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

Safety Report

NTSB/SR-06/02

PB2006-917003
Notation 7752A

National Transportation Safety Board
Washington, D.C.

this page intentionally left blank

Safety Report

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

NTSB/SR-06/02
PB2006-917003
Notation 7752A
Adopted April 25, 2006

National Transportation Safety Board
490 L'Enfant Plaza, S.W.
Washington, D.C. 20594

National Transportation Safety Board. 2006. ***Safety Report on the Treatment of Safety-Critical Systems in Transport Airplanes.*** **Safety Report NTSB/SR-06/02. Washington, DC.**

Abstract: Certification of systems that are critical to the safety of flight has been the focus of several recently concluded National Transportation Safety Board accident investigations of transport-category airplanes: USAir flight 427 in 1999; TWA flight 800 in 2000; Alaska Airlines flight 261 in 2002; and American Airlines flight 587 in 2004. Each of these investigations raised questions about the certification process used by the FAA to determine compliance with airworthiness standards.

The purpose of this safety report is to discuss the concerns about certification raised in those investigations and to identify process improvements to FAA's type certification of safety-critical systems in transport-category airplanes. The report includes three recommendations in two areas. The first area concerns the ways in which hazards to safety of flight are identified, assessed, and documented during the type certification process. The Safety Board's analysis considered how compliance with Federal regulations is demonstrated and how the safety assessment effort is documented. Of particular concern were assessments of safety-critical systems that do not include certain structural failure conditions and human/system interaction failures.

The second area focused on the ongoing assessment of safety-critical systems throughout the life of the airplane. The Board concluded that a program must be in place, once the type certification process is completed, to ensure the ongoing assessment of risks to safety-critical systems. Such a program must recognize that ongoing decisions about design, operations, maintenance, and continued airworthiness must be done in light of operational data, service history, lessons learned, and new knowledge, for designs that are derivatives of previously certificated airplanes.

Contents

Appendixes

Acronyms and Abbreviations

AAI	Office of Accident Investigation
AAM	Office of Aerospace Medicine
AAMP	Advanced Aircraft Maneuvering Program
AC	advisory circular
ACE-100	Small Airplane Directorate
ACO	Aircraft Certification Office
ACSEP	Aircraft Certification Evaluation System
AD	airworthiness directive
AEG	Aircraft Evaluation Group
AFS	Flight Standards
AIR	Aircraft Certification Service
ANM-100	Transport Airplane Directorate
APC	aircraft-pilot coupling
ARAC	Aviation Rulemaking Advisory Committee
ATM	air traffic management
ATOS	Air Transportation Oversight System
AVS	Associate Administrator for Aviation Safety
CDR	critical design review
CFR	*Code of Federal Regulations*
CIR	conformity inspection report
CM	Condition Monitoring
CMT	Certificate Management Team
CNS	communications, navigation, surveillance
CPS	Commercial Airplane Certification Process Study
CMR	Certification Maintenance Requirement
CWT	center wing fuel tank
DAR	Designated Airworthiness Representative
DER	Designated Engineering Representative
DMIR	Designated Manufacturing Inspection Representative
DoD	Department of Defense
DODD	Department of Defense Directive
DODI	DoD Instruction

EASA	European Aviation Safety Authority
ETEB	Flight Control Engineering Test and Evaluation Board
ETOPS	Extended-Range Twin-Engine Operations
FAA	Federal Aviation Administration
FAR	Federal Aviation Regulation
FDR	flight data recorder
FHA	functional hazard assessment
FMEA	failure modes and effects analysis
FMES	failure modes and effects summary
FOEB	Flight Operations Evaluation Board
FSB	Flight Standardization Board
FTA	fault tree analysis
FTA	Federal Transit Administration
GAO	General Accounting Office
HRA	human reliability analysis
HT	Hardtime
ICA	instructions for continued airworthiness
ISC	industry steering committee
JAA	Joint Aviation Authority
JAR	Joint Aviation Requirement
MED	multiple element damage
MRB	Maintenance Review Board
MSD	multiple site damage
MSG	Maintenance Steering Group
NAS	National Airspace System
NASA	National Aeronautics and Space Administration
NPRM	Notice of Proposed Rule-Making
NRC	National Research Council
NRC	Nuclear Regulatory Commission
NRS	national resource specialist
OAMP	On-Aircraft Maintenance Planning
OC	On-Condition
PCU	power control unit
PM	project manager
PO	project officer
PPH	policy and procedures handbook

PRA	probabilistic risk assessment
PSCP	Project Specific Certification Plan
PSE	principal structural element
PSP	Partnership for Safety Plan
PSSA	preliminary system safety assessment
SAE	Society of Automotive Engineers
SCR	special certification review
SSI	Structural Significant Item
TC	type certificate
TCB	Type Certification Board
TCDS	Type Certificate Data Sheet
TIA	Type Inspection Authorization
TIR	Type Inspection Report
V_A	design maneuvering speed
WG	working group

Executive Summary

Certification of systems that are critical to the safety of flight has been the focus of several recently completed National Transportation Safety Board accident investigations of transport-category airplanes: the rudder actuator in USAir flight 427 in 1999; the center wing fuel tank in TWA flight 800 in 2000; the horizontal stabilizer jackscrew in Alaska Airlines flight 261 in 2002; and the rudder system in American Airlines flight 587 in 2004. Each of these investigations raised questions about the certification process used by the FAA to determine compliance with airworthiness standards.

The purpose of this safety report is to discuss the concerns about certification raised in those investigations and to identify process improvements to FAA's type certification of safety-critical systems in transport-category airplanes. The Safety Board recognizes that the findings in this report are presented during one of the safest periods in commercial aviation history and acknowledges that FAA's certification process has contributed significantly to that level of safety. However, the Board notes that there is room for improvement.

The report includes three recommendations in two areas. The first area concerns the ways in which hazards to safety of flight are identified, assessed, and documented during the type certification process. The Safety Board's analysis considered how compliance with Federal regulations is demonstrated and how the safety assessment effort is documented. Of particular concern were assessments of safety-critical systems that do not include certain structural failure conditions and human/system interaction failures.

The second area focuses on the ongoing assessment of safety-critical systems throughout the life of the airplane. The Board concluded that a program must be in place, once the type certification process is completed, to ensure the ongoing assessment of risks to safety-critical systems. Such a program must recognize that ongoing decisions about design, operations, maintenance, and continued airworthiness must be done in light of operational data, service history, lessons learned, and new knowledge, for designs that are derivatives of previously certificated airplanes.

Introduction

Certification of systems that are critical to the safety of flight has been the focus of several recently completed National Transportation Safety Board accident investigations of transport-category airplanes. In 1999, the Safety Board expressed concern about the Federal Aviation Administration's (FAA) certification process during its investigation of the rudder actuator in USAir flight 427.[1] In 2000, the Board suggested the need for a directed examination of the certification process in the investigation of the center wing fuel tank in TWA flight 800.[2] Subsequent investigations of the horizontal stabilizer jackscrew in Alaska Airlines flight 261[3] and the rudder system in American Airlines flight 587[4] also raised questions about the certification process used by the FAA to determine compliance with airworthiness standards. These four accidents resulted in 715 fatalities and accounted for 60 percent of the air carrier fatalities that occurred from 1994–2001.[5]

The purpose of this report is to discuss those concerns in more detail and to identify possible improvements to FAA's certification process for safety-critical systems in transport-category airplanes.[6] The seriousness of the four accidents listed above, in which critical systems suffered catastrophic failure, prompted the Safety Board to undertake this directed examination of the processes used by the FAA to assess safety-critical systems. The Board recognizes that the findings in this report are presented during one of the safest periods in commercial aviation history and acknowledges that FAA's certification process has contributed significantly to that level of safety. The Board believes, however, that these four major aviation accidents, when considered together, can in hindsight illustrate where process improvements can be made.

---

[1] *Uncontrolled Descent and Collision with Terrain, USAir Flight 427, Boeing 737-300, N513AU Near Aliquippa, Pennsylvania, September 8, 1994,* Aircraft Accident Report NTSB/AAR-99/01 (Washington, DC: National Transportation Safety Board, 1999), p. 281. As a result of this investigation, the Safety Board revised its report of the United Airlines flight 585 accident.

[2] *In-flight Breakup Over the Atlantic Ocean, Trans World Airlines Flight 800, Boeing 747-131, N93119, Near East Moriches, New York, July 17, 1996,* Aircraft Accident Report NTSB/AAR-00/03 (Washington, DC: National Transportation Safety Board, 2000), p. 298.

[3] *Loss of Control and Impact with Pacific Ocean, Alaska Airlines Flight 261, McDonnell Douglas MD-83, N963AS, About 2.7 Miles North of Anacapa Island, California, January 31, 2000,* Aircraft Accident Report NTSB/AAR-02/01 (Washington, DC: National Transportation Safety Board, 2002).

[4] *In-Flight Separation of Vertical Stabilizer, American Airlines Flight 587, Airbus Industrie A300-605R, N14053, Belle Harbor, New York, November 12, 2001,* Aircraft Accident Report NTSB/AAR-04/04 (Washington, DC: National Transportation Safety Board, October 26, 2004).

[5] The airplanes involved in these four accidents operate under the authority of 14 CFR Part 121, which specifies the operating requirements for domestic, flag, and supplemental air carrier operations. From 1994–2001, 24 fatal Part 121 accidents resulted in 1,166 fatalities, excluding the events of September 11, 2001.

[6] A transport-category airplane is defined in Federal Aviation Regulations as all jets with 10 or more seats or greater than 12,500-pound Maximum Takeoff Weight, and all propeller driven airplanes with greater than 19 seats or greater than 19,000-pound Maximum Takeoff Weight. The definition of a transport-category airplane is provided by the FAA at <http://www.faa.gov/aircraft/air_cert/design_approvals/transport/>.

The Safety Board limited the scope of this report to the type certification of transport-category airplanes and the processes that the FAA uses to assess risks to safety-critical systems. The Board found that the FAA's type certification process is sound and produces a high level of safety, but improvements are warranted for the following reasons:

1. The process for assessing risks to aircraft systems does not adequately address important failure conditions associated with structures and with human/system interaction.
2. The results of the process for assessing risks to safety-critical systems are not adequately preserved to support continued airworthiness of certificated airplanes.
3. Existing policy, practices, and procedures for the ongoing assessment of risks to safety-critical systems do not ensure that the underlying assumptions made during design and certification are adequately and continuously assessed in light of operational experience, lessons learned, and new knowledge.

Consequently, this report includes recommendations, in two areas, for improvements in type certification and the treatment of safety-critical systems. The first area concerns the ways in which hazards[7] to safety of flight are identified, assessed, and documented during the type certification process. The Safety Board's analysis considers the ways in which compliance with federal regulations is demonstrated and how the safety assessment effort is documented. Of particular concern are assessments of safety-critical systems that do not include certain structural failure conditions and human/system interaction failures.

The second area focuses on the monitoring and ongoing assessment of safety-critical systems throughout the life of the airplane. Once hazards to safety of flight have been identified, assessed, and eliminated or controlled during certification, a program must be in place to ensure continued airworthiness and the ongoing assessment of risks to safety-critical systems. Such a program can recognize that the certification process can change throughout the life of an airplane and that ongoing decisions about design, operations, maintenance, and continued airworthiness must be done in light of operational data, service history, lessons learned, and new knowledge. This is especially true for airplane designs that were certificated many years before any changes in the certification process occurred. To that end, this report also considers the relationship between the FAA's Aircraft Certification Service (AIR) and Flight Standards (AFS).

The safety assessment process, which is governed by 14 *Code of Federal Regulations* (CFR) 25.1309, "Equipment, Systems, and Installations," and described in FAA Advisory Circular (AC) 25.1309-1A, *System Design and Analysis*, is used during

[7] This report uses U.S. Department of Transportation, Federal Aviation Administration Order 8040.4, *Safety Risk Management,* Appendix 1, to define a *hazard* as a condition, event, or circumstance that could lead to or contribute to an unplanned or undesired event. This definition is also consistent with U.S. Department of Defense *Standard Practice for System Safety*, MIL-STD-882D, which defines a hazard as "any real or potential condition that can cause injury, illness, or death to personnel; damage to or loss of a system, equipment or property; or damage to the environment."

certification to identify and analyze safety-critical functions performed by systems. It is worth noting that neither certification regulations nor advisory materials provide a list of safety-critical functions or the systems associated with them, nor do they explicitly define the term "safety-critical."[8] As this report will show, the criticality of systems is determined during type certification through a safety assessment process that evaluates "the effects on safety of foreseeable failures or other events, such as errors or external circumstances, separately or in combination, involving one or more system functions."[9] This is the position taken by the FAA in its most recent policy on the identification and evaluation of "flight critical system components"[10] and is consistent with industry practice for assessing the criticality of hazards to safety of flight.[11] For the sake of clarity, this report employs the following working definition: a safety-critical system is one where a failure condition[12] would prevent the safe flight of the airplane, or would reduce the capability of the airplane or the ability of the crew to cope with adverse operating conditions. This definition focuses on the severity of a failure condition and how that failure affects the functional capability of the overall airplane system—a definition that is consistent with FAA regulations and advisory materials,[13] FAA system safety guidelines,[14] Department of Defense (DoD) system safety standards,[15] and industry-recommended practice.[16]

[8] U.S. Department of Transportation, Federal Aviation Administration Advisory Circular (AC) 25.1309-1A, *System Design and Analysis*, June 21, 1988, refers only to "safety-critical functions" without defining them.

[9] AC 25.1309-1A, *System Design and Analysis*, June 21, 1988, paragraph 7a.

[10] U.S. Department of Transportation, Federal Aviation Administration Memorandum ANM-03-117-10 *Identification of Flight Critical System Components*, July 24, 2003.

[11] *Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment,* Society of Automotive Engineers (SAE) ARP4761 (Warrendale, PA: Society of Automotive Engineers, 1996).

[12] AC 25.1309-1A, paragraph 6, defines a *failure condition* as the "effects on the airplane and its occupants, both direct and consequential, caused or contributed to by one or more failures, considering relevant adverse operational or environment conditions." A *failure* is a "loss of function, or a malfunction, of a system or a part thereof."

[13] As referenced in 14 CFR 25.1309*,* and as defined in AC 25.1309-1A.

[14] *System Safety Handbook: Practices and Guidelines for Conducting System Safety Engineering and Management* (Washington, DC: Federal Aviation Administration, 2000).

[15] U.S. Department of Defense, MIL-STD-882D, *Standard Practice for System Safety*, Appendix A, paragraph A.3.2.10.

[16] *Safety Assessment of Transport Airplanes in Commercial Service* SAE ARP5150 (Warrendale, Pennsylvania: Society of Automotive Engineers, 2003) and SAE ARP4761.

Type certification is a regulatory process that the FAA uses to ensure that the design of a transport-category airplane meets applicable safety standards. Safety standards are embodied in Federal Aviation Regulations (FARs),[17] with associated guidance provided in directives[18] and advisory circulars.[19] Unlike engineering design that must balance potentially conflicting safety, cost, schedule, performance, aesthetic, and manufacturing elements of a design, certification focuses on a single aspect of the design—safety—to ensure that it meets the minimum standards established by law. The Safety Board recognizes that issuing a type certificate (TC) is just one of the first steps in the life of a transport-category airplane, and any recommended changes to the type certification process may have significant implications for operations and for maintenance. Although this report focuses on type certification, the analysis considers safety-critical systems within the overall context of the life cycle of the airplane.

This report is organized as follows:

- A review of selected major accident investigations to illustrate the role of certification in identifying, evaluating, and tracking safety-critical systems.
- An examination of the type certification process, specifically emphasizing methods and techniques used during certification to assess safety-critical systems.
- A review of other FAA certification process studies, noting parallels between Safety Board findings and the results of those studies.
- An analysis of key certification concerns and relevant issues, with conclusions and recommendations.

The four accident case studies discussed in the next section provide an accident investigation context for the Safety Board's concerns about type certification. In each of these accidents, the Board identified a specific safety-critical system and the failure modes

[17] As stated in U.S. Department of Transportation, Federal Aviation Administration Order 8100.5A, *Aircraft Certification Service: Mission, Responsibilities, Relationships, and Programs*, September 30, 2003, paragraph 4.1:

> AVIATION REGULATIONS are in 14 CFR. These regulations set the minimum requirements for certification and alteration of civil aviation products and other appliances, and for the approval of FAA designees.

[18] As stated in FAA Order 8100.5A, paragraph 4.2:

> DIRECTIVES are comprised of FAA orders and notices. The FAA staff develops directives for FAA personnel, designees, and delegated organizations. Directives transmit information, guidance, policy, instructions, and mandatory procedures for AIR to carry out its mission. Directives are internal, intended for FAA employees. Notices transmit similar information as orders and are for internal FAA use. Unlike orders, which remain in force until canceled, notices expire 1 year after they are issued.

[19] As stated in FAA Order 8100.5A, paragraph 4.3:

> ADVISORY CIRCULARS (AC) are written for the aviation industry (such as manufacturers, designers, and installers), FAA customers, and the public. ACs show an acceptable way, but not the only way, for the reader to comply with a certification requirement or set of certification requirements. ACs may also show how to comply with a regulation, or how to harmonize implementation for the international aviation community. ACs do not have the force of regulations.

that resulted in the catastrophic loss of that system, recommended design reviews of that system, and called for FAA action to ensure that any changes to the design, operational procedures, or maintenance practices were implemented. This report uses these four accidents to examine specific aspects of FAA's type certification process and includes selected facts, analyses, conclusions, and recommendations from the accident investigations as they were presented in the original Board aircraft accident reports, which are available on the Safety Board's website at <www.ntsb.gov/Publictn/A_Acc1.htm)>.

Certification Issues in Accident Investigation

The feasibility of using an accident-based, data-driven methodology was considered in the planned approach to this report. A set of candidate accidents was derived from worldwide accident investigation records from 1962–2001. Initially, staff talked with investigators and engineers to identify a candidate list of aircraft-related accidents. The Safety Board's Office of Aviation Safety (AS) reviewed this list to confirm that the accidents were good candidates for researching certification issues. Board accident records and those of other investigative organizations were analyzed for potential certification issues. The 55 accidents listed in Appendix C were then identified and categorized in terms of the aircraft component or system that failed. Because information about certification was not routinely collected during many of these investigations, a statistical treatment of accident-related certification issues was not possible. However, the four accidents reviewed in the following sections provided the extensive documentation needed to address certification-related issues, and are used to support a case study analysis of the issue.

USAir Flight 427

On September 8, 1994, a Boeing 737-300 being operated as USAir flight 427 entered an uncontrolled descent while maneuvering to land at Pittsburgh International and crashed into hilly, wooded terrain about 6 miles northwest of the airport. The airplane was destroyed by impact forces and fire and all 132 occupants were killed. After a lengthy investigation, the Safety Board determined the probable cause of the accident as follows:

> A loss of control of the airplane resulting from the movement of the rudder to its blowdown limit. The rudder surface most likely deflected in a direction opposite to that commanded by the pilots as a result of a jam of the main rudder power control unit servo valve secondary slide to the servo valve housing offset from its neutral position and overtravel of the primary slide.[20]

The investigation also discovered that when a full rudder reversal occurred under certain flight conditions (flaps 1 position[21] and airspeed below 187 knots), pilots would not be able to stop the subsequent roll with full deflection of the ailerons.[22]

In its final report on USAir flight 427, issued in 1999, the Safety Board found that "the dual-concentric servo valve used in all Boeing 737 main rudder power control units is not reliably redundant."[23] The main rudder power control unit (PCU) operates by converting

[20] USAir flight 427, NTSB/AAR-99/01, p. 295.

[21] By selecting the flaps 1 position, the flaps are fully extended and the trailing edge moves down 1 degree.

[22] USAir flight 427, NTSB/AAR-99/01, p. 63-64.

[23] USAir flight 427, NTSB/AAR-99/01, p. 294.

either a mechanical input from the rudder pedals or by an electrical signal from the yaw damper system into motion of the rudder. The PCU moves the rudder when actuated by rudder pedal or trim inputs or by an electrical signal from the yaw damper. The 737 PCU servo valve is a dual-concentric tandem valve composed of a primary slide that moves within a secondary slide, which in turn moves within the servo valve housing. When rudder motion is commanded, the internal input shaft moves the servo slides so that the rudder system hydraulic circuits are connected and the flow of hydraulic fluid moves the rudder.[24] The 737 is the only twin-engine, transport-category airplane with wing-mounted engines that is designed with a single panel rudder controlled by a single actuator. Both the Boeing 757 and the 767 use three independent, redundant actuators that do not rely on dual concentric servo valves. The 757 and 767 design allows pilot input to overpower a failed or jammed actuator valve and eliminates the possibility of the failed PCU controlling the movement of a flight surface.

Early in the design and certification of the rudder servo valve, two potential problems were identified and corrected: the potential for a jammed servo valve to lead to a malfunction of the rudder control system and the potential for a reversal of hydraulic fluid flow in the servo valve. (A timeline of significant events discussed in the investigation is shown in figure 1.)

The first problem, the potential for a jam in the servo valve, was addressed during the certification of the Boeing 737-100 and -200 series airplanes in 1965. At that time, FAA certification personnel raised questions about the redundancy of the single panel, power-activated rudder design.[25] Boeing responded that the servo valve assembly would accommodate a single jam without loss of control because, if either slide in the servo jammed, the other slide would still move and connect the proper flow paths. Additional Boeing analysis showed that aileron roll control authority exceeded rudder control authority at all rudder angles, implying that any roll resulting from a jammed servo unit could be countered with aileron input. Not until 1995, during the USAir flight 427 investigation, did testing reveal that full deflection of the ailerons could not overcome the roll generated by full deflection of the rudder if airspeed was below 187 knots with the airplane in the flaps 1 position.

The second problem, the potential for a reversal of hydraulic fluid flow in the servo valve, was detected in a prototype of the 737 and was corrected in 1966; engineering documents from that year revealed that changes were made to the prototype to "insure accumulated tolerances will not cause reverse flow"[26] and to remove the potential for secondary slide overtravel. In 1999, Parker Hannefin stated in its letter to the Safety Board that "reverse flow" referred to cross-flow or higher-than-desirable internal leakage in the servo valve and was not related to a reversal in the dual-concentric valve.[27] For both problems, the FAA accepted the solutions that were incorporated into the design during certification.

---

[24] A detailed explanation of the main rudder PCU and servo valve design and operation can be found in USAir flight 427, NTSB/AAR-99/01, pp. 29-33.

[25] USAir flight 427, NTSB/AAR-99/01, p. 164.

[26] USAir flight 427, NTSB/AAR-99/01, p. 32.

[27] USAir flight 427, NTSB/AAR-99/01, p. 32.

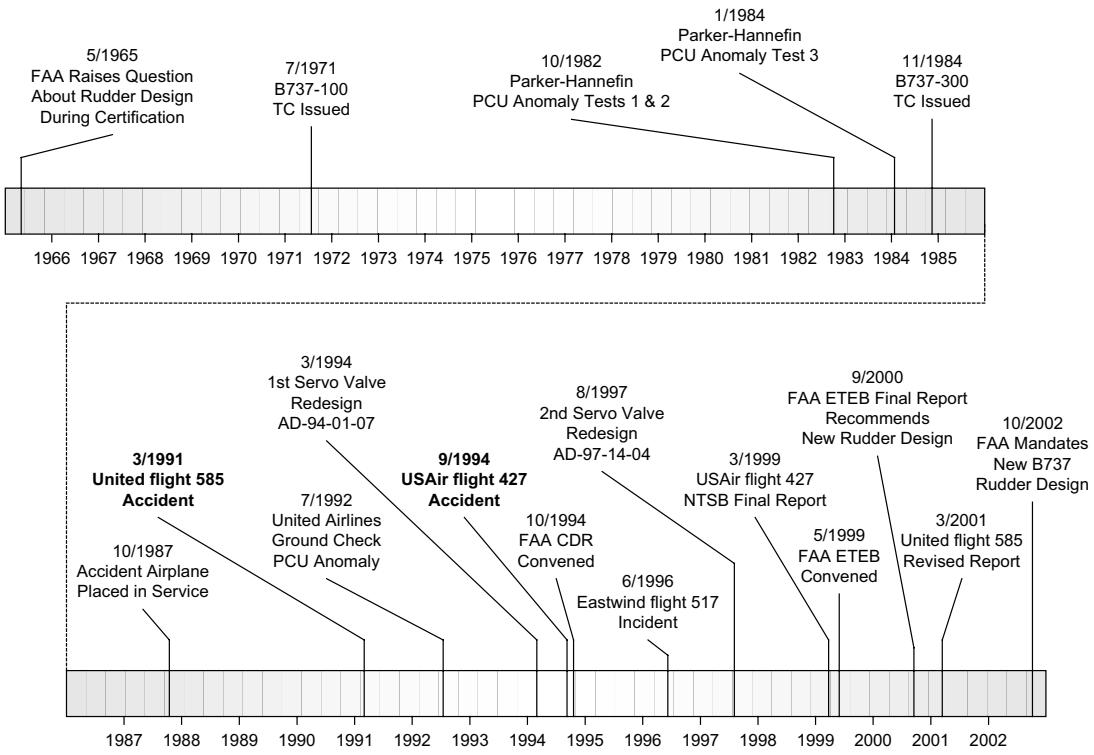

Figure 1. Chronology of Significant Events Discussed in USAir flight 427 Investigation

When simulator tests of various flight control and system failure scenarios were conducted in 1994, only a rudder hardover scenario produced results consistent with data obtained from the USAir flight 427 flight data recorder (FDR). This result prompted additional investigation of rudder hardover scenarios and focused attention on the PCU. Evidence that implicated the servo valve was not obtained until almost 2 years later in 1996 when thermal tests of the PCU—where hot hydraulic fluid was injected into a cold PCU—showed that the secondary slide in the servo unit could jam and that subsequent overtravel of the primary slide could result in an increased system return flow that could cause a rudder actuator reversal.[28]

Several 737 rudder incidents came to light during the USAir flight 427 investigation. In June 1996, Eastwind flight 517 experienced a yaw/roll upset at 4,000 feet during its approach to land at the Richmond, Virginia, airport. The airplane yawed abruptly to the right and then rolled to the right. The captain, who was flying the airplane, reported applying immediate full left rudder and aileron input, and that the rudder pedal felt stiff and did not respond as normal. The captain had to advance the right throttle to obtain differential power to stop the rolling tendency of the airplane. The upset event ended when the crew performed the emergency checklist and disconnected the yaw damper. Review of the airplane's logbook records showed a series of flight crew-reported

[28] USAir flight 427, NTSB/AAR-99/01, p. 80.

rudder-related anomalies,[29] and a review of the incident airplane's rudder system components revealed several anomalous conditions.[30] The final report for the USAir flight 427 investigation also documented a number of related incidents that occurred from 1974 to 1995, including servo slide jams due to debris and corrosion, insufficient lock nut torque, and a PCU anomaly and jam when tested at colder temperatures under hydraulic pressure.[31]

Another incident of note was the rudder reversal and rudder jam during ground operations of a 737 in 1992.[32] During a preflight rudder control ground check at Chicago-O'Hare International Airport, the captain of a United Airlines 737-300 reported that the left rudder pedal stopped and jammed at about 25 percent pedal travel. The captain reported that he had been moving the rudder pedals back and forth rapidly, and when he removed foot pressure from the left pedal, it returned to a neutral position. The PCU was removed from the aircraft, and subsequent testing showed that the secondary slide could move beyond its design limits, allowing an abnormal flow that would produce a rudder reversal. These results suggested that the problem of accumulated tolerances identified in the original prototype was still evident. In November 1992, the Safety Board recommended a design review of the dual-concentric servo valves with a design similar to the 737, and design changes of the servo valve that would preclude the possibility of rudder reversals attributed to the overtravel of the secondary slide.[33]

In light of this evidence, the FAA issued Airworthiness Directive (AD) 94-01-07 in March 1994 aimed at the overtravel problem. The AD established new inspection criteria for main rudder PCUs and required installation of the redesigned servo valve in all 737s within the next 5 years. The servo valve was redesigned again in 1996 after the Safety Board's USAir flight 427 PCU tests revealed the potential for primary valve overtravel if the secondary slide jammed. However, in 1998 this new servo valve was found to suffer from cracking problems and was associated with two in-flight rudder anomalies in 1999.

In its final report on USAir flight 427, the Safety Board concluded that redundancy in the dual-concentric servo valve design in existing Boeing 737 main rudder PCUs was compromised for the following reasons: no method existed for the pilot to reliably detect the presence of a jammed primary or secondary slide within the servo valve; the dual-concentric servo valve design allowed for failure modes in which one slide could affect the operation of the other slide; recent design changes did not eliminate the possibility that a maintenance error could result in a servo valve anomaly; and the dual load path provided structural redundancy, but not functional redundancy. The Board also pointed out that

[29] USAir flight 427, NTSB/AAR-99/01, p. 263.

[30] USAir flight 427, NTSB/AAR-99/01, p. 264. Evidence included a misadjusted yaw damper and chafed wiring between the yaw damper coupling and the main rudder PCU. Examination of the PCU also revealed similarities to the USAir flight 427 servo valve, including relatively tight clearances that are more likely to jam.

[31] USAir flight 427, NTSB/AAR-99/01, pp. 148-157.

[32] USAir flight 427, NTSB/AAR-99/01, pp. 152-154.

[33] NTSB Safety Recommendations A-92-120 and 121; full text and status are shown in Appendix D.

during certification of the Boeing 737-100 series, the FAA had expressed concern about the airplane's single-panel, single-actuator rudder system and "recognized the possibility of undetected latent failures in the servo valve, thereby negating the system's redundancy." The Board went on to state that "the rudder system's history of service difficulties (some of which still remain unresolved), particularly the servo valve's history of jamming, validates those concerns."[34]

In 1999, just 2 months after the Safety Board issued its final report on USAir flight 427, the FAA established the government/industry Boeing 737 Flight Control Engineering Test and Evaluation Board (ETEB). The ETEB was formed in response to Safety Board Recommendation A-99-21 to the FAA, which was issued as a result of the USAir flight 427 investigation:

> Conduct a failure analysis to identify potential failure modes, a component and subsystem test to isolate particular failure modes found during the failure analysis, and a full-scale integrated systems test of the Boeing 737 rudder actuation and control system to identify potential latent failures and validate operation of the system without regard to minimum certification standards and requirements in Title 14 of the Code of Federal Regulations (14 CFR) part 25.[35]

The ETEB conducted a comprehensive analysis of the Boeing 737 rudder system and found multiple failure modes. As a result of its analysis, the ETEB issued a final report in September 2000 recommending the redesign and retrofit of a new rudder control system. The Safety Board's response to the ETEB proposal was favorable in that the result was consistent with investigative findings.[36]

The investigation of USAir flight 427 also prompted the Safety Board to reconsider the conclusions of a similar Boeing 737 accident. On March 3, 1991, United Airlines flight 585 crashed while maneuvering to land at Colorado Springs, Colorado, killing all 25 people onboard. The final report issued by the Board on December 8, 1992, concluded that it "could not identify conclusive evidence to explain the loss of United Airlines flight 585." In light of the investigative work on USAir flight 427, the Board reexamined evidence for the flight 585 accident, issued an updated final report in March 2001, and concluded that a rudder reversal was caused by the jam of the rudder servo unit.

Certification Issues

The Safety Board believes that the investigations of USAir flight 427 and United flight 585 provide insights into a number of certification issues. First, the Board is concerned that the ability to completely characterize failure modes in a safety-critical system during certification may be compromised by incomplete or inadequate engineering analysis. The USAir flight 427 investigation, the FAA's critical design review (CDR)

---

[34] USAir flight 427, NTSB/AAR-99/01, p. 279.

[35] Full text and status of this recommendation are shown in Appendix D.

[36] *Statement of NTSB Chairman Jim Hall on FAA Release of ETEB Study on 737 Rudders*, NTSB Advisory (Washington, DC: September 14, 2000).

team,[37] and the ETEB devoted considerable effort to identifying potential single and multiple failures, failure scenarios and malfunctions, and potentially hazardous latent failures in the rudder control system. The multiple failure modes found by the ETEB in its analysis indicated that the engineering analysis that was accepted by the FAA during the original certification process may not have completely characterized all of the significant failure modes in the rudder control system. The CDR team also concluded that the assumptions made by the manufacturer during certification about roll control using ailerons were not based on sufficient analysis of all relevant flight conditions, and that the potential for latent design failures in flight control systems (such as jamming of servo valves) was great enough that "the alternate means of control, the lateral control system, must be fully available and powerful enough to rapidly counter the rudder and prevent entrance into a hazardous flight condition."[38]

The USAir flight 427 investigation also highlighted the need to better integrate lessons learned and operational data into the assessment of safety-critical systems throughout the life of the airplane. The FAA had expressed concerns about the rudder system during certification of the Boeing 737-100, and the history of rudder service difficulties led the Safety Board to conclude that those concerns were valid. The USAir flight 427 investigation also indicated that the certification process had to be more responsive to the lessons learned from operational experience with an airplane.[39] The ability to effectively reevaluate design assumptions using operational experience would also help alleviate the Board's concerns with derivative designs. Although regulations govern the approval of changes to a TC, the results of the USAir flight 427 investigation suggest that the approval process for derivative designs may not consider issues raised during previous certification activities. Once the FAA issued the original Boeing 737 type certificate in 1967, the opportunities to reconsider the design of the rudder servo unit or the validity of the assumptions underlying the original design, in light of operational experience, were limited. Finally, the Safety Board believes that the need to better integrate lessons learned into the assessment of safety-critical systems illustrates areas in which the relationships between design and operations could be improved.

TWA Flight 800

On July 17, 1996, TWA flight 800, a Boeing 747-131, crashed into the Atlantic Ocean near East Moriches, New York, after departing John F. Kennedy International Airport on a scheduled flight to Charles DeGaulle International Airport, Paris, France. All 230

[37] The FAA began a CDR of the Boeing 737 flight control systems with emphasis on roll control and directional flight control systems in October 1994. This review also considered failure events in flight control systems that could result in an uncommanded deflection or jam of a flight control surface. See *B737 Flight Control System Critical Design Review* (Washington, DC: Federal Aviation Administration, May 3, 1995) for more details.

[38] *B737 Flight Control System Critical Design Review*, p. 16.

[39] Regulations place reporting requirements on both manufacturers and operators for failures, malfunctions, and defects. Title 14 CFR 21.3 applies to manufacturers, and 14 CFR 121.703-705 applies to operators.

people on board were killed and the airplane was destroyed. The Safety Board determined that the probable cause of the TWA flight 800 accident was—

> an explosion of the center wing fuel tank (CWT), resulting from ignition of the flammable fuel/air mixture in the tank. The source of ignition energy for the explosion could not be determined with certainty, but, of the sources evaluated by the investigation, the most likely was a short circuit outside of the CWT that allowed excessive voltage to enter it through electrical wiring associated with the fuel quantity indication system.

The Safety Board went on to state the following:

> Contributing factors to the accident were the design and certification concept that fuel tank explosions could be prevented solely by precluding all ignition sources and the design and certification of the Boeing 747 with heat sources located beneath the CWT with no means to reduce the heat transferred into the CWT or to render the fuel vapor in the tank nonflammable.[40]

A timeline of significant events discussed in the TWA flight 800 investigation is shown in figure 2.

The Safety Board's concerns with certification of the Boeing 747 fuel tanks were stated in recommendations A-96-174 and -175 issued in 1996[41] before the investigation was completed. These recommendations requested design and operational changes that would reduce the potential for flammable fuel/air mixtures in airplane fuel tanks. In the letter accompanying the recommendations, the Board stated "that the existence of a flammable fuel/air mixture in transport-category airplane fuel tanks was inconsistent with the basic tenet of transport-aircraft design that no single-point failure should prevent continued safe flight and landing."[42] The basic tenet referred to in the letter is the fail-safe design concept incorporated in transport-category airworthiness standards. The elimination of flammable fuel/air vapors in fuel tanks on transport-category airplanes was considered of such high importance that recommendations A-96-174 and A-96-175 were included on the Board's Most Wanted List.[43] In November 2005, A-96-175 was classified Closed—Unacceptable Response and removed from the Most Wanted List while A-96-174 was retained and classified Open—Acceptable Response due to the progress being made in the development and testing of fuel inerting technologies.

---

[40] TWA flight 800, NTSB/AAR-00/03, p. 308.

[41] Full text and status of these recommendations are shown in Appendix D.

[42] TWA flight 800, NTSB/AAR-00/03, p. 299.

[43] The Most Wanted List is a Safety Board transportation safety improvement program to increase the public's awareness of, and support of, action to adopt safety steps that can help prevent accidents and save lives. The list of recommendations can be found at <www.ntsb.gov/Recs/mostwanted/index.htm>.

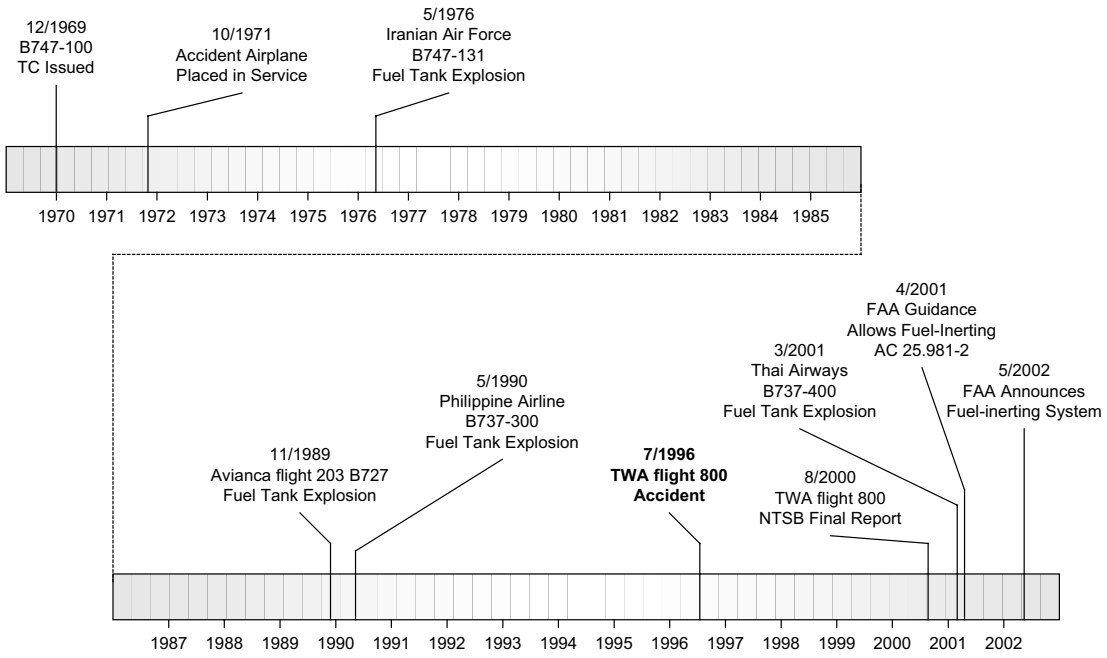

Figure 2. Chronology of Significant Events Discussed in TWA flight 800 Investigation

The Safety Board's concern with certification in the TWA flight 800 investigation was also reflected in the November 1996 request to Boeing to produce a fault tree analysis of CWT ignition failure modes for use in the investigation and in the July 1998 request for the National Aeronautics and Space Administration (NASA) to review the Boeing analysis. A fault tree analysis is one of the techniques currently used during certification to demonstrate compliance with Federal regulations, but was not required when the 747 was certified. Board and NASA reviews of the analysis indicated that the exposure times and failure rates appeared to be too low for some events, resulting in overly optimistic probability data. Problems in the analysis raised concerns that "similarly questionable data may have been used to develop other fault tree analyses that have been submitted to and accepted by the FAA in connection with aircraft certifications."[44] Contributing to the possibility that fault tree analyses could be based on inaccurate data is the fact that the Board investigation found no single source for reliable and comprehensive data on component failures or malfunctions. Because the calculations in an analysis can be based on failure rates, incomplete or inappropriate failure data can significantly skew the results. The Board pointed out in its investigation that there were various sources of such information (including data collected and maintained by manufacturers from operators, and the FAA's Service Difficulty Report program), but that the data were incomplete.

In its recommendations, the Safety Board urged the FAA to develop and to implement design or operational changes that would "preclude the operation of

[44] TWA flight 800, NTSB/AAR-00/03, p. 296.

transport-category airplanes with explosive fuel/air mixtures in the fuel tanks."[45] In 1997, the FAA responded by stating that the airworthiness standards of 14 CFR Part 25 always assume that combustible fuel vapor is present in an aircraft's fuel system, and design requirements dictate elimination of ignition sources.[46] According to the FAA, control of the flammability characteristics of fuel tank contents (as recommended by the Safety Board) would be a major change in design philosophy, and the use of fuel-inerting technologies was cost prohibitive. A 1998 FAA Aviation Rulemaking Advisory Committee (ARAC) estimated the cost to be greater than $20 billion. In 1999, the FAA initiated rulemaking changes to the regulations governing certification of airplane fuel tanks. The Safety Board discussed the proposed changes in the final report on TWA flight 800:

> For purposes of certification, the FAA and the transport-category airplane manufacturers have historically assumed that a flammable fuel/air mixture exists in fuel tanks at all times and have attempted to preclude fuel tank explosions by eliminating ignition sources in fuel tanks.[47]

The Safety Board then went on to state its disagreement with this design philosophy, and concluded the following:

> A fuel tank design and certification philosophy that relies solely on the elimination of all ignition sources, while accepting the existence of fuel tank flammability, is fundamentally flawed because experience has demonstrated that all possible ignition sources cannot be predicted and reliably eliminated.[48]

After much discussion of the Safety Board recommendations, changes in Federal regulations regarding transport-category airplane fuel tank design and certification were made. The latest version of 14 CFR 25.981, paragraph c, "Fuel Tank Ignition Prevention," issued in 2001, states that the installation of a fuel tank must include the following:

1. Means to minimize the development of flammable vapors in the fuel tanks (in the context of this rule, "minimize" means to incorporate practicable design methods to reduce the likelihood of flammable vapors); or
2. Means to mitigate the effects of an ignition of fuel vapors within fuel tanks such that no damage caused by an ignition will prevent continued safe flight and landing.

In May 2002, the FAA developed a prototype inerting system that could be retrofitted into existing airplanes. The system was flight-tested by the FAA in conjunction with NASA, Boeing, and Airbus, and the results indicated that fuel tank inerting was practical and effective.

---

[45] NTSB Recommendation A-96-174. Full text and status of this recommendation are shown in Appendix D.

[46] FAA AC 25.981-1B, *Fuel Tank Ignition Source Prevention Guidelines*, April 18, 2001, Section 9c, states that, for analysis purposes, the environment inside the fuel tank is always flammable.

[47] TWA flight 800, NTSB/AAR-00/03, p. 294.

[48] TWA flight 800, NTSB/AAR-00/03, pp. 297-298.

Certification Issues

The final report of the TWA flight 800 investigation included a number of the Safety Board's concerns about certification. First, the Board clearly stated its concern about the use of various risk assessment techniques and the reliance on them to evaluate failure modes: "Failure modes and effects analyses and fault tree analyses should not be relied upon as the sole means of demonstrating that an airplane's fuel tank system is not likely to experience catastrophic failure."[49] These statements were a direct comment on the methods that can be used in certification to demonstrate compliance with Federal regulations. Much of the Board's concern was based on the lack of comprehensive and reliable data about failures for use in the analysis to estimate probabilities—data that could only come from testing or operational experience. The Board questioned, too, the validity of some of the assumptions underlying risk assessments, including underestimation of exposure times and failure rates, incomplete sets of failure modes, flawed assumptions of independence, and reliance on maintenance and inspection programs.[50]

Second, the Safety Board was concerned with "the FAA's apparent premise that minimizing, rather than eliminating, fuel tank flammability is an acceptable goal."[51] As previously discussed, the Board argued that a design and certification philosophy based solely on the elimination of ignition sources was fundamentally flawed. The Board's recommendations for preclusion of flammable vapors was, in effect, a call to accept, for the purpose of demonstrating compliance, solutions that would eliminate the flammability of vapors in fuel tanks. In 2000, in its comments to the FAA concerning Notice of Proposed Rule-Making (NPRM) 99-18, the Board stated "that the goal should be to completely eliminate the development of flammable vapors in fuel tanks to the greatest extent technically feasible (such as would result from the use of inerting systems)." The Board went on to state an additional concern about the FAA's failure to "propose any regulatory changes that address fuel tank flammability in current designs and in the existing fleet."[52]

The Safety Board's concerns about risk assessment techniques underscore the need to improve methods for demonstrating compliance and to improve the relationship between certification and operations through better collection and integration of operational data in the assessment of hazardous conditions during certification. The concerns about the design of the CWT speak directly to the ability of the FAA to rapidly accommodate new technologies and design philosophies.

[49] TWA flight 800, NTSB/AAR-00/03, p. 307.

[50] TWA flight 800, NTSB/AAR-00/03, pp. 294-298.

[51] TWA flight 800, NTSB/AAR-00/03, p. 300.

[52] As quoted in TWA flight 800, NTSB/AAR-00/03, p. 301.

Alaska Airlines Flight 261

On January 31, 2000, Alaska Airlines flight 261, a McDonnell Douglas MD-83, crashed into the Pacific Ocean about 2.7 miles north of Anacapa Island, California, killing all 88 people onboard. The Safety Board investigation determined that the probable cause of the accident was a loss of airplane pitch control resulting from the in-flight failure of the acme nut threads in the horizontal stabilizer trim system jackscrew assembly. The thread failure was caused by excessive wear resulting from Alaska Airlines' insufficient lubrication of the jackscrew assembly. The Board also determined that the lack of a fail-safe mechanism that would prevent a total catastrophic failure of the jackscrew assembly contributed to the accident.

During recovery of the wreckage, the investigation found evidence of stripped threads in the jackscrew assembly. Considerable effort was expended during the investigation to determine the cause of the acme nut thread failure, including metallurgical examination, analysis and testing of the load capability of the jackscrew assembly and its components, examinations and measurements of jackscrew assemblies, analyses and testing of the wear characteristics of grease, and evaluation of jackscrew assembly inspection intervals and lubrication intervals. Safety Board investigators considered both the design of the horizontal stabilizer trim system and the maintenance requirements initially established during certification and subsequently changed by Alaska Airlines and the manufacturer.

MD-80 series airplanes are based on the original DC-9 type certificate issued in 1965 and manufactured by McDonnell Douglas (as shown in figure 3).[53] When the MD-80 was certified in 1980, the longitudinal trim control system containing the jackscrew assembly was treated as a derivative design based on the original DC-9 type certificate. The design was assumed to comply with certification standards in that the combination of jackscrew and torque tube provided both structural and operational redundancy. Compliance materials presented during original type certification supported the design assertions and showed that the acme screw and torque tube could withstand loads far greater than those that could be produced by aerodynamic forces acting on the horizontal stabilizer.[54] The design was based on the assumptions "of a new, intact acme screw and nut that met design specifications, and that the acme screw and nut threads were intact and engaged to act as a load path."[55]

Certification materials also showed that the jackscrew assembly could carry limit loads in the following scenarios: a fractured acme screw where loads were supported by the torque tube; a fractured torque tube where loads would be carried by the acme screw and nut; the loss of 90 percent of the acme screw and nut threads; and the failure of one entire thread

[53] The Boeing Commercial Airplane Group and the McDonnell Douglas Corporation merged in August 1997. The Douglas Aircraft Company became the McDonnell Douglas Corporation in April 1967 when it merged with the McDonnell Aircraft Company.

[54] See Alaska Airlines flight 261, NTSB/AAR-02/01, pp. 13-19, for a description of the longitudinal trim control system.

[55] Alaska Airlines flight 261, NTSB/AAR-02/01, p. 21.

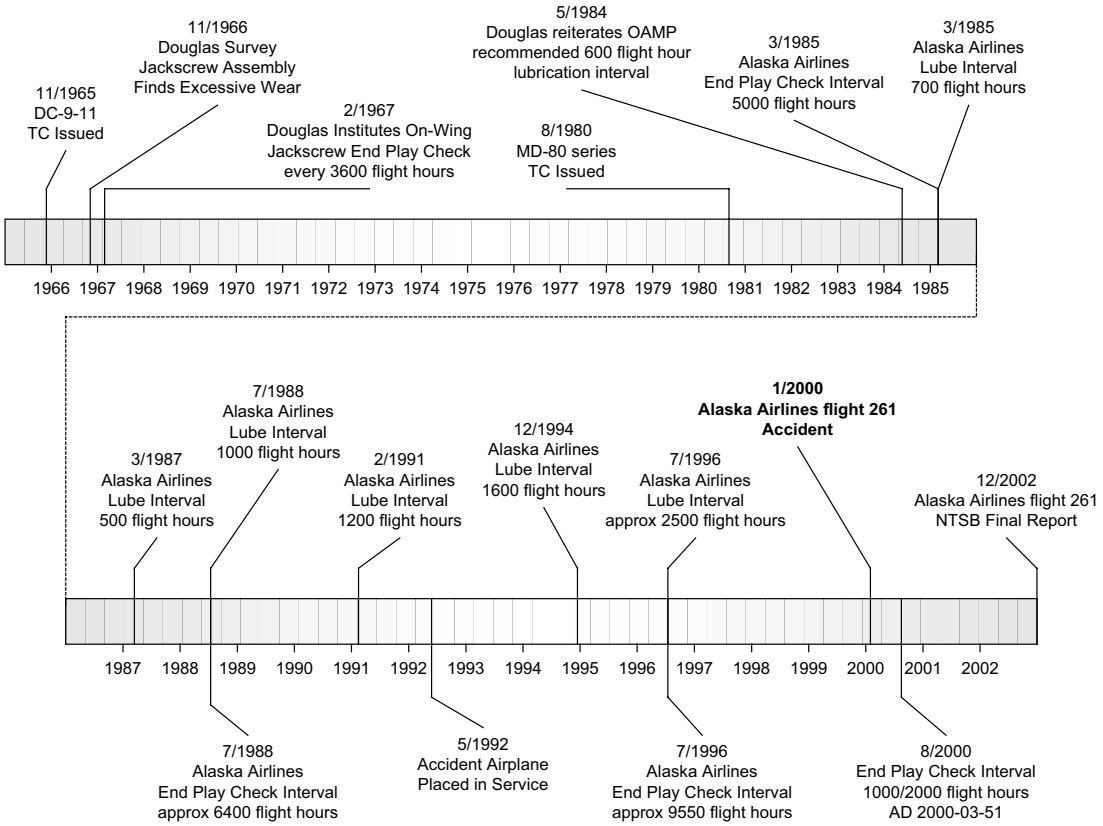

Figure 3. Chronology of Significant Events Discussed in Alaska Airlines Flight 261 Investigation

spiral in the acme screw or nut.[56] All of the scenarios assumed that at least one set of acme nut and screw threads would be intact; none of the scenarios considered the complete loss of acme nut threads. In the accident flight, all of the threads inside the acme nut had completely sheared off, and the torque tube had fractured, allowing the leading edge of the horizontal stabilizer to move up beyond its normal limits. The investigation found no evidence in certification documents that the accident aircraft scenario—where both sets of acme nut threads were lost due to wear—had been considered.

When the investigation explored design issues in more detail, the approach to certification of such systems became apparent. In testimony given at the Safety Board's public hearing, an FAA certification engineer clarified the regulatory distinction between systems and structures and the implications of that distinction for demonstrating compliance with Federal regulations. He stated that the jackscrew assembly was a "combination structural element and system element…and [that] as such, the systems portion would fall under the systems requirements, and the structures portion would be required to address the structural requirements."[57]

[56] Alaska Airlines flight 261, NTSB/AAR-02/01, pp. 21-22.

[57] Alaska Airlines flight 261, NTSB/AAR-02/01, p. 23.

Separating components of the aircraft into structural elements or system elements divides the methods of demonstrating compliance into essentially two types: methods (typically deterministic) that demonstrate compliance of aircraft structure and performance capabilities through adherence to specific design and test criteria; and methods that demonstrate compliance using probabilistic risk assessment techniques to evaluate failure conditions in systems. In the case of Alaska Airlines flight 261, FAA engineers indicated that the acme nut and screw in the jackscrew assembly were considered primary structures, and these elements of the assembly would have to comply with the strength, fatigue, and load-bearing capabilities outlined in Federal regulations pertaining to aircraft structures. Wear of the acme nut was not considered a failure mode in a safety analysis because the failure rate for a wear element could not be determined. Because certain parts of the jackscrew assembly were defined as structural components, there was no requirement during certification to comprehensively evaluate the jackscrew assembly as a system or to consider the failure conditions associated with loss of acme screw and nut threads.[58]

Boeing stated at the public hearing that the integrity of the jackscrew design was dependent upon maintenance, and, more specifically, monitoring and managing thread wear.[59] Original McDonnell Douglas certification documents from 1964 did specify an initial recommended minimum scheduled lubrication interval for the jackscrew assembly of 300 to 350 flight hours (or approximately 1 month of typical operation). The jackscrew assembly was originally designed for a service life of 30,000 flight hours and was not subject to periodic inspection for wear. In 1966, however, several jackscrew assemblies exhibited excessive wear, and in 1967, Douglas instituted an on-wing jackscrew assembly end play check as an indicator of wear.[60] The end play measurement was to be performed at every C-check or every 3,600 flight hours. Consequently, wear of the acme nut was managed by establishing intervals both for jackscrew lubrication and for jackscrew end play measurement and inspection.

The investigation revealed that after 1967, both the manufacturer and the air carrier extended the original intervals for lubrication and inspection. The original jackscrew assembly lubrication interval recommended for the DC-9 was 300 to 350 flight hours. The initial MD-80 On-Aircraft Maintenance Planning (OAMP) document

---

[58] A similar distinction between structure and system, and accepted by the FAA during certification, was found during the Safety Board's investigation of the Atlantic Southeast Airlines flight 2311 accident on April 5, 1991, in Brunswick, Georgia. In that accident, an Embraer EMB 120 crashed during approach to Glynco Jetport, killing all 23 people on board. The Board determined that the probable cause of the accident was the loss of control in flight as a result of the malfunction of the left engine propeller control unit, which allowed the propeller blade angles to go below the flight idle position. The Board also determined that the design and approval of the propeller control unit contributed to the accident. During certification, the transfer tube and quill in the control unit had been treated as a structural component of the engine rather than part of the control system; consequently, analysis of propeller response to failure of these components was not required. See *Atlantic Southeast Airlines, Inc., Flight 2311, Uncontrolled Collision with Terrain, An Embraer EMB-120, N270AS, Brunswick, Georgia, April 5, 1991*, Aircraft Accident Report NTSB/AAR-92/03 (Washington, DC: National Transportation Safety Board, 1992).

[59] Alaska Airlines flight 261, NTSB/AAR-02/01, p. 162.

[60] Alaska Airlines flight 261, NTSB/AAR-02/01, pp. 38-39. The excessive wear rate was discovered from reports by six operators to Douglas. A subsequent study by Douglas resulted in the end play measurement check and an end play measurement limit of 0.040 inch. If the end play exceeded that limit, the entire jackscrew assembly was to be replaced.

produced by McDonnell Douglas specified lubrication intervals of 600 to 900 flight hours.[61] In 1996, McDonnell Douglas issued a revised OAMP document calling for lubrication of the jackscrew assembly at C-check intervals (every 3,600 flight hours or 15 months, whichever occurred first). During investigation of Alaska Airlines flight 261, Boeing witnesses testified that neither the decision to extend the lubrication interval to 600/900 hours in 1980 nor the subsequent extension to 3,600 hours in 1996 considered the original recommended 300- to 350-hour interval. According to Boeing witnesses at the Safety Board's public hearing, the longer intervals were based on reliability data from both air carriers and manufacturers, and Boeing design engineers "were not consulted about nor aware of the extended lubrication interval"[62] specified in the maintenance documents.

Review of Alaska Airlines maintenance records during the investigation revealed that the air carrier extended lubrication intervals of the jackscrew assembly several times: in 1988 to 1,000 flight hours after every eighth A-check; in 1991 to 1,200 flight hours when the A-check interval increased; in 1994 to 1,600 flight hours when the A-check interval was again increased; and in 1996 when the A-check interval was extended to every 8 months or about 2,500 flight hours.[63] These changes led the Safety Board to conclude that the extended lubrication intervals, and the FAA's approval of those extensions, increased the likelihood that a missed or inadequate lubrication would contribute to a lack of lubricant and excessive wear of the acme nut threads. The Alaska Airlines flight 261 investigation found no evidence of effective lubrication of the acme screw and nut at the time of the accident.[64]

The investigation also revealed changes to the jackscrew assembly inspection intervals. The end play check procedure instituted by McDonnell Douglas in 1967 was the method to be used to monitor thread wear of the jackscrew assembly, and the procedure was to be done at every C-check (every 3,600 flight hours). Excessive thread wear would result in an end play measurement exceeding a maximum permissible limit and would indicate the need for jackscrew assembly replacement.

---

[61] An OAMP is produced during certification as part of the MRB activities. Under the guidance of the current MSG-3 process, an MRB Report is used to develop and produce tasks and associated time-in-service intervals for the initial maintenance time limitations in an air carrier's continuous airworthiness maintenance program. On the basis of the MRB Report, the manufacturer will issue OAMP documents and generic task cards for specific maintenance tasks. The role of the MRB in certification is discussed in more detail in the *Project Specific Certification Plan* section of this report and in FAA Advisory Circular AC 121-22A, *Maintenance Review Board Procedures*.

[62] Alaska Airlines flight 261, NTSB/AAR-02/01, p. 32.

[63] Alaska Airlines flight 261, NTSB/AAR-02/01, p. 28. Escalation of an individual maintenance task interval (currently performed at or in excess of the interval recommended in the applicable aircraft's OAMP document) to greater than 10 percent of the current interval.

[64] Alaska Airlines flight 261, NTSB/AAR-02/01, p. 178.

Two Maintenance Review Board (MRB) reports and accompanying OAMP documents derived from the MSG-2[65] and MSG-3[66] processes provide the current basis for maintenance of the MD-80. Alaska Airlines' continuous airworthiness maintenance program for its MD-80 fleet received initial FAA approval in March 1985 and was based on the FAA-accepted MRB report for DC-9/MD-80 airplanes derived from the MSG-2 maintenance program development document. The MRB report and the resulting OAMP document recommended C-check intervals of 3,500 flight hours or 15 months, whichever came first. The Alaska Airlines C-check interval was originally set in 1985 at 2,500 flight hours. Based on the MSG-2 process, the C-check inspection interval was extended in 1988 to every 13 months (or approximately every 3,200 flight hours based on Alaska Airlines' average airplane use rate). In 1996, the C-check interval was extended to 15 months based on the guidance and philosophy found in the MSG-3 process.

The important difference in the switch from MSG-2 to MSG-3 was the change in philosophy underlying maintenance requirements. MSG-2 based requirements on the type of maintenance process to be employed (for example, hardtime limits, on-condition maintenance, and condition monitoring[67]). MSG-3 introduced a top-down, task-oriented approach and functional decision logic that helped remove the MSG-2 "confusion associated with the various interpretations of Condition Monitoring (CM), On-Condition (OC), Hardtime (HT) and the difficulties encountered when attempting to determine what maintenance was being accomplished on an item that carried one of those process labels."[68] MSG-3 used a decision logic that explicitly analyzed functional failures and could handle concurrent and multiple failures. For the first time, MSG-3 included servicing and lubrication tasks in the decision logic and task analysis.

The extensions in C-check inspection intervals by Alaska Airlines using the MSG-2 and MSG-3 guidance effectively extended the recommended end-play inspection intervals.[69] In 1985, the Alaska Airlines end play check occurred at every other C-check, or every 5,000 flight hours. By 1996, the Alaska Airlines C-check interval was set at 15 months (with no flight hour requirement), with the end play check of the jackscrew assembly occurring at every other C-check. This change effectively extended the

---

[65] The Maintenance Steering Group (MSG) MSG-2 process was introduced in 1970 to develop the initial minimum scheduled maintenance/inspection recommendations for aircraft and powerplants. It grew out of the original MSG-1 development of maintenance procedures for the Boeing 747 aircraft.

[66] The MSG-3 process was introduced in 1980 to update the MSG-2 process to improve the decision logic, the distinction between economics and safety, and the treatment of functional failures. More detail about the MSG-3 process can be found in *Operator/Manufacturer Scheduled Maintenance Development,* Revision 2003.1, ATA MSG-3 (Washington, DC: Air Transport Association of America, 2003).

[67] A *Hardtime Limit* (HT) is a preventive maintenance process that requires that a system, component, or appliance be either overhauled periodically (time limits) or removed from service (life-limit). *On-Condition* (OC) is a preventive maintenance process that requires that a system, component, or appliance be inspected periodically or checked against some appropriate physical standard to determine if it can remain in service. *Condition Monitoring* (CM) is a process for finding and resolving problems, and typically applies to aircraft elements that do not have HT or OC maintenance requirements. See FAA Order 8300.10, *Airworthiness Inspector's Handbook* (January 30, 2002), Chapter 66, for more details.

[68] Air Transport Association of America ATA MSG-3, p. 6.

[69] Alaska Airlines flight 261, NTSB/AAR-02/01, p. 178.

jackscrew end play check procedure to about 9,550 flight hours (based on aircraft use rates), far exceeding the manufacturer's recommended flight-hour interval limit of 7,000 to 7,200 flight hours.[70] At the time of the accident, the accident airplane had accumulated more than 8,800 flight hours since its last end play check in September 1997.[71]

The investigation was unable to document what information, if any, the FAA used to justify the extensions, and the Safety Board concluded that the extensions were made without adequately demonstrating that the change would not pose a potential hazard. The Board also concluded that the Alaska Airlines maintenance program had widespread systemic deficiencies, and that the FAA "did not fulfill its responsibility to properly oversee the maintenance operations at Alaska Airlines."[72] In addition, the investigation found that Alaska Airlines maintenance personnel had difficulty correctly performing the end play check procedure, resulting in inaccurate end play measurements. These facts led the Board to state the following in its final report:

> Alaska Airlines' extension of the end play check interval and the FAA's approval of that extension allowed the accident acme nut threads to wear to failure without the opportunity for detection and, therefore, was a direct cause of the excessive wear and contributed to the Alaska Airlines flight 261 accident.[73]

Certification Issues

The investigation of Alaska Airlines flight 261 highlighted two Safety Board concerns about certification. First, the Board focused considerable attention on the FAA and Alaska Airlines extensions to lubrication and inspection intervals. The Board was concerned that these extensions were made without sufficient analysis, justification, and consideration of design assumptions made during certification. As a result, the lubrication intervals and inspection procedures adopted by both the FAA and the operator were inadequate to ensure the design integrity of the jackscrew assembly. The testimony of the FAA's MD-80 MRB chairman at the public hearing underscored the problem by indicating that the changes in the C-check intervals for the MD-80 did not involve a specific analysis of each task that would be affected by the changed interval.[74] These concerns led the Board to recommend that the maintenance procedures and intervals for all critical aircraft components be reviewed to ensure that all were based on sound engineering justification, and that any extensions to those intervals "(1) take into account assumptions made by the original designers, (2) are supported by adequate technical data and analysis, and (3) include

---

[70] Alaska Airlines flight 261, NTSB/AAR-02/01, p. 152. The recommended end play check interval was set by the manufacturer at every other C-check. By 1996, the C-check interval was set to every 3,600 flight hours or 15 months, whichever came first. This resulted in an end play measurement check being performed every 7,000 flight hours, or 30 months under MSG-2, and every 7,200 flight hours, or 30 months under MSG-3.

[71] The last C-check for the accident airplane that included an end play check occurred September 26, 1997, and the airplane had accumulated 17,699 flight hours. At the time of the accident, the accident airplane had accumulated 26,584 flight hours.

[72] Alaska Airlines flight 261, NTSB/AAR-02/01, p. 180.

[73] Alaska Airlines flight 261, NTSB/AAR-02/01, p. 153.

[74] Alaska Airlines flight 261, NTSB/AAR-02/01, p. 32.

an appropriate safety margin that takes into account the possibility of missed or inadequate accomplishment of the maintenance task."[75]

The fact that the lubrication and inspection intervals were extended without adequate regard for the effects of those extensions led the Safety Board to conclude that excessive wear of the jackscrew assembly could occur before being detected. The Board's recommendation to review all maintenance tasks of safety-critical systems highlighted the need to consider the designer's original assumptions, as well as the requirement to support any changes to manufacturer maintenance requirements with the appropriate data and analysis.[76] Monitoring critical systems was of particular concern to the Board, resulting in a recommendation to establish a maintenance program that would track and analyze jackscrew wear and end play measurements by aircraft registration number and jackscrew assembly serial number, and to report those results to the FAA.[77] Its concern with monitoring critical systems also led the Board to recommend that, for proposed changes in maintenance task intervals that could affect critical aircraft components, operators obtain written approval "from the principal maintenance inspector and written concurrence from the appropriate FAA aircraft certification office."[78]

The second concern focused on the design of the jackscrew assembly and the different ways in which aircraft structures and aircraft systems were treated during certification. The failure of the acme nut threads led the Safety Board to conclude that the dual-thread design of the acme screw and nut was not redundant with respect to wear and that the design did not account for the loss of threads as a catastrophic single-point failure mode. The failure mode for the jackscrew system was excessive wear-rate because the nut was designed to accommodate wear and the manufacturer had made an assumption about acceptable wear-rate. In addition, a fail-safe characteristic of the jackscrew was dependent upon a recommended maintenance program that would be expected to detect excessive wear before a failure occurred. The Board recommended that the FAA review the jackscrew assembly design, and if practicable, require installation of fail-safe mechanisms to eliminate the effects of a catastrophic single-point failure mode.[79] The Board also stated that "because the loss of acme nut threads in flight most likely would result in the catastrophic loss of the airplane," the acme nut should be considered as "a critical element of the horizontal stabilizer trim control system; therefore, it should have been covered by the certification philosophy and regulations applicable to all other flight control systems."[80] The Board went on to recommend the following to the FAA:

---

[75] NTSB Safety Recommendation A-02-41; full text and status are shown in Appendix D.

[76] NTSB Safety Recommendations A-02-41 and A-02-42; full text and status are shown in Appendix D.

[77] NTSB Safety Recommendation A-02-45; full text and status are shown in Appendix D.

[78] NTSB Safety Recommendation A-02-43; full text and status are shown in Appendix D.

[79] NTSB Safety Recommendation A-02-49; full text and status are shown in Appendix D.

[80] Alaska Airlines flight 261, NTSB/AAR-02/01, p. 164.

> 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.[81]

These recommendations were in response to the FAA's treatment of some components of the jackscrew assembly as aircraft structure and other components as elements of a system. Although the Safety Board acknowledged that applying risk assessment techniques to all aircraft components would not necessarily uncover all potential failures, such techniques would require the FAA and the manufacturer to consider all failure modes in safety-critical systems during certification, to the extent possible.

American Airlines Flight 587

Shortly after takeoff from John F. Kennedy International airport on November 12, 2001, American Airlines flight 587, an Airbus Industrie A300-605R, crashed into the residential area of Belle Harbor, New York, killing all 260 people on board and 5 people on the ground. Flight data from the accident airplane showed that cyclic rudder motions created a 10- to 12-degree sideslip and exposed the vertical stabilizer to aerodynamic loads that were twice the certified limit load design envelope, resulting in the separation of the vertical stabilizer from the airplane's fuselage. The investigation determined that the first officer was flying the aircraft at the time of the accident and that the cyclic rudder motions after a second wake encounter were the result of the first officer's rudder pedal inputs. The Safety Board determined the probable cause of the accident "was the in-flight separation of the vertical stabilizer as a result of the loads beyond ultimate design that were created by the first officer's unnecessary and excessive rudder pedal input."[82] Contributing to these rudder inputs, stated the Board, were characteristics of the airplane's rudder system design and elements of the airline's pilot training program, as discussed below. Figure 4 shows a timeline of significant events discussed in the American Airlines flight 587 report.

The Safety Board stated that "the in-flight separation of the vertical stabilizer from the fuselage of a transport-category airplane is an extremely rare, if not unprecedented, occurrence."[83] Consequently, considerable attention was paid to the design of the vertical stabilizer and the behavior of the composite materials used in its construction. After conducting a number of tests to ensure that the vertical stabilizer's performance was consistent with design and certification standards, the investigation considered the factors that led to the sideslip and build-up of aerodynamic loads that fractured the vertical stabilizer main attachment fittings.

---

[81] NTSB Safety Recommendation A-02-50; full text and status are shown in Appendix D.

[82] American Airlines flight 587, NTSB/AAR-04/04, p. 160.

[83] American Airlines flight 587, NTSB/AAR-04/04, p. 134.

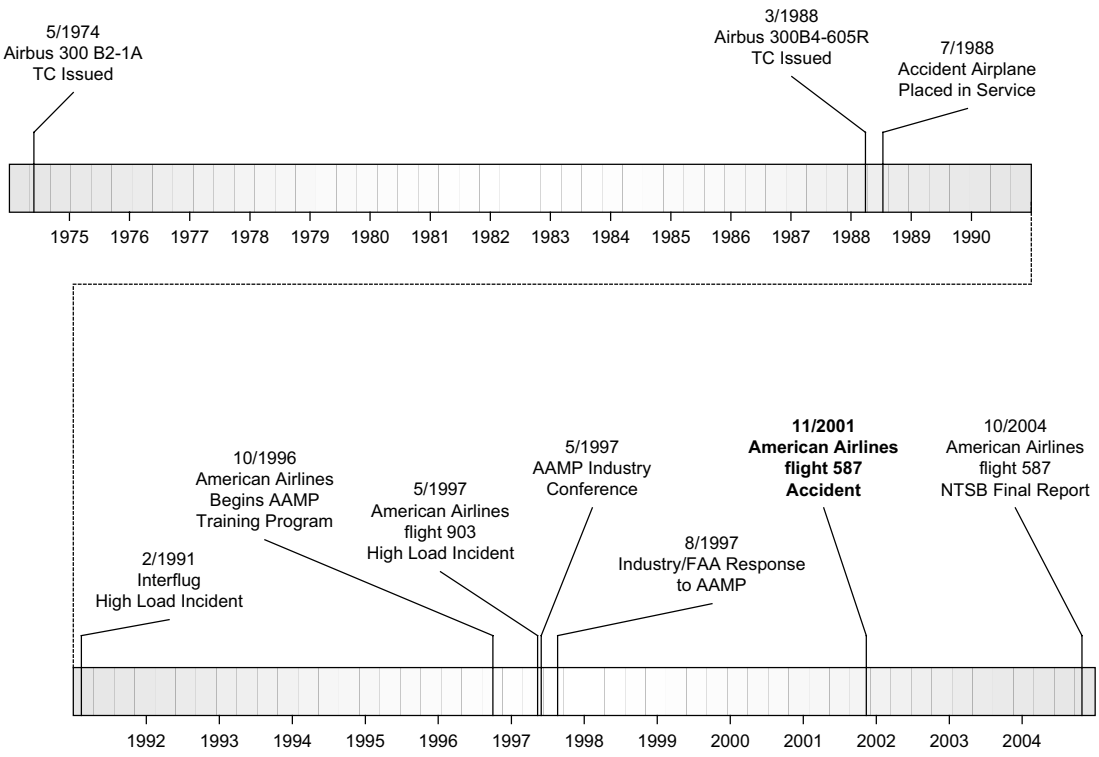

Figure 4. Chronology of Significant Events Discussed in American Airlines Flight 587 Investigation

The first officer's multiple full-deflection, alternating flight control inputs became the focus of the investigation. The Safety Board noted that regulations do not require that such alternating pedal inputs be considered during certification, and that the absence of rudder control system features that mitigate the adverse effects of alternating rudder pedal inputs at high speed does not necessarily constitute a design deficiency. The Board therefore recommended that the FAA modify certification standards to ensure safe handling qualities in the yaw axis,[84] and once those changes to the regulations had been made, to "review the designs of existing airplanes to determine if they meet the standard."[85]

The Safety Board also recommended that the Direction Général de l'Aviation Civile (the French civil aviation authority responsible for certification) review options for modifying the Airbus A300-600 and A310 to provide increased protection against a pilot making hazardous rudder inputs at high airspeeds, and, if necessary, require that modifications be made to those aircraft to provide increased protection from such rudder inputs at high speeds.[86]

[84] NTSB Recommendation A-04-56; full text and status are shown in Appendix D.

[85] NTSB Recommendation A-04-57; full text and status are shown in Appendix D.

[86] NTSB Recommendation A-04-63; full text and status are shown in Appendix D.

The Safety Board went on to say that rudder design features (such as hinge moment capacity limits and yaw damper characteristics[87]) can help mitigate the potential hazards associated with rudder inputs, especially at high speeds. However, in the case of the A300-600 yaw damper system, pilot input can override a compensatory yaw damper command under certain conditions. Simulations conducted during the investigation indicated that without this override feature, the yaw damper would have moved the rudder partially back to neutral during the accident sequence, "thereby lessening (but not preventing) the buildup of the sideslip angle and the aerodynamic loads on the vertical stabilizer."[88] The Board stated that "such a delay could have provided an additional level of safety because the initial response of the airplane to a sustained rudder pedal input would not have been as severe and could have reduced the chance of pilot surprise or confusion."[89]

The Safety Board also concluded that "the Airbus A300-600 rudder control system couples a rudder travel limiter system that increases in sensitivity with airspeed, which is characteristic of variable stop designs, with the lightest pedal forces of all the transport-category aircraft evaluated by the Safety Board during this investigation."[90] Noting the absence of certification standards for rudder pedal sensitivity other than the requirement that the angle of sideslip be substantially proportional to rudder angle,[91] the Board defined pedal sensitivity for the purposes of the investigation as "the amount of initial lateral acceleration produced in the cockpit per pound of pedal force above the breakout force,"[92] and *breakout force* as the amount of force required to move the rudder pedal from its neutral resting position. The design of the Airbus 300-600 rudder limiter system had a breakout force of 22 pounds and required only an additional 10 pounds of force to reach the pedal maximum limit.[93]

The design of the rudder travel limiter system also contributed to the sensitivity of the A300-600 pedal. Unlike the variable ratio design used in the A300B2/B4, which allows a constant range of rudder pedal travel but reduces the amount of rudder deflection as airspeed increases, the variable stop design of the A300-600 limits rudder pedal travel as airspeed increases. Where the A300B2/B4 has a pedal travel of 4 inches, the A300-600 variable stop design has a pedal travel of 4 inches at 135 knots that is reduced to 1.2 inches at 250 knots. When translated to pedal sensitivity (as defined in the investigation), the A300B2/B4 variable ratio design produces a relatively constant pedal sensitivity at all airspeeds, and the A300-600 variable stop design produces an increase in pedal sensitivity as airspeed increases. In other words, the same amount of force applied to the pedals in an A300-600 at a high airspeed produced more lateral G-forces than that same force applied at a lower speed.

---

[87] American Airlines Flight 587, NTSB/AAR-04/04, p. 153.

[88] American Airlines Flight 587, NTSB/AAR-04/04, p. 154.

[89] American Airlines Flight 587, NTSB/AAR-04/04, p. 154.

[90] American Airlines Flight 587, NTSB/AAR-04/04, p. 160.

[91] See 14 CFR 25.177*: Static lateral-directional stability*, section c.

[92] American Airlines flight 587, NTSB/AAR-04/04, p. 25.

[93] By comparison, the breakout force of the Airbus A340-300 is 32 pounds and requires an additional 17 pounds to reach the pedal maximum limit. The same forces for the Boeing 777 are 18 pounds and an additional 42 pounds. For more details, see NTSB/AAR-04/04, pp. 24-29.

The investigation concluded that "the A300-600 would be twice as responsive to pedal displacement at 250 KCAS as it would be at 165 KCAS" and that the "increase in rudder pedal sensitivity as airspeed increases creates a control system change that pilots may not expect."[94] This characteristic, combined with the lightest pedal forces of all the transport-category airplanes evaluated during the investigation, led the Safety Board to also conclude that "these characteristics likely played a role in the accident sequence."[95] Airbus stated during the investigation that the variable stop design was chosen for the A300-600 over the variable ratio design because it was less complex and its failure modes were less severe. The change was evaluated during certification during flight testing.

The investigation also considered the possibility that the accident sequence was characteristic of an aircraft-pilot coupling (APC) event. APC events, according to the National Research Council (NRC) report cited by the Safety Board, are unintended excursions caused by anomalous interactions between the aircraft and the pilot and can be oscillatory or divergent and potentially catastrophic. The Safety Board pointed out that the FAA's AC 25-74, *Flight Test Guide for Certification of Transport Category Airplanes,* addresses APC and "cautions against flight controls with small displacements and light force gradients—features that are both present on the A300-600 rudder system at higher speeds."[96] The Board concluded that "certification standards are needed to ensure that future airplane designs minimize the potential for APC susceptibility and to better protect against high loads in the event of large rudder inputs"[97] and issued Safety Recommendation A-04-57 to that effect.

The investigation also looked for information to explain why the first officer used multiple full-deflection, alternating flight control inputs in response to a wake turbulence encounter. Airbus stated throughout the investigation that ailerons were the primary roll control and that the pilot did not need to use the rudder pedals in turbulence because the yaw damper was designed to deal with that situation.[98] In its submission to the investigation, Airbus stated the following:

> On civil transport-category airplane, the rudder pedal is more a zeroing flight control to compensate for any yaw asymmetry than a primary flight control to create yaw asymmetry as it is on some military fighter aircraft. In flight it has to be used only in case of an engine out condition or during landing for decrab.[99]

---

[94] American Airlines flight 587, NTSB/AAR-04/04, pp. 145-146.

[95] American Airlines flight 587, NTSB/AAR-04/04, p. 146.

[96] American Airlines flight 587, NTSB/AAR-04/04, p. 152.

[97] American Airlines flight 587, NTSB/AAR-04/04, p. 153.

[98] National Transportation Safety Board Transcript of Public Hearing, *American Airlines flight 587, Belle Harbor, New York*, Tuesday, October 29, 2002, p. 165.

[99] Airbus submission to the National Transportation Safety Board, for the American Airlines Flight 587 Belle Harbor, New York, November 12, 2001, accident investigation, NTSB/AAR-04/04, pp. 13-14, March 3, 2004.

Airbus went on to state that "rudder doublets—full stop-to-stop pedal deflections such as those observed in this accident—are not recognized design conditions, nor is there ever an operational need for them in transport-category aircraft."[100]

When the investigation studied pilot response to uncommanded, in-flight upsets, the Safety Board found that the American Airlines flight 587 first officer was not unique in his use of rudder pedals and was not the only pilot to produce high aerodynamic loads on an Airbus vertical stabilizer. In total, the investigation documented seven vertical stabilizer high-loading events (including flight 587) on A300-600 and A310 airplanes, some of which involved the use of alternating rudder inputs resulting in aircraft recovery.[101] In addition, the Board reviewed a NASA special study of 33 uncommanded, in-flight upsets during the 6-month period of May 1 to October 31, 1995. Most of the upsets in the study were induced by wake turbulence and pilots reported using the rudder during recovery in 11 of the 33 events.

Excessive use of the rudder by the accident airplane's first officer also prompted the investigation to study American Airlines' pilot training program. American Airlines' Advanced Aircraft Maneuvering Program (AAMP) was introduced in 1996 after a review of worldwide accidents from 1987 to 1996 involving large, multi-engine transport-category airplanes. The review found that loss of control was a leading causal factor in these accidents.[102] AAMP was introduced to train pilots to recognize and respond to airplane upsets. The investigation found that AAMP's ground school and simulator training encouraged pilots to use the rudder to assist with roll control during recovery from upsets, and that specific characteristics of the simulated wake encounter event in the AAMP simulator might cause pilots to associate an uncontrollable roll with wake turbulence.[103] In addition, to ensure that the airplane reached the 90-degree bank angle required by the AAMP simulator exercise, the aerodynamic effectiveness of control wheel and rudder pedal inputs was inhibited. The pilot and first officer of American Airlines flight 587 first attended AAMP in 1997 and had received annual recurrent training. These factors led the Safety Board to conclude the following:

> The American Airlines AAMP excessive bank angle simulator exercise could have caused the first officer to have an unrealistic and exaggerated view of the effects of wake turbulence; erroneously associate wake turbulence encounters with the need for aggressive roll upset recovery techniques; and develop control strategies that would produce a much different, and potentially surprising and confusing, response if performed during flight.[104]

American Airlines had been cautioned by industry and government representatives about the emphasis in AAMP on rudder use for roll control. American Airlines held a

---

[100] Airbus, March 3, 2004.

[101] American Airlines flight 587, NTSB/AAR-04/04, pp. 103-110.

[102] American Airlines flight 587, p. 80.

[103] For a more detailed discussion of the AAMP simulator wake encounter event, see American Airlines flight 587, NTSB/AAR-04/04, pp. 80-87.

[104] American Airlines flight 587, NTSB/AAR-04/04, p. 142-143.

2-day AAMP Industry Conference in May 1997 to solicit comments on its training program, and the conference was attended by representatives from the FAA, Boeing, McDonnell-Douglas, Airbus, and the U.S. military. Feedback was provided in August 1997 to American Airlines by a joint response from Boeing, Airbus, and the FAA that covered a number of topics, including the use of rudder. The letter stated a concern that AAMP emphasized the use of rudder in high angle-of-attack situations and went on to state that the use of rudder could defeat the purpose of yaw dampers and turn coordinators in such situations. The letter also stated that pilots taking AAMP might be left with the misconception that rudder must be used in all high angle-of-attack situations and that the training program needed to discuss the criticality of sideslip angle. The letter was specific in its concern about rudder and sideslip angle:

> Large or abrupt rudder usage at high angle of attack can rapidly create large side slip angles and can lead to rapid loss of controlled flight. Rudder reversals such as those that might be involved in dynamic maneuvers created by using too much rudder in a recovery attempt can lead to structural loads that exceed the design strength of the fin and other associated airframe components.[105]

AAMP did not discuss the variable stop design of the A300-600 rudder travel limiter system, and the operating manuals provided by the manufacturer and the airline only referenced rudder deflection limits at higher airspeeds. The Safety Board therefore stated that a pilot's lack of knowledge regarding restricted rudder pedal travel could lead to confusion if an unexpected pedal limit was encountered in flight. The Board went on to state the following:

> In such a situation, the pilot may fail to associate the airplane response with control inputs, instead attributing the response to some external cause (such as wake turbulence). Consequently, the pilot may not recognize the potential risk to the airplane and may continue making inappropriate control inputs.[106]

The investigation also learned that many pilots do not fully understand the meaning of the design maneuvering speed (V_A). Maneuvering speed is a design parameter that specifies the maximum speed at which an airplane will be able to sustain, without damage, full control input from an initial 1 G flight condition limited only by control stops or the maximum effort of the pilot. However, as the investigation discovered, many pilots believe that an airplane will not be damaged by full *alternating* control input as long as the airspeed is below maneuvering speed. The Safety Board pointed out that FAA certification regulations pertaining to maneuvering speed may have contributed to that misunderstanding, both in terms of the definition found in 14 CFR 25.1583 and the explanation found in AC 61-23C, *Pilot's Handbook of Aeronautical Knowledge.* The handbook stated that "any combination of flight control usage, including full deflection of the controls, or gust loads created by turbulence should not create an excessive air load if the airplane is operated below maneuvering

[105] NTSB Public Docket Document No. 14, "Operations 2—Attachment H—Correspondence from Airplane Manufacturers to American Airlines and Response" (September 20, 2002).

[106] American Airlines flight 587, NTSB/AAR-04/04, p. 143.

speed."[107] The Board concluded that a widespread misunderstanding exists among pilots about the degree of structural protection that exists when full or abrupt flight control inputs are made at airspeeds below the maneuvering speed.

The investigation summarized the first officer's rudder pedal inputs as the confluence of a number of factors: his predisposition to overreact to wake turbulence encounters, perhaps aggravated by an upset training program in simulators that could encourage pilots to use large control inputs, including rudder, in response to wake turbulence; a highly sensitive rudder design; and a variable stop rudder design that, if not fully understood by pilots, might result in unexpectedly large rudder inputs, especially at high speed.[108] From a type certification perspective, the Safety Board was concerned about the A300-600 rudder system design characteristics that affect safe handling qualities in the yaw axis, the protection provided by those design characteristics in response to rudder inputs at high speed, and the sensitivity of the rudder system and its potential to increase the likelihood of an APC event.

Certification Issues

Although it did acknowledge that no certification standards for rudder pedal sensitivity exist, the Safety Board stated the following:

> If a pilot assumed the sensitivity of the rudder on any airplane remained relatively constant across a range of airspeeds, this assumption would lead to the erroneous expectation on an airplane equipped with a variable stop rudder travel limiter system that the response to a given pedal input, including the subsequent rolling moment, would be about the same regardless of the airspeed.[109]

Such evidence led the Safety Board to state that "a system with large pedal displacements would make achieving these inputs more demanding physically, providing greater feedback regarding the magnitude of the pilot's efforts on the controls."[110] One could conclude that Airbus did not appear to fully consider the potential adverse effects of light pedal forces of a variable stop rudder limiter design on crew behavior and performance, or assess its propensity to trigger an APC event (despite the FAA caution in advisory materials to avoid flight controls with small displacement and light gradient forces).

The Safety Board investigation also revealed that certification standards were deficient with respect to pilot interaction with the A300-600 rudder system. Specific standards set forth in regulations to address pedal force requirements, proportional rudder movements, and handling qualities did not appear to the Board to sufficiently address the risks associated with pilot use of rudder, especially at high airspeeds. This led the Board to conclude that there was no certification standard regarding rudder pedal sensitivity or

---

[107] FAA AC 61-23C, *Pilot's Handbook of Aeronautical Knowledge* (1997), pp. 1-20. AC 61-23C was replaced by FAA H-8083-25 *Pilot's Handbook of Aeronautical Knowledge* in December 2003.

[108] American Airlines flight 587, NTSB/AAR-04/04, p. 152.

[109] American Airlines flight 587, NTSB/AAR-04/04, p. 146.

[110] American Airlines flight 587, NTSB/AAR-04/04, p. 152.

any requirement for the sensitivity to remain constant at all airspeeds. In addition, the Board concluded that certification standards were needed to ensure that future airplane designs would minimize the potential for APC susceptibility and better protect against high loads in the event of large rudder inputs. The Board's concerns led to a recommendation "to include a certification standard that will ensure safe handling qualities in the yaw axis throughout the flight envelope, including limits for rudder pedal sensitivity."[111]

Finally, the investigation highlighted the Safety Board's concerns about the relationship between certification and operations, especially regarding FAA use of operational data, service history, and accident/incident data to manage safety-critical systems. American Airlines sought input for its AAMP in 1997 from government, military, and industry representatives. The responses to the program were favorable in general. However, a joint industry response (which included Airbus and Boeing) and subsequent discussions between Airbus and American Airlines indicated that the AAMP might have over-emphasized the use of rudder in upset recovery. Further, as previously discussed, the evidence that pilots used rudder in upset recoveries did not prompt either the FAA or Airbus to reconsider the assumptions underlying rudder pedal sensitivity. Although the FAA, the manufacturer, and the operator communicated with each other, no action was taken, suggesting that merely communicating was not enough and a more systematic approach to assessing and responding to continued airworthiness and operational issues was required. The fact that the FAA was also involved in these discussions and co-authored the response to American Airlines about AAMP suggests that the mechanisms for managing potential airworthiness and operational problems were not adequate.

[111] NTSB Safety Recommendation A-04-56; full text and status are shown in Appendix D.

Methodology for Examining Type Certification

The four accident case studies described above show that investigative records can and do reveal deficiencies in certification. In these accidents, the Safety Board derived conclusions and recommendations addressing certification using a retrospective methodology based on historical records and interviews. Investigators traced the decision-making process through design and certification and documented the rationale that led to acceptance of the design. This approach, applied case-by-case, revealed a number of important certification issues that were contributing factors in the accident. To relate the issues found in the accidents to type certification, the Safety Board employed a retrospective methodology similar to that used during the accident investigations and considered the specific processes that the FAA used to assess hazards to the safety of flight.

A process analysis was used as a retrospective methodology to examine and describe type certification and describe how the FAA assesses hazards to safety of flight. This section summarizes key type certification activities that relate to the assessment of safety-critical systems and that are most closely associated with the four accident case studies. These activities include establishing the certification basis; demonstrating compliance; and conducting safety assessments. Detailed descriptions of the FAA's type certification process and the role of AIR are provided in Appendix A. Before discussing safety-critical systems specifically, however, the report first describes the type certification process.

The FAA Certification Process

AIR is responsible for type certification and is one of seven organizations under the FAA Associate Administrator for Aviation Safety (AVS). Directorates within AIR develop and implement regulatory requirements, policy, and procedures. The Transport Airplane Directorate (ANM-100) in Renton, Washington, is responsible for type certification of transport-category airplanes and for oversight and inspection of production certificate holders and manufacturing facilities.

Within each directorate are Aircraft Certification Offices (ACOs) that serve as the directorate's engineering operational elements. These offices are responsible for "approving the design certification of aircraft, aircraft engines, propellers, and replacement parts for those products."[112] Within the Transport Airplane Directorate are three ACOs—located in Seattle, Denver, and Los Angeles—that conduct activities related to certification of transport-category airplanes.

[112] FAA Order 8100.5A, paragraph 2.9e.

To obtain a TC, an applicant must demonstrate to the FAA that the airplane or aviation product complies with all applicable Federal regulations. The Federal regulations applicable to type certification of transport-category airplanes are contained in 14 CFR Parts 21, 25, 33, 34, and 36 (and are described in more detail in Appendix A). The regulations in 14 CFR Part 25 are the ones most relevant to this report's focus on safety-critical systems. The Part 25 regulations are those concerned with the airworthiness standards for transport-category airplanes and are organized into the subparts shown in table 1. The subparts of greatest interest to this report are C and D, which deal with structures, design, and construction, and E, which deals with systems. The important point about the subparts is that the regulations are organized into groups related to the airplane elements of concern, and the regulations in each subpart may not apply to elements of the airplane governed by regulations in other subparts.

Table 1. Subparts of 14 CFR Part 25, "Airworthiness Standards for Transport-Category Airplanes"

Subpart	Applicable Area
A. General	Applicability, special requirements
B. Flight	Critical speed and performance values, weight, center of gravity, stability
C. Structure	Limit and ultimate loads, strength, design airspeeds, damage and fatigue tolerance
D. Design and Construction	Suitability and durability of materials, fabrication, casting, installation, doors
E. Powerplants	Installation, isolation, restart, auxiliary power, thrust reversers, fuel tanks
F. Equipment, Systems, and Installations	Systems, limitations, instruments, avionics, hydraulics, flight controls
G. Operating Limitations and Information	Flight manual, emergency procedures, airspeed and powerplant limits

According to 14 CFR 21.21 and FAA Order 8110.4C,[113] the applicable Federal regulations for a specific transport-category airplane are contained in the type certification basis, which is established by the FAA in the early stages of the certification project. These regulations represent the minimum standards for airworthiness; an applicant's design may exceed these standards and the applicant's tests and analyses may be more extensive than required by regulation. An important point is that the responsibility for the design engineering and analysis lies with the applicant, not the FAA; as stated in FAA Order 8110.4C, "The FAA approves the data, not the analytical technique, so the FAA holds no list of acceptable analyses, approved computer codes, or standard formulas. Use of a well established analysis technique is not enough to guarantee the validity of the result. The applicant must show the data are valid."[114]

[113] U.S. Department of Transportation, Federal Aviation Administration Order 8110.4C, *Type Certification*, October 26, 2005.

[114] FAA Order 8110.4C, paragraph 2-6g.

The current type certification process, described in *The FAA and Industry Guide to Product Certification,*[115] is governed by procedures set forth in 14 CFR Part 21 and is described in detail in FAA Orders 8100.5A and 8110.4C. Because the industry guide was not in effect during certification of any of the aircraft described in the four accidents, certain products required now were not required when the Boeing 737-300, 747-131, MD-83, and Airbus 300-605R investigated in the four accident case studies were certified. However, the five phases of the certification process described in the industry guide are consistent with the processes that were required at that time, and represent the FAA's current view of type certification. The deliverables and the time course of activities across the five phases of type certification are shown in table 2, and are also described in more detail in Appendix A. As highlighted in table 2, the type certification activities that most closely relate to the certification issues of concern are the certification basis, safety assessments, and compliance demonstrations.

Establishing the Type Certification Basis

There is considerable incentive on the part of the applicant and the FAA to quickly and accurately establish the type certification basis for an airplane because the applicable regulations determine the extent of the compliance effort. In addition, once the certification basis is established, the set of regulations and standards will not be changed or new policy introduced unless a change is required to correct an unsafe condition. Establishing the type certification basis is an important milestone.

Federal regulations represent the minimum set of safety standards required for a TC and may not cover all potential safety issues. For example, the investigation of American Airlines flight 587 showed that certification standards did not exist for certain rudder pedal characteristics (for example, pedal sensitivity) or for assessing certain types of pilot behavior with the rudder control system. None of the existing certification regulations, other than the cautions about APC potential in advisory material, would have required the FAA to look more closely at the variable stop design in the A300-600 and A310 airplanes. Such situations, called special conditions, are provided for in the regulations and are described in more detail in Appendix A.

[115] The industry guide was introduced in 1999 as part of a certification process improvement initiative and revised in 2004. It emphasizes "establishing up-front a clear understanding of the needs and expectations of both parties in the product certification process." By applying the principles in the industry guide, "the FAA and the Applicant can lay a foundation from which to build mutual trust, leadership, teamwork, and efficient business practices," and enable them to "expedite certification of products while focusing on safety significant issues." The guide, implemented by FAA Notice 8110.80, *The FAA and Industry Guide to Product Certification*, February 26, 1999, is available at <http://www.faa.gov/aircraft/air_cert/design_approvals/>.

Table 2. Product Timeline of Certification Process

Pre-Product Certification	Phase I	Phase II	Phase III	Phase IV	Phase V
Partnership for Safety Plan					
	Project Specific Certification Plan				
	Type Certification Basis				
			Compliance Checklist		
	Type Design				
		Type Certificate Application			
		Certification Project Notification			
	Safety Assessments				
	Issue Papers				
	Special Conditions				
	Equivalent Safety Findings				
		Maintenance Review Board Report			
	Applicant Inspection, Ground Test, Flight Test Results				
	Compliance Demonstrations				
	Conformity Inspection Results				
				Type Inspection Authorization	
				Type Inspection Report: Ground	
				Type Inspection Report: Flight	
				Flight Manual	
				Instructions for Continued Airworthiness	
				Type Certificate	
					Compliance Summary Document
					Certificate Management Plan

An applicant can use an existing certification basis to substantially reduce the costs of compliance by showing that the type design being presented for approval is derived from a previously certified airplane. These derivative designs, or "changed products,"[116] allow applicants to propose changes to type designs of previously certified airplanes and retain the original TC. The FAA will approve changes to the original TC if they find that the changes are not significant. If the FAA finds that a proposed change is significant (as defined by 14 CFR 21.101[117]), the applicant must establish a new certification basis. Further, if the changes incorporate new or novel features that are not covered by regulation, the certification basis may also include special conditions, as discussed in Appendix A.

For applicants, the advantages of a derivative design are twofold. First, the applicant can save considerable time and money by using the results of the analyses, tests, and inspections conducted during the original type certification process to demonstrate compliance. Second, the regulations that apply to the derivative design are those that were in effect on the date of the original TC, not the date of the application for the new TC. Although the FAA encourages applicants to update the certification basis with any changes to requirements issued after the original TC was approved, those updates are not required.

Approval of a derivative design may allow design deficiencies introduced with the original TC to be carried over into subsequent models, as indicated by the USAir flight 427 and Alaska Airlines flight 261 investigations. The Safety Board found that, for flight 427, the FAA had stated its concerns about the Boeing 737 rudder servo valve design during the original certification, and Boeing had also detected and corrected problems with the design prototype. As for flight 261, the Board found that early experience with the DC-9 jackscrew assembly wear rate prompted McDonnell Douglas to introduce the end play check procedure and wear limit. Because subsequent models of the 737 and the DC-9 were derivative designs, there was no requirement for these issues to be revisited during subsequent certification activities.

Demonstrating Compliance

Once the certification basis is established, the applicant demonstrates to the FAA that the airplane design complies with Federal regulations. This is the type certification phase that is the most time consuming and resource intensive and is most closely related to

[116] Title 14 CFR 21.101, *Changes to Type Certificates*. Guidance for changed products is found in U.S. Department of Transportation, Federal Aviation Administration Advisory Circular, AC 21.101-1, *Establishing the Certification Basis for Changed Aeronautical Products*, April 28, 2003.

[117] Title 14 CFR 21.101, paragraph b(1), states that a change is automatically considered significant if "(i) the general configuration or the principles of construction are not retained," and "(ii) The assumptions used for certification of the product to be changed do not remain valid." In addition, 14 CFR 21.19, *Changes Requiring a New Certificate,* indicates that a proposed design is significantly different from an existing design when the proposed changes are "so extensive that a substantially complete investigation of compliance with the applicable regulations is required."

the certification issues identified in the four accident case studies. The extent of the activities associated with demonstrating compliance is shown in tables B1–B6 in Appendix B.

In its most basic form, demonstrating compliance is conducting either analyses or tests. Establishing the certification basis determines, to a large extent, which analyses and tests must be conducted, and the applicant can select from among a number of different methodologies. There are two basic types of compliance methods:[118]

- methods that demonstrate compliance through adherence to specific design and test criteria, and are typically deterministic, or
- methods that demonstrate compliance using probabilistic risk analysis techniques.

Many of the airworthiness standards spelled out in 14 CFR Part 25 are of the first type, requiring adherence to specific design criteria concerned with aerodynamic performance, flight characteristics, and structural loads and strength requirements. Those regulations set specific design and/or performance criteria, and compliance is demonstrated through engineering analysis, simulation, or ground and flight tests. The evaluation of design features is assumed to be deterministic so that specific tolerances and limits can be explicitly stated and analyzed. Failures are treated as deterministic, and analyses and tests focus on the ability of the damaged structure or component to allow continued safe flight and operation.

In general, human factors considerations for certification are also specified in regulations as specific design criteria. For example, the workspace environment required by the flight crew is covered by 14 CFR 25.771–25.785, which specifies minimum standards for occupant space, sightlines through windows, and cockpit control knob shape. Other regulations, such as 14 CFR D25.1, state in general terms human factors requirements related to minimum crew, workload, and functionality of aircraft systems. Some of the advisory material made available by the FAA provides very specific design guidance related to human factors, especially in the area of avionics. AC 25-11[119] provides detailed design criteria for displays, covering such topics as color-coding, symbology, clutter, and attention-capturing requirements. AC-25.1329 also provides detailed human factors design criteria for the autopilot and the requirements for assessing human interaction with the autopilot during flight tests. In general, compliance with human factors requirements is demonstrated by adherence to specific design criteria stated in regulation and is evaluated with mock-ups and simulators or during ground and flight tests.

[118] A deterministic approach assumes the same result for a given set of initial conditions, while a probabilistic (stochastic) approach assumes that randomness is present, even when given an identical set of initial conditions. Consequently, a probabilistic approach will always assume uncertainty in the result. Probabilistic methods can be viewed as inclusive of all deterministic events with a finite probability of occurrence.

[119] FAA AC 25.11, *Transport Category Airplane Electronic Display Systems* (July 16, 1987).

In contrast to specific design criteria stated in regulations, the second type of method for determining compliance outlined in AC 25.1309-1A[120] and governed by 14 CFR 25.1309 treat failures as *probabilistic* and use a stochastic approach to assess the consequences of system failures. The focus is on understanding the functional significance of aircraft systems, determining the risks to safety of flight associated with a failure condition, and using probability distributions to determine the frequency of occurrence of a failure condition and its effects on overall system function. In the context of 14 CFR 25.1309, the systems of interest are equipment and their installations. Guidance provided by AC 25.1309-1A specifically states that the regulation does not apply to Subparts B and C of 14 CFR Part 25 that pertain to performance, flight characteristics, and structural load and strength requirements.[121]

Fail-Safe Design Concept

Fundamental to the notion of safety-critical systems in certification is the fail-safe design concept, which "considers the effects of failures and combinations of failures in defining a safe design."[122] The concept has a different meaning for structures than for systems: fail-safe for *structures* is concerned with residual strength after sustaining damage; fail-safe for *systems* is concerned with the functional implications of a failure condition and its probability of occurrence. Although both concepts have the same goal—a safe design—the approaches to achieving that goal are different.

Fail-safe for structures is governed by 14 CFR 25.571 and the methods of compliance are outlined in AC 25.571-1C.[123] In general, the structural components of an airplane (such as the airframe and wings) are designed such that "an evaluation of the strength, detail design, and fabrication must show that catastrophic failure due to fatigue, corrosion, manufacturing defects, or accidental damage, will be avoided throughout the operational life of the airplane."[124] However, after the 1988 Aloha Airlines flight 243 accident,[125] where 18 feet of the upper crown skin and structure separated from the fuselage, there has been a greater emphasis on damage tolerance. A damage tolerance evaluation of structure ensures that "should serious fatigue, corrosion, or accidental damage occur within the design service goal of the airplane, the remaining structure can withstand reasonable loads without failure or excessive structural deformation until the damage is detected."[126]

---

[120] The process is also described in SAE ARP4761.

[121] FAA AC 25.1309-1A, section 3.

[122] FAA AC 25.1309-1A, paragraph 5.

[123] FAA AC 25.571-1C, *Damage Tolerance and Fatigue Evaluation of Structure*, April 29, 1998.

[124] Title 14 CFR 25.571, section a.

[125] National Transportation Safety Board, *Aloha Airlines, Flight 243, Boeing 737-200, N73711, near Maui, Hawaii, April 28, 1988,* Aviation Accident Report NTSB/AAR-89/03 (Washington, DC: NTSB, 1989).

[126] FAA AC 25.571-1C, *Damage Tolerance and Fatigue Evaluation of Structure*, section 6a.

Fatigue safe-life was the predominant approach to evaluating structure before the shift to damage tolerance.[127] The emphasis was empirical with the fatigue life of a structure defined as the number of bending cycles to failure. Once the fatigue life of a structure was determined, a safety factor was added to the estimated fatigue life to arrive at the safe-life of a structure. Damage tolerance emphasizes the physics of crack growth and is concerned with setting life limits (that is, inspection intervals that are based on the time for a crack to grow or propagate).[128] Regulations and advisory materials are very specific about the design features to be used to ensure damage tolerance, including multiple load path construction, crack stoppers, materials and stress levels that provide a slow rate of crack propagation, and designs that ensure detection before unacceptable or widespread damage occurs.

A damage tolerance evaluation typically "consists of a deterministic evaluation of the design features"[129] to ensure that airplane structural components are damage-tolerant. AC 25.571-1C identifies these components as principal structural elements (PSE),[130] and may include components of wings and empennage, fuselage, landing gear and attachments, and engine mounts. The evaluation identifies failures in terms of loading conditions and possible damage and then uses structural tests or analyses to substantiate that the design objective was achieved. The evaluation also generates data needed for inspection programs to ensure detection of damage during the operational life of the component. Such evaluations and tests rely on engineering analyses—such as finite element analysis and structural analysis—and use quantitative approaches to establish the response of an aircraft component to various conditions of fatigue, corrosion, manufacturing defects, or accidental damage.

Fail-safe for systems treats failures differently. A *failure*, as defined in AC 25.1309-1A and in Society of Automotive Engineers (SAE) ARP4761,[131] is a loss of function or a malfunction of a system, and differs from a *failure mode*, which is the way a failure in an item occurs. The focus is on understanding the functional significance of aircraft systems, determining the risks to safety of flight associated with a failure condition, and using probability distributions to determine the frequency of occurrence of a failure condition and its effects on overall system function. The purpose of the fail-safe design concept for systems is to meet the following design objectives stated in 14 CFR 25.1309:

> Airplane systems and associated components, considered separately and in relation to other systems, must be designed so that—

---

[127] U.S. Department of Transportation, Federal Aviation Administration, *Damage Tolerance Assessment Handbook*, *Vol. I: Introduction, Fracture Mechanics, Fatigue Crack Propagation* (Cambridge, MA: Volpe National Transportation Systems Center, 1993), Section 1.3.

[128] FAA *Damage Tolerance Assessment Handbook,* Section 1.3.2.

[129] FAA AC 25.571-1C, section 6c.

[130] FAA AC 25.571-1C, section 6d, defines a PSA as "an element of structure that contributes significantly to the carrying of flight, ground, or pressurization loads, and whose integrity is essential in maintaining the overall structural integrity of the airplane" and lists examples.

[131] SAE ARP4761.

> The occurrence of any failure condition which would prevent the continued safe flight and landing of the airplane is extremely improbable,[132] and
>
> The occurrence of any other failure condition which would reduce the capability of the airplane or the ability of the crew to cope with adverse operating conditions is improbable.[133]

The regulation also specifies that warning information about the failure condition be provided to the crew so that they may take the appropriate corrective action. These two design objectives provide the basis for airplane certification standard practices and establish the approach to be used to determine the relative importance (and severity) of a system failure condition.

The two approaches to demonstrating compliance reveal a regulatory distinction between aircraft systems and aircraft structures. Demonstrating compliance for *aircraft structures* and *aircraft performance* typically uses *deterministic* methods that apply predetermined standards or criteria to assess the effects of fatigue, corrosion, and aerodynamic forces on aircraft components and aircraft strength capabilities. For example, 14 CFR 25.301 states that "strength requirements are specified in terms of limit loads (the maximum loads to be expected in service) and ultimate loads (limit loads multiplied by prescribed factors of safety),"[134] and 14 CFR 25.303 states that "a factor of safety of 1.5 must be applied to the prescribed limit load which are considered external loads on the structure."[135]

Conversely, demonstrating compliance for *systems* uses *probabilistic* risk assessment methods that use qualitative and quantitative risk analysis techniques to assess the effects of failures on system *function* and *performance*. According to 14 CFR 25.1309, the analysis must consider possible failure modes (including malfunctions and damage from external sources), the probability of multiple failures and undetected failures, and the effects of those failures on the aircraft and its occupants. For example, 14 CFR 25.1333, "Instrument Systems," states that—

> the equipment, systems, and installations must be designed so that one display of the information essential to the safety of flight which is provided by the instruments, including attitude, direction, airspeed, and altitude will remain available to the pilots, without additional crewmember action, after any single failure or combination of failures that is not shown to be extremely improbable.[136]

---

[132] FAA AC 25.1309-1A, paragraph 10b, defines *extremely improbable* failure conditions as those having a probability on the order of $1x10^{-9}$ or less (1 in one billion).

[133] FAA AC 25.1309-1A, paragraph 10b, defines *improbable* failure conditions as those having a probability on the order of $1x10^{-5}$ or less (1 in 100,000), but greater than on the order of $1x10^{-9}$.

[134] Title 14 CFR 25.301, section a.

[135] Title 14 CFR 25.303.

[136] Title 14 CFR 25.1333, section b.

Both approaches for demonstrating compliance have their advantages. The use of engineering analysis and tests has a long regulatory history that has produced design criteria developed over decades of flight experience. The design criteria in regulations evolve, changing as the need arises and as experience is gained with specific types of materials, components, and design features. Consequently, in certain areas of airplane design, the knowledge required to evaluate structures and components is well established.

A difficulty arises when the distinction between structure and systems is not clear, as in the case of the Alaska Airlines flight 261 MD-83 jackscrew assembly. During the public hearing for that accident, the FAA acknowledged that the jackscrew assembly had both structural and systems elements and therefore required compliance with different sets of regulations. The distinction was also used to justify an approach to demonstrating compliance where the kinds of risk analysis outlined in AC 25.1309-1A would not apply. Consequently, the notion of assessing higher-level airplane system function based on lower-level component failure modes (for example, the loss of threads in the acme nut and screw) was not required by regulation. Although new policy outlined in ANM-03-117-10 places greater emphasis on a systems approach to flight-critical systems, the criteria for identifying those components apply only to airplane systems and associated non-structural components.[137] Furthermore, none of the regulations, including 14 CFR 25.1309 (and the concomitant material in AC 25.1309-1A), explicitly address human error or the potential risks associated with crew interaction with airplane systems.

Conducting Safety Assessments

The risks to systems that are critical to safe flight and operation are evaluated in type certification during safety assessments. Safety assessments are the primary means by which the certification process identifies failure conditions, evaluates the potential severity of those failures, and determines their likelihood of occurrence. The safety assessment process is outlined in AC 25.1309-1A, described in detail in SAE guidelines,[138] and summarized in Appendix A of this report. All safety assessments are conducted by the applicant and are reviewed and accepted by the FAA.

A system is deemed critical if its failure would prevent the continued safe flight and landing of the airplane, or if it would reduce the capability of the airplane or the ability of the crew to cope with adverse operating conditions. AC 25.1309-1A establishes an approach that uses risk and hazard analysis to identify safety-critical systems. The emphasis in the analysis is on identification of a *failure condition*, not a failed *component*, and on the functional effects of the failure (or failures) on the airplane and its occupants. This point bears repeating: *the criticality of a failure condition—not the criticality of a faulty component—will determine if a system is safety critical.*

[137] FAA Memorandum ANM-03-117-10, p. 2.

[138] SAE ARP4761.

For example, a jammed elevator caused by a broken linkage may not be a threat to flight safety unless the fault (the broken linkage) results in a failure condition (an airplane attitude caused by the jammed elevator) that adversely affects the functional ability of the airplane to fly or land or the crew's ability to maintain control. Consequently, the criticality of a system becomes evident through the assessment of risk during safety assessments and is based on the adverse effect on overall system function. As previously discussed, safety assessments exclude consideration of failures that pertain to performance, flight characteristics, and structural load and strength requirements.

The FAA is developing new guidance policy[139] to clarify the use of risk assessment techniques in safety assessments and in the identification of flight-critical system components. According to that policy, the upcoming revision to AC 25.1309-1A includes five severity classes: no safety effect, and minor, major, hazardous, and catastrophic effects.[140] A component is critical, states the policy, if a single failure results in a hazardous or catastrophic failure condition; if two failures result in a hazardous failure condition or a combination of three failures results in a catastrophic failure condition; or all components contribute to a significant latent failure.[141] The differences among the classes are associated with effects on the airplane, effects on occupants and crew, and the qualitative and quantitative estimates of failure condition probability. The choice of functions and failure conditions provides the foundation for all assessment of risks to systems. Poor choices can lead to incomplete analyses and incorrect classification of failure condition severity. As a result, potentially dangerous failure conditions can remain undetected, especially if the assumptions underlying the analysis do not adequately reflect operational scenarios and service history. The importance of a comprehensive, systematic process for identifying failure conditions was evident when the FAA's ETEB review of the Boeing 737 rudder system, conducted after the USAir flight 427 investigation, identified multiple failure conditions that had not been considered in the original type certification process.

Safety assessments do not begin with a pre-determined set of safety-critical systems, but must identify potential hazards through analysis. Safety assessments proceed in a stepwise, data-driven fashion, starting with systems at the functional level, and adding more specific design and implementation detail to address specific hazards, the potential effects of those hazards on the airplane and occupants, and possible solutions. The probability of a failure and the level of hazard classification are then used to determine the level of detail in an analysis for a particular system and its corresponding equipment. Thus, the final definition and characterization of a safety-critical system is the result of the analyses conducted during a safety assessment.

Analytic and qualitative methods used in safety assessments include functional hazard assessments, preliminary system safety assessments, preliminary hazard analyses, and system safety assessments. Methods may incorporate specific techniques, such as

[139] FAA Memorandum ANM-03-117-10.

[140] FAA ANM-03-117-10, App. 2, Sec. 3.

[141] FAA ANM-03-117-10, page 3.

fault tree analyses, failure modes and effects analyses, failure modes and effects summaries, dependence diagrams, and Markov analyses. The techniques can be characterized as providing either a top-down or bottom-up analysis of a design. A top-down analysis, using functional hazard assessments and preliminary system safety assessments, begins with high-level functional descriptions and design objectives and produces a high-level description of the system architecture and associated failure conditions and a classification of failure severity. Functions are defined and, once the system design is finalized, failures are mapped to specific system components. A bottom-up analysis—using failure modes and effects analysis, for example—typically begins with a single failure condition at the lowest level of a system. The purpose of a bottom-up analysis is to determine how a failure condition at one level affects the system at the next higher level. This analysis usually begins with basic components and component data and builds upon those data to conduct the requisite levels of analysis. The challenge for the analyst is to ensure that the systems and failure conditions identified in a bottom-up analysis are reconciled with the functions and functional failures identified in the top-down analysis.[142]

Issue papers are another means by which the FAA can recommend additional or more comprehensive safety assessments. In general, issue papers are used by the FAA to identify and resolve any significant certification issue or problem that arises (the process for generating issue papers and resolving the issues in them is discussed in Appendix A). What constitutes a significant issue is defined in FAA Order 8110.4C and can include new technology or novel design, the certification basis and means of compliance, environmental considerations, unsafe conditions, and special conditions. Issue papers in draft form are "prepared by government employees for use in effecting project management containing opinions, advice, deliberations and recommendations made in the course of developing official action by the government"[143] and are exempt from public disclosure. Once issue papers are approved by the appropriate FAA directorate, they may be available for public release.

The USAir flight 427 investigation provides an example of how an issue paper is used. In 1996, the FAA developed an issue paper to address flight control jams in the certification of Boeing 737-600, -700, and -800 series airplanes. In that issue paper, the FAA defined "normally encountered roll/yaw control positions" and outlined requirements for compliance of the -600, -700, and -800 series airplanes using the control positions and scenarios defined by Boeing. One of the requirements was that normal roll/yaw control positions would be those required to counteract rudder jams during normal approach and landing configurations. The FAA used the issue paper to define both "normal" control positions and the scenarios for demonstrating compliance. The USAir flight 427 investigation found (and confirmed by the FAA's CDR team in 1995) that the control positions and scenarios defined in the issue paper did not sufficiently characterize all of the situations that might be encountered in normal operations.

[142] See FAA AC 25.1309-1A and SAE ARP4761.

[143] FAA Order 8110.4C, Appendix 12, paragraph 3c.

The primary advantage of an issue paper is that one can be proposed at any time in the certification process up to issuance of the TC (as shown in table 2). An issue paper is therefore a powerful tool for the government in alerting project management—both the FAA's and the applicant's—of the need to address a specific certification issue and is most commonly used in safety assessments to require additional or more comprehensive analyses. An important point is that issue papers, which are considered to be draft material, are not part of the official certification project file and are therefore exempt from public disclosure. Thus, there is no requirement that issue papers be maintained as part of the official documentation for the airplane's TC.

Post-Certification Processes

Issuing the TC marks the end of the type certification process and the beginning of the transition to production and air carrier operations. The Instructions for Continued Airworthiness (ICA),[144] which represent the basic initial maintenance plan for the airplane, are an important component of the TC for air carrier operations. The ICA is an important document because it conveys to operators and maintainers the manufacturer's assumptions concerning requirements for preserving the airworthiness of an airplane and its components while in service.

The ICA is required by regulation to have two parts: the airplane maintenance manual and the maintenance instructions.[145] The airplane maintenance manual describes the airplane and its components, component operation, and necessary maintenance and preventive maintenance. Also included is any servicing information that—

> covers details regarding servicing points, capacities of tanks, reservoirs, types of fluids to be used, pressures applicable to the various systems, location of access panels for inspection and servicing, locations of lubrication points, lubricants to be used, equipment required for servicing, tow instructions and limitations, mooring, jacking, and leveling information.[146]

Maintenance instructions provide the scheduling information for all airplane maintenance. The MRB Report using the MSG-3 process, described under *Project Specific Certification Plan,* is part of the maintenance instructions. These instructions are especially important in that they specify the applicant's recommendations for overhaul periods and provide cross-references to airworthiness limitations, troubleshooting information, requirements for removing and ordering the removal of parts, and procedures for testing components. These are the instructions that McDonnell Douglas and Boeing provided to Alaska Airlines stating the recommended lubrication and inspection intervals for the MD-80 jackscrew assembly.

---

[144] Title 14 CFR 21.50b.

[145] Title 14 CFR H25.3.

[146] Title 14 CFR H25.3, paragraph a-4.

In addition to establishing the requirements for continued airworthiness and operator oversight, other post-certification activities concentrate on documenting the certification process and establishing plans for managing the certificate. Details of these post-certification activities are provided in Appendix A, but are summarized here.

Several products are used to document the certification process. The Certification Summary Report is "an executive summary containing high-level descriptions of major issues and their resolution. The report should be used as a means for retaining corporate knowledge and lessons learned that could be beneficial for future type certification projects involving the same or similar type design."[147] The summary is not intended to be comprehensive, but focuses on lessons learned, areas for process improvement, and significant technology issues or novel design features. The ACO also prepares and maintains a project file that contains only those documents showing a decision or action by the FAA and copies of all of the major certification products.[148]

Provisions are made during post-certification to ensure that continued airworthiness issues will be handled after the aircraft is in service. To that end, a certificate management plan and a continued airworthiness plan are the final products of the certification process. As part of this process, specific provisions are made for in-depth post-certification reviews of potentially unsafe design features or products. Called special certification reviews (SCRs), these reviews are a way for the FAA "to evaluate the type certification project and potentially unsafe design features on previously approved products." An SCR may be initiated by the accountable directorate or "as service experience dictates."[149] When concerned with compliance, an SCR may explore every aspect of the safety problem, including the applicant's original certification data, inspection of prototype and production articles, and "the adequacy of the applicable regulations and policy material."[150]

Other mechanisms are also in place to identify problems encountered during operations and maintenance that may lead to FAA oversight action. The FAA's Air Transportation Oversight System (ATOS) was implemented in 1998 to enhance the Flight Standards air carrier surveillance requirement. According to the FAA, the ATOS "process assesses the safety of air carrier operating systems using system safety principles, safety attributes, risk management, and structured system engineering practices."[151] The purpose of ATOS is to put in place a Part 121 air carrier surveillance program under the supervision of the FAA's Principal Inspectors and Certificate Management Team (CMT). FAA guidance states, "ATOS surveillance assesses an air carrier against established performance measures in relation to specific regulatory requirements and safety attributes for each element of an air carrier's systems."[152]

---

[147] FAA Order 8110.4C, paragraph 2-7a(1).

[148] For a complete list, see FAA Order 8110.4C, appendix 10, figure 1.

[149] FAA Order 8110.4C, paragraph 2-7e(1a).

[150] FAA Order 8110.4C, paragraph 2-7(1f).

[151] U.S. Department of Transportation, Federal Aviation Administration Order 8400.10, *Air Transportation Operations Inspector's Handbook,* April 6, 2005, Appendix 6, Section 2, paragraph 122.

[152] FAA Order 8400.10, Appendix 6, Section 2, paragraph 125.

The ATOS process focuses on risk identification, assessment, and management, and includes a number of environmental and operational risk indicators. Surveillance data are gathered and contained in databases and are analyzed using a variety of qualitative and quantitative risk management and hazard analysis techniques. The initial phase of ATOS implementation began with 10 major air carriers including American Airlines and Alaska Airlines. A General Accounting Office (GAO) report on ATOS in 1999 was generally favorable, but pointed out a number of critical areas for improvement, including inspector training and data requirements for effective analysis. GAO recommended that the FAA not expand the ATOS program beyond the initial 10 air carriers until the problems identified in the report were corrected. According to congressional testimony given by the FAA's associate administrator for regulation and certification in 2002, ATOS was fully implemented for the original 10 air carriers, and many improvements had been made to ATOS since its inception. The associate administrator went on to state that a new version of ATOS was anticipated in 2004 that would further enhance risk assessment capabilities.[153] In April 2005, major revisions were made to ATOS policies and procedures that allow "CMTs to apply ATOS policies and procedures more consistently for all air carriers."[154]

Other programs are also in place to support certificate management and continued airworthiness issues. The FAA's Aircraft Certification Evaluation System (ACSEP)[155] is concerned with ensuring that the holders of a type production approval or delegated facilities meet the requirements set forth in Federal regulations. ACSEP uses FAA engineering, flight test, and manufacturing inspection personnel to evaluate control of FAA-approved type design, production activities, and design approval systems. Consequently, the program focuses oversight and inspection on manufacturers, part suppliers, and delegated facilities and their adherence to Federal regulations. Once these continued airworthiness and certificate management plans are put in place, the airplane is ready for service in air carrier operations.

In summary, the TC (and its accompanying ICA) and other post-certification activities establish the transition from certification to operations and provide the basis for continued airworthiness and operations oversight.

---

[153] Testimony of Nicholas A. Sabatini, Associate Administrator for Regulation and Certification, Federal Aviation Administration, before the U.S. Congress Committee on Transportation and Infrastructure, Subcommittee on Aviation, on FAA Oversight of Passenger Aircraft Maintenance, April 11, 2002.

[154] FAA Order 8400.10, Appendix 6, Section 1, paragraph 104.

[155] U.S. Department of Transportation, Federal Aviation Administration Order 8100.7C, *Aircraft Certification Systems Evaluation Program,* October 12, 2005.

Other Efforts to Study Certification

Certification has been the focus of several other recent studies: the FAA Commercial Airplane Certification Process Study; the RTCA Task Force 4 on Certification, and the National Research Council (NRC) assessment of the FAA Aircraft Certification Service's safety management process. Many of the certification issues revealed in the Safety Board's investigations were also of interest to these groups. Rather than provide a comprehensive review of the three studies, this report highlights the issues in these studies that parallel the issues in this report.

FAA Commercial Airplane Certification Process Study

The FAA organized a joint government/industry certification study that specifically addressed safety-related processes. The Commercial Airplane Certification Process Study (CPS) was initiated in 2001 to assess the effectiveness of the Agency's certification process throughout the life cycle of an aircraft. CPS used historical reports and accident data to identify critical certification issues. The list of accidents used by CPS to identify issues significantly overlaps the accidents shown in Appendix C. CPS results, published in 2002, were a series of findings that highlighted the need to identify and track critical systems, conduct airplane-level assessments, improve communication between certification and operations, and better use lessons learned in design, operations, and maintenance.

CPS reported that it conducted a process analysis of certification to identify process improvement opportunities, but the final report did not document the methodology used to conduct the analysis. The report referred to both top-down and bottom-up analytic approaches; however, much of the analysis presented in the final report appeared to be based on a review of an accident list and on information provided by government and industry representatives. Overall, the focus of the report was high level and primarily concerned with issues related to communications and information interfaces between certification, operations, and maintenance.

The CPS team noted that critical safety systems are the product of both the design and the safety assurance decision-making process accomplished during certification. The criticality of a system becomes evident when design assumptions and functional interactions among safety-critical features are explored. The CPS team also indicated that critical systems are not consistently identified during design and certification, and the assumptions underlying the risk analysis associated with those systems are rarely revisited once the aircraft is placed in service. As a result, the CPS team is considering mechanisms for identifying and tracking critical systems throughout the life cycle of the airplane.

Although the team acknowledged the importance of safety assessments in the identification of safety-critical systems and was considering airplane-level risk and hazard analysis as a way to address overall aircraft system performance, neither the final report nor the strategic plan recommended adoption of a comprehensive systems engineering approach in certification. Furthermore, CPS did not discuss a 1998 NRC recommendation for a comprehensive safety assessment process emphasizing the principles of risk management and the use of risk analysis tools. The recommendation was a result of a study conducted by the NRC as a result of an FAA request to study AIR's safety management process. (The NRC study is discussed in more detail in the following section.) In fact, the CPS final report did not mention the NRC study.

The life cycle of a product was discussed in CPS and characterized in its Strategic Plan in terms of various life cycle "themes," including critical safety systems, data management, human factors, and operator oversight. The CPS final report stated that "as with all design assurance processes, for the safety assessment to be effective, it must trace through the entire life cycle of the product."[156] CPS pointed out in its final report the need for better communication between certification and operations and maintenance, and made recommendations to change or clarify regulations, policy, and guidance. But the report did not recommend adoption of a life-cycle engineering approach where tracking, monitoring, and continuously assessing critical systems would be inherent activities and would require the flow of information among the various parties involved in certification, operations, and maintenance.

CPS also identified human factors as one of nine major themes and concluded that "design techniques, safety assessments, and regulations do not adequately address the subject of human error in design or in operations and maintenance."[157] The report went on to recommend that the processes used to incorporate human behavior and performance in safety assessments during certification must be improved, but provided no specific recommendations on how such improvements should be made.

RTCA Task Force 4 on Certification

Begun in 1998, the RTCA study on certification focused on communications, navigation, surveillance (CNS), and air traffic management (ATM) systems. RTCA, Inc., is a private, nonprofit corporation contracted by the Federal government to address requirements and technical concepts for aviation. Many RTCA activities for the FAA concern developing standards and technical advisory documents (for example, RTCA/DO 178B for software systems). The RTCA Task Force was organized in response to the FAA's focus on modernization of the National Airspace System (NAS) and its initiatives to implement free flight. The Task Force was organized into four working groups (WGs);

[156] U.S. Department of Transportation, Federal Aviation Administration, *Commercial Airplane Certification Process Study* (Washington, DC: Federal Aviation Administration, March 2002), p. 7.

[157] FAA *Commercial Airplane Certification Process Study*, p. 9.

one of the four—WG4—was concerned with the certification process and services provided by the FAA and international certification authorities.

Although the Task Force did not specifically address aircraft, its treatment of the NAS did consider how the FAA's certification process dealt with new products and equipment. One of the major findings of the Task Force was that the overall, end-to-end system was not being properly addressed, a finding consistent with this report's conclusion of the lack of a comprehensive systems engineering approach. In its final report, the Task Force stated that "safety and performance assessments are done on the elements of a system, but without the overall understanding of the relationship of individual elements' responsibilities and contribution to performance and safety."[158] The Task Force also pointed out that no person or organization is responsible for ensuring that an overall system perspective is included during certification.

Task Force findings again supported the conclusion that an overall systems engineering approach to certification was required, but did not make specific recommendations about the application of systems engineering or life cycle engineering principles to certification.

National Research Council Report on Improving Continued Airworthiness

The FAA asked the NRC to evaluate the safety assessment process used by the AIR. One goal of the NRC study focused on AIR's safety management process and the ability of that organization to identify and manage risk. The final report was published in 1998 with recommendations.

The NRC identified the need for a comprehensive safety assessment process that would allow the FAA to take corrective action based on accident, incident, and operational data. Such a process could be put in place, concluded the committee, by emphasizing the principles of risk management and the use of risk analysis tools. In addition to putting together a comprehensive risk management program, the committee believed that the FAA's failure data analysis efforts could be improved "by relying more on scientific and engineering information to supplement operational and maintenance data."[159] The NRC also found FAA's data collection and analysis to be fragmented and recommended that the FAA develop a process to facilitate communication and coordination between Certification and Flight Standards. Such an exchange of continued airworthiness information, stated the committee, was necessary for an effective safety assessment program.[160]

---

[158] *Final Report of RTCA Task Force 4, Certification* (Washington, DC: RTCA, Inc., 1999), p. 69.

[159] National Research Council, *Improving the Continued Airworthiness of Civil Aircraft* (Washington, DC: National Academy Press, 1998), p.35

[160] *Improving the Continued Airworthiness of Civil Aircraft,* pp. 45-46.

Both the NRC study and the Safety Board investigation of TWA flight 800 were concerned about the effectiveness of risk analysis and risk management methods, but for different reasons. Whereas the NRC study believed, in general, that the FAA needed to improve its risk assessment process, the Board stated a concern "that undue reliance is being placed on such analyses as proof that ignition sources have been precluded" and the possibility that "unrealistic or otherwise flawed data can be used to develop fault trees."[161] The Board's concerns were the result of a review by NASA of the risk analysis provided by Boeing during the investigation to evaluate the potential risk of explosion in the center wing fuel tank. The lack of good data, adequate probability estimates, and validation of the methodology were all central to the Safety Board's concerns about the validity of the risk assessments, and led the Board to conclude that FMEAs and fault tree analyses "should not be relied upon as the sole means of demonstrating that an airplane's fuel tank system is not likely to experience a catastrophic failure."[162]

FAA's ability to continuously assess safety-critical systems in light of service history and lessons learned was another area where considerable agreement occurred between the NRC and the Safety Board. In the USAir flight 427 investigation, evidence of rudder anomalies in a number of incidents indicated a potential problem with the rudder system. In Alaska Airlines flight 261, changes to lubrication and inspection intervals were made by the air carrier without sufficient consideration of the adverse effects on the jackscrew assembly. The history of rudder use by pilots in upset recovery, revealed during the investigation of American Airlines 587 and in the NASA special study of in-flight upsets, indicated that the original assumptions about pilot use of rudder were perhaps not valid. TWA flight 800, Alaska Airlines flight 261, and American Airlines flight 587 highlight the NRC conclusion that a more comprehensive risk assessment program for all aspects of aircraft certification and continued airworthiness is needed.

[161] NTSB/AAR-00/03, p. 295.

[162] NTSB/AAR-00/03, p. 297.

Analysis

As discussed in the *Introduction*, the Safety Board has two concerns about type certification: how risks to safety-critical systems are identified, assessed, and documented during the certification process, and how risks to safety-critical systems are assessed throughout the life of the airplane. The first concern most closely relates to the certification phase in which an applicant demonstrates compliance with Federal regulations. The second concern relates to post-certification activities and the interactions among certification, operations, and maintenance.

Identifying and Assessing Safety-Critical Systems

The FAA uses the safety assessment process to identify and evaluate safety-critical functions in systems. The methods and techniques used in safety assessments are well established and the process can be effective in identifying and evaluating hazards to safety of flight. Through the safety assessment process, a system is deemed critical if its failure would prevent the continued safe flight and landing of the airplane, or if its failure would reduce the capability of the airplane or the ability of the crew to cope with adverse operating conditions. The process, as previously discussed, uses risk and hazard analysis to identify failure conditions, evaluate the potential severity of those failures, and determine their likelihood of occurrence. Safety assessments do not begin with a pre-determined set of safety-critical systems, but rather, with a set of criteria for determining the criticality of systems. The analysis emphasizes the identification of a *failure condition*, not a failed component, and the functional effects of the failure (or failures) on the airplane and its occupants. *Safety-critical systems* are defined in this report using the criteria set forth in FAA guidance material for identifying and evaluating failure conditions that are classified as major or catastrophic. The Safety Board concludes that the safety assessment process is an effective way to identify safety-critical systems during type certification. However, the Board believes that the process can be improved in a number of ways.

First, based on an evaluation of failure conditions in the aircraft, safety assessments can produce a list of safety-critical systems associated with those failures that can accompany the TC. FAA's Certification Process Study recognized that the "processes for identification of safety critical features of the airplane do not insure that future alterations, maintenance, repairs, or changes to operational procedures can be made with cognizance of those safety features."[163] Had such a list been available to Alaska Airlines, it would have provided for access to certification analysis information about the design integrity of the jackscrew assembly for the purpose of deciding about changes to lubrication and inspection intervals. The Safety Board concludes that the lack of a

[163] FAA *Commercial Airplane Certification Process Study*, p. 27.

requirement to prepare a list of safety-critical systems during the type certification of a transport-category airplane compromises the ongoing assessment of these systems. Such a list of safety-critical systems could be identified based on the outcomes of the safety assessment process.

Second, the FARs do not explicitly require that the results of safety assessments be preserved in the official type certification project file for ongoing safety analysis. AC 25.1309-1A specifies that safety assessment results be included with the analysis presented to the FAA, and the Certification Summary Report described in Order 8110.4C "is a high-level description of major issues and their resolution"[164] that may not capture the details required to effectively evaluate service history and operational experience. In addition, not all projects require a summary report. Consequently, the rationale, analysis methods, failure scenarios, supporting evidence, and associated issue papers used to identify and assess safety-critical systems may not be available for future review and consideration by the FAA, the manufacturer, or the operators. For example, such materials may have proved useful in assessing the assumptions underlying the US Air flight 427 Boeing 737 servo valve during certification activities for subsequent derivative designs, especially in light of the airplane's rudder-related incident history.

Finally, issue papers that are used to specify the scope and depth of a safety assessment are not necessarily available for future review and consideration. As previously discussed, the FAA uses issue papers to identify and resolve any significant certification issue or problem that arises during the certification process. Significantly, the FAA, not the applicant, generates issue papers as a means to identify potentially unsafe conditions and systems that may require further scrutiny. For example, when new technology or novel designs are proposed for certification, an issue paper can be used to recommend that applicants consider more detailed testing or analysis to determine the effects of potential failure conditions. Issue papers do not, however, necessarily become part of the official type certification project file; according to the FAA, they are exempt from public disclosure in draft form, and are retained only at the discretion of the ACO Manager.

The Safety Board concludes that systems are identified as safety critical through the safety assessment process, but the results of that process—including the rationale, analysis methods, failure scenarios, supporting evidence, and associated issue papers used to identify and assess safety-critical systems—are not consistently documented for future review and consideration. Therefore, the Safety Board recommends that the FAA compile a list of safety-critical systems derived from the safety assessment process for each type certification project, and place in the official type certification project file the documentation for the rationale, analysis methods, failure scenarios, supporting evidence, and associated issue papers used to identify and assess safety-critical systems. [165]

[164] FAA Order 8110.4C, paragraph 2-7a(1).

[165] The project file is described in the *Data Retention* section of FAA Order 8110.4C, paragraph 2-7f.

Excluding Structural Failures from Safety Assessments

Excluding structural failures from safety assessments occurs because Federal regulations specify different methods of compliance for systems and for structures. Although the methods for demonstrating compliance are well founded, this distinction can hinder the identification of safety-critical systems and the application of the fail-safe design concept. For instance, fail-safe, as it pertains to *systems*, applies only to the mitigation of failure conditions covered by 14 CFR 25.1309. Fail-safe, as it pertains to *structures*, "is the attribute…that permits [the structure] to retain its required residual strength for a period of unrepaired use after the failure or partial failure of a principal structural element."[166] The performance of structure is based on the number of operational events (for example, flights, landings, and flight hours) required to reduce the strength of a structural element below its design ultimate value due to cracking.[167] The guidance provided by AC 25.1309-1A specifically states that 14 CFR 25.1309 does not apply to 14 CFR Part 25, Subparts B and C, which pertain to performance, flight characteristics, and structural load and strength requirements.[168] Consequently, structural failures are excluded from safety assessments. Although new policy outlined in ANM-03-117-10 places greater emphasis on a systems approach to flight-critical systems, the criteria for identifying those components apply only to airplane systems and associated non-structural components.[169] The Safety Board found no provisions in existing type certification regulations and advisory materials for considering the functional implications of structural failures in the assessment of safety-critical systems.

The problem created by excluding the functional implication of structural failures from consideration was evident in the Alaska Airlines flight 261 investigation. The FAA used the distinction between structures and systems to explain during the public hearing why a safety assessment of the entire jackscrew assembly did not occur, either during certification of the DC-9 when regulations called for a fault analysis, or during subsequent certification of MD-80 series airplanes covered by the more comprehensive requirements of AC 25.1309-1A. In all cases, because the acme nut was not considered part of a system, it was not required to comply with airplane systems certification requirements.[170] The Safety Board concluded in the Alaska Airlines flight 261 report, however, that "catastrophic single-point failure modes should be prohibited in the design of all future airplanes with horizontal stabilizer trim systems, regardless of whether any element of that system is considered structure rather than system or is otherwise considered exempt from certification standards for systems."[171] A damage-tolerance approach to the design of principal structural elements in transport-category airplanes recognizes that some failures, short of catastrophic, can occur. As a result of the analysis conducted for this report, the

[166] FAA AC 25.571-1C, paragraph 3b.

[167] FAA AC 25.571-1C, paragraph 3c.

[168] FAA AC 25.1309-1A, section 3.

[169] FAA ANM-03-117-10, p. 2.

[170] Alaska Airlines flight 261, NTSB/AAR-02/01, p. 23.

[171] Alaska Airlines flight 261, NTSB/AAR-02/01, p. 180.

Safety Board is concerned that the effect of structural failures on the performance of related systems is not being considered in risk assessments for type certification.

Excluding Human Error from Safety Assessments

Human error is a major, recurring issue in most aviation accidents. The Safety Board has consistently cited personnel as the major cause or factor of accidents, exceeding the proportion of accidents related to aircraft or environmental causes by a large margin. As previously mentioned, human factors considerations for certification purposes are specified in regulations as specific design criteria, and in a way similar to the criteria found for airplane performance, structures, and flight characteristics. Furthermore, a human factors certification plan is advised, but not required. The most rigorous evaluations of human/airplane system interaction occur as part of ground or flight tests using experienced test pilots. This phase of testing occurs late in the certification process after most of the safety assessments are finished and the design finalized.

Human error is referenced in 14 CFR 25.1309, but only in terms of the probability that a failure will adversely affect the crew: "The airplane systems and associated components…must be designed so that…the occurrence of any other failure condition which would reduce the capability of the airplane or the ability of the crew to cope with adverse operating conditions is improbable."[172] Title 14 CFR 25.1309 also addresses the effect of warning information on crew response to a failure condition. Only implicitly does AC 25.1309 suggest the need to analyze the risks associated with human/airplane system interaction failures by considering the "effects on the crewmembers, such as increases above their normal workload that would affect their ability to cope with adverse operational or environmental conditions or subsequent failures."[173]

Safety Board investigations have shown that the potential for human/airplane system interaction failures is increased when an airplane design contains complexities that are difficult for people to discern in an operational context. The problem with a rudder pedal design that produces maximum rudder pedal travel at high speeds with only a fraction of the travel available on the ground was evident to the Safety Board in its investigation of American Airlines flight 587: "The first officer may have failed to perceive that his control wheel and rudder inputs were the cause of the airplane motion in part because that motion may have appeared out of proportion to his pedal inputs."[174]

Unlike other regulations pertaining to airplane structures, performance, and systems, regulations pertaining to human performance do not provide specific guidance about appropriate compliance methods. FAA policy addresses human factors issues in transport-category airplane type certification in terms of procedural and workload

[172] Title 14 CFR 25.1309 paragraph b(2).

[173] FAA AC 25.1309 paragraph 7b(2).

[174] American Airlines flight 587, NTSB/AAR-04/04, pp. 149-150.

analyses and tests, and through mock-ups, simulators, and in-flight evaluations.[175] The functional implications of failures that could result from human interaction with airplane systems and components are not analyzed in safety assessments. The Safety Board is concerned that human interaction failures are not addressed in the assessment of safety-critical systems.

In contrast to commercial aviation, other Federal agencies (like the Department of Energy and DoD, for example) explicitly address human performance in design and development and incorporate human factors knowledge in risk and hazard analyses. The Nuclear Regulatory Commission pioneered the development and use of human reliability analysis and the application of human error probabilities to tasks performed by human operators in nuclear power plant control rooms.[176] As a result, the Nuclear Regulatory Commission's *Handbook of Human Reliability Analysis* has become one of the important references for human reliability analysis. [177]

Department of Defense Directive (DODD) 5000.1 calls for military systems development to "apply human systems integration to optimize total system performance (hardware, software, and human), operational effectiveness, and suitability, survivability, safety, and affordability."[178] The policy directive concludes that this approach will ensure safety especially when it is related to human-system interfaces.[179] DoD MIL-STD-882D, *Standard Practice for System Safety,* outlines the methods and techniques to be used to conduct risk and hazard analyses (including human error analysis) and specifically lists the kinds of human performance that define unacceptable safety-critical conditions.[180] Additional guidance is provided in the *Defense Acquisition Guidebook*[181] and in DoD Handbook, MIL-HDBK-46855a, *Human Engineering Program Process and Procedures,* which references the use of human performance reliability analysis as one way to identify factors that hinder reliable human performance in military systems.[182] Both MIL-STD-882D and MIL-HDBK-46855a are referenced in the guidance and in advisory materials for the FAA's safety risk management program.

---

[175] U.S. Department of Transportation, Federal Aviation Administration Memorandum ANM-99-2, *Guidance for Reviewing Certification Plans to Address Human Factors for Certification of Transport Airplane Flight Decks* (September 29, 1999).

[176] Probabilistic risk assessment (PRA) is one form of risk analysis that, in its latest form, combines event trees that capture the sequence of events in a scenario with fault trees that allow the analysis of all the factors contributing to failure events in the scenario.

[177] A.D. Swain and H.E. Gutman, *Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications*, NUREG/CR – 1278 (Washington, DC: U.S. Nuclear Regulatory Commission, 1983).

[178] DODD 5000.1, *The Defense Acquisition System* (May 12, 2003). paragraph E1.29.

[179] DODD 5000.1, paragraph E1.23.

[180] MIL-STD-882D, paragraph A.4.3.3.1.1.

[181] DODD 5000.1, Chapter 6.

[182] U.S. Department of Defense Handbook MIL-HDBK-46855A, *Human Engineering Program Process and Procedures* (Washington, DC: May 17, 1999), paragraph 8.3.16.

The extensive use of risk-based approaches to human performance by other Federal agencies highlights the importance of human factors issues and the need to specifically consider the risks to system performance associated with human behavior. The extensive procedural character of commercial aviation operations, the well-documented research on pilot behavior and performance, and the preponderance of aviation accidents attributed to human error would appear to support the use of human performance analysis in the assessment of safety-critical systems.

While 14 CFR 25.1309 may be interpreted as implicitly including failures associated with human interaction with airplane systems and the types of structural failures discussed in the previous section, the Safety Board believes that the accepted methods of compliance described in related advisory materials do not require such failure conditions to be explicitly considered. The Board concludes that consideration of structural failure conditions and human/airplane system interaction failure conditions are not required in the certification-related assessments of safety-critical systems, and these exclusions limit the scope of the failure conditions considered during the safety assessment process. The Board recommends that the FAA amend the advisory materials associated with 14 CFR 25.1309 to include consideration of structural failures and human/airplane system interaction failures in the assessment of safety-critical systems.

Monitoring and the Ongoing Assessment of Safety-Critical Systems

Once safety-critical systems have been identified, assessed, and documented during type certification, feedback mechanisms are needed to ensure that the underlying assumptions made during design and certification are continuously assessed in light of operational experience, lessons learned, and new knowledge. These mechanisms require coordination between FAA organizations responsible for certification, continued airworthiness, and operational oversight.

The importance of feedback in the ongoing assessment of safety-critical systems was illustrated by the Alaska Airlines flight 261 accident investigation. The investigation found that changes to maintenance practices and intervals were made without sufficient analysis, justification, and consideration of design assumptions made during certification. As a result, the Safety Board recommended to the FAA that the maintenance procedures and intervals for all critical aircraft components be reviewed to ensure a sound engineering justification, and that any extensions to those intervals "(1) take into account assumptions made by the original designers, (2) are supported by adequate technical data and analysis, and (3) include an appropriate safety margin that takes into account the possibility of missed or inadequate accomplishment of the maintenance task."[183] Monitoring and tracking safety-critical systems was of particular concern to the Board, resulting in a recommendation to establish a program that would track and analyze

[183] NTSB Safety Recommendation A-02-41; full text and status are shown in Appendix C.

jackscrew wear and end play measurements by aircraft registration number and jackscrew assembly serial number, and to report those results to the FAA.[184]

USAir flight 427 and American Airlines flight 587 also illustrate how operational experience may indicate a need to reconsider assumptions made during certification. With regard to USAir flight 427, the FAA was concerned about the rudder system during certification of the Boeing 737-100, and the history of rudder service difficulties uncovered during the investigation led the Safety Board to conclude that those concerns were valid. Review of the 737 rudder system by the FAA's ETEB also identified multiple failure modes that had not been previously considered during certification. The history of rudder use by pilots in upset recovery, revealed during the investigation of American Airlines 587 and in the NASA special study of in-flight upsets, indicated that the original assumptions about pilot use of rudder were perhaps not valid. CPS also recognized the need to validate assumptions made during certification with respect to service experience and added that "certification standards may not reflect the actual operating environment."[185]

USAir flight 427, Alaska Airlines flight 261, and American Airlines flight 587 also provide evidence to support a number of the FAA's CPS findings. CPS found that the processes for identifying safety-critical features of an airplane "do not ensure that future alterations, maintenance, repairs, or changes to operational procedures can be made with cognizance of those safety features."[186] In addition, CPS found no reliable process for validating assumptions made in safety assessments in light of operational and maintenance experience, and that operators may be unaware of those assumptions when making operations and maintenance decisions. CPS also found that existing FAA processes do not capture "the lessons learned from specific experiences in airplane design, manufacturing, maintenance, and flight operations" or make them readily available.[187] The Safety Board agrees with these findings and the need to revise the process to ensure the ongoing assessment of safety-critical systems.

SAE ARP5150, *Safety Assessment of Transport Airplanes in Commercial Service,*[188] provides a process accepted by industry for ongoing assessment of safety-critical systems that would address Safety Board concerns and correct the deficiencies found by CPS. The practice outlined in SAE ARP5150 describes guidelines, methods, and tools for conducting ongoing safety assessments. The process has five general, ongoing, iterative steps, which are summarized in table 3. Critical to the process is the identification and monitoring of safety-related parameters that are used to identify significant safety events and to assess the risks of those events. SAE ARP5150 provides an example that starts with a set of parameters for step 1 (drawn from operators, manufacturers, and the FAA), continues with a set of potential significant safety events for consideration in step 2, and

[184] NTSB Safety Recommendation A-02-45; full text and status are shown in Appendix C.

[185] FAA *Commercial Airplane Certification Process Study*, p. 18.

[186] FAA *Commercial Airplane Certification Process Study*, p. 27.

[187] FAA *Commercial Airplane Certification Process Study*, p. 50.

[188] SAE ARP5150.

elaborates the risk assessment tools and techniques that can be used in step 3. Considerable emphasis is placed on the ongoing and iterative nature of the process. The document states that "to improve safety during the complete airplane life cycle, it is not sufficient to assess the safety of the airplane only during its design phase" and that—

> differences exist or can develop between the assumptions made during the design phase and how the airplanes are actually operated and maintained. For these reasons, safety should be assessed also during the "In-Service" phase of the airplane life cycle. In order to do that, information must be collected, monitored, and analyzed.[189]

Table 3. Steps in the Ongoing Safety Assessment Process.

Step	Description
1. Establish Monitor Parameters	Determine the specific safety structure, objectives, and goals for ongoing safety assessments. Establish the monitoring parameters and their values.
2. Monitor for Events	A continuous process of looking for events of concern. Monitoring is based on the monitor parameters established in step 1.
3. Assess Event and Risk	Initiated when an event is detected, includes assessment of the event sufficient to determine if the event is of concern and preliminary determination of risk for use in prioritizing action plan development. Scope and detail of risk assessment based on seriousness of event.
4. Develop Action Plan	Establishes the correction or improvement to be made to design, operations, maintenance, or training.
5. Disposition Action Plan	Implementation and evaluation of the action plan.

The Safety Board believes that the ongoing safety assessment process outlined in SAE ARP5150 can provide the basis for the continuous assessment of safety-critical systems throughout the life of a transport-category airplane. Properly implemented, the process provides the feedback mechanisms necessary to assess safety-critical systems in light of operational experience, lessons learned, and new knowledge. In addition, an ongoing safety assessment process can provide the basis for collecting service history and operational data that can be used to validate assumptions made during certification, operations, and maintenance, and to prompt timely and comprehensive reviews of potential airworthiness problems. If such an approach is in place when questions arise about service experience (for example, the rudder anomalies uncovered in the USAir flight 427 investigation or the amount of rudder deflection in Airbus airplanes uncovered in the American Airlines flight 903 investigation), a systematic evaluation and review of design features, certification procedures, and operational and maintenance practices can occur.

[189] SAE ARP5150, p. 4.

The ongoing safety assessment process outlined in SAE ARP5150 is consistent with existing provisions in certification regulations that allow reconsideration of airworthiness issues after the airplane is placed in service. Special certification reviews can be initiated to consider potentially unsafe design features of previously approved products.[190] An SCR is initiated by the accountable directorate, which has considerable discretion in the use of evaluation procedures to ensure that "every significant aspect and ramification of the potential safety problem in question" is thoroughly explored, including the "adequacy of the applicable regulations and policy materials."[191] Certification regulations also provide for FAA fact-finding investigations in response to reports or allegations of certification basis noncompliance, which help the FAA decide what action to take. The opportunity for reviews based on these types of triggering events can be part of an ongoing safety assessment program.

Finally, ongoing safety assessments could improve the FAA's ability to evaluate derivative designs. In both the USAir flight 427 and the Alaska Airlines flight 261 investigations, the Safety Board found that some issues raised during the original certification of the aircraft were not addressed during subsequent certification efforts. Once the TC was issued in 1967, questions raised by the FAA about the original Boeing 737 rudder servo unit design were not revisited until the 1992 ground check incident and were not adequately resolved until after the USAir flight 427 investigation was complete. Certification of the MD-83 involved in the Alaska Airlines flight 261 accident was based on the original DC-9 TC issued in 1965. The jackscrew was treated as a derivative design and the potential latent problems associated with the original DC-9 design assumptions were passed along to the MD-80. Despite subsequent extensions to MD-80 lubrication and inspection intervals requiring MRB review and acceptance, no questions were raised about the strength and wear-rate assumptions underlying the design of the jackscrew assembly and its maintenance requirements. Certification activities that accompany a derivative design could be treated as a critical event in the ongoing safety assessment process and provide an opportunity to re-assess, if necessary, safety-critical systems.

The Safety Board concludes that the policy, practices, and procedures put in place for continued airworthiness do not ensure that the underlying assumptions made during design and type certification about safety-critical systems are assessed in light of operational experience, lessons learned, and new knowledge. The Board therefore recommends that the FAA adopt SAE ARP 5150 into 14 *Code of Federal Regulations* Parts 21, 25, 33, and 121 to require a program for the monitoring and ongoing assessment of safety-critical systems throughout the life cycle of the airplane. Safety-critical systems will be identified as a result of A-06-36. Once in place, use this program to validate that the underlying assumptions made during design and type certification about safety-critical systems are consistent with operational experience, lessons learned, and new knowledge.

[190] An example of an SCR is the one initiated by the FAA to investigate Santa Barbara Aerospace's STC ST00236LA-D, after the Swiss Air flight 111 accident. The SCR ultimately resulted in the withdrawal of the in-flight entertainment network certification.

[191] FAA Order 8110.4C, paragraph 2-7e1(f).

A key aspect of an ongoing safety assessment program is the involvement of all parties in the assessment of the airplane from inception to disposal. SAE ARP5150 outlines ways to involve the regulator, designer, manufacturer, operator, and maintainer in the assessment process that are based on life-cycle engineering. Life-cycle engineering is a well-established, goal-driven approach that considers all aspects of the product, personnel, organizations, and facilities that must be put in place to design, manufacture, operate, maintain, and dispose of the product. DODD 5000.1, for instance, specifically references life-cycle engineering in the context of a total systems approach.[192] FAA's own systems safety process emphasizes product life cycle[193] and provides specific guidance for conducting risk assessments throughout the life cycle of the product.[194]

Fostering relationships among certification, operations, and maintenance requires more than establishing lines of communication among the FAA, manufacturers, operators, and maintainers. The investigation of American Airlines flight 587 showed that considerable communication had taken place between manufacturer and operator, including both a written response to a request from American Airlines to review its AAMP pilot training and discussion of pilot use of rudder during upset recovery. Despite discussions between Airbus and American Airlines about the potential risk of emphasizing the use of rudder in upset recovery training, no action was taken by either party or the FAA to systematically review the risks of the training program or pilot use of rudder. Without a systematic approach that translates communication into action, any bridges built to link certification, operations, and maintenance will be inadequate.

[192] DODD 5000.1, paragraph E1.29.

[193] FAA Order 8040.4, paragraph 5.

[194] FAA *System Safety Handbook*.

Conclusions

1. The safety assessment process is an effective way to identify safety-critical systems during type certification.

2. The lack of a requirement to prepare a list of safety-critical systems during the type certification of a transport-category airplane compromises the ongoing assessment of these systems.

3. Systems are identified as safety critical through the safety assessment process, but the results of that process—including the rationale, analysis methods, failure scenarios, supporting evidence, and associated issue papers used to identify and assess safety-critical systems—are not consistently documented for future review and consideration.

4. Consideration of structural failure conditions and human/airplane system interaction failure conditions are not required in the certification-related assessments of safety-critical systems, and these exclusions limit the scope of the failure conditions considered during the safety assessment process.

5. The policy, practices, and procedures put in place for continued airworthiness do not ensure that the underlying assumptions made during design and type certification about safety-critical systems are assessed in light of operational experience, lessons learned, and new knowledge.

Recommendations

As a result of the analysis provided in this Safety Report, the National Transportation Safety Board makes the following recommendations to the Federal Aviation Administration.

Compile a list of safety-critical systems derived from the safety assessment process for each type certification project, and place in the official type certification project file the documentation for the rationale, analysis methods, failure scenarios, supporting evidence, and associated issue papers used to identify and assess safety-critical systems. (A-06-36)

Amend the advisory materials associated with 14 *Code of Federal Regulations* 25.1309 to include consideration of structural failures and human/airplane system interaction failures in the assessment of safety-critical systems. (A-06-37)

Adopt Society of Automotive Engineers ARP5150 into 14 *Code of Federal Regulations* Parts 21, 25, 33, and 121 to require a program for the monitoring and ongoing assessment of safety-critical systems throughout the life cycle of the airplane. Safety-critical systems will be identified as a result of A-06-36. Once in place, use this program to validate that the underlying assumptions made during design and type certification about safety-critical systems are consistent with operational experience, lessons learned, and new knowledge. (A-06-38)

BY THE NATIONAL TRANSPORTATION SAFETY BOARD

MARK V. ROSENKER
Acting Chairman

ELLEN ENGLEMAN CONNERS
Member

DEBORAH A. P. HERSMAN
Member

KATHRYN O'LEARY HIGGINS
Member

Adopted: April 25, 2006

Resource Documents

Air Transport Association of America ATA MSG-3, *Operator/Manufacturer Scheduled Maintenance Development*, Revision 2003.1 (Washington, DC: ATA, 2003).

The Boeing Company News Release, March 16, 1998, *Boeing Next-Generation 737-800 Receives FAA Approval*.

National Aeronautics and Space Administration, *Fault Tree Handbook with Aerospace Applications*, Version 1.1 (Washington, DC: NASA, 2002).

National Aeronautics and Space Administration, *Probabilistic Risk Assessment Procedures Guide for NASA Managers and Practitioners*, Version 1.1 (Washington, DC: NASA, 2002).

National Research Council, *Improving the Continued Airworthiness of Civil Aircraft* (Washington, DC: National Academy Press, 1998).

National Transportation Safety Board, *Aloha Airlines, Flight 243, Boeing 737-200, N73711, near Maui, Hawaii, April 28, 1988,* Aviation Accident Report NTSB/AAR-89/03 (Washington, DC: NTSB, 1989).

National Transportation Safety Board, *Atlantic Southeast Airlines, Inc., Flight 2311, Uncontrolled Collision with Terrain, An Embraer EMB-120, N270AS, Brunswick, Georgia, April 5, 1991*, Aircraft Accident Report NTSB/AAR-92/03 (Washington, DC: NTSB, 1992).

National Transportation Safety Board, *Uncontrolled Descent and Collision with Terrain, USAir Flight 427, Boeing 737-300, N513AU Near Aliquippa, Pennsylvania, September 8, 1994,* Aircraft Accident Report NTSB/AAR-99/01 (Washington, DC: NTSB, 1999).

National Transportation Safety Board, *In-flight Breakup Over the Atlantic Ocean, Trans World Airlines Flight 800, Boeing 747-131, N93119, Near East Moriches, New York, July 17, 1996,* Aircraft Accident Report NTSB/AAR-00/03 (Washington, DC: NTSB, 2000).

National Transportation Safety Board, *Loss of Control and Impact with Pacific Ocean, Alaska Airlines Flight 261, McDonnell Douglas MD-83, N963AS, About 2.7 Miles North of Anacapa Island, California, January 31, 2000,* Aircraft Accident Report NTSB/AAR-02/01 (Washington, DC: NTSB, 2002).

National Transportation Safety Board, *In-Flight Separation of Vertical Stabilizer, American Airlines Flight 587, Airbus Industrie A300-605R, N14053, Belle Harbor, New York, November 12, 2001,* Aircraft Accident Report NTSB/AAR-04/04 (Washington, DC: NTSB, 2004).

National Transportation Safety Board Safety Recommendations A-92-120 and 121, A-96-174, A-02-50, A-02-51, A-02-41, A-02-42, A-02-45, R-97-22.

National Transportation Safety Board Public Docket Document No. 14, "Operations 2—Attachment H—Correspondence from Airplane Manufacturers to American Airlines and Response," September 20, 2002.

RTCA, *Final Report of RTCA Task Force 4: Certification* (Washington, DC: RTCA, 1999).

K. Sabbagh, *Twenty-First Century Jet: The Making and Marketing of the Boeing 777* (New York: Scribner, 1996).

W. Scacchi and P. Mi, "Process Life Cycle Engineering: A Knowledge-Based Approach and Environment," *Intelligent Systems in Accounting, Finance and Management*, Vol. 6, 83-107 (1997).

Society of Automotive Engineers, *Certification Considerations for Highly-Integrated or Complex Aircraft Systems,* SAE ARP4754 (Warrendale, PA: SAE, 1996).

Society of Automotive Engineers, *Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment,* SAE ARP4761 (Warrendale, PA: SAE, 1996).

Society of Automotive Engineers, *Safety Assessment of Transport Airplanes in Commercial Service,* SAE ARP5150 (Warrendale, PA: SAE, 2003).

Statement of NTSB Chairman Jim Hall on FAA Release of ETEB Study on 737 Rudders, NTSB Advisory (Washington, DC: September 14, 2000).

U.S. Department of Defense Directive (DODD) 5000.1, *The Defense Acquisition System* (May 12, 2003).

U.S. Department of Defense Instruction (DODI) 5000.2, *Operation of the Defense Acquisition System* (May 12, 2003).

U.S. Department of Defense MIL-STD-882D, *Standard Practice for System Safety* (February 10, 2000).

U.S. Department of Defense, *Defense Acquisition Guidebook* (December 20, 2004) and available online at <http://akss.dau.mil/dag/welcome.asp>.

U.S. Department of Defense Handbook MIL-HDBK-46855A, *Human Engineering Program Process and Procedures* (May 17, 1999).

U.S. Department of Transportation, Federal Aviation Administration, *Damage Tolerance Assessment Handbook*, *Vol. I: Introduction, Fracture Mechanics, Fatigue Crack Propagation* (Cambridge, MA: Volpe National Transportation Systems Center, 1993).

U.S. Department of Transportation, Federal Aviation Administration, *Commercial Airplane Certification Process Study* (Washington, DC: FAA, 2002).

U.S. Department of Transportation, Federal Aviation Administration, H-8083-25, *Pilot's Handbook of Aeronautical Knowledge* (Washington, DC: FAA, 2003).

U.S. Department of Transportation, Federal Aviation Administration Report, *B737 Flight Control System Critical Design Review* (Washington, DC: FAA, May 3, 1995).

U.S. Department of Transportation, Federal Aviation Administration Memorandum, ANM-03-117-10, *Identification of Flight Critical System Components* (July 24, 2003).

U.S. Department of Transportation, Federal Aviation Administration Memorandum, ANM-99-2, *Guidance for Reviewing Certification Plans to Address Human Factors for Certification of Transport Airplane Flight Decks* (September 29, 1999).

U.S. Department of Transportation, Federal Aviation Administration Memorandum, ANM-112, *Requirement for Fail-Safe Wing Flap Design* (May 15, 1984).

U.S. Department of Transportation, Federal Aviation Administration Advisory Circular, AC 25.11, *Transport Category Airplane Electronic Display Systems* (July 16, 1987).

U.S. Department of Transportation, Federal Aviation Administration Advisory Circular, AC 21-23B, *Airworthiness Certification of Civil Aircraft, Engines, Propellers, and Related Products Imported to the United States* (November 17, 2004).

U.S. Department of Transportation, Federal Aviation Administration Advisory Circular, AC 21.101-1, *Establishing the Certification Basis for Changed Aeronautical Products* (April 28, 2003).

U.S. Department of Transportation, Federal Aviation Administration Advisory Circular, AC 25.571-C, *Damage Tolerance and Fatigue Evaluation of Structure* (April 29, 1998).

U.S. Department of Transportation, Federal Aviation Administration Advisory Circular, AC 25.981-1B, *Fuel Tank Ignition Source Prevention Guidelines* (April 19, 2001).

U.S. Department of Transportation, Federal Aviation Administration Advisory Circular, AC 25.1309-1A, *System Design and Analysis* (June 21, 1988).

U.S. Department of Transportation, Federal Aviation Administration Advisory Circular, AC 61-23C, *Pilot's Handbook of Aeronautical Knowledge* (1997).

U.S. Department of Transportation, Federal Aviation Administration Advisory Circular, AC 121-22A, *Maintenance Review Board Procedures* (March 7, 1997).

U.S. Department of Transportation, Federal Aviation Administration Order 8040.4, *Safety Risk Management* (June 26, 1998).

U.S. Department of Transportation, Federal Aviation Administration Order 8100.5A, *Aircraft Certification Service: Mission, Responsibilities, Relationships, and Programs* (September 30, 2003).

U.S. Department of Transportation, Federal Aviation Administration Order 8100.7C *Aircraft Certification Systems Evaluation Program (ACSEP)* (October 12, 2005).

U.S. Department of Transportation, Federal Aviation Administration Order 8100.8B, *Designee Management Handbook* (October 12, 2005).

U.S. Department of Transportation, Federal Aviation Administration Order 8110.4C, *Type Certification* (October 26, 2005).

U.S. Department of Transportation, Federal Aviation Administration Order 8300.10, *Airworthiness Inspector's Handbook* (January 30, 2002).

U.S. Department of Transportation, Federal Aviation Administration Order 8400.10, Appendix 6, *Air Transportation Operations Inspector's Handbook* (April 6, 2005).

U.S. Department of Transportation, Federal Aviation Administration Notice N8110.80, *The FAA and Industry Guide to Product Certification* (January 26, 1999).

U.S. Department of Transportation, Federal Transit Administration, DOT-FTA-MA-26-5005-00-01, *Hazard Analysis Guidelines for Transit Projects* (January 2000).

U.S. Department of Transportation, Federal Aviation Administration, *System Safety Handbook: Practices and Guidelines for Conducting System Safety Engineering and Management* (Washington, DC: FAA, 2000).

U.S. Environmental Protection Agency, *Life Cycle Engineering Guidelines*, EPA/600/R-01/101 (November 2001).

U.S. Nuclear Regulatory Commission, NUREG/CR – 1278, *Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications,* by A.D. Swain and H.E. Gutman (Washington, D.C.: Nuclear Regulatory Commission, 1983).

this page intentionally left blank

Appendix A: Type Certification Process Description

This appendix presents a process analysis that examines and describes type certification with particular emphasis on how the Federal Aviation Administration (FAA) assesses hazards to safety of flight. It identifies the chronology of certification actions, the products produced by those actions, and the relationships among the parties involved. The analysis is based on Federal regulations, orders, advisory materials, certification study reports, and interviews with Safety Board, FAA, and industry professionals experienced in transport-category airplane certification. Tables showing the results of the analysis for each step in type certification are presented in Appendix B and are discussed in more detail in the following sections. Each of the tables in Appendix B is subdivided into management goals and technical goals to distinguish between planning and coordination activities that are typically done by FAA and applicant management, and technical activities that are typically done by applicant engineers and FAA engineers, designees, inspectors, test pilots, and national resource specialists.[1]

Aircraft Certification

Certification is the process used by the Aircraft Certification Service (AIR) to promote aviation safety through oversight of "design, production, and airworthiness certification programs to ensure compliance with prescribed safety standards."[2] AIR is one of seven organizations (figure A1) under the FAA Associate Adminstrator for Aviation Safety (AVS), which provides oversight and direction for the certification and continued airworthiness of aircraft; the certification of pilots, mechanics, and others in safety-related positions; the certification of all operations and maintenance enterprises in domestic civil aviation; and the development of regulations. AIR comprises the nine offices shown in figure A1. The 4 directorates develop and implement regulatory requirements, policy, and procedures for type, production, airworthiness certification, and continued airworthiness. Within the 4 directorates, the 10 Aircraft Certification Offices (ACOs) are the directorate's engineering operational elements, which are responsible for "approving the design certification of aircraft, aircraft engines, propellers, and replacement parts for those products,"[3] and all the certification activity within their geographic area. Although the focus of this report is on AIR, the relationship of AIR to

[1] FAA National Resource Specialists are considered experts in a specific area, and, in certification, provide professional technical guidance, advice, and assistance in their discipline.

[2] U.S. Department of Transportation, Federal Aviation Administration Order 8100.5A, *Aircraft Certification Service: Mission, Responsibilities, Relationships, and Programs* (September 30, 2003), paragraph 2-1d.

[3] FAA Order No. 8100.5A, paragraph 2-9e.

other organizations in AVS, especially Flight Standards Service (AFS), is also of interest. Flight Standards is responsible for certification and oversight of all certificated aviation personnel, air carriers, training facilities, and designees. In general, AFS is responsible for the oversight of an aircraft's operation and maintenance once it is placed in service.

AIR's Transport Airplane Directorate in Renton, Washington, is responsible for type certification of transport-category airplanes and for oversight and inspection of production certificate holders and manufacturing facilities. When the certification project involves powerplants and propellers, the Engine and Propeller Directorate in Burlington, Massachusetts, is involved. The Transport Airplane Directorate also has regional responsibilities within the United States, providing guidance for certification activities in 11 western states.[4] Within the Transport Airplane Directorate are three ACOs—located in Seattle, Denver, and Los Angeles—that conduct activities related to certification of transport-category airplanes. The ACO in Boston is responsible for certification of engines and propellers and works with the Seattle and Los Angeles ACOs—the two ACOs responsible for the majority of the transport-category airplane certification effort—when a project requires it. The Transport Airplane Directorate and its three ACOs employ approximately 250 technical people to assist in certification activities.

Although the number of technical personnel available for certification of transport-category airplanes may appear small, the FAA can call upon more than 4,600 designees, approved by the FAA and paid by the applicant or manufacturer of a product, to assist in the review, inspection, and approval of data and products. Designees can be involved in all aspects of the certification process.

The designee program has roots as far back as 1927, and the rules governing the program were established when the FAA was created in 1958[5] to allow designees to act as surrogates for the FAA in examining aircraft designs, production quality, and airworthiness.[6] Type certification designees can be Designated Engineering Representatives (DERs), Designated Manufacturing Inspection Representatives (DMIRs), or Designated Airworthiness Representatives (DARs). The FAA oversees designee activities and remains responsible for determining whether the products and processes examined by designees meet certification standards and safety requirements.

To obtain a type certificate (TC) for an aircraft, engine or propeller, an applicant must demonstrate to the FAA that the design complies with all applicable Federal regulations. The type certification process used by the FAA is presented in the following sections.

---

[4] See FAA Order No. 8100.5A, p. 13, for more details.

[5] Title 14 CFR Part 183 contains the regulations governing the appointment of designees and went into effect on June 30, 1962.

[6] The designee program is described in detail in FAA Order 8100.8B, *Designee Management Handbook,* July 14, 2003.

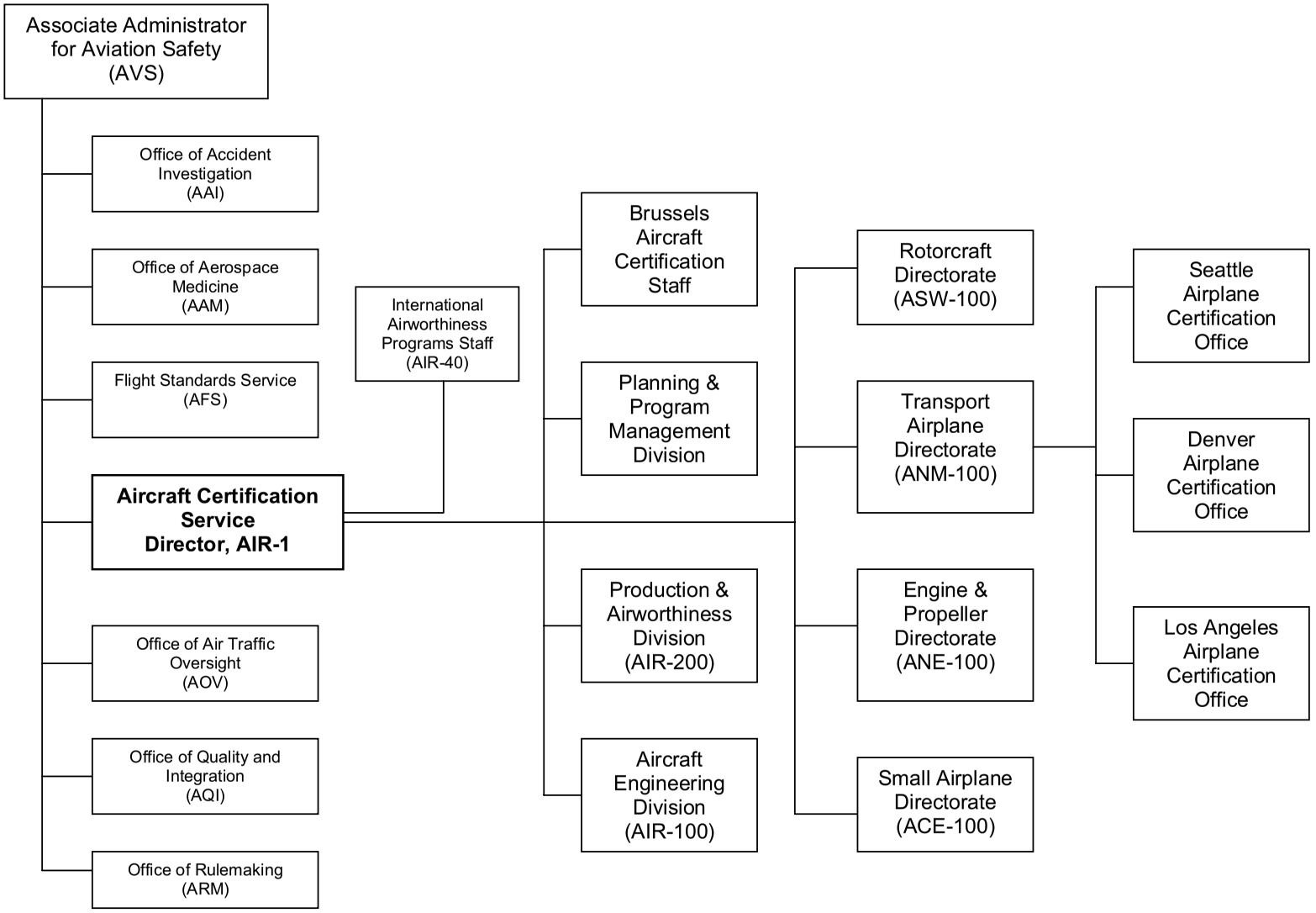

Figure A1: FAA Organization for Associate Adminstrator for Aviation Safety and the Aircraft Certification Service

The Type Certification Process

Type certification is a regulatory process that the FAA uses to ensure that aircraft manufacturers comply with Federal Airworthiness Regulations. The goal of certification for the manufacturer of a new or derivative transport-category airplane is the type certificate. To obtain a TC, the manufacturer must demonstrate to the FAA that the aircraft or product being submitted for approval complies with all applicable FARs. According to 14 *Code of Federal Regulations* (CFR) 21.21,

> An applicant is entitled to a type certificate for an aircraft in the normal, utility, acrobatic, commuter, or transport-category, or for a manned free balloon, special class of aircraft, or an aircraft engine or propeller, if—
>
> (a) The product qualifies under Sec. 21.27; or
>
> (b) The applicant submits the type design, test reports, and computations necessary to show that the product to be certificated meets the applicable [airworthiness, aircraft noise, fuel venting, and exhaust emission] requirements of the Federal Aviation Regulations and any special conditions prescribed by the Administrator, and the Administrator finds—
>
> (1) Upon examination of the type design, and after completing all tests and inspections, that the type design and the product meet the applicable [noise, fuel venting, and emissions] requirements of the Federal Aviation Regulations, and further finds that they meet the applicable airworthiness requirements of the Federal Aviation Regulations or that any airworthiness provisions not complied with are compensated for by factors that provide an equivalent level of safety; and
>
> (2) For an aircraft, that no feature or characteristic makes it unsafe for the category in which certification is requested.[7]

The Federal regulations that apply to type certification of transport-category airplanes are shown in table A1. The regulations in 14 CFR Part 25 are the ones most relevant to this report's focus on safety-critical systems. The Part 25 regulations are those concerned with the airworthiness standards for transport-category airplanes and are organized into the subparts shown in table A2. The subparts of greatest interest to this report are C and D, which deal with structures, design, and construction, and E, which deals with systems. The important point about the subparts is that the regulations are organized into groups related to the airplane elements of concern, and the regulations in each subpart may not apply to elements of the airplane governed by regulations in other subparts.

According to 14 CFR 21.21 and FAA Order 8110.4C, the Federal regulations that apply to a specific transport-category airplane are contained in the type certification basis that is established by the FAA in the early stages of the certification project. These

[7] Title 14 CFR Part 21.21. Part 21.27 refers to issuing type certificates for surplus military aircraft.

regulations represent the minimum standards for airworthiness; an applicant's design may exceed these standards and the applicant's tests and analyses may be more extensive than required by regulation. An important point is that the responsibility for the design engineering and analysis lies with the applicant, not the FAA; as stated in FAA Order 8110.4C, "The FAA approves the data, not the analytic technique, so the FAA holds no list of acceptable analyses, approved computer codes, or standard formulas. Use of a well established analysis technique is not enough to guarantee the validity of the result."[8]

Table A1. FARs Applicable to Transport-Category Airplane Certification

FAR	Applicable Area of Compliance
Part 21	Certification procedures for products and parts, including TCs for transport-category aircraft
Part 25	Airworthiness standards for transport-category airplane flight characteristics, performance and operating limits, structures, loads and strength capabilities, and installed equipment
Parts 33, 34, and 36	Airworthiness standards for engine performance and operating limits, durability, vibration, endurance, and engine exhaust and fuel venting emissions

Table A2. Title 14 CFR Part 25, "Airworthiness Standards for Transport-Category Airplanes"

Subpart	Applicable Area
A. General	Applicability, special requirements
B. Flight	Critical speed and performance values, weight, center of gravity, stability
C. Structure	Limit and ultimate loads, strength, design airspeeds, damage and fatigue tolerance
D. Design and Construction	Suitability and durability of materials, fabrication, casting, installation, doors
E. Powerplants	Installation, isolation, restart, auxiliary power, thrust reversers, fuel tanks
F. Equipment, Systems, and Installations	Systems, limitations, instruments, avionics, hydraulics, flight controls
G. Operating Limitations and Information	Flight manual, emergency procedures, airspeed and powerplant limits

[8] FAA Order 8110.4C, paragraph 2-6g.

Table A3. Summary of the Certification Process from *The FAA and Industry Guide to Product Certification.*

	Goals and Objectives
Partnership for Safety Plan	The FAA and applicant develop a Partnership for Safety Plan (PSP). A PSP is a written agreement that states how the FAA and applicant will conduct product certification, establish the general timelines and expectations, and identify deliverables.
Phase I Conceptual Design	The applicant begins design concept for a product that may lead to a viable certification project. The FAA and the applicant begin formulating a preliminary Project Specific Certification Plan (PSCP).
Phase II Requirements Definition	Product definition and the associated risks are clarified, and specific regulatory requirements and methods of compliance or critical issues are formulated. A more formal preliminary PSCP is developed.
Phase III Compliance Planning	The PSCP is completed, the TC application submitted, and the project team and Type Certification Board are put in place. Preliminary certification basis is established, and initial safety assessments are conducted.
Phase IV Implementation	The FAA and the applicant do the technical work of demonstrating compliance with the requirements in the certification basis for the project. The project is managed in accordance with the PSCP. When all tests and inspections are completed and approved, the TC is issued.
Phase V Post Certification	Certification project closeout activities provide basis for continued airworthiness activities and certificate management for the remainder of the product's life cycle.

The current type certification process has two parts. The first part—an overall, non-specific safety plan put in place by the FAA and the applicant—is called a Partnership for Safety Plan. The second part is an aviation product-specific five-phase certification project described in the Project Specific Certification Plan. The two parts are described in *The FAA and Industry Guide to Product Certification*[9] (and referred to in this report as "the Guide"). The Guide is governed by procedures set forth in FAR Part 21 and is described in detail in FAA Orders 8100.5A[10] and 8110.4C.[11] The purpose of the *Guide* is to describe "how to plan, manage, and document an effective, efficient product certification process and working relationship between the FAA and an Applicant."[12] The two parts to the type certification process are summarized in table A3 and briefly described below.

[9] Introduced in 1999 as part of a certification process improvement initiative and revised in 2004, the Guide emphasizes "establishing up-front a clear understanding of the needs and expectations of both parties in the product certification process." By applying the principles in the *Guide*, "the FAA and the Applicant can lay a foundation from which to build mutual trust, leadership, teamwork, and efficient business practices," and enable them to "expedite certification of products while focusing on safety significant issues." The Guide, available at http://www.faa.gov/certification/aircraft/av-info/dst/CPIGUIDE.pdf, was implemented by FAA Notice 8110.80, *The FAA and Industry Guide to Product Certification*, February 26, 1999.

[10] FAA Order 8100.5A.

[11] FAA Order 8110.4C.

[12] *The FAA and Industry Guide to Product Certification*, p. 1.

The Partnership for Safety Plan (PSP), the first part of the certification process, is a management and planning document that establishes the relationship between the applicant and the FAA. This document provides the working umbrella agreement for all subsequent product-specific certification activities with that applicant.

The Project Specific Certification Plan (PSCP) describes the second part of the certification process and includes the five phases shown in tables A3 and A4. The PSCP details the project schedule, the type certification basis, means of compliance, applicant and FAA coordination, test plans and conformity inspections, and post-certification requirements. The PSCP becomes the official agreement between the applicant and the FAA and is the official plan for the certification project. Approval of the PSCP is a major milestone in the project because it serves as the agreement between the FAA and the applicant on the required activities to show compliance. Approval of the PSCP signifies the point at which the applicant can proceed with the compliance effort. As previously mentioned, the ultimate goal of type certification is a TC for the airplane, and to reach that goal, a number of deliverables are produced during the five phases of the PSCP. (See table A4.)

Table A4. Product Timeline of Certification Process.

Pre-Product Certification	Phase I	Phase II	Phase III	Phase IV	Phase V
Partnership for Safety Plan					
	Project Specific Certification Plan				
	Type Certification Basis				
			Compliance Checklist		
	Type Design				
		Type Certificate Application			
		Certification Project Notification			
	Safety Assessments Results				
	Issue Papers				
	Special Conditions				
	Equivalent Safety Findings				
		Maintenance Review Board Report			
	Applicant Inspection, Ground Test, Flight Test Results				
	Compliance Demonstrations				
	Conformity Inspection Results				
				Type Inspection Authorization	
				Type Inspection Report: Ground	
				Type Inspection Report: Flight	
				Flight Manual	
				Instructions for Continued Airworthiness	
				Type Certificate	
					Compliance Summary Document
					Certificate Management Plan

Phase I initiates the type certification process. The primary activities in this phase are compliance planning and establishing the type certification basis, activities that continue into Phase III. The type certification basis is a very important deliverable because it establishes the time and effort that an applicant must devote to demonstrating compliance with airworthiness regulations. Given that demonstrating compliance for a transport-category airplane can be a lengthy and costly process for an applicant and may involve hundreds of Federal regulations, an applicant and the FAA devote considerable time and effort to establishing the type certification basis. In Phase I (and until the type certification basis is finalized in Phase III), the FAA determines which regulations require demonstrations of compliance, thereby specifying which features of the airplane must be analyzed or tested.

Phase I also initiates early development of the design concept that will be defined in more detail in Phase II. This effort involves definition and identification of new features or design concepts that will require specific attention in risk-based safety assessments or treatment as special conditions or equivalent safety findings. During Phase I, the emphasis is on defining critical issues and developing plans to resolve them; in Phase II, the issues become better defined, with greater emphasis on identifying risks and finalizing regulatory and compliance requirements and methodologies.

Phase III marks the beginning of the official type certification project. When the applicant submits a TC application to the FAA, and the applicable ACO issues a certification project notification to the appropriate directorates, the project begins. At that time, the FAA begins its official review of the plans, type design,[13] materials, processes, documentation, tests, and analysis results provided by the applicant. Finalizing the PSCP and the type certification basis during Phase III establishes the requirements that are placed on the applicant to demonstrate compliance with Federal regulations.

Demonstrating compliance with Federal regulations occurs in Phase IV. Most of the official FAA technical work occurs after the Type Inspection Authorization (TIA) is issued and the official FAA ground and flight test programs begin. Until that point in the certification process, virtually all responsibility for design, compliance, safety assessments, and initial flight and ground testing rests with the applicant and is reviewed

[13] Title 14 CFR 21.31 states that the type design consists of the following:

> (a) The drawings and specifications, and a listing of those drawings and specifications, necessary to define the configuration and the design features of the product shown to comply with the requirements of that part of this subchapter applicable to the product; (b) Information on dimensions, materials, and processes necessary to define the structural strength of the product; (c) The Airworthiness Limitations section of the Instructions for Continued Airworthiness as required by Parts 23, 25, 27, 29, 31, 33, and 35 of this chapter, or as otherwise required by the Administrator; and as specified in the applicable airworthiness criteria for special classes of aircraft defined in Sec. 21.17(b); (d) For primary category aircraft, if desired, a special inspection and preventive maintenance program designed to be accomplished by an appropriately rated and trained pilot-owner; and (e) Any other data necessary to allow, by comparison, the determination of the airworthiness, noise characteristics, fuel venting, and exhaust emissions (where applicable) of later products of the same type.

and accepted by the FAA. Once all of the actions specified in the TIA have been completed, documented in the Type Inspection Reports, and approved by the FAA, the TC is issued.

Finally, post-certification activities occur in Phase V. In this phase, the project is documented, instructions for continued airworthiness (ICAs) are produced, and the materials that accompany the airplane into service are prepared.

As previously mentioned, the vast majority of the applicant's time and effort is devoted to demonstrating compliance with Federal regulations. Of course, compliance can be demonstrated in a number of different ways, and the means of compliance are proposed by the applicant and approved by the FAA. For example, an applicant can substantially reduce the costs of compliance by showing that the airplane type design being presented for approval is derived from a previously certified aircraft. Commonly referred to as "derivative designs" and by regulations as "changed aeronautical products,"[14] this approach allows an applicant to propose changes to the type design of a previously certified airplane and retain the original TC.

For airplanes manufactured outside of the United States, the FAA has bilateral airworthiness agreements with the foreign certification authorities. A bilateral agreement signifies that the FAA has confidence in a foreign authority's technical competence and regulatory capability for performing airworthiness certification functions. For instance, the FAA has a bilateral agreement with the French government, and the United States and the European community have worked to harmonize U.S. Federal aviation regulations with Europe's Joint Aviation Requirement (JAR) and the newly established European Aviation Safety Authority (EASA) certification specifications.[15] For airplanes that are based on a previous model, like the Airbus A300-605R, the FAA accepts the foreign certification as long as the aircraft's service history is satisfactory, and the certification process is consistent with U.S. regulations.

To illustrate the time and effort involved in certification, a timeline showing important milestones for certification of Boeing's 777 is shown in table A5. The process took approximately 5 years from concept development to issuance of the TC and involved more than 6,500 Boeing employees (and an unknown number of subcontractors), 9 airplanes, 4,900 test flights, and more than 7,000 hours of flight time.[16] By the time the Boeing Board of Directors gave the go-ahead for production at the end of October 1990, much of the preliminary design of the airplane was complete.[17] By that time, the equivalent of

[14] Title 14 CFR 21.101, "Changes to Type Certificates: Designation of Applicable Regulations"; FAA Order 8110.48, *How to Establish the Certification Basis for Changed Aeronautical Products*, April 25, 2003, and FAA AC 21.101-1, *Establishing the Certification Basis of Changed Aeronautical Products*, April 28, 2003.

[15] The requirements for a bilateral agreement are governed by 14 CFR 21.29, *Issue of Type Certificate: Import Products* and described by in FAA AC 21-23B *Airworthiness Certification of Civil Aircraft, Engines, Propellers, and Related Products Imported to the United States*, November 17, 2004.

[16] See <http://www.boeing.com/commercial/777family/pf/pf_milestones.html>.

[17] K. Sabbagh, *Twenty-First Century Jet: The Making and Marketing of the Boeing 777* (New York: Scribner, 1996).

Phases I, II, and III was complete and the certification basis was established. The authorization to begin FAA flight-testing occurred shortly after the 777's first flight in 1994, and the joint issuance of FAA and Joint Aviation Authority (JAA) type certificates occurred in 1995.

Table A5. Milestones in the Boeing 777 Development and Certification Program (from <http://www.boeing.com/commercial/777family/pf/pf_milestones.html>)

Date	Milestone
October 29, 1990	The Boeing Board of Directors met and gave formal approval, launching into production the new 777 airplane family.
May, 21, 1991	Boeing and Japanese airframe manufacturers signed a final agreement outlining the participation of Mitsubishi, Kawasaki, and Fuji Heavy Industries.
January 21, 1993	Major assembly of the 777 wing spar and nose began.
May 13, 1993	The first major airplane body sections for the 777 arrived from Japan Aircraft Development Corp.
December 15, 1993	The first 777 sections entered final body join. This was the first time the 777 resembled a completed airplane.
April 9, 1994	Ceremonial rollout of the first 777.
June 12, 1994	First flight: 3 hours, 48 minutes. Flight testing began.
October 28, 1994	Fourth 777 entered flight test program for long-distance route testing.
April 19, 1995	The 777 received joint FAA/Joint Aviation Authority type certificate and FAA production certificate.
May 15, 1995	The first 777 was delivered to United Airlines.
May 30, 1995	The 777 received Extended-Range Twin-Engine Operations (ETOPS) approval.

The process analysis used to summarize the FAA type certification process characterizes each phase in terms of goals, initiating conditions, actions, products and deliverables, and responsible party and participants. Tables showing the detailed analysis for each of the phases are presented in Appendix B. Each of the tables is subdivided into technical goals, which are typically implemented by applicant engineers and FAA engineers, designees, inspectors, test pilots, and national resource specialists, from management goals. The following sections describe each of the products shown in table A4 in more detail.

Partnership for Safety Plan

The Partnership for Safety Plan was introduced to the certification process with adoption of the Guide in 1999 and is used to establish an early working relationship between the FAA and an applicant before any specific certification project begins. The PSP is not specific to any individual certification project and may be developed before an official, product-specific certification project is begun. The PSP enables applicants to

begin certification discussions even at the conceptual stage of design. In effect, the PSP is the applicant's agreement with the FAA that certification projects will be conducted in a particular way. Thus, the PSP is a management document that an applicant can use for all products (including engines, propellers, and equipment).

According to the FAA, the PSP provides the vision for product certification, which results in timely product design and production approvals. Notice that early in the certification process, the emphasis is on how the project will be managed, how oversight will occur, and how critical issues will be resolved.

Project Specific Certification Plan

Under the working agreement established by the PSP, a Project Specific Certification Plan is developed to describe the project in detail. The PSCP establishes the project schedule, certification basis, means of compliance, and requirements for coordination between the applicant and the FAA for test plans, conformity inspections, and post-certification activities. (A summary of the elements of a PSCP is shown in table A6.) The PSCP becomes the official certification agreement between the applicant and the FAA and the official plan for the certification project.

Table A6. Components of the Project Specific Certification Plan.

Section	Description
Project Description	Briefly describes the certification project.
Project Schedule	Identifies in detail all major milestones, including project reviews and scheduled deliverables.
Certification Basis	Identifies the applicable regulations with which the applicant must show compliance. Also includes the need for special conditions, exemptions, and equivalent safety findings.
Means of Compliance	Summarizes the applicable FARs with the agreed means of compliance that will be met for type certification.
Communication and Coordination	Describes the communication and coordination paths among the FAA, the applicant, and other participants.
Delegation	Identifies the oversight and documentation requirements of engineers, inspectors, and flight test pilot designees.
Testing Plan	Contains requirements for planning, preparing, and conducting FAA-required testing. Subsections for ground tests, flight tests, and conformity inspections are in this section.
Compliance Documentation	Describes the procedures for submitting and processing compliance documentation, including what data will be submitted and by whom.
Post Certification Requirements	Includes compliance summary document, instructions for continued airworthiness, and continued airworthiness management plan.
Project Issues Planning	Establishes methods to be used for tracking resolution of certification issues.
Continuous Improvement	Identifies measures for evaluating the project, including project schedules, commitments, agreements, milestones, and deliverables.

Critical to the type certification process is the type design, a document that accompanies the PSCP.[18] As previously discussed, the type design is a preliminary document consisting of drawings, specifications, and data that define the configuration and design features of the aircraft and show the airworthiness of the design and its compliance with applicable regulations. The type design may be conceptual at this point so that the applicant and the FAA can review concepts and discuss potential certification issues before the detailed design is finalized. As the type design is developed and data become complete, the FAA conducts a design evaluation to ensure compliance with applicable regulations defined in the certification basis. How type design data are used to demonstrate compliance is typically spelled out in the certification plan.

Finally, Federal regulations do not require an applicant to prepare a human factors certification plan nor include one in the PSCP. However, FAA Policy Statement Number AMN-99-2 does provide guidance about developing an acceptable human factors certification plan and clearly states the need to consider crew response to failure conditions as part of the safety assessment process. Note that these materials are advisory and do not require demonstrating compliance with Federal regulations.

The PSCP evolves throughout Phases II and III. Because the PSCP is an official document that details the requirements for a TC, the final version takes some time to develop. Early formulation of the PSCP begins in Phase I and much of its early development is devoted to establishing the type certification basis.

TC Application. Once the PSCP has been produced in Phase II, the applicant submits an application for a TC to the appropriate ACO. The application must include a three-dimensional drawing of the aircraft and all available basic data. If a new engine is involved, an application for an engine TC, including a description of the engine design features, operating characteristics, and proposed operating limitations, must also be submitted. Note in table A4 that the application is not submitted until Phase II and that by then, other preliminary certification activities are already underway. However, the TC application (FAA Form 8110-12) effectively signals the official start of a type certification project. The date of the application is important because it establishes the effective date for all regulations to be considered during certification. Only regulations in force at or before the application date will be considered as part of the certification basis (unless any subsequent regulations are directly associated with correcting an unsafe condition). Special conditions may be added to the certification basis, and the applicant may elect to comply with later regulations.

Certification Project Notification. Once the TC application is submitted, the ACO issues the Certification Project Notification, its mechanism for notifying relevant FAA participants of the certification project: the accountable directorate for oversight and management; National Resource Specialists for participation in the project team; and the Flight Standards Office, through the appropriate Aircraft Evaluation Group (AEG), to provide inspectors, test flight pilots, and engineers. At this time, the ACO appoints an FAA project manager.

[18] As defined in 14 CFR Part 21.31.

AEGs are part of Flight Standards, and each of the five AEGs is co-located with an ACO that it supports.[19] Accordingly, the AEG serves as the interface between the ACO and Flight Standards. The AEG determines the operational suitability of FAA-approved designs, specifically as they relate to recommended maintenance programs and the ICA. As stated by FAA about the AEG, "we ensure that the manufacturer provides the instructions for continued airworthiness for the products that they sell."[20]

The certification project notification also initiates appointment of four boards staffed by FAA personnel: the Type Certification Board (TCB), the Flight Standardization Board (FSB), the Flight Operations Evaluation Board (FOEB), and the Maintenance Review Board (MRB). The TCB arbitrates all certification issues, and the other three boards address issues related to aircraft type rating, operations, and maintenance.

Type Certification Board. A TCB is established for all projects that require complete type certification.[21] Its primary purpose is to resolve significant problems and issues, establish schedules and milestones, review the applicant's certification basis, and review and accept the applicant's certification, compliance, and test plans. TCB members include a chairman (the ACO manager), the project manager, the project officer, senior managers, and personnel from appropriate engineering disciplines, flight testing, and the assigned AEG.

TCB meetings represent significant milestones in the certification process. The familiarization TCB meeting establishes the partnership between the FAA and the applicant and occurs in Phase I after the PSP is developed. This meeting may be combined with the preliminary TCB meeting where the certification basis and new and novel design features are discussed. As the need arises, interim TCB meetings typically focus on specific certification issues. The pre-flight TCB meeting, for example, addresses any issues related to upcoming flight tests, and, if all compliance and conformity issues have been resolved, the type inspection authorization is issued. The final TCB meeting is held during Phase IV when the applicant demonstrates compliance with all applicable airworthiness standards and the flight test program is complete. The TC is issued as a result of this meeting.

The Interface Between Certification and Operations

The FSB, FOEB, and MRB are concerned with certification issues related to maintenance and operations, and the members of those boards are appointed by the AEG.

[19] The AEG for Powerplants and Propellers is located in Boston; for small Part 23 aircraft, in Kansas City; for rotorcraft, in Fort Worth; and for large Part 25 aircraft, in Seattle, Denver, and Long Beach.

[20] Testimony given by Lee R. Koegel, Aviation Safety Inspector, FAA AEG, Long Beach, California, at the Public Hearing for the Alaska Airlines flight 261 aircraft accident, Washington, DC, December 14, 2000, transcript, p. 481.

[21] A TCB may be established for projects involving changes to the type design, or any significant project.

These three boards not only provide the interface between certification and air carrier operations, they also bring service history and operational data into the certification process. Primary responsibility for the interface between the ACO and Flight Standards lies with the AEG. As previously discussed, the AEG is the only section of Flight Standards that directly interfaces with ACO and FAA certification engineers, and is involved in conformity inspections, ground and flight tests, and the development of maintenance and operations materials to accompany the airplane into service.

The three boards are put in place at the start of the type certification project and remain in place throughout the life of the airplane. The FSB determines the airplane type rating requirement and the minimum training requirements for flight crew qualification. The FSB comprises inspectors from district offices, representatives from the Air Transportation Division and FAA Headquarters, and a chairman from AEG Operations, who directs FSB tasks.

The FEOB conducts the operational evaluation of the aircraft. This board typically comprises airworthiness and operations inspectors, a flight test pilot, an FAA Headquarters representative, and an operations inspector acting as chairman. The FEOB is also responsible for producing the airplane's master minimum equipment list.

The MRB is responsible for the aircraft's maintenance and inspection requirements and oversees the MSG-3 process (described in AC 121-22A and ATA MSG-3 Revision 2003.1), which includes development of the MRB Report. The MRB comprises AEG personnel, Flight Standards inspectors, and engineers from the appropriate aircraft and engine directorates and is typically chaired by a member of the AEG. Again, as previously discussed, the AEG determines the operational suitability of FAA-approved designs, especially as they relate to recommended maintenance programs and the ICA. The AEG is responsible for reviewing and accepting any subsequent requests from the manufacturer or operators to change the MRB Report.

The MSG-3 process is used to establish tasks and associated time-in-service intervals for the initial maintenance time limits in an air carrier's continuous airworthiness maintenance program. Using this process, the MRB provides support to the industry steering committee (ISC) and various industry working groups who are developing the MRB Report. ISC membership comprises representatives from manufacturers and intended air carriers; the working groups comprise industry representatives and FAA advisors. The final MRB Report "contains the initial minimum scheduled maintenance/inspection requirements for a particular transport-category aircraft and on-wing engine program, but does not establish off-wing engine maintenance programs required by the Regulations."[22] The MRB Report emphasizes maintenance and structurally significant items and the safety and operational effects of maintenance-related failure conditions. Once approved by the FAA, the MRB Report is provided to an air carrier as the initial, recommended maintenance and inspection program and becomes part of the ICA, discussed under *Post-Certification Products*.

[22] FAA AC 121-22A, *Maintenance Review Board Procedures,* March 7, 1997, Chapter 1, Section 2.b, p. 6.

The proposed MRB Report is drafted by the ISC and is forwarded to the applicant for review and discussion. The applicant then presents the proposed MRB Report to the MRB, either as recommended or revised, for approval as part of the ICA. The MRB approves all revisions to the MRB Report and is responsible for its recommended annual review. It is important to note that (1) the proposed MRB Report is drafted by industry and (2) the MRB Report approved by the FAA is recommended, not mandatory.

The MRB and the MRB Report played an important role in establishing maintenance procedures for the jackscrew assembly investigated in the Alaska Airlines flight 261 accident. The MRB provided the interfaces between certification, operations, and maintenance, and was instrumental in bringing service history and operational experience into the certification process. The MRB approved both the original lubrication intervals for the MD-80 series airplanes and subsequent extensions to the lubrication intervals supported by reliability data from the air carriers and the manufacturer.

Type Certification Basis

As the name implies, the type certification basis is the foundation for the entire certification project. The certification basis establishes the set of relevant FARs and determines the extent of the compliance effort. Once the certification basis is established and the FAA agrees to it, the set of regulations and standards will not be changed or new policy introduced unless a change is required to correct an unsafe condition.

Establishing the certification basis is an important milestone. As table A4 shows, this effort starts early (Phase I), but may not be complete until Phase III, after other activities concerned with identifying certification issues and conducting preliminary safety assessments are finished. Not surprisingly, the applicant wants to finalize the certification basis as early in the process as possible in order to define the extent and the associated costs of the compliance effort.

Type Certification Basis and Derivative Designs

An applicant can use an existing certification basis to substantially reduce the costs of compliance by showing that the type design being presented for approval is derived from a previously certified airplane. As previously discussed, these derivative designs, or "changed products,"[23] allow applicants to propose changes to type designs of previously certified airplanes and retain the original TC. The FAA will approve changes to the original TC if they find that the changes are not significant.

Title 14 CFR 21.101 states that a change is automatically considered significant if "(i) The general configuration or the principles of construction are not retained," and

[23] Title 14 CFR 21.101.

"(ii) The assumptions used for certification of the product to be changed do not remain valid."[24] In addition, 14 CFR 21.19 indicates that a proposed design is significantly different from an existing design when the proposed changes are "so extensive that a substantially complete investigation of compliance with the applicable regulations is required."[25] The following design changes would be considered significant enough to require a new compliance effort and TC:

- A design change to a component, equipment installation, or system that extensively invalidates the compliance demonstration of the original design.
- A design change that significantly affects the basic structural loads.
- A design change that introduces novel or unusual methods of construction or new materials.
- A design change that includes new state-of-the-art systems or components that have not been previously certified.

If the FAA finds that a proposed change is significant, the applicant must establish a new certification basis. Further, if the proposed change incorporates new or novel features that are not covered by regulation, the certification basis may also include special conditions, discussed in the next section. In both cases, the change will require the applicant to demonstrate compliance with applicable Federal regulations.

For applicants, the advantages of a derivative design are twofold. First, the applicant can save considerable time and money by using the results of the analyses, tests, and inspections conducted during the original type certification process to demonstrate compliance. Second, the regulations that apply to the derivative design are those that were in effect on the date of the original TC, not the date of the application for the new TC. Although the FAA encourages applicants to update the certification basis with any changes to requirements issued after the original TC was approved, those updates are not required, except under certain conditions specified by 14 CFR 21.101.

Special Conditions

When existing regulations or safety standards applicable to the design feature being certified are inadequate or inappropriate, the FAA can declare a special condition. Title 14 CFR 21.16 states that if "the airworthiness regulations of this subchapter do not contain adequate or appropriate safety standards for an aircraft, aircraft engine, or propeller because of a novel or unusual design feature of the aircraft, aircraft engine or propeller,"[26] the FAA can initiate rulemaking to produce standards that establish a level of safety equivalent to existing regulations. "Novel or unusual" design features are

[24] Title 14 CFR 21.101, paragraph b(1).

[25] Title 14 CFR Part 21.19, paragraph a.

[26] Title 14 CFR Part 21.16.

interpreted in the context of existing airworthiness standards; thus, deviation of specific design features from existing standards is the catalyst for special conditions, which are unique to a specific certification project and are treated on a case-by-case basis.

Special conditions begin with an issue paper. The FAA uses issue papers (discussed in the next section) to identify and resolve any significant certification issue or problem—such as a special condition—that arises during certification. An issue paper establishes the basis for a special condition by summarizing novel and unusual design features and regulatory inadequacies, and by proposing wording of the regulatory change that will meet the special condition. The contents of the issue paper for a special condition are found in 14 CFR 21.16 and FAA Order 8110.4C.

The issue paper is developed by the ACO, with full participation by the applicant and other relevant participants. Once developed, the proposed special condition is forwarded to the appropriate directorate, which reviews it and coordinates review, approval, and publication of the rule change in the *Federal Register*. Special conditions that are found to be generally applicable may result in a notice of proposed rulemaking (NPRM) and as an amendment to FARs.

Related to special conditions are equivalent safety findings. An equivalent level of safety finding is made when literal compliance with a certification regulation cannot be shown, but the applicant presents compensating factors that can provide an equivalent level of safety.[27] This process allows the FAA, after reviewing the pertinent issues and data provided by the applicant, to determine if an equivalent safety finding can be established as part of the type certification basis. These findings also become part of the compliance effort. Note from table A4 that equivalent safety findings can be produced as early as Phase I and up to the issuance of the TIA in Phase V. An issue paper is the typical mechanism for initiating and resolving equivalent safety findings.

Issue Papers

FAA uses issue papers to identify and resolve any significant certification issue or problem that arises during the certification process. The FAA generates issue papers to identify potentially unsafe conditions and/or systems that may require further scrutiny. Issue papers are most commonly used to provide the basis for special conditions described in the previous section.

What constitutes a significant issue is defined in 14 CFR 21.101 and can include new technology or novel design, the certification basis and means of compliance, environmental considerations, unsafe conditions, and special conditions. In general, an issue is significant if TCB involvement or a special certification review (SCR) is required for resolution (SCR is discussed under *Post-Certification Products*). Issue papers are "prepared by government employees for use in effecting project management containing

[27] Title 14 CFR Part 21.21, paragraph b-1.

opinions, advice, deliberations and recommendations made in the course of developing official action by the government."[28] The format for an issue paper is shown in FAA Order 8110.4C.

The primary advantage of an issue paper is that one can be proposed at any time in the certification process up to issuance of the TC (as shown in table A4). An issue paper is therefore a powerful tool for the government in alerting project management—both the FAA's and the applicant's—of the need to address a specific certification issue. Contained in an issue paper is a statement and discussion of the issue, the FAA's position, the applicant's position, background information, and conclusions about how the issue should be resolved. Resolution is, of course, issue-specific, but the FAA has used issue papers to recommend methods for demonstrating compliance, including specific tests and analysis techniques. FAA also uses issue papers to recommend additional or more comprehensive safety assessments for systems or components. Consequently, issue papers provide a way for the FAA to require further assessment of a design feature or a critical system.

Issue papers are usually developed and resolved in stages. The preliminary stage may include no more than a statement of the issue, with TCB review and discussion to clarify the issue and to lay out a plan for resolving it. Until an issue is approved for resolution by the TCB, all issue papers are considered to be drafts. By accepting the conclusions presented in an issue paper, the TCB chairman defines the FAA requirement for the certification project. Once approved, an issue paper becomes part of the issues book, which is compiled for a certification project and is used as the central compendium of issues and as a means of tracking issue resolution.

An important point is that issue papers, as draft materials, are not part of the official certification project file and are therefore exempt from public disclosure. Issue papers are assembled and published in the form of an Issues Book, and once the TC is issued, the Issues Book could be used to prepare the Certification Summary Report. The Certification Summary Report "serves as a single source document that summarizes the record of the FAA examination of the type design, which is the basis for issuing the TC" under 14 CFR 21.21.[29] Thus, there is no requirement that issue papers be maintained as part of the official documentation for the airplane's TC.

Demonstrating Compliance: Structures and Systems

Up to this point, interactions between the applicant and the FAA focus on planning, establishing the certification basis, conducting preliminary reviews of the type design data, and dealing with issue papers and special conditions. Once the certification plan is finalized and approved in Phase III, the activities associated with official demonstrations of compliance begin and the FAA takes a more active role in evaluating the airplane design. This is the phase of the project that is the most time consuming and

[28] FAA Order 8110.4C, paragraph 3c.

[29] FAA Order 8110.4C, paragraph 4d.

resource intensive and is most closely related to the certification issues identified in the four accident case studies. The extent of the activities associated with demonstrating compliance is shown in tables B1–B6 in Appendix B.

One tool used by the FAA and the applicant to track the compliance effort is the Compliance Checklist developed in Phase III. The Compliance Checklist lists all regulations requiring compliance, the methods to be used to demonstrate compliance (for example, ground test, flight test, analysis, similarity, equivalent means of compliance) and what will be submitted to show compliance.

In its most basic form, demonstrating compliance is conducting either analyses or tests. The certification basis determines, to a large extent, which analyses and tests must be conducted. As previously discussed in the *Type Certification Basis* section, one way an applicant may avoid costly analyses and tests is to relate the new airplane to an existing TC. No new tests or analyses are required, and the associated costs are eliminated. Derivative designs are common in transport-category airplane certification.

If analyses and tests are required, the applicant selects from among a number of different methodologies. These methods of compliance fall into two basic types:[30]

- methods that demonstrate compliance through adherence to specific design and test criteria, and are typically deterministic, or
- methods that demonstrate compliance using the probabilistic risk analysis techniques outlined in AC 25.1309-1A.

Many of the airworthiness requirements spelled out in 14 CFR Part 25 are of the first type, requiring adherence to specific design criteria concerned with aerodynamic performance, flight characteristics, and structural loads and strength requirements. Those regulations set specific design and/or performance criteria, and compliance is demonstrated through engineering analysis, simulation, or ground and flight tests. The evaluation of design features is assumed to be deterministic so that specific tolerances and limits can be explicitly stated and analyzed. Failures are treated as deterministic, and the analyses and tests focus on the ability of the damaged structure or component to allow continued safe flight and operation.

In general, human factors considerations are also specified in FARs as specific design criteria. For example, the workspace environment required by the flight crew is covered by 14 CFR 25.771–25.785, regulations that specify minimum standards for occupant space, sightlines through windows, and cockpit control knob shape. Other regulations, such as 14 CFR 25.1301, state in general terms human factors requirements related to minimum crew, workload, and functionality of aircraft systems. Some of the

[30] A deterministic approach assumes the same result for a given set of initial conditions, while a probabilistic (stochastic) approach assumes that randomness is present, even when given an identical set of initial conditions. Consequently, a probabilistic approach will always assume uncertainty in the result. Probabilistic methods can be viewed as inclusive of all deterministic events with a finite probability of occurrence.

advisory materials made available by the FAA provide very specific design guidance related to human factors, especially in avionics. AC 25-11 provides detailed design criteria for displays, covering such topics as color-coding, symbology, clutter, and attention-capturing requirements. AC-25.1329 also provides detailed human factors design criteria for an autopilot and the requirements for assessing human interaction with the autopilot during flight tests. In general, compliance with human factors requirements is demonstrated by adherence to specific design criteria stated in regulation and is evaluated with mock-ups and simulators, or during ground and flight tests.

In contrast to specific design criteria stated in regulations, the second type of method for determining compliance outlined in AC 25.1309-1A[31] and governed by 14 CFR 25.1309 treats failures as *probabilistic* and uses a stochastic approach to assess the consequences of system failures. The focus is on understanding the functional significance of aircraft systems, determining the risks to safety of flight associated with a failure condition, and using probability distributions to determine the frequency of occurrence of a failure condition and its effects on overall system function. In the context of 14 CFR 25.1309, the systems of interest are equipment and their installations. Guidance provided by AC 25.1309-1A specifically states that the regulation does not apply to Subparts B and C of 14 CFR Part 25 that pertain to performance, flight characteristics, and structural load and strength requirements.[32]

Fundamental to the notion of safety-critical systems in certification is the fail-safe design concept, which "considers the effects of failures and combinations of failures in defining a safe design."[33] The concept has a different meaning for structures than for systems: fail-safe for *structures* is concerned with residual strength after sustaining damage; fail-safe for *systems* is concerned with the functional implications of a failure condition and its probability of occurrence. Although both concepts have the same goal—a safe design—the approaches to achieving that goal are different.

Fail-Safe for Structures

Fail-safe for structures is governed by 14 CFR 25.571 and the methods of compliance are outlined in AC 25.571-1C. In general, the structural components of an airplane (such as the airframe and wings) are designed such that "an evaluation of the strength, detail design, and fabrication must show that catastrophic failure due to fatigue, corrosion, manufacturing defects, or accidental damage, will be avoided throughout the operational life of the airplane."[34] However, after the 1988 Aloha Airlines flight 243 accident where 18 feet of the upper crown skin and structure separated from the fuselage, there has been a greater emphasis on damage tolerance. A damage tolerance evaluation of

[31] The process is also described in SAE ARP4761.

[32] FAA AC 25.1309-1A, section 3.

[33] FAA AC 25.1309-1A, paragraph 5.

[34] Title 14 CFR 25.571, section a.

structure ensures that "should serious fatigue, corrosion, or accidental damage occur within the design service goal of the airplane, the remaining structure can withstand reasonable loads without failure or excessive structural deformation until the damage is detected."[35]

Fatigue safe life was the predominant approach to evaluating structure before the shift to damage tolerance.[36] The emphasis was empirical with the fatigue life of a structure defined as the number of bending cycles to failure. Once the fatigue life of a structure was determined, a safety factor was added to the estimated fatigue life to arrive at the safe-life of a structure. Damage tolerance emphasizes the physics of crack growth, and is concerned with setting life limits (that is, inspection intervals that are based on the time for a crack to grow or propagate).[37] Regulations and advisory materials are very specific about the design features to be used to ensure damage tolerance, including multiple load path construction, crack stoppers, materials and stress levels that provide a slow rate of crack propagation, and designs that ensure detection before unacceptable or widespread damage occurs.

A damage tolerance evaluation typically "consists of a deterministic evaluation of the design features"[38] to ensure that airplane structural components are damage tolerant. AC 25.571-1C identifies these components as principal structural elements (PSE),[39] and may include components of wings and empennage, fuselage, landing gear and attachments, and engine mounts. A damage-tolerance evaluation is intended to ensure that the failed components of an aircraft structure can withstand reasonable loads without further damage or failure.[40] Regulations and advisory materials are very specific about design criteria with respect to damage-tolerant design features; for example, AC 25.571-1C states the following:

> Design features that should be considered in attaining a damage-tolerant structure include the following:
>
> 1. Multiple load path construction and the use of crack stoppers to control the rate of crack growth, and to provide adequate residual static strength;
>
> 2. Materials and stress levels that, after initiation of cracks, provide a controlled slow rate of crack propagation combined with high residual strength;

---

[35] FAA AC 25.571-1C, section 6a.

[36] U.S. Department of Transportation, Federal Aviation Administration, *Damage Tolerance Assessment Handbook*, *Vol. I: Introduction, Fracture Mechanics, Fatigue Crack Propagation* (Cambridge, MA: Volpe National Transportation Systems Center), October, 1993, Section 1.3.

[37] FAA *Damage Tolerance Assessment Handbook,* Section 1.3.2.

[38] FAA AC 25.571-1C, section 6c.

[39] FAA AC 25.571-1C, section 6d, defines a PSA as "an element of structure that contributes significantly to the carrying of flight, ground, or pressurization loads, and whose integrity is essential in maintaining the overall structural integrity of the airplane" and lists examples.

[40] FAA AC 25.571-1C, paragraph 6.

3. Arrangement of design details to ensure a sufficiently high probability that a failure in any critical structural element will be detected before the strength has been reduced below the level necessary to withstand the loading conditions specified in 14 CFR 25.571(b), so as to allow replacement or repair of the failed elements; and

4. Provisions to preclude the possibility of widespread fatigue damage (MSD or MED [multiple site damage or multiple element damage)[41] prior to reaching the design service goal and to prevent or control the effects of such damage beyond that time.

Each evaluation first considers components that are designed to be damage-tolerant, loading conditions, and extent of possible damage, and then uses structural tests or analyses to substantiate that the design objective has been achieved. The evaluation also generates data needed for inspection programs to ensure detection of damage during the operational life of the component. Such evaluations and tests rely on engineering analyses—such as finite element analysis and structural analysis—and use quantitative approaches to establish the response of an aircraft component to various conditions of fatigue, corrosion, manufacturing defects, or accidental damage.

Fail-Safe for Systems

Fail-safe for systems treats failures differently. A *failure*—as defined in AC 25.1309-1A and in SAE ARP4761—is a malfunction or loss of function and differs from a *failure mode*, which is the way a failure in an item occurs. The focus is to understand the functional significance of failures in aircraft systems, use probability distributions to determine the contribution of a specific failure condition to overall system function, and to determine the risks to safety of flight associated with a failure condition. The purpose of the fail-safe design concept for systems is to meet the following design objectives stated in 14 CFR 25.1309:

> Airplane systems and associated components, considered separately and in relation to other systems, must be designed so that—
>
> 1. The occurrence of any failure condition which would prevent the continued safe flight and landing of the airplane is extremely improbable,[42] and

[41] FAA AC 25.571-1C defines multiple site damage (MSD) as "a source of widespread fatigue damage characterized by the simultaneous presence of fatigue cracks in the same structural element;" and multiple element damage (MED) as "a source of widespread fatigue damage characterized by the simultaneous presence of fatigue cracks in adjacent structural elements."

[42] FAA AC 25.1309-1A, paragraph 10b, defines *extremely improbable* failure conditions as those having a probability on the order of $1x10^{-9}$ or less.

2. The occurrence of any other failure condition which would reduce the capability of the airplane or the ability of the crew to cope with adverse operating conditions is improbable.[43]

Title 14 CFR 25.1309 also specifies that warning information about the failure condition be provided to the crew so that they may take the appropriate corrective action. These two design objectives provide the basis for airplane certification standard practices and establish the approach to be used to determine the relative importance (and severity) of a failure condition in a system. The fail-safe design concept requires that failures be considered in the following way:

- In any system or subsystem, the failure of any single element, component, or connection during any one flight (for example, brake release through ground deceleration to stop) should be assumed, regardless of its probability. Such single failures should not prevent continued safe flight and landing, or significantly reduce the capability of the airplane or the ability of the crew to cope with the resulting failure conditions.
- Subsequent failures during the same flight, whether detected or latent, and combinations thereof, should also be assumed, unless their joint probability with the first failure is shown to be extremely improbable.[44]

For certification, 14 CFR 25.1309 defines *systems* within the context of equipment and their installations, but the term is not applied to aircraft performance, structures, or strength capabilities. The way in which safety-critical systems are identified and treated by certification begins with establishment of the certification basis. Again, the focus is on understanding the functional significance of a failure in an aircraft system. Identifying the regulations that apply effectively determines how compliance with those regulations is accomplished, and the selection of a compliance method will determine how safety-critical systems are identified and evaluated.

A Distinction Between Structures and Systems

The two approaches to demonstrating compliance reveal the regulatory distinction between aircraft systems and aircraft structures. Demonstrating compliance for *aircraft structures* and *aircraft performance* typically uses *deterministic* methods that apply predetermined standards or criteria to assess the effects of fatigue, corrosion, and aerodynamic forces on aircraft components and aircraft strength capabilities. Conversely, demonstrating compliance for *systems* uses *probabilistic* risk assessment methods to assess the effect of failures on system *function* and *performance*.

---

[43] FAA AC 25.1309-1A, paragraph 10b, defines *improbable* failure conditions as those having a probability on the order of $1x10^{-5}$ or less, but greater than on the order of $1x10^{-9}$.

[44] FAA AC 25.1309-1A, paragraph 5.a

Both approaches to demonstrating compliance have their advantages. The use of engineering analysis and tests has a long regulatory history that has produced design criteria developed over decades of flight experience. Design criteria in regulations evolve, changing as the need arises and as experience is gained with specific types of materials, components, and design features. Consequently, in certain areas of airplane design, the knowledge required to evaluate structures and components is well established.

The very nature of modern aircraft makes the distinction between structures and systems increasingly difficult to define. Part of this trend is due to the advent of digital control and avionic systems where the standard approaches to engineering analysis cannot effectively deal with the complexities and uncertainties inherent in integrated software systems. Fly-by-wire systems, for instance, eliminate many of the mechanical links between components by substituting electronic digital control. The complexity of such systems and the accompanying control software dictate that they be evaluated using risk and hazard analyses; the tests for strength and durability required of traditional electromechanical systems no longer suffice. Further, because modern airplane systems are so complex and interdependent, safety assessments are needed at all functional levels. This is true of structural and flight components that are under software control, not just equipment that is contained within the purview of 14 CFR 25.1309. However, as previously stated, airplane-level risk and hazard analyses are neither required by certification regulation nor recommended by FAA advisory materials.

Conducting Safety Assessments

Safety assessments begin during Phase I and may continue until final approval of the TIA during Phase IV. All safety assessments are conducted by the applicant, and are reviewed and accepted by the FAA. Safety assessment results are not complete until the type certification basis is finalized in Phase III because the certification basis establishes the compliance requirements and the means for demonstrating compliance. Up to that point, safety assessments are preliminary and may be reviewed and commented upon by the FAA. The safety assessment process is outlined in AC 25.1309-1A and described in detail in SAE ARP4761. Although the safety assessment process outlined in the AC is not mandatory, applicants who choose not to conduct safety assessments must demonstrate compliance in another, FAA-approved way (for example, by conducting ground or flight tests).

Safety assessments do not begin with a predetermined set of safety-critical systems. Consequently, the first step in conducting a safety assessment is to establish criteria for selecting systems that are critical to safe operation. Selection criteria directly relate to failures and the effects of failures on system function. As stated in 14 CFR 25.1309, a system is deemed critical if its failure would prevent the continued safe flight and landing of the airplane, or if it would reduce the capability of the airplane or the ability of the crew to cope with adverse operating conditions. Title 14 CFR 25.1309 establishes an approach that uses risk and hazard analysis to identify safety-critical systems and considers the following:

1. possible failure modes as discussed in AC25.1309-1A,
2. the probability of multiple failures and undetected failures,
3. the resulting effects on the airplane and occupants, considering the stage of flight and operating conditions, and
4. crew warning cues, corrective action required, and the capability of detecting faults.

Note that the emphasis in 14 CFR 25.1309 is on a *failure condition*, not a failed component, and on the functional effects of the failure (or failures) on the airplane and its occupants. This point bears repeating: *the criticality of a failure condition—not the criticality of a faulty component—will determine if a system is safety critical.* For example, a jammed elevator caused by a broken linkage may not be a threat to flight safety unless the fault (the broken linkage) results in a failure condition (an airplane attitude caused by the jammed elevator) that adversely affects the functional ability of the airplane to fly or land or the crew's ability to maintain control. Consequently, the criticality of a system becomes evident through the assessment of risk during the safety assessment and is based on the adverse effect on overall system function.

Once the criteria for conducting a safety assessment are established, the applicant conducts system-specific analyses to identify and evaluate failure conditions and identify ways either to eliminate the adverse effects of a failure or to ensure that a failure is highly improbable.

Analytic and qualitative methods for conducting safety assessments include functional hazard assessments, preliminary system safety assessments, preliminary hazard analyses, and system safety assessments. Techniques that may be used to conduct the safety assessments include fault tree analyses, failure modes and effects analyses, failure modes and effects summaries, dependence diagrams, and Markov analyses. The techniques can be characterized as providing either a top-down or a bottom-up analysis of a design.

A top-down analysis, using functional hazard assessments and preliminary system safety assessments, begins with high-level functional descriptions and design objectives and produces a high-level description of the system architecture and associated failure conditions and a classification of failure severity. Functions are defined and, once the system design is finalized, failures are mapped to specific system components.

A bottom-up analysis—using failure modes and effects analysis, for example—typically begins with a single failure condition at the lowest level of a system. The purpose of a bottom-up analysis is to determine how a failure condition at one level affects the system at the next higher level. This is usually done by starting with basic components and component data and then building upon those data to conduct the requisite levels of analysis. The challenge for the analyst is to ensure that the systems and failure conditions identified in a bottom-up analysis are reconciled with the functions and functional failures identified in the top-down analysis.[45]

[45] See FAA AC 25.1309-1A and SAE ARP4761.

A functional hazard assessment (FHA)[46] typically provides the initial, top-level assessment of a design and addresses the operational vulnerabilities of system function. The FHA is therefore used to establish the safety requirements that guide system architecture design decisions. Performed independently of any specific design solution, an FHA is a deductive method that begins with an undesired event and works backward to find the root causes.[47] Such a top-down analysis can provide both airplane- and system-level examinations of functions and failure conditions. An FHA is conducted early in the design and development cycle to identify failure conditions and classify them by severity. An FHA is accomplished by defining all airplane system functions and then postulating all potential failures associated with those functions. The adverse effects of a failure condition on the airplane and crew provide the basis for assessing severity, with severity establishing the class of a failure condition.

The latest draft of the upcoming revision to AC 25.1309-1A includes five severity classes: no safety effect, and minor, major, hazardous, and catastrophic.[48] The differences among the classes are associated with effects on the airplane, effects on occupants and crew, and the qualitative and quantitative estimates of failure condition probability. The choice of functions and failure conditions is critical because the FHA provides the foundation for all subsequent analyses. Poor choices can lead to situations where more detailed analyses are not conducted because the criticality of a function is incorrectly classified. As a result, potentially dangerous failure conditions can remain undetected. The FAA is also developing new guidance policy[49] to clarify the use of risk assessment techniques in safety assessments and in the identification of flight-critical system components.

A Preliminary System Safety Assessment (PSSA) is used to determine how failure conditions can lead to the functional hazards identified in the FHA. The purpose of a PSSA is to evaluate the design and system architecture (1) to determine what requirements are needed and (2) to verify that the proposed architecture can meet the safety requirements established by the FHA. The PSSA is the first step in identifying specific solution strategies for meeting safety requirements and with this assessment, the focus shifts from airplane-level functions to potential design solutions for meeting safety requirements. The PSSA considers the system architecture at all levels, at a depth and detail commensurate with the complexity, novelty, and potential integration requirements of the proposed design solution. This iterative assessment method is initiated early in the design process and may be conducted throughout design and certification.

Once the applicant completes the FHA and the PSSA is underway, the FAA may review both analyses during Phase II before approving the certification plan. The safety

---

[46] See FAA AC 25.1309-1A and SAE ARP4761.

[47] *Fault Tree Handbook with Aerospace Applications* (Washington, DC: National Aeronautics and Space Administration, 2002.

[48] See FAA ANM-03-117-10, *Identification of Flight Critical System Components* (July 24, 2003), Appendix 2, Sec. 3.

[49] FAA ANM-03-117-10.

requirements derived from the FHA and the PSSA are used as input for system safety assessments. A system safety assessment is a systematic evaluation of a design solution and implemented system and can be accomplished using a number of different techniques: qualitative and quantitative fault tree analysis (FTA), failure modes and effects analysis (FMEA), failure modes and effects summary (FMES), dependence diagrams, and Markov analysis.

- An FTA is a structured, deductive, top-down graphical analysis that depicts the logical relationships between each failure condition and its primary causes and can use an FMEA as the basis for the analysis.
- An FMEA provides a qualitative and quantitative way to identify the effects of a single function or system failure at the next-higher level of a system.
- An FMES is a summary of the failures and failure probabilities identified by an FMEA and can be used as the input to a fault tree analysis.
- Dependence diagrams are analytically identical to the fault tree analysis and can play the same role, but do not show the output of the intermediate logical events that appear in the fault tree.
- A Markov analysis is a stochastic method that represents various system states and the probabilistic transition function from one state to the next. A Markov analysis can be used to represent the state transition network for a system, the interdependency among system states, and failure combination probabilities. Such an analysis is capable of handling the complexity of multiple, interdependent systems and has proven useful when an analysis includes many operational and maintenance factors.

In summary, safety assessments are the primary means by which the certification process identifies and evaluates *systems* (as opposed to identifying structures or airplane performance characteristics) that are critical to safe flight and operation. Safety assessments proceed in a stepwise, data-driven fashion, starting with systems at the functional level, and adding more specific design and implementation detail to address specific hazards, the potential effects of those hazards on the airplane and occupants, and possible solutions. The probability of a failure and the level of hazard classification are then used to determine the level of detail in an analysis for a particular system and its corresponding equipment. Thus, the final definition and characterization of a safety-critical system is the result of the analyses conducted during a safety assessment.

Conformity Inspections

AIR manufacturing inspectors or their designees conduct conformity inspections to ensure that the manufactured product conforms to the design reviewed and approved by the FAA. In the case of a transport-category airplane, inspections focus on the quality of the manufactured airplane, including tolerances, clearance, and compatibility with other installations. Although responsibility for conformity lies with the ACO, “manufacturing

inspectors determines whether the applicant satisfactorily shows the final product conforms to the type design and is in a condition for safe operation."[50] Conformity inspections can occur at any time in the certification process, but the request for an inspection must be accompanied by the applicant's statements of conformity and supporting design documents. The results of the inspections are reported in the Conformity Report, FAA Form 8100-1.

An applicant's manufacturing experience will determine the extent of the production conformity inspections, and under these circumstances, FAA inspectors may rely on sampling rather than 100 percent inspection, or they may rely on company inspectors. Deviations from standard manufacturing or inspection methods require considerable documentation and review by FAA inspectors. More scrutiny is also required for designs that are complex, require new and innovative manufacturing techniques, or significantly affect safety. Manufacturing inspectors also participate in engineering conformity inspections of test articles (for example, test and calibration equipment), and witness static, endurance, operational, and environmental tests. All conformity inspections are typically completed before the TIA is issued during Phase IV.

Type Inspection Authorization

The TIA is an important milestone, signaling the FAA's confidence that all regulations are being met and the start of the official FAA flight-test program. The TIA is issued by the Type Certification Board (in Phase IV) when the FAA is satisfied that the design is expected to be found compliant, and when the FAA has determined that testing can be performed at an acceptable level of safety. The FAA typically requires all structural analyses and many of the system safety assessments to be completed. However, issuance of the TIA does not indicate the end of the technical review of design data, analyses, and safety assessments, or the processing of issue papers, special conditions, equivalent safety findings, and exemptions. These efforts may continue throughout Phase IV.

Issuance of the TIA means that the FAA and the applicant agree that the type design has reached a level of maturity that will satisfy certification requirements. It also means that data are sufficient to guarantee a significant level of safety for certification flight test crews. Included in the TIA is the Type Inspection Report, which provides the record of all the conformity inspections and ground and flight tests authorized by the TIA, and will not be completed until all the testing is completed. The Type Inspection Report has two parts: part 1, concerning ground inspections, and part 2, concerning flight tests.

The purpose of the ground inspections is to determine if the airplane presented to the FAA for flight tests "meets the minimum requirements for quality, conforms with the technical data, and is safe for the intended flight tests."[51] Ground tests are progressive and are performed in three steps. Step 1 is a preliminary ground inspection of the prototype

[50] FAA Order 8110.4C, Chapter 5-2a.

[51] FAA Order 8110.4C, Chapter 5-15a.

conducted during the course of development and manufacture. Step 2, the Official Ground Inspection of the complete prototype, is conducted before FAA flight tests. During this inspection, the applicant makes the requisite statements of conformity and deems the airplane ready for inspection. Once this inspection is complete and the TIA is issued, the applicant can do no further work on the prototype unless an FAA inspector grants permission. Steps 1 and 2 comprise part 1 of the Type Inspection Report and are finished when FAA Form 8110-5 is complete and an FAA inspector grants permission to proceed to step 3.

During step 3, the coordinated ground-flight inspection, an FAA manufacturing inspector ensures that the aircraft is airworthy and ready for flight tests. Once flight tests begin, the inspector coordinates with the ACO project manager and FAA flight test pilots to ensure that any certification issues or problems detected during the test flight have been resolved as required for continued safe flight testing.

Part 2 of the Type Inspection Report is the record of flight tests conducted by the FAA. Flight tests are based on test plans and test articles developed for the TIA and requirements for flight testing outlined in 14 CFR 21.35. Although the testing plan is laid out in some detail in the PSCP (see table A5), it is the certification flight test plan approved at the pre-flight TCB meeting that appears in the TIA and determines how flight-testing will be conducted. The tests may range from assessments of basic flight characteristics to endurance tests required for certifying ETOPS, which allow flight over water for up to 207 minutes of flight time away from approved landing sites should one of the engines fail. Although the TIA may be issued before all conformity inspections and analyses are complete, the authorization will not be issued unless all the applicant's ground and flight tests are complete and the results reviewed and accepted by the FAA.

The FAA may request conformity inspections related to the TIA before flight-testing begins. Of particular importance are the test articles to be used in the flight tests and the documented condition of the flight test prototype. If the conformity inspection identifies any test article deviations, as defined in part 1 of the Type Inspection Report, the deviations are presented by FAA manufacturing inspectors to FAA engineering for resolution. If the deviations are accepted, the airplane is issued an experimental airworthiness certificate to show compliance with regulations. This means that the FAA accepts the airplane as the test article defined in part 1 of the Type Inspection Report and that certification flight-testing can proceed. The Type Inspection Report also reflects a level of risk determined acceptable by the Aircraft Certification Service Flight Safety Program. At this point, the FAA assesses crew interaction with airplane systems and determines if airplane performance requirements comply with regulations.

This phase of certification is complete when all FAA flight-test pilots and engineers agree that all tests listed in the TIA have been successfully completed. Regulations require that the flight test be at least 150 flight hours, or at least 300 flight hours if the aircraft is using turbine engines not previously used in a type-certificated aircraft.[52] Boeing has reported that during the flight test program for the 737-800 (a

[52] Title 14 CFR Part 21.35, paragraph f-1.

derivative design), the three test airplanes completed more than 760 flights, 550 hours of ground testing, and 740 hours of flight-testing.[53] During the certification flight-test program, the FAA and the applicant prepared the flight manual and conducted function and reliability testing.

The flight-testing program is also used to satisfy flight operational requirements for AEG technical specialists in support of activities for introducing an airplane into service. During flight tests, the FAA also reviews and approves the aircraft flight manual, thereby concurring with the applicant that the performance section, operational limits, and normal and emergency procedures in the flight manual are correct. The Type Inspection Report, which provides a record of all conformity inspections and ground and flight tests authorized by the TIA, becomes a permanent part of the official TC record.

For a new airplane design, the applicant has already conducted inspections and tests similar to those specified in the TIA. Before and during the early phases of the certification process, the applicant designs, develops, and tests components and prototypes. The applicant may expend considerable time and effort during this phase, and the FAA may be involved in the review and acceptance of preliminary design data. In fact, the applicant may have already conducted a flight-test program with FAA participation, especially if the applicant applied for an experimental-category special airworthiness certificate. A research and development program for a new aircraft is one reason for issuing an experimental airworthiness certificate.[54]

Type Certificate

The TC is issued at the final TCB meeting after the successful completion of all inspections and tests contained in the TIA. For the applicant, issuance of the TC is the culmination of the compliance effort and is the acknowledgement by the FAA that the airplane design meets all applicable Federal regulations and can be placed in service.

The Type Certificate Data Sheet (TCDS) is the part of the TC that documents the conditions and limitations of airworthiness. The TCDS has a specific format[55] describing the airplane model configuration, operating and performance limits, control surface movements and limits, weight and balance, crew requirements, passenger and cargo capacity, and fuel and oil capacities. Any subsequent models of the airplane based on the TC or any supplements to the TC also appear on the TCDS. The FAA must complete the TCDS within 2 weeks of the issuance of the TC.

The Instructions for Continued Airworthiness are also a part of the TC.[56] The ICA is required by regulation to have two parts: the airplane maintenance manual and the

[53] Boeing News Release, "Boeing Next-Generation 737-800 Receives FAA Approval," (March 16, 1998).

[54] Title 14 CFR 21.191, *Experimental Certificates*.

[55] FAA Order 8110.4C, paragraph 3-3d.

[56] Title 14 CFR 21.50b.

maintenance instructions.[57] The airplane maintenance manual describes the airplane and its components, component operation, and necessary maintenance and preventive maintenance. Also included is any servicing information that—

> covers details regarding servicing points, capacities of tanks, reservoirs, types of fluids to be used, pressures applicable to the various systems, location of access panels for inspection and servicing, locations of lubrication points, lubricants to be used, equipment required for servicing, tow instructions and limitations, mooring, jacking, and leveling information.[58]

Maintenance instructions provide the scheduling information for all airplane maintenance. The MRB Report using the MSG-3 process, described under *Project Specific Certification Plan,* is part of the maintenance instructions. These instructions are especially important in that they specify the applicant's recommendations for overhaul periods and provide cross-references to airworthiness limitations, troubleshooting information, requirements for removing and ordering the removal of parts, and procedures for testing components. These are the instructions that McDonnell Douglas and Boeing provided to Alaska Airlines stating the recommended lubrication and inspection intervals for the MD-80 jackscrew assembly.

The ICA, then, represents the basic initial maintenance plan for the airplane. The ICA must be complete, but not necessarily in its final form, when the TC is issued. An important point is that the ICA is produced by the applicant to meet operational and maintenance requirements by the AEG. In this role, the AEG assists the ACO to determine compliance of the ICA with applicable regulations. Thus, the AEG, representing Flight Standards, determines the maintenance and operational acceptability of the materials prepared by the applicant. The ICA is an important document because it conveys to operators and maintainers the manufacturer's assumptions concerning requirements for preserving the airworthiness of an airplane and its components while in service.

Post-Certification Products

Issuing the TC marks the end of Phase IV and the beginning of the post-certification activities that ensue during Phase V. These activities focus on documenting the certification process and establishing plans for managing the certificate and continued airworthiness.

A number of products are used to document the certification process. The Certification Summary Report is "an executive summary containing high-level descriptions of major issues and their resolution. The report should be used as a means for retaining corporate knowledge and lessons learned that could be beneficial for future type

[57] Title 14 CFR H25.3.

[58] Title 14 CFR H25.3, paragraph a-4.

certification projects involving the same or similar type design."[59] The summary is not intended to be comprehensive, but focuses on lessons learned, areas for process improvement, and significant technology issues or novel design features. The ACO also prepares and maintains a project file that contains only those documents showing a decision or action by the FAA and copies of all of the major certification products.[60] Type design and substantiating data may also be maintained by the FAA, at the discretion of the ACO (although the applicant may be required to maintain type design data and substantiating materials as defined by FAA Order 8110.4C, Appendix 10, Figure 2). Other kinds of information, such as draft issue papers or correspondence, are treated as working papers and are not necessarily maintained as part of the project file.[61]

Provisions are made during post-certification to ensure that continued airworthiness issues will be handled after the aircraft is in service. To that end, a certificate management plan and a continued airworthiness plan are the final products of the certification process (Phase V). A certificate management plan includes specific provisions for in-depth post-certification reviews of potentially unsafe design features or products. Called SCRs, these reviews are "a way to evaluate the type certification project and potentially unsafe design features on previously approved products." [62] SCRs can be initiated to review a number of potential problem areas, including the following:

- Complex or unique design features
- Advanced concepts in design and manufacturing
- Potentially unsafe features used on similar, previous designs requiring further analysis and evaluation
- Areas of compliance critical to safety
- Unsafe operational or maintainability characteristics
- Equivalent level of safety determinations
- Complicated interrelationships of unusual features

An SCR may be initiated by the accountable directorate or "as service experience dictates."[63] When concerned with compliance, an SCR may explore every aspect of the safety problem, including the applicant's original certification data, inspection of prototype and production articles, and "the adequacy of the applicable regulations and policy material."[64] Such a review becomes part of continued airworthiness for a TC. In addition to SCRs, the certificate management plan may provide for fact-finding

[59] FAA Order 8110.4C, paragraph 2-7a(1).

[60] For a complete list, see FAA Order 8110.4C, appendix 10, figure 1.

[61] FAA Order 8110.4C,appendic 12, paragraph 3-c.

[62] FAA Order 8110.4C, paragraph 2-7e(1).

[63] FAA Order 8110.4C, paragraph 2-7e(1a).

[64] FAA Order 8110.4C, paragraph 2-7e(1f).

investigations to gather evidence of potential noncompliance, to conduct accident investigations, and to store and retain records and data.

Other mechanisms are also in place to identify problems encountered during operations and maintenance that may lead to an AD. The FAA's ATOS was implemented in 1998 to enhance the Flight Standards air carrier surveillance requirement. According to the FAA, ATOS "uses system safety principles and risk management to make sure that air carriers have safety built into their operating systems."[65] The purpose of ATOS is to put in place a Part 121 air carrier surveillance program under the supervision of the FAA's Principal Inspectors and Certificate Management Team. FAA guidance states, "ATOS surveillance assesses an air carrier against established performance measures in relation to specific regulatory requirements and safety attributes for each element of an air carrier's systems."[66]

The ATOS process focuses on risk identification, assessment, and management, and uses a number of automated tools to allow the CMT to assess an air carrier's operation. The assessment includes a number of environmental and operational risk indicators. Surveillance data are gathered and contained in databases and are analyzed using a variety of qualitative and quantitative risk management and hazard analysis techniques. The initial phase of ATOS implementation began with 10 major air carriers including American Airlines and Alaska Airlines.

Finally, the FAA's Aircraft Certification Evaluation System (ACSEP)[67] ensures that holders of type production approvals and delegated facilities meet the requirements set forth in Federal regulations. ACSEP uses FAA engineering, flight test, and manufacturing inspection personnel to evaluate control of FAA-approved type design, production activities, and design approval systems. Consequently, the program focuses oversight and inspection on manufacturers, part suppliers, and delegated facilities and their adherence to Federal regulations. Once these continued airworthiness and certificate management plans are put in place, the airplane is ready for service in air carrier operations.

---

[65] FAA Order 8400.10, Appendix 6, *Air Transportation Operations Inspector's Handbook* Section 2, paragraph 122.

[66] FAA Order 8400.10, Appendix 6, Section 2, paragraph 125.

[67] FAA Order 8100.7B, *Aircraft Certification Systems Evaluation Program (ACSEP)* (July 1, 2003).

Appendix B: Certification Process Tables

Table B1: Establishing Partnership for Safety Plan
Source: *The FAA and Industry Guide to Product Certification*, 2nd Ed.

Goal	Initiating Condition	Action	Responsible Party	Participants
Management Goals				
Obtain training on certification process	Applicant presents design concept to Aircraft Certification Office (ACO)	Conduct training	ACO management	ACO and applicant management
Develop Partnership for Safety Plan (PSP)	Applicant and ACO initial meeting	Establish policy, practices Establish project schedule/milestones Establish procedures Establish communications protocol Establish issues resolution process Determine norms for evaluation	ACO management	ACO and applicant management
Submit PSP	Completed PSP	Sign PSP	ACO management	ACO and applicant management
Technical Goals				

Table B2: Phase I, Conceptual Design

Source: *The FAA and Industry Guide to Product Certification*, 2nd Ed., Phase I; FAA Orders 8110.4C, 8100.5A

Goal	Initiating Condition	Action	Responsible Party	Participants
Management Goals				
Establish project	Applicant contacts ACO with design concept	Assign project manager (PM) Assign project officer (PO) Assign project team members (as necessary in concept phase) Establish Type Certification Board (TCB)	ACO management	ACO and applicant
Conduct early familiarization TCB meetings	Establishment of project	Discuss new designs, technology, materials, and processes Document decisions, agreements, schedules, milestones, and action items	TCB	PM, PO, applicant, project engineers, technical specialists
Formulate Project Specific Certification Plan (PSCP) (also referred to as "Certification Program Plan" in 8110.4C)	Early familiarization TCB meeting	Become familiar with PSCP requirements Establish action items for— project schedule certification basis compliance coordination conformity testing production	PM	PO, applicant
Plan for resolution of critical issues	Early familiarization TCB meeting	Initiate planning for resolution of critical issues Establish deadline for resolution	PM	PO and applicant management
Process special condition	Identification of potential special condition	Notify Directorate and obtain concurrence Initiate special condition project Draft special condition document Forward draft to Directorate	PM	PO and applicant management
Coordinate special condition	Special condition published in *Federal Register*	Forward to applicant	PM	Applicant

Table B2: Phase I, Conceptual Design (continued)

Goal	Initiating Condition	Action	Responsible Party	Participants
Management Goals				
Conduct Phase I project evaluation	All aspects of Phase I completed	Complete Phase I evaluation checklist	PM	PM, PO, applicant
Technical Goals				
Establish preliminary certification basis	Early familiarization meeting	Review need for certification and basis requirements Determine intended means of compliance Identify applicable set of regulations Identify potential safety assessments and analyses	PO	Project engineers, technical specialists, flight-test pilot
Define critical issues	Early familiarization meeting	Identify new designs, technologies, processes Determine potential for: special conditions exemptions equivalent safety findings Develop method for tracking critical issues Develop issue papers	PM	PO, project engineers, technical specialists, flight-test pilot
Resolve critical issues	Definition of critical issues	Discuss technical issues Review design data and hardware Develop plan for resolution of critical issues Track resolution of critical issues	PM	PO, project engineers, technical specialists, flight-test pilot

Table B3: Phase II, Requirements Definition

Source: *The FAA and Industry Guide to Product Certification*, 2nd Ed., Phase II

FAA Orders 8110.4C, 8100.5, AC 25.1309, AC 121-22A

Goal	Initiating Condition	Action	Responsible Party	Participants
Management Goals				
Submit application for type certificate (TC)	Design of new aircraft or modification to existing aircraft	Complete form 8110-12 Submit drawings and basic design data to ACO	Applicant	ACO
Establish TC project	Application for TC submitted to ACO	Obtain basic design data Assign project number Notify appropriate Directorate Complete assignments to project team	ACO PM	ACO, applicant
Certification project notification	Submission of TC application	Complete Certification Project Notification (CPN) form Notify Aircraft Evaluation Group (AEG) and national resource specialist Establish Flight Standardization Board (FSB), Flight Operations Evaluation Board (FOEB), Maintenance Review Board (MRB)	PM	PO, applicant, AEG, NRS
Establish TCB	Certification project notification	Assign TCB members	ACO manager	PM, PO, applicant, ACO management, AEG management, flight test
Establish MSG-3 process	Establishment of MRB	Assign members to MSG-3 Establish Industry Steering Committee (ISC) Establish working groups Initiate preparation of MRB Report (MRBR) proposal Review basic design data Identify potential certification maintenance requirements (CMR)	MRB Chairman	AEG, PM, PO, project team, applicant

Table B3: Phase II, Requirements Definition (continued)

Goal	Initiating Condition	Action	Responsible Party	Participants
Management Goals				
Conduct preliminary TCB meeting	Establishment of TCB	Review project Work to establish certification basis Review and discuss design details, possible problem areas Identify areas requiring special compliance teams Identify novel or unique design features Establish schedule for project	TCB	PM, PO, applicant, project team
Produce preliminary PSCP (also referred to as Certification Program Plan in 8110.4C)	Preliminary TCB meeting	Determine schedule, milestones, program reviews Develop PSCP	TCB	PM, PO, applicant
Establish preliminary TC basis	Preliminary TCB meeting	Identify minimum set of applicable regulations Develop compliance plan	PM	PM, PO, applicant, relevant project team members
Plan for resolution of critical issues	Preliminary TCB meeting	Initiate planning for resolution of critical issues Define need for special conditions, exemptions, equivalent safety findings Establish deadline for resolution	PM	PO and applicant management
Process special condition	Identification of potential special condition	Notify Directorate and obtain concurrence Initiate special condition project Draft special condition document Forward draft to Directorate	PM	PO and applicant management
Coordinate special condition	Special condition published in *Federal Register*	Forward to applicant	PM	Applicant
Conduct Phase II project evaluation	All aspects of Phase II completed	Complete Phase II evaluation checklist	PM	PM, PO, applicant
Technical Goals				
Review basic design data	Application for TC submitted to ACO	Review drawings and basic design data Identify areas for technical review and discussion in TCB		

Table B3: Phase II, Requirements Definition (continued)

Goal	Initiating Condition	Action	Responsible Party	Participants
Management Goals				
Finalize preliminary certification basis	Preliminary TCB meeting	Review set of applicable regulations Determine means of compliance Identify need for safety assessments and risk analyses Identify special conditions, exemptions, equivalent safety findings Develop issue papers	PO	Project team, resource specialists, flight-test pilot
Prepare MRBR proposal	Establishment of MRB	Review MSG-3 requirements Develop initial minimum maintenance and inspection requirements Prepare Policy and Procedures Handbook (PPH) Formulate analysis approach and methods for identifying failures Identify Maintenance Significant Items (MSI) and Structural Significant Items (SSI) Provide working groups with data for MSI/SSI analysis Identify potential CRM Submit MRBR proposal to MRB	Applicant, ISC	Working groups
Process special conditions, exemptions, equivalent safety findings	Preliminary TCB meeting Issue paper	Identify new designs, technologies Determine need for— special conditions exemptions equivalent safety findings Track critical issues Develop issue papers	PM	PO, project engineers, technical specialists, flight-test pilot

Table B3: Phase II, Requirements Definition (continued)

Goal	Initiating Condition	Action	Responsible Party	Participants
Management Goals				
Resolve special conditions, exemptions, equivalent safety findings	Identification of special condition	Review issue papers and discuss technical issues Review design data and hardware Develop plan for resolution Plan safety assessments Request interim TCB meeting	PM	PO, project engineers, technical specialists, flight-test pilot
Conduct initial safety assessments	Plan for resolution of special conditions, exemptions, equivalent safety findings Issue paper	Identify design elements for safety assessments and risk analysis Plan safety assessments using: functional hazard analysis preliminary system safety assessment (PSSA) fault tree analysis (FTA) failure modes and effects analysis (FMEA) Conduct safety assessments	Applicant	PM, PO, project team

Table B4: Phase III, Compliance Planning

Source *The FAA and Industry Guide to Product Certification*, 2nd Ed. Phase III
FAA Orders 8110.4C, 8100.5, AC 25.1309-1A

Goal	Initiating Condition	Action	Responsible Party	Participants
Management Goals				
Conduct interim TCB meetings	As need arises	Review issues, problems Determine plan for resolution	TCB	PM, PO, applicant, project team (as required)
Produce final PSCP (also referred to as Certification Program Plan)	Initial safety assessments Stage 1 issues resolution Complete certification basis	Review PSCP Identify any outstanding action items Develop final PSCP Sign PSCP	TCB	PM, PO, applicant
Complete project schedule	Final PSCP	Establish milestones for— Safety assessments Test plan submission Type inspection authorization (TIA) Compliance and conformity Flight tests AEG evaluations and inspections Critical issues resolution	PM	PM, PO, applicant, project team
Establish TC basis	Completion of compliance plan Identification of complete set of applicable regulations	Review TC basis Approve TC basis Produce compliance checklist	PM	PM, PO, applicant, relevant project team members
Complete initial draft of all issue papers	Plan for resolution of critical issues Issue paper	Develop plan for resolving issue papers	PM	PO, applicant, project team
Complete initial safety assessments	Plan for resolution of critical issues Issue paper	Review status of safety system assessments Identify action items for completing initial assessments	PM	PO, applicant
Process special condition	Identification of potential special condition Issue paper	Notify Directorate and obtain concurrence Initiate special condition project Draft special condition document Forward draft to Directorate	PM	PO and applicant management

Table B4: Phase III, Compliance Planning (continued)

Goal	Initiating Condition	Action	Responsible Party	Participants
Management Goals				
Coordinate special condition	Special condition published in *Federal Register*	Forward to applicant	PM	Applicant
Obtain equivalent level of safety finding	Proposed equivalent level of safety submitted by applicant	Review proposal Obtain technical input Submit proposal to Directorate with recommendations for decision	PM	PO, applicant, relevant project team members
Process petition for exemption	Submission of petition for exemption	Review petition Submit petition to applicable Directorate	PM	PM, applicant
Determine conformity procedures	Draft PSCP	Identify elements of design requiring tests and inspections for conformity Establish procedures for conformity tests and inspections	PM	PO, applicant, project team
Identify stakeholders	Draft PSCP	Develop list of stakeholders, including: Suppliers Installers	PM	PM, applicant
Define oversight delegation	Draft PSCP	Identify oversight and documentation requirements Determine which elements of project to be delegated Identify designees Include delegations and oversight criteria in final PSCP	PM	Applicant
Conduct Phase III project evaluation	All aspects of Phase III completed	Complete Phase III evaluation checklist	PM	PM, PO, applicant
Technical Goals				
Review basic design data	Application for TC submitted to ACO	Review drawings and basic design data Identify areas for technical review and discussion in TCB		

Table B4: Phase III, Compliance Planning (continued)

Goal	Initiating Condition	Action	Responsible Party	Participants
Management Goals				
Finalize preliminary certification basis	Preliminary TCB meeting	Review set of applicable regulations Determine means of compliance Identify need for safety assessments and risk analyses Identify special conditions, exemptions, equivalent safety findings Develop issue papers	PO	Project team, resource specialists, flight-test pilot
Assess equivalent level of safety finding proposal	Proposed equivalent level of safety submitted by applicant	Review proposal and compensating factors Provide input for recommendation	PM	PO, relevant project team members
Develop issue paper	As need arises	Identify certification issue or problem Conduct technical discussion with project team Draft issue paper Submit to TCB for resolution	Project team	PM, PO, project engineers, technical specialists, flight-test pilot, inspectors
Process issue paper	Issue paper	Review issue papers and discuss technical issues Develop plan for resolution Plan safety assessments and risk analyses Present plans and results to TCB	PM	PO, project team, project engineers, resource specialists, flight-test pilot, inspectors
Conduct safety assessments	Plan for resolution of special conditions, exemptions, equivalent safety findings Issue paper	Identify design elements for safety assessments Plan safety assessments using: functional hazard analysis (FHA) PSSA FTA FMEA Conduct safety assessments and risk analyses	Applicant	PM, PO, project team

Table B5: Phase IV, Implementation

Source: *The FAA and Industry Guide to Product Certification*, 2nd Ed. Phase IV

FAA Orders 8110.4C, 8100.5A, AC 25.1309-1A

Goal	Initiating Condition	Action	Responsible Party	Participants
Management Goals				
Conduct interim TCB meetings	As need arises	Review issues, problems Determine plan for resolution	TCB	PM, PO, applicant, project team (as required)
Prepare for pre-flight TCB meeting	Resolution of compliance and conformity issues	Identify outstanding conformity and compliance issues	TCB	PM, PO, applicant
Demonstrate compliance	Submission of type design and substantiating data by applicant	Determine if all conformity and compliance issues have been resolved Determine if all appropriate engineering activities have been accomplished	TCB	PM, PO, applicant
Approve MRB Report	Submission of MRBR proposal by applicant	Review ISC and working group (WG) reports Review and resolve any outstanding problems or issues Approve MRBR	MRB	Applicant, AEG, ISC, WGs
Conduct pre-flight TCB Meeting	Compliance demonstrated	Review Aircraft Certification Service (AIR) Risk Assessment Process results Identify any outstanding: Conformity inspection issues Engineering compliance issues Issue TIA	TCB	PM, PO, applicant
Process special condition	Identification of potential special condition Issue paper	Notify Directorate and obtain concurrence Initiate special condition project Draft special condition document Forward draft to Directorate	PM	PO and applicant management
Coordinate special condition	Special condition published in *Federal Register*	Forward to applicant	PM	Applicant
Obtain equivalent level of safety finding	Proposed equivalent level of safety submitted by applicant	Review proposal Obtain technical input Submit proposal to Directorate with recommendations for decision	PM	PO, applicant, relevant project team members

Table B5: Phase IV, Implementation (continued)

Goal	Initiating Condition	Action	Responsible Party	Participants
Management Goals				
Process petition for exemption	Submission of petition for exemption	Review petition Submit petition to applicable Directorate	PM	PM, applicant
Conduct final TCB meeting	Completion of all tests	Review status of all outstanding items and issues Formalize decision to issue TC Issue TC when all items and issues resolved	TCB	PM, PO, applicant
Conduct Phase IV project evaluation	All aspects of Phase IV completed	Complete Phase IV evaluation checklist	PM	PM, PO, applicant
Technical Goals				
Evaluate and approve design data	Submission of type design and substantiating data by applicant	Review data, drawings, specifications, and reports Identify applicable airworthiness standards Identify any operational considerations Determine if compliance is complete Update and complete test plan Identify necessary tests and inspections	FAA engineer	PO, project team, AEG
Develop plan for certification testing	Submission of type design and substantiating data by applicant	Define test articles Develop test plan Submit test plan	Applicant	PM, PO
Review test plan	Test plan submitted by applicant	Review test plan Determine if test plan is complete for all necessary products Approve test plan	FAA engineer	PO, project team
Develop issue paper	As need arises	Identify certification issue or problem Conduct technical discussion with project team Draft issue paper Submit to TCB for resolution	Project team	PM, PO, project engineers, technical specialists, flight-test pilot, inspectors

Table B5: Phase IV, Implementation (continued)

Goal	Initiating Condition	Action	Responsible Party	Participants
Management Goals				
Process issue paper	Issue paper	Review issue papers and discuss technical issues Develop plan for resolution Plan safety assessments and risk analyses Present plans and results to TCB	PM	PO, project team, project engineers, resource specialists, flight-test pilot, inspectors
Assess equivalent level of safety finding proposal	Proposed equivalent level of safety submitted by applicant	Review proposal and compensating factors Provide input for recommendation	PM	PO, relevant project team members
Conduct conformity inspections	Submission of type design and substantiating data by applicant	Identify products requiring inspections Request and schedule inspections Review results of inspection Prepare Conformity Inspection Report (CIR)	FAA inspector	PO, project team, AEG inspectors
Conduct engineering and AEG compliance inspections	Submission of type design and substantiating data by applicant	Identify products/installations/systems requiring inspection for compliance with regulations Review and inspection maintenance procedures Delegate to appropriate designated engineering representative (DER) Schedule inspections Ensure compliance and conformity Review results and issue notification of noncompliance where appropriate Produce Type Inspection Reports (TIRs) Prepare Conformity Inspection Record (CIR) Produce issue papers	FAA inspector	PO, AEG, project team

Table B5: Phase IV, Implementation (continued)

Goal	Initiating Condition	Action	Responsible Party	Participants
Management Goals				
Prepare flight and ground test plan	Issuance of TIA	Review compliance with regulations Perform AIR risk management process Determine— Test article configuration Test equipment configuration Expected results Identify tests to be witnessed Identify any nonconformities and report Prepare test plan	AEG inspector	PM, PO, applicant, project team
Conduct operational and airworthiness evaluations	Issuance of TIA	Review maintenance programs Develop MRB Review flight manuals Develop master minimum equipment list Establish type rating requirements Determine crew compliment Establish training requirements Produce issue papers Prepare TIRs Prepare Conformity Inspection Record (CIR)	AEG inspector	FSB, AEG, PO, project team
Conduct ground tests	Approval of test plan	Conduct preliminary ground tests (Phase I) Obtain statement of conformity Conduct official ground inspection of complete prototype (Phase II) Conduct coordinated ground-flight inspections (Phase III) Prepare TIRs	AEG inspector	FOEB, PM, PO, AEG, flight-test pilot, project team
Conduct flight tests	Completion of ground tests and inspections Flight test report from applicant	Conduct flight tests in plan		
Approve flight manual	Submission of type design and substantiating data by applicant	Review operational limitations, normal and emergency procedures Review performance section of manual	PO	PM, FOEB, AEG, flight-test pilot, applicant

Table B6: Phase V, Post Certification

Source: *The FAA and Industry Guide to Product Certification*, 2nd Ed. Phase V, FAA Orders 8110.4C, 8100.5A

Goal	Initiating Condition	Action	Responsible Party	Participants
Management Goals				
Develop compliance summary report	Issuance of TC	Summarize record of FAA examinations Discuss significant safety issues Describe how complied with applicable airworthiness, noise and emissions requirements	ACO	PM, PO, applicant
Prepare TIRs	Completion of all TIA inspections and tests	Prepare TIR, Part I, Ground Inspection Prepare TIR, Part II, Flight Test	ACO	PM, PO, AEG
Prepare Instructions for Continued Airworthiness (ICA)	Completion of all TIA inspections and tests	Review ICA and airworthiness limitations Approve ICA Publish ICA	ACO	PM, PO, AEG
Develop Certificate Management Plan	Completion of all TIA inspections and tests	Establish Certificate Management Team Incorporate airworthiness, maintenance, and operations requirements in plan Incorporate provisions for Special Certification Reviews (SCR)	ACO	AEG
Conduct Phase V project evaluation	All aspects of Phase V completed	Complete Phase V evaluation checklist	PM	PM, PO, applicant

`

Appendix C: Transport-Category Airplane-Related Accidents

Table C1. Transport-Category Airplane-Related Accidents, 1962–2000

Failed Airplane Element	Number of Airplane-Related Accidents	Type of System or Component Failure
Airplane Structure	14	Wing failure/separation Cargo door failure Engine pylon separation Bulkhead failure Jackscrew assembly failure
Engine/Propulsion System	9	Thrust reverser deployed Beta in flight Propeller moved below idle Propeller separation in flight
Engine Containment	6	Fan rotor failure Combustor failure Front hub failure
Flight/Ground Control System	10	Ground spoiler deployment Uncommanded rudder movement Yaw damper failure Vertical stabilizer separation
Fuel Tank System	6	Fuel tank explosion, loss of wing Fuel tank explosion, in-flight breakup Fuel tank fire
Fire Suppression or Detection	2	Cargo hold fire Cockpit electrical fire
Structural Icing	8	Wing icing Fixed leading edge Uncommanded aileron movement

Airplane Structure				
Air Carrier	**Airplane Make/Model**	**Location**	**Date**	**Cause/Factor**
Braniff Airlines	L-188	Buffalo, NY	9/29/59	structural failure of the left wing resulting from forces generated by undamped propeller whirl mode
Northwest Airlines	L-188	Cannelton, IN	3/17/60	separation of the right wing in flight due to flutter induced by oscillations of the outboard nacelles. Contributing factors were a reduced stiffness of the structure
Turkish Airlines	DC-10	Paris, France	3/03/74	ejection in flight of the aft cargo door and sudden decompression due to incorrect engagement of the door latching mechanism before takeoff
American Airlines	DC-10	Windsor, Canada	6/12/72	improper engagement of latching mechanism for aft cargo door during preparation for flight
DAN AIR	B-707	Lusaka, Zambia	5/14/77	right hand horizontal stabilizer rear spar top chord failed prior to the accident flight due to long-term fatigue damage
American Airlines	DC-10	Chicago, IL	5/25/79	separation of the No.1 engine and pylon assembly during takeoff due to improper maintenance
Aloha Airlines	B-737	Maui, HI	4/28/88	failure of the lap joint and the separation of the fuselage upper lobe due to a failure to detect presence of disbonding and fatigue damage
United Airlines	B-747	Honolulu, HI	6/15/90	sudden opening of the forward cargo door in flight and the subsequent decompression attributed to faulty door control system which permitted electrical actuation of the door latches
Air India	B-747	Delhi, India	5/07/70	partial separation of No. 1 engine during landing roll due to improperly installed diagonal-brace aft fuse-pin on engine
China Air	B-747	Wanli, Taiwan	12/29/91	Separation of No. 3 and 4 engines due to pylon failures
El Al	B-747	Amsterdam, Holland	10/04/92	Separation of No. 3 and 4 engines due to fatigue in pylon and inadequate pylon design
Japan Airlines	B-747	Mt. Ogura, Japan	8/21/95	rear pressure bulkhead failure
Delta Airlines	L-1011	Pacific Ocean	8/23/95	bulkhead failure and in-flight decompression due to fatigue cracking
Alaska Airlines	MD-83	Point Hueneme, Ca	1/31/00	loss of pitch control resulting from the in-flight failure of the acme nut threads in the horizontal stabilizer trim system jackscrew assembly

Engine/Propulsion Systems				
Air Carrier	**Airplane Make/Model**	**Location**	**Date**	**Cause/Factor**
Lauda	B-767	Thailand	5/26/91	thrust reverser deployed in flight
TAM	Fokker 100	Sao Paulo, Brazil	10/31/96	thrust reverser deployed on take-off
TWA	B-717	Milwaukee, WI	2/19/01	thrust reverser deployed on take-off
Fisher Brothers Aviation	Casa-212	Romulus, MI	3/04/87	beta in flight due to inadequate lockout
Executive Air	Casa-212	Mayaguez, PR	5/08/87	beta in flight
ASA	Embraer-120	Brunswick, GA	4/05/91	propeller moved below flight idle in flight
Executive Air	Casa-212	Mayaguez, PR	6/07/92	beta in flight
American Eagle	Saab-340	New Roads, LA	2/01/94	propeller moved below flight idle in flight
ASA	Embraer-120	Carrollton, GA	8/21/95	propeller separation in flight

Flight/Ground Control Systems				
Air Carrier	**Airplane Make/Model**	**Location**	**Date**	**Cause/Factor**
Air Canada	DC-8	Toronto, Canada	7/05/70	deployment of ground spoilers in landing flare due to inadequate design of lockout mechanism
United Airlines	B-737	Colorado Springs, CO	3/03/91	uncommanded rudder movement due to jam of main rudder PCU servo valve
United Airlines	B-737	Chicago, Il	7/16/92	rudder anomaly at ground check, M. Moore
USAir	B-737	Aliquippa, PA	9/08/94	uncommanded rudder movement due to jam of main rudder PCU servo valve
Eastwind Airlines	B-737	Richmond, VA	6/09/96	uncommanded rudder movement due to jam of main rudder PCU servo valve
Metrojet	B-737	Salisbury, MD	2/23/99	uncommanded rudder movement
various	B-737			yaw damper events
British Airways	B-747	London, England	10/07/93	uncommanded elevator movement on depart
Alaska Airlines	MD-83	Point Hueneme, CA	1/31/00	loss of pitch control resulting from the in-flight failure of the acme nut threads in the horizontal stabilizer trim system jackscrew assembly
American Airlines	A300-605R	Belle Harbor, NY	11/12/01	separation of vertical stabilizer due to high sideslip angle caused by pilot's rudder inputs

Fuel Tank System				
Air Carrier	**Airplane Make/Model**	**Location**	**Date**	**Cause/Factor**
Pan American Airlines	B-707	Elkton, MD	12/08/63	explosive disintegration of the left outer wing and loss of control due to lightning-induced ignition of the fuel/air mixture in the No. 1 reserve fuel tank
Iranian Air Force	B-747	Madrid, Spain	5/09/76	separation of left wing due to lightning strike in vicinity of No. 1 fuel tank
Avianca	B-727	Bogota, Colombia	11/27/89	separation of wings due to explosive device igniting the fuel-air vapors in the center or No. 2 tank
Philippines Airlines	B-737	Manila, Philippines	5/11/90	center wing fuel tank explosion on ground due to ignition of fuel tank vapors
TWA 800	B-747	East Moriches, NY	6/17/96	explosion of the center wing fuel tank, resulting from ignition of fuel/air mixture in the tank most probably due to a short circuit outside of the tank
Thai Airways	B-737	Bangkok, Thailand	3/02/01	CFT, pump, wire short

Fire Suppression/Detection				
Air Carrier	**Airplane Make/Model**	**Location**	**Date**	**Cause/Factor**
ValuJet	DC-9	Everglades, FL	5/11/96	cargo hold fire due to ignition of oxygen generators
SwissAir	MD-11	Nova Scotia, Canada	9/02/98	electrical fire due to improper installation of in-flight entertainment system

Engine Containment				
Air Carrier	**Airplane Make/Model**	**Location**	**Date**	**Cause/Factor**
National Airlines	DC-10	Albuquerque, NM	11/03/73	Fan rotor failure
British Airtours	B-737	Manchester, Englnd	8/22/85	Combuster can failure
Midwest Express	DC-9	Milwaukee, WI	9/06/85	HPC spacer failure
United Airlines	DC-10	Sioux City, IA	10/08/92	Fan rotor failure
ValuJet	DC-9	Atlanta, GA	6/08/95	7^{th} stage HPC disk rupture
Delta	MD-88	Pensacola, FL	3/31/98	front hub failure

Structural Icing				
Air Carrier	**Airplane Make/Model**	**Location**	**Date**	**Cause/Factor**
Air Florida	B-737	Washington, DC	1/13/82	icing- wing/engines
Airborne Express	DC-9	Philadelphia, PA	2/05/85	wing icing
Continental Airlines	DC-9	Stapleton, CO	11/15/87	during take-off, 27 min after deicing resulting in a fixed leading edge
Mid Pacific Airlines	YS-11A	West Lafayette, IN	3/15/89	icing on approach
Ryan International	DC-9-15	Cleveland, OH	2/17/91	during take-off, after deicing resulting in a fixed leading edge
USAir	F-28	Flushing, NY	3/22/92	during take-off, after deicing resulting in a fixed leading edge
American Eagle	ATR-72	Roselawn, IN	10/31/94	uncommanded aileron movement
COMAIR	EMB-120	Monroe, MI	1/09/97	wing ice while holding resulting in a fixed leading edge

Appendix D: Status and Disposition of NTSB Safety Recommendations

Safety Recommendation Letter Status

The full text of the NTSB Safety Recommendations for each of the accident investigations discussed in the report is presented in this appendix. Included are current status of the recommendation and the date of the latest correspondence showing the source and the recipient, as of April 21, 2005. More details about each of the recommendations can be found on the National Transportation Safety Board website at <www.ntsb.gov/Recs/index.htm.>

United Airlines Flight 585

A-92-120
Require operators, by airworthiness directive, to incorporate design changes for the B-737 main rudder power control unit servo valve when these changes are made available by Boeing. These changes should preclude the possibility of rudder reversals attributed to the overtravel of the secondary slide.

Status: Closed—Acceptable Action
Most Recent Correspondence: NTSB response to FAA on 8/11/1994

A-92-121
Conduct a design review of servo valves manufactured by Parker Hannifin having a design similar to the B-737 rudder power control unit servo valve that control essential flight control hydraulic power control units on transport-category airplanes certified by the Federal Aviation Administration to determine that the design is not susceptible to inducing flight control malfunctions due to overtravel of the servo slides.

Status: Closed—Acceptable Action
Most Recent Correspondence: NTSB response to FAA on 6/10/1993

USAir Flight 427 Accident Investigation

A-99-21
Convene an engineering test and evaluation board to conduct a failure analysis to identify potential failure modes, a component and subsystem test to isolate particular failure modes found during the failure analysis, and a full-scale integrated systems test of the Boeing 737 rudder actuation and control system to identify potential latent failures and validate operation of the system without

regard to minimum certification standards and requirements in 14 Code of Federal Regulations Part 25. Participants in the engineering test and evaluation board should include the Federal Aviation Administration (FAA); National Transportation Safety Board technical advisors; the Boeing Company; other appropriate manufacturers; and experts from other government agencies, the aviation industry, and academia. A test plan should be prepared that includes installation of original and redesigned Boeing 737 main rudder power control units and related equipment and exercises all potential factors that could initiate anomalous behavior (such as thermal effects, fluid contamination, maintenance errors, mechanical failure, system compliance, and structural flexure). The engineering board's work should be completed by March 31, 2000, and published by the FAA.

Status: Closed—Acceptable Action
Most Recent Correspondence: NTSB response to FAA on 4/25/2001

A-99-23
Amend 14 Code of Federal Regulations Section 25.671(c)(3) to require that transport-category airplanes be shown to be capable of continued safe flight and landing after jamming of a flight control at any deflection possible, up to and including its full deflection, unless such a jam is shown to be extremely improbable.

Status: Open—Unacceptable Response (referral to ARAC does not mean recommended action has been taken)
Most Recent Correspondence: NTSB response to FAA on 4/25/2001

TWA Flight 800

A-96-174
Require the development of and implementation of design or operational changes that will preclude the operation of transport-category airplanes with explosive fuel-air mixtures in the fuel tank: (a) significant consideration should be given to the development of airplane design modifications, such as nitrogen-inerting systems and the addition of insulation between heat-generating equipment and fuel tanks. Appropriate modifications should apply to newly certificated airplanes and, where feasible, to existing airplanes.

Status: Open—Acceptable Response
Most Recent Correspondence: FAA response to NTSB on 2/1/2005

A-96-175
Require the development of and implementation of design or operational changes that will preclude the operation of transport-category airplanes with explosive fuel-air mixtures in the fuel tanks: (b) pending implementation of design modifications, require modifications in operational procedures to reduce the potential for explosive fuel-air mixtures in the fuel tanks of transport-category aircraft. In the B-747, consideration should be given to refueling the center wing fuel tank (CTW) before flight whenever possible from cooler ground fuel tanks, proper monitoring and management of the CWT fuel temperature, and maintaining an appropriate minimum fuel quantity in the CWT.

Status: Closed—Unacceptable Action
Most Recent Correspondence: NTSB response to FAA on 11/15/2005

Alaska Airlines Flight 261

A-02-41
Review all existing maintenance intervals for tasks that could affect critical aircraft components and identify those that have been extended without adequate engineering justification in the form of technical data and analysis demonstrating that the extended interval will not present any increased risk and require modifications of those intervals to ensure that they (1) take into account assumptions made by the original designers, (2) are supported by adequate technical data and analysis, and (3) include an appropriate safety margin that takes into account the possibility of missed or inadequate accomplishment of the maintenance task. In conducting this review, the Federal Aviation Administration should also consider original intervals recommended or established for new aircraft models that are derivatives of earlier models and, if the aircraft component and the task are substantially the same and the recommended interval for the new model is greater than that recommended for the earlier model, treat such original intervals for the derivative model as "extended" intervals.

Status: Open—Acceptable Alternate Response
Most Recent Correspondence: NTSB response to FAA on 1/13/2005

A-02-42
Conduct a systematic industrywide evaluation and issue a report on the process by which manufacturers recommend and airlines establish and revise maintenance task intervals and make changes to the process to ensure that, in the future, intervals for each task (1) take into account assumptions made by the original designers, (2) are supported by adequate technical data and analysis, and (3) include an appropriate safety margin that takes into account the possibility of missed or inadequate accomplishment of the maintenance task.

Status: Open—Acceptable Response
Most Recent Correspondence: NTSB response to FAA on 1/13/2005

A-02-43
Require operators to supply the Federal Aviation Administration (FAA), before the implementation of any changes in maintenance task intervals that could affect critical aircraft components, technical data and analysis for each task demonstrating that none of the proposed changes will present any potential hazards, and obtain written approval of the proposed changes from the principal maintenance inspector and written concurrence from the appropriate FAA aircraft certification office.

Status: Open—Acceptable Response
Most Recent Correspondence: NTSB response to FAA on 1/13/2005

A-02-45
Require operators to permanently (1) track end play measures according to airplane registration number and jackscrew assembly serial number, (2) calculate and record average wear rates for each airplane based on end play measurements and flight times, and (3) develop and implement a program to analyze these data to identify and determine the cause of excessive or unexpected wear rates, trends, or anomalies. The Federal Aviation Administration (FAA) should also require operators to report this information to the FAA for use in determining and evaluating an appropriate end play check interval.

Status: Open—Acceptable Alternate Response
Most Recent Correspondence: NTSB response to FAA on 1/13/2005

A-02-49
Conduct a systematic engineering review to (1) identify means to eliminate the catastrophic effects of total acme nut thread failure in the horizontal stabilizer trim system jackscrew assembly in Douglas DC-9 (DC-9), McDonnell Douglas MD-80/90 (MD-80/90), and Boeing 717 (717) series airplanes and require, if practicable, that such fail-safe mechanisms be incorporated in the design of all existing and future DC-9, MD-80/90, and 717 series airplanes and their derivatives; (2) evaluate the horizontal stabilizer trim systems of all other transport-category airplanes to identify any designs that have a catastrophic single-point failure mode and, for any such system; (3) identify means to eliminate the catastrophic effects of that single-point failure mode and, if practicable, require that such fail-safe mechanisms be incorporated in the design of all existing and future airplanes that are equipped with such horizontal stabilizer trim systems.

Status: Open—Acceptable Response
Most Recent Correspondence: NTSB response to FAA on 1/13/2005

A-02-50
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.

Status: Open—Acceptable Response
Most Recent Correspondence: NTSB response to FAA on 1/13/2005

A-02-51
Review and revise aircraft certification regulations and associated guidance applicable to the certification of transport-category airplanes to ensure that wear-related failures are fully considered and addressed so that, to the maximum extent possible, they will not be catastrophic.

Status: Open—Acceptable Response
Most Recent Correspondence: NTSB response to FAA on 1/13/2005

American Airlines Flight 587

A-04-56
Modify 14 Code of Federal Regulations Part 25 to include a certification standard that will ensure safe handling qualities in the yaw axis throughout the flight envelope, including limits for rudder pedal sensitivity.

Status: Open—Acceptable Response
Most Recent Correspondence: NTSB response to FAA on 8/3/2005

A-04-57
After the yaw axis certification standard recommended in Safety Recommendation A-04-56 has been established, review the designs of existing airplanes to determine if they meet the standard. For existing airplanes designs that do not meet the standard, the FAA should determine if the airplanes would be adequately protected from the adverse effects of a potential aircraft-pilot coupling (APC) after rudder inputs at all airspeeds. If adequate protection does not exist, the FAA should require modifications, as necessary, to provide the airplanes with increased protection from the adverse effects of a potential APC after rudder inputs at high airspeeds.

Status: Open—Acceptable Response
Most Recent Correspondence: NTSB response to FAA on 8/3/2005

A-04-58
Review the options for modifying the Airbus A300-600 and the Airbus A310 to provide increased protection from potentially hazardous rudder pedal inputs at high airspeeds and, on the basis of this review, require modifications to the A300-600 and A310 to provide increased protection from potentially hazardous rudder pedal inputs at high airspeeds.

Status: Open—Acceptable Response
Most Recent Correspondence: NTSB response to FAA on 8/3/2005

A-04-60
Amend all relevant regulatory and advisory materials to clarify that operating at or below maneuvering speed does not provide structural protection against multiple full control inputs in one axis or full control inputs in more than one axis at the same time.

Status: Open—Acceptable Response
Most Recent Correspondence: NTSB response to FAA on 8/3/2005

A-04-63
Review the options for modifying the Airbus A300-600 and the Airbus A310 to provide increased protection from potentially hazardous rudder pedal inputs at high airspeeds and, on the basis of this review, require modifications to the A300-600 and A310 to provide increased protection from potentially hazardous rudder pedal inputs at high airspeeds.

Status: Open—Acceptable Response
Most Recent Correspondence: NTSB response to EASA on 8/3/2005

this page intentionally left blank