sev10

Hazard analysis and assumed safety goals (SEooC)

Electro-mechanical brake corner ECU

Quillon Motors · Brake-by-wire with blended braking · TIDA-020106 PCB VerB

Document no.	S10-QLN-HARA-001
Revision	B (draft for client review)
Date	2026-09-28
Prepared by	F. Walsh, sev10
Reviewed by	Pending: sev10 internal verification; Quillon functional safety
Classification	Confidential. Prepared for Quillon Motors.

Revision history

Rev	Date	Description	Author
A	2026-09-27	Draft for client review. Safety goals assumed pending the vehicle HARA (OQ-006)	F. Walsh
B	2026-09-28	Added HE-20 and SG-07 (ECU thermal event, ASIL B) and assumption A-12, following the DFMEA (OQ-044)	F. Walsh

Contents

1 Scope....2
2 Method....3
3 Item definition (assumed)....4
4 Hazard analysis and risk assessment....7
5 Assumed safety goals....11
6 Findings....12
7 Recommended actions and next deliverables....12
8 Open questions and assumptions....13
9 Abbreviations and references....14
Appendix A Function and guide-word analysis....15
Appendix B Preliminary check of TI's component ratings....15

1 Scope

This document is the hazard analysis and risk assessment (HARA) for the electro-mechanical brake (EMB) corner ECU that Quillon Motors has selected for the brake-by-wire system of its pickup truck. The ECU is built on the Texas Instruments TIDA-020106 reference design, PCB VerB (design files SLVMF37A–41A, SLVC962A). One ECU sits at each wheel and drives that wheel's brake caliper and, at the rear, its parking brake.

The ECU is an element, not a complete item. Following ISO 26262-10 clause 9 (safety element out of context, SEooC), this document assumes an item definition for the brake-by-wire system, identifies the vehicle-level hazards the ECU can cause or contribute to, and derives **assumed safety goals** for them. These assumptions let the element's safety analyses (DFMEA, FMEDA, dependent failure analysis) proceed. They must be checked against Quillon Motors' own HARA when it is available (OQ-006).

Status: Rev B, draft for client review. Every S, E and C rating in this document is provisional until Quillon Motors confirms it. Values that rest on a specific assumption about the vehicle or its timing are shaded orange and marked ASSUMED; section 3.3 lists every assumption in one place.

In scope

- Service-brake actuation at one wheel: clamp-force control of the caliper's BLDC motor (DRV3263-Q1 gate driver, three-phase inverter, phase-current sensing, TMAG6180-Q1 motor-angle sensing).
- Friction brake contribution during blended braking (friction fill-in as regenerative braking changes).
- Electric parking brake (EPB) apply, hold, release and driver-requested dynamic apply (DRV8263-Q1 H-bridge).
- Wheel-speed acquisition (WSS001) and reporting.
- Brake-pedal force and travel inputs read by the ECU (fall-back demand path), degradation reporting, CAN communication (TCAN1043H-Q1), power supply (LM74930-Q1, LM68645-Q1, TPS62902-Q1, TPS653860-Q1 PMIC) and the F29P329 controller.
- This ECU's contribution to hazards that involve several wheels (section 4.3).

Out of scope

- Central brake controller and blending strategy, vehicle motion control, ABS and ESC algorithms.
- Brake pedal unit, pedal-feel simulator and pedal sensors (only their interface to this ECU is in scope).
- Caliper mechanics, BLDC motor, gearbox, EPB spindle; the e-machine and inverter providing regenerative braking.
- Rating of vehicle-level hazards that need several ECUs to fail: that belongs to the vehicle HARA. Section 4.3 states the goals assumed here and what this ECU must provide towards them.

2 Method

ISO 26262-3:2018 clause 6. Malfunctioning behaviours were derived by applying seven guide words (no, less, more, unintended, stuck, late, erroneous) to each function in section 3.4. Appendix A records the result for every function and guide word, including the reason when a combination is not a hazard or is a cause for the DFMEA.

Each malfunctioning behaviour was combined with every relevant operational situation; the table in section 4.2 keeps the combinations that set the highest ASIL for each safety goal, and Appendix A shows the rest.

Severity (S0–S3), exposure (E0–E4) and controllability (C0–C3) follow ISO 26262-3 Tables 1–3; the ASIL follows Table 4. Exposure uses frequency of the situation for events that happen at an instant

and duration for continuous situations; the basis is stated per situation. SAE J2980 examples are used as guidance.

Controllability assumes an average driver and a single-corner fault: the other three wheels keep braking normally. No credit is taken for this ECU's own safety mechanisms, for ABS or ESC (they act through the same corner ECUs), or for degradation reporting.

Rating tables

Class	0	1	2	3	4
Severity S	No injuries	Light and moderate injuries	Severe injuries, survival probable	Life-threatening or fatal injuries	—
Exposure E	Incredible	Very low	Low (a few times a year)	Medium (once a month or more)	High (almost every drive)
Controllability C	Controllable in general	Simply controllable (≥ 99% of drivers)	Normally controllable (≥ 90%)	Difficult or uncontrollable	—

ASIL from ISO 26262-3 Table 4: with S, E and C at least 1, S + E + C = 10 gives ASIL D, 9 gives C, 8 gives B, 7 gives A, and anything lower is QM.

Assumed values

Marking	Meaning
ASSUMED	Orange cells rest on an assumption about the vehicle, its regulation or its timing. Each assumption is listed in section 3.3 and linked to an entry in the open questions log (S10-QLN-OQL-001); it is replaced when Quillon Motors answers it. Independently of the shading, all S, E and C ratings are provisional (section 1).

3 Item definition (assumed)

3.1 Vehicle and braking concept

Quillon Motors' truck brakes by wire: the brake pedal is a sensor, and each wheel's brake is applied by an electric motor in the caliper. When the driver presses the pedal, the brake controller works out the total deceleration wanted, takes as much as it can from regenerative braking on the rear e-machine, and asks the four corner ECUs for the rest as friction clamp force. As regeneration fades (low speed, full battery, an ABS event), the friction share has to rise just as fast, or the driver feels the truck stop slowing down.

Aspect	Assumption used in this HARA	Basis
Vehicle	Battery-electric pickup truck, rear-wheel drive, single rear e-machine with open differential	ASSUMED (A-01)

Aspect	Assumption used in this HARA	Basis
Mass and class	Curb about 2,700 kg, GVWR up to 3,500 kg (category N1); trailer towing permitted; top speed ≥ 130 km/h	ASSUMED (A-02)
Regulation	FMVSS 135 and UN R13-H, including secondary braking and parking-brake hold on a 20% gradient	ASSUMED (A-02)
Brake system	Dry brake-by-wire: an EMB caliper and corner ECU at all four wheels, no hydraulic back-up; pedal unit with feel simulator; central brake controller	ASSUMED (A-03)
Blending	Brake controller splits demand between rear-axle regeneration and friction; corner ECUs receive clamp-force requests over CAN and fill in friction when regeneration drops out	ASSUMED (A-04)
Partitioning	Corner ECUs split into two independent power and communication domains (e.g. diagonal), so no single supply or bus fault affects more than two wheels	ASSUMED (A-09)
Pedal path	Pedal force (PFS) and travel (PTS) sensors are also wired to this ECU as a fall-back demand path	ASSUMED (A-05)
Parking brake	EPB in the rear calipers; self-locking spindle holds without power; driver-requested dynamic apply while moving; auto-hold at standstill	ASSUMED (A-06)
Supply	48 V variant (TIDA-020106 Table 1-1, 32–60 V)	ASSUMED (A-07)
Caliper when unpowered	Service brake releases (clamp force decays) when the motor is de-energised	ASSUMED (A-08)
Operating modes	Sleep, wake, drive, standstill hold, parked, workshop/service (EPB service mode, J10 boot)	—

3.2 Boundary and interfaces

Interface	Direction	Signal / carrier	Board reference
Battery supply	in	48 V (or 12 V) supply, reverse/surge protected	J3 (+), J4 (GND); LM74930-Q1 (U1)
Brake controller	in/out	Clamp-force request, status, degradation; CAN FD ×2	J17–J20; U8, U10 (TCAN1043H-Q1)
Pedal sensors	in	Pedal force and travel, analog or SENT; sensor supplies 5Vp1/5Vp2	J12, J14; J15, J11
Caliper BLDC motor	out	Three-phase drive, 16 A RMS nominal at 48 V	J7–J9; DRV3263-Q1 (U5)
Motor angle	in	Sine/cosine from two TMAG6180-Q1	U12, U13; J21, J22
EPB motor	out	Brushed DC drive with current sense	J5, J6; DRV8263-Q1 (U7)
Wheel-speed sensor	in	Active wheel-speed sensor current interface	J1, J2; WSS001 (U6)
Debug / boot	in	UART RX and BOOT1 on header	J10 (OQ-015)

3.3 Assumptions

ID	Assumption	Open question
A-01	Rear-wheel-drive BEV pickup, single rear e-machine, open differential	OQ-020
A-02	Curb about 2,700 kg, GVWR ≤ 3,500 kg (N1), towing permitted, ≥ 130 km/h; FMVSS 135 / UN R13-H apply	OQ-024
A-03	EMB at all four corners, no hydraulic back-up, central brake controller	OQ-020
A-04	Blending in the brake controller; regeneration on the rear axle only	OQ-020
A-05	Pedal sensors also wired to the corner ECU as a fall-back path	OQ-009
A-06	Rear EPB with self-locking spindle; dynamic apply on request; auto-hold	OQ-023, OQ-026
A-07	48 V supply variant	OQ-011
A-08	Service brake releases when the caliper motor is unpowered	OQ-023
A-09	Two independent power and communication domains across the four corners	OQ-025
A-10	Fault-tolerant time intervals as given in section 5 (placeholders)	OQ-021
A-11	Fail-silent corner (release and report) is acceptable at vehicle level with driver warning	OQ-022
A-12	ECU mounted at the wheel corner; an ECU thermal event is rated at vehicle level (smoke or fire can spread to the tyre, harness or cabin)	OQ-044

3.4 Functions

ID	Function	Behaviour required
F1	Service braking	Apply the requested clamp force at the wheel within the specified response time; hold it; release on request
F2	Friction fill-in	Follow changes in the friction share so total deceleration stays as requested while regeneration changes
F3	Parking brake	Apply and hold at standstill on request; auto-hold at standstill; dynamic apply while moving only on driver request; release on request
F4	Wheel speed	Measure wheel speed and report it with correct value and timing, including the standstill indication
F5	Pedal demand (fall-back)	Read pedal force and travel and use them when the CAN request path is lost
F6	Degradation reporting	Report loss or limitation of any function to the brake controller in time for the other corners to compensate and the driver to be warned
F7	Energy containment	Keep internal faults (48 V shorts, overheated parts or joints) from producing smoke, fire or hot surfaces, in every operating mode

4 Hazard analysis and risk assessment

4.1 Operational situations

ID	Situation	E	Basis
OS-01	Highway, ≥ 100 km/h, straight, curve or lane change, dry	E4	Duration: > 10% of operating time
OS-02	Braking from highway speed, normal deceleration	E4	Frequency: most trips
OS-03	Emergency braking from ≥ 80 km/h, dry	E2	Frequency: a few times a year
OS-04	Braking on split friction (one side on ice or gravel)	E2	Frequency: a few times a year
OS-05	Urban driving and braking, 30–60 km/h, pedestrians and cyclists nearby	E4	Duration: > 10% of operating time
OS-06	Regeneration withdrawn during braking at speed (battery full, e-machine fault, ABS event)	E3	Frequency: once a month or more (full battery at the start of a descent, cold battery)
OS-07	Braking on low friction (wet, snow, ice), including ABS braking	E3	Frequency: several times a month in winter markets (worst-case market)
OS-08	Parked on a gradient, driver out of the vehicle, people nearby	E3	Frequency: once a month or more
OS-09	Laden or towing, long downhill descent with sustained braking	E2	Frequency: a few times a year
OS-10	Held at standstill on a slope with the driver in the vehicle (traffic, auto-hold)	E4	Frequency: most trips
OS-11	Service braking lost; driver pulls the EPB switch to stop (secondary braking)	E1	Frequency: rarely, only after a service-brake failure

4.2 Hazardous events

ID	Malfunctioning behaviour	Fn	Situation	Hazard	S	E	C	ASIL	Rationale	Goal
HE-01	Unintended clamp force at one wheel (no request)	F1	OS-01	Sudden yaw and lane departure; collision with oncoming traffic or roadside objects	S3	E4	C3	D	S: Side or head-on impact at high speed. C: Sudden full braking of one wheel at speed; most drivers cannot correct in time.	SG-01
HE-02	Clamp force not released after braking (stuck applied)	F1	OS-01	Yaw and loss of control once the driver accelerates back to speed	S3	E4	C3	D	S: As HE-01. C: Full residual force at speed is not controllable.	SG-01

ID	Malfunctioning behaviour	Fn	Situation	Hazard	S	E	C	ASIL	Rationale	Goal
HE-03	Clamp force above request at one wheel during braking	F1	OS-02	Wheel lock and yaw during braking; loss of lateral stability	S3	E4	C3	D	S: Loss of control at speed. C: No credit for ABS or ESC, which act through the same corner ECUs.	SG-01
HE-04	Clamp force applied at the wrong wheel (position coding or request addressed to the wrong corner)	F1	OS-02	Braking on the wrong side; yaw in the wrong direction during a stability intervention	S3	E4	C3	D	S: Loss of control at speed. C: Driver cannot anticipate the direction.	SG-01
HE-05	Friction fill-in above request when regeneration is withdrawn (rear axle)	F2	OS-07	Rear wheel lock on low friction; oversteer and spin	S3	E3	C3	C	S: Loss of control. C: Rear lock on low friction is not correctable by an average driver.	SG-01
HE-06	Partial residual drag on a laden or towing descent	F1	OS-09	Brake overheating and fade; loss of braking later in the descent; wheel-end fire	S3	E2	C2	A	S: Collision with reduced braking. C: Driver notices pull and fade, can reduce speed with remaining corners.	SG-01
HE-07	No clamp force at one front wheel during braking	F1	OS-02	Deceleration reduced by about a third; pull towards the braking side; collision ahead	S3	E4	C2	C	S: Collision at speed. C: Normal deceleration leaves margin; driver brakes harder and counter-steers.	SG-02
HE-08	No clamp force at one front wheel during emergency braking	F1	OS-03	Longer stopping distance and strong yaw at high deceleration	S3	E2	C3	B	S: Collision at speed. C: At maximum deceleration on dry road the yaw moment is largest and there is no margin.	SG-02
HE-09	No clamp force at one wheel on split friction	F1	OS-04	Yaw moment when the high-friction wheel loses braking	S3	E2	C3	B	S: Loss of control. C: Little time to correct.	SG-02
HE-10	Clamp force below request at one wheel in urban braking	F1	OS-05	Reduced deceleration and mild pull; pedestrian or cyclist struck	S3	E4	C1	B	S: Vulnerable road user at 30–60 km/h. C: Driver presses harder; other wheels compensate.	SG-02
HE-11	Friction fill-in late or too small when regeneration is withdrawn	F2	OS-06	Sudden drop in deceleration while braking; collision ahead	S3	E3	C2	B	S: Collision at speed. C: Driver notices the drop and presses harder.	SG-02
HE-12	Loss of function not reported (corner fails silently before or during a demand)	F6	OS-02	Other corners do not compensate; reduced braking and pull as HE-07 without warning	S3	E4	C2	C	S: Collision at speed. C: As HE-07; no warning given.	SG-02
HE-13	Unintended parking-brake application while driving (rear)	F3	OS-01	Rear wheel lock at speed; spin	S3	E4	C3	D	S: Loss of control at high speed. C: Rear lock at speed is not controllable, and the self-locking spindle keeps the force once built.	SG-03

ID	Malfunctioning behaviour	Fn	Situation	Hazard	S	E	C	ASIL	Rationale	Goal
HE-14	Loss of parking-brake hold, or unintended release, while parked	F3	OS-08	Vehicle rolls away; people struck or crushed	S3	E3	C3	C	S: Pedestrian run over. C: No driver in the vehicle.	SG-04
HE-15	Unintended release of standstill hold with the driver present	F3	OS-10	Vehicle rolls into the vehicle or pedestrian behind or ahead	S2	E4	C2	B	S: Low-speed impact. C: Driver present and can press the pedal.	SG-04
HE-16	No dynamic parking-brake apply when the driver requests it as a secondary brake	F3	OS-11	No means of stopping after a service-brake failure	S3	E1	C3	A	S: Collision. C: No other braking available.	SG-06
HE-17	Parking brake fails to release	F3	OS-05	Vehicle cannot drive away	S0	—	—	QM	S: No injury (availability).	QM
HE-18	Erroneous wheel speed reported (too high, too low, frozen)	F4	OS-07	ABS or ESC acts on a wrong value: wheel locks or braking released wrongly	S3	E3	C2	B	S: Loss of control or collision. C: Driver can still steer and brake; other wheels' signals allow plausibility.	SG-05
HE-19	Erroneous pedal demand used by the fall-back path	F5	OS-01	Unintended braking at this wheel (see HE-01), without ABS	S3	E4	C3	D	S: As HE-01. C: As HE-01.	SG-01
HE-20	Thermal event of the corner ECU (smoke, fire) from an internal fault	F7	OS-01	Fire in the wheel arch spreading to the tyre, harness or cabin; occupants and people nearby exposed to smoke or fire	S3	E4	C1	B	S: Burns or smoke inhalation; fire can become life-threatening. C: Smoke is noticed early; most drivers can stop and leave the vehicle before injury.	SG-07

4.3 Hazards involving several wheels

These need faults at more than one corner and are rated in the vehicle HARA. They are listed because this ECU's design decides how likely they are. The ASILs are assumed so the element can be developed against them.

ID	Vehicle-level hazard	Common causes involving this ECU	Assumed vehicle ASIL	What this ECU must provide
MC-01	Loss of braking at two or more wheels	Shared supply or CAN domain; identical software on all corners; fail-silent release (A-08); bus-blocking fault	D (ASSUMED)	Stay within its partition (A-09); must not block the bus; software faults covered by the element's systematic capability; latent-fault detection before demand
MC-02	Unintended braking at two or more wheels	Shared erroneous request or pedal fall-back value; identical software	D (ASSUMED)	Plausibility of requests against pedal inputs and vehicle state; end-to-end protection of CAN requests

ID	Vehicle-level hazard	Common causes involving this ECU	Assumed vehicle ASIL	What this ECU must provide
MC-03	Loss of wheel-speed information at several wheels	Shared supply or bus	C (ASSUMED)	Report invalid signals; stay within its partition

5 Assumed safety goals

Each goal takes the highest ASIL of the hazardous events it covers.

ID	Safety goal	ASIL	From	Safe state	FTTI
SG-01	Avoid braking at a wheel that was not requested: unintended, excessive, misdirected or unreleased clamp force.	D	HE-01 to HE-06, HE-19	Clamp force released at that wheel (actively if the caliper does not release by itself); corner reported unavailable; driver warned	TBD; provisional 100 ms (ASSUMED)
SG-02	Avoid loss of, insufficient or late braking at a wheel when braking is requested, including friction fill-in and reporting of lost function.	C	HE-07 to HE-12	Corner reported unavailable or limited; remaining corners and regeneration compensate; driver warned	TBD; provisional 200 ms (ASSUMED)
SG-03	Avoid parking-brake application while the vehicle is moving, unless the driver requests it.	D	HE-13	EPB actively released and further apply inhibited (de-energising alone keeps the force on a self-locking spindle)	TBD; provisional 300 ms (ASSUMED)
SG-04	Avoid loss of parking or standstill hold while the vehicle is stationary.	C	HE-14, HE-15	Hold maintained or re-applied (other rear corner, re-clamp); driver warned; transmission park lock if fitted	TBD; provisional 1 s (ASSUMED)
SG-05	Avoid erroneous wheel-speed information being used by the braking and stability functions.	B	HE-18	Wheel speed marked invalid; braking functions use the other wheels	TBD; provisional 50 ms (ASSUMED)
SG-06	Provide parking-brake deceleration when the driver requests it and service braking is unavailable.	A	HE-16	Not applicable (availability goal): the function itself is the safety measure	TBD
SG-07	Avoid a thermal event (smoke, fire) of the corner ECU.	B	HE-20	Energy removed from the faulty circuit (supply cut-off or fuse), corner reported unavailable, driver warned to stop	TBD; set by the time from a resistive fault to ignition (ASSUMED, OQ-044)

The fault-tolerant time intervals are placeholders. TI states an EMB force response of 80–100 ms (TIDUFI0 §1), so an unintended apply can reach full force within about the provisional 100 ms: detection and release have to act on a force or rate threshold, not after the fact. Real values must come from vehicle dynamics (yaw rate and lateral deviation against the actuator's force ramp) and be set by the vehicle owner (OQ-021). DFMEA ratings that depend on them are provisional.

Not safety-relevant (QM): failure to release the parking brake (HE-17), and a corner reporting a fault it does not have (false trip). Both stay in the DFMEA as availability items.

Warning and degradation concept (assumed)

- One corner unavailable: warning lamp and message; the brake controller redistributes braking; speed limited (value to be set by the vehicle) until the fault is cleared at a workshop.

- Second corner unavailable, or a corner unavailable with no second domain: request a controlled stop.
- Parking-brake fault: warning; the vehicle must not be left without a confirmed hold (park lock or other rear corner).

6 Findings

ASIL D is driven by unintended or unreleased braking at a wheel (SG-01) and by parking-brake application while moving (SG-03). Loss of braking at a single corner rates ASIL C (SG-02); loss of braking at several corners is an assumed vehicle-level ASIL D goal that this ECU supports through partitioning and fault containment (section 4.3).

1. Unintended braking and parking-brake application at speed are the uncontrollable events. Both actuators (the caliper motor and the EPB) therefore need a way to stop or remove force that does not depend on the part that failed.

2. The parking brake is the harder of the two: its spindle holds force without power, so the safe state needs an active release, and the EPB must still apply on driver request as the secondary brake (SG-06).

3. Degradation reporting (F6) is part of SG-01's safe state and carries SG-02's ASIL: a corner that fails silently without reporting is the same hazard as a lost corner with no warning (HE-12).

4. Blending adds two timing requirements: friction must fill in fast enough when regeneration drops out (HE-11) and must not overshoot on the rear axle on low friction (HE-05). Both limits are vehicle-level values (OQ-021).

5. SG-01's safe state (release) is SG-02's hazard (no braking). Releasing is acceptable only because the other corners compensate and the driver is warned; that depends on partitioning (A-09) and the degradation concept above (OQ-022).

6. On PCB VerB, the two motor-angle sensors (U12, U13) sit on opposite sides of the board over the same magnet and share the 3.3 V rail, so they cannot be counted as independent channels without further measures (Appendix B).

7 Recommended actions and next deliverables

#	Action	Owner	Due
1	Confirm or replace the assumed item definition, vehicle data, situations and ratings with the vehicle HARA	Quillon FuSa	2026-10-16
2	Set fault-tolerant time intervals, fill-in response and overshoot limits	Quillon FuSa	2026-10-16

#	Action	Owner	Due
3	Confirm partitioning of corner ECUs, fail-silent strategy and degradation concept	Quillon brake system	2026-10-16
4	Confirm caliper and EPB mechanics (release when unpowered, self-locking, dynamic apply, auto-hold)	Quillon brake system	2026-10-16
5	Internal verification of this document; independent confirmation review before release (ISO 26262-2 Table 1, I3)	sev10 / independent assessor	2026-10-23
6	Functional safety concept: functional safety requirements per safety goal	sev10	After actions 1–4
7	Technical safety concept, FMEDA (SPFM, LFM, PMHF) and dependent failure analysis for the ECU; DFMEA in parallel	sev10	After action 6

8 Open questions and assumptions

Open questions raised while reviewing the design inputs are in S10-QLN-OQL-001. Those this HARA relies on are OQ-006 (no vehicle HARA supplied), OQ-009 (pedal path), OQ-011 (supply variant), OQ-012 (EPB control names swapped against the driver pins), OQ-013 (single supply input), OQ-014 (overvoltage cut-off path) and, for Appendix B, OQ-001, OQ-002, OQ-008, OQ-015 and OQ-019.

This HARA raises the following questions, added to the log:

ID	Question	Working assumption
OQ-020	Vehicle brake architecture: EMB at all four corners without hydraulic back-up? Where does blending run?	ASSUMED: A-01, A-03, A-04
OQ-021	Fault-tolerant time intervals per safety goal; friction fill-in response time and overshoot limit	ASSUMED: placeholders in section 5
OQ-022	Is a fail-silent corner acceptable at vehicle level? What is the degradation and warning concept?	ASSUMED: yes, section 5 concept
OQ-023	Does the service brake release when unpowered, and does the EPB spindle self-lock?	ASSUMED: releases; self-locks
OQ-024	Vehicle mass, GVWR, towing limits and applicable brake regulation	ASSUMED: A-02
OQ-025	How are the four corner ECUs partitioned across power supplies and CAN buses?	ASSUMED: two independent domains (A-09)
OQ-026	Are dynamic EPB apply (secondary braking) and auto-hold functions of this ECU?	ASSUMED: yes (A-06)
OQ-027	TIDUFI0 §2.4.1.7 says the PMIC disables the EPB driver, but no PMIC safe-state output reaches U7 on PCB VerB. Intended?	Not credited

9 Abbreviations and references

Term	Meaning
ASIL	Automotive Safety Integrity Level (A lowest to D highest); QM = quality management, no ASIL
S / E / C	Severity, exposure, controllability ratings (ISO 26262-3)
SEooC	Safety element out of context: an element developed on assumed safety goals (ISO 26262-10 clause 9)
OS / HE / SG	Operational situation / hazardous event / safety goal
FTTI	Fault-tolerant time interval: time from fault to hazard if no safety mechanism acts
EMB / EPB	Electro-mechanical brake / electric parking brake
FSC / TSC	Functional safety concept / technical safety concept
FMEDA	Failure modes, effects and diagnostic analysis; SPFM, LFM, PMHF are its hardware metrics
DFA	Dependent failure analysis (common cause and cascading failures)
CMPSS	Comparator subsystem of the F29 MCU, used for supply monitoring
NVM	Non-volatile memory (factory configuration of the PMIC)
SENT	Single Edge Nibble Transmission, a sensor interface (SAE J2716)
E2E	End-to-end protection of messages (CRC, counter, timeout)

Ref	Document
[1]	ISO 26262-2, -3, -9, -10:2018 Road vehicles – Functional safety
[2]	SAE J2980 (2021) Considerations for ISO 26262 ASIL hazard classification
[3]	UN Regulation No. 13-H; FMVSS 135 Light vehicle brake systems
[4]	Texas Instruments TIDUFI0, Electro-Mechanical Brake (EMB) Reference Design (design guide)
[5]	Texas Instruments TIDA-020106 design files: SLVMF37A schematic, SLVMF38A layout, SLVMF39A BOM, SLVMF40A assembly, SLVC962A fabrication
[6]	Texas Instruments SDAA375, Achieving Functional Safety Goals for DC/DC Converters Using F29x
[7]	S10-QLN-OQL-001 Open questions log (sev10)

Limitations: this analysis is based on the published TI reference design and sev10's assumptions about the vehicle. It does not replace the vehicle manufacturer's HARA and is not a release for production.

Appendix A Function and guide-word analysis

Every function crossed with every guide word. Each cell names the hazardous event it leads to, the event it is covered by ("As"), or why it is not a hazard.

Function	No	Less	More	Unintended	Stuck	Late	Erroneous
F1 Service braking	HE-07, HE-08, HE-09	HE-10	HE-03	HE-01	HE-02, HE-06	As HE-07 (C) or HE-02 (release)	HE-04 (wrong wheel)
F2 Friction fill-in	HE-11	HE-11	HE-05	As HE-01	As HE-05 or HE-11	HE-11	As HE-05 / HE-11
F3 Parking brake	HE-14 (no hold), HE-16 (no dynamic apply)	HE-14 (weak hold)	Cause: overload (DFMEA)	HE-13 (moving), HE-15 (release)	HE-17 (no release, QM)	Not a hazard: parking is slow by design	As HE-13 / HE-14
F4 Wheel speed	HE-18	HE-18	HE-18	Not applicable	HE-18 (frozen)	HE-18 (late)	HE-18; false standstill gates SG-03
F5 Pedal fall-back	As HE-07 at this corner; MC-01	As HE-10	As HE-03	HE-19; MC-02	As HE-02	As HE-11	HE-19
F7 Energy containment	HE-20 (no containment)	HE-20	Not applicable	HE-20 (thermal event)	HE-20 (fault energy not removed)	HE-20 (cut-off too slow)	Not applicable
F6 Degradation reporting	HE-12	HE-12	Availability only (false trip): QM	Availability only (false trip): QM	HE-12	HE-12	HE-12 / wrong corner reported: as HE-04

Appendix B Preliminary check of TI's component ratings

TI's design guide (TIDUFI0, Fig. 2-1) labels most blocks with an ASIL. This check compares those labels with the assumed safety goals, for the parts fitted on PCB VerB. It is input to the technical safety concept, not part of the hazard analysis, and it does not assess TI's own development.

Block (TI Fig. 2-1)	Part on PCB VerB	TI tag	Needed by	Observation
Controller	F29P329SM2 (U14)	ASIL D	SG-01, SG-03 (D)	Matches. Certificate coverage of the fitted variant open (OQ-001)

Block (TI Fig. 2-1)	Part on PCB VerB	TI tag	Needed by	Observation
PMIC and watchdog	TPS653860-Q1 (U3)	ASIL D	SG-01, SG-03 (D)	Matches. NVM configuration open (OQ-002)
BLDC gate driver	DRV3263-Q1 (U5)	ASIL D	SG-01 (D)	Matches
Motor angle sensing	TMAG6180-Q1 ×2 (U12, U13)	ASIL B	SG-01 (D)	Below the goal unless decomposed. On VerB both sensors read the same magnet and share the 3.3 V rail, so B(D) + B(D) decomposition needs added independence
48 V to 12 V buck	LM68645-Q1 (U2)	ASIL C	SG-01 (D), supply	Below the goal unless covered by the F29 CMPSS overvoltage/undervoltage cut-off described in SDAA375, which acts through the CAN transceiver's INH output (OQ-014). Fitted variant undocumented (OQ-019)
Core buck	TPS62902-Q1 (U4)	QM	SG-01 (D), supply	Needs coverage by PMIC and MCU supply monitoring
Ideal diode / surge	LM74930-Q1 (U1)	QM	SG-01, SG-02, supply	Needs coverage by downstream supply monitoring
EPB H-bridge	DRV8263-Q1 (U7)	ASIL B	SG-03 (D), SG-04 (C)	Below the goals unless a second path stops the EPB. TI provides a supply cut-off (DRV3263 CUTOFF1 → Cutoff_EPB → Q11, also driven by the MCU via Q6). Its independence from the MCU is open, and no PMIC safe-state output reaches U7 on VerB (OQ-027)
Wheel-speed decoder	WSS001 (U6)	ASIL B	SG-05 (B); standstill check for SG-03 (D)	Matches SG-05. The standstill indication used to gate the EPB needs SG-03's ASIL or an independent source. Shares an SPI bus with U7 (OQ-015); no public datasheet (OQ-008)
CAN transceivers	TCAN1043H-Q1 (U8, U10)	QM	SG-01, SG-02 requests	Requests need end-to-end protection (CRC, counter, timeout) in the software. Also in the overvoltage cut-off path (OQ-014)
Pedal travel sensor	off-board LDC5072-Q1 + TMAG3101-Q1	ASIL D	MC-02; SG-01 via F5	Vehicle-level. Force sensor has no TI tag. This ECU's input path inherits the goal if the fall-back is used (OQ-009)