



National Transportation Safety Board

Washington, D.C. 20594

Safety Recommendation

Date: MAY 17 2006

In reply refer to: A-06-36 through A-06-38

Honorable Marion C. Blakey
Administrator
Federal Aviation Administration
Washington, D.C. 20591

Certification of systems that are critical to safety of flight has been an issue in several 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 261³ and the rudder system in American Airlines flight 587⁴ 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 In each of these accidents, the Board identified a safety-critical system that suffered a catastrophic failure, and issued certification-related recommendations to address system-specific design, operational, or maintenance issues.⁶

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 operated 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 The following certification-related recommendations were issued by the Safety Board for the four accidents: for USAir flight 427, A-99-020 through 023, and 027; for TWA flight 800, A-96-174, 175, and 177, A-98-034 through

As a result, the Safety Board examined the FAA's type certification process for safety-critical systems in transport-category airplanes to determine possible improvements. To relate the issues found in the four accidents to type certification, the Safety Board employed a retrospective methodology to examine the specific processes that are used to assess hazards to safety of flight. A process analysis was used to identify key certification activities related to the assessment of safety-critical systems and most closely associated with the findings from the four accidents. The resulting *Safety Report on the Treatment of Safety-Critical Systems in Transport Airplanes* presents the Safety Board's findings and uses the four accident investigations mentioned above to highlight the Board's concerns.⁷

As a result of its analysis, the Safety Board's report identifies three type certification safety issues: identification and documentation of safety-critical systems, enhancements to safety assessments, and the ongoing assessment of safety-critical systems. The Board makes recommendations to the FAA to address each of these issues.

During development of this safety report, the Safety Board also considered a number of recent certification studies, including the FAA's *Commercial Airplane Certification Process Study* (CPS).⁸ The FAA published a series of CPS findings in 2002, and an implementation plan in 2004, and made its progress report available to the Board in April 2006. The Board is encouraged by FAA progress in implementing the 2004 plan. The Board also believes that its safety report provides insights into a number of areas where additional improvements are needed, and that the recommendations contained in this letter are consistent with CPS efforts.

Identifying and Evaluating Safety-Critical Systems

The FAA uses the safety assessment process to identify and evaluate safety-critical functions in systems. The process 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. As described in the Board's report, 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." This is the position taken by the FAA in its most recent policy on the identification and evaluation of "flight critical system components" and is consistent with industry practice for assessing the criticality of hazards to safety of flight.

The Safety Board concludes in its safety report that the safety assessment process is an effective way to identify safety-critical systems during type certification. However, the Board

036, 038, and 039, and A-00-105 and 106; for Alaska Airlines flight 261, A-01-041, 042, and 045, A-02-039 through 045 and 049 through 051; and for American Airlines flight 587, A-04-056 through 057, 058, 060, and 063.

⁷ The Safety Board unanimously adopted this report on April 25, 2006.

⁸ *Commercial Airplane Certification Process Study* (Washington, DC: Federal Aviation Administration, March 2002).

also concludes that the lack of a requirement to prepare such a list during type certification compromises the ongoing assessment of safety-critical systems.

The Safety Board has also found that the Federal Aviation Regulations 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. Further, the Board finds that the Certification Summary Report generated after the certification process is complete and described in Order 8110.4C “is a high-level description of major issues and their resolution”⁹ that may not capture the details required to effectively evaluate service history and operational experience on an ongoing basis.

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.¹⁰ (A-06-36)

Enhancements to Safety Assessments

In addition to improving the documentation of safety-critical systems derived from the safety assessment process, the Safety Board has determined that safety assessments could be improved by including two types of important functional hazards that are currently excluded: failures in structures that have a functional effect on systems and failures associated with human interaction with airplane systems.

Structural failures are excluded from safety assessments because Federal regulations specify different methods of compliance for systems and for structures. Further, 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.¹¹ Consequently, structural failures are excluded from safety assessments, which can hinder the identification of safety-critical systems.

The problem created by excluding the functional implication of structural failures was evident in the Alaska Airlines flight 261 investigation. During the public hearing, the FAA used the distinction between structures and systems to explain why a safety assessment of the entire jackscrew assembly had not occurred, either during certification of the DC-9 when regulations

⁹ FAA Order 8110.4C, paragraph 2-7a(1).

¹⁰ The project file is described in the *Data Retention* section of FAA Order 8110.4C, paragraph 2-7f.

¹¹ FAA AC 25.1309-1A, section 3.

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 each case, the acme nut was not considered part of a system and therefore was not required to comply with certification requirements for airplane systems. The Safety Board concludes that the effects of structural failures on the performance of related systems are not adequately considered in risk assessments for type certification, and that a general application of the Board's Safety Recommendation A-02-50 from Alaska 261 should be applied to all safety-critical systems.

In addition to excluding structural failures, the Safety Board has found that safety assessments do not adequately address human/system interaction failures. Human error is a major, recurring issue in aviation accidents. Human factors considerations for certification purposes are specified in regulations as specific design criteria, and in a way similar to the criteria for airplane performance, structures, and flight characteristics. However, 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."¹² The most rigorous evaluations of human/airplane system interaction occur late in the certification process 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.

The importance of evaluating human performance during safety assessments was illustrated in American Airlines flight 587. The investigation showed that there were no certification criteria for rudder pedal sensitivity, and that there was evidence of pilot use of rudder in upset recovery. The Safety Board concluded that the potential for human error is increased when an airplane design contains complexities that are difficult for people to discern in an operational context. In its flight 587 accident report, the Board described 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: "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."¹³

Although 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 Safety Board concludes that these exclusions limit the scope of the failure conditions considered during the safety assessment process. The Safety Board therefore 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. (A-06-37)

¹² FAA AC 25.1309, paragraph 7b(2).

¹³ American Airlines flight 587, pp. 149-150.

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 among the 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 261 accident investigation, which found that changes to maintenance practices and intervals were made without sufficient analysis, justification, and consideration of design assumptions made during certification.

USAir 427 and American 587 also illustrated how operational experience may indicate a need to reconsider assumptions made during certification. With regard to USAir 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 conducted by the FAA's Engineering Test and Evaluation Board in 2000 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 587 and in the National Aeronautics and Space Administration special study of in-flight upsets, indicated that the original assumptions about pilot use of rudder were perhaps not valid.

Society of Automotive Engineers (SAE) ARP5150, *Safety Assessment of Transport Airplanes in Commercial Service*,¹⁴ provides a process accepted by industry for ongoing assessment of safety-critical systems. The practice outlined in SAE ARP5150 describes guidelines, methods, and tools for conducting ongoing safety assessments. The process has five ongoing, iterative steps: establish safety-related parameters that are used to identify significant safety events and to assess the risks of those events (step 1); monitor the process for potential significant safety events based on the parameters established in step 1 (step 2); assess the event and risk (step 3); develop an action plan (step 4); and implement and evaluate the action plan (step 5). 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."¹⁵

The Safety Board believes that the ongoing safety assessment process outlined in SAE ARP5150 can provide the basis for continuous assessment of safety-critical systems throughout the life of a transport-category airplane. Properly implemented, the process will provide feedback mechanisms necessary to assess safety-critical systems in light of operational experience, lessons-learned, and new knowledge. In addition, such an ongoing safety assessment process can provide the basis for collecting service history and operational data that can be used to validate

¹⁴ *Safety Assessment of Transport Airplanes in Commercial Service* SAE ARP5150 (Warrendale, Pennsylvania: Society of Automotive Engineers, 2003).

¹⁵ SAE ARP5150, p. 4.

assumptions made during certification, operations, and maintenance, and for prompting timely and comprehensive reviews of potential airworthiness problems. If such an approach is in place when questions arise about service experience, a systematic evaluation and review of design features, certification procedures, and operational and maintenance practices can occur.

In addition, ongoing safety assessments could improve the FAA's ability to evaluate derivative designs. In both the USAir 427 and the Alaska 261 investigations, the Safety Board found that some issues raised during the original certification of the aircraft were not addressed during subsequent certification efforts. 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.

A key aspect of an ongoing safety assessment program is the involvement of all parties from the airplane's inception to its 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. However, fostering such relationships requires more than establishing lines of communication. Without a systematic approach that translates communication into action, any bridges built to link certification, operations, and maintenance will be inadequate.

The Safety Board concludes that 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 ARP5150 into 14 CFR 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 Safety Recommendation A-06-36. Once in place, the FAA should 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)

Therefore, as a result of the analysis provided in *Safety Report on the Treatment of Safety-Critical Systems in Transport Airplanes*, 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)

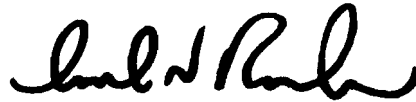
Amend the advisory materials associated with 14 *Code of Federal Regulations* 25.1309 to include consideration of structural failures and human/airplane system interaction failures in the assessment of safety-critical systems. (A-06-37)

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)

In your response to the recommendations in this letter, please refer to Safety Recommendations A-06-36 through A-06-38.

Acting Chairman ROSENKER and Members ENGLEMAN CONNORS, HERSMAN, and HIGGINS concurred in these recommendations.

A handwritten signature in black ink, appearing to read 'Mark V. Rosenker', written in a cursive style.

By: Mark V. Rosenker
Acting Chairman