODIFIABLE BY, GENERATED APPLICATION CODE** (freedom from interference).
> 2. Generated code may *request* torque within platform-enforced limits; it shall not be able to inhibit, bypass, delay, or reconfigure any safety mechanism or safe-state path.
> 3. The safe state (immediate SSO, Section 2.3) is hardware-enforced and does not depend on any property of generated code.
> 4. The code generator itself is a software tool whose output affects safety-relevant behavior. Under ISO 26262-8 tool-confidence terminology it shall be treated as requiring at least **TCL2/TCL3-LEVEL CONFIDENCE**; no tool qualification has been performed and this is recorded as an open limitation (Section 9, GAP-SW-04).
> 5. Interface contract between generated code and the base image (allowable request ranges, update rates, permitted modulation schemes, sanity envelopes) shall be defined in a separate Interface Control Document. This HARA assumes such a contract exists and is enforced by the base image.
> 6. The safety coprocessor executes only fixed, project-maintained firmware; no generated code runs on the coprocessor, and its monitoring and actuation functions are trusted without qualification. On the main MCU, the safety-critical base image (fault detection and response, safe state management) is likewise outside the generated-code surface.

2.7. Gate Drivers (Non-ASIL)

Six **onsemi NCV57100** isolated high-current IGBT gate drivers. Automotive-qualified per AEC-Q100. These devices are **not ISO 26262 safety elements** - no safety manual, FMEDA, or ASIL claim is available.

Table 5 - NCV57100 Safety-Relevant Features

Feature	Specification	Safety Role
Reinforced isolation	>5 kV_{rms}, 1200 V working	HV-to-logic barrier
Complementary inputs (IN+/IN−)	Internal anti-shoot-through logic	Prevents HS+LS simultaneou
DESAT protection	V_{TH} = 6.5 V, prog. blanking	Short-circuit detection every (
Soft turn-off	Controlled slope on DESAT	Limits di/dt overvoltage
Active Miller clamp	Internal N-FET	Prevents dV/dt turn-on
Gate active pull-down	OUT pulled low on fault/UVLO	Ensures IGBT OFF
UVLO	V_{UVLO+} = 12.2 V, V_{UVLO-} = 11.3 V	No operation at low gate drive
Negative gate drive	VEE2 to −9 V	Robust OFF-state
FLT output	Open-drain, active low	Fault reporting to MCU

NON-ASIL GATE DRIVER IMPLICATIONS:

The NCV57100 internal protections provide valuable hardware-level risk reduction but cannot be counted toward ASIL metrics. The OR'd FLT output is monitored by **both** the main MCU (via TIM1_BKIN) and the coprocessor (via independent GPIO). Either MCU detecting FLT can trigger SSO. The coprocessor additionally monitors the combined NCV57100 READY output and can detect a stuck-active FLT line through its independent PWM output monitoring (all 6 phase high/low signals). This dual monitoring closes the single-point FLT path gap.

2.8. Future Considerations

SAFETY COPROCESSOR - STM32G474RCTX (IMPLEMENTED)

The Safety Coprocessor is a **STM32G474RCTX** (170 MHz Cortex-M4+FPU, 3x FDCAN, advanced motor-control timers) that operates as an **independent safety monitor** alongside the main STM32H723ZG. It is part of the current design and provides:

- **INDEPENDENT GATE DRIVER SUPPLY KILL** (GATE_DRIVE_PWR2_ENABLE, Path 2b) - 1oo2 with main MCU's GATE_DRIVE_PWR1_ENABLE. Independent feedback via GATE_DRIVE_PWR2_FB.
- **INDEPENDENT ADC MONITORING** of all current sensors, temperature sensors, and encoder signals via voltage divider networks
- **CHALLENGE-RESPONSE WATCHDOG** with the main STM32 via inter-MCU UART
- **INDEPENDENT PWM OUTPUT MONITORING** - all 6 phase high/low signals monitored for deadtime violations, stuck-on, stuck-off
- **INDEPENDENT GATE DRIVER FLT MONITORING** via OR'd fault line + combined READY signal
- **INDEPENDENT CAN BUS SNOOPING** via FDCAN2 + FDCAN3 - cross-checks torque commands and heartbeat timing
- **BIDIRECTIONAL NRST** - coprocessor can reset main MCU; main MCU can reset coprocessor

The coprocessor enables **TARGET ASIL D CLAIMS FOR SG-01 AND SG-13 VIA ASIL B(D) + ASIL B(D) DECOMPOSITION**. Both MCUs must independently agree that operation is safe; either can trigger SSO.

3. Operational Situations

Operational Situations are **application-specific** and are defined in the applicable Application Profile document:

- OV-SAF-HARA-PROF-MOTO - Motorcycle Application Profile

Environmental operating conditions for the core platform hardware: ambient −20 °C to +50 °C (storage/qualification −40 °C to +85 °C per front matter), humidity 0–100% condensing, altitude 0–3,000 m MSL, high-vibration mobile mounting. Profiles shall refine these per application.

4. Hazard Identification (HAZID) - Core Platform

Hazards are identified via systematic Functional Hazard Analysis (FHA) combining top-down FMEA perspective, expert judgment on power electronics and traction drive dynamics, and ISO 26262 hazard category checklists. Core-platform hazards are stated at the **drive boundary** (torque production and HV state) with application-neutral harmed parties. Application-specific hazards are defined in the applicable profile document and are additive to this table.

Table 6 - Identified Hazards (Core Platform)

ID	Malfunctioning Behavior	Drive-Boundary
H-01	Unintended positive tractive effort production not requested by operator	Unintended accel
H-02	Unintended reverse tractive effort	Unexpected rearv
H-03	Sudden loss of tractive effort (inability to produce requested tractive effort)	Unexpected loss
H-04	Inability to produce requested regenerative braking tractive effort	Extended stoppin
H-05	Unintended regenerative braking tractive effort (uncommanded)	Unexpected dece
H-06	Excessive tractive effort exceeding design limits	Wheel spin / load
H-07	Failure to limit tractive effort during over-temperature	Fire, thermal dam
H-08	Motor overspeed due to loss of rotor position feedback	Loss of FOC cont
H-09	HV electrical isolation failure	Electric shock, po
H-10	DC link bus overvoltage not detected / not limited	Component ruptu
H-12	IGBT shoot-through (HS and LS simultaneously ON)	Immediate DC lin
H-13	Failure to execute safe state (SSO) on detected fault	Hazardous opera
H-14	Corrupted or latched tractive effort command held indefinitely	Persistent uninter
H-15	Incorrect tractive effort command due to software error	Non-requested tra
H-16	Gate driver fault (DESAT/UVLO/TSD) not acted upon	Phase loss, imbal
H-17	PWM deadtime violation or stuck-on not detected upstream	Shoot-through, D

Application-profile-specific hazards:

ID	Defined In	Summary
H-03a	OV-SAF-HARA-PROF-MOTO	Loss of tractive effort in an application-specific operating situ

5. Risk Assessment Methodology

Severity, Exposure, and Controllability classifications follow ISO 26262-3:2018 Tables 1–3 for road-vehicle profiles. Non-road profiles use the equivalent domain classification (future profile documents). The class definitions below are reproduced for convenience; the per-hazard ratings are **application-specific and are assigned in the annexes**, not in this core section.

5.0.1. Severity (ISO 26262-3 Table 1)

Class	Description
S1	Light and moderate injuries
S2	Severe, life-threatening (survival probable)
S3	Life-threatening to fatal (survival uncertain)

5.0.2. Exposure (ISO 26262-3 Table 2)

Class	Description
E1	Very low probability (<1% of time)
E2	Low (1–10% of time)
E3	Medium (10–50% of time)
E4	High (>50% of time)

5.0.3. Controllability (ISO 26262-3 Table 3)

Class	Description
C1	Simply controllable
C2	Normally controllable (requires attention/skill)
C3	Difficult to control or uncontrollable

> **TARGET ASSIGNMENT POLICY (DELIBERATE CONSERVATISM):**
>
> Profile documents assign ASIL targets per ISO 26262-3 Table 4, and may then **raise a target by up to one level** for hazards whose mitigation depends substantially on software integrity (e.g., software plausibility checks, software fault handling), where a single systematic software fault could defeat multiple nominal mitigations simultaneously. This policy intentionally produces some targets above the Table 4 lookup value (e.g., H-01, H-13, H-15 at ASIL D from S3/E3/C3 inputs). The elevation is a design choice, not a Table 4 result, and shall be read as such.

6. Safety Goals - Core Platform

Safety Goals are platform-level. The **Target** integrity level shown is assigned by the applicable profile document; each profile shall assign targets per its own S/E/C assessment. "Achievable" reflects the current architecture's capability, not verified compliance.

Table 7 - Safety Goals

SG	Safety Goal
SG-01	Prevent unintended positive tractive effort when the operator is not requesting propulsion. Unin
SG-02	Prevent unintended reverse tractive effort. Reverse requests outside permitted conditions shall
SG-03	On loss of tractive effort due to fault, transition to the torque-free state immediately; fault-detect
SG-04	Monitor regenerative braking availability; on loss of regen, the operator shall be informed and f
SG-05	Prevent unintended regenerative braking. Uncommanded regen >10 Nm for >200 ms → safe s
SG-06	Limit max tractive effort to calibrated max. Over-torque >110% → safe state within 100 ms.
SG-07	Detect over-temperature, progressively derate (pre-fault thermal management). Critical temp –
SG-08	Detect loss of rotor position → safe state within 100 ms.
SG-09	Maintain HV isolation (>500 Ohm/V). Isolation fault → safe state.
SG-10	Detect DC link bus overvoltage, limit regen. Critical OV → safe state.
SG-12	Prevent IGBT shoot-through. Risk → PWM disable <10 us via hardware.
SG-13	Achieve safe state (SSO) within 200 ms of any fault. Safe state entry shall be independent of t
SG-14	Detect any NCV57100 fault (DESAT, UVLO, TSD) and transition to safe state.
SG-15	Detect PWM deadtime violations and stuck-on faults. Deadtime collapse or stuck-high >100 us

7. Functional Safety Requirements

Requirements use "shall" for binding provisions and "should" for recommendations. "Tgt" is the target integrity level assigned by the applicable profile document; "Now" is the level achievable with the current architecture.

Table 8 - Functional Safety Requirements (FSRs)

FSR	Requirement
FSR-01	The system shall read dual redundant tractive effort control pots on both MCUs. A discrepanc
FSR-02	The system shall perform tractive effort command plausibility: commanded current reference v
FSR-03	The tractive effort control input shall be rate-limited. Max tractive effort application rate: 500 N
FSR-04	The system shall reject reverse tractive effort when speed >0. Reverse shall be permitted onl
FSR-05	On detection of any fault requiring safe state entry, the system shall transition to SSO **immedi**
FSR-06	The system shall monitor regenerative braking tractive effort continuously. Uncommanded reg
FSR-07	Max tractive effort shall be limited by software LUT on both MCUs with cross-check. Dual-MC
FSR-08	Two IGBT NTC temperature sensors (1oo2 voting) plus one DC link capacitor NTC. Derate at
FSR-09	Encoder loss shall cause transition to safe state within 100 ms. No sensorless fallback is impl
FSR-10	HVIL shall be monitored continuously. Interruption shall cause immediate PWM disable + HV
FSR-11	DC link bus voltage shall be monitored with isolated ADC. OV warning threshold → immediate
FSR-12	NCV57100 complementary inputs (IN+/IN−) shall prevent HS+LS simultaneous conduction. P
FSR-13	NCV57100 DESAT detection shall be active on all six IGBTs. A DESAT event shall cause loca
FSR-14	The STM32 breakpoint input shall cause HW PWM disable within <10 us on any critical fault,
FSR-15	An independent windowed watchdog shall be maintained. Failure to service shall cause autor
FSR-16	Power-on self-test (POST) shall cover: ADC references, current sensor offsets, gate driver co
FSR-17	CAN heartbeat timeouts shall apply safe-state defaults. IO board heartbeat (1 s) loss → safe-
FSR-18	The tractive effort control limit switch shall be monitored independently of the analog pots. Act
FSR-19	Boot-time CRC-32 shall be computed over safety-critical code and calibration data. Mismatch
FSR-20	ECC RAM shall be used for all safety-critical variables. Single-bit errors shall be corrected (SE
FSR-21	DC link bus undervoltage shall be monitored. UV → tractive effort derate; critical UV → safe s
FSR-22	Generated application code (Section 2.6) shall not be able to inhibit, bypass, delay, or reconfi

8. Current Design Coverage

Table 9 - Honest Assessment of Design vs. FSRs

Status vocabulary used throughout this document: **Covered** (implemented in current design), **Planned** (specified, not yet implemented), **Partial** (partially implemented), **To implement** (not started), **Limited** (implemented with documented constraint). No status in this document shall be read as "verified by test" - verification evidence is produced only by execution of the fault-injection test plan OV-TEST-FAULT-INJECTION and is recorded separately per that plan's evidence framework.

FSR	Tgt	Now	Status	Existing / Planned
FSR-01	D	D	Covered	Dual pots on both MCUs; independent voters
FSR-02	D	D	Planned	Commanded vs. measured cross-check on both MCUs
FSR-03	D	C	Covered	Rate limiter implemented
FSR-04	B	B	Planned	Reverse interlock: speed >100 rpm → reverse clamped
FSR-05	C	C	Covered	Immediate SSO on fault (design decision, Section 2.3); ha
FSR-06	C	C	Planned	Uncommanded regen monitor on both MCUs
FSR-07	C	C	Covered	Dual-MCU independent current monitoring (STM32 analo
FSR-08	B	B	Planned	Dual IGBT temp sensors + DC link capacitor sensor (hard
FSR-09	C	C	Limited	Single encoder (external constraint)
FSR-10	B	B	Covered	HVIL digital input implemented
FSR-11	B	B	Covered	DC link isolated ADC
FSR-12	C	A	Covered	NCV57100 complementary inputs
FSR-13	C	A	Covered	NCV57100 DESAT on all six
FSR-14	D	D	Covered	Breakpoint input to HW PWM disable + 1oo2 gate drive p
FSR-15	D	C	Covered	Independent watchdog on STM32
FSR-16	D	C	Partial	NCV57100 DESAT self-test exists
FSR-17	C	C	Planned	1-second heartbeat timeout confirmed
FSR-18	D	C	Covered	Limit switch input implemented
FSR-19	D	C	To implement	STM32 flash CRC peripheral available
FSR-20	D	C	Covered	STM32H723 has ECC RAM
FSR-21	B	B	Planned	DC link ADC can measure UV
FSR-22	D	C	Planned	Base-image enforcement of interface contract

9. Gap Analysis

9.1. Architecture Gaps

GAP-ARCH-01: SINGLE-CORE MCU WITHOUT INDEPENDENT MONITOR (P0)

ISSUE:

All safety mechanisms execute on one STM32H723. A single MCU fault (clock failure, latch-up, supply collapse) can disable all safety functions simultaneously. The independent watchdog is on-chip and subject to common-cause failure.

IMPACT:

SG-01 and SG-13 target ASIL D, achievable via dual-MCU ASIL B(D) + ASIL B(D) decomposition (Table 7). The remaining gap is the formal ASIL D claim, pending the Dependent Failure Analysis (LIMIT-08).

MITIGATION PATH:

Dual-MCU ASIL B(D) decomposition - implemented. Main MCU + coprocessor each achieve ASIL B(D); combined via 1oo2 voter on safe state actuation.

GAP-ARCH-02: POWER KILL WITHOUT FEEDBACK MONITORING (P1, WAS P0)

ISSUE:

The GATE_DRIVE_PWR1_ENABLE (main MCU) and GATE_DRIVE_PWR2_ENABLE (coprocessor) paths provide a 1oo2 active SSO mechanism. **Feedback:** GATE_DRIVE_PWR1_FB and GATE_DRIVE_PWR2_FB provide independent per-supply status. When the NCV57100 detects VDD_UVLO (loss of gate drive supply), it asserts FLT (active low), which both MCUs can read. The 1oo2 architecture means a stuck-high GATE_DRIVE_PWR1_ENABLE is not a single-point failure - the coprocessor can still achieve SSO via GATE_DRIVE_PWR2_ENABLE (Path 2b), GATE_DRIVE_RESET (Path 4), or NRST (Path 5). The shared 3.3V rail provides a passive SSO path (NCV57100 pull-down on VDD loss, Path 3).

IMPACT:

SG-13 targets ASIL D via ASIL B(D) decomposition. Six SSO pathways exist (see Section 2.2). The 1oo2 power kill with independent feedback provides diagnostic coverage for the supply kill path.

MITIGATION PATH:

Implemented - GATE_DRIVE_PWR1_FB (main MCU) and GATE_DRIVE_PWR2_FB (coprocessor) provide independent per-supply feedback. Six SSO pathways (TIM1_BKIN; 1oo2 power kill via GATE_DRIVE_PWR1_ENABLE / GATE_DRIVE_PWR2_ENABLE; 3.3 V rail loss; GATE_DRIVE_RESET; coprocessor watchdog/NRST; coprocessor independent fault trigger) provide extensive redundancy. Verify feedback paths in C-17, C-26, C-27, S-10, and S-11.

GAP-ARCH-03: GATE DRIVER PROTECTION CREDIT - CLOSED

ISSUE:

NCV57100 internal protections are hardware-level and not ASIL-rated (Section 2.7). The OR'd FLT output is a single shared wire, though it is read by both MCUs.

IMPACT ASSESSMENT:

Reviewed per affected safety goal. SG-15 (PWM deadtime violations) does not depend on the gate drivers at all - it is enforced by the coprocessor's independent monitoring of all 6 PWM output pairs; unaffected. SG-12 (shoot-through) is covered by the NCV57100 complementary inputs as the hardware first line, with coprocessor deadtime/stuck monitoring and DESAT (SG-14) as independent detection - no gap in practice. SG-14 (gate driver fault detection) retains one diagnosed path concern - a stuck-active or stuck-inactive OR'd FLT wire - which is caught by the coprocessor's combined READY monitoring and its PWM output cross-check (a real gate fault that the FLT wire fails to report still appears as anomalous phase switching). The residual limitation is the absence of manufacturer qualification data (safety manual/FMEDA), which is not available for this part; no ASIL credit is claimed for the internal protections anywhere in this document.

RESOLUTION:

Closed - analysis complete. No safety goal depends on an ASIL rating of the gate driver; the monitoring coverage above addresses the shared FLT wire. Verification of the cross-check logic remains in C-14, C-15, C-16.

9.2. Component and Software Gaps

GAP-HW-01: HARDWARE OVERCURRENT DETECTION - CLOSED (NOT REQUIRED)

Hard short-circuit protection is handled by NCV57100 DESAT (<2 us). Regular overcurrent (below the DESAT threshold) is detected within
10 US BY THE STM32 ANALOG WATCHDOGS
: both the main STM32H723 and the coprocessor STM32G474 independently monitor all four current sense channels with hardware analog watchdog comparators, so detection does not depend on software sampling rate. Either MCU detecting overcurrent triggers SSO via its independent gate drive power kill path, providing full redundancy - and the coprocessor side runs only fixed, trusted firmware (Section 2.6), so the redundant path does not share the main MCU's software fault surface. **Closed - dual-MCU analog watchdog monitoring is sufficient.**

GAP-HW-02: TRACTIVE EFFORT RAMP-DOWN - CLOSED (REJECTED BY DESIGN DECISION)

Software-controlled torque ramp-down on fault (≤200 Nm/s before SSO) was evaluated and **REJECTED** (Section 2.3): a controlled ramp requires a trustworthy controller, which cannot be assumed once a fault has been detected; hardware paths (DESAT, TIM1_BKIN) force immediate SSO regardless; and a ramping state machine in the base safety image would add safety-critical states and verification burden while being incompatible with the generated-code trust model (Section 2.6). The requirement is replaced by FSR-05 (immediate SSO; detection-to-SSO ≤200 ms). The resulting abrupt-torque-loss exposure is recorded as accepted residual risk for H-03/H-03a (Section 2.3; applicable profile document). **Closed - no implementation planned.**

GAP-SW-01: NO BOOT CRC (P1)

FSR-19: Boot CRC verification is not yet implemented. Add a boot-time CRC-32 using the STM32 CRC peripheral to validate safety-critical code and calibration data before PWM enable.

GAP-SW-03: SENSORLESS FALLBACK POLICY - CLOSED

Policy: immediate SSO on encoder loss (FSR-09). No sensorless fallback mode is implemented; a bounded fallback would require trusting speed estimation derived from potentially faulted sensing, which is incompatible with the Section 2.3 philosophy.

GAP-SW-04: CODEGEN TOOL CONFIDENCE AND INTERFACE CONTRACT UNDEFINED (P1, NEW IN V5.0)

The node-based code generation toolchain (Section 2.6) is under development. Open items: (1) no software tool confidence assessment of the generator (ISO 26262-8 TCL); (2) the interface contract between generated code and the base safety image (FSR-22) is not yet documented; (3) freedom-from-interference between generated code and safety mechanisms has not been analyzed or tested. Mitigation: define the contract ICD, enforce limits in the base image, and extend the fault injection plan with generated-code fault cases (e.g., generated code requests out-of-envelope torque, generates no request, or corrupts its own state) before any public release of the codegen feature.

9.3. Gap Summary

Table 10 - Gap Mitigation Priority

Gap	Priority	Mitigation
Dual MCU with coprocessor	**RESOLVED**	STM32G474RCTx implemented - 1oo
HW overcurrent detection	**CLOSED**	Dual-MCU STM32 analog watchdogs
Torque ramp-down on fault	**CLOSED - REJECTED**	Replaced by FSR-05 immediate SSO
Power kill feedback monitoring	**P1**	GATE_DRIVE_PWR1_FB and GATE_
Gate driver protection credit	**CLOSED**	No SG depends on gate-driver ASIL r
Boot CRC	**P1**	STM32 CRC peripheral
Sensorless policy	**CLOSED**	Immediate SSO on encoder loss (FSI
Codegen tool confidence + contract	**P1**	Contract ICD, base-image enforceme
No DFA (ISO 26262-9)	**P0**	Dependent Failure Analysis
No EMI/EMC pre-compliance	**P1**	CISPR 25 pre-compliance test

Note: With the dual-MCU architecture (STM32H723 + STM32G474 coprocessor), ASIL D is achievable for SG-01 and SG-13 via ASIL B(D) decomposition. The four hazards previously limited to ASIL A (H-06, H-16, H-17, and H-13 safe state failure) are now fully covered: H-06 by dual-MCU independent current monitoring (10 us analog watchdog detection + independent power kill), H-16 by coprocessor FLT/READY/PWM monitoring, H-17 by coprocessor independent deadtime monitoring, and H-13 by six redundant SSO pathways. GAP-HW-01 (HW overcurrent detection) is closed - dual-MCU analog watchdog monitoring is sufficient. No hazards remain below their target ASIL under the applicable profile assessment.

10. Fault Injection Test Plan

The fault-injection test plan that validates the safety mechanisms, safe-state entry paths, and timing budgets defined in this HARA has been extracted to a standalone document in the Testing tree: OV-TEST-FAULT-INJECTION - Fault Injection Test Plan. It defines 92 tests in four categories - component-level (C-01 to C-50), system-level (S-01 to S-19), integration-level (I-01 to I-18), and environmental (E-01 to E-12, deferred type tests) - with per-test executability status, evidence requirements, pass/fail criteria, Safety Goal / FSR / hazard traceability matrices, and a recommended execution order with hardware damage risk classification. Every Safety Goal, Functional Safety Requirement, and identified hazard in this document is covered by at least one executable test case in that plan. Test execution records and evidence are maintained separately as described in the plan.

11. Implementation Roadmap

11.1. Phase 1: Safety-Critical Foundation (Immediate)

Table 11 - Phase 1 - Safety-Critical Foundation

Gap	Action
GAP-HW-01	**CLOSED** - Dual-MCU STM32 analog watchdog monitoring (10 us).
GAP-HW-02	**CLOSED - REJECTED** - Immediate SSO adopted (Section 2.3); FSR-05 rewritten accor
GAP-SW-01	Implement boot CRC-32 (STM32 CRC peripheral) over safety-critical code + calibration b
GAP-SW-03	~~Define sensorless fallback policy~~ - closed: immediate SSO on encoder loss (FSR-0

11.2. Phase 2: Monitors and Platform Hardening (Short Term)

Table 12 - Phase 2 - Monitors and Platform Hardening

Item	Action
FSR-06	Implement uncommanded regen monitor (>10 Nm for >200 ms → safe state).
FSR-02	Implement command-vs-measured current plausibility (>20% for >100 ms → sa
FSR-17	Implement CAN heartbeat timeouts with safe-state defaults.
FSR-08	Implement 1oo2 IGBT temperature voter; thresholds in ECC memory.
FSR-22 / GAP-SW-04	Define the codegen interface contract ICD; implement base-image enforcemen
GAP-TEST-01	Define a dedicated SG-04 loss-of-regen test (command regen, suppress invert

11.3. Phase 3: Test Execution and Validation

Table 13 - Phase 3 - Test Execution and Validation

Activity	Effort	Description
Execute component tests (C-01 to C-50, executable set)	High	Bench campaign per the recomm
Execute system tests (S-01 to S-19)	High	Dyno campaign. Measure detec
Execute integration tests (I-01 to I-18)	Medium	CAN simulation campaign.
Conditional LV-rail tests (C-21, C-22, C-24, C-25)	Low	Schedule once a small program
Application-level characterization (LIMIT-01)	High	In-application testing per the app
Verification report	Medium	Compile executed results and ev

11.4. Coprocessor Integration Validation

The STM32G474RCTx safety coprocessor is **part of the current hardware design**. The following table maps coprocessor capabilities to safety goals:

Table 14 - Coprocessor Capability to Safety Goal Mapping

Feature	Description
Independent throttle monitoring	Coprocessor reads throttle channels via independent ADC. Discr
Independent current monitoring	Coprocessor samples all 4 current sense channels + REF. Cross
Challenge-response watchdog	Main MCU must respond within the window. Failure → NRST →
PWM integrity monitoring	All 6 PWM output pairs monitored for deadtime violations, stuck-
1oo2 gate drive power kill	GATE_DRIVE_PWR2_ENABLE in OR with GATE_DRIVE_PWR
Independent CAN snooping	FDCAN2 + FDCAN3 monitor both buses; cross-check torque cor
Independent temperature monitoring	All heatsink + motor temps via independent ADC; 1oo2 cross-che
FRAM logging	CY15B102Q-SXET 256 KB FRAM (main MCU SPI): fault logs, c

The dual-MCU architecture makes **ASIL D achievable for SG-01 and SG-13 via ASIL B(D) + ASIL B(D) decomposition** under the applicable profile assessment. The coprocessor firmware shall be validated alongside the main firmware - see C-14, S-16 through S-19, and I-16.

12. References

Table 15 - Referenced Standards and Documents

Reference	Title / Description
ISO 26262-1:2018	*Road vehicles - Functional safety - Part 1: Vocabulary*.
ISO 26262-3:2018	*Part 3: Concept phase*. HARA methodology, ASIL assignment, safety goal deriva
ISO 26262-5:2018	*Part 5: Product development at the hardware level*. Hardware architectural metric
ISO 26262-8:2018	*Part 8: Supporting processes*. Software tool confidence (codegen tool, GAP-SW-
ISO 26262-9:2018	*Part 9: ASIL-oriented and safety-oriented analyses*. Decomposition, DFA.
ISO 6469-3:2018	*Electrically propelled road vehicles - Part 3: Electrical safety*. HV isolation (>500
IEC 61800-5-2:2016	*Adjustable speed drives - Safety - Functional*. STO/SS1/SLS vocabulary; Section
IEC 61508	*Functional safety of E/E/PE safety-related systems*. SIL terminology.
EN 50155:2021	*Railway applications - Electronic equipment on rolling stock*. Reference for future
AEC-Q100	*Failure Mechanism Based Stress Test Qualification for ICs*. NCV57100 qualificati
STM32H723ZG	*STM32H723/733 Reference Manual (RM0433)*. STMicroelectronics.
STM32G474RCTx	*STM32G474/484 Reference Manual (RM0440)*. STMicroelectronics.
CY15B102Q-SXET	*2-Mbit Serial (SPI) F-RAM*. Infineon/Cypress.
NCV57100	*Isolated IGBT Gate Driver with Desaturation Protection*. onsemi datasheet.

Note: the Cincon EC7BW-110S12 DC/DC converter resides on the IO side and is **excluded from this HARA** (Section 1.3). It appears here neither as a safety element nor as a referenced component.

13. Document History

Table 16 - Revision History

Version	Date	Changes
1.0	2026-06-13	Initial unified HARA document.
2.0	2026-06-13	Major expansion: 30 new component tests, 14 system tests, 11 integration te
3.0	2026-06-14	LIMIT-07/08/09; CORDIC subsection; dual ASIL evaluations; state machine t
3.1	2026-06-14	S-16 to S-19 modulation transition tests.
4.0	2026-07-08	Dual-MCU primary architecture; six SSO pathways; GAP-HW-01 closed; 1oo
4.1	2026-07-13	Editorial consistency pass; test counts corrected to 99; TPS389006-Q1 integ
5.0	2026-07-30	**Restructure into Core Platform (Layer 0) + Application Profiles (Layer 1)**

5.1	2026-07-30	Document set split: Core Platform (this document, OV-SAF-HARA-CORE) and Motorcycle Application Profile (OV-SAF-HARA-PROF-MOTO) are now separate documents. Core made profile-neutral; application annexes removed; car/rail/industrial profiles deferred to future documents. Formatting constrained for automated PDF generation (stable YAML front matter, document IDs, standard Markdown tables only).
5.2	2026-07-30	Consistency fixes: wrong test cross-references in Table 10 gap summary corrected (S-16–S-19 are modulation tests; power-kill feedback verified by C-17/C-26/C-27/S-10/S-11); contactor wording aligned with BMS-domain authority (VCU requests, BMS actuates); SG-04 reworded (availability monitoring, not availability guarantee); §2.3 residual-risk sentence upgraded with SSO-is-freewheel argument (aligns with OV-SAF-HARA-PROF-MOTO v1.1 H-03a re-rating to ASIL A); §2.7 retitled (coprocessor is implemented, not future); status-count phrasing corrected.
5.3	2026-07-30	Review pass: (1) deliberate-conservatism target policy added to §5 (targets may exceed Table 4 by one level for software-integrity-dependent hazards); (2) HV contactor references removed where out of VCU domain (BMS actuates contactors); (3) SG-04 coverage marked indirect with GAP-TEST-01 added (dedicated loss-of-regen test to be defined); (4) S-12 converted to offline bench test, no dyno; (5) LIMIT-05 rewritten - shared-rail common-cause is fail-safe by construction (Path 3) and TPS389006-Q1 hardware shutdown path (SIL 3 / ASIL D-capable per TI) documented; stray-statistic scan clean.
5.4	2026-07-31	HV contactor scope cleanup: contactor actuation, weld detection, and contactor-related hazards are BMS/OEM-domain and excluded (Section 1.3). H-11 and SG-11 removed; HARA now covers only VCU-side interface behavior (HVIL → PWM disable + CAN1 contactor open request per FSR-10). I-15 retains the VCU response to a BMS weld-detected message (fatal log + lockout).
5.5	2026-07-31	Application-neutrality pass: core document scoped to the platform only; application-specific wording moved to profile documents, which the core now references generically (Sections 1.3, 2.3, 4, 6, 10). No technical content changed.
5.6	2026-07-31	Core scoping cleanup: remaining application-specific descriptors removed; the core now points to the application profile documents generically without naming a reference

application. No technical content changed. |
| 5.7 | 2026-07-31 | Review pass: (1) disclaimer reframed as best-effort functional safety practice with explicit goal of readiness for full compliance work; (2) no DC source type assumed - BMS references generalized to an optional CAN1 source management node; (3) Table 2 restructured (external interfaces table + per-layer descriptions); (4) power-stage-dependent parameters removed from the control-module table (module is power-stage agnostic); (5) gate-driver qualification stated once (Section 2.7), AEC-Q100 elsewhere; (6) GAP-ARCH-03 closed with per-SG analysis (SG-15 independent of gate drivers, SG-12 covered, SG-14 FLT-wire fault caught by coprocessor cross-check); (7) GAP-HW-01 re-based on STM32 analog watchdogs (10 us, dual-MCU redundant); (8) GAP-SW-02 removed, GAP-SW-03 closed (immediate SSO, no sensorless fallback); (9) method notes moved into Section 10.4, Section 10.2.4 removed, HV-safety equipment row removed; (10) tests removed as not executable or not meaningful on this hardware: C-37, C-38, C-40, C-44, C-46, C-47, C-48; C-43 key-cycle requirement replaced by heartbeat/plausibility restoration; (11) phase-to-phase shorts restructured one pair at a time (C-31 U-V, C-32 V-W, C-33 U-W), phase-to-DC-rail merged into C-34; (12) temperature sensing updated to 2 IGBT NTC (1oo2) + 1 DC link capacitor NTC with capacitor derate 90 °C / SSO 105 °C; (13) coprocessor firmware explicitly trusted (no generated code). Plan now 92 tests. |
| 5.8 | 2026-08-13 | Fault-injection test plan extracted to OV-TEST-FAULT-INJECTION (standalone document under Testing/); Section 10 replaced by a reference to the standalone plan. |