EASA Part 21J Safety Management System – Workshop Task - Boeing 737 MAX Groundings

Sofema Aviation Services (SAS) www.sassofia.com Workshop Task to understand the root Causes associated with the Boeing Max Catastrophic Events and to focus on the Understanding of Design Shortfall and Mitigations required to preclude similar recurrence in the future.

The failure to recognize the risk of a single-point failure in the AoA sensor underscores the importance of a safety-first culture, rigorous independent oversight, and redundant design in complex systems like aircraft automation.

Introduction – What Happened & Why?

The Boeing 737 MAX aircraft faced extensive grounding after two fatal crashes—Lion Air Flight 610 (October 2018) and Ethiopian Airlines Flight 302 (March 2019)—leading to the death of 346 people.

The crashes were linked to a design issue in the Maneuvering Characteristics Augmentation System (MCAS), which caused automated nose-down actions under certain conditions, contributing to a loss of control. Initially, Boeing did not disclose MCAS details in pilot training materials or manuals, leading to pilots being unaware of how to handle such malfunctions.

Following investigations, regulators worldwide grounded the aircraft, and Boeing incurred severe financial losses. Further inspection requirements and design modifications were mandated before the MAX could return to service.

Discussion on Design Failures in the Boeing 737 MAX

MCAS Overreach and Faulty Activation

- **Excessive Control Authority Failure**: MCAS was designed to counteract the MAX's tendency to pitch up due to engine placement.
    - However, its control authority was excessive, leading to repetitive, uncommanded nose-down inputs when the system received erroneous data from a single Angle of Attack (AoA) sensor.
- **Excessive Control Authority Failure** - **Underlying Reason**: Boeing wanted the MAX to handle similarly to previous 737 models to minimize pilot retraining costs.
    - This focus on reducing training costs influenced the decision to implement an overly aggressive MCAS without adequate redundancy or pilot awareness.

- **Single Point of Failure in AoA Sensor -** A single point of failure in the Angle of Attack (AoA) sensor is a critical risk because it makes the entire system dependent on one component.
- **MCAS Single Point Failure**: MCAS depended on input from a single AoA sensor, making it vulnerable to sensor failures, as seen in both Lion Air and Ethiopian Airlines accidents.
    - **Underlying Reason**: The decision to use a single sensor input instead of two likely stemmed from cost-saving measures and Boeing's confidence that the system was fail-safe, which resulted in insufficient consideration of sensor reliability.
- **Cockpit Design and Display Limitations -** The limitations in the cockpit design and available information directly impacted the crew's situational awareness and their ability to respond to system malfunctions**.**
- **Cockpit Design Failure**: Boeing omitted adequate display warnings or alerts related to MCAS or AoA discrepancies in the cockpit.
    - **Underlying Reason**: Boeing did not consider the need for new cockpit alerts or indicators as part of the design, as it focused on cost containment and minimizing system changes from previous models.
    - This led to a lack of critical feedback for pilots when MCAS engaged unexpectedly.

Understanding the Shortfall related to Design Analysis Considerations

The failure to identify the potential hazard and associated risk of the single-point failure in the AoA (Angle of Attack) sensor on the Boeing 737 MAX highlights critical lapses in both design foresight and due diligence processes.

This oversight stemmed from several factors, including

- Assumptions made during the development,
- Limitations in risk assessment methodologies, and
- The regulatory structure that allowed for certain safety shortcuts.

Consider the following:

Assumptions About MCAS Functionality and Risk Mitigation

- Boeing's engineers and designers assumed that the MCAS would operate with minimal risk, based on its role as an augmentation system rather than a primary flight control mechanism.

- They believed it was a low-risk addition, designed merely to assist pilots in specific situations rather than actively manage aircraft stability.

Assumptions About MCAS Functionality and Risk Mitigation - Why It Was Missed ?

- The incorrect assumptions led Boeing to forego a more rigorous hazard analysis.

- The decision to base MCAS inputs on a single AoA sensor, without cross-referencing a second sensor, was considered "acceptable" because engineers believed the likelihood of an AoA sensor failure was minimal and that pilots would quickly counter any system misbehavior.
    - Note however, this confidence in pilot capability to handle the malfunction without adequate backup disregarded the reality of how quickly MCAS would react and how challenging it would be for pilots to recognize and address the issue.

Inadequate Hazard and Risk Analysis Procedures

- The hazard analysis for MCAS did not fully account for the consequences of an AoA sensor failure leading to repeated, uncommanded nose-down inputs.
    - Boeing classified MCAS as a "non-critical" system, which subjected it to a lower level of scrutiny.

Inadequate Hazard and Risk Analysis Procedures - Why It Was Missed?

- The analysis used did not foresee the cascading impact of an AoA sensor failure, nor did it incorporate worst-case scenarios.
    - A single-point failure in a safety-critical system should have prompted a higher classification for MCAS, requiring a more detailed failure mode and effects analysis (FMEA).
    - Instead, the analysis assumed MCAS would not present a catastrophic risk and focused more on ensuring that it would pass certification rather than thoroughly assessing all potential hazards.
    - The reliance on a single sensor was rationalized as being in line with industry standards, though in retrospect, it was a significant risk due to the critical nature of the information the AoA sensor provided.

Pressure to Limit Changes and Training Costs

- Boeing aimed to certify the 737 MAX as an incremental improvement to the existing 737 model. This goal was to ensure that airlines would not need extensive retraining for pilots transitioning from earlier 737 models to the MAX, keeping costs and training times down.

Pressure to Limit Changes and Training Costs - Why It Was Missed:

- Boeing's focus on cost and time efficiency drove design decisions to limit significant changes, and the addition of a second AoA sensor input was seen as unnecessary complexity that could require additional training and certification steps.
    - By minimizing system modifications and simplifying training needs, Boeing avoided triggering a reclassification that would demand more rigorous safety evaluations.
    - This commercial incentive directly impacted the depth of risk analysis, sidelining concerns over single points of failure.

Lack of Independent Review and Regulatory Oversight

- Boeing's role in the FAA's Organization Designation Authorization (ODA) program gave it the authority to conduct its own safety assessments with limited external scrutiny.
    - This system allows companies to make certain certification determinations on behalf of the FAA.

Lack of Independent Review and Regulatory Oversight - Why It Was Missed:

- Due to Boeing's self-certification in some areas, regulatory checks that might have caught the hazard of the single-point failure in the AoA sensor were not as comprehensive.
- With limited independent oversight, the decision to rely on one sensor did not undergo the same level of review it might have under stricter regulatory conditions.
- The FAA accepted Boeing's classification of MCAS as non-critical and did not mandate a dual-sensor setup.
    - This lack of regulatory pushback was a contributing factor to the oversight.

Focus on Product Similarity for Market Competitiveness

- Overview: Boeing designed the 737 MAX with the intent that it would handle similarly to earlier 737 models, maintaining fleet compatibility and giving it an advantage in the market over competitor aircraft like the Airbus A320neo.

Focus on Product Similarity for Market Competitiveness - Why It Was Missed:

- To preserve this market advantage, Boeing prioritized product similarity over fundamental design changes that would add safety redundancy.
- Implementing dual AoA sensors or other safeguards might have compromised the similarity Boeing wanted to maintain between models.

- As a result, the design change and safety review processes were influenced by commercial concerns, leading to a risk tolerance that underestimated the potential for a catastrophic outcome.

Actions to Mitigate Future Occurrences in Boeing 737 MAX and Similar Aircraft

- **Enhanced Redundancy and MCAS Redesign**:
  - **Actions**: The MCAS system was reprogrammed to use inputs from both AoA sensors, ensuring the system only activates if both sensors agree. The updated MCAS also limits its authority, preventing repeated nose-down commands, and allows pilots to override the system.
  - **Expected Outcome**: Increased reliability in flight control systems and prevention of single-point failures, reducing the likelihood of erroneous MCAS activation.
- **Increased Regulatory Oversight and Certification Reforms**:
  - **Actions**: The FAA has revoked Boeing's authority to self-certify certain safety components, enforcing stricter oversight. New certification procedures now require direct FAA approval for key systems and modifications, and all MAX aircraft must pass updated airworthiness checks.
  - **Expected Outcome**: Greater regulatory control over aircraft design and testing, enhancing public confidence in aircraft safety and reducing risks associated with self-certification.
- **Improved Production Quality Controls**:
  - **Actions**: Boeing implemented additional inspections and quality audits on assembly lines, especially on critical components like door plugs, sensors, and control systems. The company is also working on an independently monitored safety compliance program as part of legal settlements.
  - **Expected Outcome**: Higher production standards and component reliability, reducing manufacturing flaws that could lead to in-service incidents and ensuring quality consistency across the fleet.
- **Strengthened Communication and Transparency with Regulators**:
  - **Actions**: Boeing committed to transparent communication regarding all safety features and risks, including openly disclosing design changes and system functionalities to both the FAA and international regulators.

- **Expected Outcome**: Enhanced collaboration between manufacturers and regulators, fostering a safety-first culture and ensuring any design risks are addressed early in the certification process.

These measures collectively reinforce aircraft safety, improve regulatory compliance, and ensure that both pilots and manufacturers are better prepared to handle potential safety issues before they escalate into larger crises.

Next Steps

For more information, visit the following training course: EASA Part 21 Subpart J Safety Management System Implementation – 2 Days or contact us at team@sassofia.com.

https://sassofia.com/course/easa-part-21-subpart-j-safety-management-system-implementation-2-days/