sev10

Hardware safety analysis: DFMEA and FMEDA

Electro-mechanical brake corner ECU

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

Document no.	S10-QLN-HWA-001
Revision	A (draft for client review)
Date	2026-09-28
Prepared by	F. Walsh, sev10
Reviewed by	sev10 internal review (four reviewers, 2026-09-28); client review pending
Classification	Confidential. Prepared for Quillon Motors.

Revision history

Rev	Date	Description	Author
A	2026-09-28	First issue: DFMEA Rev A and FMEDA Rev A summarised for client review	F. Walsh

Contents

1 Executive summary....2
2 Scope....7
3 Method....9
4 DFMEA results....12
5 FMEDA results....29
6 Recommendations and next steps....47
7 Open questions....49
8 Abbreviations and references....53
Appendix A Effect library....55
Appendix B FIT data....56
Appendix C Traceability....59
Appendix D Review record....59

1 Executive summary

1.1 What was analysed

This document reports the design FMEA (DFMEA) and the hardware-metric analysis (FMEDA) of the electro-mechanical brake corner ECU that Quillon Motors has selected for its brake-by-wire pickup. The ECU is the Texas Instruments TIDA-020106 reference design, PCB VerB, analysed as a safety element out of context against the safety goals of S10-QLN-HARA-001 Rev B. The DFMEA covers 783 failure chains in 11 circuit blocks. The FMEDA computes SPFM, LFM and PMHF for 6 of the 7 safety goals, for the hardware as published and with the DFMEA actions applied.

Result. As published, no ASIL C or D goal meets its single-point fault metric. With the recommended actions, 1 of the 6 computed goals meet their targets; SG-03 is 0.35 points short, pending TI confirmation of the supply-monitor coverage. The latent fault metric is met for every goal. PCB VerB is not usable as published for the ASIL C and D goals: seven hardware changes (section 6.1) and TI's failure data are required.

Illustrative engagement: Quillon Motors is a fictional client and the vehicle assumptions are sev10's. TIDA-020106 is analysed from Texas Instruments' published design files; TI has not reviewed or endorsed this analysis. TI, Texas Instruments and the TI part numbers are trademarks of Texas Instruments Incorporated.

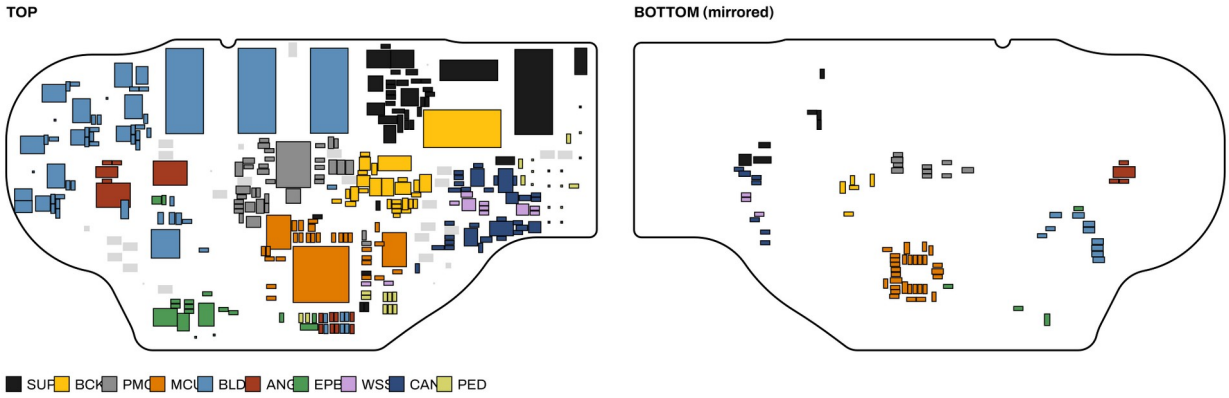


Figure 1. PCB VerB, top and bottom, parts coloured by DFMEA circuit block. Drawing by sev10 from TI Gerber and IPC-356 data.

1.2 Headline results

Table 1. Hardware metrics by safety goal. Black = below target. PMHF is for one corner, against an item-level budget not yet allocated (OQ-046): SG-01 with the actions uses 9.9 FIT of the 10 FIT ASIL D item budget at a single corner, so any allocation across four corners fails.

Goal		ASIL	SPFM as built	SPFM with actions	LFM with actions	PMHF with actions (FIT)	Target SPFM / LFM	Verdict with actions
SG-01	Unintended or unreleased braking	D	87.5 %	97.36 %	96.8 %	9.9	99 % / 90 %	Misses SPFM
SG-02	Loss of braking	C	80.8 %	90.42 %	99.2 %	31.2	97 % / 80 %	Misses SPFM
SG-03	EPB applied while moving	D	96.7 %	98.65 %	94.7 %	1.6	99 % / 90 %	Misses SPFM
SG-04	Loss of parking hold	C	94.0 %	95.60 %	94.4 %	4.6	97 % / 80 %	Misses SPFM
SG-05	Erroneous wheel speed	B	92.8 %	92.85 %	97.5 %	4.4	90 % / 60 % (rec.)	Meets SPFM and LFM (recommended targets)
SG-06	Secondary braking by EPB	A	—	—	—	—	None (ASIL A)	Not computed
SG-07	ECU thermal event	B	60.3 %	75.96 %	87.2 %	13.9	90 % / 60 % (rec.)	Misses SPFM (recommended targets)

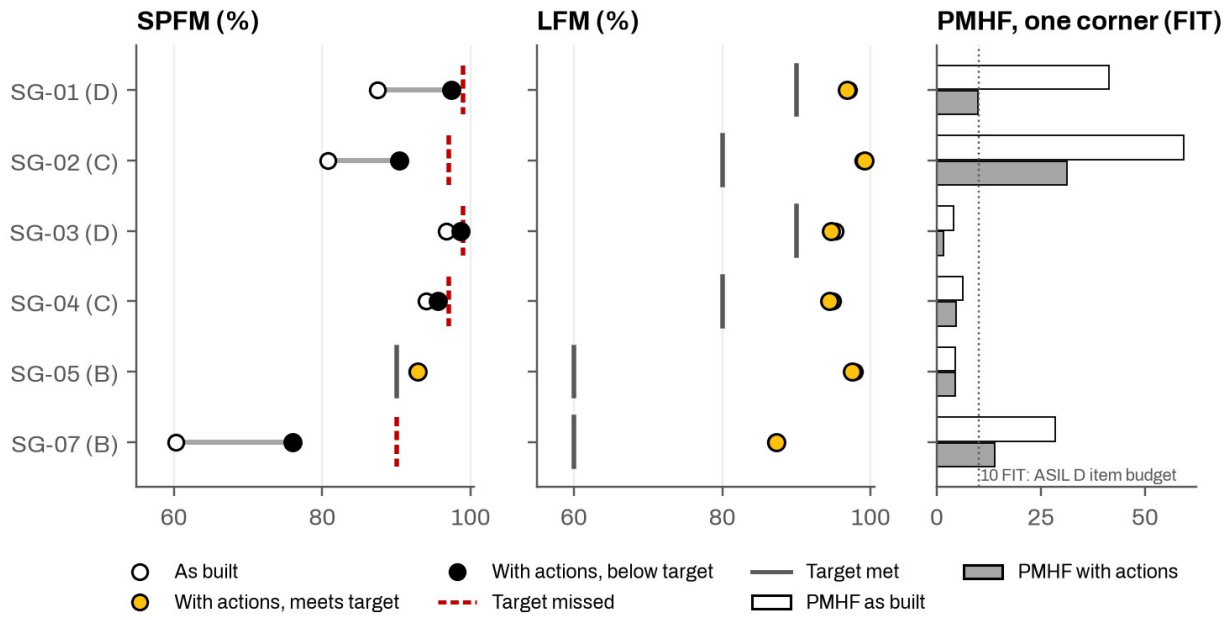


Figure 2. SPFM and LFM as built and with the DFMEA actions against the ISO 26262-5 targets; PMHF per corner.

How to read these results. TIDA-020106 is a laboratory reference design: TI describes it as an ASIL-D compatible design for lab use only (TIDUFI0), not a finished product. The board carries no certification. Of its integrated circuits, only the F29P329SM-Q1 MCU holds a certificate (TÜV SÜD, SFFSBK8), and the MCU part number on the published BOM is outside it (OQ-001); TI's other categories (Functional Safety-Compliant or -Capable) are TI's own process claims. The metrics are provisional in both directions: IC values without published TI data are deliberately conservative placeholders, while 391 DFMEA rows and several FMEDA credits rest on software and brake-controller mechanisms that are specified but not yet implemented. Section 5.6 lists which choice moves which result.

1.3 Top findings

Table 2. Findings that drive the results.

#	Finding	Consequence	Direction	DFMEA rows
1	**No stop path is independent of the MCU.**	The PMIC safe-state output is unconnected; both motor drivers take DRVOFF and nSLEEP from the MCU only. A runaway MCU that still services the watchdog keeps an apply going.	Wire PMIC SAFE_OUT1 to both drivers' nSLEEP; define the release after an independent stop.	EPB-408, BLD-120, PMC-401
2	**The EPB supply cut-off cannot open as published.**	R58 ties the Q11 gate to the 48 V bus, so the only switch independent of the EPB driver is defeated. The EPB driver's own output-stage faults are single-point faults of SG-03.	Fit R58, Q6, R53 and C63 as DNP; add an independent OUTA/OUTB readback that opens the cut-off.	EPB-401, EPB-211, EPB-404
3	**The published BOM is not a buildable 48 V variant.**	Option links for other variants are all fitted: R22 and R97 put the battery on the 12 V rail, R146 enables a second core regulator, both boot straps are fitted.	Issue a variant-controlled BOM; treat option fits as special characteristics.	BCK-401, CAN-401, MCU-101

#	Finding	Consequence	Direction	DFMEA rows
4	**A shorted inverter FET brakes the caliper motor after the stop.**	Dominant SG-01 single-point fault (24 of 31 FIT as built): the shorted phase and the body diodes of the other legs brake the motor, so the caliper may not self-release in the FTTI.	Motor-phase isolation driven independently of U5 (BLD-201); confirm the release profile (OQ-048).	BLD-201, BLD-212
5	**A silent corner is the dominant SG-02 fault.**	About half of the SG-02 failure rate (155 of 309 FIT) is faults that silence the MCU and both CAN channels together; only the brake controller's status timeout sees them.	Make the corner-status timeout a vehicle safety requirement with HIL proof (PMC-118, OQ-050).	PMC-118, PMC-419, CAN-105
6	**Resistive faults on the 48 V bus heat without tripping the breaker.**	Capacitor crack shorts and CAF growth below the U1 trip level dominate SG-07; the breaker sees only hard shorts.	Soft-termination or fail-open bus capacitors, an IMON supply-current check, CAF-resistant laminate (OQ-054, OQ-056).	PCB-202, PCB-303, EPB-423
7	**The 12 V overvoltage cut-off depends on two QM transceivers and is not latched.**	Any bus wake-up ends the cut-off; the path is credited at Medium coverage only.	Add a hardware latch or an INH pull-down independent of the transceivers.	CAN-415, CAN-408, BCK-303

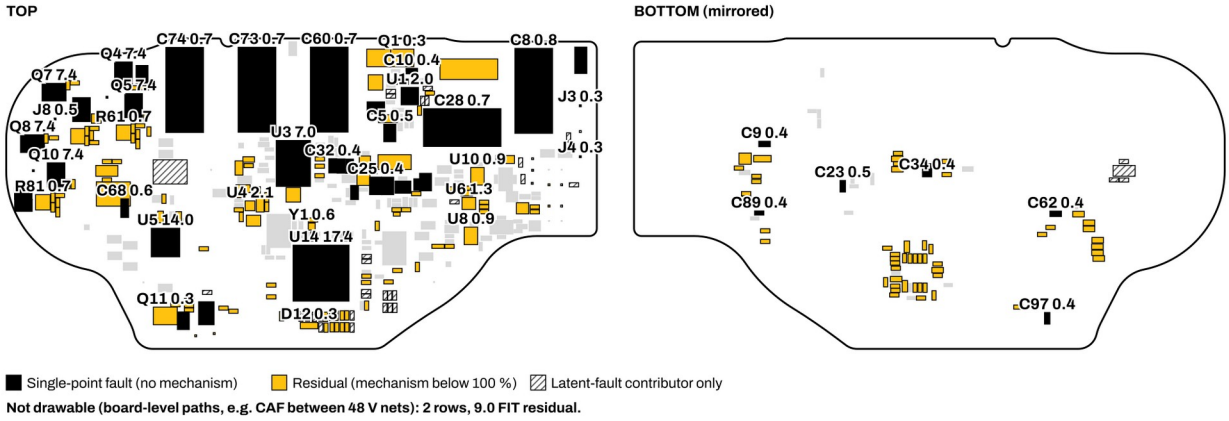


Figure 3. Where the single-point faults sit, as published: every part whose failure violates a safety goal with no mechanism (black), or with a mechanism below full coverage (yellow). All computed goals combined.

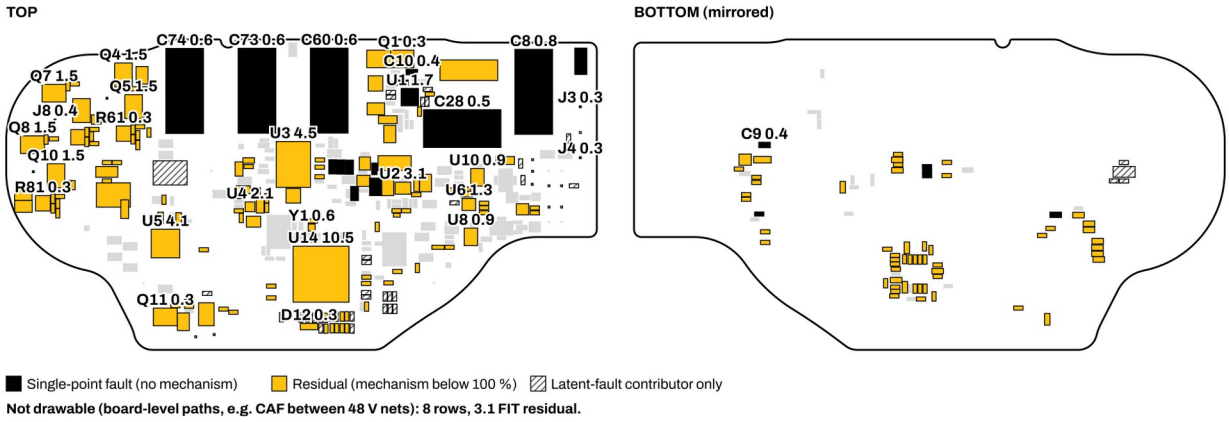


Figure 4. The same map with the DFMEA actions applied. Single-point rows that remain, by goal: SG-01 1, SG-07 10. The SG-07 rows are 48 V bus capacitors, CAF paths and pads that the breaker cannot see; the SG-01 row is the motor-phase pads J7–J9.

1.4 What is needed from Quillon Motors and TI

Table 3. Inputs that close the largest assumptions.

From	Needed	Open questions
TI (via Quillon Motors)	FMEDA and safety manual for U14, U3, U5, U7 and U2; WSS001 documentation	OQ-007, OQ-008, OQ-002
Quillon Motors	PMHF budget per corner for each goal	OQ-046
Quillon Motors	Fault-tolerant time intervals and caliper release profile	OQ-021, OQ-047, OQ-048
Quillon Motors	Mission profile (temperature, operating hours, lifetime)	OQ-010
Quillon Motors	Fitted configuration of the option links (variant BOM)	OQ-011, OQ-029
Quillon Motors	Brake-controller checks credited as assumptions of use (corner status, wheel speed)	OQ-049, OQ-050

2 Scope

2.1 Hardware under analysis

TIDA-020106 PCB VerB as published by TI: schematic SLVMF37A, layout SLVMF38A, BOM SLVMF39A, assembly SLVMF40A, fabrication SLVC962A. The BOM fits every option link of every variant (OQ-011); the analysis treats the published fit as the as-built scenario and the 48 V fit list of TIDUFI0 Fig. 2-5 as part of the recommended actions.

Table 4. DFMEA circuit blocks.

Block	Function	ASIL	Rows
01 Supply input	Pass the 48 V (or 12 V) battery supply to the board; block reverse polarity; clamp surges; cut off on ...	D	95
02 12 V buck	Generate the 12 V rail for the PMIC and gate drivers from 48V/12V_P	D	52
03 PMIC	Generate and monitor 3.3 V, 3.3Vref, 5 V, 5Vp1/5Vp2 and the 1.25 V core; supervise the MCU (watchdog, error ...	D	70
04 MCU	Run the brake control and safety software; sample currents, angle and supply voltages; command the drivers; ...	D	80
05 BLDC inverter	Drive the caliper BLDC motor through the three-phase inverter; measure phase currents; cut off the drive on ...	D	104
06 Motor angle	Measure rotor angle for commutation and clamp-force estimation	D	48
07 EPB	Apply and release the electric parking brake; measure motor current; remove its supply on a fault	D	106
08 Wheel speed	Supply the active wheel-speed sensor and decode its current signal; report speed and standstill	D	56
09 CAN	Receive clamp-force requests and send status on two CAN FD buses; wake the board (INH)	D	87
10 Pedal input	Supply the pedal force and travel sensors and condition their SENT signals for the MCU (fall-back path, A-05)	D	55
11 PCB	Carry every circuit: copper, spacing, stack-up, thermal paths and solder joints	D	30

2.2 Safety goals

Table 5. Assumed safety goals from S10-QLN-HARA-001 Rev B. FTTIs are provisional (ASSUMED, OQ-021).

Goal	Safety goal	ASIL	Safe state	FTTI	Events
SG-01	Avoid braking at a wheel that was not requested (unintended, excessive, misdirected or unreleased clamp force)	D	Clamp force released at that wheel; corner reported unavailable; driver warned	TBD; provisional 100 ms (ASSUMED)	HE-01 to HE-06, HE-19
SG-02	Avoid loss of, insufficient or late braking at a wheel when braking is requested	C	Corner reported unavailable or limited; other corners and regeneration compensate; driver warned	TBD; provisional 200 ms (ASSUMED)	HE-07 to HE-12
SG-03	Avoid parking-brake application while the vehicle is moving, unless the driver requests it	D	EPB actively released and further apply inhibited (de-energising alone keeps the force on a self-locking spindle)	TBD; provisional 300 ms (ASSUMED)	HE-13
SG-04	Avoid loss of parking or standstill hold while the vehicle is stationary	C	Hold maintained or re-applied; driver warned; transmission park lock if fitted	TBD; provisional 1 s (ASSUMED)	HE-14, HE-15

Goal	Safety goal	ASIL	Safe state	FTTI	Events
SG-05	Avoid erroneous wheel-speed information being used by the braking and stability functions	B	Wheel speed marked invalid; braking functions use the other wheels	TBD; provisional 50 ms (ASSUMED)	HE-18
SG-06	Provide parking-brake deceleration when the driver requests it and service braking is unavailable	A	Not applicable (availability goal)	TBD	HE-16
SG-07	Avoid a thermal event (smoke, fire) of the corner ECU	B	Energy removed from the faulty circuit; corner reported unavailable; driver warned to stop	TBD; U1 acts in microseconds to 1 ms, the IMON check needs the time to ignition to exceed its period plus debounce (ASSUMED, OQ-044)	HE-20

2.3 Out of scope

- Software: the DFMEA records every software safety requirement it depends on (section 6.2); the software itself is not analysed.
- Vehicle-level functions: the brake controller, blending, ABS and ESC. Checks they perform are credited only as assumptions of use, each with an open question.
- Systematic faults of the design (wrong part rating, variant fitting): recorded in the DFMEA as design deficiencies; excluded from the random-fault metrics and listed in section 5.5.
- EMC and ESD beyond the interface ratings; production process FMEA.

2.4 Input documents

Table 6. Inputs. TI documents are used under TI's terms and are not redistributed.

Document	Content	Use
TIDUFI0	TI design guide for TIDA-020106	Architecture, intended fit, test results
SLVMF37A–41A, SLVC962A	Schematic, layout, BOM, assembly, Gerber and IPC-356 data	Structure, parts, nets, board drawings
TI FIT/FMD documents	SFFS950 (U1), SFFS465A (U4), SLLA525A (U8, U10), SFFS685 (Y1)	Sourced failure rates and splits
TI certificates and datasheets	SFFSBK8 (TÜV SÜD, F29P329), device datasheets	Ratings, on-chip mechanisms
S10-QLN-HARA-001 Rev B	Hazard analysis, assumed safety goals	Goals, ASILs, safe states
S10-QLN-OQL-001	Open questions log	Assumptions and their closure

3 Method

3.1 DFMEA

3.1.1 Structure and function

AIAG-VDA FMEA handbook, seven steps. Each block is a focus element; each row is one failure chain: failure mode of the focus element, failure cause at the next lower level (a named part or net), and the end effect picked from a fixed effect library (Appendix A) that carries the severity, goal and ASIL. Every fact in a row cites its source document and page.

3.1.2 Rating and action priority

Severity comes from the effect library (S = 10 for every goal-violating effect). Occurrence is rated from the failure rate of the cause and the prevention controls in the published design. Detection rates the design verification that would find the chain before release, not the on-board diagnostics, which are recorded as safety mechanisms and credited in the FMEDA. Action priority (AP) follows the AIAG-VDA table.

Why 765 of 783 rows are High as published. A reference design ships without design verification evidence, so all 783 rows carry D = 9 or 10. With S = 9–10 and D = 9–10 the AIAG-VDA table gives High for every occurrence above 1; the 18 rows that are not High have S of 8 or less. High AP here means that no verification evidence exists and every chain needs an action, not that every chain is a design defect.

3.1.3 Filters

Filter	Meaning	Rows
LAT	Latent: a safety mechanism is lost with no effect until a second fault	191
CC	Common cause shared with another channel or block (input to the dependent-failure analysis)	166
SC	Special characteristic to be controlled in production (PFMEA, control plan)	133

3.2 FMEDA

3.2.1 Row classification

ISO 26262-5:2018 clauses 8 and 9, Annexes C and D. One row per component failure mode, per safety goal. Each row is classed per scenario as Safe, Direct (violates the goal alone: single-point if no mechanism acts, residual otherwise), Latent (violates it only by disabling a mechanism that is active in that scenario) or n/a. Faults with no path to the goal are n/a, not Safe, so they do not inflate the SPFM.

3.2.2 Scenarios

Table 7. Scenarios. A = VerB as built; B = with the DFMEA actions. The report uses "as built" and "with actions" for A and B throughout.

Scenario	Hardware and mechanisms
A, as built	Published hardware (R58 fitted, PMIC SAFE_OUT1 unconnected, no EPB terminal readback). Software safety mechanisms the hardware allows are credited as the DFMEA specifies them (ASSUMED, OQ-032).
B, all goals (EPB)	R58, Q6, R53 and C63 not fitted (EPB-401, EPB-404, EPB-406), SAFE_OUT1 pulls U7 nSLEEP low (EPB-408), 10 kOhm DRVOFF pull-up (EPB-121), OUTA/OUTB voltage readback (EPB-211, EPB-314), periodic cut-off test (EPB-411)
B, SG-01	U5 input pull resistors (BLD-102), SAFE_OUT1 also to U5 nSLEEP (BLD-120), motor-phase isolation driven independently of U5 (BLD-201, BLD-118), angle-input pull-downs (ANG-101), split ADC modules and a reference check (ANG-306, PMC-201)
B, SG-05	a WSSO pull-down at U14.31 (WSS-302)
B, SG-02	the corner-status timeout as a vehicle requirement (PMC-118), stay unavailable after an unplanned reset (PMC-419), a drive-response monitor (BLD-104, BLD-110, BLD-202) and per-channel CAN loss reporting (CAN-105)
B, SG-07	soft-termination AEC-Q200 bus capacitors away from the board edge (SUP-417, BCK-103, BCK-104, BLD-401, EPB-201, PCB-201), 50 V 125 C parts on the 12 V rail (BCK-403, BCK-409), an IMON supply-current check (PCB-202, SUP-314) and CAF-resistant laminate with wider 48 V spacing (PCB-302, PCB-303)

3.2.3 Metrics

Metric	Definition
λ counted	Σ λ mode over rows not classed n/a
SPFM	1 – Σ(λ SPF + λ RF) / Σλ counted
LFM	1 – Σλ MPF,latent / (Σλ counted – Σλ SPF – Σλ RF)
PMHF	Σλ SPF + Σλ RF + Σ(λ MPF,latent × partner λ) × T / 10^9, T = operating hours over life (8,000 h, ASSUMED, OQ-010); no ½ factor

3.2.4 Coverage credit rules

- A mechanism is credited only if it can detect that failure mode and its reaction reaches the goal's safe state within the FTTI. Where a reaction only stops an actuator without releasing it, the credit is conditional and carries an open question (OQ-047, OQ-048).
- Annex D values (Low 60 %, Medium 90 %, High 99 %) are maximums. Values at a ceiling are argued in the mechanism's basis; most are credited one band below what the vendor claims until the vendor data arrives.
- Partner rows are named per latent row, and their λ enters the dual-point PMHF term by formula.

3.3 Failure-rate basis and mission profile

Table 8. Failure-rate sources.

Class	Source in Rev A	Status
TI ICs with FIT/FMD documents (U1, U4, U8, U10, Y1)	TI document, IEC TR 62380 / ISO 26262-11 basis	Sourced
TI ICs with data on request (U14, U3, U5, U7, U2, U12, U13)	Order-of-magnitude rate; shares by sev10	ASSUMED (GATED, OQ-007)
WSS001-Q1 (U6)	Order-of-magnitude rate; shares by sev10	ASSUMED (UNRELEASED, OQ-008)
Passives, discretes, joints, PCB	SN 29500-order class values at 85 °C; class splits	ASSUMED (OQ-010)
Mission profile	–40 to +105 °C, 15 years, 8,000 operating hours	ASSUMED (OQ-010)

3.4 Assumed values

A value that rests on an assumption is shaded orange and carries the word ASSUMED, a reason code (GATED, UNRELEASED, NO-CLIENT-DATA, JUDGMENT, PROVISIONAL) and the open question that closes it. The workbooks list every assumed value; the FMEDA register groups them by what closes them.

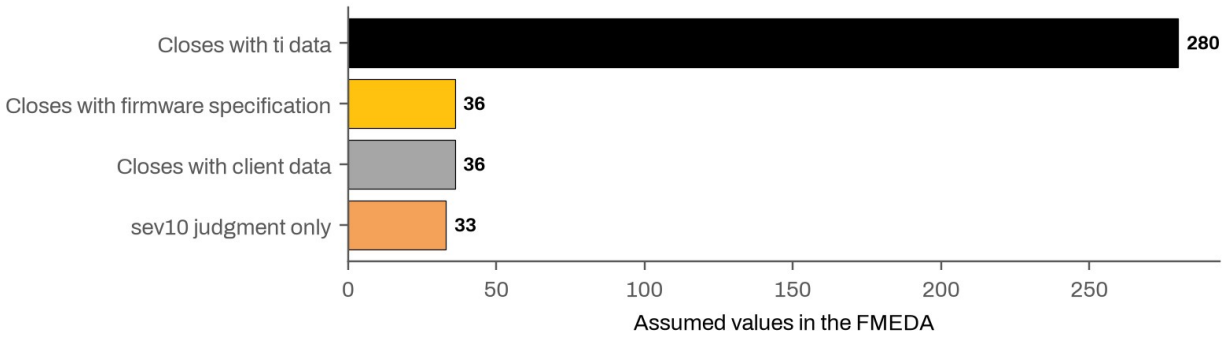


Figure 5. FMEDA assumed values by what closes them.

3.5 Review and verification

- DFMEA: four checkpoints, each reviewed by a separate sev10 reviewer; an automated consistency check verifies every row's effect, parts, nets, ratings and source citation (783 rows, 0 errors).
- FMEDA: three separate sev10 reviews (method, sourcing, client view), each finding applied or dropped with a reason (Appendix D). Every metric is a live workbook formula, checked against an independent calculation.
- This report: four separate reviews (technical accuracy, writing, figures, client view) before issue.
- All reviews are internal to sev10; independence per ISO 26262-2 Table 1 is to be arranged for the confirmation review.

4 DFMEA results

4.1 Overview

783 failure chains, 769 with a recommended action. As published 765 rows are High priority; with the actions 23 remain High. 391 rows depend on a software safety requirement.

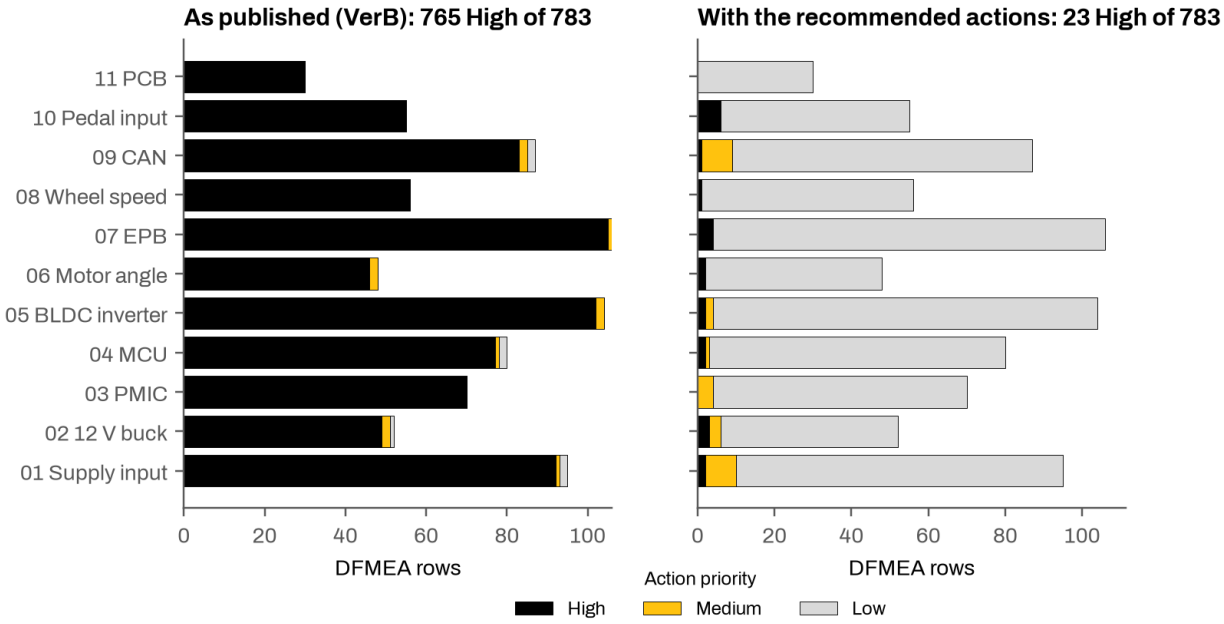


Figure 6. Action priority per block, as published and with the actions.

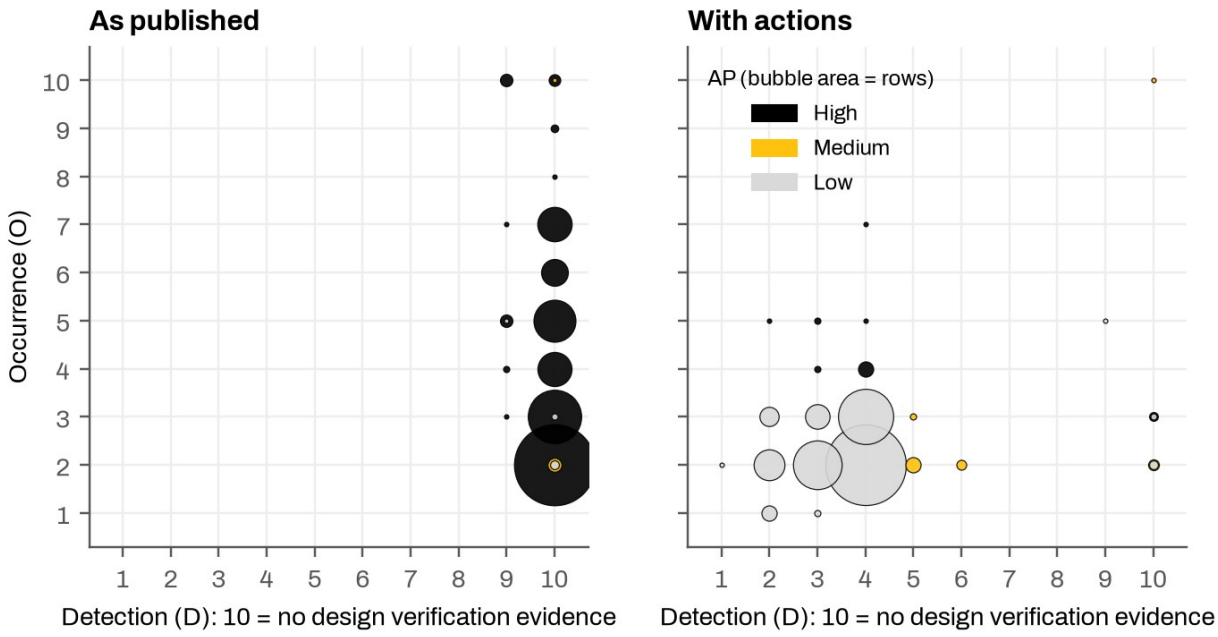


Figure 7. Occurrence against detection. As published every chain sits at D = 9–10 (no verification evidence); with the actions 760 of 783 rows reach D ≤ 5, and occurrence drops where the design changes.

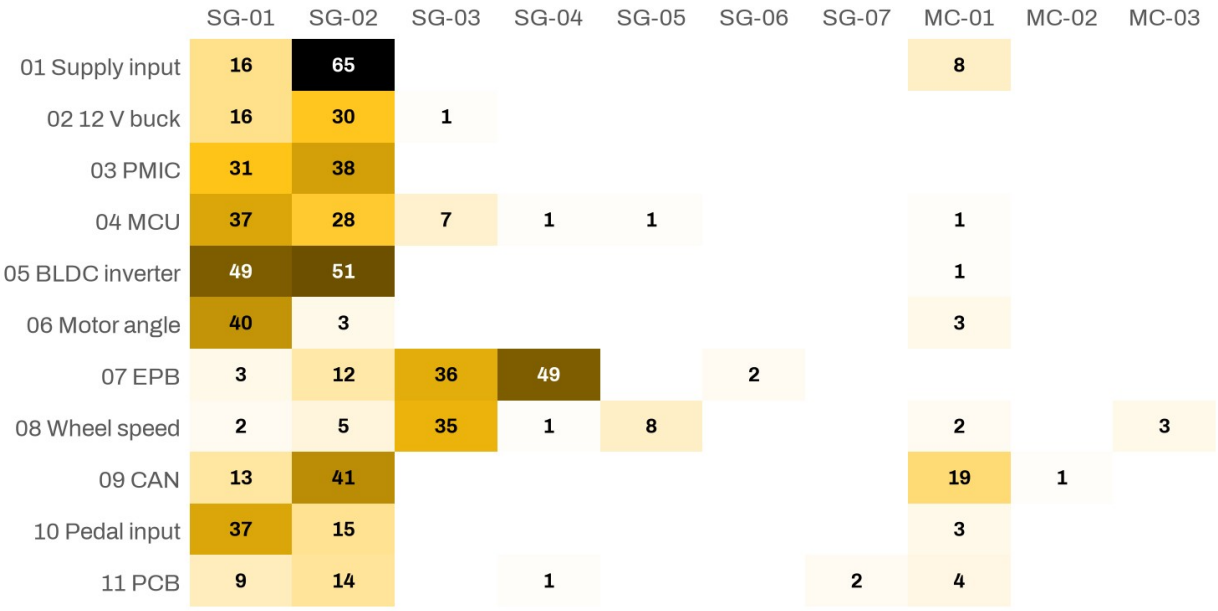


Figure 8. DFMEA rows by block and by the goal their effect violates (MC-01 to MC-03 are the multi-corner goals of the HARA). 39 rows with QM or regulatory effects are not shown.

4.2 Findings by circuit block

4.2.1 Supply input

Function	Boundary	Goals	Rows	High (pub. → actions)
Pass the 48 V (or 12 V) battery supply to the board; block reverse polarity; clamp surges; cut off on overvoltage and overcurrent	J3/J4 supply pads to the protected rail 48V/12V_P: U1 LM74930-Q1, back-to-back FETs Q1/Q2, TVS D1, L1, sense and gate networks	SG-01, SG-02, SG-03, SG-04, MC-01, SG-07	95	92 → 2

1. D1 breaks down inside the 52-60 V band and U1 trips at 57.9-64.9 V: fast surges pass before the cut-off acts. Size clamp and OV response to an agreed surge profile (SUP-101, 102, 304, OQ-017).

2. Q1 exceeds its SOA charging about 1.1 mF at every power-up. Add a pre-charge path sized against the transceiver start-up window, not a slower gate ramp (SUP-201, CAN-417).

3. D10 (62 V zener on VS) conducts from the battery below the OV trip when cold, and D2/D3 are commercial-grade. Use the 60 V reference zener and AEC-Q101 parts (SUP-204, 120, OQ-018).

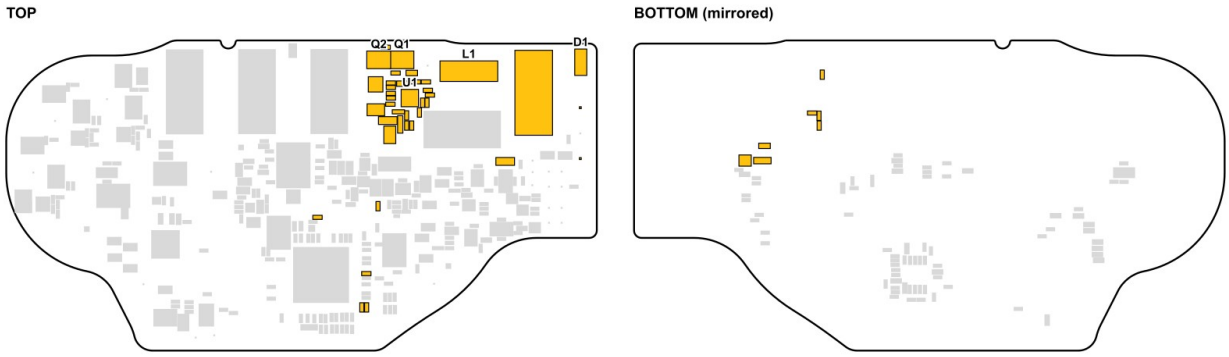


Figure 9. Supply input: parts of the block on PCB VerB (yellow).

Table 9. Rows still High with the actions. Block SUP.

Row	Failure mode	Recommended action	AP after
SUP-219	Q2 cannot block	Confirm whether reverse connection and negative surges apply to the 48 V input (OQ-017); if yes, a periodic check is not possible, so budget the fault as latent in the FMEDA.	H
SUP-304	OV cut-off too slow for a fast overvoltage from a stiff source: 48V/12V_P follows the input above 70 V	Agree the 48 V surge model (OQ-017: level, edge rate, energy, source impedance) and dimension the input clamp (SUP-101, SUP-102) and the OV response against it as one task. Keep C17 until the stiff-source case shows a need; any reduction must be re-checked for nuisance trips against SUP-301 and SUP-310.	H

4.2.2 12 V buck

Function	Boundary	Goals	Rows	High (pub. → actions)
Generate the 12 V rail for the PMIC and gate drivers from 48V/12V_P	U2 LM68645-Q1, L2, feedback and enable networks, output capacitors, power-good indication	SG-01, SG-02, SG-03, SG-04, SG-07	52	49 → 3

1. As published, R22 ties the 12V rail to the 48 V bus, overstressing the PMIC, the gate-driver supply and 25 V capacitors. Fit R22 DNP under variant control (BCK-401, 402, OQ-011).

2. The 12 V disconnect cannot isolate a buck high-side short: Q3 is rated 30 V and Q12 is not guaranteed to turn on from a 3.3 V GPIO. Re-design the disconnect (BCK-101, 301, 302).

3. 12 V over/undervoltage protection rests on an undocumented U2 variant with no UVP and on unspecified comparator firmware. Get TI data and write the SW requirements (BCK-204, 218, 304).

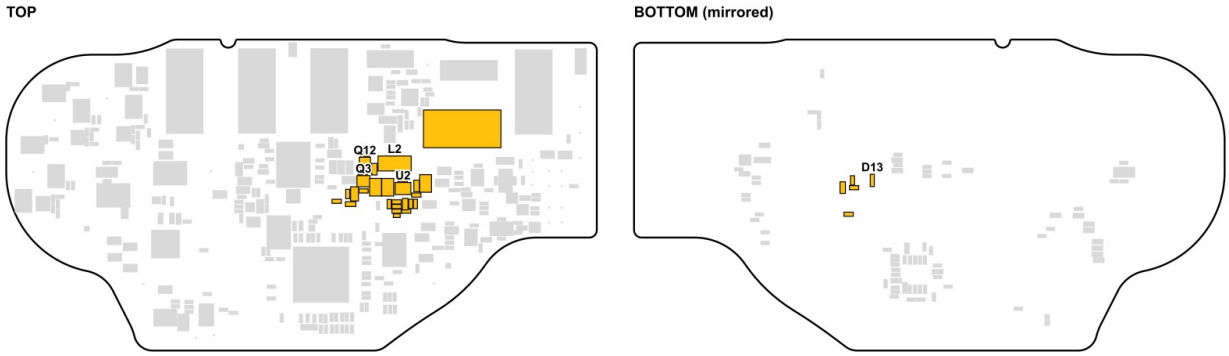


Figure 10. 12 V buck: parts of the block on PCB VerB (yellow).

Table 10. Rows still High with the actions. Block BCK.

Row	Failure mode	Recommended action	AP after
BCK-206	U2 overvoltage protection or FAULT output cannot act	Request to TI (source: LM68645-Q1 FMEDA and safety manual, OQ-007): confirm whether ABIST covers the OVP comparator and FAULT driver; credit latent-fault coverage in the FMEDA only as TI states it	H
BCK-207	Output voltage error not seen by the redundant monitor (common cause)	Request to TI (source: LM68645-Q1 safety manual, OQ-007): confirm the OVP comparator uses a reference independent of the FB error amplifier; otherwise credit only CMPSS4 for OV in the FMEDA and the dependent-failure analysis	H
BCK-304	U2 does not assert FAULT on an output fault, or its FAULT drive of Q3 differs from what the design assumes	Request to TI (source: full LM68645-Q1 datasheet and safety manual for the SC variant, OQ-019, OQ-007); credit SM-4 only for the fault classes TI states	H

4.2.3 PMIC

Function	Boundary	Goals	Rows	High (pub. → actions)
Generate and monitor 3.3 V, 3.3Vref, 5 V, 5Vp1/5Vp2 and the 1.25 V core; supervise the MCU (watchdog, error signal); drive the safe state	U3 TPS653860-Q1 (NVM variant O386005), U4 TPS62902-Q1 core buck, L3/L4, rail capacitors, SPI and diagnostic lines to the MCU	SG-01, SG-02, SG-03, SG-04, SG-05	70	70 → 0

1. No PMIC path switches the drivers off: SAFE_OUT1 is unwired and the only reaction is a U14 reset of unstated timing. Wire SAFE_OUT1 to U5/U7 nSLEEP (PMC-401, BLD-120, OQ-027).

2. EXT_VMON1 is the only core overvoltage protection, too slow for a shorted U4 high side (about 1 us to 1.5 V). Add a fast 1.25 V clamp and fit R146 DNP (PMC-303, 304, 217, OQ-042).

3. 3.3Vref is the only ADC and comparator reference and nothing cross-checks it. Add an independent reference check before force control relies on it (PMC-201, 202, OQ-043).

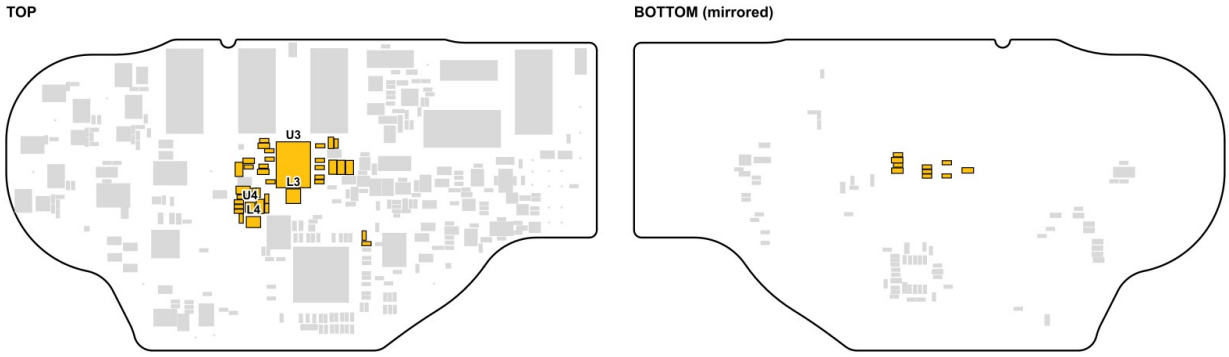


Figure 11. PMIC: parts of the block on PCB VerB (yellow).

Table 11. Highest-occurrence rows and their actions. Block PMC.

Row	Failure mode	Recommended action	AP after
PMC-101	U3 VBAT and its input capacitors at the 48 V class instead of 12 V	For the 48 V variant, make R22 DNP and release a variant-controlled BOM (fit list per OQ-011). Dependent-failure analysis of a 12 V overvoltage on U3, U5 and U6 (with BCK-101) to confirm or exclude unintended clamp force through shorted inverter FETs (A-08, OQ-023)	L
PMC-217	3.3V overloaded: LDO1 in current limit or U3 in overtemperature	Do not fit R146; tie VREGENZ high to VDDIO so U4 is the single VDD source and the EXT_VMON1 supervision is supported (SPRSP93E p.94, p.122-123)	L
PMC-103	Bulk capacitor degrades to a short on 12V or VCC_6V0	Replace with AEC-Q200 X7R (or X7S) parts rated to 125 C, 50 V, with at least the same effective capacitance at 12 V / 6 V (1206 if needed); same change for C27 and C57	L

4.2.4 MCU

Function	Boundary	Goals	Rows	High (pub. → actions)
Run the brake control and safety software; sample currents, angle and supply voltages; command the drivers; hold boot straps	U14 F29P329SM-Q1 (all symbol parts), Y1 CDC6C-Q1 oscillator, J23, analog reference filters, boot straps, J10 header, status LEDs	SG-01, SG-02, SG-03, SG-04, SG-05	80	77 → 2

1. The BOM MCU part is not a production orderable and is outside the TUV certificate, so no U14 diagnostic coverage can be claimed. Order the certified part (MCU-501, OQ-001).

2. R146 enables the internal VREG beside U4, which TI does not support. Leave R146 unfitted, tie VREGENZ high with a pull-up and remove the footprint (MCU-101, 103, OQ-042).

3. Each boot pin has 10 k up and 10 k down (about 1.65 V), and the 329SM2 has 4 CMPSS (8 comparators) for 9 credited trips. Fit pull-ups only and re-allocate trips (MCU-205, 301).

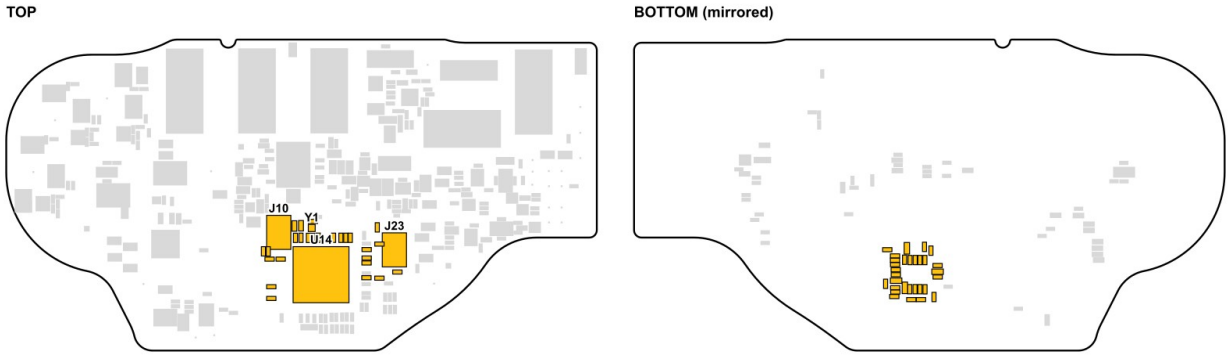


Figure 12. MCU: parts of the block on PCB VerB (yellow).

Table 12. Rows still High with the actions. Block MCU.

Row	Failure mode	Recommended action	AP after
MCU-509	Flash content lost beyond ECC correction; U14 resets or does not start	Obtain TI retention data versus TJ (OQ-007); thermal analysis of U14 TJ over the mission profile (OQ-010); keep TJ-hours above 85 C within TI's retention limit, or add a scheduled reflash/refresh at service.	H
MCU-514	U14 permanent-fault rate rises with operating life (loss of this corner)	Thermal analysis of U14 TJ over the mission profile with TI's lifetime calculator (SPRSP93E p.109 reference); keep R146 DNP so the internal VREG loss (up to about 1.2 W at its 500 mA load limit) is not dissipated in U14; confirm the thermal via array under the PowerPAD.	H

4.2.5 BLDC inverter

Function	Boundary	Goals	Rows	High (pub. → actions)
Drive the caliper BLDC motor through the three-phase inverter; measure phase currents; cut off the drive on command	U5 DRV3263-Q1, inverter FETs Q4/Q5/Q7-Q10, shunts R61/R80/R81, bootstrap and snubber networks, bulk capacitors, Q6 cut-off transistor, J7-J9	SG-01, SG-02, SG-07	104	102 → 2

1. No BLDC disable path is independent of the MCU: DRVOFF and nSLEEP come only from U14. Wire PMIC SAFE_OUT1 to U5 nSLEEP as specified in BLD-120 (OQ-027).

2. While U14 is in reset the U5 disable and PWM inputs float, and U5 internal pulls are unpublished. Add defined pull-downs and confirm the reset state with TI (BLD-102, 118, OQ-007).

3. A high-side phase-to-GND short bypasses the low-side shunts; only the U5 VDS monitor stops it. Set its threshold from the FET withstand time and self-test it (BLD-317, 222, OQ-032).

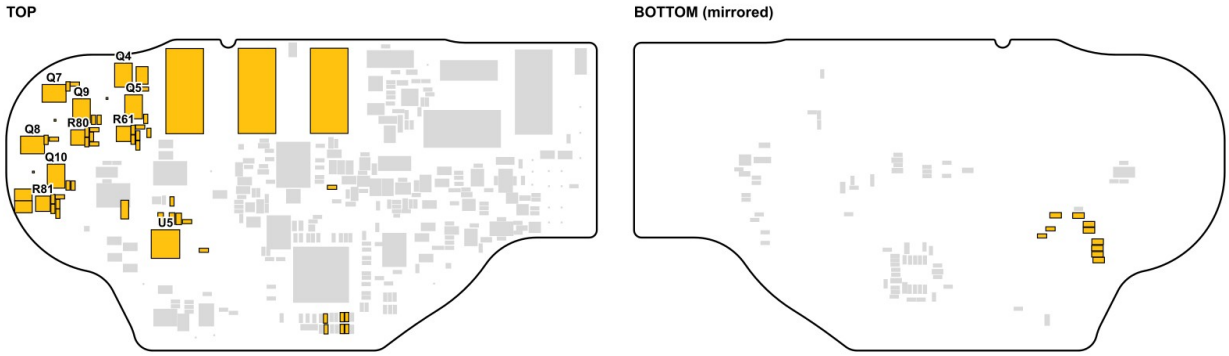


Figure 13. BLDC inverter: parts of the block on PCB VerB (yellow).

Table 13. Rows still High with the actions. Block BLD.

Row	Failure mode	Recommended action	AP after
BLD-212	Phase output short; inverter overcurrent, then braking torque on the motor	Phase isolation as BLD-201; specified sealed, keyed production connector with strain relief (OQ-004) for the caliper lead; harness routing and chafe protection of the phase wires (OQ-037).	H
BLD-317	Shunt-based overcurrent trips blind to phase-to-GND fault current (coverage gap)	No hardware change proposed. Requires SW: enable U5 VDS overcurrent with threshold, blanking and deglitch set so that detection plus turn-off stays below the SQJA90EP short-circuit withstand budget derived in BLD-222 (not the 100 us SOA current); credit the shunt trips in the FMEDA only for faults that pass a ...	H

4.2.6 Motor angle

Function	Boundary	Goals	Rows	High (pub. → actions)
Measure rotor angle for commutation and clamp-force estimation	U12 and U13 TMAG6180-Q1 (top and bottom side, same magnet), J21/J22, supply decoupling and output filters	SG-01, SG-02	48	46 → 2

1. No pull resistors on either angle sensor, so a sensor fault state reads as a frozen, valid angle for hundreds of ms. Fit 100 kOhm pull-downs (ANG-101, 201).

2. The two sensors share one magnet, the 3.3V rail, 3.3Vref and the MCU, so common causes pass the channel compare. Specify the compare and a diverse check (ANG-301, 309, 113).

3. The 100 us sensor filters lag about 35 deg electrical at top motor speed. Reduce them to about 10 us and compensate lag in software (ANG-112, OQ-034).

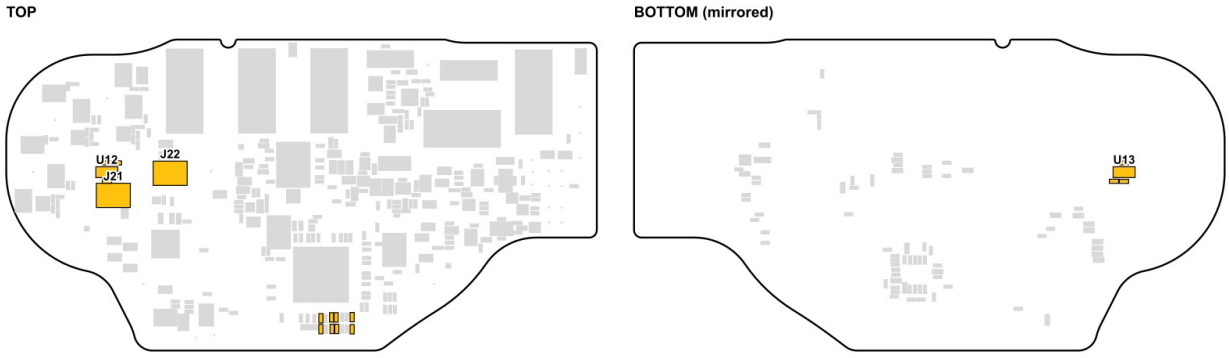


Figure 14. Motor angle: parts of the block on PCB VerB (yellow).

Table 14. Rows still High with the actions. Block ANG.

Row	Failure mode	Recommended action	AP after
ANG-301	Angle channels are not independent enough to support ASIL D by decomposition; common-cause faults defeat the channel comparison	Run a dependent-failure analysis (ISO 26262-9 cl. 7) of the angle function and decide the architecture: at least supply U13 from a separate regulator (PMIC LDO4 is unused on VerB), convert the channels on different ADC modules (ch1 ADC A/B, ch2 ADC C/D: pins 24 and 16 reach C25/D27) and add a diverse check ...	H
ANG-304	Common angle error that grows with motor current; both channels agree	Keep phase conductors and motor leads away from the sensor axis; state a stray-field budget (e.g. < 1 % of the minimum magnet field in-plane) in the motor/ECU interface	H

4.2.7 EPB

Function	Boundary	Goals	Rows	High (pub. → actions)
Apply and release the electric parking brake; measure motor current; remove its supply on a fault	U7 DRV8263-Q1, cut-off FET Q11 and its gate network (Cutoff_EPB), current-sense network, J5/J6	SG-03, SG-04, SG-06, SG-07	106	105 → 4

1. As published the EPB cut-off cannot open: R58 ties the Q11 gate to 48 V and Q6 (50 V) sits near 60 V. Fit per TI's 48 V build: R58, Q6, R53, C63 out (EPB-401 to 406).

2. No EPB stop path is independent of the MCU, and cutting the supply blocks the active release SG-03 needs. Decide the SG-03 reaction in the TSC (EPB-408, 409, OQ-027).

3. C96 (general-grade 1210 on 48 V) can crack-short the EPB branch at up to ~1 kW below the breaker, taking the corner down. Use a fail-open part and a branch limit (EPB-201, 423).

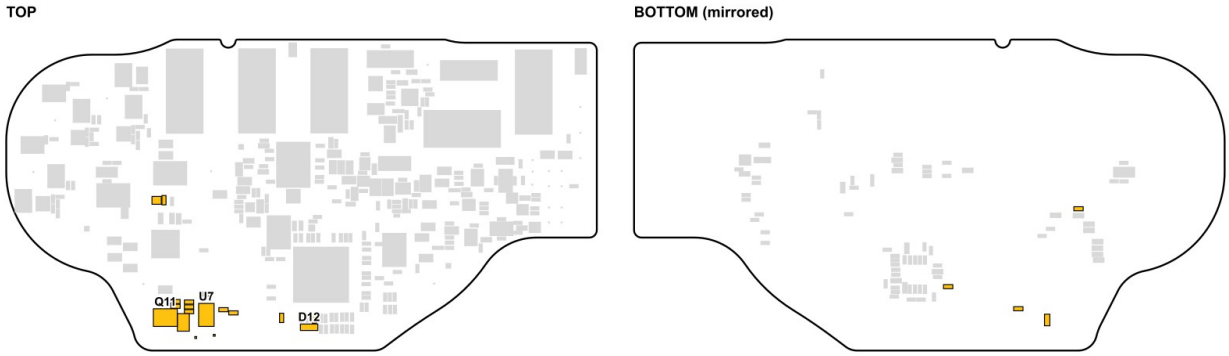


Figure 15. EPB: parts of the block on PCB VerB (yellow).

Table 15. Rows still High with the actions. Block EPB.

Row	Failure mode	Recommended action	AP after
EPB-221	OCP lost (latent): a later output short is not current-limited	Obtain the DRV8263-Q1 FMEDA and safety manual (OQ-007): OCP failure rate, any latent-fault diagnostic or start-up test; if none, add an EPB-branch current limit or fuse (see EPB-201) so that a U7 short cannot latch off the ECU supply.	H
EPB-409	Cut-off stops an apply but removes the only means of active release	Technical safety concept: define the SG-03 reaction (cut-off timing budget from EPB force ramp vs rear-lock threshold; conditions under which VM is restored for a release through a path independent of the fault)	H
EPB-410	Cut-off opens (EPB unpowered) whenever the BLDC gate driver is off or faulted	Keep the EPB supply path independent of the BLDC driver state (separate cut-off driver or defined CUTOFF1 state that stays on in U5 fault/sleep unless the EPB itself must stop); document in the safety concept	H
EPB-412	Q11 held on: CUTOFF1 stays high regardless of the command	SW requirement: cyclic readback of U5 cut-off registers; cut-off test as EPB-411	H

4.2.8 Wheel speed

Function	Boundary	Goals	Rows	High (pub. → actions)
Supply the active wheel-speed sensor and decode its current signal; report speed and standstill	U6 WSS001-Q1, ESD protection D5, input filters, J1/J2, SPI and WSSO lines to the MCU	SG-05, SG-03	56	56 → 1

1. If this wheel alone grants the EPB apply permission (assumed, OQ-035), any fault that stops the pulses reads as standstill after the timeout. Add a second source (WSS-315).

2. A 48 V harness short onto WSP/WSN overloads the 24 V clamp D5 and R86/R88. Use a TVS rated 60 V or more, series protection and segregated routing (WSS-205, OQ-037).

3. WSSO has no pull and an unconfirmed capture route to the MCU. Add a defined pull and route WSSO to an eCAP input with a confirmed X-BAR path (WSS-304, 302).



Figure 16. Wheel speed: parts of the block on PCB VerB (yellow).

Table 16. Rows still High with the actions. Block WSS.

Row	Failure mode	Recommended action	AP after
WSS-212	U6 sensor pins damaged or degraded by ESD or surge on the harness	Obtain WSS001 pin ESD and surge ratings (OQ-008); place D5 at the connector pins in the production layout	H

4.2.9 CAN

Function	Boundary	Goals	Rows	High (pub. → actions)
Receive clamp-force requests and send status on two CAN FD buses; wake the board (INH)	U8/U10 TCAN1043H-Q1, ESD U9/U11, chokes L5/L6, termination, J17-J20	SG-01, SG-02, MC-01, MC-02	87	83 → 1

1. A 48 V short on a CAN line exceeds the 50 V common-mode chokes and the unreleased ESD2CAN48 is unrated for it: the bus can be lost at every node (CAN-313, 314, OQ-008).

2. Brake requests pass QM transceivers with no E2E, no loss-of-CAN reaction and no corner identity. Specify E2E with a per-corner data ID (CAN-101, 102, 131, OQ-040).

3. Split termination is fitted on every ECU although this corner is not a bus end node: extra terminations lower bus impedance for all nodes. Fit per bus position (CAN-316, OQ-039).



Figure 17. CAN: parts of the block on PCB VerB (yellow).

Table 17. Rows still High with the actions. Block CAN.

Row	Failure mode	Recommended action	AP after
CAN-417	ECU start-up aborted by the transceiver undervoltage timer	One worst-case analysis with the SUP-201 inrush/SOA analysis and the load start profile: VSUP rise to 5V and 3.3V valid against tUV 159 ms with margin, U2 and the PMIC starting early in the 48V/12V_P ramp rather than after it settles, at -40 C and the item's specified minimum start-up input (at least the worst-case ...	H

4.2.10 Pedal input

Function	Boundary	Goals	Rows	High (pub. → actions)
Supply the pedal force and travel sensors and condition their SENT signals for the MCU (fall-back path, A-05)	J11-J16, input dividers and filters R1-R6/C1-C4, 0-ohm SENT routing links; sensor supplies from the PMIC tab. ASSUMED role (A-05, OQ-009, OQ-038): fall-back ...	SG-01, SG-02, MC-02	55	55 → 6

1. At the assumed 3 us SENT tick neither pedal input decodes SENT: the 41 us input RC passes frames only above about 11 us. Redesign the receiver to tau 2 us or less (PED-101, 201, OQ-036).

2. The fall-back has no specified CAN timeout, source arbitration or plausibility, so an erroneous pedal value becomes a brake demand after CAN loss. Specify them (PED-302, 310, OQ-038).

3. Both SENT and analog paths are fitted, and in the analog build pin leakage can shift both readings alike. Fit one path per variant and control it in the BOM (PED-103, 217, OQ-011).

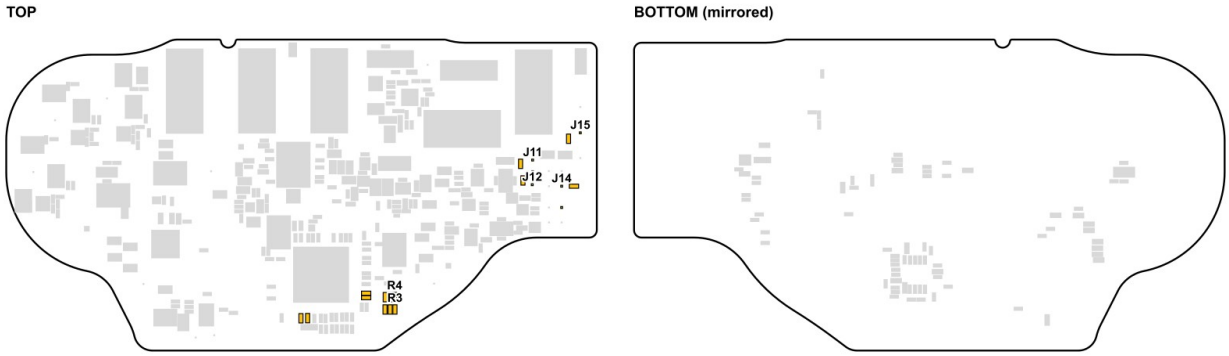


Figure 18. Pedal input: parts of the block on PCB VerB (yellow).

Table 18. Rows still High with the actions. Block PED.

Row	Failure mode	Recommended action	AP after
PED-106	Force input stuck at full scale	Requires SW: range check with the invalid band defined from the sensor specification (OQ-036); analog variant: pull-down instead of pull-up (PED-104).	H
PED-108	No force signal reaches U14 (fall-back demand lost)	Requires SW: diagnose loss of the fall-back input cyclically and report it (makes the fault detected rather than latent).	H
PED-109	Force sensor supply shorted to ground	Requires SW: map the PLDO1 UV/current-limit flag to fall-back unavailability; confirm the NVM reaction does not reset the MCU on a sensor-supply fault (OQ-002).	H
PED-204	Travel input stuck at full scale (analog) or static high (SENT)	Requires SW: range check with the invalid band defined from the sensor specification (OQ-036); analog variant: pull-down instead of pull-up (PED-205).	H
PED-206	No valid travel frames reach U14 SENT1: line static low or SENT input disconnected	Requires SW: fall-back unavailable reported to the brake controller and driver warning at the first missed-frame timeout	H

4.2.11 PCB

Function	Boundary	Goals	Rows	High (pub. → actions)
Carry every circuit: copper, spacing, stack-up, thermal paths and solder joints	Bare board !PCB1 and board-level causes common to all tabs: clearance and creepage at 48 V, adjacent-pad shorts, CAF, thermal, solder fatigue	SG-01, SG-02, SG-03, SG-04, SG-05, MC-01, SG-07	30	30 → 0

1. Several 48 V gaps between terminations are below the 0.5 mm IPC-2221B value for an uncoated board, and the vias are untented. Coat the board or re-space (PCB-101, 102, OQ-030).

2. C75/C76 (general-grade 1210 across 48 V) sit 0.3-1.4 mm from the routed edge with no fuse behind them. Move them, use a fail-open part and add a branch fuse (PCB-201, 202, 204).

3. No thermal analysis exists for the released stack-up, pours and housing, and TI rates the board to 75 C open frame only. Define the heat path and verify at 105 C (PCB-401, 404, OQ-010).

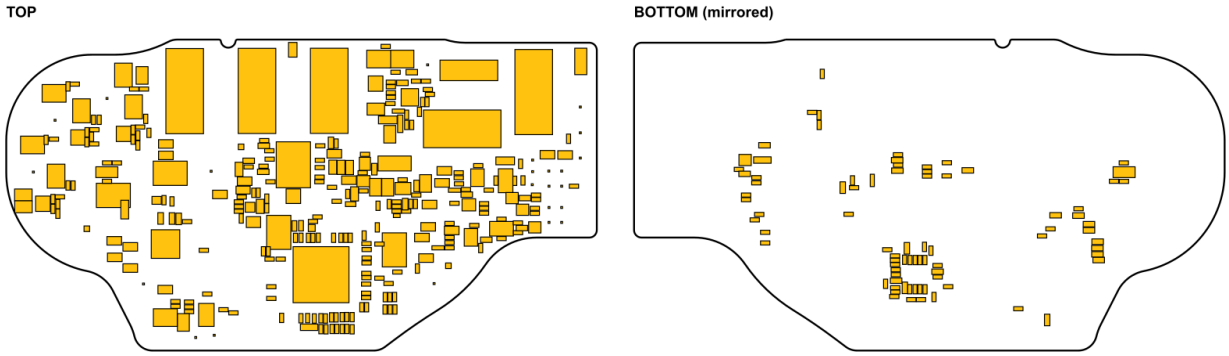


Figure 19. PCB: parts of the block on PCB VerB (yellow).

Table 19. Highest-occurrence rows and their actions. Block PCB.

Row	Failure mode	Recommended action	AP after
PCB-202	Partial (resistive) short on 48V/12V_P not isolated; the capacitor overheats	Use fail-open capacitors on the 48 V bus (floating-electrode 100 V MLCCs, or two soft-termination parts in series) or add a fuse or eFuse below the U1 OCP band; specify the IMON idle-current check as a SW safety requirement.	L
PCB-404	Board-wide overtemperature at sustained load	Define the housing heat path (thermal pad or gap filler from the power-stage and input-FET area to the housing) and the brake duty cycle; add an NTC at the power stage read by U14 with a derating and report requirement.	L
PCB-101	Surface leakage or bridging across 48 V-class gaps at several places at once	Define the board protection concept: conformal coating (IPC-CC-830 qualified) over at least the 48 V zones, an ionic cleanliness limit for assembly, and the housing sealing and breather requirement. Tent or plug all vias outside component pads (IPC-4761 Type VI or VII), or cover them with the coating. Otherwise ...	L

4.3 Cross-cutting findings

Table 20. Findings that span several blocks.

Finding	Direction	Rows
No MCU-independent way to stop either motor	The PMIC safe-state output is unconnected and the EPB and BLDC drivers take DRVOFF/nSLEEP only from the MCU. Wire PMIC SAFE_OUT1 to both drivers' nSLEEP, and define how the brake is released after an independent stop.	EPB-408, EPB-409, BLD-120, PMC-401 (OQ-027)
The published BOM is not a buildable 48 V variant	Option links for other variants are all fitted: R22 and R97 put the battery on the 12 V rail and the CAN supply, R58 defeats the EPB cut-off, R146 enables a second core regulator, and both boot straps are fitted. Issue a variant-controlled BOM and treat fits as special characteristics.	BCK-401, CAN-401, EPB-401, MCU-101, MCU-205 (OQ-011, OQ-029, OQ-042)
The 12 V overvoltage cut-off is not latched and depends on two QM transceivers	The cut-off works only if both CAN transceivers go to sleep, and any bus wake-up ends it. Add a hardware latch or an INH pull-down path independent of the transceivers, and specify the comparator configuration.	CAN-415, CAN-408, SUP-405, BCK-303 (OQ-014, OQ-041)
48 V pads sit closer than IPC-2221B allows for an uncoated board	Several 48 V-class gaps between component terminations are below the 0.5 mm uncoated value, the vias are untented, and two 1210 capacitors across the 48 V bus sit within 4 mm of the board edge. Coat the board or re-space, and move or replace the edge capacitors.	PCB-101, PCB-102, PCB-201, EPB-110, EPB-407 (OQ-030)

4.4 Recommended actions

769 actions, all open: 411 Quillon HW, 202 Quillon SW, 149 Quillon V&V, 7 TI (via Quillon).

Table 21. The 23 rows that remain High priority with the actions.

Row	Block	Failure mode	Prevention action	Detection action	Owner	Due
SUP-219	SUP	Q2 cannot block	Confirm whether reverse connection and negative surges apply to the 48 V input (OQ-017); if yes, a periodic check is not possible, so budget the fault as latent in the FMEDA.	Fault injection: Q2 shorted, reverse connection at -54 V through the agreed source impedance: pass if the harness fuse (OQ-025) clears or the reverse current stays below 1 A within 100 ms, with no damage outside the corner.	Quillon V&V	2026-12-18
SUP-304	SUP	OV cut-off too slow for a fast overvoltage from a stiff source: 48V/12V_P follows the input above 70 V	Agree the 48 V surge model (OQ-017: level, edge rate, energy, source impedance) and dimension the input clamp (SUP-101, SUP-102) and the OV response against it as one task. Keep C17 until the stiff-source case shows a need; any reduction must be re-checked for nuisance trips against SUP-301 and SUP-310.	Worst-case analysis of the OV response against the agreed surge model, with C8 impedance at -40 C and the bulk tolerance; surge test per ISO 21780 at the agreed edge rate and source impedance with 48V/12V_P monitored: pass if 48V/12V_P stays below 65 V. DFA of a 48 V-class overvoltage on the 12 V ...	Quillon HW	2026-11-13
BCK-206	BCK	U2 overvoltage protection or FAULT output cannot act	Request to TI (source: LM68645-Q1 FMEDA and safety manual, OQ-007): confirm whether ABIST covers the OVP comparator and FAULT driver; credit latent-fault coverage in the FMEDA only as TI states it	—	Quillon HW	2026-11-13
BCK-207	BCK	Output voltage error not seen by the redundant monitor (common cause)	Request to TI (source: LM68645-Q1 safety manual, OQ-007): confirm the OVP comparator uses a reference independent of the FB error amplifier; otherwise credit only CMPSS4 for OV in the FMEDA and the dependent-failure analysis	—	Quillon HW	2026-11-13
BCK-304	BCK	U2 does not assert FAULT on an output fault, or its FAULT drive of Q3 differs from what the design assumes	Request to TI (source: full LM68645-Q1 datasheet and safety manual for the SC variant, OQ-019, OQ-007); credit SM-4 only for the fault classes TI states	Bench fault injection before design freeze at 60 V input: FB open, and SW forced to VIN through a power resistor; pass if FAULT asserts each time, 12V never exceeds 15 V, and the corner goes fail-silent and is reported within 200 ms (SG-02 FTTI, provisional)	Quillon HW	2026-11-13
MCU-509	MCU	Flash content lost beyond ECC correction; U14 resets or does not start	Obtain TI retention data versus TJ (OQ-007); thermal analysis of U14 TJ over the mission profile (OQ-010); keep TJ-hours above 85 C within TI's retention limit, or add a scheduled reflash/refresh at service.	Thermal test at 105 C ambient with the worst motor duty: measure U14 case temperature and derive TJ; pass = TJ-hours above 85 C within TI's stated retention budget.	Quillon HW	2026-12-18
MCU-514	MCU	U14 permanent-fault rate rises with operating life (loss of this corner)	Thermal analysis of U14 TJ over the mission profile with TI's lifetime calculator (SPRSP93E p.109 reference); keep R146 DNP so the internal VREG loss (up to about 1.2 W at its 500 mA load limit) is not dissipated in U14; confirm the thermal via array under the PowerPAD.	Thermal test at 105 C ambient with the worst motor duty; pass = TJ time-at-temperature within TI's lifetime estimate for 15 years.	Quillon HW	2026-12-18
BLD-212	BLD	Phase output short; inverter overcurrent, then braking torque on the motor	Phase isolation as BLD-201; specified sealed, keyed production connector with strain relief (OQ-004) for the caliper lead; harness routing and chafe protection of the phase wires (OQ-037).	Phase-short fault injection (the one test for BLD-212, BLD-222, BLD-229 and BLD-317): hard phase-to-GND, phase-to-48V/12V_P, phase-to-phase and phase-to-12 V network shorts at J7-J9, at 60 V bus, -40 C and 125 C, drive running and during a hold. Pass: bridge off within VDS blanking plus deglitch ...	Quillon HW	2026-11-13
BLD-317	BLD	Shunt-based overcurrent trips blind to phase-to-GND fault current (coverage gap)	No hardware change proposed. Requires SW: enable U5 VDS overcurrent with threshold, blanking and deglitch set so that detection plus turn-off stays below the SQJA90EP short-circuit withstand budget derived in BLD-222 (not the 100 us SOA current); credit the shunt trips in the FMEDA only for faults that pass a low-side FET	The phase-short fault-injection test of BLD-222 (one test for BLD-212, BLD-222 and BLD-317): phase-to-GND, phase-to-bus and phase-to-phase at J7 with the drive running, 60 V, -40 C and 125 C. Pass: shutdown within blanking plus deglitch, below the withstand budget; no FET damage (RDS(on) and IDSS ...	Quillon HW	2026-12-18

Row	Block	Failure mode	Prevention action	Detection action	Owner	Due
ANG-301	ANG	Angle channels are not independent enough to support ASIL D by decomposition; common-cause faults defeat the channel comparison	Run a dependent-failure analysis (ISO 26262-9 cl. 7) of the angle function and decide the architecture: at least supply U13 from a separate regulator (PMIC LDO4 is unused on VerB), convert the channels on different ADC modules (ch1 ADC A/B, ch2 ADC C/D: pins 24 and 16 reach C25/D27) and add a diverse check (observer-based angle or the off-board sensor on J21/J22 with its own supply); obtain the TMAG618X-Q1-FS ...	DFA report with each shared resource listed and its measure; HIL fault injection of the common causes in ANG-302 to ANG-310 with pass criterion: fault detected and corner released and reported within the SG-01 FTTI (100 ms provisional)	Quillon HW	2026-11-13
ANG-304	ANG	Common angle error that grows with motor current; both channels agree	Keep phase conductors and motor leads away from the sensor axis; state a stray-field budget (e.g. < 1 % of the minimum magnet field in-plane) in the motor/ECU interface	Locked-rotor test on the target motor with encoder reference: angle error at 0, 16 A RMS and peak phase current in all electrical positions; pass: current-dependent error < 1 deg mechanical	Quillon V&V	2026-12-18
EPB-221	EPB	OCP lost (latent): a later output short is not current-limited	Obtain the DRV8263-Q1 FMEDA and safety manual (OQ-007): OCP failure rate, any latent-fault diagnostic or start-up test; if none, add an EPB-branch current limit or fuse (see EPB-201) so that a U7 short cannot latch off the ECU supply.	No design verification can reveal the cause (inside the die). Ask TI for an OCP test mode or production test: pass if TI documents a test that verifies the OCP threshold of each part. The FMEDA latent-fault metric (SG-02, SG-04, including the EPB branch) is not detection and earns no D.	TI (via Quillon)	2026-11-13
EPB-409	EPB	Cut-off stops an apply but removes the only means of active release	Technical safety concept: define the SG-03 reaction (cut-off timing budget from EPB force ramp vs rear-lock threshold; conditions under which VM is restored for a release through a path independent of the fault)	Timing analysis and HIL test of an injected unintended apply at speed; pass if residual clamp force stays below the rear-lock threshold (vehicle data) and release completes within the SG-03 FTTI	Quillon SW	2026-12-18
EPB-410	EPB	Cut-off opens (EPB unpowered) whenever the BLDC gate driver is off or faulted	Keep the EPB supply path independent of the BLDC driver state (separate cut-off driver or defined CUTOFF1 state that stays on in U5 fault/sleep unless the EPB itself must stop); document in the safety concept	Dependent failure analysis of SG-02 vs SG-06; fault injection: U5 DRVOFF/nSLEEP asserted and 12 V removed: pass if 48V/12V_BDC stays above the U7 VMUV threshold and the EPB completes a dynamic apply with the BLDC gate driver off	Quillon HW	2026-11-13
EPB-412	EPB	Q11 held on: CUTOFF1 stays high regardless of the command	SW requirement: cyclic readback of U5 cut-off registers; cut-off test as EPB-411	Fault injection by SPI (wrong CUTOFF1 configuration) on the bench; pass if detected within one test interval	Quillon SW	2026-12-18
WSS-212	WSS	U6 sensor pins damaged or degraded by ESD or surge on the harness	Obtain WSS001 pin ESD and surge ratings (OQ-008); place D5 at the connector pins in the production layout	ISO 10605 ESD (+/-8 kV contact, +/-15 kV air, 150 pF and 330 pF / 330 ohm) on J1/J2, powered and unpowered: pass if no loss of function and speed error within tolerance afterwards	Quillon V&V	2026-12-18
CAN-417	CAN	ECU start-up aborted by the transceiver undervoltage timer	One worst-case analysis with the SUP-201 inrush/SOA analysis and the load start profile: VSUP rise to 5V and 3.3V valid against tUV 159 ms with margin, U2 and the PMIC starting early in the 48V/12V_P ramp rather than after it settles, at -40 C and the item's specified minimum start-up input (at least the worst-case U1 UVLO rising threshold, 37.6 V as fitted, SUP-303)	Bench test: 100 cold starts at -40 C at the item's specified minimum start-up input, with the production PMIC NVM and the SUP-201 inrush ramp: pass if 5V and 3.3V are valid within 100 ms every time	Quillon HW	2026-11-13
PED-106	PED	Force input stuck at full scale	Requires SW: range check with the invalid band defined from the sensor specification (OQ-036); analog variant: pull-down instead of pull-up (PED-104).	Fault injection: PFS shorted to 5Vp2; pass if the input is flagged invalid within 10 ms and no demand is issued.	Quillon SW	2026-12-18
PED-108	PED	No force signal reaches U14 (fall-back demand lost)	Requires SW: diagnose loss of the fall-back input cyclically and report it (makes the fault detected rather than latent).	Fault injection: FORCE_SENSOR_SENT to GND and R145 removed; pass if fall-back unavailability is reported within 100 ms.	Quillon SW	2026-12-18
PED-109	PED	Force sensor supply shorted to ground	Requires SW: map the PLDO1 UV/current-limit flag to fall-back unavailability; confirm the NVM reaction does not reset the MCU on a sensor-supply fault (OQ-002).	Fault injection: 5Vp2 shorted at J11; pass if the PMIC and MCU stay up and fall-back unavailability is reported within 100 ms.	Quillon SW	2026-12-18

Row	Block	Failure mode	Prevention action	Detection action	Owner	Due
PED-204	PED	Travel input stuck at full scale (analog) or static high (SENT)	Requires SW: range check with the invalid band defined from the sensor specification (OQ-036); analog variant: pull-down instead of pull-up (PED-205).	Fault injection: PTS shorted to 5Vp1: pass if the input is flagged invalid within 10 ms and no demand is issued	Quillon SW	2026-12-18
PED-206	PED	No valid travel frames reach U14 SENT1: line static low or SENT input disconnected	Requires SW: fall-back unavailable reported to the brake controller and driver warning at the first missed-frame timeout	Fault injection on the bench: short PTS to GND at J14 and at C2. Pass: fault reported within the FTTI placeholder (A-10), no demand change	Quillon V&V	2026-12-18
PED-210	PED	Sensor supply 5Vp1 shorted to GND	Configure PMIC NVM so a PLDO1/PLDO2 fault only flags (SPI/interrupt) and never resets the MCU; requires SW: read the PLDO2 status and report the fall-back unavailable	Fault injection on the bench: short J15 to GND for 1 s and continuously, while braking. Pass: service braking continues, fall-back reported unavailable, PLDO2 recovers when the short clears	Quillon HW	2026-12-18

5 FMEDA results

5.1 Hardware metrics summary

Table 22. A = VerB as built, B = with the DFMEA actions. Black = below target.

Goal	ASIL	λ counted A / B (FIT)	SPFM A	SPFM B	LFM A	LFM B	PMHF A	PMHF B	Single-point rows A → B
SG-01	D	330 / 376	87.5 %	97.36 %	97.1 %	96.8 %	41.4	9.9	6 → 1
SG-02	C	309 / 326	80.8 %	90.42 %	99.0 %	99.2 %	59.4	31.2	2 → 0
SG-03	D	121 / 121	96.7 %	98.65 %	95.2 %	94.7 %	4.0	1.6	2 → 0
SG-04	C	103 / 105	94.0 %	95.60 %	94.9 %	94.4 %	6.2	4.6	1 → 0
SG-05	B	62 / 62	92.8 %	92.85 %	97.8 %	97.5 %	4.5	4.4	0 → 0
SG-07	B	72 / 58	60.3 %	75.96 %	87.2 %	87.2 %	28.5	13.9	16 → 10

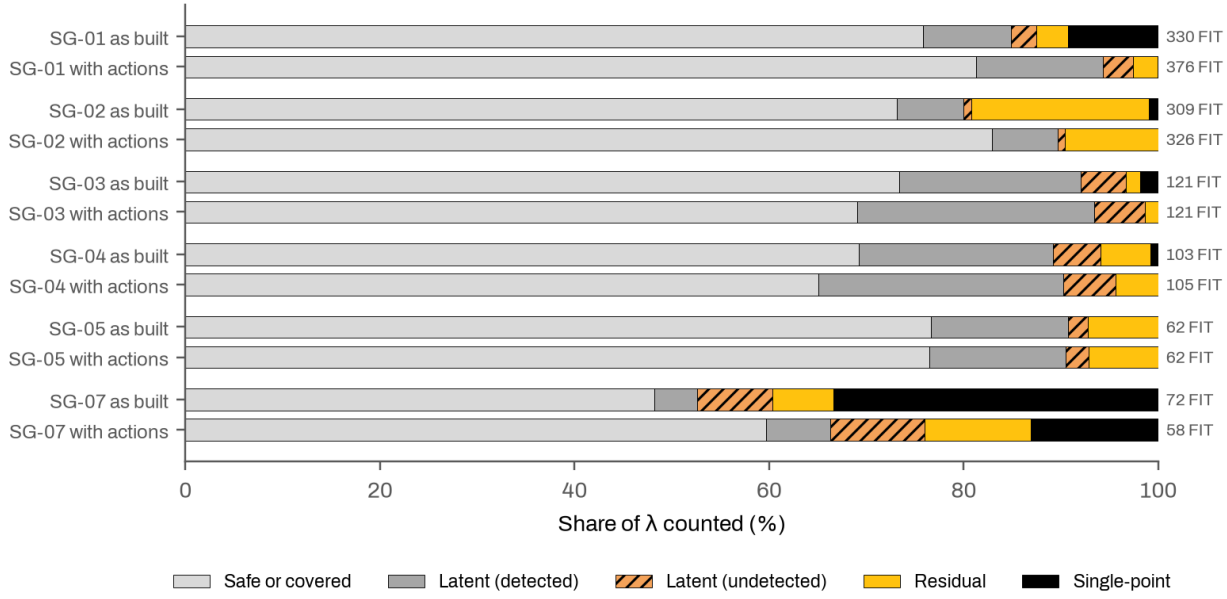


Figure 20. What the counted failure rate becomes, per goal and scenario.

5.2 Results by goal

SG-06 (secondary braking by the EPB, ASIL A) is not computed: ISO 26262-5 sets no hardware metric targets at ASIL A, and the DFMEA and the safety requirements cover it.

5.2.1 SG-01 Unintended or unreleased braking

Goal	ASIL	Safe state	FTTI	Events	Rows
Avoid braking at a wheel that was not requested (unintended, excessive, misdirected or unreleased clamp force)	D	Clamp force released at that wheel; corner reported unavailable; driver warned	TBD; provisional 100 ms (ASSUMED)	HE-01 to HE-06, HE-19	90

	SPFM	LFM	PMHF (FIT)	Residual (FIT)	Latent (FIT)
As built	87.47 %	97.05 %	41.38	41.38	8.51
With actions	97.36 %	96.81 %	9.90	9.90	11.65
Target	99 %	90 %	Item budget, OQ-046		

1. As built, a shorted inverter FET (6 × 40 % of 10 FIT) is the dominant single-point fault: after the U5 stop the shorted phase and the body diodes of the other legs brake the motor, so the caliper cannot self-release on time, and VerB has no way to disconnect the motor (BLD-201). U5 die faults that drive on their own (BLD-118, BLD-227) have no stop that avoids U5. Direction: phase isolation driven independently of U5, SAFE_OUT1 to nSLEEP, defined reset-state pulls (BLD-102, BLD-120, BLD-201).

2. The angle and current checks that most rows lean on are software the DFMEA asks for but VerB does not specify (OQ-032, OQ-038), and faults common to both angle channels or to both current and angle readings (LDO1/LDO3 drift inside the monitor window, a shared ADC module or reference) have no detection as built (MCU-302, ANG-306).

3. Even with the actions every credited reaction only stops torque; the SG-01 safe state (force released) then depends on A-08 and on the unpowered release time, which is not known (OQ-023, OQ-034). If the caliper does not release within 100 ms, most of the coverage below falls away.

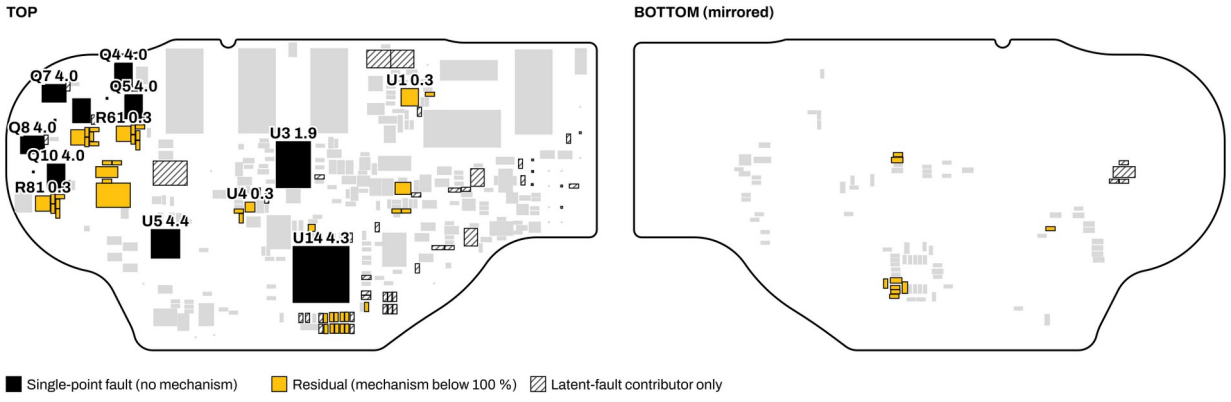


Figure 21. SG-01 as built: single-point (black), residual (yellow) and latent-only (grey) parts.

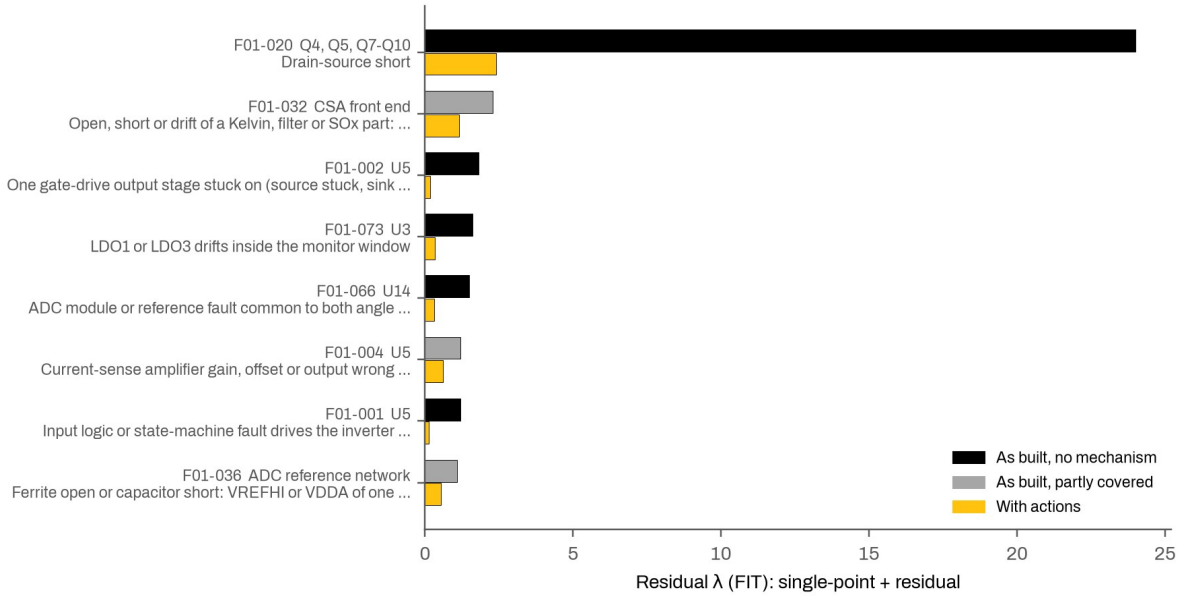


Figure 22. SG-01: largest residual contributors.

Table 23. SG-01 single-point faults as built, largest first.

Row	Part	Failure mode	λ (FIT)	With actions
F01-020	Q4, Q5, Q7-Q10	Drain-source short	24.00	Direct (SM-11)
F01-002	U5	One gate-drive output stage stuck on (source stuck, sink lost): FET held on whatever U5 is commanded	1.80	Direct (SM-11)
F01-073	U3	LDO1 or LDO3 drifts inside the monitor window	1.60	Direct (SM-15)
F01-066	U14	ADC module or reference fault common to both angle channels (both converted on one module)	1.50	Direct (SM-15)
F01-001	U5	Input logic or state-machine fault drives the inverter regardless of DRVOFF, nSLEEP and PWM inputs	1.20	Direct (SM-11)
F01-025	J7, J8, J9	Short to an adjacent phase pad or to the harness	0.45	Single-point

5.2.2 SG-02 Loss of braking

Goal	ASIL	Safe state	FTTI	Events	Rows
Avoid loss of, insufficient or late braking at a wheel when braking is requested	C	Corner reported unavailable or limited; other corners and regeneration compensate; driver warned	TBD; provisional 200 ms (ASSUMED)	HE-07 to HE-12	90

	SPFM	LFM	PMHF (FIT)	Residual (FIT)	Latent (FIT)
As built	80.80 %	98.98 %	59.40	59.40	2.54
With actions	90.42 %	99.16 %	31.19	31.19	2.48
Target	97 %	80 %	Item budget, OQ-046		

1. SG-02 rests on one mechanism outside this ECU: the brake controller's timeout of the corner status frames (SM-30, DFMEA PMC-118). About half of the SG-02 λ (155 of 309 FIT as built) is supply, rail and reset faults that take U14 and both CAN channels down together, so the corner cannot send a last message. The timeout, its value and the reaction are not specified (OQ-022, OQ-040); it is credited at Medium in both scenarios. As built SPFM is 80.8 %; High coverage of the timeout (PMC-118 specification and HIL proof) would add about 4.5 points.

2. With the actions SG-02 reaches 90.4 % against its 97 % target on the ASSUMED data. The gap is the silent-corner faults above and the drive that stops following its command while the corner still reports "available": inverter FETs, U5 outputs and gate supply, the isolation FETs the SG-01 actions add. Only the drive-response monitor sees those (SM-31, BLD-104, BLD-202), credited at Medium with the actions. SM-30 and SM-31 both at High would give 97.2 %.

3. As built the largest single-point faults are the ones SG-01 already names: LDO1/LDO3 drift inside the PMIC window and an ADC fault common to both angle channels scale the torque at this wheel with nothing to see it (PMC-201, ANG-306, MCU-302). The actions that fix them for SG-01 (SM-15) fix them here. PMHF is about 59 FIT as built and 31 FIT with the actions for one corner; with four corners on the item budget (OQ-046) the as-built value would exceed 100 FIT.

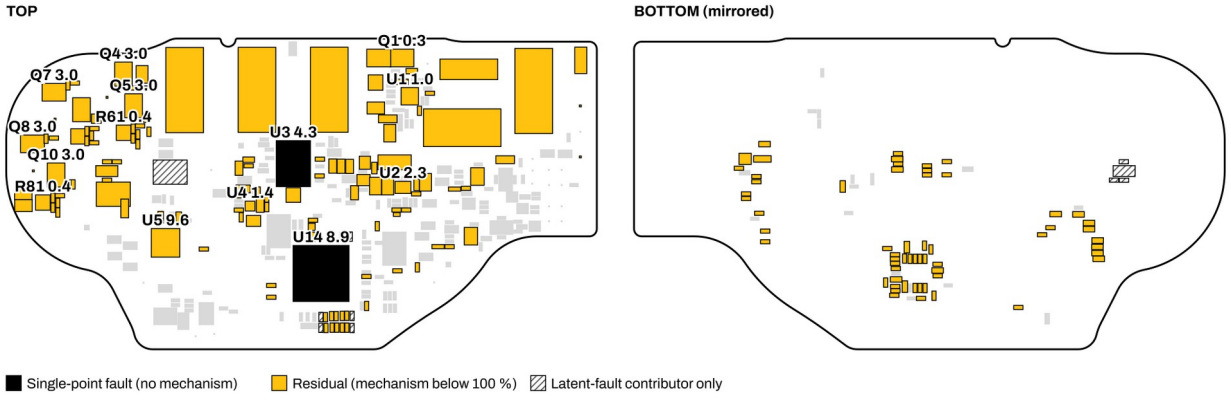


Figure 23. SG-02 as built: single-point (black), residual (yellow) and latent-only (grey) parts.

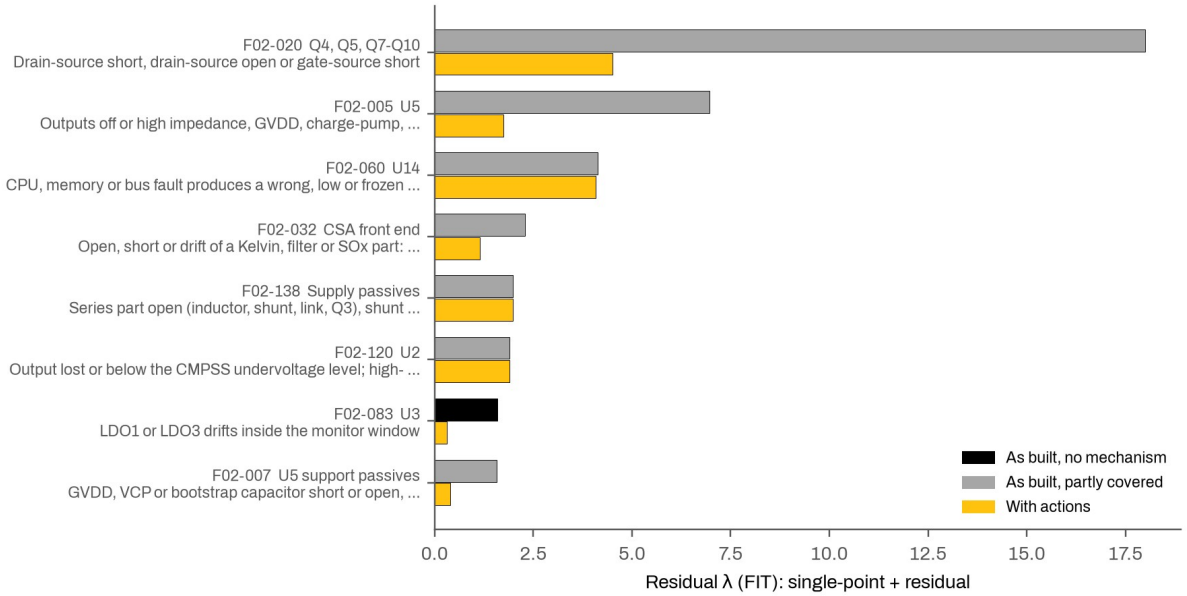


Figure 24. SG-02: largest residual contributors.

Table 24. SG-02 single-point faults as built, largest first.

Row	Part	Failure mode	λ (FIT)	With actions
F02-083	U3	LDO1 or LDO3 drifts inside the monitor window	1.60	Direct (SM-15)
F02-065	U14	ADC module or reference fault common to both angle channels (both converted on one module)	1.50	Direct (SM-15)

5.2.3 SG-03 EPB applied while moving

Goal	ASIL	Safe state	FTTI	Events	Rows
Avoid parking-brake application while the vehicle is moving, unless the driver requests it	D	EPB actively released and further apply inhibited (de-energising alone keeps the force on a self-locking spindle)	TBD; provisional 300 ms (ASSUMED)	HE-13	93

	SPFM	LFM	PMHF (FIT)	Residual (FIT)	Latent (FIT)
As built	96.70 %	95.19 %	3.99	3.99	5.64
With actions	98.65 %	94.65 %	1.63	1.63	6.39
Target	99 %	90 %	Item budget, OQ-046		

1. As built, SG-03 has two single-point faults: a U7 output stage that drives the apply direction on its own (the only independent switch, the Q11 cut-off, cannot open because R58 ties its gate to the bus) and U14 EPB pins stuck in the drive state (the lockstep does not see a port fault and the only reaction runs through those pins). A U7 input fault is covered at Low only, because its reaction acts in the same die. Direction: R58 not fitted, OUTA/OUTB readback, SAFE_OUT1 to nSLEEP (EPB-211, EPB-401, EPB-408).

2. With the actions SG-03 still falls just short of its SPFM target on the ASSUMED data. The remaining gap is supply overvoltage on the MCU rails (U4 core, U3 LDO1, U2 12 V), credited at Medium until the PMIC monitor thresholds and reaction are known (OQ-002, OQ-014); High coverage there closes it. The cut-off reactions stop an apply without releasing it, so their credit holds only if they act before the force is hazardous (EPB-409, OQ-047).

3. The PMHF cannot be judged until the corner ECU's share of the item budget is set (OQ-046): with two EPB corners per vehicle, SG-03 alone takes about twice the value shown.

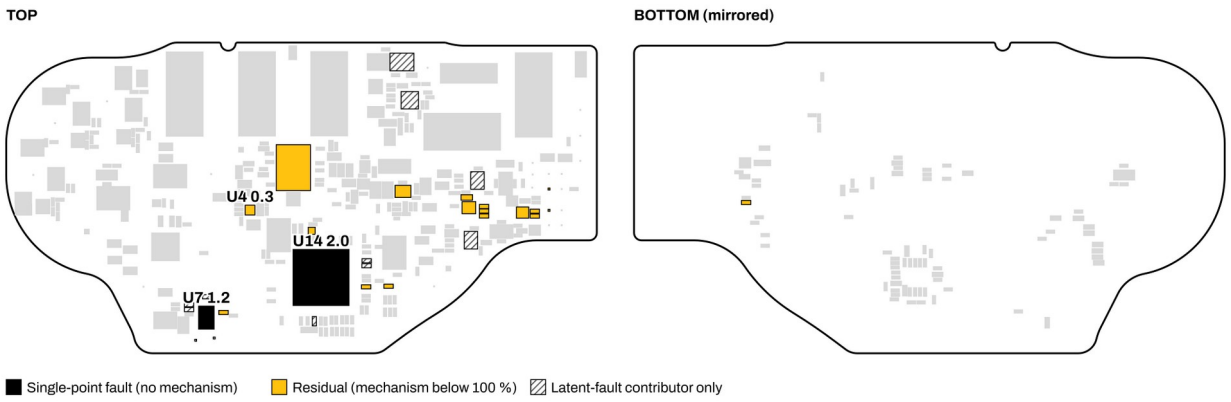


Figure 25. SG-03 as built: single-point (black), residual (yellow) and latent-only (grey) parts.

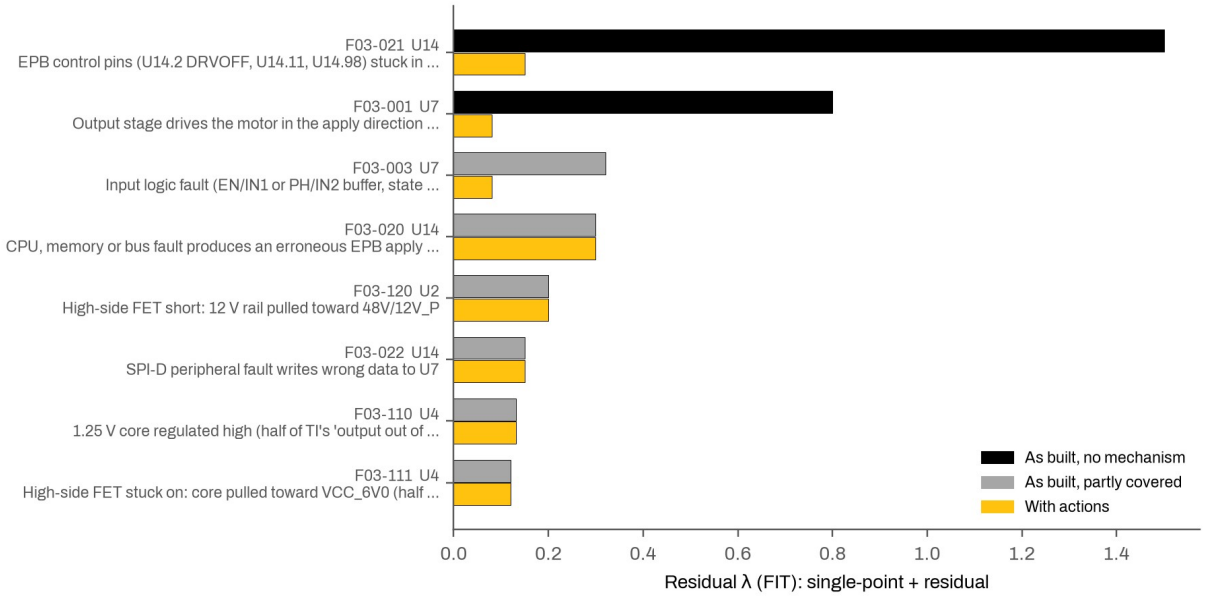


Figure 26. SG-03: largest residual contributors.

Table 25. SG-03 single-point faults as built, largest first.

Row	Part	Failure mode	λ (FIT)	With actions
F03-021	U14	EPB control pins (U14.2 DRVOFF, U14.11, U14.98) stuck in the drive state (port fault the lockstep does not ...	1.50	Direct (SM-03)
F03-001	U7	Output stage drives the motor in the apply direction without a command (diagonal FET pair shorted or gate ...	0.80	Direct (SM-04)

5.2.4 SG-04 Loss of parking hold

Goal	ASIL	Safe state	FTTI	Events	Rows
Avoid loss of parking or standstill hold while the vehicle is stationary	C	Hold maintained or re-applied; driver warned; transmission park lock if fitted	TBD; provisional 1 s (ASSUMED)	HE-14, HE-15	81

	SPFM	LFM	PMHF (FIT)	Residual (FIT)	Latent (FIT)
As built	94.02 %	94.86 %	6.17	6.17	4.98
With actions	95.60 %	94.40 %	4.63	4.63	5.63
Target	97 %	80 %	Item budget, OQ-046		

1. As built, SG-04 has one single-point fault: a U7 output stage that drives the release direction on its own. Nothing observes the motor terminals independently of U7, the IPROPI mirror is blind to a shorted high-side FET, and the only stop outside the die (Q11) cannot open because R58 ties its gate to the bus. U7 is the only drive path, so the corner cannot re-clamp: the hold must come from the other rear corner (EPB-211, EPB-314, EPB-401). U14 EPB pins stuck in the release state are covered only by a report to the other corner (SM-40, Low as built).

2. With the actions SG-04 still misses its SPFM target (95.6 % against 97 %; 94.0 % as built) on the ASSUMED data. The dominant residual is not unintended release but the faults that leave the EPB unable to apply (U7 outputs off, Q11 open, pads open), whose apply-completion check is capped at Medium, and the faults that end an apply early on a false stall: a current reading that is too high (D12 short or leakage, R95 open, IPROPI gain). SG-03 treats a high reading as safe-side; for SG-04 it is the hazard, and only gross errors are seen without a second current or force measurement (EPB-309, EPB-318). Closing the gap needs that second measurement, or High coverage of the no-drive faults. The vehicle answer on single-corner hold (OQ-052) decides whether a detected no-apply at one corner reaches the safe state at all.

3. The safe states of SG-03 (release, inhibit apply) and SG-04 (hold) conflict, and so do SG-01's (release to zero force on a request timeout, CAN-102; release first after a PMIC reset, PMC-419) if the standstill hold uses the service brake. Every fault reaction needs an arbitration that holds unless independent motion is confirmed; a false "moving" at standstill must not turn an SG-03 reaction into a release. The Q11 cut-off helps SG-04 (it stops a release and the spindle keeps the rest) but removes the only way to re-clamp this corner.

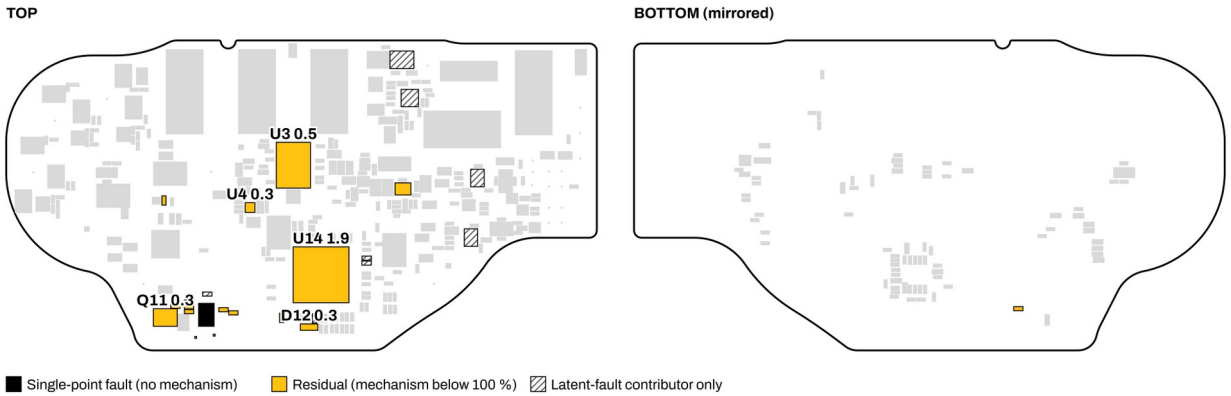


Figure 27. SG-04 as built: single-point (black), residual (yellow) and latent-only (grey) parts.

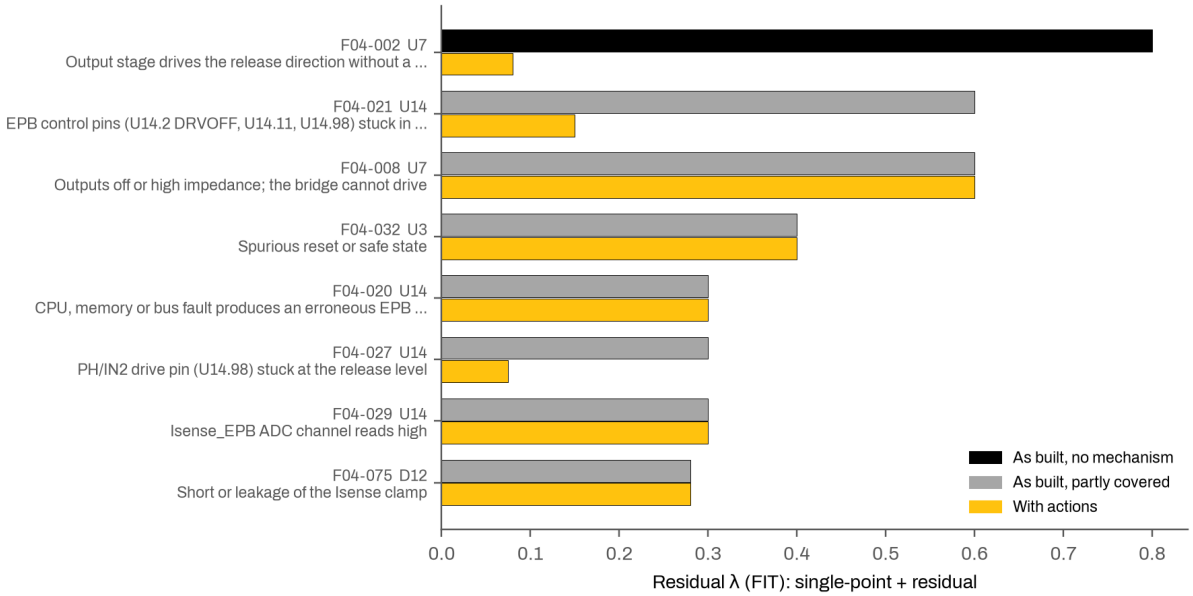


Figure 28. SG-04: largest residual contributors.

Table 26. SG-04 single-point faults as built, largest first.

Row	Part	Failure mode	λ (FIT)	With actions
F04-002	U7	Output stage drives the release direction without a command (diagonal FET pair shorted or gate drive stuck on)	0.80	Direct (SM-04)

5.2.5 SG-05 Erroneous wheel speed

Goal	ASIL	Safe state	FTTI	Events	Rows
Avoid erroneous wheel-speed information being used by the braking and stability functions	B	Wheel speed marked invalid; braking functions use the other wheels	TBD; provisional 50 ms (ASSUMED)	HE-18	60

	SPFM	LFM	PMHF (FIT)	Residual (FIT)	Latent (FIT)
As built	92.79 %	97.77 %	4.45	4.45	1.28
With actions	92.85 %	97.47 %	4.44	4.44	1.46
Target	90 %	60 %	Item budget, OQ-046		

1. SG-05 rests on mechanisms in the brake controller, not in this ECU: cross-wheel plausibility (SM-20), the loss-of-pulse check (SM-23) and the E2E timeout (SM-24). SM-20 sees only deviations above its threshold (ASSUMED max(2 km/h, 5 %) for 20 ms) and is weakest during an ABS intervention, where a low reading looks like a locking wheel. A small speed error from U6, the capture path or the clock is not detected. These checks, their threshold and their timing within the 50 ms FTTI have to be allocated to the brake controller as assumptions of use.

2. The largest residual is lost CAN frames (U8, U10: F05-100, 1.7 FIT), which rests only on the E2E timeout being specified (SM-24, OQ-040). Next comes U6 (about 1.2 FIT), whose FIT and failure-mode split are UNRELEASED assumptions (OQ-008). Its wrong-speed mode (F05-001) is covered by SM-20 alone. The 5 V LDO2 is a common cause for U6 and both CAN transceivers. A lost or shorted 5 V silences the corner, which reveals itself. A 5 V running high relies on the PMIC overvoltage monitor (SM-08), whose LDO2 threshold and reaction are in NVM (OQ-002).

3. The DFMEA actions change little for SG-05. The only hardware action in the chain is the WSSO pull-down (WSS-302), which turns an open WSSO path into a steady low that SM-23 detects. On the ASSUMED data both scenarios reach the recommended ASIL B values: SPFM about 93 %, LFM about 97 %, PMHF about 4.4 FIT. The step that matters is TI's WSS001 FMEDA and a confirmed brake-controller plausibility specification.

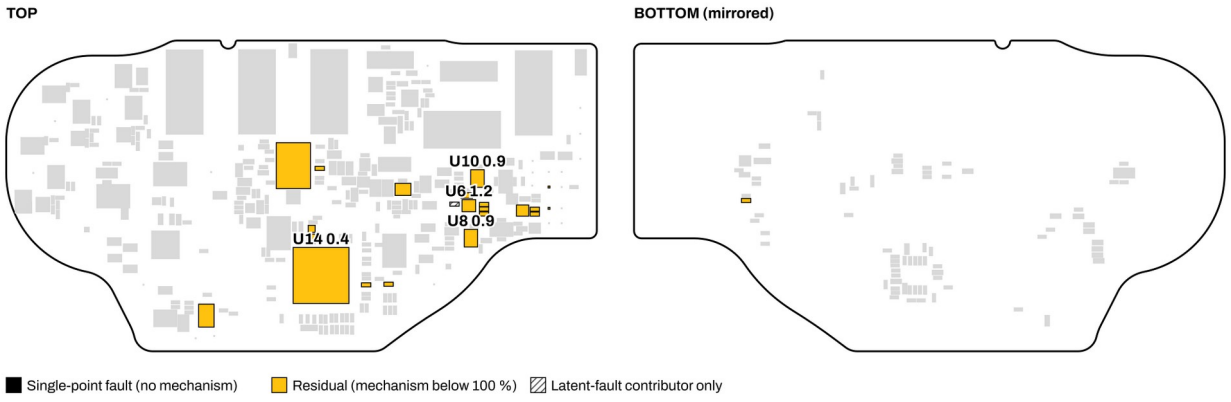


Figure 29. SG-05 as built: single-point (black), residual (yellow) and latent-only (grey) parts.

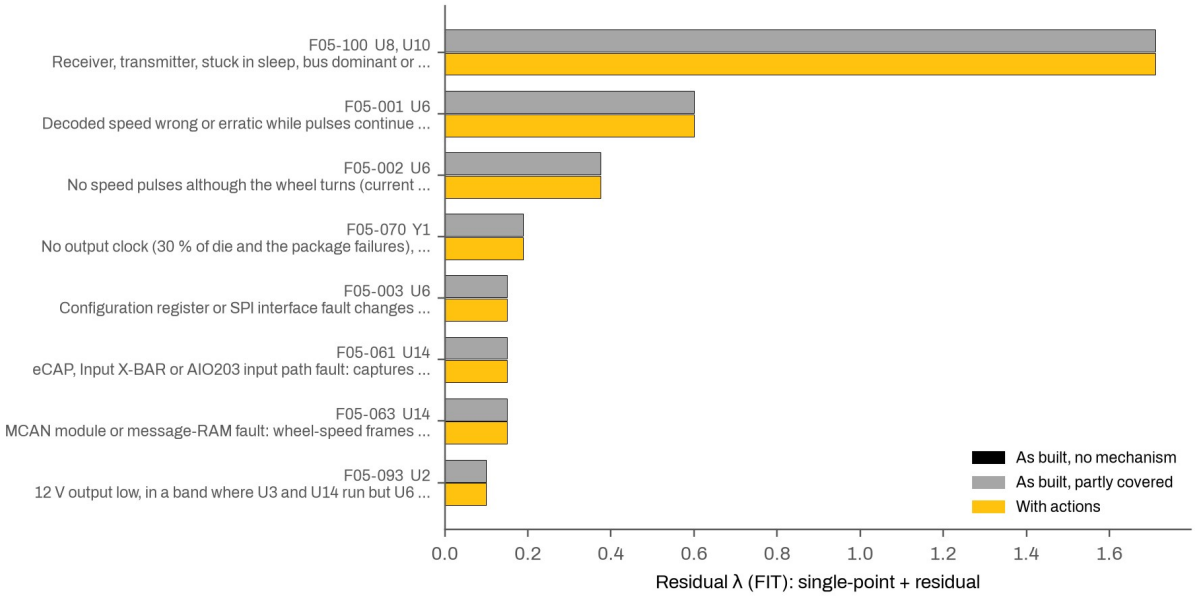


Figure 30. SG-05: largest residual contributors.

5.2.6 SG-07 ECU thermal event

Goal	ASIL	Safe state	FTTI	Events	Rows
Avoid a thermal event (smoke, fire) of the corner ECU	B	Energy removed from the faulty circuit; corner reported unavailable; driver warned to stop	TBD; U1 acts in microseconds to 1 ms, the IMON check needs the time to ignition to exceed its period plus debounce (ASSUMED, OQ-044)	HE-20	70

	SPFM	LFM	PMHF (FIT)	Residual (FIT)	Latent (FIT)
As built	60.29 %	87.22 %	28.45	28.45	5.52
With actions	75.96 %	87.23 %	13.86	13.86	5.59
Target	90 %	60 %	Item budget, OQ-046		

1. As built, nothing on VerB sees a fault that draws less than the U1 breaker band (18-27 A): the resistive half of every 48 V and 12 V capacitor short, every CAF path, a hot power-pad joint and a leaky input TVS are single-point faults, and the whole input side ahead of R7 is protected only by the vehicle fuse for hard shorts. The U1 short-circuit comparator and breaker are the only mechanism, and their loss (U1 SCP/OCP, the set network, R7) is latent with no test. SPFM as built is about 60 % against the 90 % recommended; LFM (about 87 %) meets 60 % only because the latent faults are small next to the covered hard shorts. PMHF about 28 FIT for one corner, so four corners alone exceed the 100 FIT item value (OQ-046).

2. With the actions the gap narrows but stays. The IMON supply-current check (PCB-202, SUP-314) sees only the high-power end (above about 3 A), and the actions leave CAF ahead of R7 and on the phases, hot pad joints and 12 V rail shorts without any mechanism. Closing it needs a fail-safe element rather than more software: fail-open (floating-electrode) bus MLCCs or an eFuse below the U1 band (PCB-202), a current limit on the 12 V rail, an idle-current trip on the EPB branch through Q11 (an extension of EPB-423), and CAF-resistant laminate with 0.5 mm inner spacing (PCB-302, PCB-303). SPFM with the actions is about 76 %, PMHF about 14 FIT.

3. Several thermal chains are systematic and sit outside these metrics: D1 (SMBJ51CA) conducts continuously near 60 V (SUP-101); as built Q11 runs as a source follower and dissipates tens of watts in every EPB actuation (EPB-402, R58); C27 and C31-C33 are 85 C parts at a 105 C board (BCK-409); Q1 exceeds its SOA at every start (SUP-201). Each must be closed by design before the random-fault metrics mean anything.

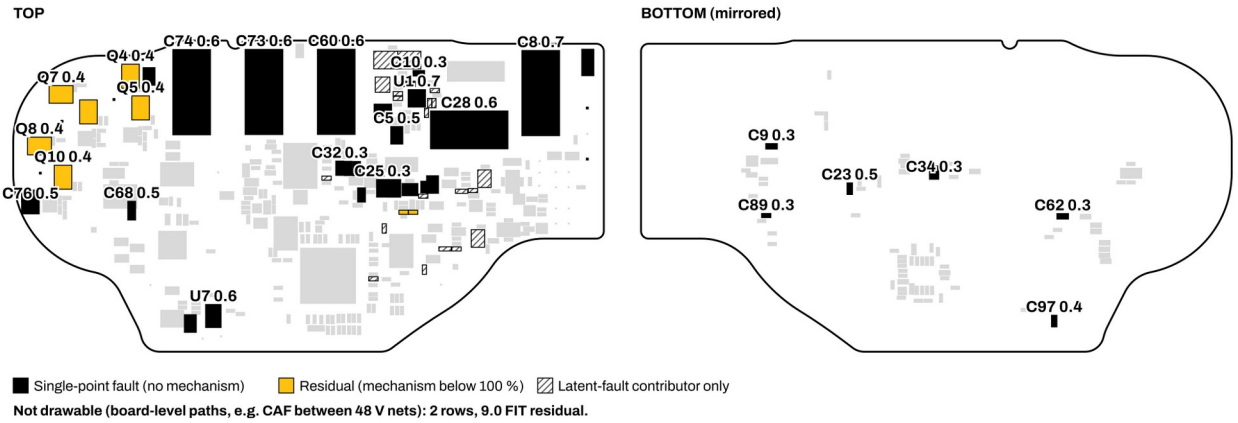


Figure 31. SG-07 as built: single-point (black), residual (yellow) and latent-only (grey) parts.

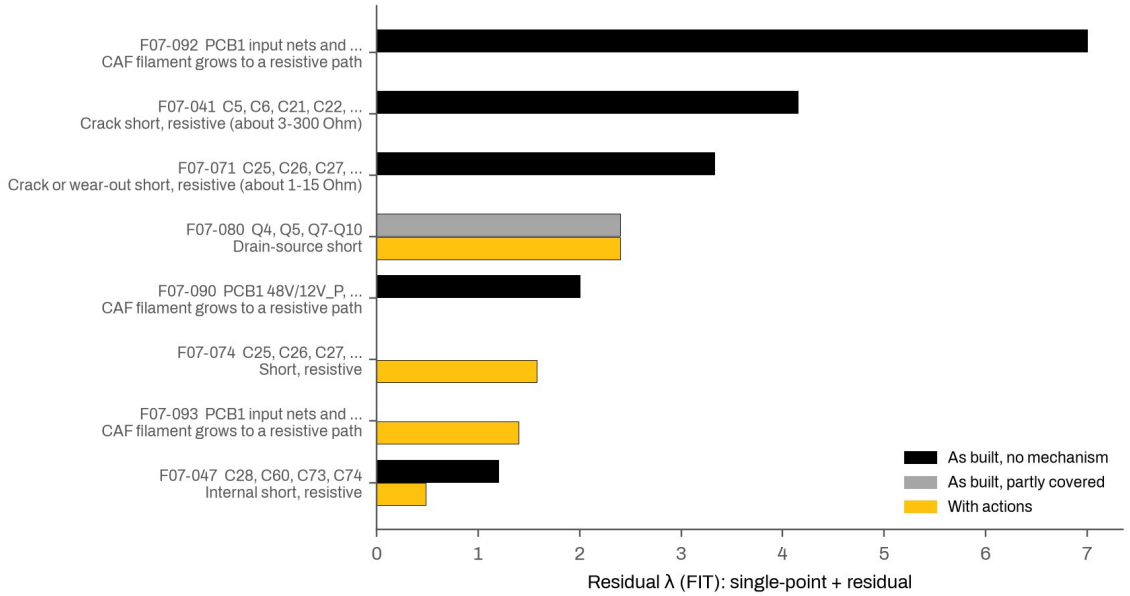


Figure 32. SG-07: largest residual contributors.

Table 27. SG-07 single-point faults as built, largest first.

Row	Part	Failure mode	λ (FIT)	With actions
F07-092	PCB1 input nets and phases	CAF filament grows to a resistive path	7.00	Part replaced by the actions
F07-041	C5, C6, C21, C22, C61, ...	Crack short, resistive (about 3-300 Ohm)	4.15	Part replaced by the actions
F07-071	C25, C26, C27, C31-C36, ...	Crack or wear-out short, resistive (about 1-15 Ohm)	3.33	Part replaced by the actions
F07-090	PCB1 48V/12V_P, ...	CAF filament grows to a resistive path	2.00	Part replaced by the actions
F07-047	C28, C60, C73, C74	Internal short, resistive	1.20	Direct (SM-71)
F07-048	C28, C60, C73, C74	Venting after internal heating (ESR rise with ripple)	1.20	Single-point
F07-024	U1	Pin-to-pin short (TI 5 %)	0.70	Single-point
F07-051	C96, C97	Crack short, resistive (EPB-201: 2-20 A)	0.70	Part replaced by the actions

5.3 Sensitivity and what TI must confirm

SG-03 with the actions sits 0.35 points below its SPFM target. The chart varies one assumption at a time.

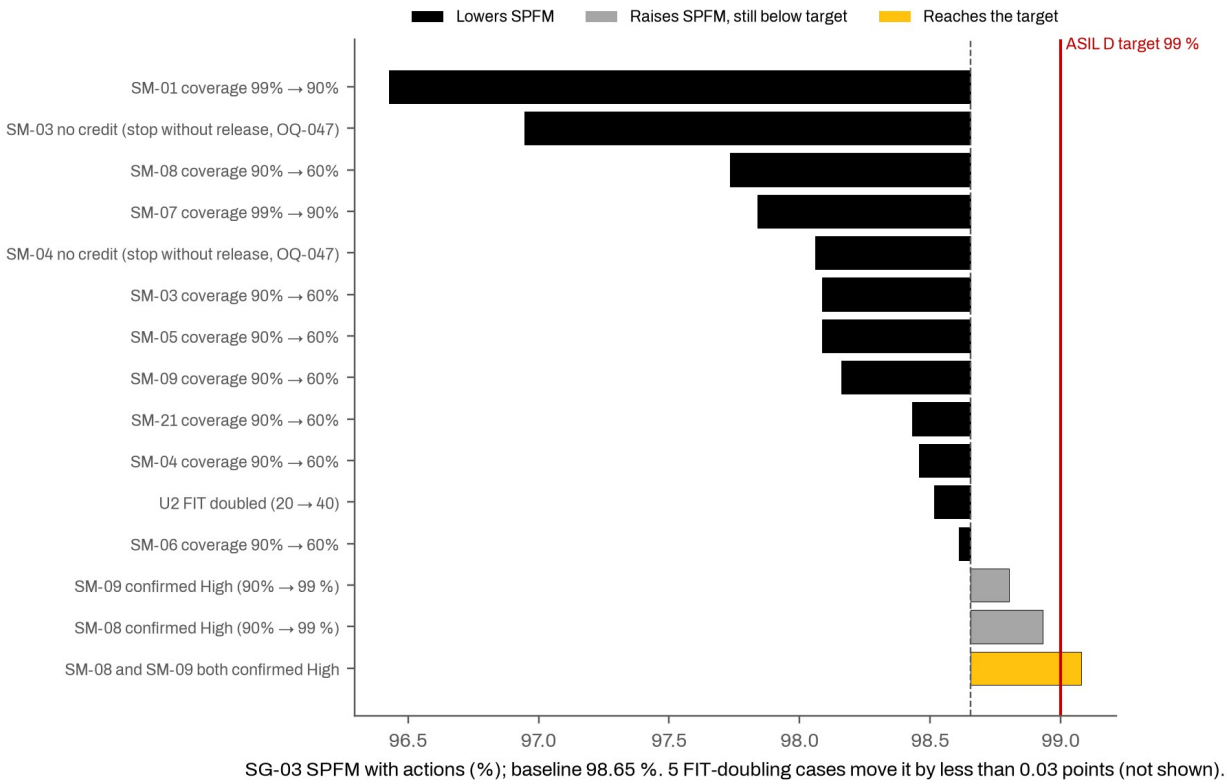


Figure 33. SG-03 SPFM with actions: each bar is one change. Only confirmation of High coverage for the supply monitors (SM-08, SM-09) reaches the target.

Table 28. TI functional-safety data per IC.

Part	Ref	TI category	Public data	Needed from TI
F29P329SM-Q1	U14	Functional Safety-Compliant	SFFSBK8 (TUV SUD certificate); SWAB014	Safety manual (request)
TPS653860-Q1	U3	Functional Safety-Compliant	SLVAFX2 (F29x power design app note; not FS data)	Safety manual + FMEDA (myTI request)
DRV3263-Q1	U5	Functional Safety-Compliant	—	SFFSBB3 safety manual (stamped TI Confidential - NDA; ...
LM68645-Q1	U2	Functional Safety-Compliant	—	FMEDA (request)
TMAG6180-Q1	U12, U13	Functional Safety-Compliant (ASIL B)	—	TMAG618X-Q1-FS (request)
DRV8263-Q1	U7	Functional Safety-Compliant Targeted (datasheet SLVSHH3A p.1)	—	DRV8263-Q1-FS (request)
LM74930-Q1	U1	Functional Safety-Capable	SFFS950 (FIT/FMD/pin FMA)	None: data public
TPS62902-Q1	U4	Functional Safety-Capable	SFFS465A (FIT/FMD/pin FMA)	None: data public
TCAN1043H-Q1	U8, U10	Functional Safety-Capable	SLLA525A (FIT/FMD/pin FMA)	None: data public
CDC6C-Q1	Y1	Functional Safety-Capable	SFFS685 (FIT/FMD/pin FMA)	None: data public
WSS001-Q1	U6	unreleased (no product page)	—	Device documentation

5.4 Safety mechanisms credited

51 mechanisms: 34 that prevent a violation and 17 that detect latent faults. The table lists the 22 credited on the most FMEDA rows; the FMEDA workbook lists all.

Table 29. Safety mechanisms credited on the most FMEDA rows. DC A / DC B = diagnostic coverage as built / with actions.

ID	Mechanism	Annex D basis	DC A	DC B	Status	Rows
SM-01	MCU lockstep cores, ECC and error-signal module; the PMIC resets the MCU on an error	Processing units: hardware redundancy, dual-core lockstep (High)	99%	99%	ASSUMED (GATED, OQ-007)	8
SM-05	SPI integrity for U7 (REG_LOCK, SPI_IN lock, cyclic readback of COMMAND, SPI_IN and CONFIG, status byte check)	Information redundancy, read-back of configuration (Medium; the frame has no ...	90%	90%	ASSUMED (PROVISIONAL, OQ-032)	8
SM-06	Direction plausibility of EPB motion (a release that ends in a rising current to stall is an apply; an apply that ends at the release end stop is a ...	Plausibility check of outputs (Low as built; Medium with terminal readback)	60%	90%	ASSUMED (PROVISIONAL, OQ-032)	8
SM-07	Standstill confirmed by an independent source (other rear wheel or vehicle speed over CAN); loss of pulses is invalid, never standstill	Plausibility check with an independent redundant sensor (High)	99%	99%	ASSUMED (PROVISIONAL, OQ-038)	8
SM-08	PMIC rail monitoring (EXT_VMON1 on the 1.25 V core; LDO1, LDO2 and LDO3 over- and undervoltage) resets U14; the drivers turn off	Power supply: voltage monitoring of the output with a reaction (High ...	90%	90%	ASSUMED (GATED, OQ-002)	26
SM-09	12 V overvoltage cut-off (U14 CMPSS window on VMON drives nSTB_CAN low; both transceivers drop INH; U1 removes 48V/12V_P)	Power supply: voltage monitoring of the input with a switch-off (Medium)	90%	90%	ASSUMED (PROVISIONAL, OQ-014)	12
SM-12	Phase-current plausibility (three-shunt sum, voltage/speed model, zero-current offset at standstill, range check, CSA gain readback) stops the ...	Plausibility check of redundant measurements (Medium claimable)	60%	80%	ASSUMED (PROVISIONAL, OQ-038)	30
SM-14	Angle plausibility (U12/U13 channel compare, sin^2+cos^2 window, 10-90 % range, quadrant consistency, motion check) stops the drive and reports	Comparison of redundant sensors (High claimable)	90%	97%	ASSUMED (PROVISIONAL, OQ-038)	19
SM-20	Cross-wheel speed plausibility in the brake controller (deviation from the vehicle reference speed above max(2 km/h, 5 %) for 20 ms, or wheel ...	Sensor rationality check against redundant sensors (Medium)	80%	80%	ASSUMED (PROVISIONAL, OQ-049)	17
SM-21	MCU clock monitoring: missing-clock detection (limp to INTOSC, CLOCKFAIL) and the DCC comparing X1/PLLRAWCLK with INTOSC continuously; on an error ...	Clock: monitoring with an independent time base (Medium)	90%	90%	ASSUMED (GATED, OQ-007)	12
SM-23	Loss-of-pulse check: no WSSO edge for two expected periods (from the vehicle reference) while the reference is above 5 km/h marks the wheel invalid, ...	Sensor rationality check against redundant sensors (Medium)	90%	90%	ASSUMED (PROVISIONAL, OQ-049)	26
SM-24	End-to-end protection of the wheel-speed signal and its validity flag (CRC, alive counter, timeout of 3 cycles) checked by the brake controller; ...	Communication bus: information redundancy with frame counter and timeout ...	90%	90%	ASSUMED (PROVISIONAL, OQ-040)	10
SM-30	Corner-status timeout in the brake controller: this corner's status frame (CRC, alive counter, 10 ms cycle) missing, frozen or corrupt beyond the ...	Communication bus: information redundancy with frame counter and timeout ...	90%	90%	ASSUMED (PROVISIONAL, OQ-022)	32
SM-31	Drive-response monitor in U14: commanded current or duty with no or too little phase current (per phase and total), no rotor motion under breakaway ...	Monitoring of outputs, plausibility check of the actuator response (Medium ...	60%	90%	ASSUMED (PROVISIONAL, OQ-032)	25
SM-41	Apply-completion check on every park and auto-hold apply (inrush within a set time, stall reached within the expected window, U7 STATUS/FAULT and ...	Monitoring of outputs, plausibility of the effect against the command (Medium)	90%	90%	ASSUMED (PROVISIONAL, OQ-032)	31

ID	Mechanism	Annex D basis	DC A	DC B	Status	Rows
SM-42	Holding-force plausibility of each apply: rest-offset check of Isense_EPB before the apply, stall accepted only after a minimum run time or ripple ...	Plausibility check of a sensor against a model (Low)	60%	60%	ASSUMED (PROVISIONAL, OQ-043)	10
SM-70	U1 short-circuit comparator (26.9-34 A, 3.5-5.5 us) and circuit breaker (18-27 A, about 1 ms) open Q1 and latch off (R21 across C_TMR); the corner ...	Power supply: current control of the output (48V/12V_P) with switch-off (High ...	90%	90%	ASSUMED (JUDGMENT, OQ-028)	14
LM-02	Current-sense path test (inrush plausibility at each commanded operation, key-on self-test)	Plausibility of a sensor against a known stimulus (Medium)	90%	90%	ASSUMED (PROVISIONAL, OQ-032)	18
LM-04	MCU start-up self-tests (logic and memory BIST, error-module test)	Self-test by hardware at start-up (Medium to High)	90%	90%	ASSUMED (GATED, OQ-007)	12
LM-05	PMIC start-up self-test and test of the reset and safe-state outputs	Self-test by hardware at start-up; test of the reset path (Medium)	90%	90%	ASSUMED (GATED, OQ-007)	26
LM-06	U7 status byte, DEVICE_ID and nFAULT/FAULT consistency on every access	Information redundancy on the interface (Medium)	90%	90%	ASSUMED (PROVISIONAL, OQ-032)	16
LM-13	Supply cut-off test (key-off drop of INH with the bridges off, confirm DC_BUS decays and U14 loses power within 10 ms; CMPSS VMON trip checked by ...	Test of the switch-off path at shut-down (Low to Medium)	60%	60%	ASSUMED (PROVISIONAL, OQ-014)	28

5.5 Dependent failures

Table 30. Shared causes that the random-fault metrics do not see.

#	Shared cause	Mechanism at risk	Goals	Disposition	Status
1	Both lockstep cores and the MCU I/O share one supply (U4 1.25 V core, U3 LDO1 3.3 V)	SM-01 (lockstep)	SG-01, SG-02, SG-03	Covered by SM-08: the PMIC monitors the core rail through EXT_VMON1 in a separate die. LDO1's monitor shares its die with the regulator (Medium credit). Thresholds in PMIC NVM (OQ-002).	Open (OQ-002)
2	U7 input logic fault and its reaction (DRVOFF) in the same die	SM-03 as built	SG-03	As built: Low coverage only. With the actions the reaction opens Q11 or puts U7 to sleep through SAFE_OUT1, both outside U7.	Closed by actions
3	U14 both commands the EPB and runs the software mechanisms (SM-03 to SM-07, LM-01 to LM-08)	All SW mechanisms	SG-03	Faults in the U14 CPU are covered by SM-01 and the PMIC reset path (different die). Port faults: detection in software, reaction through Q11 or SAFE_OUT1 on different pins and peripherals than the stuck ones. Freedom from interference for ...	Open: pin and peripheral independence to be shown
4	Shared SPI-D bus between U6 (wheel speed) and U7 (EPB)	SM-05, SM-07	SG-03, SG-05	Standstill is taken from WSSO pulse timing and the other wheels over CAN, never from SPI data; U7 configuration is locked and read back cyclically.	Requirement in the TSC
5	5 V LDO2 feeds U6 and both CAN transceivers	SM-07	SG-03, SG-05	Loss of 5 V removes the pulses and the independent speed together. The rule 'loss of pulses is invalid, never standstill' is local and needs neither; EPB static apply inhibited on loss of both buses.	Requirement in the TSC
6	Y1 clocks U14, so it times the wheel-speed capture and the command sequence	SM-07	SG-03, SG-05	The PMIC Q&A watchdog runs on its own oscillator and breaks its window on a U14 frequency error (SM-02).	Covered
7	A 48 V bus short at the H-bridge overstresses the Q11 gate	SM-03, SM-04 reaction	SG-03, SG-07	The same event that shorts the bus can rupture the Q11 gate oxide, leaving the cut-off unable to open. Branch current limit and a gate-source clamp are DFMEA actions.	Open (DFMEA actions)

#	Shared cause	Mechanism at risk	Goals	Disposition	Status
8	External surge or load dump through the supply input	U1, SM-09	All	Not a random hardware fault of the ECU: U1 overvoltage cut-off and the CMPSS window (SM-09) remove 48V/12V_P. Coupling faults (common supply to U3, U5, U7) are listed here, not in the metrics.	Open (OQ-014, OQ-017)
9	EMC coupling onto the long SPI-D stubs	SM-05	SG-03	Cyclic readback of U7 configuration and the register lock; the frame has no CRC.	Covered (PROVISIONAL)
10	Board-level thermal event near the EPB stage (C96 crack short)	EPB stop paths	SG-03, SG-07	Removes the EPB supply (safe for SG-03); its thermal risk is counted on SG-07.	Counted on SG-07
11	The Q11 cut-off serves opposite goals: it stops an unintended apply (SG-03) and an unintended release (SG-04), but once open it removes the only way to re-clamp this ...	SM-03, SM-04, LM-03	SG-03, SG-04	Any opening at standstill (a false trip, the LM-03 test) leaves the hold with no re-apply at this corner. LM-03 must run only with both rear EPBs applied; the reaction when standstill cannot be confirmed is for the client.	Open (OQ-053)
12	Systematic thermal chains outside the random-fault rows: D1 conducting near 60 V, Q11 in linear mode as built, Q6 at 58-66 V, 25 V capacitors at 105 °C, aluminium ...	SM-70 to SM-73	SG-07	Design deficiencies, not random faults: corrected by the DFMEA actions, not by a safety mechanism. Listed so the SG-07 metrics are not read as covering them.	Open (DFMEA actions; OQ-011, OQ-017, OQ-029, OQ-030)

5.6 Limits of this revision

The metrics are provisional in both directions. The choices below move them; each closes when the data or decision behind it arrives.

Table 31. Choices that move the results.

Choice	Direction	Effect	Closes with
Order-of-magnitude FIT and sev10 shares for TI ICs without published data	Conservative	All goals; IC residuals credited below TI's likely claims	OQ-007
Supply monitors credited Medium (90 %)	Conservative	SG-03 reaches 99 % with High (99 %)	OQ-002
Shorted phase assumed to miss the SG-01 FTTI	Conservative	SG-01 as built rises by several points if it does not	OQ-048
Corner-status timeout credited Medium	Conservative	SG-02 rises by about 4 points at High	OQ-050
50 % of capacitor shorts assumed resistive	Uncertain	Half of the SG-07 capacitor residual	OQ-054
Faults with no path to the goal counted n/a, not Safe	Conservative	Lowers every SPFM (Table below)	—
Passive failure rates at 85 °C against a profile to +105 °C, no stress factors	Optimistic	Passive λ rises at the mission profile	OQ-010
Software mechanisms credited as specified in the DFMEA (391 rows), none implemented	Optimistic	Credits hold only once implemented and verified	OQ-032
Brake-controller checks credited as assumptions of use (SM-20, SM-23, SM-24, SM-30)	Optimistic	SG-02 and SG-05 coverage depends on another ECU	OQ-049, OQ-050
Item-level PMHF budget, no corner allocation	—	PMHF not judged	OQ-046

Table 32. Effect of the n/a convention. This analysis excludes IC functions and parts with no path to the goal; counting them Safe, as is common, raises the SPFM without any change to the design.

Goal	SPFM with actions, as analysed	If no-effect faults were counted Safe (indicative)	Target
SG-01	97.36 %	98.00 %	99 %
SG-02	90.42 %	94.49 %	97 %
SG-03	98.65 %	99.55 %	99 %
SG-04	95.60 %	98.61 %	97 %
SG-05	92.85 %	98.37 %	90 %
SG-07	75.96 %	93.63 %	90 %

6 Recommendations and next steps

6.1 Hardware changes

Table 33. Hardware changes, largest effect on the metrics first.

#	Change	Rows	Goals helped
1	PMIC SAFE_OUT1 to U7 and U5 nSLEEP through series resistors; MCU drives nSLEEP through the resistor	EPB-408, BLD-120	SG-01, SG-03
2	R58, Q6, R53, C63 DNP (48 V fit); variant-controlled BOM with option fits as special characteristics	EPB-401, EPB-404, EPB-406	SG-03, SG-04
3	OUTA/OUTB voltage readback to spare MCU ADC inputs; periodic cut-off test	EPB-211, EPB-411	SG-03, SG-04
4	Motor-phase isolation driven independently of U5	BLD-201, BLD-118	SG-01
5	Pull resistors on U5 inputs and angle-sensor outputs; split angle channels across ADC modules with a reference check	BLD-102, ANG-101, ANG-306	SG-01
6	Soft-termination or fail-open 48 V capacitors away from the board edge; CAF-resistant laminate; IMON current check	PCB-201, PCB-202, PCB-303	SG-07
7	Hardware latch for the 12 V overvoltage cut-off independent of the transceivers	CAN-415, BCK-303	All (not modelled in scenario B)

6.2 Software safety requirements

391 DFMEA rows credit a mechanism that exists only as a software requirement. Each is PROVISIONAL until specified in the technical safety concept and verified.

Block	Rows	Example requirement
EPB	63	Isense_EPB current with no apply command -> DRVOFF high.
MCU	62	ADC plausibility (all channels saturated) -> fail-silent and report.
BLDC inverter	50	phase current and force plausibility against the request -> DRVOFF high, report within 100 ms
Motor angle	41	U12/U13 channel compare every control period (ANG-309) and an angle-motion check; an ADC range check does not see the held value.
CAN	41	E2E check of every request (CRC over data and data ID, alive counter, timeout) and plausibility against pedal inputs and vehicle state (MC-02)
Pedal input	37	report the fall-back path unavailable and warn the driver.
Wheel speed	32	read U6 status over SPI (VBAT undervoltage and sensor-current window flags, if WSS001 has them) every cycle and treat any fault or loss of pulses ...
PMIC	25	CMPSS4, X-BAR and pin 40 (GPIO238) configured at start-up (OQ-014). The cut-off is not latched (rated once in CAN-415). U2 FAULT and MOS_LM68645 -> ...
Supply input	18	key-off test (drop INH with bridges off, check that DC_BUS decays, store the result).
PCB	12	compare U1 IMON (0.135 V/A, U14.35) with the expected draw while both bridges are idle, switch the ECU supply off (U1 EN/INH path) and report. The ...
12 V buck	10	count supply-loss resets and hold the corner in a reported degraded state after repeated restarts.

6.3 Data requests to TI

Through Quillon Motors: the FMEDA and safety manual of U14, U3, U5, U7 and U2; the TMAG618X-Q1 safety manual; WSS001 documentation; the NVM configuration of the fitted PMIC variant (O386005). Section 5.3 shows which coverage SG-03 depends on; the FMEDA workbook states the coverage each IC must reach.

6.4 Decisions for Quillon Motors

- PMHF budget per corner for each goal (OQ-046).
- FTTIs and the caliper and EPB force profiles (OQ-021, OQ-047, OQ-048).
- Reaction when standstill cannot be confirmed, and SG-03/SG-04 arbitration (OQ-053).
- Fail-safe for the 48 V bus capacitors (OQ-056).
- ASIL of SG-07 (OQ-044).

6.5 Next deliverables

- A per-goal review separating genuine design gaps from conservative assumptions, with the expected result once TI's data confirms typical coverage.
- Technical safety concept with the reactions and software requirements above.
- Full dependent-failure analysis (ISO 26262-9 clause 7).
- FMEDA Rev B on TI data: latent-fault test intervals against the FTTI, mechanism-to-requirement matrix, design-gap review per goal.

7 Open questions

Table 34. Open questions (S10-QLN-OQL-001): 55 open, 1 closed.

ID	Area	Question	Owner	Status	Used by
OQ-001	MCU (U14)	The BOM fits F29P329SM2QPZSQ1. TÜV SÜD certificate Z10 088989 0059 Rev. 00 (issued 2026-09-15, valid to 2031-09-14) lists F29P329SM1QPZSRQ1, F29P329SM1QRFSRQ1 and F29P329SM2QRFSRQ1: the SM2 appears only in the RFS package, and every certified OPN carries the R packing code that the BOM part lacks. Is the fitted part a sample/pre-production number, and is it covered by the certificate and TI's safety manual?	Client (via TI)	Open	DFMEA
OQ-002	PMIC (U3)	U3 is ordered as O386005QDCARQ1, a TPS653860-Q1 orderable listed as Active / Production in the datasheet's package addendum (SLVSFQ1A). TI uses O3860xx part numbers for NVM-configured variants (TI E2E thread 1611363). Which NVM configuration does O386005 carry (monitor thresholds, watchdog mode and timing, reset and SAFE_OUT behaviour)?	Client (via TI)	Open	DFMEA, FMEDA
OQ-003	Scope	TIDUFI0's block diagram includes parts that aren't on the VerB board: DRV3233-Q1 and DRV8243-Q1 (12 V-variant alternates), TCAN1051H-Q1 (no-wake CAN alternative), TCAN1043-Q1 (§2.3.12), a second LM74930-Q1 on Vbat2, and the pedal sensor TMAG3101-Q1 + LDC5072-Q1 (marked "Not On Board"). Please confirm the production configuration.	Client	Open	DFMEA
OQ-004	Harness interface (J1–J23)	J1–J9 and J11–J20 are single-pin wire solder pads with no part fitted (BOM item 33, Pin_* footprints). They include battery input (J3/J4, 12 A) and motor phases (J7–J9, 16 A RMS). J10 (UART and BOOT1) and J21–J23 (angle sensor SIN/COS) are 2.54 mm pin headers. What is the production harness and connector concept?	Client	Open	DFMEA, FMEDA
OQ-005	CAN (U8, U10)	TCAN1043HG pin 11 is unconnected on both transceivers. Intentional?	sev10	Closed	—
OQ-006	Safety goals / HARA	No HARA, safety goals or functional safety concept were provided. TIDUFI0 describes individual safety mechanisms (§2.4.1.1 CMPSS overvoltage cut-off, §2.4.1.6–2.4.1.7 PMIC protection), and TI's EMB application note SDAA375 discusses the safety architecture. sev10 will derive assumed safety goals for this element (ISO 26262-10, safety element out of context). Please confirm, or supply the vehicle-level HARA.	Client	Open	DFMEA
OQ-007	Supplier safety data	The following safety documents are available only on request or under NDA: TPS653860-Q1 safety manual/FMEDA; DRV3263-Q1 safety manual (SFFSBB3, marked "TI Confidential – NDA"; sev10 has not used it); DRV8263-Q1 FS package ("DRV8263-Q1-FS"); TMAG6180-Q1 FS package ("TMAG618X-Q1-FS"); LM68645-Q1 FMEDA; F29P32x safety manual. In addition, the public datasheets for TPS653860-Q1 (SLVSFQ1A, 14 pp) and DRV3263-Q1 (SLVSLU5, 13 pp) are abbreviated; the full datasheets, with electrical characteristics and diagnostic descriptions, are on request. Can the client obtain them under its NDA with TI?	Client (via TI)	Open	DFMEA, FMEDA
OQ-008	Unreleased parts	WSS001 (U6, wheel-speed decoder) and ESD2CAN48-Q1 (U9, U11, CAN ESD protection) have no public product page or datasheet on ti.com. What is their release status, and can datasheets be provided? For the FMEDA: the WSS001 register map, reset flag and frame integrity (CRC or fixed bits), the VBAT and VCC5 limits, and the split of the wrong-speed failure mode into gross and small errors.	Client (via TI)	Open	DFMEA, FMEDA
OQ-009	Pedal sensor interface	Pedal force (PFS, J12) and pedal travel (PTS, J14) come in through wire pads as analog or SENT signals (TIDUFI0: "Analog/SENT"; the input circuit has a 10 kΩ pull-up and a 69.8 kΩ/100 kΩ divider). Each signal is routed to two MCU pins (R128/R145, R129/R144). The sensors are powered from 5Vp1/5Vp2 (J15/J11). Which signal type, which sensors (TI shows TMAG3101-Q1 + LDC5072-Q1 for travel; force sensor unspecified), and what plausibility checks does the application use?	Client	Open	DFMEA, FMEDA
OQ-010	Mission profile	What mission profile applies: temperature at the ECU mounting location, operating hours, lifetime? TI specifies the reference design for –25 to 75 °C open-frame lab use only, which is not an automotive profile.	Client	Open	DFMEA, FMEDA
OQ-011	Fitted configuration	The published BOM (single variant, "No Variations") fits all 0 Ω option links, including links TI describes as either/or:	Client	Open	DFMEA
OQ-012	EPB control	The net named IN2_EPB connects to DRV8263 pin 9 (EN/IN1) and IN1_EPB to pin 10 (PH/IN2). Is this intentional, and does the firmware pin mapping follow the pins or the names?	Client	Open	DFMEA
OQ-013	Supply redundancy	TIDUFI0's block diagram shows two supplies (Vbat1/Vbat2), with the second LM74930-Q1 off-board. The VerB board has a single battery input (J3/J4). Is a single supply the intended architecture for this ECU, or is redundancy provided at system level?	Client	Open	DFMEA

ID	Area	Question	Owner	Status	Used by
OQ-014	Overvoltage safety mechanism	TIDUFI0 §2.4.1.1 and SDAA375 describe an overvoltage cut-off in which the F29 CMPSS acts through the TCAN1043H EN/INH pins to shut down the supply chain. TI classifies TCAN1043H-Q1 as Functional Safety-Capable, not developed to an ASIL. What ASIL decomposition and fault-tolerant time interval apply? And since the CMPSS must be configured by firmware, which is available only through TI sales, how is the mechanism verified?	Client (via TI)	Open	DFMEA, FMEDA
OQ-015	Dependent failures	The wheel-speed decoder U6 and the EPB driver U7 share one SPI bus (SDIEPB/CLKEPB on U6.10/11 and U7.14/13). The MCU boot-mode pin BOOT1 (U14.80) is brought out on header J10. Is the shared bus accepted in the safety concept, and is J10 depopulated in production?	Client	Open	DFMEA
OQ-016	PCB construction	The IPC-356 header lists a six-layer stackup (Top, GND, Power, Sig4, GND, Bottom), but the Gerber package contains outer copper layers only (GTL/GBL). What is the production stackup, copper weight and PCB material?	Client	Open	DFMEA, FMEDA
OQ-017	Voltage class	The 48 V variant is specified for 32–60 V, and the LM74930-Q1 overvoltage trip is set at 60.6 V. Which 48 V supply standard (ISO 21780 / LV 148) and which transient and load-dump profiles apply?	Client	Open	DFMEA, FMEDA
OQ-018	Component qualification	26 BOM lines don't state an AEC-Q grade. For several, the part-number series suggests general-purpose rather than automotive parts: Murata GRM (items 4, 10, 14, 16, 21), TDK C1608 (item 17) and KEMET C0402C...RAC (item 13; KEMET's link resolves to its commercial X7R series datasheet). sev10 will confirm each against the manufacturer datasheet during the datasheet step. Are the confirmed commercial-grade parts replaced by AEC-Q200 equivalents in production?	Client	Open	DFMEA, FMEDA
OQ-019	BOM integrity	Three fitted part numbers don't appear in the orderable lists of their own datasheets:	Client	Open	DFMEA
OQ-020	Vehicle brake architecture	Does the truck use EMB calipers at all four corners with no hydraulic back-up, and where does the blending (regenerative/friction split) run?	Client	Open	DFMEA
OQ-021	Timing	What fault-tolerant time intervals apply to each safety goal, and how fast must the corner follow a change in friction share when regeneration drops out? For the FMEDA: how the SG-05 FTTI divides between detection in this ECU, CAN transport and the brake controller's reaction.	Client	Open	DFMEA, FMEDA
OQ-022	Safe state	Is a fail-silent corner (brake released, fault reported, other corners and yaw control compensate) acceptable at vehicle level?	Client	Open	DFMEA, FMEDA
OQ-023	Caliper and EPB mechanics	Does the service brake release when the caliper motor is unpowered, and does the EPB spindle hold without power?	Client	Open	DFMEA, FMEDA
OQ-024	Vehicle data	What are the curb mass, GVWR, towing limits and axle loads, and which brake regulation applies (FMVSS 135 / UN R13-H for ≤ 3.5 t, or FMVSS 105 / R13)?	Client	Open	—
OQ-025	Partitioning	How are the four corner ECUs split across power supplies and CAN buses?	Client	Open	DFMEA, FMEDA
OQ-026	Parking-brake functions	Is this ECU responsible for dynamic EPB apply on driver request (secondary braking) and for auto-hold at standstill?	Client	Open	DFMEA
OQ-027	EPB shut-off	TIDUFI0 §2.4.1.7 says the PMIC disables the motor drivers, but on PCB VerB no PMIC safe-state output reaches the EPB driver U7 (DRVOFF_EPB goes only to the MCU). Intended, or a change for production?	Client (via TI)	Open	DFMEA
OQ-028	Design verification	Which design verification will the module receive before release (bench functional tests, fault injection, worst-case circuit analysis, environmental and EMC testing per ISO 16750 / ISO 21780 / CISPR 25, HIL)? TI's published test results for TIDA-020106 cover the PMIC power-on sequence and MCU reset only.	Client	Open	DFMEA, FMEDA
OQ-029	EPB cut-off drive	The published BOM fits R57, R58 and Q6 together with the DRV3263A (U5). The schematic labels U5 pin 31 "PVDD for DRV3233", so R58 is the DRV3233 supply strap; with the DRV3263 fitted it ties CUTOFF1 (pin 31), and through R57 the gate of the EPB cut-off FET Q11, to 48V/12V_P. Q6 is the alternative VCP-based gate drive for the DRV3233. Which of R57, R58, Q6, R53 and C63 are fitted in the production configuration, and which device drives Q11?	Client (via TI)	Open	DFMEA, FMEDA
OQ-030	PCB spacing	Is the board conformally coated in production? The design rules in the Gerber package set 7.87 mil (0.2 mm) general clearance and 15.75 mil (0.4 mm) for the 48 V to GND rule; several 48 V pads sit 0.4–0.6 mm from other nets (for example C96 to R91, which is on 3.3 V).	Client	Open	DFMEA, FMEDA
OQ-031	EPB actuator	What are the EPB motor's inrush, running and stall currents (including at -40 °C), its winding resistance and inductance, the harness length, and the apply time and force ramp to holding force?	Client	Open	DFMEA

ID	Area	Question	Owner	Status	Used by
OQ-032	EPB and BLDC driver firmware	How does the firmware configure and supervise U7? Specifically: idle state of DRVOFF_EPB and IN1/IN2, S_MODE, OCP_SEL, S_ITRIP, fault reaction (latch or retry), SPI_IN and register lock, DRV_SEL, periodic readback, reaction to a persistent nFAULT, stall-termination threshold, minimum run time and timeout. Are there software safety requirements for the EPB?	Client	Open	DFMEA, FMEDA
OQ-033	EPB driver (U7)	Three DRV8263-Q1 points need TI to confirm. (1) The powered-off-braking default: p.38 says enabled, but the CONFIG3 reset value 40h gives EN_POB = 0. (2) The DRVOFF low level with series resistance up to 45 kΩ against the 150 kΩ minimum internal pull-up. (3) Device behaviour with VDD open while EN/IN1, PH/IN2 or nSCS are driven high (back-powering).	Client (via TI)	Open	DFMEA
OQ-034	BLDC motor and magnet data	What are the caliper BLDC motor pole-pair count and maximum speed, the angle magnet grade, size, holder and the board side it faces, the air gap to U12 (top) and U13 (bottom) over temperature and life, and centring tolerance?	Client	Open	DFMEA, FMEDA
OQ-035	Wheel-speed vehicle data and sensor type	Tone-wheel tooth count, tyre rolling circumference, the SG-03 standstill speed threshold and confirmation time, and the wheel-speed sensor type (2-level, AK, HR-AK) with its reverse-polarity behaviour.	Client	Open	DFMEA, FMEDA
OQ-036	Pedal sensor interface parameters	Pedal force and travel sensors: SENT tick time and frame format (secure or redundant data), output type (push-pull or open drain) and VOH, supply current, and the supplier recommended receiver network.	Client	Open	DFMEA
OQ-037	Harness routing, segregation and ESD at ECU pins	Does the production harness route sensor, CAN or pedal wires alongside 48 V class conductors (BLDC phases, EPB motor, battery feed)? What ESD level (ISO 10605) and transient immunity apply at each ECU wire pad?	Client	Open	DFMEA
OQ-038	Sensor plausibility and ADC allocation in firmware	Which plausibility checks does the firmware apply to the angle channels (channel compare, sin^2+cos^2, quadrant consistency, range), wheel speed (standstill confirmation) and pedal inputs (dual-sensor compare)? Which ADC modules and triggers are used for each channel? Also: which angle channel the firmware uses for commutation, and whether the other channel is used only for comparison or fused into the angle (the SG-01 FMEDA treats U13 as the monitor channel).	Client	Open	DFMEA, FMEDA
OQ-039	CAN network architecture and parameters	Do both CAN buses carry the clamp-force requests and status to every corner, or does each corner get its requests on one bus only? What are the arbitration and data bit rates, sample points, transmitter delay compensation, node count, cable lengths, and which nodes terminate each bus? For the FMEDA: which CAN channel or channels carry the wheel speed, and the CAN bit-timing tolerance.	Client	Open	DFMEA, FMEDA
OQ-040	Corner identity and end-to-end protection	How is each corner ECU's position (and the CAN data IDs that follow from it) set in production: coding pins, end-of-line coding or software variant? Which E2E profile (CRC, alive counter, data ID, timeout) protects the brake request and status frames, and what reaction is required on timeout?	Client	Open	DFMEA, FMEDA
OQ-041	Holding the overvoltage cut-off	After the SDAA375 CMPSS trip drops INH_CAN, how is the off state held? Normal bus traffic is a valid wake-up pattern and restores INH within milliseconds; EN or WAKERQ state can also block the sleep. Must firmware stop both motors before any intentional INH drop, and is a hardware latch or a clamp/chopper on 48V/12V_P acceptable?	Client (via TI)	Open	DFMEA, FMEDA
OQ-042	MCU core supply configuration	R146 is fitted, which ties U14 VREGENZ low and enables the internal VREG while U4 (TPS62902) also drives VDD 1.25 V and the PMIC supervises that rail. TI requires VREGENZ high and a single VDD source when VDD is supplied externally, and limits the P32x CPU to 100 MHz in internal-VREG mode. Which configuration is intended for production?	Client (via TI)	Open	DFMEA
OQ-043	Clamp-force accuracy and overshoot tolerance	What clamp-force accuracy and overshoot tolerance per corner does the vehicle require, i.e. at what force error does a deviation become a safety effect (wrong force, SG-01/SG-02) rather than a quality deviation? Is clamp force estimated from motor current and angle (no force sensor)?	Client	Open	DFMEA, FMEDA
OQ-044	ECU thermal event (smoke or fire)	Several board faults (a resistive crack short of a 48 V bus capacitor below the U1 trip level, CAF on 48 V nets, an overheated wire pad) can char the laminate and cause smoke or fire at the wheel corner. The HARA has no hazardous event or safety goal for a thermal event of the ECU. Should one be added at vehicle level, and with what ASIL?	Client	Open	DFMEA, FMEDA
OQ-045	Special characteristics (control plan)	Quillon Motors, do you intend to mark these fitting-variant parts as special characteristics (SC) in your control plan? R22, R97, R99, R58, R146, the boot straps R147-R150, and the DRV3233 option parts Q6, R53 and C63, which are fitted on the published BOM together with the DRV3263.	Client	Open	—
OQ-046	FMEDA, PMHF allocation	ISO 26262-5 sets the PMHF target per safety goal for the whole item (for ASIL D below 10 FIT). What share of each goal's budget is allocated to one corner brake ECU, given four corners and the central brake controller?	Client	Open	FMEDA
OQ-047	FMEDA, SG-03 fault reaction	When the EPB is applied without a request while the vehicle moves, how much rear clamp force can build before vehicle stability is affected at speed, and how fast does the EPB actuator build force (force against time from the start of motion)? The SG-03 stops open the supply cut-off (Q11) or put U7 to sleep: they end the apply but do not release the force already built.	Client	Open	FMEDA

ID	Area	Question	Owner	Status	Used by
OQ-048	FMEDA, SG-01 safe state	How fast does the service caliper release when the motor is de-energised, and how much does a shorted inverter phase or a shorted winding (motor braked by back-EMF) slow that release? Please give clamp force against time after de-energising, from full force, with the phases open and with one phase shorted, together with the motor's back-EMF constant and winding resistance.	Client	Open	FMEDA
OQ-049	Wheel-speed monitoring in the brake controller (assumption ...	Which checks does the brake controller apply to each corner's wheel speed: cross-wheel deviation threshold and confirmation time, wheel-acceleration limit, loss-of-pulse timeout, E2E timeout, and handling of a sensor fault during an ABS or ESC intervention? What wheel-speed error at one wheel does ABS/ESC tolerate without a hazard?	Client	Open	FMEDA
OQ-050	FMEDA SG-02 (corner loss reporting)	What status does each corner ECU send to the brake controller (content, cycle, E2E profile, on which CAN channels), what timeout and reaction does the brake controller apply when the status stops, freezes or reports "unavailable/limited", and how long may a corner take from an unplanned reset to reporting again? Is the corner required to hold "unavailable" after a reset whose cause it did not command until its start-up tests pass?	Client	Open	FMEDA
OQ-051	FMEDA SG-02 (corner loss reporting)	What clamp-force build-up time and force shortfall at one corner does the vehicle tolerate before it counts as "insufficient or late braking" (FE-05, FE-06), at the lowest unrestricted bus voltage and -40 C? What thresholds and debounce should the corner use to declare itself "limited" rather than "unavailable"?	Client	Open	—
OQ-052	FMEDA SG-04 (EPB hold)	Can one rear EPB alone hold the vehicle at GVWR, with a trailer if towing is permitted, on the steepest parking gradient, (a) at its normal clamp force and (b) after a re-clamp? How fast does the other rear corner re-clamp after a CAN report that this corner lost its hold? How much clamp force does the EPB lose in the first 50, 100 and 300 ms of an unintended release?	Client	Open	FMEDA
OQ-053	FMEDA SG-04 (EPB hold)	When the corner detects a fault and standstill cannot be confirmed (wheel speed invalid, CAN speed missing), which reaction applies to the EPB: release and inhibit (SG-03) or hold (SG-04)? Does losing the standstill confirmation during auto-hold ever release the hold? If the standstill hold is first taken by the service brake, do the SG-01 reactions (release to zero force on a request timeout, CAN-102; release first after a PMIC reset, PMC-419) wait for the EPB to take over?	Client	Open	FMEDA
OQ-054	FMEDA SG-07 (thermal event)	What share of 48 V MLCC crack shorts and aluminium-electrolytic internal shorts on this board stay in the resistive band (about 3 Ohm to a few hundred Ohm at 54 V) long enough to heat the site, rather than going straight to a hard short that trips U1? And what is the lowest sustained power at a 1210, 0805 and 0603 site on this stack-up that reaches the laminate decomposition temperature? Both can come from the fault injection that PCB-202, BLD-401 and PCB-303 already plan (1-20 Ohm across C22, C76, C96 at 54 V).	Client	Open	FMEDA
OQ-055	FMEDA SG-07 (thermal event)	Is a thermal event while the vehicle is parked and unattended (key off, 48 V still present at J3/J4) in the scope of HE-20, and should the FMEDA then use calendar hours for the nets that stay biased in sleep (48V/12V_IN, 48V/12V_IN_FILTERED, NetC7_2, NetQ2_5, D1, C7-C10, C8)?	Client	Open	FMEDA
OQ-056	FMEDA SG-07 (thermal event)	Which fail-safe does Quillon Motors choose for the 48 V bus capacitors: fail-open (floating-electrode or series) MLCCs, an eFuse or fuse below the U1 breaker band, or AEC-Q200 soft-termination parts with the IMON check? The DFMEA actions (PCB-202, EPB-201, BLD-401, SUP-417, BCK-103) allow any of them.	Client	Open	—

8 Abbreviations and references

Term	Meaning
AP	Action priority (AIAG-VDA): High, Medium, Low
S / O / D	Severity, occurrence, detection ratings
SPFM / LFM	Single-point fault metric / latent fault metric (ISO 26262-5)
PMHF	Probabilistic metric for random hardware failures, in FIT
FIT	Failures per 10^9 device hours
DC	Diagnostic coverage
FTTI	Fault-tolerant time interval
SEooC	Safety element out of context
CAF	Conductive anodic filament growth in the laminate
DNP	Do not populate
E2E	End-to-end protection of messages (CRC, counter, timeout)
ASIL / QM	Automotive safety integrity level (A–D) / quality managed, no ASIL
HARA	Hazard analysis and risk assessment
TSC	Technical safety concept
HIL	Hardware-in-the-loop test
BOM	Bill of materials
ECU	Electronic control unit
EPB / EMB	Electric parking brake / electro-mechanical brake
BLDC	Brushless DC motor
PMIC / MCU	Power-management IC / microcontroller
NVM	Non-volatile memory (PMIC factory configuration)
CMPSS	Comparator subsystem of the F29 MCU
ECC / ESM	Error-correcting code / error signalling module
BIST	Built-in self-test
MLCC / TVS	Multilayer ceramic capacitor / transient-voltage suppressor
SENT	Single Edge Nibble Transmission sensor interface (SAE J2716)
SG / HE / FE	Safety goal / hazardous event / failure effect
MC-01 to MC-03	Multi-corner goals of the HARA: faults that propagate to several wheels
SM / LM	Safety mechanism that prevents a violation / that detects latent faults (FMEDA)
OQ	Open question in S10-QLN-OQL-001
A-xx	Assumption of the HARA item definition
LAT / CC / SC	DFMEA filters: latent, common cause, special characteristic
As built (A) / with actions (B)	The two FMEDA scenarios, section 3.2.2
Quillon	Quillon Motors, the (fictional) client

Ref	Document
[1]	ISO 26262-2, -5, -9, -10, -11:2018 Road vehicles – Functional safety
[1a]	SN 29500 (Siemens) and IEC 61709: failure rates of components; IEC TR 62380 reliability data handbook
[2]	AIAG-VDA FMEA Handbook, 1st edition 2019
[3]	TI TIDUFI0, Electro-Mechanical Brake (EMB) Reference Design
[4]	TI TIDA-020106 design files SLVMF37A–41A, SLVC962A
[5]	S10-QLN-HARA-001 Rev B; S10-QLN-DFMEA-001 Rev A; S10-QLN-FMEDA-001 Rev A (sev10)
[6]	S10-QLN-OQL-001 Open questions log (sev10)

Illustrative engagement: Quillon Motors is a fictional client and the vehicle assumptions are sev10's. TIDA-020106 is analysed from Texas Instruments' published design files; TI has not reviewed or endorsed this analysis. TI, Texas Instruments and the TI part numbers are trademarks of Texas Instruments Incorporated.

Appendix A Effect library

Table 35. Failure-effect library.

Effect	S	Goal	ASIL	End effect
FE-01	10	SG-01	D	Unintended clamp force at this wheel (no request): sudden yaw at speed
FE-02	10	SG-01	D	Clamp force not released after braking: residual drag or lock at speed
FE-03	10	SG-01	D	Clamp force above request at this wheel (incl. fill-in overshoot on the rear axle): wheel lock and yaw
FE-04	10	SG-01	D	Clamp force applied at the wrong wheel (corner identity or request addressing): yaw in the wrong direction
FE-05	10	SG-02	C	No or too little clamp force at this wheel when requested: longer stop, pull
FE-06	10	SG-02	C	Clamp force late (response slower than required), incl. friction fill-in when regeneration drops out
FE-07	10	SG-02	C	Loss or limitation of this corner not reported: other corners do not compensate, no driver warning
FE-08	10	SG-03	D	Parking brake applied while the vehicle moves, not requested: rear wheel lock at speed
FE-09	10	SG-03	D	Parking brake cannot be actively released after an unintended apply (safe state of SG-03 lost)
FE-10	10	SG-04	C	Parking or standstill hold lost or released unintentionally: vehicle rolls away
FE-11	10	SG-04	C	Parking brake does not reach holding force on apply: vehicle may roll
FE-12	10	SG-06	A	No dynamic parking-brake apply when the driver requests secondary braking
FE-13	10	SG-05	B	Erroneous wheel speed reported (too high, too low, frozen or late): ABS/ESC act on a wrong value
FE-14	10	SG-03	D	False standstill indication: parking-brake apply permitted while moving
FE-15	10	MC-01	D	Fault propagates beyond this corner (bus blocked, shared supply pulled down): braking lost at several wheels
FE-16	10	MC-02	D	Erroneous request or pedal value accepted and acted on: unintended braking (at several wheels if shared; at one corner this is HE-19 under SG-01)
FE-17	10	SG-01	D	Safety mechanism for SG-01 (service brake) unavailable (latent): the next fault is not controlled
FE-18	10	SG-02	C	Safety mechanism for SG-02 (braking availability, reporting) unavailable (latent): the next fault is not controlled
FE-19	9	REG	QM	Regulatory noncompliance (EMC emissions or immunity, UN R10; brake warning requirements)
FE-20	8	QM	QM	Parking brake will not release: vehicle cannot drive away (HE-17)
FE-21	7	QM	QM	False trip: corner reported unavailable without a real fault; braking degraded, driver warned
FE-22	6	QM	QM	Auto-hold or other convenience function unavailable
FE-23	2	QM	QM	Debug, programming or status indication unavailable (workshop only)
FE-24	1	QM	QM	No discernible effect
FE-25	10	SG-03	D	Safety mechanism for SG-03 (no parking-brake apply while moving) unavailable (latent): the next fault is not controlled
FE-26	10	SG-04	C	Safety mechanism for SG-04 (standstill hold) unavailable (latent): the next fault is not controlled
FE-27	10	SG-05	B	Safety mechanism for SG-05 (wheel-speed integrity) unavailable (latent): the next fault is not controlled
FE-28	10	MC-03	C	Wheel-speed information lost or wrong at several wheels (shared supply, bus or cause)
FE-29	10	SG-07	B	Thermal event of the corner ECU (smoke, fire) from an internal fault

Appendix B FIT data

Table 36. Failure rates and failure-mode splits.

Key	Description	λ (FIT)	Source	Split	Status
U14	MCU F29P329SM-Q1 (whole device)	150	Order of magnitude for a large automotive MCU with flash, before safety mechanisms	Per row on the goal tabs (TI FMEDA not public)	ASSUMED (GATED, OQ-007)
U7	EPB H-bridge driver DRV8263-Q1	20	Order of magnitude for a 65 V H-bridge driver	Per row on the goal tabs (TI FS document on request)	ASSUMED (GATED, OQ-007)
U3	Safety PMIC TPS653860-Q1	40	Order of magnitude for a multi-rail safety PMIC	Per row on the goal tabs (TI FMEDA on request)	ASSUMED (GATED, OQ-007)
U5	BLDC gate driver DRV3263-Q1	30	Order of magnitude for a three-phase gate driver	Per row on the goal tabs (TI safety manual under NDA)	ASSUMED (GATED, OQ-007)
U6	Wheel-speed interface WSS001-Q1	15	Order of magnitude for a wheel-speed interface IC	Per row on the goal tabs (no public datasheet)	ASSUMED (UNRELEASED, OQ-008)
FET-80V	Power MOSFET 80 V (SQJA90EP)	10	Order of magnitude under motor-drive stress; no vendor FIT for ISO 26262 use	D-S short 40 %, D-S open 20 %, G-S short 15 %, on-resistance increase 25 %	ASSUMED (JUDGMENT, OQ-010)
DTR	Dual digital transistor (BCR22PN)	2	SN 29500-order value for a small-signal transistor pair	C-E short 40 %, open 40 %, gain drift 20 %	ASSUMED (NO-CLIENT-DATA, OQ-010)
RES-0402	Thick-film chip resistor 0402	0.3	SN 29500-order value	Open 60 %, short 10 %, drift 30 %	ASSUMED (NO-CLIENT-DATA, OQ-010)
RES-0R	Zero-ohm link 0402	0.1	SN 29500-order value	Open 100 % (no other credible mode)	ASSUMED (NO-CLIENT-DATA, OQ-010)
MLCC-0402	MLCC 0402, 50 V	0.5	SN 29500-order value	Short 50 %, open 30 %, capacitance loss 20 %	ASSUMED (NO-CLIENT-DATA, OQ-010)
MLCC-0603	MLCC 0603, 100 V soft termination	0.8	SN 29500-order value	Short 50 %, open 30 %, capacitance loss 20 %	ASSUMED (NO-CLIENT-DATA, OQ-010)
MLCC-1210	MLCC 1210, 100 V general grade	2	SN 29500-order value raised for flex-crack exposure (DFMEA PCB-201)	Short 50 %, open 30 %, capacitance loss 20 %	ASSUMED (NO-CLIENT-DATA, OQ-010)
DIODE-SS	Small-signal Schottky diode (BAT46W)	1	SN 29500-order value	Short 50 %, open 30 %, leakage 20 %	ASSUMED (NO-CLIENT-DATA, OQ-010)
PAD	Wire pad and solder joint (one pad)	0.5	SN 29500-order value for a soldered connection under vibration	Open 70 %, short to adjacent pad or harness 30 %	ASSUMED (NO-CLIENT-DATA, OQ-010)
MLCC-0603G	MLCC 0603, 25-50 V general	0.5	SN 29500-order value	Short 50 %, open 30 %, capacitance loss 20 %	ASSUMED (NO-CLIENT-DATA, OQ-010)
U4	1.25 V core buck TPS62902-Q1	12	TI SFFS465A Table 2-1, IEC TR 62380 / ISO 26262-11 at the 0.5 W column (die 8 + package 4); column chosen by …	TI SFFS465A: output out of spec 22 %, HS or LS FET stuck on 20 %, power FET damage 36 %, …	ASSUMED (JUDGMENT, OQ-010)
U2	12 V buck LM68645-Q1	20	Order of magnitude for a 65 V synchronous buck	Per row on the goal tabs (TI FMEDA on request)	ASSUMED (GATED, OQ-007)

Key	Description	λ (FIT)	Source	Split	Status
U1	Ideal diode and surge stopper LM74930-Q1	14	TI SFFS950 Table 2-1, IEC TR 62380 / ISO 26262-11 motor-control profile, 42 mW (die 3 + package 11)	TI SFFS950 section 3 (gate drives, IMON, OCP, SCP, UV/OV, pin shorts)	Sourced
Y1	MCU clock CDC6C-Q1 (BAW oscillator)	3	TI SFFS685 section 2.4, DLY package (die 2 + package 1)	TI SFFS685: clock degraded 40 %, wrong frequency 30 %, no clock 30 %	Sourced
TCAN	CAN FD transceiver TCAN1043H-Q1 (VSON)	9	TI SLLA525A Table 2-1, IEC TR 62380 / ISO 26262-11 motor-control profile, 126 mW (die 3 + package 6)	TI SLLA525A: receiver 35 %, transmitter 35 %, stuck in sleep 15 %, bus dominant 5 %, pin ...	Sourced
U12-U13	Angle sensor TMAG6180-Q1	10	Order of magnitude for an analog Hall/AMR angle sensor (reference.yaml)	Per row on the goal tabs (TI FS manual TMAG618X-Q1-FS on request)	ASSUMED (GATED, OQ-007)
SHUNT	Metal-element current shunt 0.5 mOhm (BVN-Z)	1	SN 29500-order value for a metal-strip resistor	Open 30 %, resistance drift 70 % (no credible short)	ASSUMED (NO-CLIENT-DATA, OQ-010)
U5-PAS	U5 support passives (C62, C64, C65, C67, C69, C72, C77, ...	5.6	Sum of class values: 7 MLCC 0603 25 V at 0.5 (MLCC-0603G), 3 resistors 0603 at 0.3, 4 resistors 0402 at 0.3	Per row (aggregated; all modes safe for SG-01)	ASSUMED (NO-CLIENT-DATA, OQ-010)
BUS-CAP	48V/12V_P bus capacitors (C60, C73, C74 330 uF aluminium; ...	16	Sum of class values: 3 aluminium electrolytics at 3 FIT, 3 MLCC 1210 at 2 (MLCC-1210), 1 MLCC 1206 at 1	Per row (aggregated)	ASSUMED (NO-CLIENT-DATA, OQ-010)
CSA-FE	Phase-current sense front end (R60, R63, R78, R79, R82, ...	8.2	Sum of class values: 9 resistors 0402 at 0.3, 11 MLCC 0402 at 0.5	Reading error 70 %, no effect 30 % (aggregated)	ASSUMED (NO-CLIENT-DATA, OQ-010)
ADCREF-FE	ADC reference network (L7, L8, L10 ferrites; C44, C83, ...	5.4	Sum of class values: 3 ferrite beads at 0.5, 3 MLCC 0402 at 0.5, 3 MLCC 0603 at 0.8	Reference lost (bead open, capacitor short) 50 %, other 50 % (aggregated)	ASSUMED (NO-CLIENT-DATA, OQ-010)
ANG-FE	Angle sensor front end, one channel (2 × 1 kOhm, 2 × 100 ...	3.7	Sum of class values: 4 resistors 0402 at 0.3, 3 MLCC 0402 at 0.5, header 4 pins at 0.25	Signal error 70 %, other 30 % (aggregated)	ASSUMED (NO-CLIENT-DATA, OQ-010)
PED-FE	Pedal sensor input network, one channel (3 resistors 0402, ...	2.1	Sum of class values: 3 × 0.3, 2 × 0.1 (RES-0R), 2 × 0.5	Value error 70 %, other 30 % (aggregated)	ASSUMED (NO-CLIENT-DATA, OQ-010)
INH-NET	Transceiver INH network (D6, D7 1N4148WS; R102, R112, ...	3.8	Sum of class values: 2 small-signal diodes at 1.0 (DIODE-SS), 6 resistors 0402 at 0.3	R156 open 5 %, other 95 % (aggregated)	ASSUMED (NO-CLIENT-DATA, OQ-010)
TVS-ESD	Dual ESD protection diode ESD2CAN24-Q1 (SOT-23)	1	SN 29500-order value for a TVS array (the value used for D5 inside WSS-FE)	Short 40 %, open 30 %, leakage or degraded clamp 30 %	ASSUMED (NO-CLIENT-DATA, OQ-010)
RAIL-DEC	Logic-rail decoupling capacitors (1.25V, 3.3V, 5V, 12V, ...	31.3	Sum of class values: 39 MLCC 0402 at 0.5 (MLCC-0402), 4 MLCC 0603 10 uF 10 V at 0.5 (MLCC-0603G), C26 0603 ...	Short 50 % (rail collapse), open or capacitance loss 50 % (class split of MLCC-0402)	ASSUMED (NO-CLIENT-DATA, OQ-010)
PWR-PASS	Supply-chain passives and small switches outside the rail ...	45	Sum of class values: D1 power TVS 2.0; D3, D11 at 1.0 (DIODE-SS); R99 0.3; 4 MLCC 1210 at 2 (C5, C6, C21, ...	Supply lost 44 % (TVS short 0.8, D3/D11/R99 open 0.78, capacitor shorts 7.0 + 1.8, ...	ASSUMED (NO-CLIENT-DATA, OQ-010)
ALU-100V	Aluminium electrolytic 100 V SMD (EMVE, 100-330 uF), one ...	3	SN 29500-order value for a wet aluminium electrolytic at 85 C board temperature, no ripple stress factor ...	Short 20 %, open 30 %, capacitance loss or ESR rise 40 %, venting 10 %	ASSUMED (NO-CLIENT-DATA, OQ-010)
TVS-SMB	Power TVS diode SMBJ51CA (SMB, 600 W)	2	SN 29500-order value for a power suppressor diode; no AEC-Q101 statement for the fitted part (OQ-018)	Short 40 %, open 30 %, leakage or degraded clamp 30 % (as TVS-ESD)	ASSUMED (NO-CLIENT-DATA, OQ-018)
U1-NET	U1 current sense and OCP/SCP set network (R7 1 mOhm shunt; ...	2.9	Sum of class values: R7 at 1 (SHUNT), 3 resistors at 0.3 (RES-0402; R11 is an ATC 504L thin-film part), 2 ...	Disables OCP or SCP or raises its trip level 38 % (R11 open 0.18, R20 short 0.03, R21 ...	ASSUMED (NO-CLIENT-DATA, OQ-010)
BUS-MLCC	48V/12V_P bus MLCCs as built (C5, C6, C21, C22, C61, C75, ...	16.6	Sum of class values: 7 × 2 (MLCC-1210, raised for flex-crack exposure), 2 × 0.8 (MLCC-0603), 1 × 1 (1206 100 ...	Short 50 % (hard or resistive per row), open 30 %, capacitance loss 20 %	ASSUMED (NO-CLIENT-DATA, OQ-018)
BUS-MLCC-B	48V/12V_P bus MLCCs with the DFMEA actions (the seven 1210 ...	9.6	Sum of class values: 7 × 1 (1210 AEC-Q200 soft termination: the SN 29500-order value without the flex-crack ...	Short 50 %, open 30 %, capacitance loss 20 %	ASSUMED (NO-CLIENT-DATA, OQ-018)

Key	Description	λ (FIT)	Source	Split	Status
BDC-MLCC	48V/12V_BDC EPB bulk as built (C96 GRM 1210 100 V general ...	2.8	Sum of class values: 2 (MLCC-1210) + 0.8 (MLCC-0603)	Short 50 % (hard or resistive per row), open 30 %, capacitance loss 20 %	ASSUMED (NO-CLIENT-DATA, OQ-018)
BDC-MLCC-B	48V/12V_BDC EPB bulk with the DFMEA actions (C96 AEC-Q200 ...	1.8	Sum of class values: 1 (1210 AEC-Q200 soft termination) + 0.8 (MLCC-0603)	Short 50 %, open 30 %, capacitance loss 20 %	ASSUMED (NO-CLIENT-DATA, OQ-018)
CAP-12V	12 V rail capacitors as built (C25 GRM 1210; C27, C31-C33 ...	13.3	Sum of class values: C25 2 (MLCC-1210); C27, C31-C33 4 × 2 (SN 29500-order 1 FIT doubled for operation above ...	Short 50 % (hard or resistive per row), open or capacitance loss 50 %	ASSUMED (NO-CLIENT-DATA, OQ-010)
CAP-12V-B	12 V rail capacitors with the DFMEA actions (C25 AEC-Q200 ...	6.3	Sum of class values: C25 1; 4 × 0.5 (automotive X7R within its temperature rating, as MLCC-0603G); C26 0.8; ...	Short 50 %, open or capacitance loss 50 %	ASSUMED (NO-CLIENT-DATA, OQ-010)
CAF-48V	CAF path from one 48 V-class net to GND inside the board, ...	1	No handbook value for CAF. DFMEA PCB-302/PCB-303 rate O 4, which scales.yaml anchors at 1-10 FIT for the ...	Resistive path 100 % (PCB-303: resistive long before it becomes a hard short)	ASSUMED (JUDGMENT, OQ-016)
CAF-48V-R	CAF path from one 48 V-class net to GND with the DFMEA ...	0.2	DFMEA after-occurrence O 2 (< 1 FIT per row, scales.yaml); a fifth of the as-built value per net pair	Resistive path 100 %	ASSUMED (JUDGMENT, OQ-016)
WSS-FE	Wheel-speed front end (D5, R84, R86, R88, C88, C90, C93, ...	5.4	Sum of the class values above: 3 resistors 0.9, 5 MLCC 2.5, TVS 1.0, 2 pads 1.0	Loss of pulses 60 %, other 40 % (aggregated, detailed on the SG-05 tab)	ASSUMED (NO-CLIENT-DATA, OQ-010)

Appendix C Traceability

Table 37. Hazardous event → goal → DFMEA effect → FMEDA.

Goal	Events	DFMEA effects	DFMEA rows	FMEDA rows	Mechanisms used
SG-01	HE-01 to HE-06, HE-19	FE-01, FE-02, FE-03, FE-04, FE-17	253	90	LM-04, LM-05, LM-10, LM-11, LM-12, LM-13, LM-14, LM-15, SM-01, SM-02, SM-08, SM-09, SM-10, SM-11, SM-12, SM-13, SM-14, ...
SG-02	HE-07 to HE-12	FE-05, FE-06, FE-07, FE-18	302	90	LM-04, LM-05, LM-12, SM-12, SM-13, SM-14, SM-15, SM-16, SM-21, SM-30, SM-31, SM-32, SM-33, SM-34
SG-03	HE-13	FE-08, FE-09, FE-14, FE-25	79	93	LM-01, LM-02, LM-03, LM-04, LM-05, LM-06, LM-07, LM-08, LM-13, SM-01, SM-03, SM-04, SM-05, SM-06, SM-07, SM-08, SM-09, ...
SG-04	HE-14, HE-15	FE-10, FE-11, FE-26	52	81	LM-01, LM-02, LM-03, LM-04, LM-05, LM-06, LM-13, LM-40, SM-01, SM-03, SM-04, SM-05, SM-06, SM-08, SM-09, SM-40, SM-41, ...
SG-05	HE-18	FE-13, FE-27	9	60	LM-04, LM-05, LM-20, SM-01, SM-08, SM-20, SM-21, SM-22, SM-23, SM-24
SG-06	HE-16	FE-12	2	—	—
SG-07	HE-20	FE-29	2	70	LM-13, LM-70, SM-09, SM-70, SM-71, SM-72, SM-73

SG-07: most DFMEA thermal chains are still rated under their functional effect (FE-05, SG-02); only two carry FE-29. Re-rating them is an open DFMEA action; the SG-07 FMEDA cites them directly.

Appendix D Review record

The FMEDA was audited by three independent reviewers (method and math, data and sourcing, completeness and client view) and each finding applied or dropped with a reason. Principal corrections: a watchdog credit for a fault it cannot see was removed; supply faults were brought into the metrics; faults with no path to a goal were counted n/a rather than Safe; latent classes were limited to mechanisms active in the scenario; the PMHF is no longer shown as meeting the item budget. The full record is kept with the FMEDA (S10-QLN-FMEDA-001 audit record). This report was reviewed separately for technical accuracy, writing, figures and client view before issue.