NTSB/SR-06/02

Safety Report on the Treatment of Safety-Critical Systems in Transport Airplanes

Objective of Article

- Extend the learning loop to the certification process
  - Identify process failings and recommend improvements
  - Each accident's investigation 'raised questions about the certification process used by the FAA to determine compliance with airworthiness standards'

- Highlight the need for ongoing risk-assessment to safety critical systems
  - Ensure the safety of previously certified airplanes
  - Each accident had operational incidents that foreshadowed the accidents in the investigation

Preliminary Information

- **Safety-Critical System:** ‘one where a failure condition would prevent the safe flight of the airplane, or would reduce the capability of the airplane or the crew to cope with adverse operating conditions’
- **Report Scope:** Investigate the type certification of transport category planes and the processes that the FAA uses to assess risks to safety critical systems
- **Report Topics:** Fatal accidents on four US carriers between 1994 and 2001

NTSB (National Transportation Safety Board) Background

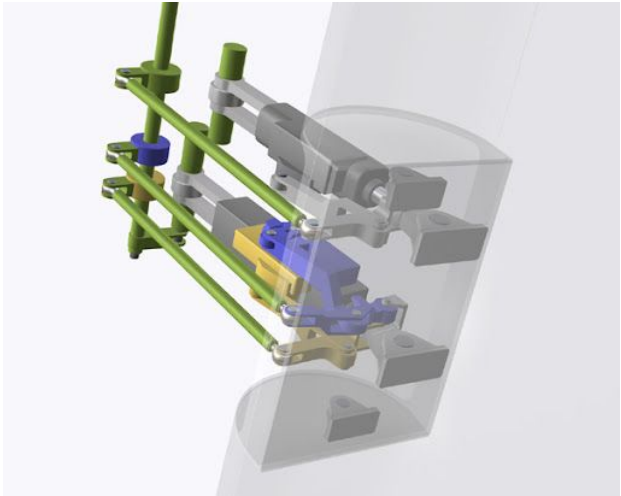
- 1967 Congress establishes NTSB as part of DOT
  - Desire for high level of safety in the transportation system
- 1974 NTSB becomes a separate entity from DOT - reports to congress
  - “No federal agency can properly perform such (investigation) functions unless it is totally separate and independent from any other” - Piper Alpha
- NTSB has no authority, only recommendations
- Congress requires DOT to respond to changes within 90 days
- Federal assistance to families of accident victims

FAA (Federal Aviation Administration)

- Goal is to provide the safest, most efficient aerospace systems in the world
- Must both promote and regulate air travel
- Criticism for being too friendly with industry
- Largest agency within the DOT
- Responsibilities include:
  - ATO - navigation services within the National Airspace System
  - AVS - aeronautical certification of aircraft and personnel
  - ARP - develop the national airport system
  - AST - protect assets during launch or re-entry
  - ASH - risk reduction of terrorism

Accident 1: USAir Flight 427

- Boeing 737-300 crashed Sep 8, 1994 after entering an uncontrolled descent while maneuvering to land at Pittsburgh International. All 132 occupants were killed.
- Jam of the main rudder power control unit servo valve



Disaster Breakdown (9:30 to 12:18)

USAir Flight 427- Accident Investigation & LL

- Pilots not able to correct for rudder reversal
- Investigation determined full rudder reversal occurred under certain flight conditions
- Failure to incorporate system redundancy into main power control unit
  - Unlike on the 757 & 767
- Accident revealed that full aileron deflection could not overcome rudder
  - Issue assumed to be fixed in 1965
- Preceding accidents concerning rudder reversal

Certification Issues/Process Improvements

- Ability of the FAA to characterize failure modes in safety-critical systems
- FAA needs to sufficiently analyze all relevant flight conditions
- The FAA needs to better integrate lessons learned
  - Safety critical systems
- Gain ability to effectively reevaluate design assumptions
  - New operational experience
  - NTSB concerned with derivative designs

Accident 2: TWA Flight 800

- July 17, 1996, Boeing 747-131 crashes into Atlantic with 230 fatalities
- Explosion in center wing fuel tank determined to be probable cause
- Short circuit outside CWT allowing voltage into tank wiring determined to be probable ignition
- Heat sources below CWT with no heat dissipation and no way to render vapor inflammable

Certification Issues

- FAA required that ignition sources be eliminated, but assumed that a flammable mixture would always exist
  - Declared fuel inerting to be cost-prohibitive
- Five aircraft were destroyed in fuel tank explosions before FAA changed its guidance to allow fuel-inerting
  - NTSB investigated Iranian Air Force ULF48 accident in 1976
- NTSB declared that current FAA accepted failure assessment needed operational experience to provide data
- Current data sources were incomplete and optimistic

TWA Flight 800 - Process Improvements

- Failure tree analysis now standard for certification
- Rules for inter-agency investigations improved
- In 2001, FAA regulations changed to require fuel tanks to have:
  - ‘Means to minimize the development of flammable vapors in the fuel tanks‘
  - ‘Means to mitigate the effects of an ignition of fuel vapors within fuel tanks such that no damage will prevent safe flight and landing’
- In 2002, the FAA developed an inerting system to be retrofitted to existing aircraft
  - Flight testing with NASA, Boeing, and Airbus indicated inerting was practical and effective

Accident 3: Alaska Airlines Flight 261

- Accident: McDonnell Douglas MD-83 crashed into the Pacific Ocean about 2.7 miles north of Anacapa Island, California on Jan 31, 2000. All 88 people on board were killed.
- Probable Cause: Loss of airplane pitch control resulting from the in-flight failure of the acme nut threads in the horizontal stabilizer trim system jackscrew assembly.
- Design Flaw: Lack of fail-safe mechanism that would prevent a total failure of the jackscrew assembly.

Disaster Breakdown (3:23-6:57)

Maintenance Issues

- The original jackscrew assembly lubrication interval recommended for the DC-9 was 300-350 flight hours.
- The initial MD-80 maintenance plan (OAMP) specified lubrication intervals of 600-900 flight hours.
- 1988: Extended to 1000 flight hours
- 1991: Extended to 1200 flight hours
- 1994: Extended to 1600 flight hours
- 1996: OAMP revised interval to 3,600 flight hours
- End play check of the jackscrew assembly was also extended to 9,550 hours from the original 7,200

Certification Issues

- MD-80 series airplanes are based on the DC-9. When the MD-80 was certified in 1980, the trim control system containing the jackscrew assembly was treated as a derivative design and assumed to comply with certification standards.
- Scenarios used for certification included a fractured acme screw, fractured torque tube, and 90% loss of acme screw and nut threads. All scenarios assumed that at least one set of acme nut and screw threads would be intact.
- Certain parts of the jackscrew assembly were defined as structural components so there was no requirement to evaluate the jackscrew assembly as a system. Structural elements and system elements were evaluated differently for certification.
- Wear of the acme nut was not considered a failure mode because the failure rate for a wear element could not be determined.

NTSB Recommendations

“Modify the certification regulations, policies, or procedures to ensure that new horizontal stabilizer trim control system designs are not certified if they have a single-point catastrophic failure mode, regardless of whether any element of that system is considered structure rather than system or is otherwise considered exempt from certification standards for systems.”

Accident 4: American Airlines Flight 587

- Airbus A-300 crashes after vertical stabilizer exposed to massive aerodynamic loading, vertical stabilizer detaches from fuselage
- Loading caused by large (over 12 degrees), cyclic rudder inputs in each direction
- Rudder inputs caused by pilot's response to wake turbulence
- Rudder intended to utilize small deflections to compensate for yaw asymmetry, rather than create such asymmetry
- Vertical stabilizer separation was considered extremely rare occurrence, however:
- Interflug Incident (1991)
- American Airlines Flight 903 (1997)

Flight 587- Certification Issues

- NTSB found that there is no regulation for consideration of alternating pedal inputs
- Suggestions for yaw damper improvements could help delay buildup of aerodynamic loads on rudder, But:
- A300-600 pedal and yaw-damper system design came with unique issues
- Multiple issues with AAMP pilot training noticed
- Existing standards for pedal force, rudder movements, and handling did not sufficiently address pilot's use of rudder at high speeds

Flight 587- Process Improvements

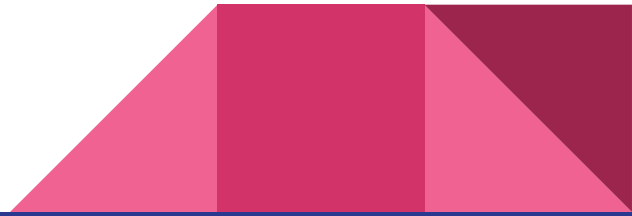
- NTSB recommended standards for yaw handling qualities
- Suggested certification standards for aircraft-pilot coupling events
- Conference held regarding AAMP training program
- Investigation concluded pilot training and rudder design were main contributors to accident
- Ensure certification standard to ensure safe handling qualities in yaw axis
- Concluded that communication between FAA, manufacturers, and operators was insufficient without a specific plan or system of action to be taken

Internal Commonalities

- Accidents caused by scenarios not considered in certification testing
- Critical failure modes in each accident had appeared in fatal or non-fatal operational incidents prior to investigation accidents
- Unpredicted human-system interactions contributing to failure

Commonalities With Previous Case Studies

- Tendency to want to blame single person or party who was at the sharp end of safety value chain
- Failure of imagination - insufficient contingency testing
- Tradeoff between production and safety



Perception of the Article

Positives

- Engineer accessible writing, easy to understand
- Logical recommendations and consistent themes (important to reputation of NTSB as an advisory body)
- Appropriate down selection of accidents
- Good use of figures to represent accident precursors

Negatives

- Missing prior accident contextual information
- Ambiguous evidence (failure to create compelling recommendation underlines purpose of NTSB)
- FAA recommendations/improvements often not quantified or explained in detail
- Lack of visual representation for aircraft system components

Delta L

- Original lack of certification data and change in certification process
- Process difference between certification for structures and systems
- Relationship and history between NTSB and FAA
- Near misses were treated as proof of safety instead of catastrophic accident precursors
- Effective communication between agencies/departments often fails without sufficient regulatory intervention