OpenVVVF

TEST PLAN

Fault Injection Test Plan

> Safety-mechanism validation by fault injection across component, system, and integration levels; exercises the control module and the C2 power stage as one test article. Extracted from the HARA Core document.

Supported by

MOUSER ELECTRONICS

MITSUBISHI ELECTRIC

SendCutSend

This document is the fault-injection test plan for the OpenVVVF control module. It was extracted verbatim from the HARA Core document (OV-SAF-HARA-CORE) at its version 5.7, where it was Section 10. References of the form "Section 10.x" below are internal to this document; references to other section numbers (e.g., Section 2.3) refer to OV-SAF-HARA-CORE.

This plan is filed directly under `Testing/` rather than under a domain folder because its categories span all of them: the mechanisms under test are firmware safety functions, but the stimulus is physical fault injection into control-module and power-stage hardware (C-series), the closed-loop system (S-series), and external interfaces (I-series). Test execution records and evidence are maintained separately per the evidence framework defined herein: each execution campaign produces a dated `Test Report` document filed as a sibling of this plan, referencing it by doc_id and test ID. Evidence reports are immutable once released; this plan's status tables are the living roll-up.

1. Fault Injection Test Plan

1.1. Test Philosophy

The purpose of this Fault Injection Test Plan is to provide a comprehensive, traceable methodology for verifying that the safety mechanisms implemented in the control module detect faults and transition to the defined safe state (immediate SSO, Section 2.3) within the required time budgets. The test plan defines **92 tests** organized into four categories:

- **Component-Level Tests (C-01 to C-50):** Individual hardware component validation - inject faults into a single sensor, input, or protection circuit and verify detection and safe state entry.
- **System-Level Tests (S-01 to S-19):** Full-system fault scenarios with the complete hardware and software running closed-loop control.
- **Integration-Level Tests (I-01 to I-18):** External interface and communication fault scenarios (DC source management node, IO board, CAN bus).
- **Environmental Tests (E-01 to E-12):** Environmental and stress type tests. **The entire E-series is deferred** - the project does not currently have access to an environmental chamber, vibration table, EMC chamber, ESD gun, or water spray rig. The E-series is retained as a stub reference plan (Section 10.7) for a future type-test campaign and shall not be cited as covering any Safety Goal, FSR, or hazard in the current campaign.

Each test case is designed with the following principles:

1. **Every Safety Goal (SG-01 through SG-15) is covered by at least one test case** that is executable with available equipment.
2. **Every Functional Safety Requirement (FSR-01 through FSR-22) is covered by at least one executable test case** (FSR-22 coverage is planned as generated-code fault cases per GAP-SW-04 and is not yet elaborated).

3. **Every identified hazard (H-01 through H-17, including H-03a) is covered by at least one executable test case** at the drive-boundary level; vehicle-level validation limits are documented in Section 10.10.
4. **Response time requirements shall be verified** where measurable (e.g., <10 us HW PWM disable, ≤50 ms WDT timeout, ≤200 ms detection-to-SSO).
5. **Fault injection shall be realistic** - faults represent credible failure modes observed in traction power electronics systems.
6. **Tests shall be independently executable** where possible to allow incremental validation as software matures.
7. **Only tests that can actually be executed with available equipment are scheduled in the current campaign.** Each test carries an explicit executability status (Section 10.3).

1.1.1. Test Status Vocabulary

The following vocabulary shall be used consistently for every test and requirement:

Term	Meaning
Defined	Test procedure and acceptance criteria written; not yet executed.
Executable	All required equipment and facilities are available; the test can be run in the current camp
Conditional	Executable subject to a stated minor prerequisite (e.g., a small LV bench supply).
Deferred	Cannot be executed with available equipment or facilities; scheduled for a future campaig
Executed	Test has been run; raw evidence (telemetry, video, scope captures) recorded per Section
Verified	Executed, passed, and reviewed; evidence reference entered in the traceability matrices.

1.1.2. Statement on Execution Records

> This section
> **DEFINES**
> the fault injection test plan and acceptance criteria. Test execution records, measured results, telemetry logs, and video/scope evidence shall be maintained separately in the OpenVVVF verification evidence repository and summarized in the OpenVVVF Verification Report(s). This document shall be updated only to reflect changes to the plan itself. As of this revision, all tests are **Defined**; none are **Executed** or **Verified**.

1.2. Test Environment

1.2.1. Available Test Equipment

The following equipment is **available** for the current campaign. Tests requiring anything not on this list are marked Conditional or Deferred.

Table 11 - Available Test Equipment

Item	Description
Test article	Control module PCB with STM32H723 + STM32G474, six NCV57100, IG
DC link source	Programmable bidirectional DC supply, 0–1500 V DC, −50 A to +50 A (cu
Dyno	4-quadrant motor dynamometer with speed and torque measurement and
Test motor	Low-voltage PMSM on dyno
Oscilloscope	4-channel, with HV differential probes and current probes
CAN interface	USB-CAN adapter (PCAN or equivalent)
Debug probe	ST-Link / J-Link with halt and memory access
Throttle simulation	Two programmable DC supplies feeding the throttle wiper inputs
Thermal camera	Infrared camera
Heat gun	Localized heating of NTC sensors
RTE (Real Time Examiner)	Host tool connected via CAN or debug interface
Video recording	Camera(s) covering DUT, scope screen, and test area

1.2.2. Equipment Not Available (Drives Deferred Status)

Item	Conse
Insulation tester (megohmmeter) / HiPot tester	C-50 us
Short-circuit contactor	C-31–C
Small programmable LV bench supply (for 3.3 V / 12 V / 5 V rail wiggling)	C-21, C
Thermal chamber, humidity chamber, vibration table, EMC chamber, ESD gun, water spray rig	E-01 th
Shaft voltage / bearing-current brush rig	C-36 **D**

1.2.3. Test Records and Evidence

Every executed test shall produce the following evidence artifacts:

1. **Telemetry log** - RTE/CAN capture of internal variables, fault status, and tractive effort commands for the full test duration.
2. **Video recording** - continuous video covering the DUT, the oscilloscope screen, and the test area, narrated with the procedure step being performed.
3. **Scope captures** - saved waveforms for every timing-critical measurement (PWM disable, DESAT response, deadtime, etc.).

Naming convention: `<TestID>_run<N>_<YYYY-MM-DD>_<condition>.<ext>`, e.g., `C-15_run2_2026-08-14_60V.mp4`, with the telemetry log and scope captures sharing the same base name. Evidence references shall be entered into the per-test **Evidence** field and the traceability matrices (Section 10.8) upon execution. Evidence shall be published alongside this document in the project repository.

1.3. Test Status Summary

Table 12 - Executability Summary (v5.0 Campaign)

Block	Tests	Status
Sensor/input faults	C-01–C-09	**Executable** (th
DC link & HVIL	C-10–C-12	**Executable**
MCU/safety-path faults	C-13–C-20, C-39, C-41, C-43	**Executable**
LV rail faults	C-21, C-22, C-24, C-25	**Conditional** - r
Rail/gate-supply shorts	C-23, C-26, C-27	**Executable** (cu
Phase faults (open)	C-28–C-30	**Executable** (m
Phase faults (short)	C-31–C-34	**Executable** via
Cap temp / ADC / SPI / thermal runaway / deadtime	C-35, C-41, C-42, C-45, C-49	**Executable**
Bearing current	C-36	**Deferred** - requ
Isolation	C-50	**Executable** via
System tests	S-01–S-19	**Executable** (4-
Integration tests	I-01–I-18	**Executable** (C
Environmental tests	E-01–E-12	**Deferred** - type

Counts: **84 Defined-Executable, 4 Defined-Conditional (C-21, C-22, C-24, C-25 - pending LV bench supply), 1 Deferred-equipment (C-36), 12 Deferred-type-test (E-series).** Total 101 line items including the E-series stubs; 92 tests in the current plan.

1.4. Component-Level Tests

Method note - throttle simulation: For C-01 through C-04 and S-01, the dual throttle potentiometer wipers shall be simulated by two programmable DC supplies (0–5 V, common ground with the DUT). This permits precise, repeatable discrepancy, drift, short-to-rail, and short-to-ground injection. This method simulates the wiper signal only; it does not exercise ratiometric behavior against the sensor 5 V rail (rail faults are covered separately by C-24). At least one test in the campaign (C-05) shall use the real mechanical throttle assembly including the end-travel limit switch so the end-to-end path through the physical connector is exercised.

Method note - manual fault injection: Open-circuit faults shall be injected by physically disconnecting the relevant wire or connector during operation (no relay rig is used in this campaign). Gradual-drift faults shall be injected by ramping or stepping the simulating DC supply. Actual injection timing shall be captured from the telemetry record and video; exact repeatability of the injection instant is not required.

C-01: Tractive Effort Control Potentiometer 1 Open Circuit

Objective: Verify FSR-01 - dual tractive effort control plausibility shall detect an open circuit on the primary channel.

Covered: SG-01 (ASIL D), FSR-01, H-01
Status: Executable - Defined | **Evidence:** -

Procedure:

1. Connect throttle simulation supplies (Section 10.2.1) with both channels functional. System at key-on, traction motor not running.
2. Apply 50% tractive effort request via both channels (matched within 2%).
3. While maintaining input, open-circuit channel 1 (disconnect at PCB).
4. Observe system response via RTE and oscilloscope on PWM outputs.
5. Repeat with traction motor spinning at 50% rated speed under dyno load.

Acceptance Criteria: The system shall detect channel 1 out-of-range / discrepancy >5% within <100 ms and shall transition to SSO. No tractive effort shall be produced after the fault. The fault shall be logged with the correct DTC.

Rationale: An open circuit on one channel is a credible wiring failure. The dual-channel plausibility check (FSR-01) must detect the discrepancy and enter safe state before any unintended tractive effort can be commanded. Directly addresses H-01.

C-02: Tractive Effort Control Channel 2 Shorted to +5 V

Objective: Verify FSR-01 - the plausibility check shall detect short-to-rail on the secondary channel.

Covered: SG-01 (ASIL D), FSR-01, H-01
Status: Executable - Defined | **Evidence:** -

Procedure:

1. Both channels functional. System at key-on.
2. Apply 25% request on channel 1; drive channel 2 to +5 V via the simulation supply (simulating wiring short).
3. Observe response via RTE and scope.
4. Repeat with traction motor running at 25% speed under load.

Acceptance Criteria: Discrepancy >5% shall be detected within <100 ms. Safe state shall be entered. Fault shall be logged.

Rationale: Short-to-rail is a common wiring fault (chafed harness). Distinct failure mode from C-01; verifies the plausibility check works for high anomalies.

C-03: Tractive Effort Control Channel 1 Shorted to Ground

Objective: Verify FSR-01 - short-to-ground detection on the primary channel.

Covered: SG-01 (ASIL D), FSR-01, H-01
Status: Executable - Defined | **Evidence:** -

Procedure: Drive channel 1 to 0 V / ground while channel 2 is at 50%. Observe response. Repeat under motor load.

Acceptance Criteria: Discrepancy shall be detected within <100 ms. Safe state shall be entered. Fault shall be logged.

Rationale: Ground short is distinct from open and +5 V short (different ADC reading). Verifies robustness across all three common wiring fault modes.

C-04: Tractive Effort Control Drift (Gradual Divergence)

Objective: Verify FSR-01 shall detect gradual channel mismatch (sensor degradation).

Covered: SG-01 (ASIL D), FSR-01, H-01
Status: Executable - Defined | **Evidence:** -

Procedure: Using the throttle simulation supplies, gradually increase the offset between channel 1 and channel 2 from 0% to 10% over 10 seconds while the traction motor runs at constant speed. Record the trip point from telemetry.

Acceptance Criteria: The fault shall trigger when discrepancy exceeds the 5% threshold. No false trips shall occur below threshold.

Rationale: Gradual drift (wear, aging) must be distinguished from normal variation. Verifies threshold calibration - neither nuisance trips nor missed faults.

C-05: Tractive Effort Control Limit Switch Activation at Speed

Objective: Verify FSR-18 - the limit switch shall independently command zero tractive effort, overriding analog values.

Covered: SG-01 (ASIL D), FSR-18, H-01
Status: Executable - Defined | **Evidence:** -

Procedure: This test shall use the **real mechanical throttle assembly** (not the simulation supplies).

1. Traction motor running at 50% rated speed under dyno load with 50% tractive effort request applied.
2. Activate the tractive effort control limit switch (mechanical end-stop) while maintaining potentiometer position.
3. Observe tractive effort command and PWM output via RTE and scope.

Acceptance Criteria: The tractive effort command shall drop to zero within <50 ms of limit switch activation, regardless of potentiometer position. PWM shall be disabled or zero duty. Fault shall be logged.

Rationale: The limit switch is an independent hardware path to zero tractive effort - the last-resort protection against stuck cable or sensor malfunction. Also exercises the physical connector path end-to-end.

C-06: Phase Current Sensor Offset Drift

Objective: Verify FSR-02 - tractive effort command plausibility shall detect current sensor offset error.

Covered: SG-01 (ASIL D), SG-06 (ASIL C), FSR-02, H-01, H-06
Status: Executable - Defined | **Evidence:** -

Procedure:

1. Traction motor running at 50% rated tractive effort under dyno load.
2. Inject DC offset (+20% of rated current) into one phase current sensor via external bias circuit.
3. Observe commanded tractive effort vs. measured current. Record the trip point.
4. Repeat with −20% offset.

Acceptance Criteria: Plausibility deviation >20% shall be detected within <100 ms. Safe state shall be entered.

Rationale: Sensor offset drift causes the MCU to misread actual current. Verifies the end-to-end plausibility chain (FSR-02).

C-07: DC Link Current Sensor Open Circuit

Objective: Verify FSR-02 - loss of DC link current sensor shall be detected.

Covered: SG-01 (ASIL D), FSR-02, FSR-07, H-01, H-06
Status: Executable - Defined | **Evidence:** -

Procedure: Open-circuit the DC link current sensor signal wire while the traction motor runs at 25% load. Observe plausibility check and safe state entry.

Acceptance Criteria: Sensor out-of-range shall be detected. If a reference signal is present: reference mismatch shall be detected. Safe state within <200 ms.

Rationale: The DC link sensor provides the sum-current check against phase currents. Verifies graceful handling of its loss.

C-08: IGBT Overtemperature (Simulated)

Objective: Verify FSR-08 - 1oo2 temperature voting and progressive derating.

Covered: SG-07 (ASIL B), FSR-08, H-07
Status: Executable - Defined | **Evidence:** -

Procedure:

1. Use a heat gun or programmable resistor to elevate one IGBT temp sensor reading above the warning threshold while the other remains normal.
2. Observe tractive effort derating via RTE.
3. Elevate the second sensor to the warning threshold. Verify further derating.
4. Elevate both above the critical threshold. Verify SSO entry.
5. Test single-sensor failure: one sensor stuck implausibly high while the other is normal. Verify discrepancy detection triggers the fault response (a stuck-high sensor causes derating - safety over availability).

Acceptance Criteria: Progressive derate shall occur at warning thresholds. SSO shall be entered at the critical threshold. Either sensor reaching threshold shall trigger the response (1oo2); sensor discrepancy shall be detected. Response times: derate <500 ms; SSO <1 s from critical threshold crossing.

Rationale: IGBT thermal runaway is a credible failure mode. Verifies both the temperature response curve and the voting logic. Note: derating is pre-fault thermal management; once the critical threshold is crossed, the response is immediate SSO (Section 2.3).

C-09: Traction Motor Encoder Signal Loss

Objective: Verify FSR-09 - encoder loss detection and safe state entry.

Covered: SG-08 (ASIL C), FSR-09, H-08
Status: Executable - Defined | **Evidence:** -

Procedure:

1. Traction motor spinning at 50% rated speed under dyno load (closed-loop FOC).
2. Disconnect encoder channel (manual open circuit).
3. Observe FOC behavior and safe state entry via RTE and scope.
4. Repeat with encoder supply disconnected (all channels lost).
5. If sensorless fallback is implemented: verify bounded operation (≤2 s, ≤30% tractive effort) before SSO.

Acceptance Criteria: Encoder loss shall be detected within <100 ms. Safe state shall be entered. If sensorless fallback: bounded to ≤2 s and ≤30% tractive effort, then SSO. Fault shall be logged with the correct DTC.

Rationale: Loss of position feedback at speed causes FOC to lose synchronization (H-08). The single encoder has no redundancy; immediate SSO is required.

C-10: DC Link Bus Overvoltage (Simulated)

Objective: Verify FSR-11 - DC link overvoltage detection and regen disable.

Covered: SG-10 (ASIL B), FSR-11, H-10
Status: Executable - Defined | **Evidence:** -

Procedure:

1. System running with DC link at nominal voltage (≤140 V). Traction motor spinning with regen active (4-quadrant dyno driving, supply sinking).
2. Gradually raise the DC link voltage via the programmable supply to the OV warning threshold.
3. Verify regen is disabled/reduced.
4. Continue raising to the critical OV threshold (do not exceed 175 V on the 200 V-class board).
5. Verify SSO within <50 ms of critical threshold crossing.

Acceptance Criteria: Regen shall be disabled at the warning threshold. SSO shall occur at the critical threshold within <50 ms. No overvoltage damage to DC link capacitors or semiconductors.

Rationale: Overvoltage occurs during hard regen or source-side voltage excursions. Both thresholds (warning → regen disable; critical → SSO) must be verified.

C-11: DC Link Bus Undervoltage (Simulated)

Objective: Verify FSR-21 - DC link undervoltage detection and response.

Covered: SG-03 (ASIL C), SG-10 (ASIL B), FSR-21, H-03
Status: Executable - Defined | **Evidence:** -

Procedure: Gradually reduce the DC link voltage via the programmable supply while the traction motor runs at 50% load. Observe derating and safe state entry at the critical UV threshold.

Acceptance Criteria: Tractive effort shall be derated progressively as bus voltage drops. Safe state shall be entered at critical UV (immediate SSO per FSR-05). No overcurrent event shall occur due to insufficient DC link voltage.

Rationale: Insufficient DC link voltage saturates the current controller, risking overcurrent when voltage recovers.

C-12: HVIL Interruption

Objective: Verify FSR-10 - HVIL loop interruption detection and response.

Covered: SG-09 (ASIL A), FSR-10, H-09
Status: Executable - Defined | **Evidence:** -

Procedure:

1. System at key-on with HVIL loop intact.
2. Open the HVIL loop (disconnect HVIL connector - the intended field mechanism).
3. Measure time from HVIL open to PWM disable and to contactor open request on CAN1.

Acceptance Criteria: PWM shall be disabled within <50 ms. Contactor open request shall be transmitted on CAN1 within <100 ms. Fault shall be logged.

Rationale: HVIL interruption indicates connector disconnection or interlock trigger. Both VCU-side responses (PWM disable, CAN1 open request) shall be verified; contactor actuation is BMS/OEM-domain.

C-13: Watchdog Timeout (STM32 Failure to Service)

Objective: Verify FSR-15 - the independent watchdog shall detect MCU runaway and force reset.

Covered: SG-13 (ASIL D), SG-01 (ASIL D), FSR-15, H-13, H-14
Status: Executable - Defined | **Evidence:** -

Procedure:

1. Traction motor running at 50% load.
2. Via debug probe, halt CPU execution (simulating code runaway).
3. Measure time from CPU halt to PWM disable and system reset.
4. Alternatively, use a firmware build that intentionally stops servicing the watchdog after a trigger condition.

Acceptance Criteria: PWM disable and system reset shall occur within the watchdog timeout (≤50 ms). No tractive effort shall be produced during or after reset until POST completes and a key cycle occurs.

Rationale: CPU runaway can leave PWM at constant duty (H-14). The halt-via-debug method is a realistic fault injection for this failure mode.

C-14: STM32 Breakpoint Input (HW PWM Disable)

Objective: Verify FSR-14 - the hardware breakpoint input shall disable all PWM within <10 us, independent of software.

Covered: SG-13 (ASIL D), FSR-14, H-13
Status: Executable - Defined | **Evidence:** -

Procedure:

1. Traction motor running at 50% load with active PWM.
2. Assert the breakpoint input pin via external switch.
3. Measure time from assertion to all six PWM outputs low, using the oscilloscope.
4. Verify PWM remains disabled while the breakpoint is held.
5. De-assert and verify PWM does NOT resume without system reset and POST.

Acceptance Criteria: All PWM outputs shall be disabled within <10 us of assertion. This shall be demonstrated with the CPU halted via debugger (hardware-only path). PWM shall not auto-resume.

Rationale: The breakpoint input is the fastest safe-state path and must work with a completely non-functional CPU. The <10 us requirement addresses shoot-through and other time-critical faults.

C-15: Gate Driver DESAT (Simulated Short Circuit)

Objective: Verify FSR-13 - NCV57100 DESAT protection shall detect and respond to a simulated short circuit.

Covered: SG-12 (ASIL C), SG-14 (ASIL C), FSR-13, H-12, H-16
Status: Executable - Defined | **Evidence:** -

Procedure:

1. System at key-on with DC link present. Gate drivers active.
2. Use a DESAT test fixture to momentarily pull the DESAT pin above threshold (or inject a brief low-energy overcurrent pulse).
3. Measure FLT response time and PWM disable via scope.
4. Verify soft turn-off slope (not hard shutoff).
5. Verify FLT is latched and readable by both MCUs.

Acceptance Criteria: DESAT shall be detected and PWM disabled within <2 us. Soft turn-off shall be observed. FLT shall be asserted and latched. The system shall enter safe state.

Rationale: DESAT is the primary short-circuit protection. Verifying its response time and behavior is essential to the overall safety argument and forms the basis for the self-test (C-16).

C-16: Gate Driver DESAT Self-Test at Power-On

Objective: Verify FSR-16 - the DESAT self-test shall confirm protection circuit function before PWM enable.

Covered: SG-12 (ASIL C), SG-14 (ASIL C), FSR-16, H-12, H-16
Status: Executable - Defined | **Evidence:** -

Procedure: Power cycle the system. Observe the DESAT self-test sequence. Verify PWM is not enabled until all six gate drivers pass. Introduce a fault in one DESAT circuit (e.g., open DESAT diode) and verify the system refuses to enable PWM.

Acceptance Criteria: Self-test shall complete on all six channels. PWM enable shall be gated by self-test pass. With an injected DESAT fault: the system shall remain in safe state, log the fault, and never enable PWM.

Rationale: A failed DESAT circuit is a latent fault that would prevent short-circuit detection. POST must catch it before operation (latent fault coverage).

C-17: Gate Driver UVLO (Simulated Low Supply)

Objective: Verify gate driver UVLO shall prevent operation at insufficient gate drive voltage.

Covered: SG-12 (ASIL C), FSR-12, H-12
Status: Executable - Defined | **Evidence:** -

Procedure: Gradually reduce the +15 V gate driver supply while the system is operating. Record the UVLO trigger point and PWM disable.

Acceptance Criteria: UVLO shall trigger at $V_{UVLO-} \approx 11.3$ V. All PWM shall be disabled. FLT shall be asserted. Safe state shall be entered.

Rationale: Insufficient gate drive causes linear-region IGBT operation and thermal destruction. UVLO forces gate OFF when supply is inadequate.

C-18: ECC RAM Single-Bit Error Injection

Objective: Verify FSR-20 - ECC RAM shall correct single-bit errors and allow continued operation.

Covered: SG-13 (ASIL D), SG-15 (ASIL C), FSR-20
Status: Executable - Defined | **Evidence:** -

Procedure: Use the STM32 ECC error injection capability (if available) or the debug probe to flip a single bit in a safety-critical RAM location (e.g., tractive effort limit variable). Observe system behavior via RTE.

Acceptance Criteria: The single-bit error shall be detected and corrected. The system shall continue operating. The error shall be logged. No unsafe state shall be entered.

Rationale: Radiation and EMI can corrupt RAM. SECDED ECC must handle single-bit errors transparently without false trips.

C-19: ECC RAM Double-Bit Error Injection

Objective: Verify FSR-20 - double-bit errors shall trigger safe state (uncorrectable).

Covered: SG-13 (ASIL D), FSR-20
Status: Executable - Defined | **Evidence:** -

Procedure: Flip two bits in a safety-critical RAM location. Observe system response.

Acceptance Criteria: The double-bit error shall be detected. Safe state shall be entered immediately. A fatal error shall be logged. The system shall require reset.

Rationale: Double-bit errors are uncorrectable; corrupted data could be a safety-critical variable.

C-20: Boot CRC Mismatch

Objective: Verify FSR-19 - boot CRC shall prevent operation with corrupted firmware.

Covered: SG-01 (ASIL D), SG-13 (ASIL D), FSR-19, H-15
Status: Executable - Defined | **Evidence:** -

Procedure: Deliberately corrupt one byte in the safety-critical code flash region (debugger or flash tool). Power cycle and observe boot behavior.

Acceptance Criteria: The CRC-32 mismatch shall be detected at boot. PWM enable shall be prevented. The fault shall be logged. The system shall remain in safe state.

Rationale: Corrupted firmware could modify tractive effort mapping, safety thresholds, or fault handling (H-15).

C-21: STM32 Supply Brownout - Gradual Vdd Drop

Objective: Verify brownout detection (BOR) shall trigger safe state before MCU operation becomes unreliable.

Covered: SG-13 (ASIL D), FSR-14, FSR-15, H-13, H-14
Status: Conditional - requires small programmable LV bench supply | **Evidence:** -

Procedure:

1. System operating at 50% tractive effort. Vdd = 3.3 V nominal.
2. Using the LV programmable supply, ramp Vdd down gradually at 10 mV/s.
3. Observe BOR threshold. Verify reset/assertion before Vdd reaches 2.5 V.
4. Verify PWM disabled at BOR assertion and safe state entered.
5. Repeat at 100 mV/s and 1 mV/s; repeat at idle, full load, and regen.

Acceptance Criteria: BOR shall assert at a consistent threshold (±50 mV). PWM shall be disabled before Vdd < 2.5 V. No erratic PWM behavior shall occur during decay. Tractive effort shall be zero before the MCU becomes unreliable.

Rationale: A declining supply can put the MCU in an undefined region with random PWM output. BOR must catch this first.

C-22: Brownout Recovery - Power Dip Ride-Through

Objective: Verify system behavior during brief power dips and recovery.

Covered: SG-13 (ASIL D), FSR-16, H-13
Status: Conditional - requires small programmable LV bench supply | **Evidence:** -

Procedure:

1. System operating at 50% tractive effort.
2. Apply brief Vdd dip: 3.3 V → 2.8 V for 10 ms (above BOR). Verify continued operation.
3. Apply brief Vdd dip: 3.3 V → 2.6 V for 5 ms (below BOR). Verify BOR reset.
4. Apply Vdd interruption: 3.3 V → 0 V for 100 ms → 3.3 V. Verify full POST on recovery.
5. Repeat with dip on the +12 V rail while monitoring gate driver UVLO.

Acceptance Criteria: Dips above BOR: uninterrupted operation. Dips below BOR: clean reset, PWM disabled, POST on recovery. +12 V dip: NCV57100 UVLO triggers, PWM disabled. In all cases the safe state shall be maintained during the anomaly.

Rationale: Real-world power disturbances must produce clean ride-through or clean reset - never an undefined operational state.

C-23: +12 V Logic Rail Short to Ground

Objective: Verify system response when the +12 V logic rail is shorted to ground.

Covered: SG-13 (ASIL D), FSR-14, FSR-15, H-13
Status: Executable - Defined | **Evidence:** -

Procedure:

1. System operating at 50% tractive effort. +12 V rail monitored.
2. Apply a controlled short to ground on the +12 V rail via current-limited fixture (<5 A).
3. Observe: STM32 supply (3.3 V via dedicated DC/DC), gate driver supplies, CAN transceivers.
4. Record which subsystems lose power and which remain operational.
5. Remove short. Verify recovery behavior.

Acceptance Criteria: If +12 V collapse causes 3.3 V dropout: BOR shall trigger and safe state shall be entered. Gate driver isolated supplies shall remain operational or UVLO shall trigger safe state. No erratic PWM during collapse. Short removal shall require key cycle to resume.

Rationale: A +12 V short (chafed wiring, failed load, moisture) must fail safely via BOR and/or gate driver UVLO.

C-24: +5 V Sensor Rail Short to Ground

Objective: Verify system response when the +5 V sensor supply is shorted.

Covered: SG-01 (ASIL D), SG-13 (ASIL D), FSR-01, FSR-09, H-01, H-08
Status: Conditional - requires current-limited LV fixture/supply | **Evidence:** -

Procedure:

1. System operating. +5 V rail powers throttle pots, current sensor references, encoder.
2. Apply a controlled short on the +5 V rail (current-limited to <2 A).
3. Observe throttle readings (zero/OOR) and current sensor reference loss.
4. Verify FSR-01 catches pot OOR; verify FSR-09 catches encoder loss (if encoder powered from +5 V).
5. Verify safe state entry before any incorrect tractive effort is produced.

Acceptance Criteria: The +5 V short shall be detected via sensor OOR. Safe state shall be entered within <200 ms. No tractive effort shall be produced from invalid sensor data. Fault shall be logged with a distinct DTC.

Rationale: A shorted sensor rail makes all sensors read zero/OOR; the system must recognize fault, not "zero throttle."

C-25: +3.3 V MCU Supply Short to Ground

Objective: Verify safe state behavior on MCU supply collapse.

Covered: SG-13 (ASIL D), FSR-14, FSR-15, H-13
Status: Conditional - requires current-limited LV fixture/supply | **Evidence:** -

Procedure:

1. System operating at 50% tractive effort. 3.3 V rail monitored.
2. Apply a controlled short on the 3.3 V rail (current-limited).
3. Observe BOR behavior; if the short is faster than BOR response, observe gate driver behavior independently.
4. Verify breakpoint PWM disable triggers as the supply collapses.
5. Verify watchdog triggers if the CPU stalls.

Acceptance Criteria: At least one safe-state path shall trigger (BOR, watchdog, or breakpoint). PWM shall be disabled. No sustained erratic operation. Key cycle shall be required after short removal.

Rationale: The 3.3 V short is the worst-case supply fault; multiple independent safe-state paths must exist.

C-26: Gate Driver +15 V Supply Short

Objective: Verify NCV57100 UVLO response when a +15 V gate drive supply is shorted.

Covered: SG-12 (ASIL C), SG-14 (ASIL C), FSR-12, FSR-13, H-12, H-16
Status: Executable - Defined (energize-into-fault variant permitted) | **Evidence:** -

Procedure:

1. System operating. Individual gate driver +15 V supplies monitored.
2. Short the +15 V supply of one gate driver (U-phase high-side) to ground via current-limited fixture. (If mid-run shorting is judged hazardous, the short may be bolted on de-energized and the system energized into the fault; record which variant was used.)
3. Observe NCV57100 UVLO trigger. Measure the threshold (typ. 11.3 V).
4. Verify FLT asserted; PWM disabled for that phase; system safe state (not single-phase operation).
5. Repeat for all six gate driver positions.

Acceptance Criteria: UVLO shall trigger at V_{UVLO-} ≈ 11.3 V (±0.5 V). FLT shall be asserted. PWM shall be disabled. Safe state shall be entered. All six positions shall behave consistently. No IGBT damage.

Rationale: Each gate driver has its own isolated +15 V supply; a short must produce FLT + safe state, not phase imbalance.

C-27: Gate Driver −9 V Supply Short

Objective: Verify NCV57100 response when the negative gate drive supply is lost/shorted.

Covered: SG-12 (ASIL C), FSR-12, H-12
Status: Executable - Defined (energize-into-fault variant permitted) | **Evidence:** -

Procedure: As C-26, but short the −9 V supply to ground for each gate driver position.

Acceptance Criteria: Negative supply loss shall be detected. FLT shall be asserted. Safe state shall be entered. No shoot-through shall occur.

Rationale: Loss of the negative rail removes the Miller current return path and risks dv/dt-induced false turn-on.

C-28: Phase U Open Circuit (Motor Disconnect)

Objective: Verify the system shall detect and respond to an open-circuited motor phase.

Covered: SG-08 (ASIL C), FSR-09, H-08
Status: Executable - Defined | **Evidence:** -

Procedure:

1. System operating at 30% tractive effort on dyno, closed-loop FOC.
2. Open Phase U (manual disconnect at the series junction).
3. Observe current readings: Phase U → zero; V/W imbalanced.
4. Verify FSR-02 plausibility detects commanded vs. actual mismatch.
5. Verify safe state entry within <200 ms.
6. Repeat at low speed, high speed, and regen.

Acceptance Criteria: The open phase shall be detected via current imbalance. Safe state shall be entered within <200 ms. No sustained single-phase operation. Fault shall be logged with a specific DTC.

Rationale: FOC cannot maintain control with one phase open; single-phase operation causes severe torque ripple and potential motor damage.

C-29: Phase V Open Circuit

Objective: As C-28 for Phase V.

Covered: SG-08 (ASIL C), FSR-09, H-08
Status: Executable - Defined | **Evidence:** -

Procedure: Identical to C-28, opening Phase V.

Acceptance Criteria: As C-28.

Rationale: All three phases shall be independently validated; detection behavior may differ per phase due to FOC coordinate transform dependencies.

C-30: Phase W Open Circuit

Objective: As C-28 for Phase W.

Covered: SG-08 (ASIL C), FSR-09, H-08
Status: Executable - Defined | **Evidence:** -

Procedure: Identical to C-28, opening Phase W.

Acceptance Criteria: As C-28.

Rationale: As C-29.

C-31: Phase-to-Phase Short (U-V) - Energize-Into-Fault

Objective: Verify DESAT and overcurrent protection respond to a phase-to-phase short circuit.

Covered: SG-12 (ASIL C), SG-14 (ASIL C), FSR-13, H-12, H-16
Status: Executable - Defined | **Evidence:** -

> **METHOD NOTE (NO SHORTING CONTACTOR AVAILABLE):**
>
> This test uses the **energize-into-fault** method. The short is bolted across the phase leads with the system fully de-energized and verified with a DMM. The DC link is then energized via the programmable supply (which provides both the contactor function and current limiting), starting at reduced voltage. Mid-operation short injection is not performed in this campaign (LIMIT-10).

Procedure:

1. De-energize the system. Confirm DC link fully discharged per the pre-charge/discharge protocol.
2. Bolt a low-inductance short between Phase U and Phase V leads. Verify continuity with DMM.
3. Install blast shield. Establish remote supply activation. Clear personnel from the test area. Start video and telemetry recording.
4. Confirm DESAT self-test (C-16) passed on the same day. **If C-16 has not been run within 24 hours, do not proceed.**
5. Energize the DC link at 50 V with the supply current limit set low. Command a single PWM pulse / minimal duty on the shorted phases.
6. Measure DESAT response time (<2 us target), peak current, and soft turn-off on the scope.
7. De-energize. Inspect IGBTs (visual + thermal camera). Verify FLT latched and fault logged.
8. If the protection operated correctly, repeat at stepped voltages (e.g., 75 V, 100 V, 140 V maximum on the 200 V-class board), inspecting after each step.

Acceptance Criteria: DESAT shall trigger within <2 us. Peak current shall be limited by circuit inductance. Soft turn-off shall be observed. No IGBT damage. FLT latched. Safe state entered. System shall require reset.

Rationale: Phase-to-phase short is the most severe inverter fault (H-12). Validates the full chain: DESAT → soft turn-off → FLT → safe state. **WARNING:** even at reduced voltage, fault energy is destructive if protection fails. Remote operation and blast shielding are mandatory.

C-32: Phase-to-Phase Short (V-W) - Energize-Into-Fault

Objective: As C-31 for the V-W phase combination.

Covered: SG-12 (ASIL C), SG-14 (ASIL C), FSR-13, H-12
Status: Executable - Defined | **Evidence:** -

Procedure: Identical to C-31 (energize-into-fault), with the short bolted across V-W. One phase pair is tested at a time; each pair is a separate, complete run with its own evidence set.

Acceptance Criteria: As C-31.

C-33: Phase-to-Phase Short (U-W) - Energize-Into-Fault

Objective: As C-31 for the U-W phase combination.

Covered: SG-12 (ASIL C), SG-14 (ASIL C), FSR-13, H-12
Status: Executable - Defined | **Evidence:** -

Procedure: Identical to C-31 (energize-into-fault), with the short bolted across U-W. One phase pair is tested at a time; each pair is a separate, complete run with its own evidence set.

Acceptance Criteria: As C-31.

Rationale (C-31 to C-33): All three phase-pair combinations shall be independently validated, one pair at a time - never two shorts installed simultaneously.

C-34: Phase-to-DC-Rail Short - Energize-Into-Fault

Objective: Verify protection response when a motor phase is shorted to a DC link rail (DC+ and DC−).

Covered: SG-12 (ASIL C), FSR-13, H-12
Status: Executable - Defined | **Evidence:** -

Procedure:

1. Energize-into-fault method per C-31: bolt the short from the selected phase to the selected rail, de-energized; verify with DMM. One short is installed at a time - never two simultaneously.
2. Energize the DC link at 50 V (stepped up per C-31 only after success).
3. Command a single pulse on the shorted phase: if the high-side IGBT is driven (DC+ case), DESAT shall trigger immediately; if the low-side is driven, a shoot-through path is created through the winding and overcurrent protection shall trigger. The DC− case exercises the complementary paths.
4. De-energize, inspect, verify FLT and fault log.
5. Repeat for the other rail, and for each of the three phases (six configurations total, each a separate run).

Acceptance Criteria: Protection shall trigger within <10 us. No hardware damage at reduced voltage. Safe state entered. Fault logged, for every configuration.

Rationale: Simulates motor winding insulation failure at DC rail potential - a common failure mode (insulation degradation, moisture, mechanical damage). The current path depends on which switch conducts; DESAT or overcurrent monitoring must catch either, for every phase and rail.

C-35: DC Link Capacitor Temperature Monitoring

Objective: Verify DC link capacitor temperature sensing and thermal protection.

Covered: SG-07 (ASIL B), FSR-08 (extended), H-07
Status: Executable - Defined | **Evidence:** -

Procedure:

1. Install temperature sensor(s) on the DC link capacitor bank (if not already present).
2. Operate at various load levels while monitoring capacitor temperature.
3. Apply localized heating (heat gun) to raise capacitor temperature.
4. Verify warning threshold triggers power derate; critical threshold triggers SSO.
5. Verify reading accuracy against an external reference (±5 °C).
6. Verify sensor open/short detection (if applicable).

Acceptance Criteria: Temperature reading accurate to ±5 °C. Warning derate at 90 °C. SSO at 105 °C (capacitor rating limit). Sensor fault shall be detected and cause safe state.

Rationale: Capacitor lifetime halves every ~10 °C; overtemperature risks venting or capacitance loss.

C-36: Bearing Current / Class Y Capacitor Effectiveness

Objective: Validate that Class Y safety capacitors effectively shunt common-mode bearing currents to ground.

Covered: SG-07 (ASIL B, extended), H-07 (indirect - bearing damage leads to mechanical failure)
Status: Deferred - requires shaft voltage brush/coupling fixture | **Evidence:** -

Procedure (reference, for when the fixture is built):

1. System at rated speed and load; motor shaft grounded through insulated coupling on dyno.
2. Measure common-mode voltage at motor terminals (HV differential probe).
3. Measure shaft voltage via carbon brush or capacitive coupling.
4. Calculate bearing voltage ratio (BVR = V_{shaft}/V_{cm}). Target BVR < 0.1 with Class Y caps.
5. Temporarily remove Class Y caps; verify BVR increases significantly (>0.3); reinstall.

Acceptance Criteria: With Class Y caps: BVR < 0.1 and shaft voltage < 1 V peak. Without caps: BVR > 0.3 (confirms effectiveness).

Rationale: PWM common-mode voltage drives bearing EDM currents; Class Y caps protect the motor bearings. Long-term reliability with a safety consequence (bearing failure at speed).

C-39: Flash Bit Rot / Corruption Detection

Objective: Verify boot CRC (FSR-19) detects flash corruption from bit rot, EMI, or wear.

Covered: SG-01 (ASIL D), SG-13 (ASIL D), FSR-19, H-15
Status: Executable - Defined | **Evidence:** -

Procedure:

1. Corrupt a single bit in the safety-critical flash region (debugger).
2. Corrupt multiple bits in the same word.
3. Corrupt calibration data (torque LUT, temperature thresholds).
4. Corrupt the CRC checksum itself (leave code intact).
5. Power cycle after each corruption; observe boot behavior.

Acceptance Criteria: All corruption scenarios shall be detected at boot. PWM enable shall be prevented. The fault shall be logged with distinct DTCs for code vs. calibration corruption. The system shall remain in safe state until reprogrammed.

Rationale: Flash is subject to bit rot, EMI during write, and wear. FSR-19 prevents operating with untrusted code.

C-41: ADC Reference Voltage Drift

Objective: Verify ADC reference stability and detection of reference drift.

Covered: SG-01 (ASIL D), FSR-02, H-01, H-06
Status: Executable - Defined | **Evidence:** -

Procedure:

1. Apply a known precision voltage to one ADC channel (calibration reference).
2. Monitor the ADC reading of the precision reference over the operating temperature range achievable on the bench (ambient to +60 °C via heat gun on the reference area).
3. Verify the reading stays within ±1% of expected.
4. Monitor Vrefint as a proxy for reference stability.
5. Apply external Vref drift and verify FSR-02 plausibility catches the resulting sensor errors.

Acceptance Criteria: ADC reference shall be stable within ±1% over the tested range. Vrefint shall read in the expected range. If Vref drifts beyond ±2%: the plausibility check shall detect the sensor mismatch and enter safe state.

Rationale: Reference drift scales ALL analog readings correlatedly - dangerous because throttle and current sensors misread together. FSR-02 is the primary defense.

C-42: SPI Communication Fault (MAX22530 Isolated ADC)

Objective: Verify the system handles SPI communication failures with the isolated voltage measurement ADC.

Covered: SG-10 (ASIL B), FSR-11, H-10
Status: Executable - Defined | **Evidence:** -

Procedure:

1. System operating with MAX22530 providing DC link voltage readings.
2. Inject SPI faults: SCLK stuck, MISO open, CSN stuck high, corrupted MOSI data.
3. Verify the DC link reading becomes invalid or stale.
4. Verify the system detects loss of valid DC link data and enters safe state.

Acceptance Criteria: SPI fault shall be detected within <200 ms. Safe state shall be entered. No operation with invalid DC link measurement. Fault logged.

Rationale: Operating without DC link voltage visibility risks undetected overvoltage.

C-43: CAN Bus Off State and Recovery

Objective: Verify the system handles CAN bus-off correctly (TEC > 255).

Covered: SG-01 (ASIL D), FSR-17, H-03
Status: Executable - Defined | **Evidence:** -

Procedure:

1. System operating with active CAN communication.
2. Inject CAN errors at high rate to force TEC above 255 (bus-off).
3. Verify bus-off detection and safe-state defaults.
4. Stop error injection. Verify recovery per ISO 11898-1 (128 × 11 recessive bits).
5. Verify normal operation resumes only after valid heartbeats and plausibility checks are restored.

Acceptance Criteria: Bus-off shall be detected. Safe state shall be entered. Recovery shall follow ISO 11898-1. Tractive effort shall not resume until valid heartbeats and plausibility checks are restored.

Rationale: Bus-off must be treated as communication loss with safe defaults.

C-45: IGBT Thermal Runaway Profile

Objective: Verify thermal protection catches IGBT thermal runaway before $T_{j,max}$.

Covered: SG-07 (ASIL B), FSR-08, H-07
Status: Executable - Defined | **Evidence:** -

Procedure:

1. Operate at overload (e.g., 120% rated current with reduced cooling).
2. Monitor both IGBT sensors; compare against junction temperature estimation.
3. Verify progressive derate: 100% → 80% → 50% → 20%.
4. Continue to critical temperature; verify SSO.
5. Verify T_j never exceeds $T_{j,max}$.

Acceptance Criteria: Progressive derate shall be observed. SSO at critical temperature. $T_j < T_{j,max}$ at all times. The 1oo2 arrangement shall work correctly (test with one sensor artificially low).

Rationale: Validates the full thermal protection chain under realistic overload. Derating is pre-fault management; critical threshold crossing produces immediate SSO (Section 2.3).

C-49: PWM Deadtime Verification

Objective: Verify deadtime is always present between complementary switching edges.

Covered: SG-12 (ASIL C), FSR-12, H-17
Status: Executable - Defined | **Evidence:** -

Procedure:

1. Generate PWM at 5%, 50%, 95% duty and multiple switching frequencies.
2. Measure high- and low-side gate signals of one phase.
3. Verify deadtime present on every transition; measure duration vs. programmed value (±10%).
4. Verify no deadtime collapse at extreme duty cycles.
5. Verify breakpoint disable produces simultaneous OFF (not ON).

Acceptance Criteria: Deadtime present on every transition, duration = programmed ±10%. No collapse at any operating point. Breakpoint disable = both OFF simultaneously.

Rationale: Verifies deadtime on the actual gate signals, not just in timer registers. Should be run on every unit.

C-50: Isolation Barrier Verification - Applied-Voltage Leakage Method

Objective: Verify reinforced isolation between the HV DC link and chassis/logic ground.

Covered: SG-09 (ASIL A), FSR-10, H-09
Status: Executable - Defined (alternative method; no megohmmeter/HiPot tester available) |
Evidence: -

> **METHOD NOTE (NO INSULATION TESTER AVAILABLE):**
> Isolation shall be verified by an **applied-voltage leakage measurement**: a known HV potential is applied between DC link negative and chassis through a current-limiting series resistor, and the leakage is computed from the measured voltage drop. This yields a quantitative insulation resistance, passable against the >500 Ω/V criterion of ISO 6469-3. It is not a calibrated megohmmeter measurement and shall be recorded as an alternative method.

Procedure:

1. Test configuration: power-stage-to-chassis only. LV-side electronics with chassis-referenced paths shall be disconnected or the test point chosen so that only the HV-side barrier is stressed (gate driver isolation is rated >5 kV; other LV components are not).
2. Connect the programmable supply between DC− and chassis with a **known HV-rated series resistor** (100 kΩ–1 MΩ) in the loop. The series resistor is both the measurement element and the energy limiter.
3. Set the supply current limit to its minimum before energizing.
4. Apply 1 kV DC. Allow Y-capacitor / EMC-filter charging current to decay; record only the **steady-state** voltage drop across the series resistor. (Note in the record: charging surge is expected and shall not be interpreted as leakage.)
5. Compute insulation resistance R = f(measured drop, series R, applied V). Acceptance: R ≥ 500 Ω/V referred to maximum system voltage (≥100 kΩ for a 200 V-class system; target MΩ-range).
6. Discharge the chassis after the test. Repeat after any short-circuit test (C-31–C-34) as post-fault verification.

Acceptance Criteria: Steady-state leakage shall correspond to insulation resistance ≥500 Ω/V (≥100 kΩ at 200 V class; MΩ-range expected). No breakdown or sustained current rise during application. Post-short-test repeat shall show no degradation.

Safety: 1 kV DC is lethal. The series resistor limits fault energy; nevertheless, no contact during energization, one-hand rule, and mandatory discharge after the test.

Rationale: H-09 is HV shock from isolation failure. Barriers degrade from thermal cycling, humidity, and electrical stress; this measurement verifies barrier integrity quantitatively before and after stress tests.

1.5. System-Level Tests

System-level tests exercise complete end-to-end fault scenarios with all hardware and software running closed-loop FOC control on the dyno.

S-01: Unintended Tractive Effort from Throttle Fault

Objective: Verify SG-01, FSR-01, FSR-03, FSR-18 - the system shall reject unintended tractive effort when the throttle input is implausible.

Covered: SG-01 (ASIL D), H-01, FSR-01, FSR-03, FSR-18
Status: Executable - Defined | **Evidence:** -

Setup: Traction motor on dyno. DC link at nominal voltage. Throttle simulated by dual DC supplies (Section 10.2.1), except step 5 which uses the real assembly.

Procedure:

1. Apply 50% tractive effort request via both channels (matched). Verify corresponding tractive effort.
2. Drive channel 1 to +5 V (short-to-rail). Verify >5% discrepancy detection.
3. Repeat with channel 1 to GND, channel 1 open, and channel 2 slow drift.
4. Using the real throttle assembly: apply 50% on both pots, activate the limit switch. Verify tractive effort commands to zero regardless of pot values.

Acceptance Criteria: All fault injections shall be detected within <100 ms. Tractive effort application rate shall not exceed 500 Nm/s (FSR-03). Safe state shall be entered (immediate SSO per FSR-05). Faults shall be logged with correct DTCs. The limit switch override shall have absolute priority over all pot values.

Rationale: Highest-severity hazard (H-01). Validates the complete chain from sensor fault through detection to safe state entry.

S-02: Unintended Reverse Tractive Effort

Objective: Verify SG-02, FSR-04 - reverse tractive effort shall be rejected when speed > 0.

Covered: SG-02 (ASIL B), H-02, FSR-04
Status: Executable - Defined | **Evidence:** -

Setup: Traction motor spinning forward on dyno.

Procedure:

1. Rotate the motor forward at >100 rpm.
2. Command reverse tractive effort. Verify clamped to zero.
3. Stop (<10 rpm). Command reverse with reverse explicitly selected. Verify permitted.
4. Stop. Command reverse WITHOUT selection. Verify rejected.

Acceptance Criteria: Reverse shall be rejected at >100 rpm. Reverse shall be permitted only when stationary AND selected. All other cases → zero tractive effort, fault logged.

Rationale: The two-condition interlock (stationary + selected) prevents inadvertent reverse from software glitch or sensor fault.

S-03: Sudden Loss of Tractive Effort - Immediate SSO Timing

Objective: Verify SG-03, FSR-05 - on fault, the system shall transition to the torque-free state immediately, within the detection-to-SSO latency budget.

Covered: SG-03 (ASIL C), H-03, FSR-05
Status: Executable - Defined | **Evidence:** -

Setup: Traction motor on dyno at 80% load (high sustained-load operating point). Closed-loop control. Dyno torque transducer recording.

Procedure:

1. Stabilize at 80% rated tractive effort. Record baseline torque.
2. Inject a fault requiring safe state entry (e.g., throttle discrepancy, temperature threshold crossing, CAN timeout).
3. Measure, on the torque transducer and phase-current traces: (a) time from fault injection to detection (DTC assertion), (b) time from detection to measured torque = 0, (c) total injection-to-zero-torque latency.
4. Repeat for a hardware-path fault (DESAT, breakpoint) and record the same latencies.
5. Confirm there is **no** intermediate ramping behavior: torque shall fall monotonically to zero without a software-shaped decay profile.

Acceptance Criteria: Detection-to-SSO latency shall not exceed 200 ms for software-detected faults and <10 us for hardware-path faults (FSR-14). Measured torque shall reach zero without a software-controlled ramp and without a torque overshoot of opposite sign. No re-energization shall occur without key cycle.

Rationale: H-03 is sudden loss of tractive effort at speed. Under the v5.0 safe-state philosophy (Section 2.3) the mitigation is latency minimization, not torque shaping: the sooner the system is verifiably torque-free, the sooner the operator's own controls (brakes, steering) are the only acting forces. This test measures the latency budget end-to-end and confirms the absence of unintended torque during the transition.

S-04: Loss of Tractive Effort Under High-Load Conditions

Objective: Characterize the torque transition and verify immediate-SSO behavior at high sustained load, providing the drive-boundary data for the profile-level residual-risk assessment.

Covered: SG-03 (ASIL C), H-03a, FSR-05
Status: Executable - Defined (vehicle-level validation excluded; LIMIT-01) | **Evidence:** -

Setup: Traction motor on dyno at 60–80% rated tractive effort, high speed. Dyno torque transducer ≥10 kHz bandwidth.

Procedure:

1. Stabilize at the target operating point.
2. Inject a fault requiring safe state entry.
3. Record the torque transition: peak undershoot/overshoot, time to zero, any oscillation.
4. Repeat across the speed/torque envelope including regen-to-motoring boundary proximity.
5. Confirm identical behavior (immediate SSO) at every operating point; confirm no operating point produces a delayed or shaped response.

Acceptance Criteria: At every operating point, the torque transition shall be a single monotonic fall to zero within the FSR-05 latency budget, without opposite-sign overshoot >5% of rated torque and without oscillation. Behavior shall be identical regardless of operating point.

Rationale: H-03a (defined in the applicable profile document) concerns loss of tractive effort in an application-specific operating situation. The dyno cannot replicate application-level dynamics (LIMIT-01); what it can and shall verify is that the drive's contribution to that event - the torque transition itself - is clean, immediate, and operating-point-independent. The operator-level consequence is an accepted residual risk documented in the applicable profile and shall be characterized (not "verified safe") by in-application testing before operational use.

S-05: Uncommanded Regenerative Braking

Objective: Verify SG-05, FSR-06 - uncommanded regenerative braking shall be detected and rejected.

Covered: SG-05 (ASIL C), H-05, FSR-06
Status: Executable - Defined | **Evidence:** -

Setup: Traction motor on dyno in motoring mode; no regen requested.

Procedure:

1. Spin the motor at a mid-range cruising speed; regen request = zero.
2. Inject a software fault commanding negative Id (regen).
3. Verify the FSR-06 monitor response; record detection threshold and time.

Acceptance Criteria: Uncommanded regen >10 Nm shall be detected within <200 ms. Safe state shall be entered (immediate SSO). Friction brakes remain available (independent system).

Rationale: H-05 is unexpected deceleration on a slippery surface. FSR-06 provides the independent monitor.

S-06: Full Load Continuous Operation with Thermal Camera Survey

Objective: Identify all thermal hotspots under sustained full-load operation using infrared thermography.

Covered: SG-07 (ASIL B), FSR-08, H-07 (extended to all components)
Status: Executable - Defined | **Evidence:** -

Setup: Traction motor on dyno. Thermal camera. Emissivity-calibrated targets on key surfaces. Ambient 25 °C with controlled airflow.

Procedure:

1. Apply emissivity tape/paint (ε = 0.95) to: IGBT modules, DC link capacitors, gate driver areas, current sensors, DC/DC converter, MCUs, CAN transceivers, busbars, contactors/relays, motor terminals.
2. Run 25% load 15 min → capture. 50% 15 min → capture. 75% 15 min → capture.
3. 100% rated load for ≥60 min (or thermal steady-state), capturing every 10 min.
4. Record max temperature of every component; flag any exceeding 80% of rated max.
5. Identify unexpected hotspots.

Acceptance Criteria: All component temperatures < 80% of rated max at 100% load steady-state. No unexpected hotspot >10 °C above surroundings. IGBT T_{case} < 100 °C. DC link capacitor < 70 °C. Busbars < 80 °C.

Rationale: Point sensors cannot reveal poor solder joints, current crowding, or bad heatsink contact. Run on the first production-representative unit and after any hardware revision.

S-07: Thermal Cycling - IGBT and DC Link Capacitor (Bench Method)

Objective: Validate thermal protection and mechanical integrity under temperature changes achievable without a chamber.

Covered: SG-07 (ASIL B), FSR-08, FSR-11, H-07, H-10
Status: Executable - Defined (reduced scope: no chamber; cold-start portion Conditional on cold environment) | **Evidence:** -

Procedure:

1. Cold start from the coldest available environment (cold soak outdoors/unheated space in winter, or freezer for the unpowered control PCB only - record actual soak temperature).
2. Ramp to full load while monitoring IGBT temperature rise.
3. Verify temperature sensors read correctly at low temperature.
4. Rapid transition: full load hot (>80 °C) → shutdown → immediate restart. Verify no false fault.

5. Repeat 10 thermal cycles: cold → full-load hot → cooldown. Monitor for degradation (thermal resistance trend via camera + sensors).

Acceptance Criteria: System shall start from the documented cold-soak temperature. Temperature readings shall remain plausible across the range. No false faults during thermal shock. No measurable thermal-resistance increase after 10 cycles.

Rationale: Thermal cycling stresses solder joints and substrates via CTE mismatch. This is a screening test; extended cycling (500+ cycles) and controlled −20 °C soak are part of the deferred E-series (E-04–E-06).

S-08: Regenerative Braking at Maximum Power

Objective: Verify the regen system handles maximum regen power without overvoltage or instability.

Covered: SG-05 (ASIL C), SG-10 (ASIL B), FSR-06, FSR-11, H-05, H-10
Status: Executable - Defined | **Evidence:** -

Setup: Traction motor driven by the 4-quadrant dyno at maximum rated speed. DC link supply in sink mode (bidirectional ±50 A) absorbing regen power.

Procedure:

1. Spin the motor at rated speed via dyno.
2. Apply maximum regen torque command.
3. Monitor DC link voltage; verify it stays below the warning threshold.
4. Increase regen until the warning threshold; verify regen limiting.
5. Verify the system limits regen to what the DC link sink can accept.
6. Verify smooth torque transition into and out of regen (no oscillation).
7. Repeat at multiple speeds including field-weakening.

Acceptance Criteria: DC link voltage stable during max regen. No overvoltage events. Regen smoothly limited at sink capacity. No torque oscillation. All temperature limits respected.

Rationale: Max regen is the worst case for H-10 and stresses the H-05 monitor. Field-weakening regen is particularly challenging (back-EMF > bus voltage).

S-09: Field Weakening Region Operation

Objective: Verify stable operation above base speed.

Covered: SG-06 (ASIL C), FSR-07, H-06
Status: Executable - Defined | **Evidence:** -

Procedure:

1. Operate at base speed, rated torque.
2. Increase speed above base speed; verify field-weakening transition.
3. Verify torque derate above base speed ($T \propto 1/\omega$).
4. Operate at max field-weakening speed for 10 min.
5. Verify current does not exceed rated value; verify thermal limits.

Acceptance Criteria: Smooth transition. Correct torque derate. No current overshoot. Stable at max speed. Temperatures within limits.

Rationale: Incorrect Id control in field weakening risks overcurrent (H-06) or loss of current control.

S-10: Startup Sequence Validation

Objective: Verify correct sequence from key-on to ready-to-drive.

Covered: SG-13 (ASIL D), FSR-16, H-13
Status: Executable - Defined | **Evidence:** -

Setup: Complete system with DC link supply, CAN1 source-node simulator (when applicable), IO board simulator.

Procedure:

1. System fully powered down, DC link discharged.
2. Key ON. Verify sequence: (a) boot, (b) POST, (c) pre-charge, (d) DC link >95%, (e) gate driver self-test, (f) encoder validation, (g) CAN established, (h) READY.
3. Time each phase. Total key-on to READY < 5 s.
4. Verify tractive effort NOT available before READY.
5. Inject a fault during each phase; verify abort to safe state.

Acceptance Criteria: Sequence shall execute in correct order every time. Tractive effort shall be available only in READY. A fault at any phase shall abort to safe state. Total startup < 5 s.

Rationale: Startup transitions from unpowered to HV-active; any fault must prevent READY.

S-11: Shutdown Sequence Validation

Objective: Verify safe shutdown from any operating state.

Covered: SG-13 (ASIL D), FSR-05, H-13
Status: Executable - Defined | **Evidence:** -

Setup: System operating at various load levels on dyno.

Procedure:

1. Operate at 100% load. Key OFF. Verify: (a) immediate SSO (PWM disabled; torque to zero per FSR-05), (b) gate driver supplies disabled, (c) DC link remains on the external discharge path per service procedure (no onboard bleeder).
2. Repeat at 50% load, 25% load, and regen mode.
3. Verify key-off is treated as an immediate-SSO event (no torque shaping required; the operator's deceleration intent is handled by the normal throttle-release path, not by key-off).
4. Verify restart is impossible without a full key cycle (OFF → ON).

Acceptance Criteria: Safe shutdown from all operating points. No tractive effort after key-off. Restart shall require a full key cycle.

Rationale: Incorrect shutdown (DC link not discharged per procedure = shock hazard; PWM active after key-off = unexpected torque) creates immediate danger. HV contactor sequencing is BMS-domain and out of scope. Note: normal operator-intended deceleration is a *control* function (throttle release, FSR-03 rate limit) and is distinct from fault/shutdown response, which is immediate SSO.

S-12: Key-Cycle Stress Test

Objective: Verify reliability of startup/shutdown cycling over many repetitions.

Covered: SG-13 (ASIL D), FSR-16, H-13
Status: Executable - Defined | **Evidence:** -

Procedure:

1. Automated key cycle: ON (5 s) → OFF (5 s) → repeat, 1000 cycles.
2. Log every POST result, startup time, and fault.
3. After 1000 cycles: run functional tests C-01 through C-05 and compare against baseline.

Acceptance Criteria: 1000 cycles with zero failures. All POST passes. Startup time variation < 10%. No functional degradation.

Rationale: Life-test screening for DC link capacitor, gate-driver supply, connector, and flash wear (infant mortality). HV contactor wear is source-side / OEM-domain and out of scope.

S-13: Power Dip Ride-Through

Objective: Verify the system survives brief DC link interruptions without unsafe behavior.

Covered: SG-03 (ASIL C), FSR-05, FSR-11, FSR-21, H-03
Status: Executable - Defined | **Evidence:** -

Setup: System on dyno. Programmable DC link supply with interruption capability.

Procedure:

1. System at 50% load.

2. Interrupt DC link for 1 ms. Verify ride-through (capacitors hold the bus).
3. Interrupt for 10 ms. Verify UV detection and immediate SSO (FSR-05/FSR-21).
4. Interrupt for 100 ms. Verify SSO; verify no restart without key cycle.
5. Repeat at 25%, 75%, 100% load; repeat during regen.

Acceptance Criteria: Short dips (<5 ms): ride-through. Longer dips: immediate SSO (no torque shaping). No erratic behavior at any dip duration. Capacitor energy sufficient for safe shutdown sequencing.

Rationale: Power interruptions come from loose terminals, contactor bounce, load dump. Validates capacitor sizing and the UV response boundary.

S-14: Reverse Tractive Effort at Standstill

Objective: Verify reverse functions correctly when explicitly requested at standstill.

Covered: SG-02 (ASIL B), FSR-04, H-02
Status: Executable - Defined | **Evidence:** -

Procedure:

1. Motor stationary (<10 rpm), reverse selected.
2. Apply 25% reverse request; verify backward rotation at expected speed.
3. Apply 50%; verify stable operation.
4. Deselect reverse while moving backward; verify tractive effort to zero.
5. Select reverse while spinning forward; verify rejection until <10 rpm.

Acceptance Criteria: Reverse only when stationary AND selected. Tractive effort proportional to request. Rejection while moving forward. Clean transitions.

Rationale: Positive test for reverse (complement to S-02).

S-15: Overspeed Protection

Objective: Verify the system limits maximum motor speed.

Covered: SG-06 (ASIL C), FSR-07, H-06
Status: Executable - Defined | **Evidence:** -

Procedure:

1. Command acceleration toward rated max speed; verify the limit is enforced.
2. Attempt to exceed the limit with dyno forcing; verify the system resists (regen if needed).
3. Verify encoder-derived speed agrees with back-EMF-derived speed.
4. Verify overspeed fault logging.

Acceptance Criteria: Speed shall not exceed the programmed limit by >5%. Tractive effort shall be reduced (controlled enforcement, not SSO - overspeed approach is a control function; limit violation beyond the enforcement band → SSO). Overspeed fault logged. No mechanical damage.

Rationale: Rotor overspeed risks mechanical burst. The limit must hold even under external forcing (downhill, tow).

S-16: Modulation Scheme Transition During Acceleration - Torque Blip

Objective: Verify modulation scheme transitions do not produce perceptible torque disturbances during acceleration. Transition gating logic shall inhibit switches during high di/dt.

Covered: SG-03 (ASIL C), FSR-05, H-03, H-03a
Status: Executable - Defined | **Evidence:** -

Setup: Dyno with high-bandwidth torque transducer (≥10 kHz). DC link nominal. Automatic modulation map with ≥3 adjacent schemes.

Procedure:

1. Command smooth acceleration through the transition speed range.
2. Record torque at ≥20 kSPS during each transition.
3. Measure peak deviation from pre-transition mean.
4. Repeat with manual scheme switch via RTE during hard acceleration (>80% request).
5. Verify gating rejects/delays the manual switch during high di/dt.
6. Repeat at available temperature extremes (heat gun assisted; record actual conditions).

Acceptance Criteria: Automatic transitions shall produce <2% peak torque deviation. Manual switches during hard acceleration shall be gated or produce <5% deviation. No fault trips during transitions.

Fail Criteria: Deviation >5% on automatic transition; ungated manual switch with perceptible blip; false fault trip.

Rationale: Abrupt torque change of any origin degrades to H-03/H-03a. Bumpless crossfade and di/dt gating prevent transition disturbances from becoming hazards. (This test concerns *control* torque smoothness, not fault response; it is unaffected by the FSR-05 immediate-SSO philosophy.)

S-17: Modulation Scheme Transition During Regenerative Braking - Torque Blip

Objective: Verify modulation transitions during regen do not produce torque disturbances; FSR-06 shall not false-trip on legitimate transitions.

Covered: SG-05 (ASIL C), FSR-06, H-05, H-03
Status: Executable - Defined | **Evidence:** -

Setup: Dyno in speed-control mode driving the DUT into regen. High-bandwidth torque transducer.

Procedure:

1. Establish steady-state regen at 50% rated regen torque.
2. Command a scheme switch via RTE during active regen.
3. Record torque during the transition.
4. Ramp dyno speed through the automatic map boundary during regen.
5. Verify behavior at the regen/motoring zero-torque crossing.
6. Verify FSR-06 does not false-trip during legitimate transitions.

Acceptance Criteria: Torque deviation during regen transition <3% of rated. No FSR-06 false trip on legitimate transitions. Zero-torque crossing clean (no direction ambiguity).

Fail Criteria: Blip >5%; FSR-06 false trip; direction ambiguity at zero crossing.

Rationale: A badly managed transition during regen feels like uncommanded braking (H-05). FSR-06 must distinguish control transitions from faults.

S-18: Hysteresis at Modulation Scheme Boundary - No Jitter

Objective: Verify hysteresis prevents rapid back-and-forth switching near a scheme boundary.

Covered: SG-03 (ASIL C), H-03
Status: Executable - Defined | **Evidence:** -

Procedure:

1. Operate just below a speed-based boundary (e.g., 78% of base speed, boundary at 80%).
2. Introduce ±2% speed oscillation at 1 Hz via dyno.
3. Count scheme switches over 60 s.
4. Repeat just above the boundary; repeat with hysteresis at 1% and 10%.
5. Verify no audible jitter.

Acceptance Criteria: With default 5% hysteresis: zero switches during ±2% oscillation. With 1% hysteresis: ≤1 switch per 10 s. No audible jitter.

Fail Criteria: >1 switch/second at default hysteresis; audible jitter; torque ripple correlated with switching.

Rationale: Boundary chatter is a chronic H-03 degradation - micro-disturbances eroding control and confidence.

S-19: Full Modulation Map Traversal - End-to-End

Objective: Verify the complete automatic modulation map across all regions with no dead zones, wrong selections, or fault trips.

Covered: SG-03 (ASIL C), H-03, H-03a, H-05
Status: Executable - Defined | **Evidence:** -

Procedure:

1. Program the full map (0 to field-weakening max; zero to rated torque, motoring and regen).
2. Slow speed sweep (1% base speed/s) at constant 50% torque; record active scheme, torque, bus voltage.
3. Verify correct scheme per region; verify clean transitions (<2% deviation, no trips).
4. Repeat at 25% and 75% torque; repeat in deceleration direction.

Acceptance Criteria: Correct scheme in every region. All transitions clean. No fault trips. Identical behavior accelerating and decelerating.

Fail Criteria: Wrong scheme in any region; transition fault trip; >5% deviation; directional asymmetry.

Rationale: Integration test for the multi-modulation subsystem; catches map programming errors and boundary interactions.

1.6. Integration Tests

Tests referencing a CAN1 source management node (I-01, I-15, and related) apply when such a node (e.g., a BMS) is present in the application; the platform does not assume one.

Integration tests validate the interaction between the control module and external systems via CAN and discrete I/O, using CAN simulation.

I-01: CAN1 Source Management Node Heartbeat Loss

Objective: Verify FSR-17 - loss of the CAN1 source management node (when present) shall trigger safe degradation.

Covered: SG-01 (ASIL D), H-03, FSR-17
Status: Executable - Defined | **Evidence:** -

Procedure:

1. Normal CAN1 communication, source-node simulator heartbeat every 5 s.
2. Stop the heartbeat.
3. Measure time from last heartbeat to safe state entry.
4. Verify safe-state defaults: tractive effort restricted to zero.

Acceptance Criteria: Safe state shall be entered within 5 s + margin (<6 s total). Tractive effort shall go to zero (immediate SSO on timeout per FSR-05). Fault logged. No operation without BMS data.

Rationale: Operating without source management data risks using a faulted DC source. Validates response to loss of this external node when present.

I-02: CAN2 (IO Board) Heartbeat Loss

Objective: Verify FSR-17 - IO board CAN loss shall trigger safe-state defaults.

Covered: SG-01 (ASIL D), H-03, FSR-17
Status: Executable - Defined | **Evidence:** -

Procedure:

1. IO board simulator heartbeat every 1 s (brake=off, kickstand=up, valid).
2. Stop the heartbeat.
3. Measure time to safe state entry.
4. Verify defaults: brake=pressed, kickstand=down, external inputs invalid.

Acceptance Criteria: Safe state shall be entered within <1.5 s. Tractive effort zero. Fault logged. Defaults correctly applied (either default alone prevents tractive effort).

Rationale: The IO board provides real-time safety interlocks; its loss must assume worst-case state.

I-03: Simultaneous Throttle + Brake Request

Objective: Verify SG-01, FSR-01, FSR-18 - brake request shall always override throttle.

Covered: SG-01 (ASIL D), H-01, FSR-01, FSR-18
Status: Executable - Defined | **Evidence:** -

Procedure:

1. Apply 75% tractive effort (both channels valid, matched).
2. Set IO board brake=pressed while maintaining throttle. Verify tractive effort commands to zero.
3. Release brake. Verify tractive effort returns, ramped per FSR-03 (no step).
4. Repeat with kickstand=down.

Acceptance Criteria: Brake or kickstand shall immediately override throttle. Tractive effort zero within <100 ms. On release, re-application rate ≤500 Nm/s (FSR-03). Kickstand-down-at-speed shall be fault-logged.

Rationale: Brake input is the operator's last-resort override. Re-application rate limiting is a control function (unaffected by the immediate-SSO fault philosophy).

I-04: HVIL Interruption During Operation

Objective: Verify SG-09, FSR-10 - HVIL interruption shall trigger the VCU-side HV disconnect response.

Covered: SG-09 (ASIL A), FSR-10, H-09
Status: Executable - Defined | **Evidence:** -

Procedure:

1. System at 50% tractive effort, HVIL closed.
2. Open the HVIL loop.
3. Measure time from HVIL open to PWM disable.
4. Verify contactor open request on CAN1 within <50 ms.
5. Verify PWM is not re-enabled until HVIL restored AND key cycle.

Acceptance Criteria: PWM disabled within <50 ms. Contactor open request sent. Safe state entered. No tractive effort after HVIL open. Latch clears only on key cycle.

Rationale: HVIL is the primary HV interlock. The VCU-side obligations are PWM disable and the contactor open request; contactor actuation itself is BMS/OEM-domain. The latch prevents automatic re-energization into a persisting fault.

I-05: DC Link Overvoltage (Regen Event)

Objective: Verify SG-10, FSR-11 - DC link overvoltage shall be detected and limited.

Covered: SG-10 (ASIL B), H-10, FSR-11
Status: Executable - Defined | **Evidence:** -

Procedure:

1. Regen mode, DC link nominal (dyno driving; supply sinking).
2. Raise DC link toward the warning threshold; verify regen disable.
3. Continue to critical threshold (≤175 V); verify SSO within <50 ms.

Acceptance Criteria: Regen disabled at warning. SSO at critical within <50 ms. Distinct DTCs. No IGBT damage.

Rationale: Validates both OV thresholds and response times (complements C-10 at the integration level).

I-06: Kickstand Down at Speed

Objective: Verify safe response to kickstand-down while moving.

Covered: SG-01 (ASIL D), H-01 (indirect), FSR-17
Status: Executable - Defined | **Evidence:** -

Procedure:

1. System at 50% tractive effort; IO board reports kickstand=up; speed above the low-speed threshold.
2. IO board reports kickstand=down.
3. Verify tractive effort commands to zero immediately.
4. Verify fault logged; verify tractive effort inhibited while kickstand=down regardless of throttle.

Acceptance Criteria: Tractive effort zero within <200 ms. Fault logged. Inhibition persists until key cycle.

Rationale: Riding with the kickstand down is dangerous; the interlock must override any throttle position.

I-07: Simultaneous Multiple CAN Node Loss

Objective: Verify graceful degradation when multiple external systems fail simultaneously.

Covered: SG-01, SG-03, FSR-17
Status: Executable - Defined | **Evidence:** -

Procedure:

1. All CAN nodes active.
2. Simultaneously stop all CAN2 heartbeats. Verify safe state on the 1 s timeout.
3. Restore CAN2; verify return only after key cycle.
4. Stop both CAN1 and CAN2 heartbeats. Verify safe state on the first timeout to fire.

Acceptance Criteria: Safe state on the first timeout. No tractive effort during any CAN-loss scenario. No auto-recovery. All faults logged.

Rationale: Crash/EMI can kill multiple nodes at once; the most restrictive timeout must dominate.

I-08: CAN Bus Fuzzing - Random Frame Injection

Objective: Verify the system ignores or gracefully handles random/corrupted CAN frames.

Covered: SG-01 (ASIL D), FSR-17, H-01, H-15
Status: Executable - Defined | **Evidence:** -

Procedure:

1. Inject random frames at 10% bus load: random IDs (including source node/IO board IDs), random DLC, random payload.
2. Verify no malfunction, no tractive effort change, no spurious safe state.
3. Increase to 50% bus load; verify continued normal operation.
4. Inject valid-ID frames with corrupted CRC; verify controller rejection.

5. Inject valid source node ID with impossible payload (cell voltage 0xFFFF, temp 200 °C); verify sanity rejection.

Acceptance Criteria: No malfunction from random frames. Valid heartbeats still processed. Impossible values rejected. Bus load <100% maintained.

Rationale: Validates input validation and parser robustness against noise, failed nodes, or injection (H-15).

I-09: CAN Bus Load Test (95% Utilization)

Objective: Verify correct operation at maximum bus load.

Covered: SG-01 (ASIL D), FSR-17, H-03
Status: Executable - Defined | **Evidence:** -

Procedure:

1. Load the bus to 95% with background traffic.
2. Verify VCU transmits without excessive delay (<10 ms jitter).
3. Verify critical messages received without drops.
4. Verify heartbeat timeout accuracy (no false timeouts from congestion).
5. Inject a fault requiring safe state; verify entry is not delayed by bus load.

Acceptance Criteria: Normal operation at 95% load. No dropped critical messages. Timeout accuracy ±10%. Safe state entry not delayed.

Rationale: Bus load spikes during fault storms; critical reception must survive congestion.

I-10: CAN Bus Off Recovery

Objective: Verify correct recovery from bus-off.

Covered: SG-01 (ASIL D), FSR-17, H-03
Status: Executable - Defined | **Evidence:** -

Procedure:

1. Force bus-off (TEC > 255) via error injection.
2. Verify safe state and defaults.
3. Stop injection; allow idle recovery (128 × 11 recessive bits).
4. Verify recovery to error-active per ISO 11898-1.
5. Verify NO auto-resume; key cycle; verify normal operation.

Acceptance Criteria: Bus-off detected. Safe state entered. Recovery per ISO 11898-1. No auto-resume. Key cycle restores operation.

Rationale: Complements C-43 at the integration level.

I-11: Invalid/Corrupted CAN Frame Injection

Objective: Verify handling of valid-ID, semantically invalid data.

Covered: SG-01 (ASIL D), SG-10 (ASIL B), FSR-17, H-15
Status: Executable - Defined | **Evidence:** -

Procedure:

1. Source node frame with impossible value (e.g., cell voltage >5 V or <0 V): verify rejection → last-known-good or safe default.
2. Source node temperature = −50 °C: verify rejection.
3. IO board brake=pressed AND throttle=100%: verify brake wins.
4. IO board kickstand=down AND speed=high: verify zero tractive effort + fault.
5. DLC mismatch frames: verify safe parser handling.

Acceptance Criteria: All invalid frames rejected. Safe defaults used when valid data unavailable. No tractive effort from invalid inputs. DLC mismatch handled safely.

Rationale: Semantically invalid data passes CRC/ID filters - range, plausibility, and consistency checks are required.

I-12: Display Node Failure

Objective: Verify safe operation when the display node fails.

Covered: SG-01 (ASIL D), FSR-17, H-03
Status: Executable - Defined | **Evidence:** -

Procedure:

1. Normal operation with display active.
2. Stop display heartbeat.
3. Verify continued operation (display non-safety-critical); verify non-critical fault log.
4. Verify tractive effort unaffected; verify display recovery needs no key cycle.

Acceptance Criteria: Display loss shall NOT affect tractive effort or safety functions. Fault logged. Recovery without key cycle.

Rationale: Heartbeat handling must distinguish safety-critical nodes (source management, IO) from informational nodes (display).

I-13: Charger Node Interaction

Objective: Verify drive-away prevention while charging.

Covered: SG-01 (ASIL D), FSR-04, H-01
Status: Executable - Defined | **Evidence:** -

Procedure:

1. Charger connected and active; verify VCU detects charging state.
2. Attempt tractive effort while charging; verify rejection.
3. Verify interlock: charging active → tractive effort disabled.
4. Charger completion message; verify exit from charging state.
5. Verify tractive effort available after disconnect confirmation.
6. Inject stuck "active" charger message after physical disconnect; verify timeout clears the state.

Acceptance Criteria: No tractive effort during charging. Clean exit from charging state. Timeout for stuck charger message. Drive-away prevention functional.

Rationale: Driving away connected is a severe hazard; the interlock must be unconditional.

I-14: ABS Node Coordination

Objective: Verify correct interaction with ABS during anti-lock events.

Covered: SG-05 (ASIL C), FSR-06, H-05
Status: Executable - Defined | **Evidence:** -

Procedure:

1. System in regen. ABS simulator sends "ABS active."
2. Verify immediate regen reduction/disable.
3. Verify friction brakes unaffected.
4. ABS inactive; verify smooth regen resume.
5. Verify no tractive effort during ABS active.

Acceptance Criteria: Regen disabled/reduced within <50 ms of ABS active. Smooth resume on inactive. No interference with friction brakes.

Rationale: Regen torque can fight ABS slip control; the VCU must yield during ABS events.

I-15: Source Management Node Fault Propagation

Objective: Verify correct VCU response to source management node (e.g., BMS) fault messages, when such a node is present.

Covered: SG-01 (ASIL D), SG-10 (ASIL B), FSR-17, H-01, H-10
Status: Executable - Defined | **Evidence:** -

Procedure:

1. Source node warning (e.g., cell imbalance >50 mV): verify log + derate.
2. Source node critical (e.g., cell OV >4.25 V): verify immediate regen disable + safe state.
3. Source node critical (e.g., cell UV <2.5 V): verify immediate safe state.
4. Source node critical (e.g., over-temp >60 °C): verify derate or safe state.
5. Source node sends a contactor-weld-detected message (weld detection itself is source-side / OEM-domain): verify the VCU logs a fatal fault and locks out restart.

Acceptance Criteria: Warnings: log + derate. Critical faults: safe state within <200 ms (immediate SSO). Weld-detected message: fatal log + lockout. Responses appropriate to severity.

Rationale: The source management node is authoritative for DC source safety; a critical fault must never be treated as a warning.

I-16: Multi-Node Simultaneous Fault

Objective: Verify deterministic handling of simultaneous multi-node faults.

Covered: SG-01 (ASIL D), SG-03 (ASIL C), SG-13 (ASIL D), FSR-17, H-01, H-03, H-13
Status: Executable - Defined | **Evidence:** -

Procedure:

1. System at 50% tractive effort.
2. Simultaneously: source node critical fault AND IO heartbeat stop AND ABS active.
3. Verify safe state (most restrictive response), not delayed by multi-fault processing.
4. Verify all three faults logged with correct DTCs.
5. Repeat with different combinations. Include coprocessor-observed anomalies (CAN snoop disagreement) in one run.

Acceptance Criteria: Safe state within the single worst-case timeout (not cumulative). All faults logged. No priority inversion.

Rationale: Fault handling must be deterministic under compound faults.

I-17: CAN Bus Wiring Fault (Short and Open)

Objective: Verify response to physical CAN wiring faults.

Covered: SG-01 (ASIL D), FSR-17, H-03
Status: Executable - Defined | **Evidence:** -

Procedure:

1. Short CAN_H to CAN_L: verify bus-off and safe state.
2. Restore; verify recovery.

3. Open CAN_H: verify error-passive → bus-off → safe state.
4. Restore; verify recovery.
5. Short CAN_H to +12 V: verify transceiver protection and safe state.
6. Short CAN_L to ground: verify safe state.

Acceptance Criteria: All wiring faults detected. Safe state within timeout. No transceiver damage. Recovery after restore (key cycle required).

Rationale: Chafing, corrosion, and crash damage are common; communication loss must produce safe state.

I-18: Wake/Sleep Cycle Test

Objective: Verify correct wake-from-sleep and sleep-entry behavior.

Covered: SG-13 (ASIL D), FSR-16, H-13
Status: Executable - Defined (if sleep/wake implemented; otherwise N/A - record as not applicable) | **Evidence:** -

Procedure:

1. Trigger sleep (key off / inactivity). Verify graceful shutdown before sleep entry.
2. Verify sleep quiescent current (<1 mA typical).
3. Trigger wake (key on, CAN wake, charger connection). Verify full startup sequence.
4. Verify no stale data after wake.

Acceptance Criteria: Graceful sleep entry. Sleep current within limit. Full POST on wake. No stale data. Behavior identical to cold start.

Rationale: Wake must be a fresh start; stale pre-sleep fault data must not mask faults.

1.7. Environmental and Stress Tests (E-Series) - DEFERRED

> **STATUS: ALL E-SERIES TESTS ARE DEFERRED - TYPE TESTS.**
>
> The project does not currently have access to a thermal chamber, humidity chamber, vibration table, EMC chamber, ESD gun, or water spray rig. The E-series is retained in summary form as the reference plan for a future type-test campaign (external lab or acquired equipment). **E-series tests shall not be cited as coverage for any Safety Goal, FSR, or hazard in the current campaign**; where earlier revisions of this document cited them in the traceability matrices, those citations are removed in v5.0 and the corresponding residual risk is carried in Section 10.10 (LIMIT-02, LIMIT-09).

Table 13 - Environmental Test Stubs (Reference Plan)

ID	Test	Standard Reference	Sta
E-01	Random vibration - operating (10–1000 Hz, 5 g RMS, 8 h/axis)	ISO 16750-3	De
E-02	Sinusoidal vibration sweep - resonance search	ISO 16750-3	De
E-03	Mechanical shock (50 g, 11 ms half-sine)	ISO 16750-3	De
E-04	High temperature soak (+60 °C operating)	ISO 16750-4	De
E-05	Low temperature soak (−20 °C cold start)	ISO 16750-4	De
E-06	Thermal shock (−20 °C ↔ +60 °C, 20 cycles)	ISO 16750-4	De
E-07	High humidity operation (85% RH, 40 °C, 48 h)	ISO 16750-4	De
E-08	Radiated EMI immunity (20 MHz–6 GHz, 100 V/m)	ISO 11452-2	De
E-09	Conducted EMI immunity (BCI, 1–400 MHz)	ISO 11452-4	De
E-10	ESD - contact discharge (±4/6/8 kV)	ISO 10605	De
E-11	ESD - air discharge (±4/8/15 kV)	ISO 10605	De
E-12	Water ingress (IPX4/X5/X6; target IP54 min)	IEC 60529	De

1.8. Safety Goal Traceability

The following matrices map safety goals, FSRs, and hazards to test cases. Only **executable or conditional** tests are cited as coverage in the current campaign; deferred tests (E-series, C-36) are excluded from coverage claims. Upon execution, the evidence reference (Section 10.2.3) shall be entered against each test.

Table 14 - Safety Goal to Test Case Traceability

SG	Target	Safety Goal
SG-01	D	Prevent unintended positive tractive effort
SG-02	B	Prevent unintended reverse tractive effort
SG-03	C	Immediate torque-free state on fault; detection-to-SSO ≤200 ms
SG-04	A	Ensure regen availability (friction brakes backup)
SG-05	C	Prevent unintended regenerative braking
SG-06	C	Limit max tractive effort to calibrated max
SG-07	B	Detect over-temperature, progressively derate
SG-08	C	Detect loss of rotor position → safe state
SG-09	A	Maintain HV isolation
SG-10	B	Detect DC link bus overvoltage
SG-12	C	Prevent IGBT shoot-through
SG-13	D	Achieve safe state within 200 ms, independent of main loop and generated code
SG-14	C	Detect gate driver fault
SG-15	C	Detect PWM deadtime violations

1.8.1. FSR Coverage Matrix

Table 15 - Functional Safety Requirement Coverage by Test Cases

FSR	Requirement Summary
FSR-01	Dual throttle discrepancy >5% → safe state
FSR-02	Command vs. measured current plausibility
FSR-03	Tractive effort application rate limit ≤500 Nm/s
FSR-04	Reverse interlock (stationary + selected)
FSR-05	Immediate SSO on fault; detection-to-SSO ≤200 ms
FSR-06	Uncommanded regen >10 Nm → safe state
FSR-07	Max tractive effort limit (LUT on both MCUs + dual-MCU current monitoring)
FSR-08	2× IGBT NTC (1oo2) + 1× DC link capacitor NTC (capacitor channel: derate 90 °C, SSO 105
FSR-09	Encoder loss → safe state <100 ms
FSR-10	HVIL → PWM disable + contactor request <50 ms
FSR-11	DC link OV: regen disable / SSO
FSR-12	Gate driver complementary inputs
FSR-13	DESAT <2 us PWM disable
FSR-14	Breakpoint HW PWM disable <10 us
FSR-15	Windowed watchdog ≤50 ms
FSR-16	POST
FSR-17	CAN heartbeat timeout with safe defaults
FSR-18	Throttle limit switch independent override
FSR-19	Boot CRC-32
FSR-20	ECC RAM SECDED; double-bit → safe state
FSR-21	DC link UV derate / safe state
FSR-22	Generated code cannot affect safety mechanisms

1.8.2. Hazard Coverage Matrix

Table 16 - Hazard Coverage by Test Cases

Hazard	Description	Covering
H-01	Unintended positive tractive effort	C-01–C-0
H-02	Unintended reverse tractive effort	S-02, S-1
H-03	Sudden loss of tractive effort	C-22, S-0
H-03a	Loss of tractive effort in an application-specific situation (see profile documents)	S-04 (driv
H-04	Inability to produce regen	S-08 (ind
H-05	Uncommanded regenerative braking	S-05, S-0
H-06	Excessive tractive effort	C-06, C-0
H-07	Over-temperature	C-08, C-3
H-08	Motor overspeed / encoder loss	C-09, C-2
H-09	HV isolation failure	C-50, I-04
H-10	DC link bus overvoltage	C-10, C-4
H-12	IGBT shoot-through	C-15, C-1
H-13	Failure to execute safe state	C-13, C-1
H-14	Corrupted/latched tractive effort	C-13, C-1
H-15	Incorrect tractive effort from software error	C-06, C-0
H-16	Gate driver fault not acted upon	C-15, C-1
H-17	PWM deadtime violation / stuck-on	C-15, C-1

1.9. Pass/Fail Criteria

All test cases use the following standardized definitions. A test is **PASSED** only when all applicable criteria are met. A test is **FAILED** if any criterion is not met.

Table 17 - Test Pass/Fail Criteria Definitions

Criterion	Pass Definition
Safe State Entry	System enters the defined safe state (immediate SSO, zero tractive effort) within tl
Detection Time	Fault detected and logged within the specified limit. DTC recorded with correct coc
Torque Transition	On fault/shutdown: torque falls monotonically to zero within the FSR-05 latency bu
HW Response	Hardware protection (DESAT, breakpoint, watchdog) responds within the specified
Latching	Fault remains latched until key cycle or explicit reset. No automatic restart.
Logging	Fault recorded in non-volatile memory (FRAM). DTC matches fault type. Timestam
No Degradation	Behavior outside the fault path unaffected; other safety functions remain operation

1.9.1. Overall Test Plan Assessment

Table 18 - Overall Test Plan Assessment Criteria

Assessment	Definition
ALL TESTS PASSED	Every executed test achieves PASS on all criteria. All safety goals an
PASSED WITH EXCEPTIONS	All critical tests (P0-gap coverage) pass. Minor tests may fail with doc
FAILED - NOT ROADWORTHY	Any P0-gap test fails (throttle monitoring, safe state entry, watchdog r
INCONCLUSIVE	Tests could not be executed (equipment/environment). Results insuffi

1.10. Known Test Limitations

LIMIT-01: VEHICLE/APPLICATION-LEVEL DYNAMICS BEYOND THE DYNO

LIMITATION:

S-04 verifies the drive-boundary torque transition on a dyno but cannot replicate application-level vehicle dynamics. The interaction between abrupt tractive effort removal and the driven vehicle's dynamics can only be characterized in the final application.

V5.0 NOTE:

With the removal of software ramp-down (Section 2.3), the abrupt-torque-loss event is an **accepted residual risk**, not a mitigated one. In-application testing under this limitation is re-purposed: its objective is to *characterize* operator-level consequences and validate the controllability classification of the applicable profile, not to verify a ramp rate.

MITIGATION:

(1) S-04 verifies the torque transition is clean, immediate, and operating-point-independent. (2) In-application characterization with graduated operating points and known fault injection, per the applicable profile.

LIMIT-02: ENVIRONMENTAL STRESS (TEMPERATURE, VIBRATION, EMI)

LIMITATION:

Component and system tests are conducted at ambient on the bench. The E-series (thermal, vibration, humidity, EMC, ESD, ingress) is deferred - no environmental equipment is available (Section 10.2.2).

MITIGATION:

(1) Gate drivers automotive-qualified (AEC-Q100) for temperature. (2) S-07 bench thermal-cycling variant provides partial screening. (3) EMC and environmental type testing required before production; documented as open residual risk for field use.

LIMIT-03: LONG-TERM AGING AND WEAR

LIMITATION:

Tests are conducted on relatively new hardware. Long-term effects (capacitor aging, contactor wear, solder fatigue, connector fretting) are not covered.

MITIGATION:

(1) POST (FSR-16) catches degradation in critical protection circuits. (2) Inspection/maintenance intervals in service documentation. (3) the source management node (when present) monitors cell degradation (outside VCU scope).

LIMIT-04: SINGLE-ENCODER LIMITATION (H-08)

LIMITATION:

Single encoder, no redundant rotor position sensor. FSR-09 testing validates detection and safe state entry, but cannot prevent loss of control during the detection window (up to 100 ms).

MITIGATION:

(1) Detection window as short as possible (<50 ms target). (2) Bounded sensorless fallback if implemented (≤2 s, ≤30%). (3) Documented: operator must be prepared for occasional safe-state entry from encoder faults.

LIMIT-05: COMMON-CAUSE MCU FAILURE (SHARED 3.3 V RAIL AND SINGLE PCB)

LIMITATION:

The main STM32H723, the safety coprocessor, and the NCV57100 logic side share the same 3.3 V rail and the same PCB. A common-cause affecting the rail or the board could, in principle, affect both MCUs simultaneously.

HEADLINE MITIGATION - THE DOMINANT COMMON-CAUSE IS FAIL-SAFE BY CONSTRUCTION:

total or partial collapse of the shared 3.3 V rail does not disable the safe state, it *forces* it: NCV57100 VDD lost → internal active pull-down → SSO with no software involvement (Path 3). The largest single-point energy source in the system therefore fails toward the safe direction rather than defeating the safety architecture.

FURTHER MITIGATIONS:

(1) the **TPS389006-Q1 rail supervisor** (TI Functional Safety-Compliant; supports designs up to SIL 3 / ASIL D per TI documentation) monitors the shared 3.3 V rail, the +5 V/+12 V/sensor rails, and both gate-drive power feedbacks; on any out-of-window condition - including brownout of the rail shared by both MCUs - it asserts the shared GATE_DRIVER_FAULT line monitored by both MCUs, providing a hardware path to system shutdown independent of both CPUs (Path 4 trigger). (2) The coprocessor has its own oscillator, independent ADC channels, and independent power kill (GATE_DRIVE_PWR2_ENABLE). (3) Six redundant SSO pathways; 1oo2 power kill with independent feedback. (4) Dual-MCU ASIL B(D) + B(D) decomposition. Formal independence substantiation remains subject to the pending DFA (LIMIT-08).

LIMIT-06: GATE DRIVER NON-ASIL STATUS

LIMITATION:

NCV57100 qualified to AEC-Q100, not ASIL. Tests C-15 through C-17 validate protections function but provide no ASIL credit.

MITIGATION:

(1) No ASIL credit claimed (Table 9). (2) Coprocessor FLT/READY/PWM monitoring closes the single-point FLT gap. (3) OR'd FLT monitored by both MCUs.

LIMIT-07: SOFTWARE TEST LIBRARY - CLASS B VS. CLASS D

LIMITATION:

X-CUBE-CLASSB is IEC 60730-1 Class B only; the ISO 26262 Class D STL (X-CUBE-STL) requires an NDA unavailable to open-source projects. Consequently: no FMEDA/SPFM/LFM for this MCU configuration, no tool qualification, no fault-injection coverage evidence, no independent assessment. ASIL decomposition here is a **design and educational exercise only**.

MITIGATION:

(1) CLASSB provides CPU register test, RAM March-C, flash CRC - adequate for POST, not ASIL-traceable. (2) Software safety mechanisms independently tested via this fault injection plan. (3) Gap documented explicitly.

LIMIT-08: NO DEPENDENT FAILURE ANALYSIS (DFA)

LIMITATION:

No DFA performed. Common-cause/cascading failures between the six SSO paths are not formally analyzed; the ASIL B(D) decomposition independence claim cannot be fully substantiated.

MITIGATION:

(1) Physical separation of critical routing. (2) Independent grounds where possible. (3) Coprocessor independent oscillator; TPS389006-Q1 supervises the shared rail. (4) DFA required before any formal ASIL D audit. Blocker for a formal ASIL D claim.

LIMIT-09: NO EMI/EMC PRE-COMPLIANCE ASSESSMENT

LIMITATION:

No pre-compliance EMC assessment or design margin analysis. EMI-induced ADC noise, CAN errors, or false TIM1_BKIN triggering are unquantified risks in unknown installation environments.

MITIGATION:

(1) E-08/E-09 deferred to an external lab campaign. (2) CISPR 25 pre-compliance recommended before field deployment. (3) PCB follows best-practice grounding/shielding/filtering. (4) Documented open risk for third-party installation.

LIMIT-10: NO MID-OPERATION SHORT-CIRCUIT INJECTION (NEW IN V5.0)

LIMITATION:

Without a remote shorting contactor, phase short tests (C-31–C-34) use energize-into-fault at stepped voltage. The mid-operation short at full load - the highest-energy manifestation of H-12 - is not reproduced. DESAT physics is identical in both cases (detection is per-switching-cycle at the gate), but bus-level energy and plasma/arc behavior differ.

MITIGATION:

(1) Stepped-voltage energize-into-fault up to the board maximum (140 V nominal / 175 V max). (2) Post-test isolation re-verification per C-50. (3) A contactor-based mid-operation short variant is defined as a future test if a suitably rated, remotely operated shorting contactor is acquired.

1.11. Recommended Test Execution Order

The campaign follows **progressive validation**: non-destructive tests first, potentially destructive tests last. Advancement between groups requires all tests in the current group to pass (Table 20).

1.11.1. Execution Sequence

Table 19 - Test Execution Order and Justification

Order	Group	Tests	Risk
1	Power-On Self-Test	C-16, C-20	None
2	Supply Integrity	C-21, *C-22*, C-41	Very L
3	Gate Driver Integrity	C-49, C-17, C-26, C-27	Low
4	Isolation & HV Safety	C-50, C-12, C-08, C-35	Low-M
5	Sensor Validation	C-01–C-07, C-09, C-10, C-11, C-28–C-30, C-42	Mediu
6	Control Loop Validation	C-13, C-14, C-43, S-10, S-11	Mediu
7	Software Integrity	C-18, C-19, C-39, C-15, C-16, I-08, I-09, I-10, I-11	Mediu
8	Integration & Coordination	I-01–I-03, I-06, I-12–I-18, S-12	Mediu
9	Performance Validation	S-06, S-07, S-08, S-09, S-13, S-14, S-15	Mediu
10	Fault Response Validation	S-01–S-05, C-45, C-23–C-25*, C-31–C-34, I-05, I-07	High
11	Environmental (Deferred)	E-01–E-12	Variab

1.11.2. Stopping Criteria Between Groups

Table 20 - Inter-Group Stopping Criteria

Scenario	Required Action
Any test in Group 1–3 fails	Stop. Do not apply HV. Debug, f
Any test in Group 4–5 fails	Stop. HV permitted; no motor/loa
Any test in Group 6–8 fails	Stop. Motor connected; safe sta
Any test in Group 9 fails	Stop. Full power applied; damag
Any test in Group 10 fails	Stop. Destructive testing may ha
Conditional tests (C-21/22/24/25) not executable at time of campaign	Record as Conditional-not-run; c

1.11.3. Hardware Damage Risk Classification

Table 21 - Per-Test Hardware Damage Risk

Risk	Tests
None	C-16, C-20, C-21, C-41, C-49, I-08, I-11
Very Low	C-22, C-17, C-43, C-50*, I-09, I-10
Low	C-26, C-27, C-35, C-42, I-04, I-12, I-17
Medium	C-01–C-15, C-18, C-19, C-28–C-30, C-39, S-01–S-05, S-10–S-14, I-01–I-03, I-05–I-07
Medium-High	S-06–S-09, S-15, S-16–S-19, C-08, C-10, C-45
High	C-23–C-25, C-31–C-34 (energize-into-fault), C-06, C-07, S-13, I-05
Very High	C-31–C-34 if attempted at full DC link

SAFETY WARNING FOR PHASE SHORT TESTS (C-31 THROUGH C-34)

Phase short tests are **INHERENTLY DESTRUCTIVE IF PROTECTION FAILS**. Even at reduced voltage, fault currents of 1000+ A are possible. Mandatory precautions: (1) blast shield around the DUT; (2) remote activation of the DC supply - no manual connection of a live circuit; shorts are bolted on de-energized only; (3) supply current limit set to the minimum practical value; (4) fire suppression present; (5) no personnel in the test area during energization; (6) video recording for post-test analysis; (7) DESAT self-test (C-16) shall have passed within 24 hours before any short test; (8) voltage stepping: 50 V first, increase only after verified protection operation and inspection at each step; (9) C-50 isolation re-verification after the short series.