

Example DFMEA: Electric Power Steering (EPS)

Design FMEA of the EPS example model that ships with Spine

Illustrative example, not a safety case. Produced with Spine Evaluation Edition, not for production use. Evaluation run. Spine Evaluation Edition is for assessing the tool only, not for production or commercial engineering work. BIG Intelligence gives no confidentiality undertaking for evaluation submissions. Do not submit confidential, proprietary, trade-secret, personal, classified or export-controlled information. This does not limit rights or obligations that the law does not allow to be waived.

Model	EPS example model, built through the Spine gate from a public-domain NHTSA report <i>Built by BIG Intelligence from NHTSA, Functional Safety Assessment of a Generic Electric Power Steering System, DOT HS 812 575 (2018), a US government public-domain report. Its requirements are illustrative and not NHTSA's official position.</i>
Analysis	BIG Intelligence DFMEA service, run d1e2f3a4-5b6c-4d7e-8f90-1a2b3c4d5e6f, 1 October 2026 · run mode: evaluation
Scope	5 functional outputs at the EPS boundary · 30 failure modes · 32 causes · 27 candidate trouble codes
Action priority	High 21 · Medium 6 · Low 3
License	CC BY 4.0. © BIG Intelligence AI, LLC

Read this first

- **AI-proposed, not engineer-reviewed.** Every mode, cause and score was proposed by the DFMEA service and passed Spine's gate. No qualified engineer has reviewed the ratings, so S, O, D and AP are illustrative.
- **Trouble codes are candidates.** The model has no diagnostic library, so each code is a suggested placeholder with no ECU assigned. Every cause has a candidate code. Several codes are shared between causes and would need a pinpoint test to tell the repairs apart.
- **Thin inputs.** Three outputs (O1, O4, O5) declare no interface signals, and one block on O2 is not allocated to a part. Those sections reflect a less complete design and are marked below.
- **Hazardous events** (last page) are the vehicle-level outcomes the failure modes lead to, as the service named them. They have not been through a hazard analysis (HARA), so they carry no ASIL of their own (an ASIL D mentioned in a description is the model's existing safety requirement).
- **TARA mentions.** Where the text mentions TARA, it refers to the model's existing cybersecurity requirements. This DFMEA did not perform a threat analysis (TARA), and Spine does not perform one.
- S = severity, O = occurrence, D = detection (1–10); AP = action priority as the service assigned it.

O1 · raise steering warning matched to the severity

Thin input: no interface signals declared, so this analysis rests on less of the design than it should.

Failure mode and effect	S	AP	Cause	O	D	Candidate code	Current controls
The steering warning never illuminates when assist is withdrawn or a safe state is entered; no annunciation reaches the driver. Effect: Driver receives no cue that power assist is lost; encounters unexpectedly heavy manual steering effort with no warning, degrading controllability during the transition.	8	High	Warning-request service fails to issue the annunciation command on transition to fault-classified / safe-state.	3	6	C1A01	Watchdog on warning task; safe-state entry logs event. No direct confirmation that annunciation was commanded.
			Indicator driver output stage or telltale circuit open — command issued but lamp/telltale cannot light.	3	4	C1A00	Open-load / continuity monitor on indicator driver stage.
A warning is raised but does not match the severity — e.g. an amber/low-urgency indication is shown where a red critical warning is required. Effect: Driver under-appreciates the loss of assist and under-reacts, continuing at speed without preparing for heavy manual steering.	7	High	Severity-to-annunciation mapping defect renders a red-tier condition at a lower warning tier.	3	7	C1A02	Mapping table review during calibration; no runtime consistency monitor.
Warning telltale flickers on and off intermittently rather than holding steady while the fault condition persists. Effect: Driver perceives a transient glitch and discounts/ignores a genuine persistent assist fault, delaying appropriate response.	6	Medium	Intermittent harness/solder contact on indicator driver output causes flicker.	4	7	C1A00	Open/short monitor with debounce; transition counter.
Warning annunciation exceeds the warranted severity — full red plus escalating chime presented for a minor, non-critical degradation. Effect: Nuisance over-warning; driver may react abruptly (sudden braking/pull-over) or progressively distrust the telltale, eroding warning credibility.	5	Low	Severity classifier over-escalates minor degradation to the critical annunciation tier.	2	7	C1A03	Calibration review; hysteresis on severity classifier.
Warning is raised when no assist fault is actually present — a spurious or injected fault flag triggers annunciation. Effect: Driver is alarmed without cause; may brake/pull over abruptly. Repeated false warnings erode trust in a genuine future warning. Potential adversarial injection vector.	5	Medium	Spurious fault flag (noise, memory corruption, or unauthorized injection into the command path) raises the warning with no real fault; TARA requirement 43190433 governs the protection of the command path.	3	6	C1A04	Fault-flag ECC/CRC; access control per safety req 43190433; plausibility cross-check of warning_command vs fault_classified.

Failure mode and effect	S	AP	Cause	O	D	Candidate code	Current controls
Warning is raised, but later than the annunciation deadline after the fault is classified (violates 'as soon as the fault is classified', req 112db3de). Effect: Driver is alerted after the assist change has already been felt; the warning arrives too late to pre-empt the heavy-steering surprise.	8	High	Annunciation task scheduling/latency exceeds the fault-classification-to-warning deadline under load.	3	7	C1A05	Task priority assignment; schedulability analysis; latency timestamping.

O2 · assist torque

Thin input: the block 'Acquire Steering Torque Signal' is not allocated to a part, so this analysis rests on less of the design than it should.

Failure mode and effect	S	AP	Cause	O	D	Candidate code	Current controls
Assist torque is entirely absent; the EPS applies no motor torque to supplement driver effort. Effect: Driver reverts to unassisted mechanical steering with sudden heavy effort, especially hazardous at low speed/parking; controllability degraded.	8	High	Loss of the qualified driver steering demand signal from Acquire Steering Torque Signal (torque-sensor open circuit / acquisition fault), leaving the assist computation with no valid demand input.	3	4	C1A00	Torque-sensor plausibility and continuity monitoring; redundant torque sensing per ASIL B architecture.
Assist is present but below the commanded level; boost is insufficient relative to the computed demand. Effect: Driver perceives heavier-than-expected steering; inconsistent effort increases low-speed workload and may surprise the driver.	7	High	Degraded EPS motor power stage (phase imbalance / current limiting) delivers less torque than the commanded assist level.	4	4	C1A06	Current-feedback vs commanded-torque monitor; motor temperature derating supervision.
Assist torque cuts in and out unpredictably as the acquisition signal flickers. Effect: Driver experiences unexpected, alternating heavy/light steering effort; sudden effort changes reduce controllability and alarm the driver.	8	High	Intermittent qualified driver steering demand signal due to loose torque-sensor connector or EMI on the acquisition path, causing assist to toggle.	4	4	C1A00	Signal debounce and dropout-count supervision; EMI filtering on acquisition path.
Assist torque exceeds the commanded level, producing more motor torque than the driver demand warrants. Effect: Over-assist causes the steering to turn more than intended (self-steering), risking lane departure and loss of directional control.	10	High	Compute Required Assist Level software fault (overflow / gain error) or current-loop gain fault commands assist torque above the demand-proportional level.	2	3	C1A07	Independent redundant torque monitor with over-torque trip to Safe State 3; assist range limiting.
Assist torque is applied when no qualified driver steering demand and no qualified external request exist. Effect: Spurious assist steers the vehicle without driver intent (self-steering), a direct ASIL D controllability hazard; may also result from an injected/unauthenticated external request.	10	High	Arbitration/command-path state-machine fault or injection of an unauthenticated external steering request causes assist to be applied with no qualified driver demand present.	2	4	C1A08	Command-path integrity checks; arbitration plausibility; no-demand-no-assist supervision per req afd85c1d. Message authentication on external request path NOT confirmed (cyber gap).

Failure mode and effect	S	AP	Cause	O	D	Candidate code	Current controls
Assist torque arrives late (or prematurely) relative to the driver's steering input due to control-loop/arbitration latency. Effect: Lagging assist makes steering feel disconnected and inconsistent; sudden late catch-up can overshoot, degrading controllability.	7	High	Control-loop scheduling latency or arbitration delay causes commanded assist to lag the driver input beyond the timing budget.	3	4	C1A0B	Real-time scheduling supervision; latency monitor with budget check.

O3 · steering torque, unassisted

Failure mode and effect	S	AP	Cause	O	D	Candidate code	Current controls
The unassisted mechanical path conveys no torque — driver steering input does not reach the rack at all. Effect: Total loss of steerability after assist is lost; driver cannot steer the vehicle. Potential catastrophic outcome.	10	High	Mechanical decoupling in the column/rack-and-pinion load path (sheared intermediate shaft, stripped pinion, failed coupling) so driver torque never reaches the rack.	2	4	C1A0C	Torque-overload design margin; periodic service inspection of steering coupling.
Mechanical conveyance degraded by excess lash and friction — heavy, imprecise unassisted steering. Effect: Driver experiences heavy, sloppy steering after assist loss; reduced controllability.	8	High	Wear/corrosion increasing lash and friction in the steering gear, degrading conveyance.	3	5	C1A0D	Lubrication specification; EOL free-play check.
Intermittent binding/notchiness in the unassisted path producing unpredictable steering effort. Effect: Driver experiences sudden sticking/catching in steering after assist loss; startle and transient loss of control.	8	High	Intermittent mechanical binding from debris, thermal expansion, or bearing notchiness in the steering gear.	3	6	C1A0E	Sealing against debris; thermal qualification of bearings.
Residual motor/clutch drag not removed when assist is off adds uncommanded torque to the column. Effect: Unintended steering torque on the mechanical path — self-steering contribution in an unintended direction.	10	High	Motor/reduction-gear residual drag or clutch not released when assist is commanded off, adding uncommanded torque to the column.	2	4	C1A0F	Motor-current-off monitor; back-drivable reduction gear design.
Assist torque still present on the path that should be unassisted — assist not fully withdrawn/latched off in safe state. Effect: Assist re-applied or retained while a safe-state fault is present, undermining the deterministic unassisted fallback and masking a self-steer contribution.	9	High	Assist-disable state not fully entered — assist output not latched off while a safe-state fault is present (SR 318b235b violation).	3	5	C1A10	Safe-state latch; self-test gate on assist re-enable.

Failure mode and effect	S	AP	Cause	O	D	Candidate code	Current controls
Withdrawal timing incorrect — assist removed in one step (premature) or ramp exceeds T_SAFE_STATE (delayed) rather than graded reduction. Effect: Abrupt one-step effort change or overlong assist retention during fault — startle/transient loss of control at the fallback transition.	8	High	Withdrawal ramp timer mis-scheduled — assist removed in one step or ramp duration exceeds T_SAFE_STATE / 500 ms (SR 242215e0, caab684a).	3	4	C1A11	Watchdog on ramp timer; graded-withdrawal profile validation.

O4 · stored codes and safe-state record

Thin input: no interface signals declared, so this analysis rests on less of the design than it should.

Failure mode and effect	S	AP	Cause	O	D	Candidate code	Current controls
The EPS unit stores no fault code and no safe-state record; on tester request it returns an empty or unavailable record. Effect: Technician cannot retrieve fault evidence for a steering safe-state event; an ASIL-D fault can go undiagnosed and the vehicle returned to service unresolved; regulatory diagnostic function not met.	7	High	NVM/EEPROM write failure or full diagnostic-memory corruption prevents any code or safe-state record from being stored.	3	5	C1A12	Ignition self-test of diagnostic memory; UDS read-verify on service request.
Stored record is incomplete — freeze-frame fields or timings truncated/missing while a code is present. Effect: Technician receives partial evidence; mis-diagnosis of the underlying steering fault possible; regulatory completeness not met.	6	Medium	Partial NVM corruption / checksum failure on a record segment leaves timings or evidence fields truncated.	3	5	C1A12	Per-segment checksum; UDS read reports incomplete record flag.
Record is retrievable on some ignition cycles and absent/garbled on others due to a flaky memory cell or intermittent internal memory bus. Effect: Technician gets inconsistent results across visits; genuine safety fault evidence missed intermittently, delaying resolution of an ASIL-D fault.	7	High	Marginal NVM cell / intermittent internal memory bus yields non-deterministic record availability.	4	6	C1A12	Read-retry with retry counter; maturation counter for intermittent memory faults.
Fault-maturation/debounce defect stores excessive or false codes (code storm) that swamp or displace the genuine safe-state record. Effect: Technician faces false/excess codes, leading to unnecessary parts replacement and masking of the genuine fault.	5	Medium	Debounce/maturation logic defect sets codes without sufficient confirmation, producing a code storm.	4	4	C1A14	Fault-maturation counters; plausibility gating of code setting.

Failure mode and effect	S	AP	Cause	O	D	Candidate code	Current controls
The stored record is altered during a read, or served/modified when it should not be (e.g. unauthorised or spurious request), violating the serve-without-altering constraint. Effect: Fault evidence integrity compromised; forensic record untrustworthy; potential unauthorised access to stored maps/command paths.	6	Low	Read path lacks write-protection / access control, allowing the record to be modified during serve or served to an unauthorised requester (violates a99cc1cb and 43190433).	2	4	C1A15	UDS security access; read-only enforcement on stored record; integrity MAC on record (per TARA 43190433).
Rolling-buffer overwrites the safe-state event before it is read, or the record timestamp is stale/absent (RTC fault), so timings are wrong or evidence lost. Effect: Fault timings mis-ordered or evidence overwritten before service, impairing root-cause of a safety event and regulatory time-stamping.	6	Medium	Buffer-management policy overwrites the oldest (safe-state) record before read, or RTC/timestamp source fails, yielding stale or absent timings.	3	5	C1A16	Priority retention of safe-state record; RTC validity check on store.

O5 · request not applied

Thin input: no interface signals declared, so this analysis rests on less of the design than it should.

Failure mode and effect	S	AP	Cause	O	D	Candidate code	Current controls
The 'not applied' guarantee is absent entirely: Arbitrate Steering Demands fails to reject a conflicting external (Lane-Centering) request, so the external request is passed to the assist computation and applied against the driver's deliberate opposite demand. Effect: Conflicting external request is applied, overriding the driver -> unintended self-steering in a direction the driver is actively opposing; loss of directional control.	10	High	Driver-priority comparison in Arbitrate Steering Demands is defective; the external request is not gated out when the driver demand conflicts, so it reaches Compute Required Assist Level.	3	5	C1A17	SR f3864ab4 (follow-driver arbitration) and e818e2f0 (prevent unintended self-steering) specified; no runtime monitor or EOL screen on the arbitration-conflict path currently defined.
			Spoofed or injected external steering request on the vehicle bus is accepted as a qualified request because a single-point fault in plausibility/authentication protection is not mitigated, so it is applied against the driver.	2	6	C1A1D	SR 43190433 (prevent unauthorised access, detect/mitigate single-point faults), a4d19c14 and d012daac (out-of-range external request must not contribute) specified; no message authentication monitor DTC defined.
The conflicting external request is only partially rejected; a residual fraction is blended into the steering demand instead of being fully suppressed. Effect: Degraded arbitration: an unwanted external steering contribution adds to the demand, nudging the vehicle contrary to the driver's intent.	9	High	Blend-gain error in Arbitrate Steering Demands leaves a residual external contribution instead of driving it to zero on conflict.	3	6	C1A18	SR f3864ab4 specifies full follow-driver behaviour; no residual-contribution monitor defined.
Arbitration intermittently fails to reject the conflicting external request, applying it for brief intervals before recovering. Effect: Transient self-steering jerks against the driver during conflict windows; unpredictable, hard-to-diagnose directional disturbances.	9	High	Race condition / transient corruption on the arbitration input latch intermittently lets the rejected external request through for one or more cycles.	4	7	C1A19	SR f3864ab4 and bbcc078a (detect assist-path fault within fault-detection interval); no transient-latch monitor defined.
The conflict detector over-triggers (threshold too sensitive), so the 'not applied' behaviour over-asserts and suppresses ALL external requests including valid, non-conflicting qualified ones. Effect: Lane-Centering and other qualified external steering features are effectively disabled; customer loses the driver-assistance feature.	5	Medium	Conflict-detection threshold set too low, classifying harmless external requests as conflicts and suppressing them.	3	5	C1A1A	Calibration review; lane-centering feature validation drives.

Failure mode and effect	S	AP	Cause	O	D	Candidate code	Current controls
The 'request not applied' report is issued when it should not be — no conflict existed and the request was validly applied — a spurious rejection report to the requesting system. Effect: Lane-Centering is falsely told its valid request was overridden; it may retry, escalate, or disengage unnecessarily, degrading the feature and eroding trust.	4	Low	Conflict-classification state machine latches a 'conflict' state spuriously (e.g., stale flag not cleared), causing the 'request not applied' report to be emitted when no conflict exists.	3	5	C1A1B	SR f3864ab4 defines report semantics; no spurious-report monitor defined.
Arbitration latency exceeds the override window: the conflicting external request is applied transiently before the driver-priority decision resolves and suppresses it. Effect: Brief unintended steering contribution against the driver at the start of a conflict before the override takes effect; delayed report to the requester.	9	High	Arbitration decision latency exceeds the driver-override deadline, so the external request reaches the assist output for one or more cycles before being suppressed.	3	6	C1A1C	SR caab684a / 242215e0 (timing budgets) and bbcc078a (fault-detection interval); no runtime override-latency monitor defined.

Hazardous events

The outcomes the failure modes above can lead to, named once and reused across outputs. These events have not been classified by a HARA and carry no ASIL of their own; where a description mentions ASIL D, it refers to the EPS model's existing safety requirements.

Hazardous event	Description
Loss of driver warning for steering assist fault	The driver is not alerted (absent warning) that power steering assist has been lost or withdrawn, leaving the driver unprepared for the sudden heavy-effort mechanical steering transition.
Unintended steering warning activation	A steering warning is annunciated when no genuine assist fault exists (spurious or injected fault flag), alarming the driver without cause and eroding trust in future genuine warnings.
Loss of steering assist torque	Power steering assist torque is lost or absent, forcing the driver onto heavy-effort mechanical steering and creating a controllability hazard, especially at low speed.
Unintended self-steering	The EPS applies motor torque to the steering without a qualified driver demand or produces excess assist, steering the vehicle in an unintended direction and risking loss of control (ASIL D).
Loss of mechanical steering capability	Complete inability to convey the driver's steering torque mechanically to the road wheels when assist is withdrawn, leaving the driver unable to steer the vehicle at all — the ASIL-D last-line steering behaviour is lost.
Loss of stored fault evidence for steering safe-state events	The EPS diagnostic memory fails to store or serve the DTCs and safe-state record, so a service technician cannot retrieve the fault evidence and timings for a steering safe-state event, risking that an ASIL-D fault is returned to service undiagnosed.
Tampering with stored steering fault evidence	The stored steering fault evidence is altered during a read or served/modified when it should not be, compromising the integrity of the forensic record and potentially exposing stored maps and command paths to unauthorised access.
Loss of request-not-applied report to external steering system	The EPS fails to correctly report to the requesting system whether its steering request was applied — either omitting, delaying, or spuriously asserting the 'not applied' feedback — degrading feature coordination with the Lane-Centering System.

Requirements referenced

The requirement IDs cited above, with each requirement as stated in the EPS example model that ships with Spine. IDs are the first 8 characters of the requirement's identifier in the model.

ID	Requirement
43190433	The EPS Control Module shall prevent unauthorised access to the steering-assist algorithms, the stored maps, the calculations and the command paths, and shall detect and mitigate every single-point fault in that protection.
112db3de	If the assist output is lost without a controlled withdrawal, the steering system shall keep conveying the driver's torque to the road wheels and shall raise the red driver warning as soon as the fault is classified.
afd85c1d	While neither a qualified driver steering demand nor a qualified external steering request is present, Arbitrate Steering Demands shall issue no steering demand and Compute Required Assist Level shall compute no assist, so that Apply Assist Torque To Steering has no commanded torque to apply and no assist reaches the steering.
318b235b	While a fault that caused a safe state is still present, the steering system shall NOT re-enable the assist output.
242215e0	If assist has to be withdrawn, the steering system shall reduce it to the level the safe state allows within T_SAFE_STATE rather than removing it in one step.
caab684a	If assist has to be withdrawn, the steering system shall reduce it to the level the safe state allows within 500 ms rather than removing it in one step.
a99cc1cb	When a tester requests the stored record, the steering system shall serve the fault evidence and its timings without altering the stored record.
f3864ab4	When the driver's steering demand conflicts with an external steering request, the steering system shall follow the driver and shall report to the requesting system that its request was not applied.
e818e2f0	The Column-Assist EPS Unit shall prevent unintended self-steering in any direction under all vehicle operating conditions, to ASIL D.
a4d19c14	While an external steering request lies outside its plausible range, the steering system shall NOT let that request contribute to the steering demand.
d012daac	While an external steering request is outside its plausible range, the steering system shall NOT let that request contribute to the steering demand.
bbcc078a	If a fault in the assist path would violate a safety goal, the steering system shall detect it within its fault detection interval and shall NOT continue to assist without raising a warning.

Spine Evaluation Edition is for assessing the tool only. Licensed under CC BY 4.0 (creativecommons.org/licenses/by/4.0). Attribution: BIG Intelligence AI, LLC, "Example DFMEA: Electric Power Steering", 2026. Built by BIG Intelligence from NHTSA, Functional Safety Assessment of a Generic Electric Power Steering System, DOT HS 812 575 (2018), a US government public-domain report. Its requirements are illustrative and not NHTSA's official position.