1 Executive summary

Two Boeing 737 MAX aircraft—Lion Air Flight 610 (Oct. 29, 2018) and Ethiopian Airlines Flight 302 (Mar. 10, 2019)—were lost in accidents that exposed a tightly coupled failure across automation design, certification practice, organizational decision-making, and operator information/training. The U.S. FAA grounded the MAX on Mar. 13, 2019 and rescinded the grounding on Nov. 18, 2020. [1]

At a high level:

- A safety-relevant control function (MCAS) could command stabilizer trim based on erroneous angle-of-attack (AoA) input and repeatedly re-engage in a way crews struggled to arrest in time-critical conditions. In the Lion Air accident sequence, MCAS reportedly activated **24 times** after receiving faulty data from one AoA sensor. [2]
- The safety case and certification ecosystem did not reliably surface "what changed," "what assumptions are embedded," and "what operators must know," especially as MCAS evolved and as training determinations were formalized. [2] [3]
- Post-accident investigations and enforcement actions describe breakdowns in truthful disclosure to regulators and downstream effects on training/manual content. [4] [5]

These failures are best understood as a breakdown in **engineering safety governance** rather than a single-point technical flaw. The MAX case illustrates how modest-seeming design and certification decisions can combine—through information asymmetries, organizational incentives, and operational variability—into an accident pathway that is difficult to interrupt once triggered.

1.1 Ethical framing through ASME Canons

- **Canon 1 (Hold paramount the safety, health, and welfare of the public).** When a safety-relevant automation function can drive hazardous aircraft states under credible sensor fault conditions, the ethical burden is to demonstrate robust fault tolerance and recoverability—not merely to satisfy minimum compliance arguments or assume ideal operator response. The repeated activation behavior described in the Lion Air sequence underscores how quickly a safety margin can be consumed when a single failure mode cascades. [2]
- **Canon 2 (Perform services only in areas of competence) and Canon 3 (Continue professional development, provide opportunities for development under supervision).** Safety-critical system development demands competence not only in software or aerodynamics in isolation, but also in integrated human–automation interaction, hazard analysis, and certification logic. The institutional record suggests that key assumptions and changes were not consistently surfaced to the right reviewers and decision-makers, which is a competence and process problem as much as a "bad design" problem. [2]
- **Canon 7 (Issue public statements only in an objective and truthful manner).** Enforcement actions describe breakdowns in truthful disclosure to regulators with downstream implications for training and manuals, in aviation safety, that kind of information integrity failure functions as a direct risk amplifier because it constrains what operators and oversight bodies can do to build procedural defenses. [4] [5]
- **Canon 4 (Act as faithful agents, avoid conflicts of interest or the appearance thereof).** The certification ecosystem and internal incentives can create structural conflicts between sched-

ule/market goals and conservative safety practice. When those tensions are not actively managed through governance and transparency, ethical obligations to the public are effectively subordinated by default. [2] [3]

The ethical lesson is not "automation is bad" or "pilots made mistakes," but that safety-critical engineering requires (i) conservative fault tolerance, (ii) transparent, decision-relevant communication, and (iii) institutions designed to resist incentive-driven erosion of safety margins.

1.2 Concrete next steps (actionable reforms)

1.2.1 Technical safeguards (design + verification)

- **Require sensor plausibility and disagreement handling** for any safety-relevant automation authority path (e.g., AoA cross-checking, validity gating, explicit fault modes). This directly addresses the failure mode where erroneous AoA input can drive repeated trim commands. [2]
- **Expand verification to worst-case repetition and coupled failures,** not just single-event scenarios, including stress testing under realistic pilot workload. The accident pathway involved persistence and time pressure, so verification must explicitly cover "repeat, escalate, saturate" dynamics.
- **Treat pilot recoverability as a formal requirement** with measurable acceptance criteria (time-to-recognition, time-to-arrest, control authority margins), rather than an assumed property.

1.2.2 Organizational controls (culture + information integrity)

- **Implement a safety-critical change disclosure gate**: any change that alters system authority, activation conditions, or failure behavior must trigger a documented cross-functional review (engineering, flight ops, training, certification) and an explicit regulator-facing summary.
- **Establish protected escalation channels and audit trails** for safety concerns so they cannot be silently re-scoped or absorbed by schedule pressure. This is a governance mechanism for Canon 1 in practice.
- **Strengthen "truthfulness controls" in regulator-facing interactions** (review boards, legal/compliance sign-off, and penalties for omission). The enforcement record shows why treating disclosure as optional is ethically and operationally unsafe. [4]

1.2.3 Institutional reforms (oversight + training governance)

- **Reduce dependence on manufacturer signaling for "significant changes."** Oversight processes should include independent triggers for deeper review when safety-relevant functions change, addressing the OIG's findings about certification/delegation weaknesses. [2]
- **Bind training determinations to the safety case.** If safe operation depends on understanding a function or failure mode, that knowledge must be embedded in standardized training and documentation pathways—not left to informal diffusion. [3]
- **Require explicit documentation of embedded assumptions** (pilot response models, workload assumptions, global operator variability) and make those assumptions auditable artifacts in certification review.

Taken together, these steps operationalize engineering ethics: they turn "hold paramount public safety" into concrete design constraints, review gates, disclosure requirements, and oversight mechanisms that remain effective under real-world incentives.

2 What happened

2.1 The accident pair and grounding timeline

Lion Air Flight 610 (Oct. 29, 2018) and Ethiopian Airlines Flight 302 (Mar. 10, 2019) were fatal accidents involving 737 MAX aircraft, the FAA issued a U.S. grounding order on Mar. 13, 2019 and later rescinded it on Nov. 18, 2020. [1]

2.2 The immediate technical signature: erroneous AoA and repeated trim

Investigations describe a mismatch between sensed AoA and aircraft reality, followed by automatic nose-down trim commands that crews attempted to counter.

- For Lion Air, the FAA's return-to-service review summarizes that a replacement AoA sensor had been **mis-calibrated** during an earlier repair and the mis-calibration was not detected. [6]
- For Ethiopian Airlines Flight 302, the preliminary report states there was an AoA disagreement shortly after takeoff (left AoA $\sim 74.5^\circ$ vs right $\sim 15.3^\circ$) and multiple automatic nose-down trim commands without pilot input, the crew performed the runaway stabilizer checklist and moved stabilizer trim cutout switches to cutout. [7]

3 Why it happened

3.1 Safety-critical automation bounded by weak sensing and weak cross-checking

A core design vulnerability was allowing a stability-related control function to command trim in the presence of bad sensor input without robust, conservative validation of that input. The U.S. House investigation report states the original MCAS design lacked "rudimentary provisions" to cross-check AoA outputs. [8]

This is an engineering ethics issue because foreseeable sensor faults are not exotic edge cases in aviation, in high-stakes systems, a single-point failure that can drive the aircraft toward loss of control should trigger unusually high design conservatism and unusually strong evidence for recoverability.

3.2 Human factors assumptions treated as a substitute for technical fault tolerance

Operator response was effectively part of the control loop. Boeing pilots and engineers assumed crews would recognize unintended MCAS activation as a runaway stabilizer condition and respond accordingly. [8] But the operational reality included time pressure, startle effects, workload, and uneven training environments.

A safety argument that "the crew will always respond correctly" is ethically fragile unless it is backed by evidence across realistic conditions and realistic operator variance—and unless the system is designed so incorrect or delayed response does not quickly become unrecoverable.

3.3 Verification and test scope that did not match the worst-case dynamics

The House report also documents that Boeing tested a single unintended MCAS activation but did **not** test repeated activations, with internal discussions assuming multiple activations would be no worse than a single activation. [8] In safety-critical domains, that kind of assumption is exactly the type that must be stress-tested, not merely reasoned about.

3.4 Certification and delegation gaps that obscured system-level risk

Certification is not external to the system, it is part of the system. DOT OIG concludes that gaps in FAA guidance and processes contributed to misunderstanding MCAS, including reliance on manufacturers to flag "significant" changes and incomplete visibility into assumptions embedded in safety assessments. [2] The OIG also notes that FAA certification engineers were not aware of significant MCAS changes during certification, limiting their ability to understand aircraft-level impact. [2]

The Joint Authorities Technical Review (JATR) report is part of the broader record documenting concerns around certification practice and system-level review of the MAX flight control system. [9]

3.5 Information integrity failures that distorted downstream training and documentation

Post-incident legal actions describe a breakdown in truthful disclosure. DOJ states Boeing—through two 737 MAX Flight Technical Pilots—deceived the FAA's Aircraft Evaluation Group about an important MCAS change, contributing to training/manual materials lacking MCAS information. [4] DOJ also describes the deferred prosecution agreement and related remedies totaling over $2.5B. [5]

This matters ethically because transparency is not a public-relations preference, it is a safety control. When pilots, airlines, and regulators do not have decision-relevant information about system behavior, they cannot build the procedural defenses (training, checklists, operational limits) that compensate for technical complexity.

3.6 Global deployment and uneven operator environments

The MAX operated globally across airlines with different training resources and safety cultures. Training determinations were formalized through processes like the FAA Flight Standardization Board report (e.g., the finding that Level B differences training was sufficient for certain differences). [3] Where a design's safety depends on operator knowledge and access to robust training, ethical responsibility requires treating that variability as a first-order design input—not as background noise.

4 Ethical analysis

4.1 Holding public safety paramount

In this case, "public safety first" is not a slogan, it is a design and governance requirement. For aviation automation, that means:

- Conservative fault tolerance: treat bad sensor input and ambiguous states as normal threats, not rare anomalies.
- Clear recoverability: ensure that reasonable pilot actions can reliably restore safe flight, and that the system does not "fight" those actions in a confusing way.

- Evidence-driven human factors: do not assume idealized operator performance, validate operator interactions under realistic time pressure and surprise.

4.2 Responsibility in a distributed system

Responsibility in the MAX case cannot be assigned to a single person or a single mechanism. It is distributed across:

- Engineers responsible for requirements, hazard analyses, sensor/logic architecture, and test scope.
- Managers and executives responsible for incentive structures and for ensuring safety concerns can surface and change decisions.
- Regulators responsible for creating oversight processes that do not depend on perfect manufacturer signaling and that maintain system-level visibility. [2]

A key ethical failure mode here is "diffusion by design": complex organizations can create structures where each actor has a defensible local rationale while the overall system drifts toward unacceptable risk.

4.3 Transparency as an operational safety control

The MAX case shows how transparency failures can become causal rather than merely reputational. If regulators and operators lack accurate, salient information about a safety-relevant function and its evolution, then training, manuals, and operational safeguards can be mis-specified—raising the probability that an error becomes fatal. [4] [3]

5 What we can do

5.1 Engineering and technical changes

- **Design automation for fault tolerance, not for "pilot catch."** If a function can move primary control surfaces or trim in a way that can become unrecoverable, then sensor disagreement, plausibility checks, and conservative authority limits should be non-negotiable design constraints. [8]
- **Expand verification to cover worst-case repetition and coupled failures.** If a hazard becomes catastrophic through repetition (not just a single activation), that repetition must be explicitly tested and analyzed—not assumed away. [8]
- **Treat operator interaction as part of the system requirements.** Validate procedures and interfaces under high workload and startle effects, build automation behavior that is legible and consistent with pilot mental models.

5.2 Organizational changes

- **Create internal "information integrity" obligations.** Safety-relevant changes and assumptions must be communicated clearly across engineering, test, training, and certification interfaces—especially when changes alter system-level behavior.

- **Strengthen escalation pathways for safety concerns.** If raising risk is career-limiting, the organization will systematically under-detect hazards. A healthy safety culture makes it easier to stop the line than to explain a tragedy.
- **Align incentives with safety margins.** Schedule and market pressure will always exist, the ethical question is whether governance prevents those pressures from silently redefining "acceptable risk."

5.3 Regulatory and institutional changes

- **Reduce dependence on manufacturer signaling for "significant changes."** Oversight processes should not assume perfect disclosure, they should be robust to the realistic incentive landscape. [2]
- **Maintain system-level visibility in delegated certification structures.** The regulator must be able to see not only compliance artifacts but also the assumptions driving hazard classifications and pilot-response models. [2]
- **Treat training determinations as safety-critical decisions.** Training and documentation are part of the safety case, if a system's safe operation depends on understanding a function, then minimizing training burden cannot be the dominant objective. [3]

6 Practical constraints (and why they don't excuse preventable risk)

Real constraints exist—competitive pressure, certification timelines, legacy platform constraints, and global airline economics. But these constraints are exactly why safety-critical engineering ethics demands institutional guardrails: when pressures are predictable, designing processes to resist them is part of competent practice, not an optional ideal.

7 Conclusion

The Boeing 737 MAX incidents illustrate a classic sociotechnical failure: a safety-relevant automation function interacted with sensor faults, human factors realities, organizational incentives, and certification processes in ways that made catastrophic outcomes possible. The prevention strategy is therefore also sociotechnical: better fault-tolerant design, better evidence-based validation of operator interaction, stronger internal transparency and safety culture, and oversight mechanisms that remain effective under real-world incentives and information asymmetries. [2] [8]

References

[1] "Faa oversight of boeing's 737 max certification: Timeline of activities," U.S. Department of Transportation, Office of Inspector General, Report (Final), Jun. 29, 2020, PDF. [Online]. Available: https://www.oig.dot.gov/sites/default/files/FAA%20Oversight%20of%20Boeing%20737%20MAX%20Certification%20Timeline%20Final%20Report.pdf.

[2] "Weaknesses in faa's certification and delegation processes hindered its oversight of the 737 max 8," U.S. Department of Transportation, Office of Inspector General, Report No. AV2021020, Feb. 23, 2021, PDF. [Online]. Available: https://www.oig.dot.gov/sites/default/files/FAA%20Certification%20of%20737%20MAX%20Boeing%20II%20Final%20Report%5E2-23-2021.pdf.

[3] "Flight standardization board report: The boeing company 737, revision 17," Federal Aviation Administration, FSB Report, PDF; exact publication day may be listed inside the PDF. [Online]. Available: https://www.faa.gov/sites/faa.gov/files/2022-08/737_FSB_Report.pdf.

[4] U.S. Department of Justice, *U.s. v. the boeing company: Deferred prosecution agreement and statement of facts*, Court filing (PDF), PDF, Jan. 7, 2021. [Online]. Available: https://www.justice.gov/criminal/criminal-vns/file/1482911/dl?inline=.

[5] U.S. Department of Justice, Office of Public Affairs, *Boeing charged with 737 max fraud conspiracy and agrees to pay over $2.5 billion*, Press release, Jan. 7, 2021. [Online]. Available: https://www.justice.gov/archives/opa/pr/boeing-charged-737-max-fraud-conspiracy-and-agrees-pay-over-25-billion.

[6] "Summary of the faa's review of the boeing 737 max," Federal Aviation Administration, Report, PDF; month/day may be listed inside the PDF. [Online]. Available: https://www.faa.gov/sites/faa.gov/files/2022-08/737_RTS_Summary.pdf.

[7] "Aircraft accident investigation bureau preliminary report: Ethiopian airlines flight 302 (boeing 737-8 max, et-avj)," Aircraft Accident Investigation Bureau (Ethiopia), Preliminary Report, PDF copy hosted by a third-party site; use official host if your course requires primary hosting. [Online]. Available: https://leehamnews.com/wp-content/uploads/2019/04/Preliminary-Report-B737-800MAX-ET-AVJ.pdf.

[8] "Final committee report: The design, development & certification of the boeing 737 max," U.S. House of Representatives, Committee on Transportation and Infrastructure, Committee Report, PDF; exact publication day may be listed inside the report. [Online]. Available: https://www.govinfo.gov/content/pkg/GOVPUB-Y4_T68_2-PURL-gpo144993/pdf/GOVPUB-Y4_T68_2-PURL-gpo144993.pdf.

[9] "Boeing 737 max flight control system observations," Federal Aviation Administration, Joint Authorities Technical Review (JATR) Report, Oct. 11, 2019, PDF. [Online]. Available: https://www.faa.gov/sites/faa.gov/files/2021-08/Final_JATR_Submittal_to_FAA_Oct_2019.pdf.