What changes when a safety-critical control can act on one sensor?

Boeing 737 MAX | United States | Indonesia | Ethiopia | Accidents 2018-2019 | FAA return to service 2020

FATALITIES	ORIGINAL MCAS INPUT	US GROUNDING	REVISED MCAS INPUT
346 across two accidents	**One AOA sensor at a time**	**March 2019-November 2020**	**Both AOA sensors**
S02	S01	S01	S01

DOCUMENTED EVENT

Lion Air flight 610 crashed on 29 October 2018, killing all 189 passengers and crew; Ethiopian Airlines flight 302 crashed on 10 March 2019, killing all 157 passengers and crew. The NTSB reported that erroneous high angle-of-attack inputs resulted in MCAS activating on both accident flights and also produced multiple alerts and indications. The FAA's return-to-service review identified the original use of a single angle-of-attack sensor and repeated MCAS commands as safety issues requiring correction. The updated flight-control software uses both sensor inputs, compares them and disables the stabiliser trim system, including MCAS, for the remainder of the flight when their difference exceeds a calculated threshold. [S01 | S02]

NFRISK SCENARIO ADAPTATION - NOT AN EXTERNAL FINDING

A safety- or customer-critical automated control can initiate a consequential action from one data feed. A second independent feed exists but is used only for display or diagnosis. The system's safety assessment assumes that an operator will recognise a bad input, interpret several concurrent alerts and reverse the action within a short time. Those recognition and response assumptions have not been tested under realistic workload and ambiguity.

STRESS-TEST QUESTIONS

01 Which high-consequence automated actions can be initiated by one data source, and what happens when that source disagrees with an independent input?

02 Are assumptions about human recognition and intervention tested under realistic alert load and time pressure, or accepted from design documentation?

03 Does a detected input disagreement produce a safe degraded state, or leave operators to diagnose and reverse an active control?

04 Who has standing to reopen an approved design assumption after incidents, near misses or new operational evidence challenge it?

CONNECTED RISK

Data & Control Integrity (primary)
Technology & Change Risk (contributing)
Conduct & Governance Risk (contributing)

FRAMEWORK RELEVANCE

FAA safety issue: single AOA sensor dependency
The FAA identified erroneous data from one AOA sensor activating MCAS as a safety issue that had to be addressed, and documented the revised use of both sensor inputs and disagreement logic. [S01]

NTSB safety-assessment lens: pilot recognition and response
The NTSB questioned whether accident-flight responses were consistent with the pilot recognition and response assumptions used in the original functional hazard assessment and recommended stronger validation of those assumptions. [S02]

NFRISK PRACTITIONER INTERPRETATION

Redundancy is not achieved merely by installing a second sensor or data source; it must participate in decision logic, disagreement handling and safe degradation. Design assurance should trace each high-consequence action to its input dependencies, test plausible common and single-source failures, and validate the time and information a human needs to intervene. The central governance question is who can reopen an accepted design assumption when operational evidence challenges it.

PRIMARY-SOURCE REGISTER

S01 Federal Aviation Administration (2020)
Summary of the FAA's Review of the Boeing 737 MAX
S02 National Transportation Safety Board (2019)
Assumptions Used in the Safety Assessment Process and the...

EVIDENCE BOUNDARY Official findings are separated from the institutional scenario, framework interpretation and NFRisk practitioner view.