

oAOML: Engineering Failure Analyses

Canonical Incidents Mapped to the Five Structural Violation Types

Companion Document to Papers II and III, Foundations of the Convergent Semantic Architecture

Brent Alan Seeley · WellFlow Labs · August 2026

DOI: <https://doi.org/10.5281/zenodo.21960566>

1. Scope and Epistemic Status

This document is the engineering counterpart of the Universal Fallacy Map (Second Edition, <https://doi.org/10.5281/zenodo.21880635>). Where the map demonstrates that the classical fallacy tradition decomposes into the five structural violation types, this ledger demonstrates the same decomposition in a non-linguistic substrate: engineering failures documented by official post-mortem investigation. It is the artifact behind the evidence line Papers II and III cite as engineering failure analysis (oAOML). The o is operational: oAOML, Operational Axis-Operator-Method-Level, is the architecture's implementation program, whose verified legality layer and sealed preregistered study are the enforcement and predictive arms beside this evidence ledger (see §6).

Two epistemic registers are kept strictly apart:

- **Retrospective coverage (this document).** Each analysis classifies judgments reconstructed from an official accident report. Retrospective classification demonstrates that the five-type space is expressive enough to carry the engineering record, and that no engineering failure examined has required a sixth type. It cannot, by construction, demonstrate predictive constraint: the classifier has read the report.
- **Prospective constraint (the preregistered study).** Whether a domain kit fixed in advance correctly constrains transitions in incidents its authors have not read is the subject of a sealed preregistration in the oAOML project (tag prereg-v8). That study, not this ledger, is where the predictive claim is put at risk.

The distinction mirrors the map's own discipline: the map is the coverage demonstration; the inter-rater study is the adversarial test.

A note on audience. This is an evidence artifact, and its method is stated at the resolution an auditor needs to check the classifications, not at the resolution a practitioner needs to apply them in the field. The intervention itself is simple (repair a condition, hold the judgment fixed, observe which of three things happens); the vocabulary around it exists so that every verdict can be traced. A field-facing form of the same discipline would carry the questions and not the taxonomy.

2. Method

The method is aligned with the Universal Fallacy Map, Second Edition: the same frozen criterion, the same root/locus vocabulary, the same refusal to classify what is not regimentation-stable. Alignment matters because the cross-substrate claim (Paper II, Tier 1; Paper III, §4) is only auditable if both substrates are classified the same way.

2.1 Unit of analysis: the judgment, not the incident. An incident is a container, not a classifiable object. What is classified is a judgment: an inference, transition, or license assumed or omitted in design, implementation, operation, or process. One incident may contribute several judgments, each classified separately; this is the engineering form

of the map's dual-analysis convention. An incident's physics is never classified: emergent resonance, crack propagation, and combustion are not fallacies. What is classified is the distinction-making that failed around the physics: the modeling assumption, the validation inference, the state representation, the license assumed for a transition.

2.2 Ground truth. Every factual claim in an analysis is grounded in the official post-mortem investigation of record, cited per entry. Where the record underdetermines the judgment (or where no official investigation exists), the entry says so and the classification is recorded as unresolved rather than forced. Secondary literature may inform the reconstruction but cannot override the report of record. Each entry carries an evidence grade: **A**, an official independent investigation or adjudication of record (agency board, court, regulator, public inquiry); **B**, a peer-reviewed or scholarly reconstruction, used where no unified official record exists or to supplement a flawed one; **C**, an interested-party primary account (a self-investigation, used with that status named); **D**, no unified record (class-level or historical reconstruction). Grades bound what each classification can claim; they do not change the method.

2.3 The classification criterion (frozen; identical to the map's Second Edition).

- **1. Judgment form vs. side condition.** Write the judgment form (the shape of the inferential claim the system or its builders relied on) and list its licensing side conditions separately. No entry is classified before its judgment form is written.
- **2. Three-outcome intervention.** Repair each side condition with the judgment held fixed: inference becomes licensed, that condition is the root; failure persists, it is not the root; the judgment itself disappears, the component is the locus.
- **3. Regimentation stability.** Classify only when the verdict is stable across admissible regimentations. Instability is a finding: the incident narrative covers more than one structural error, and the judgments split.
- **4. Type 4 root reserved for unassignability.** A Type 4 root requires that no legal stratification assignment can make the judgment form well-formed, not merely that a level boundary is crossed.
- **5. Method identity.** A Type 3 classification requires a validation practice that is independently specifiable apart from the inference under audit, with an established warrant it is used outside of (a test regime, a qualification protocol, a geological survey standard, an inspection procedure).
- **6. Dual intervention for compounds.** Where two candidate violations are present, repair each while holding the other fixed; violations that each survive repair of the other are co-roots; where one carries what the other causes, the compound is root/locus.

2.3a Application notes and derived corollaries. The clauses above are the map's Second Edition criterion, unchanged. The following are results of applying it to this corpus, stated here for reference and derived in §4; they are not part of the frozen criterion, so the classifications they summarize cannot be inherited from the criterion's wording.

- **(a) Type 3 subtypes.** Applying clause 5 across the roster separates two forms: **habitat overextension**, a warranted practice applied beyond the envelope its warrant covers (Ariane 5 J2, Millennium Bridge, Patriot J2, Schiaparelli J2, CrowdStrike J2, MCAS J2), and **method displacement**, where a habitat-required practice's role is taken by a different basis. Displacement derives from clause 5, not by enlarging it: the classification is carried by the substituting basis, which must itself be an independently specifiable judgment practice with an established warrant that does not extend to the claim it displaced the habitat-appropriate method for. Engineering judgment is warranted in engineering domains and was extended into geological characterization (St. Francis J1); command authority is warranted for operational decisions and was extended over a hull-stability claim (Vasa J2). The displaced practice does the evidentiary work of showing the habitat boundary was knowable, either performed and overridden (Vasa's halted stability demonstration) or standard-of-practice and omitted (St. Francis's geological investigation); the substitute's warrant mismatch supplies the clause-5 classification. A basis with no warrant anywhere is not Type 3 at all but evidential substitution, exactly the ground on which the map's Second Edition evicted #58 Proof by Assertion; and a bare failure to use the proper test, with no substituting practice identified, remains an omission. Displacement is thus not a second root form but a two-method relational description, required practice and substituting practice, whose root remains overextension, of the substitute. The map's surviving

Type 3 entries carry the same two-method structure with the relation unannotated: each entry names the supplied method and the validation-habitats table names the required one (#47's consensus supplied where observation is required; #48's expertise supplied outside its domain). The corpus's contribution is exposing the relation explicitly where the record names both methods. Guardrail: displacement is not a category for institutional or authority-driven failure generally. It requires (i) a specific, habitat-required practice identifiable in the record, (ii) a substituting basis that is itself an independently warranted practice somewhere, and (iii) the substitution located in a particular judgment. Culture, schedule pressure, and governance dysfunction are causal context for such judgments, never classifications. The exclusion is of diffuse conditions, not of institutional failure: institutional and authority-borne judgments are classified throughout this ledger (Ariane 5 J2's requalification omission, CrowdStrike J2's validator warrant, MCAS J2's certification basis, Vasa J2's command override of a negative stability test, St. Francis J1's substitution of engineering authority for geological investigation, and Piper Alpha J1's permit system itself). A culture is not an inference; the judgments it produces are, and those are where it becomes visible to this method. An organization with a systematic warrant-transport problem appears here as a repeated Type 3 upstream signature across its incidents, which is a stronger finding than a classification of its culture would be.

- **(b) Repair kinds (derived by the intervention across the completed roster).** The successful repair's kind tracks the type. Type 1 repairs by replacement, not licensing: supplying the licensed conversion substitutes the correctly signed claim, and the ill-signed transfer is never licensed (consuming the value as pound-force seconds is not a licensed version of consuming it as newton seconds; it is a different, sound judgment). The side-condition grammar in §4.1, §4.9, and §4.10 is expository; the fallacy audit's corresponding record is that Type 1 entries dissolve. Type 2 splits by whether the operation has a licensed sub-domain: where it does and the restriction is enforceable, a domain-restriction premise confines use to it (Patriot's uptime limit and the 787's power cycle are enforceable restrictions, and both were historically enforced); where the sub-domain exists but no procedure can enforce the restriction, only the operation route is available in practice (Ariane's conversion is legal within the Ariane 4 envelope, but nothing restricts an Ariane 5 mission to it, so the repair was operational); and where the transition type has an empty license, only changing the operation repairs it, and Schiaparelli J1 is the corpus's one such case (no premise licenses consuming a qualified reading as a plain one; the fusion handling must change). The bounded-representation family admits both routes, and the historical record ran both: interim mitigations were the domain-restriction route (Therac's editing restriction, Patriot's reboot guidance, the 787's mandated power cycle, Y2K windowing), while permanent fixes were the operation route (synchronization, rescaled arithmetic, wider representations, four-digit years). Interim mitigation and permanent fix are the two repair strata, named by engineering practice *avant la lettre*. The 787's regulatory record documents the transition between them directly: AD 2015-09-07 mandated the power cycle, and AD 2018-20-15 superseded it with a generator-control-unit software fix, so the move from the domain-restriction route to the operation route is on the record rather than inferred.
- **(c) Repair-identity corollary (clause 6).** Where two candidate violations' repairs coincide, they are one condition, not a compound. First applied at the map's #78 entry (Second Edition note); applied here at Y2K (§4.13).
- **(d) Bounded-representation corollary (clauses 1 and 2).** Every bounded-representation failure in the roster (Therac J2, Ariane 5 J1, Patriot J1, the 787 counter, Y2K) classifies as Type 2 root with Type 4 locus. Each verdict is driven by the intervention alone: in every case a repairable side condition exists and its repair licenses the judgment, and in Y2K's case the repair was actually run, at scale, in history. Clause 4 contributes nothing to these classifications; it only characterizes what would remain for a Type 4 root, and the checkable finding is that nothing in the incident record satisfies it. The derived characterization: a Type 4 root is not using the wrong level; it is failure of legal levelability itself, and whatever merely crosses, truncates, aliases, or represents across levels is an operator-license question whose locus is stratified.

2.4 Role annotations. Beyond type and root/locus, each judgment carries:

- **primary / contributing:** whether the judgment is the precipitating structural failure or a contributor to a failure whose primary structure lies elsewhere (Vasa's unit standards contribute; they do not precipitate).
- **root / consequence:** a violation caused by an upstream failure is classified, but marked as consequence, and the upstream judgment is classified separately (the 2003 blackout operators' lost situational frame is a consequence; the alarm-system failure that caused it is the upstream judgment).

2.5 Type semantics. The five types carry their Second Edition definitions, with the operational readings the oAOML implementation uses for measurement systems:

Type	Name	Operational reading (engineering substrate)
1	Axis Transfer Error	quantity kind or unit changes without licensed conversion
2	Operator Overextension	an operation, command, or representation applied beyond its licensed domain; a qualified reading passed off as the real thing
3	Verification Habitat Mismatch	a value or design relied on where its validation does not transfer; a warranted practice used outside its warrant
4	Stratification Failure	root: no legal level assignment exists, legality being relative to the declared habitat (§2.2) rather than absolute; locus: an abstraction or temporal level carried an operator applied beyond its license
5	Contrast Frame Collapse	a frame-constituting distinction destroyed: represented state vs. actual state, test vs. production, design frame vs. as-built frame

2.6 A checkable structural prediction. The map's Second Edition audit evacuated Type 4 as a root category for fallacies: every reparable level-crossing was Type 2 root with Type 4 locus, and only paradoxes survived as pure Type 4. If the five types are substrate-invariant, the engineering corpus should reproduce this pattern: bounded-representation failures should classify as 2+4 root/locus by the intervention of clauses 1 and 2 alone, and no configuration satisfying clause 4's unassignability requirement should appear in the incident record. That second half is the prediction's genuinely checkable content, since it is the part no clause wording could manufacture. The completed roster bears the prediction out (§2.3a, §4.19); the word confirmed is reserved for the preregistered prospective study, since retrospective coverage cannot confirm a predictive claim (§1).

3. The Ledger

Classification records the final treatment under the §2 criterion; the per-case derivations are in §4.

Incident	Judgment(s) audited	Classification (final)	Role	Grade	Ground truth of record
Mars Climate Orbiter (1999)	Interchange value consumed under the interface-specified unit (§4.1)	Type 1	primary	A	FINAL · NASA Mishap Investigation Board, Phase I Report (1999)
Gimli Glider (1983)	Conversion chain carries target units (§4.9); dispatch judgment unresolved	Type 1	primary	A	FINAL · Lockwood, Board of Inquiry Final Report (1985)

Vasa (1628)	Two judgments (§4.10): unit standards; sailing over the aborted stability test	J1: Type 1 (contributing) · J2: Type 3 (primary among classifiable)	see §4.10	B	FINAL (limited record) · Cederlund & Hocker (2006)
Mizuho Securities / J-Com (2005)	Three judgments (§4.5): acceptance bounds; cancel-state coverage; warning override	J1: Type 2 · J2: Type 2 (severity) · J3: unresolved	primary	A	FINAL · Tokyo High Court judgment (2013), operative; District Court (2009) first instance
Patriot missile, Dhahran (1991)	Two judgments (§4.11): representation over uptime; qualified envelope	J1: Type 2 root, Type 4 locus · J2: Type 3 (upstream)	primary	A	FINAL · GAO/IMTEC-92-26 (1992)
Knight Capital (2012)	Repurposed flag treated as uniformly rebound across the fleet (§4.2)	Type 2	primary	A	FINAL · SEC Exchange Act Release No. 70694 (2013)
Schiaparelli (2016)	Two judgments (§4.7): qualified reading consumed as measurement; envelope warrant	J1: Type 2 · J2: Type 3 (upstream)	primary	A	FINAL · ESA Schiaparelli Anomaly Inquiry, DG-I/2017/546/TTN (2017)
737 MAX MCAS (2018-19)	Two judgments (§4.8): activation authority; single-sensor warrant	Type 2+3 co-roots	primary	A	FINAL · KNKT (2019); JATR (2019); House Final Report (2020)
Ariane 5, Flight 501 (1996)	Two judgments (§4.4): range-licensed conversion; requalification warrant	J1: Type 2 root, Type 4 locus · J2: Type 3 (upstream)	primary	A	FINAL · Lions Inquiry Board Report (1996)
Boeing 787 GCU counter (2015)	Counter representation over continuous-power domain (§4.12)	Type 2 root, Type 4 locus	primary	A	FINAL · FAA AD 2015-09-07
Y2K (2000)	Century-frame condition on two-digit year arithmetic (§4.13); candidate readings collapse by coinciding repairs	Type 2 root, Type 4 locus	class-level	D	FINAL (class-level) · no single report of record
Millennium Bridge (2000)	Code warrant applied outside its validated envelope (§4.14); physics excluded	Type 3	primary	B	FINAL · Dallard et al. (2001)
Therac-25 (1985-87)	Three judgments (§4.3): represented-vs-actual commit;	J1: Type 2 root, Type 5 locus · J2: Type 2 root, Type 4 locus ·	primary	B	FINAL · Leveson & Turner, IEEE

	counter rollover; interlock allocation	J3: contributing, unclassified			Computer (1993)
CrowdStrike (2024)	Two judgments (§4.6): input conformance; validator warrant	J1: Type 2 · J2: Type 3 (upstream)	primary	C	FINAL · CrowdStrike External Technical RCA, Channel File 291 (2024)
Northeast blackout (2003)	Two judgments (§4.15): silent alarm stall; operators' silence inference	J1: Type 2 root, Type 5 locus · J2: consequence (licensed in form)	primary	A	FINAL · Outage Task Force Final Report, Causes and Recommendations (2004)
Hyatt Regency walkway (1981)	Load-path equivalence under the rod substitution (§4.16)	Type 2	primary	A	FINAL · Marshall et al., NBSIR 82-2465 (1982)
St. Francis Dam (1928)	Two judgments (§4.17): foundation warrant; raised-design margin	J1: Type 3 · J2: Type 2 (contributing)	primary	A/B	FINAL · California St. Francis Dam Commission (1928); Rogers (1995)
Piper Alpha (1988)	Two judgments (§4.18): permit-schema frame; handover instance	J1: Type 5 root · J2: contributing	primary	A	FINAL · Cullen Inquiry (1990)

Removed from the seed set: Columbus (not an engineering case with a report of record; fails §2.2).

4. Worked Analyses

The eighteen cases below are complete under the §2 method: factual account from the report of record, judgment form written, criterion applied, classification final. The first four (§4.1 to §4.4) set the template the rest follow.

4.1 Mars Climate Orbiter (1999)

Report of record: Mars Climate Orbiter Mishap Investigation Board, Phase I Report, NASA (1999).

Account. Trajectory correction for the orbiter depended on modeling the small forces produced by angular momentum desaturation events. The ground software file producing that data (SM_FORCES) emitted thruster impulse in pound-force seconds; the navigation software consuming it expected newton seconds, as the Software Interface Specification required. The data was consumed as if metric, understating the modeled impulse by the conversion factor of 4.45. The error accumulated across the cruise, and the spacecraft approached Mars at approximately 57 km altitude instead of the intended capture altitude and was lost. The Board's root cause: failure to use metric units in the coding of the ground software file used in trajectory models.

Judgment form. J: the number in the interchange file is the impulse in the interface-specified unit. Side condition C1: the producing software emits in that unit (a licensed conversion applied at production, or unit identity carried and checked at the boundary).

Intervention. Repairing C1 (emit per the specification, or convert at the boundary) licenses the inference with the judgment intact: C1 is the root. There is no second candidate violation; the transfer across the interface is where the judgment lives, not a separate failed condition. The verdict is stable across regimentations (per-event value transfer or accumulated trajectory model: the same unit-identity condition fails).

Classification. Type 1 (Axis Transfer Error: unit identity assumed without licensed conversion). Primary. The Board's contributing findings (end-to-end verification not performed, navigation anomalies not adequately pursued) are process omissions rather than structural substitutions and are recorded here without classification, per §2.1.

4.2 Knight Capital (2012)

Report of record: U.S. Securities and Exchange Commission, In the Matter of Knight Capital Americas LLC, Release No. 70694 (2013).

Account. The common retelling, that test code ran in production, is not the record. Per the SEC order: Knight's order router (SMARS) retained an obsolete order-handling function, Power Peg, unused since 2003; in 2005 the cumulative-quantity tracking it relied on had been relocated, leaving Power Peg unable to recognize filled orders. For the Retail Liquidity Program launch of August 1, 2012, new code repurposed the flag that had formerly activated Power Peg. The deployment copied the new code to seven of the eight SMARS servers. Orders bearing the repurposed flag that reached the eighth server activated Power Peg, which routed child orders continuously without recognizing fills. In approximately 45 minutes Knight sent millions of orders and sustained losses exceeding 460 million dollars.

Judgment form. J: an order bearing the repurposed flag receives the new RLP handling on any production server. Side condition C1: the flag's binding was rebound uniformly across the production fleet. Side condition C2: the superseded binding (Power Peg) was removed or inert.

Intervention. Repairing C1 (complete the deployment) licenses J outright: no server interprets the flag under the old binding. Repairing C2 alone (delete Power Peg) leaves J unlicensed on the eighth server, though its failure becomes inert rather than catastrophic. Under the three-outcome test, C1 is the root; C2 is a defense-in-depth condition whose absence set the severity, not the violation. Verdict stable: a frame regimentation (test frame vs. production frame) is not admissible on the record, since Power Peg was obsolete production code, not test code; the folklore classification (Type 5 contrast collapse) does not survive §2.2.

Classification. Type 2 (Operator Overextension: a rebound operator symbol applied as if its new binding held beyond the domain where the rebinding had actually been performed). Primary.

4.3 Therac-25 (1985 to 1987)

Report of record: Leveson, N. G., and Turner, C. S., An Investigation of the Therac-25 Accidents, IEEE Computer 26(7) (1993).

Account. Six accidents involving massive radiation overdoses. Two software mechanisms are documented. In the Tyler accidents, an operator who corrected the treatment mode within the roughly eight-second window while the bending magnets were being set could leave the machine in a configuration the entered parameters no longer described: the editing was accepted on screen but not re-processed by the treatment subsystem, and an electron beam could be delivered at X-ray beam current with no target in place, while the console reported a malfunction and a substantial underdose. In the Yakima accident, a one-byte counter in the setup task rolled over to zero on every 256th pass, and on those passes the upper collimator position check was bypassed. The Therac-25 had also removed the hardware interlocks its predecessor carried, leaving enforcement to software.

Judgment forms. The incident contributes three judgments, classified separately per §2.1.

J1 (Tyler): the configuration represented on the console is the configuration of the machine. Side condition C1: every accepted edit is propagated to the treatment subsystem before the represented state is treated as committed. Repairing C1 (re-process edits; synchronize commit with representation) licenses J1 with the represented-vs-actual frame intact: C1 is the root, and the frame that makes the judgment possible is the locus where the violation was carried. Classification: Type 2 root (a commit operation applied beyond its licensed concurrency domain), Type 5 locus (the represented-state vs. actual-state distinction is what collapsed for the operator). Primary.

J2 (Yakima): the setup-complete check holds on every pass. Side condition C2: the flag variable's representation is faithful over its operating domain. Repairing C2 (a set-once flag rather than an incremented one-byte counter) licenses J2 with the check's level structure intact. Classification: Type 2 root (bounded representation incremented beyond its licensed domain), Type 4 locus (the rollover is a representation-level artifact standing in for a state-level fact). Primary.

J3 (interlock removal): a design judgment that software enforcement suffices without hardware interlocks. This is a defense-in-depth allocation whose soundness depends on the software assurance regime; the report treats it as causal context. Recorded as contributing, without forced classification.

4.4 Ariane 5, Flight 501 (1996)

Report of record: Lions, J.-L., et al., Ariane 5 Flight 501 Failure: Report by the Inquiry Board, ESA (1996).

Account. The inertial reference system software was reused from Ariane 4. A horizontal-bias variable derived from horizontal velocity was converted from 64-bit floating point to a 16-bit signed integer without overflow protection; the protection had been deliberately omitted for this variable, justified by range analysis against the Ariane 4 trajectory envelope and a processor workload ceiling. Ariane 5's trajectory produces substantially higher horizontal velocity; about 37 seconds after launch the value exceeded the 16-bit range, the resulting operand error shut down the active and backup inertial systems (identical software, identical failure), diagnostic output was interpreted downstream as flight data, the nozzles deflected fully, and the vehicle broke up and was destroyed. The function computing the value served no purpose after liftoff for Ariane 5; it continued running to satisfy an Ariane 4 hold-and-restart requirement.

Judgment forms. Two judgments, root and upstream cause separated per §2.4.

J1 (conversion): the horizontal-bias value fits the 16-bit representation throughout operation. Side condition C1: the operand's range is bounded by the operative trajectory envelope (established for Ariane 4; never established for Ariane 5). Repairing C1 (range analysis and protection against the actual envelope, or a wider representation) licenses J1 with the float-to-integer level transition intact; deleting the transition leaves nothing to evaluate. Classification: Type 2 root (a representation applied beyond its licensed range domain), Type 4 locus (the representation-level transition carried it). Primary.

J2 (requalification): Ariane 4 qualification warrants Ariane 5 operation. The qualification regime is an independently specifiable validation practice with an established warrant, the Ariane 4 envelope, used outside it. This passes the §2.3.5 method-identity test cleanly. Classification: Type 3 (Verification Habitat Mismatch). Upstream of J1: the requalification omission is why C1 was unmet. The dead-code finding (the function running after liftoff with no Ariane 5 purpose) and the downstream interpretation of diagnostic output as flight data are recorded as contributing and consequence respectively, without forced classification.

4.5 Mizuho Securities / J-Com (2005)

Record: Tokyo High Court judgment of 24 July 2013, Mizuho Securities v. Tokyo Stock Exchange (the operative record; the Tokyo District Court judgment of 4 December 2009 is the first instance, and the Supreme Court of Japan dismissed both parties' final appeals on 3 September 2015). The Tokyo Stock Exchange's 2005-06 handling was never published as a discrete investigation report; see §5.

Account. On J-Com's listing day a Mizuho trader, intending to sell one share at 610,000 yen, entered an order to sell 610,000 shares at 1 yen. The order was roughly forty times the company's outstanding shares. Mizuho's terminal displayed a warning, which the trader overrode. The exchange accepted the order into the book. Mizuho attempted to cancel; the exchange's system failed to process the cancellations in the matching state the order was in, a defect for which the court later assigned the exchange the principal share of liability. Mizuho's loss was approximately 40.7 billion yen.

Judgment forms. The entry error itself, a transposition slip, is not a judgment and is out of scope per §2.1: a typo is not distinction-making. Three judgments remain.

J1 (acceptance): an accepted order lies within the admissible operational domain of the instrument. Side condition C1: admissibility bounds (quantity against outstanding shares, price against reference bands) are enforced at acceptance. Repairing C1 keeps the acceptance judgment intact and refuses the inadmissible order: C1 is the root. Classification: Type 2 (a command accepted beyond the instrument's admissible domain). Primary.

J2 (cancellation): a cancel command issued against a live order is processed. Side condition C2: the cancel operation's licensed domain covers the matching states a live order can occupy. Repairing C2 licenses J2; the defect did not cause the violation in J1 but governed its cost. Classification: Type 2. Role: severity-setting contributor, per the Knight Capital pattern (§4.2).

J3 (override): the displayed warning does not apply to this order. The record does not establish the operator's basis, and the warning-design and override-practice questions are process findings. Recorded as contributing, classification unresolved per §2.2.

4.6 CrowdStrike (2024)

Record: CrowdStrike, External Technical Root Cause Analysis: Channel File 291 (6 August 2024). A self-investigation; no independent review has been released (Grade C, §2.2).

Account. The Falcon sensor's Content Interpreter evaluates template instances delivered as Rapid Response Content. The template type involved declared twenty-one input parameter fields; the integration code supplying inputs provided twenty. The mismatch survived testing because the instances exercised in validation matched the twenty-first field with wildcards. On July 19 an instance using a non-wildcard comparison against the twenty-first field was deployed; the interpreter read past the supplied inputs, an out-of-bounds read in kernel context, crashing approximately 8.5 million Windows hosts. The root was a schema/arity mismatch, not content becoming executable code.

Judgment forms.

J1 (conformance): a template instance's parameter references are satisfied by the inputs the integration supplies. Side condition C1: declared parameter count equals supplied input count, checked at the boundary. Repairing C1 licenses J1 with the interpretation judgment intact: C1 is the root. Classification: Type 2 (an interpretation operation applied beyond the domain its supplied inputs licensed). Primary.

J2 (validation warrant): a Content Validator pass warrants fleet deployment. The validator is an independently specifiable practice with an established warrant that did not extend to non-wildcard use of the twenty-first field; the deployment relied on it outside that warrant. Classification: Type 3. Upstream of J1, per the Ariane 5 pattern (§4.4): the warrant gap is why C1 was unmet in production. The absence of staged rollout for this content channel is recorded as contributing, without forced classification.

4.7 Schiaparelli (2016)

Record: T. Tolker-Nielsen, ESA Inspector General, EXOMARS 2016: Schiaparelli Anomaly Inquiry, ref. DG-I/2017/546/TTN (18 May 2017).

Account. During parachute descent the vehicle oscillated more strongly than the modeled envelope anticipated. The inertial measurement unit's pitch-rate measurement saturated and was flagged; the flag persisted for the maximum configured persistence time, and during that window the guidance software continued to integrate the saturated value into its attitude estimate. The corrupted estimate placed the vehicle's computed altitude below ground level; the descent sequence responded as designed to the estimate, releasing the parachute early and terminating thrust, and the lander fell approximately 3.7 km to impact.

Judgment forms.

J1 (fusion): the pitch-rate reading is admissible input to the attitude estimator. Side condition C1: a reading carrying the saturation qualifier is excluded or bounded, not integrated as a measurement. The saturated reading is a qualified value; consuming it as a plain measurement is the substitution the architecture prohibits (a qualified reading passed off as the real thing, §2.5, Type 2): the general schema $M[A] \rightarrow A$ of the map's meta-axis substitution family in avionics dress, a qualified reading discharged without license in oAOML's vocabulary. Repairing C1 licenses J1 and the descent sequence downstream of it: C1 is the root. The repair is operator-shaped: no admissible premise licenses the qualified-to-plain transition (denying the saturation changes the case; independent evidence of the true rate bypasses the transition), so the fusion handling itself must change, which makes this the roster's one Type 2 case repairable only by changing the operation (§2.3a, repair kinds). Classification: Type 2. Primary. The premature release and thrust cutoff are consequences: the sequence performed correctly against a corrupted estimate.

J2 (envelope warrant): the modeled parachute-dynamics envelope warrants the saturation-handling design. The modeling and verification regime is an independently specifiable practice whose warrant did not cover the actual oscillation regime; the persistence-time setting was designed inside that under-scoped warrant. Classification: Type 3. Upstream of J1.

4.8 737 MAX MCAS (2018 to 2019)

Record: Indonesian KNKT Final Report on Lion Air 610 (2019); Joint Authorities Technical Review, Boeing 737 MAX Flight Control System (2019); U.S. House Committee on Transportation and Infrastructure, Final Report (2020).

Account. MCAS commanded nose-down stabilizer trim from a single angle-of-attack sensor per flight. During development its authority was enlarged from the originally analyzed increment to a substantially larger one at low speed, and it could activate repeatedly as long as the triggering sensor reading persisted; the certification safety analysis reflected the earlier, smaller authority and assumed prompt crew response under the runaway-trim procedure. Erroneous high angle-of-attack values from a single failed sensor produced repeated full-increment activations on both accident flights.

Judgment forms. Two candidate violations; dual intervention per §2.3.6.

J1 (authority): each activation lies within the licensed control authority. Side condition C1: the commanded increment and its repeatability match the envelope the design justification analyzed. Repairing C1 (the original limited, non-repeating authority) leaves erroneous single-sensor activations occurring but within a survivable envelope: the violation in J2 survives the repair of C1.

J2 (sensor warrant): one sensor's reading warrants activation. Side condition C2: the evidence basis matches the hazard level of the command it licenses (voted or cross-checked input for a command of this authority). Repairing C2 (dual-sensor comparison) prevents the erroneous activations, but the enlarged, repeatable authority remains outside its analyzed envelope: the violation in J1 survives the repair of C2.

Each violation survives repair of the other: co-roots. Classification: Type 2+3 co-roots (operator authority beyond its analyzed license; a validation basis used outside the warrant appropriate to the command). Primary. The certification-process finding, that the safety analysis was not re-run as the authority grew, is the temporal face of J2's

warrant gap and is recorded with it. This is the ledger's first co-root compound: unlike the upstream Type 3 judgments of Ariane 5, CrowdStrike, and Schiaparelli, neither violation here merely explains the other. Adversarial note: two rival regimentations are rejected on the record. Treating J2 as sole root with the authority as a severity-setter fails because repairing C2 leaves J1's violation standing (the dual intervention above); collapsing the two judgments into one fails regimentation stability, since the two side conditions repair independently.

4.9 Gimli Glider (1983)

Record: G. H. Lockwood, Commissioner, Final Report of the Board of Inquiry (April 1985), a one-member inquiry constituted under section 8 of the Aeronautics Act and distinct from the Canadian Aviation Safety Board.

Account. With the fuel-quantity processor inoperative, the fuel load for Air Canada Flight 143 was established manually: dripstick readings in centimeters, converted to liters, then to mass by a specific-gravity factor. The factor applied (1.77) yields pounds per liter; the 767 was the airline's first aircraft fueled in kilograms. The computed figure was treated as kilograms, loading roughly half the required fuel. Both engines flamed out at altitude; the aircraft glided to a landing at Gimli.

Judgment form. J: the computed fuel mass is in kilograms. Side condition C1: every factor in the conversion chain carries the unit of its target quantity (a licensed chain, stated link by link, per the roster's original caution). Repairing C1 licenses J with the chain intact: C1 is the root. Classification: Type 1 (the manual, procedural form of the Mars Climate Orbiter violation: unit identity assumed without licensed conversion). Primary. The dispatch judgment under the minimum-equipment provisions with inoperative gauges is recorded as contributing, classification unresolved: the Board's findings there concern procedures and communication rather than a single stable judgment form.

4.10 Vasa (1628)

Record: No modern report of record exists; the analysis rests on archaeological and archival scholarship (Cederlund & Hocker, Vasa I, 2006) and is marked limited-record per §2.2.

Account. The ship capsized in harbor on her maiden voyage in a light gust, with insufficient stability for her high superstructure. Two findings carry structural judgments. Rulers recovered from the wreck are calibrated in different foot standards (Swedish and Amsterdam feet), consistent with the documented hull asymmetry as a contributing factor. And before sailing, a stability demonstration (thirty men running abeam) was halted after three crossings because the ship threatened to capsize; she was sailed anyway.

Judgment forms. J1 (units): members dimensioned under one foot standard compose with members dimensioned under another. Side condition: a common standard or licensed conversion. Type 1, contributing: the asymmetry contribution is plausible on the archaeological evidence but cannot be established as precipitating, and the entry does not overclaim it. J2 (sailing decision): the ship is fit to sail. The claim's habitat required the stability demonstration, an independently specifiable practice whose verdict was negative; the decision substituted command authority for the test's verdict. Classification: Type 3, displacement subtype (§2.3a): command authority is itself a warranted judgment practice for operational decisions, and its warrant does not extend to hull stability; the halted demonstration shows the habitat boundary was knowable. Primary among the classifiable judgments; the underlying stability design shortfall is not classifiable as a judgment on the surviving record.

4.11 Patriot Missile, Dhahran (1991)

Record: GAO/IMTEC-92-26, Patriot Missile Defense: Software Problem Led to System Failure at Dhahran (1992).

Account. The range-gate calculation used time since boot, accumulated in tenths of seconds under a 24-bit fixed-point representation; one-tenth has a non-terminating binary expansion, so truncation error grew with uptime. After roughly 100 hours of continuous operation the clock error reached about a third of a second, displacing the range gate by hundreds of meters at Scud closing velocity. The incoming missile was not tracked; 28 soldiers died. The system had been qualified around short mobile deployments; a software fix arrived the day after the attack.

Judgment forms. J1 (representation): the time value used in range-gate prediction is accurate over the operational uptime domain. Side condition C1: representation error bounded over the actual deployment's uptime. Repairing C1 (the fix; consistent conversion) licenses J1 with the temporal accumulation structure intact: Type 2 root, Type 4 locus (temporal). Primary. J2 (envelope): continuous fixed-site operation lies within the qualified envelope. The qualification regime's warrant covered short cycles; the deployment ran outside it. Classification: Type 3, upstream of J1, the fourth instance of the outrun-validation-regime signature (§4.19).

4.12 Boeing 787 Generator Control Units (2015)

Record: FAA Airworthiness Directive 2015-09-07 (Amendment 39-18153, 80 FR 24789, 1 May 2015); superseded by AD 2018-20-15 (2018), which replaced the mandated power cycle with a software fix.

Account. All four generator control units could simultaneously enter failsafe if powered continuously for 248 days, from an internal counter overflow, with total loss of AC electrical power as the identified hazard. The directive's interim remedy was a periodic power cycle.

Judgment form. J: the counter's representation is faithful over the continuous-power domain. Side condition C1: representation width covers the domain, or the domain is bounded by procedure. Both repairs license J (the software fix; the mandated power cycle), with the temporal structure intact: Type 2 root, Type 4 locus (temporal). Primary. Structurally identical to Patriot's J1 and Therac's J2: the bounded-representation family.

4.13 Y2K (2000)

Record: No single report of record; a failure class, largely averted, not an incident. Classified at the level of the judgment form per §2.2.

Judgment form. J: year arithmetic on two-digit fields is valid. Side condition C1: the operands share a century frame. Two readings were anticipated in the roster: a truncated representation applied beyond its licensed temporal domain (Type 2 root, Type 4 locus), and a corrupted temporal reference frame (a Type 5 flavor). The dual intervention dissolves the choice: the frame repair and the license repair are the same act, since declaring the century frame (windowing, pivot dates, four-digit expansion) is exactly what supplies the missing license. Coinciding repairs mean one condition, the repair-identity corollary of clause 6 (§2.3a), first applied at the map's #78 entry note (Second Edition). Classification: Type 2 root, Type 4 locus (temporal). Y2K is also the roster's unique case in which the three-outcome intervention was run in reality and at scale: the remediation campaign supplied the missing side condition in advance, and the licensed inference then held. The repair confirming the root is not hypothetical here; it is history. Adversarial note: the rival position, that a mostly averted failure class admits no classification, is answered by the class-level marking: what is classified is the judgment form, not an incident, and the executed remediation supplies the intervention outcome the criterion requires. The grade-D evidence status (§2.2) bounds the claim accordingly.

4.14 London Millennium Bridge (2000)

Record: Dallard et al., The London Millennium Footbridge, The Structural Engineer 79(22) (2001).

Account. On opening day the bridge developed large lateral sway under crowd loading: pedestrians synchronize their gait to small lateral motions, feeding energy back into the structure. The design complied with the applicable code, whose dynamic loading provisions addressed vertical excitation; synchronous lateral excitation lay outside what the code's validation history covered. The physics is excluded per §2.1; the audited judgment is the inference that code compliance warranted serviceability.

Judgment form. J: the code-specified dynamic load model warrants this design's serviceability. Side condition C1: the structure lies within the envelope the code's validation covers. The code is an independently specifiable practice with an established warrant, used beyond it: the method-identity clause passes cleanly. Classification: Type 3. Primary. This is the ledger's first pure Type 3 primary, as distinct from the upstream Type 3 judgments: here the outrun warrant is not behind another violation; it is the violation.

4.15 Northeast Blackout (2003)

Record: U.S.-Canada Power System Outage Task Force, Final Report on the August 14, 2003 Blackout in the United States and Canada: Causes and Recommendations (April 2004). The task force's November 2003 Interim Report is not relied on.

Account. The control-room alarm processor at FirstEnergy stalled in a race condition and failed silently: no alarms were delivered, and no indication of the failure was presented. Operators, seeing a quiet board, inferred a quiet system while contact-initiated line trips accumulated; without situational awareness, load was not shed, and the cascade spread across eight states and Ontario.

Judgment forms. J1 (alarm system): the alarm processor delivers every alarm or announces its own failure. Side condition C1: the pipeline's concurrency domain is covered, and failure is annunciated. Repairing C1 licenses J1; the live-monitoring frame, the represented-state vs. actual-state distinction the control room runs on, is where the violation was carried. Classification: Type 2 root (an operation beyond its licensed concurrency domain), Type 5 locus (the monitoring frame silently ceased to track reality). Primary. Structurally the Therac-25 J1 pattern at control-room scale.

J2 (operators): no alarms, therefore no events. This inference has the argument-from-silence form, and its side condition, a live detection channel (the map's #50 detection-expectation premise), was reasonable to assume and false because of J1. The operators' judgment was licensed in form and defeated by an upstream violation: recorded as consequence, not classified as an error. The structural failure was in the machine, not the operators. J2 is the converse of the map's #32 (Argument from Fallacy): #32 prohibits inferring a conclusion's falsity from an argument's unlicensed status, and J2 exhibits a false conclusion issuing from a fully licensed inference. Between them, the two independence directions of the false/invalid/unlicensed triple are now empirically exhibited, one in each substrate. Other findings (vegetation management, the regional state estimator) are recorded as contributing, unclassified.

4.16 Hyatt Regency Walkways (1981)

Record: Marshall et al., NBS Building Science Series (NBSIR 82-2465), Investigation of the Kansas City Hyatt Regency Walkways Collapse (1982).

Account. The approved design hung both walkways on continuous rods, each box beam carrying its own load. The as-built change substituted two rod sets, with the fourth-floor box-beam connection now carrying both walkways: the connection load doubled. The investigation found the original connection already below code capacity, and the revised one at roughly half of that. One hundred fourteen people died.

Judgment form. J: the revised connection preserves the load-bearing relation of the approved design. Side condition C1: load-path equivalence established under the substitution. Repairing C1, performing the equivalence check, refuses the substitution and forces a compliant connection; J then holds of the corrected design. Classification:

Type 2 (a composition substituted under an assumed equivalence without license: the engineering face of an unpreserved-composition error, where the preservation condition on the changed composition was never established). Primary. The review-and-seal process findings are omissions, recorded as contributing without classification.

4.17 St. Francis Dam (1928)

Record: Report of the California St. Francis Dam Commission (24 March 1928), supplemented by the modern forensic reanalysis (Rogers, 1995, Southern California Quarterly 77(1-2)), which corrected parts of the contemporary geology; both are cited per §2.2. Distinct from the separately issued Los Angeles City Council committee report.

Account. The dam failed at midnight, killing more than four hundred people. The left abutment stood on an ancient landslide mass that reactivated; the right abutment conglomerate weakened when saturated. Site geology was assessed by engineering authority rather than by geological investigation, and the dam was raised twice during construction without widening the base.

Judgment forms. J1 (foundation warrant): the foundation rock warrants the design. The claim's habitat required geological investigation, an independently specifiable practice available and in use elsewhere at the time; the validation actually supplied was engineering judgment, itself a warranted practice in engineering domains whose warrant does not extend to geological characterization. Classification: Type 3, displacement subtype (§2.3a). Primary. J2 (raising): the raised design retains the approved stability margin. Side condition: margin re-established under the modification, the Hyatt condition. Not performed. Classification: Type 2, contributing: on the record the foundation, not the margin, precipitated the failure. Adversarial note: two rival readings are rejected. The raising judgment as primary fails on the record (the foundation precipitated); and omission-rather-than-displacement fails the §2.3a guard from the other side: geological investigation was the standard practice of the era, engineering judgment is itself a warranted practice extended beyond its domain, and the substitution is located in a specific foundation-adequacy judgment. The 1928 record's own geological errors are why the modern reanalysis is co-cited (grade A/B, §2.2).

4.18 Piper Alpha (1988)

Record: The Public Inquiry into the Piper Alpha Disaster (Cullen, 1990).

Account. A condensate pump's pressure safety valve was removed for maintenance and the line blanked with a hand-tightened flange, under one permit; the pump's own overhaul was under another. At shift handover the valve-removal permit was not connected to the pump permit. When the running pump tripped that night, the control room, finding only the untouched pump permit, judged the pump available and started it. Condensate escaped at the blank flange; the explosion and escalating fire killed 167.

Judgment forms. Two readings present themselves, and unlike Y2K they do not coincide, so the entry splits per the criterion's clause 3.

J1 (system): the permit-to-work system's representation of equipment state corresponds to physical state. The Cullen Inquiry's findings are about the frame itself: the permit system had no designed cross-referencing between permits on connected equipment, no display of suspended permits, and handover procedures that could not carry the dependency. The representation's designed state-space could not express that this pump's operability depended on that removed valve. That is a mis-specified frame, not an operation outrunning a sound one. The rival regimentation, Type 2 root with Type 5 locus on the Therac and blackout pattern, requires a frame capable of representing the state that an operation then outran; the Cullen findings deny the capability: no cross-referencing mechanism existed between permits on connected equipment, and suspended permits were not displayed, so the schema lacked expressive capacity for the dependency. Under the three-outcome test, repairing the night's execution while holding the frame fixed does not license the restart judgment, because the record consulted would still not represent the dependency; repairing the frame does.

Classification: Type 5 root (the frame-constituting distinction, represented operability vs. actual configuration, was structurally unable to be maintained). Primary. This is the

roster's one confirmed Type 5 root, and it is the cleanest: the restart judgment that night was validated by exactly the method the frame prescribes, and the frame was wrong.

J2 (instance): that night's handover communication. Under J1 this is the occasion, not the root: no handover practice could reliably carry a dependency the permit schema could not represent. Recorded as contributing.

4.19 What the Ledger Shows

The roster is complete: eighteen incidents, thirty-two judgments audited, of which twenty-seven received type assignments and five were audited without one (three recorded as unresolved or contributing without a stable judgment form, one as an occasion under a system-level root, and one as a licensed-in-form inference defeated from upstream). The counts, exposed for inspection:

Result	Count
Type 1 root	3 (2 primary, 1 contributing)
Type 2 root	15
Type 3 root	8 (4 upstream, 2 displacement, 1 overextension primary, 1 co-root)
Type 4 root	0
Type 5 root	1
Type 4 locus	5
Type 5 locus	2
Co-root compounds	1 (MCAS)
Audited, no type assigned	5

Six results.

- 1. **The §2.6 prediction is borne out in the completed roster.** No pure Type 4 root appears anywhere in the engineering corpus. All five bounded-representation failures (Therac's counter, Ariane 5, Patriot, the 787 counter, Y2K) classify as Type 2 root with Type 4 locus, reproducing in engineering post-mortems the pattern the map's Second Edition audit found in the fallacy inventory. The substrate changed; the structure did not. Confirmation in the predictive sense is reserved for the preregistered prospective study (§1).

The emptiness has a mechanism, and it is the map's mechanism. For fallacies, a fallacy presupposes a well-formed judgment, so unassignability presents as paradox, exhibited by the map's witnesses W1 to W3. In engineering, genuine unassignability is a property of the specification and model space: no implementation can satisfy the complete judgment over the stipulated domain. Implementations of such specifications can be built and even deployed; what cannot exist is one meeting the whole

guarantee, which is why the configuration characteristically surfaces as an impossibility result rather than as an operational accident. Exhibited engineering witnesses, mirroring the map's:

Witness	Case	Structure	Status
E1	Asynchronous deterministic consensus	No deterministic protocol satisfies the full consensus guarantee over every admissible run of the asynchronous model with one faulty process: the complete protocol judgment admits no legal assignment over the stipulated domain (Fischer, Lynch & Paterson, 1985)	Impossibility result, not an incident
E2	Total halting decision	No total computable procedure decides the termination property over all programs and inputs: the complete decision judgment admits no legal assignment (Turing, 1936)	Impossibility result, not an incident

Fallacy is to paradox as operational violation is to impossibility result: in both substrates the Type 4 row of the deployed record is empty for the same structural reason, that genuine unassignability lives in the specification space, where it presents as proof, while everything that fails in operation turns out to be a repairable license carried at a stratified locus. This is where genuine Type 4 goes in engineering: not into rollover bugs and abstraction leaks, but into specifications that cannot be jointly satisfied. The empty incident cell is structurally intelligible, not merely zero. Stated with full caution, the intelligibility cuts the claim's strength: given the mechanism and the premise that executed judgments presuppose deployable well-formedness, the execution-level zero functions as a consistency check passed rather than an independent confirmation. The genuinely empirical cell is the design-level record: whether any deployed system's adopted specification was jointly unsatisfiable in the Type 4 sense, and the falsifier aims there. One formal obligation is recorded rather than assumed: showing that these impossibility results are failures of legal levelability specifically, and not impossible specification generally, requires representing each as unsatisfiable level constraints. Until that bridge is supplied, E1 and E2 stand as candidate architectural correspondences to the map's witnesses rather than established Type 4 instances. The obligation is scoped, and the scope matters: it bears on the formal status of E1 and E2, which stand outside the classified roster, and on no classification within it. The twenty-seven type assignments were driven by intervention on the record (§2.3), and not one of them cites an impossibility result; the roster's verdicts therefore do not move with how the bridge resolves. What the bridge would settle is whether the mechanism proposed here for the empty cell is the right one, not whether the cell is empty. The prediction is borne out in pattern; the mechanism offered for it, that unassignability lives in specification space, is proposed with its formal statement open.

- **2. A recurring cross-domain signature.** Four cases from four unrelated domains (Ariane 5, Schiaparelli, CrowdStrike, Patriot) share one structure: an unlicensed operation downstream of an outrun validation regime, Type 2 primary with Type 3 upstream. The signature spans 1991 to 2024, rocketry to endpoint security.
- **3. The criterion discriminates.** MCAS is a genuine co-root compound; the four signature cases are root-plus-upstream; Therac and the blackout are root/locus; Y2K's two candidate readings collapse into one condition by coinciding repairs. Four different compound structures, separated mechanically by the dual intervention. The apparatus does not merely sort failures into five buckets; it distinguishes different internal causal arrangements involving the same buckets.
- **4. Ground truth changes verdicts.** Knight Capital and CrowdStrike both lose their folklore classifications on their records; Vasa's popular unit-standards story survives only as a contributing factor; the blackout's operators are exonerated (their inference was licensed in form and defeated from upstream). A framework that changes its

answer when exposed to better evidence is doing more epistemic work than one that redescribes familiar stories, and this is the working answer to the objection that any accident can be reinterpreted to fit five broad categories: the method sometimes refuses the interpretation everyone expected. The defeated-but-licensed category generalizes beyond engineering: a false conclusion does not imply a fallacious inference, because the violation can reside in the provenance of a premise rather than in the reasoning that consumed it.

- **5. The Type 2/5 boundary, exhibited.** The corpus yields the cleanest statement of the boundary anywhere in the program. Type 2: the frame can represent the relevant distinction, but an operation exceeds its license. Type 5: the frame itself cannot preserve the distinction the judgment requires. Therac J1 and the blackout carry Type 5 loci with Type 2 roots (frames capable of tracking actual state, outrun by unlicensed operations); Piper Alpha is a Type 5 root because its permit schema could not express the dependency at all, so no better execution within the frame could have repaired it.
- **6. The distribution is not the map's.** This corpus is dominated by Type 2 roots with exactly one Type 5 root and two Type 1 primaries, where the fallacy inventory spreads far more evenly. A hypothesis the corpus generates (and cannot itself establish): engineered systems concentrate their distinction-making in compositions and licenses, while rhetoric concentrates in axes and frames. The result is consistent with substrate-invariant types whose observed distributions differ by substrate; these eighteen canonical incidents are not a representative sample of engineering failure, so population base rates would require a sampling design suited to that question. The stronger invariance conclusion belongs to Papers II and III, argued on both substrates together.

A closing observation the corpus earns rather than asserts. In engineering dress the five types read: identity of the quantity lost across transfer (Type 1); the operator's licensed domain exceeded (Type 2); the warrant not traveling to the current habitat, or displaced (Type 3); the level structure required for the judgment not legally maintainable (Type 4); the contrast space required to state the judgment collapsed (Type 5). Quantity, operator, warrant, level, frame: engineering systems externalize these into units, interfaces, ranges, counters, schemas, qualification regimes, and permits, which is why the distinctions are visible here as machinery. Read this way, the five violation types are the failure modes of distinction-preserving composition: identity, domain, warrant, stratification, and frame. That formulation belongs to Paper III's argument; this ledger's contribution is that independently documented engineering judgments instantiate the same structural roles under the previously frozen criterion.

5. References of Record (worked cases)

Every source below was resolved and verified on 15 August 2026. Conventions: the agency reference number or DOI is given wherever one exists, because those survive link rot when URLs do not; an archive link is given where the official host is fragile; and an access note appears wherever a source of record is not freely retrievable, since a Grade A record behind a paywall bounds what a reader can independently check.

Mars Climate Orbiter Mishap Investigation Board (1999). *Phase I Report*, 10 November 1999 (chair: A. G. Stephenson). NASA. No DOI and no NTRS record exists; the original NASA distribution point is dead. https://llis.nasa.gov/llis_lib/pdf/1009464main1_0641-mr.pdf · archive: https://web.archive.org/web/20201202235651/https://llis.nasa.gov/llis_lib/pdf/1009464main1_0641-mr.pdf Freely downloadable. Not to be confused with the Phase II report on project management (13 March 2000).

U.S. Securities and Exchange Commission (2013). *In the Matter of Knight Capital Americas LLC*. Securities Exchange Act of 1934 Release No. 70694, Administrative Proceeding File No. 3-15570, 16 October 2013. <https://www.sec.gov/files/litigation/admin/2013/34-70694.pdf> · archive: <https://web.archive.org/web/20230902010556/https://www.sec.gov/files/litigation/admin/2013/34-70694.pdf> Freely downloadable.

Leveson, N. G., & Turner, C. S. (1993). An investigation of the Therac-25 accidents. *Computer* (IEEE Computer Society), 26(7), 18-41. DOI 10.1109/MC.1993.274940. Paywalled at the publisher; authoritative open copies at https://web.mit.edu/6.033/2004/wwwdocs/papers/Therac_1.html and <https://escholarship.org/uc/item/5dr206s3>

Ariane 5 Flight 501 Inquiry Board (1996). *Ariane 5: Flight 501 Failure. Report by the Inquiry Board*, Paris, 19 July 1996 (chairman: J.-L. Lions). The Board was constituted jointly by the Director General of ESA and the Chairman of CNES; ESA is publisher, not author. <https://esamultimedia.esa.int/docs/esa-x-1819eng.pdf> · archive: <https://web.archive.org/web/20260803170012/https://esamultimedia.esa.int/docs/esa-x-1819eng.pdf> Freely downloadable, but a scanned image PDF with no text layer; a text-bearing unofficial mirror is at <http://sunnyday.mit.edu/nasa-class/Ariane5-report.html>

Tokyo High Court (2013). Judgment of 24 July 2013, *Mizuho Securities v. Tokyo Stock Exchange*. This is the operative record: the Tokyo District Court judgment of 4 December 2009 is the first instance (apportioning 70 percent to the exchange), and on 3 September 2015 the Supreme Court of Japan (First Petty Bench) dismissed both parties' final appeals, at which point the High Court judgment became final. No official English text of any of the three decisions exists; the judgments appear in Japanese commercial reporters (for the first instance: 判例時報 2072 号 54 頁; 判例タイムズ 1322 号 149 頁; 金融・商事判例 1330 号 16 頁), which are subscription or print only. The freely available official-party record of the outcome is the JPX/TSE English notice (expressly not an official translation): https://www.jpx.co.jp/english/corporate/news-releases/0063/b5b4pj000000pr1b-att/20150904_E.pdf The Tokyo Stock Exchange's 2005-06 handling was never published as a discrete investigation report; the nearest official-body records are the TSE rule-making notice of 22 March 2006 (<https://www.jpx.co.jp/rules-participants/public-comment/detail/060322.html>) and the JSDA working-group final report of 14 November 2006.

CrowdStrike (2024). *External Technical Root Cause Analysis: Channel File 291*, 6 August 2024. <https://www.crowdstrike.com/wp-content/uploads/2024/08/Channel-File-291-Incident-Root-Cause-Analysis-08.06.2024.pdf> Freely downloadable. "External" denotes publication for external audiences, not independent authorship: the analysis is CrowdStrike's own, and although third-party reviews were commissioned, none has been released, so no independent assessment exists to cite alongside it. This is the basis of the entry's Grade C.

Tolker-Nielsen, T. (2017). *EXOMARS 2016: Schiaparelli Anomaly Inquiry*. ESA Inspector General, ref. DG-I/2017/546/TTN, Issue 1 Rev 0, 18 May 2017. https://sci.esa.int/documents/33431/35950/1567260317467-ESA_ExoMars_2016_Schiaparelli_Anomaly_Inquiry.pdf · archive: https://web.archive.org/web/20260316001008/https://sci.esa.int/documents/33431/35950/1567260317467-ESA_ExoMars_2016_Schiaparelli_Anomaly_Inquiry.pdf Freely downloadable.

Komite Nasional Keselamatan Transportasi (2019). *Aircraft Accident Investigation Report: PT. Lion Mentari Airlines, Boeing 737-8 (MAX), PK-LQP, Tanjung Karawang, West Java, 29 October 2018*. Report KNKT.18.10.35.04, released 25 October 2019. <https://knkt.go.id/Repo/Files/Laporan/Penerbangan/2018/KNKT.18.10.33.04-Final-Report.pdf> · archive: <https://web.archive.org/web/20250807030417/https://knkt.go.id/Repo/Files/Laporan/Penerbangan/2018/KNKT.18.10.33.04-Final-Report.pdf> Freely downloadable. Note the repository filename (33.04) disagrees with the report number on the title page (35.04); the title-page number is correct and the URL must not be "corrected" to match it.

Joint Authorities Technical Review (2019). *Boeing 737 MAX Flight Control System: Observations, Findings, and Recommendations*, 11 October 2019 (chair: C. A. Hart). Submitted to the Associate Administrator for Aviation Safety, U.S. Federal Aviation Administration; the JATR was an independent multi-national team and the FAA is its recipient and host, not its author. https://www.faa.gov/sites/faa.gov/files/2021-08/Final_JATR_Submittal_to_FAA_Oct_2019.pdf · archive: https://web.archive.org/web/20260212051532/https://www.faa.gov/sites/faa.gov/files/2021-08/Final_JATR_Submittal_to_FAA_Oct_2019.pdf Freely downloadable.

Majority Staff, U.S. House Committee on Transportation and Infrastructure (2020). *Final Committee Report: The Design, Development & Certification of the Boeing 737 MAX*, September 2020 (released 16 September 2020). A majority-staff report, not an adopted committee-wide report. Cited from the GPO permanent copy (SuDoc Y 4.T 68/2:B 63/2): https://www.govinfo.gov/content/pkg/GOVPUB-Y4_T68_2-PURL-gpo144993/pdf/GOVPUB-Y4_T68_2-PURL-gpo144993.pdf · committee posting: <https://democrats-transportation.house.gov/imo/media/doc/2020.09.15%20FINAL%20737%20MAX%20Report%20for%20Public%20Release.pdf> · archive:

<https://web.archive.org/web/20260815165244/https://democrats->

[transportation.house.gov/imo/media/doc/2020.09.15%20FINAL%20737%20MAX%20Report%20for%20Public%20Release.pdf](https://www.transportation.house.gov/imo/media/doc/2020.09.15%20FINAL%20737%20MAX%20Report%20for%20Public%20Release.pdf) Freely downloadable. The committee posting sits on a minority-party domain whose contents move when House control changes, which is why the GPO copy is cited first.

Lockwood, G. H., Commissioner (1985). *Final Report of the Board of Inquiry Investigating the Circumstances of an Accident Involving the Air Canada Boeing 767 Aircraft C-GAUN That Effected an Emergency Landing at Gimli, Manitoba, on the 23rd Day of July, 1983*, April 1985. Ottawa: Minister of Supply and Services Canada. Cat. No. T22-64/1985E, ISBN 0-660-11884-X. A one-member Board of Inquiry constituted by Order-in-Council under section 8 of the Aeronautics Act, distinct from the Canadian Aviation Safety Board. <http://data2.collectionscanada.gc.ca/e/e444/e011083519.pdf> · archive: <https://web.archive.org/web/20260103090856/http://data2.collectionscanada.gc.ca/e/e444/e011083519.pdf> Freely downloadable; the Library and Archives Canada host is HTTP-only legacy infrastructure, so the archive link is not optional.

Cederlund, C. O. (2006). *Vasa I: The Archaeology of a Swedish Warship of 1628*. F. Hocker (ed.). Stockholm: National Maritime Museums of Sweden. ISBN 978-91-974659-0-8. <https://lccn.loc.gov/2007272563> Print only.

U.S. General Accounting Office (1992). *Patriot Missile Defense: Software Problem Led to System Failure at Dhahran, Saudi Arabia*. GAO/IMTEC-92-26, issued 4 February 1992, released 27 February 1992. <https://www.gao.gov/products/imtec-92-26> (PDF: <https://www.gao.gov/assets/imtec-92-26.pdf>) Freely downloadable. The issuing body's 1992 name is retained; the agency was renamed the Government Accountability Office in 2004.

Federal Aviation Administration (2015). *Airworthiness Directives: The Boeing Company Airplanes*. AD 2015-09-07, Amendment 39-18153, Docket No. FAA-2015-0936, 80 FR 24789, 1 May 2015. <https://www.govinfo.gov/content/pkg/FR-2015-05-01/pdf/2015-10066.pdf> (record: <https://www.govinfo.gov/app/details/FR-2015-05-01/2015-10066>) Freely downloadable. "2015-09-07" is an AD sequence number, not a date. Superseded by AD 2018-20-15 (Amendment 39-19449, effective 20 November 2018), which replaced the repetitive power-cycling task with a generator-control-unit software fix; 2015-09-07 remains the primary source for the counter overflow, and the supersession is itself evidence for the two repair routes (§2.3a-b).

Dallard, P., Fitzpatrick, A. J., Flint, A., Le Bourva, S., Low, A., Ridsdill Smith, R. M., & Willford, M. (2001). The London Millennium Footbridge. *The Structural Engineer*, 79(22), 17-33. [https://www.istructe.org/journal/volumes/volume-79-\(published-in-2001\)/issue-22/the-london-millennium-footbridge/](https://www.istructe.org/journal/volumes/volume-79-(published-in-2001)/issue-22/the-london-millennium-footbridge/) No DOI (the institution did not register DOIs for 2001 content). Members-only at the publisher; an open copy is at <https://researchcourse.pbworks.com/f/structural+engineering.pdf> Note that some secondary databases give the page range as 17-21; 17-33 is the range used in the scholarly literature.

U.S.-Canada Power System Outage Task Force (2004). *Final Report on the August 14, 2003 Blackout in the United States and Canada: Causes and Recommendations*, April 2004. <https://www.energy.gov/sites/prod/files/oeprod/DocumentsandMedia/BlackoutFinal-Web.pdf> · archive: <https://web.archive.org/web/20201223113211/https://www.energy.gov/sites/prod/files/oeprod/DocumentsandMedia/BlackoutFinal-Web.pdf> Freely downloadable; the archive link is recommended because the host path is a legacy upload directory. Distinct from the same task force's Interim Report (November 2003), which is not cited here.

Marshall, R. D., Pfrang, E. O., Leyendecker, E. V., Woodward, K. A., Reed, R. P., Kasen, M. B., & Shives, T. R. (1982). *Investigation of the Kansas City Hyatt Regency Walkways Collapse*. NBSIR 82-2465, National Bureau of Standards, U.S. Department of Commerce, February 1982. DOI 10.6028/NBS.IR.82-2465. <https://nvlpubs.nist.gov/nistpubs/Legacy/IR/nbsir82-2465.pdf> Freely downloadable. The 278-page main volume is the one cited; a companion volume NBSIR 82-2465(A) carries the same title.

California St. Francis Dam Commission (1928). *Report of the Commission Appointed by Governor C. C. Young to Investigate the Causes Leading to the Failure of the St. Francis Dam Near Saugus, California*, 24 March 1928. Sacramento: State of California (commission members: Wiley, Louderback, Ransome, Bonner, Cory, Fowler; Governor Young contributed the transmittal). <https://authors.library.caltech.edu/records/pf78d-gpy92> (full scan: <https://authors.library.caltech.edu/records/pf78d-gpy92/files/TR000563.pdf>) · also HathiTrust <https://catalog.hathitrust.org/Record/001514693> Freely downloadable. Not to be confused with the separately issued report of the committee appointed by the Los Angeles City Council.

Rogers, J. D. (1995). A man, a dam and a disaster: Mulholland and the St. Francis Dam. *Southern California Quarterly*, 77(1-2), 1-109. DOI 10.2307/41171757. Paywalled at the publisher; the author's open copy is at <https://web.mst.edu/rogersda/temp/St%20Francis%20Dam%20failure/A%20Man-A%20Dam-A%20Disaster-1995-Rogers.pdf> The same special issue was co-published as D. B. Nunis, Jr. (ed.), *The St. Francis Dam Disaster Revisited* (Historical Society of Southern California and Ventura County Museum of History and Art, 1995), ISBN 978-0-914421-13-9, at the same pagination.

Cullen, W. D., The Hon. Lord (1990). *The Public Inquiry into the Piper Alpha Disaster*, 2 vols. Cm 1310. Presented to Parliament by the Secretary of State for Energy, 13 November 1990. London: HMSO. Volume 1: <https://www.hse.gov.uk/offshore/assets/docs/piper-alpha-public-inquiry-volume1.pdf> Volume 2: <https://www.hse.gov.uk/offshore/assets/docs/piper-alpha-public-inquiry-volume2.pdf> (landing page: <https://www.hse.gov.uk/offshore/piper-alpha-disaster-public-inquiry.htm>) Freely downloadable under Open Government Licence v3.0. Some reference lists give the author as "H. L. Cullen"; the correct form is W. Douglas Cullen.

Fischer, M. J., Lynch, N. A., & Paterson, M. (1985). Impossibility of distributed consensus with one faulty process. *Journal of the ACM*, 32(2), 374-382. DOI 10.1145/3149.214121. Paywalled at the publisher.

Turing, A. M. (1936-37). On computable numbers, with an application to the Entscheidungsproblem. *Proceedings of the London Mathematical Society*, series 2, 42, 230-265. DOI 10.1112/plms/s2-42.1.230. The paper appeared in two parts during 1936 and the bound volume carries a 1937 date, which is why both years are cited in the literature. See also the author's correction: Turing, A. M. (1938), *Proceedings of the London Mathematical Society*, series 2, 43, 544-546, DOI 10.1112/plms/s2-43.6.544, which repairs a flaw in the universal-machine construction. Paywalled at the publisher; an open copy is at <https://people.math.ethz.ch/~halorenz/4students/Literatur/TuringFullText.pdf>

6. Relationship to the Series

- **Paper II** cites this ledger as Tier-1 evidence line (ii): the same violation structure in a non-linguistic substrate. The classification criterion here is the one the map's Second Edition froze, so the cross-substrate claim is carried by a single method applied twice.
- **Paper III, §4** cites the engineering substrate as one of the two independent empirical substrates filling the structural argument's form.
- **The oAOML implementation** operationalizes the five types as a verified legality layer; this ledger is the evidence document, the implementation is the enforcement artifact, and the sealed preregistration is the predictive test. Three artifacts, three distinct epistemic jobs.

Appendix A. Machine-Readable Judgment Ledger

One row per audited judgment (32 rows: 27 type-assigned, 5 audited without a type assignment). Compressed forms; the §4 analyses are authoritative. Columns: ID · incident · judgment form (compressed) · governing side condition · intervention outcome · type (root/locus) · role · evidence grade (§2.2) · source of record.

ID	Incident	Judgment form	Side condition	Intervention outcome	Type	Role	Grade	Source
----	----------	---------------	----------------	----------------------	------	------	-------	--------

MCO-J1	Mars Climate Orbiter	interchange value is in the interface-specified unit	producer emits per specification / licensed conversion	repair licenses (replacement, §2.3a-b)	T1	primary	A	NASA MIB Phase I (1999)
KNI-J1	Knight Capital	flag uniformly rebound across the fleet	C1 deployment complete; C2 old binding inert	C1 repair licenses; C2 severity only	T2	primary	A	SEC Exchange Act Rel. 70694 (2013)
THE-J1	Therac-25	represented configuration is machine configuration	accepted edits propagate before commit	repair licenses (Δ route historically: editing restriction)	T2 root / T5 locus	primary	B	Leveson & Turner (1993)
THE-J2	Therac-25	setup-complete check holds on every pass	flag representation faithful over domain	repair licenses (dual route)	T2 root / T4 locus	primary	B	Leveson & Turner (1993)
THE-J3	Therac-25	software-only enforcement suffices	defense allocation (no stable JF)	not forced	untyped	contributing	B	Leveson & Turner (1993)
ARI-J1	Ariane 5	horizontal bias fits 16-bit representation throughout operation	range bounded by operative envelope	repair licenses (operator route in practice, §2.3a-b)	T2 root / T4 locus	primary	A	Lions Board (1996)
ARI-J2	Ariane 5	Ariane 4 qualification warrants Ariane 5 operation	envelope match	warrant repair	T3 (overextension)	upstream	A	Lions Board (1996)
MIZ-J1	Mizuho / J-Com	accepted order lies in admissible domain	bounds enforced at acceptance	repair licenses	T2	primary	A	Tokyo High Court (2013)
MIZ-J2	Mizuho / J-Com	cancel against a live order is processed	cancel domain covers matching states	repair licenses	T2	severity contributor	A	Tokyo High Court (2013)
MIZ-J3	Mizuho / J-Com	warning inapplicable to this order	operator's basis (not in record)	unresolved	untyped	contributing	A	Tokyo High Court (2013)

CRO-J1	CrowdStrike	template references satisfied by supplied inputs	declared count equals supplied count	repair licenses	T2	primary	C	CrowdStrike External Tech. RCA (2024)
CRO-J2	CrowdStrike	validator pass warrants fleet deployment	warrant covers non-wildcard 21st field	warrant repair	T3 (overextension)	upstream	C	CrowdStrike External Tech. RCA (2024)
SCH-J1	Schiaparelli	reading is admissible estimator input	qualified readings excluded or bounded	operator repair only (blocked, §2.3a-b)	T2	primary	A	ESA Schiaparelli Inquiry (2017)
SCH-J2	Schiaparelli	modeled envelope warrants saturation handling	envelope covers actual regime	warrant repair	T3 (overextension)	upstream	A	ESA Schiaparelli Inquiry (2017)
MCA-J1	737 MAX MCAS	activation within licensed control authority	increment and repeatability match analyzed envelope	survives repair of C2	T2	co-root, primary	A	KNKT (2019); JATR (2019); House (2020)
MCA-J2	737 MAX MCAS	one sensor's reading warrants activation	evidence basis matches hazard level	survives repair of C1	T3	co-root, primary	A	KNKT (2019); JATR (2019); House (2020)
GIM-J1	Gimli Glider	computed fuel mass is in kilograms	conversion chain carries target units	repair licenses (replacement, §2.3a-b)	T1	primary	A	Board of Inquiry (1985)
GIM-J2	Gimli Glider	dispatch under MEL with inoperative gauges warranted	no stable judgment form	unresolved	untyped	contributing	A	Board of Inquiry (1985)
VAS-J1	Vasa	members under different foot standards compose	common standard or licensed conversion	repair licenses	T1	contributing	B	Cederlund & Hocker (2006)
VAS-J2	Vasa	the ship is fit to sail	stability demonstration's verdict governs	substitute's warrant mismatch (displacement)	T3 (displacement)	primary among classifiable	B	Cederlund & Hocker (2006)
PAT-J1	Patriot, Dhahran	time value accurate over operational uptime	representation error bounded over uptime	repair licenses (dual route, enforced)	T2 root / T4 locus	primary	A	GAO/IMTEC-92-26 (1992)

PAT-J2	Patriot, Dhahran	continuous operation within qualified envelope	warrant covers the duty cycle	warrant repair	T3 (overextension)	upstream	A	GAO/IMTEC-92-26 (1992)
787-J1	Boeing 787 GCU	counter faithful over continuous-power domain	width covers domain, or domain bounded	repair licenses (dual route, AD-enforced)	T2 root / T4 locus	primary	A	FAA AD 2015-09-07
Y2K-J1	Y2K	two-digit year arithmetic valid	operands share a century frame	coinciding repairs, one condition (§2.3a-c)	T2 root / T4 locus	class-level	D	no record of record
MIL-J1	Millennium Bridge	code load model warrants serviceability	structure within the code's validated envelope	warrant repair	T3 (overextension)	primary	B	Dallard et al. (2001)
BLK-J1	Northeast blackout	alarms delivered or failure announced	concurrency covered; failure annunciated	repair licenses	T2 root / T5 locus	primary	A	Outage Task Force (2004)
BLK-J2	Northeast blackout	no alarms, therefore no events	detection channel live	licensed in form; defeated upstream	consequence (untyped)	consequence	A	Outage Task Force (2004)
HYA-J1	Hyatt Regency	revised connection preserves load relation	load-path equivalence established	repair (the check) refuses the substitution	T2	primary	A	NBS, Marshall et al. (1982)
STF-J1	St. Francis Dam	foundation rock warrants the design	geological investigation validates	substitute's warrant mismatch (displacement)	T3 (displacement)	primary	A/B	St. Francis Dam Commission (1928); Rogers (1995)
STF-J2	St. Francis Dam	raised design retains approved margin	margin re-established under modification	repair licenses	T2	contributing	A/B	St. Francis Dam Commission (1928); Rogers (1995)
PIP-J1	Piper Alpha	permit representation corresponds to physical state	schema expresses equipment-state dependencies	frame repair only (rival rejected, §4.18)	T5 root	primary	A	Cullen Inquiry (1990)
PIP-J2	Piper Alpha	handover carries	occasion under J1	contributing under	untyped	contributing	A	Cullen Inquiry

		the dependency		J1				(1990)
--	--	----------------	--	----	--	--	--	--------

Accounting check: 32 rows; type-assigned 27 (T1: MCO-J1, GIM-J1, VAS-J1; T2: KNI-J1, THE-J1, THE-J2, ARI-J1, MIZ-J1, MIZ-J2, CRO-J1, SCH-J1, MCA-J1, PAT-J1, 787-J1, Y2K-J1, BLK-J1, HYA-J1, STF-J2; T3: ARI-J2, CRO-J2, SCH-J2, MCA-J2, PAT-J2, VAS-J2, MIL-J1, STF-J1; T5: PIP-J1); untyped 5 (THE-J3, MIZ-J3, GIM-J2, BLK-J2, PIP-J2). Matches §4.19's count table.

Companion document to: Seeley, B.A. (2026). *The Universal Fallacy Architecture. Paper II, Foundations of the Convergent Semantic Architecture. Method: Seeley, B.A. (2026). The Universal Fallacy Map (Second Edition), revision criterion.* <https://doi.org/10.5281/zenodo.21880635> Structural foundation: Seeley, B.A. (2026). *Given Distinction. Paper III, Foundations of the Convergent Semantic Architecture.*