NTSB National Transportation Safety Board

Office of Research and Engineering

Safety Report

Treatment of Safety-Critical Systems in Transport Airplanes

Airplane Certification Process

Applicant's Design

Type Certificate	• Review type design • Ensure Compliance • Establish instructions for continued airworthiness
Production Certificate	• Review manufacturing process • Ensure compliance with type design
Airworthiness Certificate	• Ensure each airplane in compliance with type design

Applicant's Certified Airplane

Genesis of the Certification Report

- USAir 427 Board Meeting (March 23-24, 1999)
- TWA 800 Board Meeting (August 22-23, 2000)
- Staff directed to “study” the issue

NTSB

Exploring an Accident Based Study

- Statistical review of certification related accidents
- 55 “certification” accidents, 1962 – 2001
- Required documentation of certification issues missing

NTSB

Exploring an Oversight Study

Considerations of scope & scale

- 250 FAA technical staff, plus many more company DERs
- Type certificate process for B-777 spanned 4 years (6,500 Boeing employees, 9 airplanes, 4,900 test flights, and more than 7,000 hours of flight time)
- Limited Safety Board resources

NTSB

Focus on the Process & Lessons Learned from Accident Experience

- Broad examination of the evolution of the FAA type certification process
- Consideration of other studies of certification issues
- Drawing lessons learned from NTSB investigation “case studies”

NTSB

Accident Case Studies

- **USAir Flight 427**
  - Accident occurred September 8, 1994
  - Final report adopted March 24, 1999
- **TWA Flight 800**
  - Accident occurred July 17, 1996
  - Final report adopted August 23, 2000
- **Alaska Airlines Flight 261**
  - Accident occurred January 31, 2000
  - Final report adopted December 30, 2002
- **American Airlines Flight 587**
  - Accident occurred November 12, 2001
  - Final report adopted October 26, 2004

NTSB

USAir Flight 427

September 8, 1994
Aliquippa, Pennsylvania

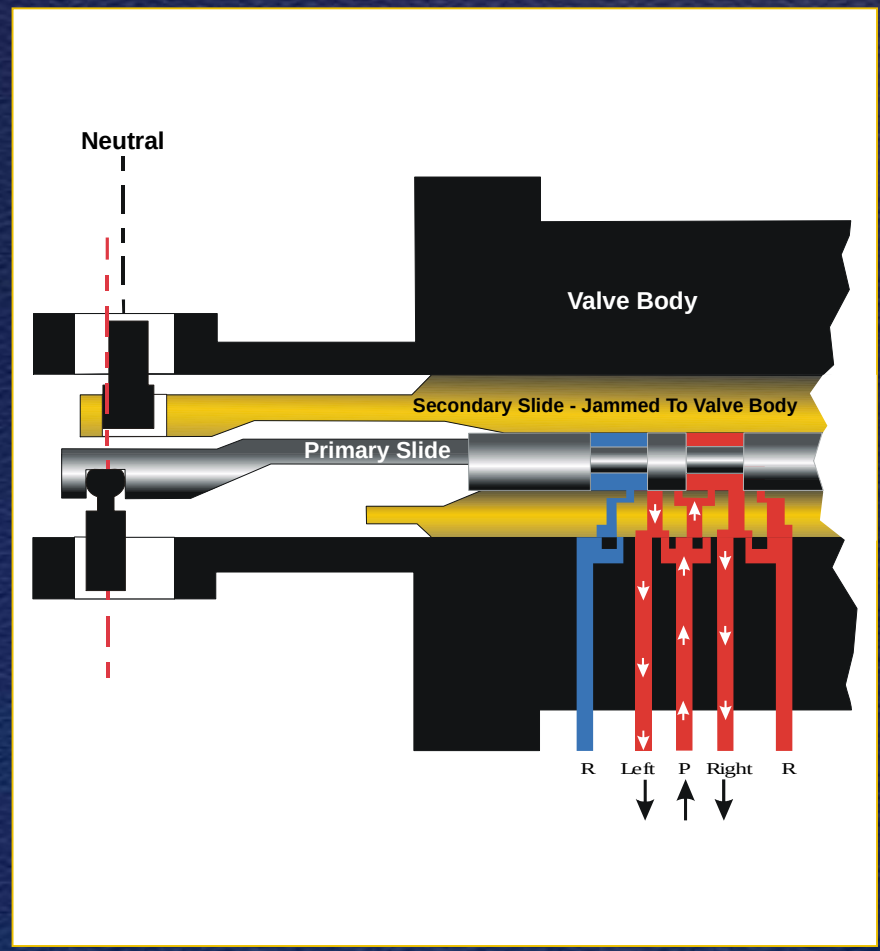
132 onboard, all fatal

Boeing 737-300

- Based on 1967 B737-100 type certificate
- Accident airplane placed in service October 1987

Safety-Critical System

- Main rudder power control unit (PCU) servo valve



NTSB

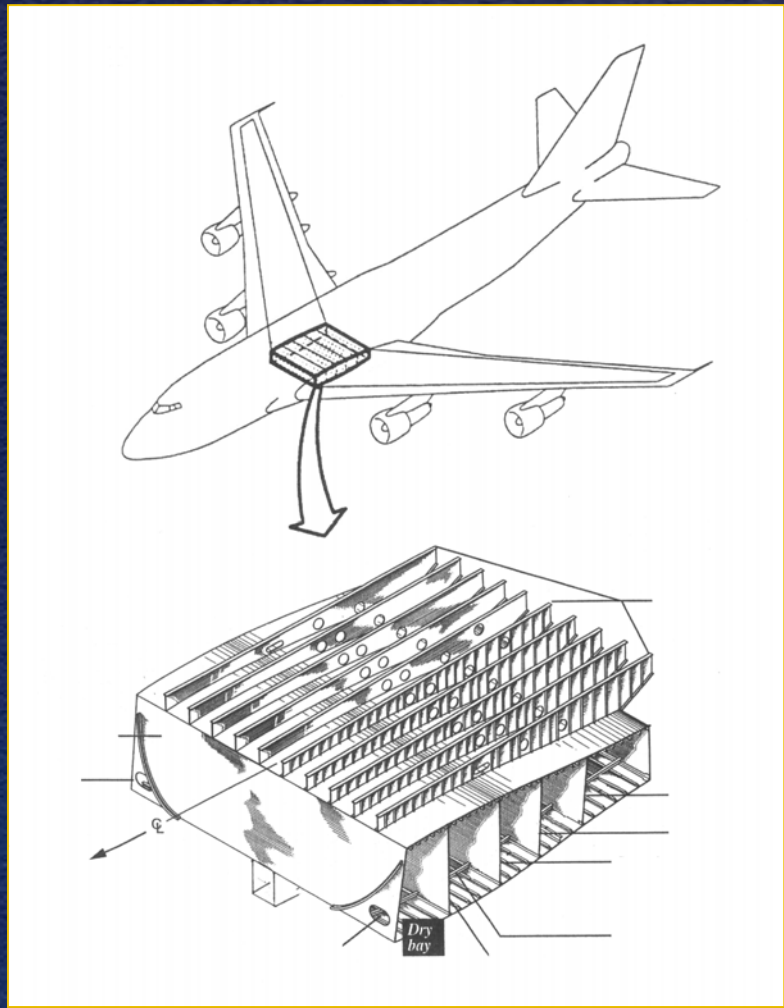
USAir Flight 427

- Certification Issues
  - Identification of failure modes
  - Use of lessons learned and operational data in safety assessments
  - Approval of derivative designs

NTSB

TWA Flight 800

- July 17, 1996, near East Moriches, New York
- 230 onboard, all fatal
- Boeing 747-131
  - Based on 1969 B747-100 type certificate
  - Accident airplane placed in service October 1971
- Safety-Critical System
  - Center wing fuel tank



NTSB

TWA Flight 800

- Certification Issues
  - Collection and use of comprehensive and reliable failure data
  - Reliance on a flawed design and certification philosophy that focused only on eliminating ignition sources

NTSB

Alaska Airlines Flight 261

- January 31, 2000, near Anacapa Island, California
- 88 onboard, all fatal
- McDonnel Douglas MD-83
  - Based on 1965 DC-9 type certificate
  - Accident airplane placed in service May 1992
- Safety-Critical System
  - Horizontal stabilizer trim system jackscrew assembly

NTSB

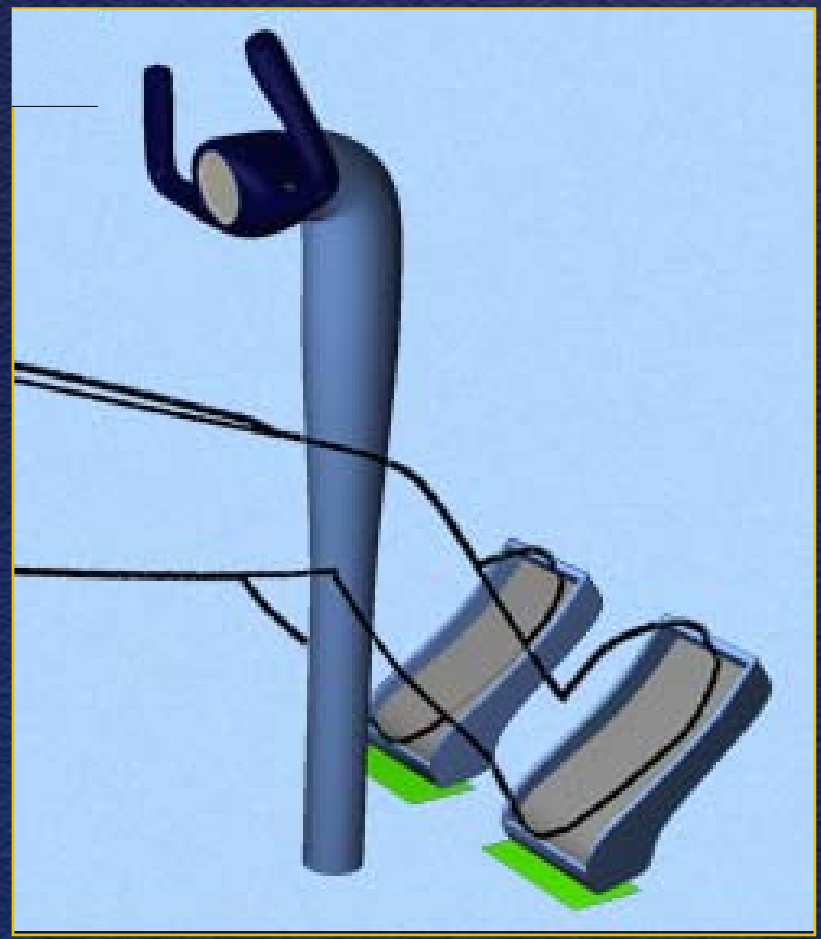
Alaska Airlines Flight 261

- Certification Issues
  - Design assumptions not considered in maintenance decisions
  - Need to monitor and analyze critical systems
  - Differential treatment of structures and systems

NTSB

American Airlines Flight 587

- November 12, 2001, Belle Harbor, New York
- 260 onboard, 5 on ground, all fatal
- Airbus Industrie A300-605R
  - Based on 1984 A-300 B2-1A type certificate
  - Accident airplane placed in service July 1998
- Safety-Critical System
  - Rudder control system



NTSB

American Airlines Flight 587

- Certification Issues
  - Deficient certification standards
  - Use of information about aircrew behavior
  - Use of accident/incident data, service history, and operational data

NTSB

NTSB National Transportation Safety Board

Type Certification Process

Applicable Federal Regulations

FAR	Area of Compliance
Part 21	Certification procedures
Part 25	Airworthiness standards for transport category airplanes
Parts 33, 34 & 36	Airworthiness standards for engines, noise, emissions

Applicant responsible for design engineering and analysis

Part 25 Subparts

A. General
B. Flight
C. Structure
D. Design and Construction
E. Powerplants
F. Equipment, Systems, and Installations
G. Operating Limitations and Information

Foreign Manufactured Airplanes

- FAA type certificate required for imported airplanes
- Governed by 14 CFR Part 21.29 and guidance provided in AC 21-23B
- Bilateral Agreement for Airworthiness
  - a government-to-government agreement
  - establishes procedures for accepting technical competence and regulatory capability of the aviation authority of the exporting country

NTSB

Safety-Critical Systems

- Governed by 14 CFR Part 25, Subpart F: Equipment, Systems & Installations
- No explicit list of safety-critical systems
- No definition of “safety critical”
- Criticality identified in safety assessments

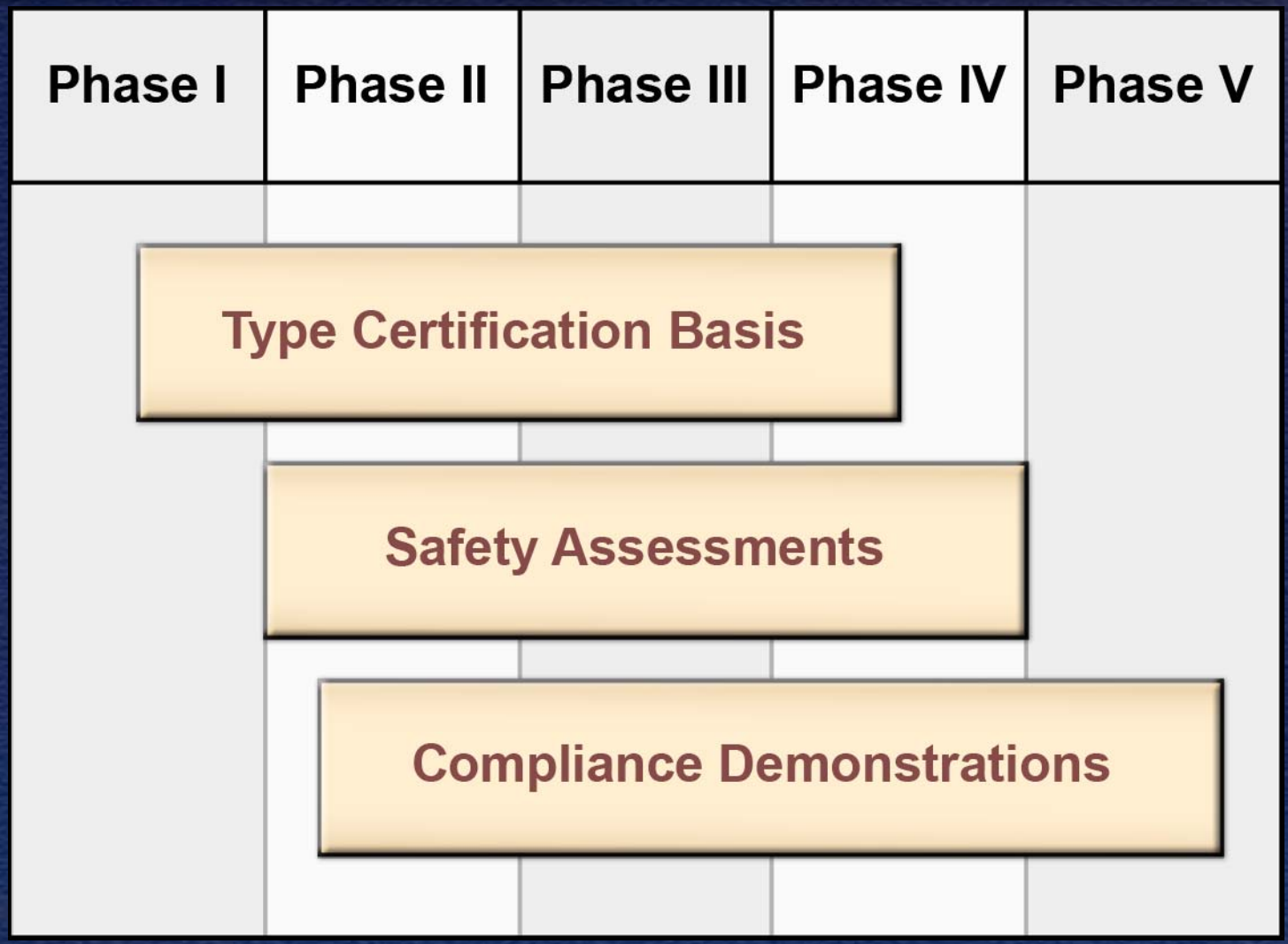
NTSB

Safety-Critical Systems

- Report definition
  - where a failure condition would prevent the safe flight of the airplane, or
  - reduce the capability of the airplane or the ability of the crew to cope with adverse operating conditions

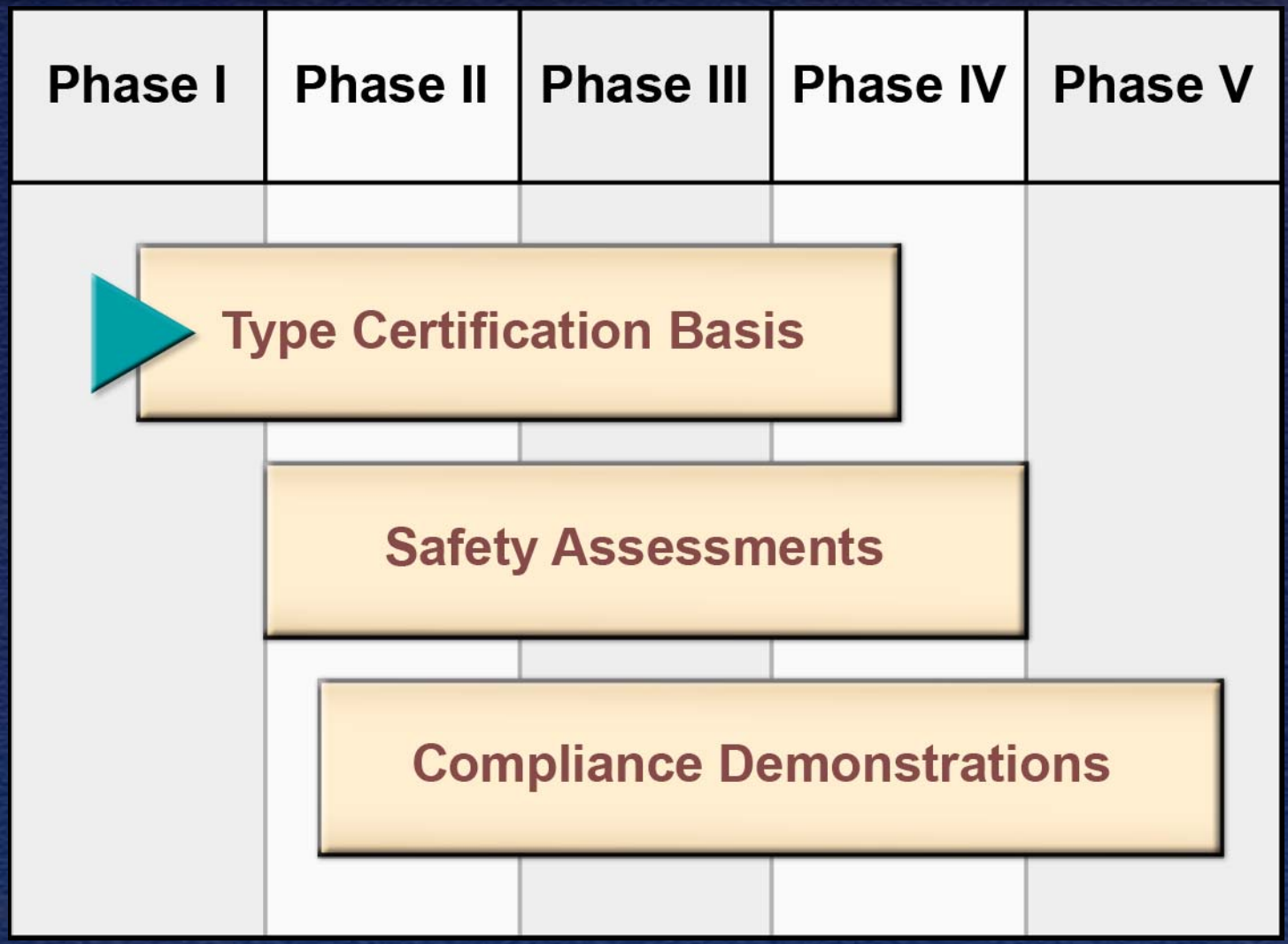
NTSB

Type Certification Activities



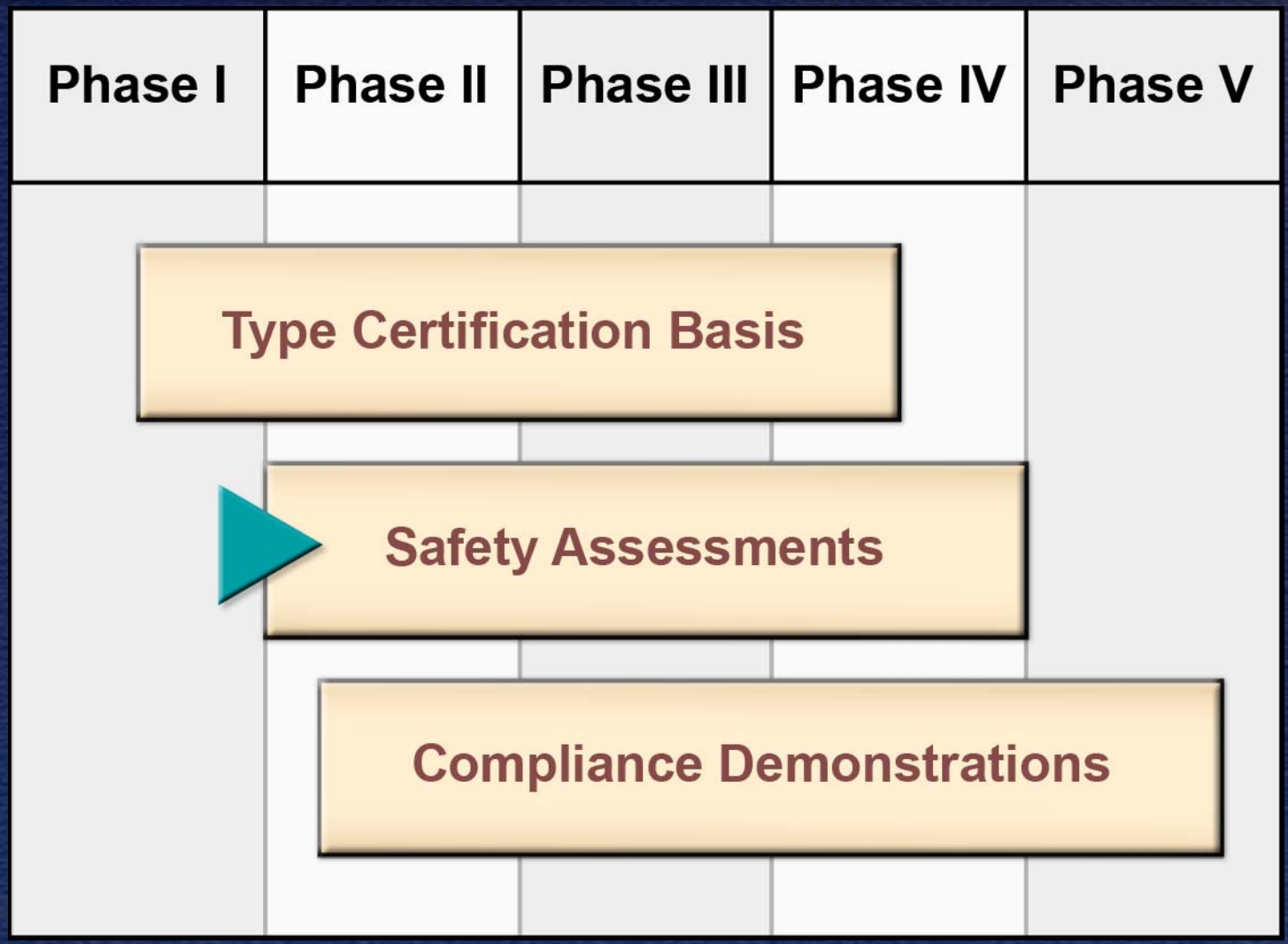
NTSB

Type Certification Activities



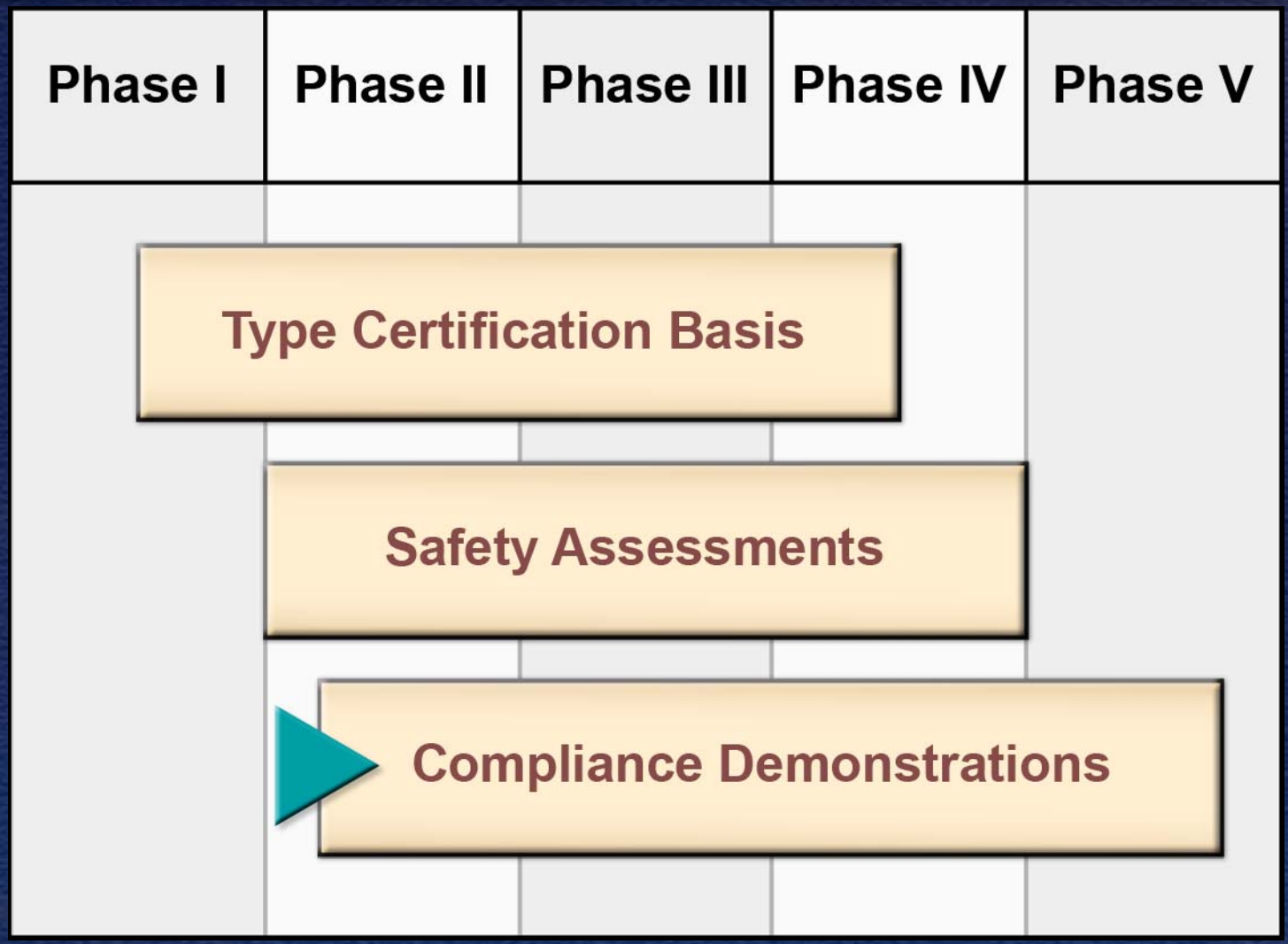
NTSB

Type Certification Activities



NTSB

Type Certification Activities



NTSB

Safety Assessments

Governed by 14 CFR 25.1309 and outlined in AC25.1309-1A

- Identify hazards and determine criticality
- Use formal risk analysis techniques
- Scope can be established by issue paper
- Identify safety-critical systems

NTSB

NTSB National Transportation Safety Board

Analysis of Certification Safety Issues

Certification Safety Issues

1. Identification and documentation of safety-critical systems
2. Enhancements to safety assessments
3. Ongoing assessment of safety-critical systems

NTSB

Safety Issue 1

- Identification and documentation of safety-critical systems
  - Safety assessments can identify safety-critical systems
  - Results not consistently documented
  - Ongoing assessments compromised

NTSB

Accident Case Study Support

- USAir Flight 427
  - ETEB discovery of multiple failure modes
- Alaska Airlines Flight 261
  - Changes to maintenance schedules without consideration of design assumptions

NTSB National Transportation Safety Board

Safety Issue 2

Enhancements to Safety Assessments

Safety Issue 2

- Enhancements to safety assessments
  - Including failures associated with structures
  - Including failures associated with human interaction with airplane systems

Safety Issue 2

- Including structural failures in safety assessments
  - No provision for considering effects of structural failures on systems
  - Different compliance methods
    - Specific design and test criteria for structures
    - Methods for assessing risk to systems

Accident Case Study Support

- Alaska Airlines Flight 261
  - Distinction between structures and systems
  - Structural components of jackscrew assembly not evaluated as part of system
  - Issued recommendations to consider structural failures in risk assessments of horizontal stabilizer trim systems

Safety Issue 2

- Including human/system interaction failures in safety assessments
  - Not explicitly considered
  - Human factors specified as standards or design criteria
  - Evaluation occurs late in process during ground and flight tests with experienced pilots

Other Agency Approaches

- Design and development explicitly consider human performance
- Evaluated in risk and hazard analyses
- Experience supports analysis of human performance in safety assessments

Accident Case Study Support

- American Airlines Flight 587
  - No criteria for rudder pedal sensitivity
  - Evidence of pilot use of rudder in upset recovery
  - Pilot perception of rudder pedal effects

NTSB National Transportation Safety Board

Safety Issue 3

Ongoing Safety Assessments

Safety Issue 3

- Ongoing safety assessments
  - Assess safety-critical systems in light of experience, lessons learned, and new knowledge
  - Conduct assessments throughout life of airplane
  - Require organizational coordination

Accident Case Study Support

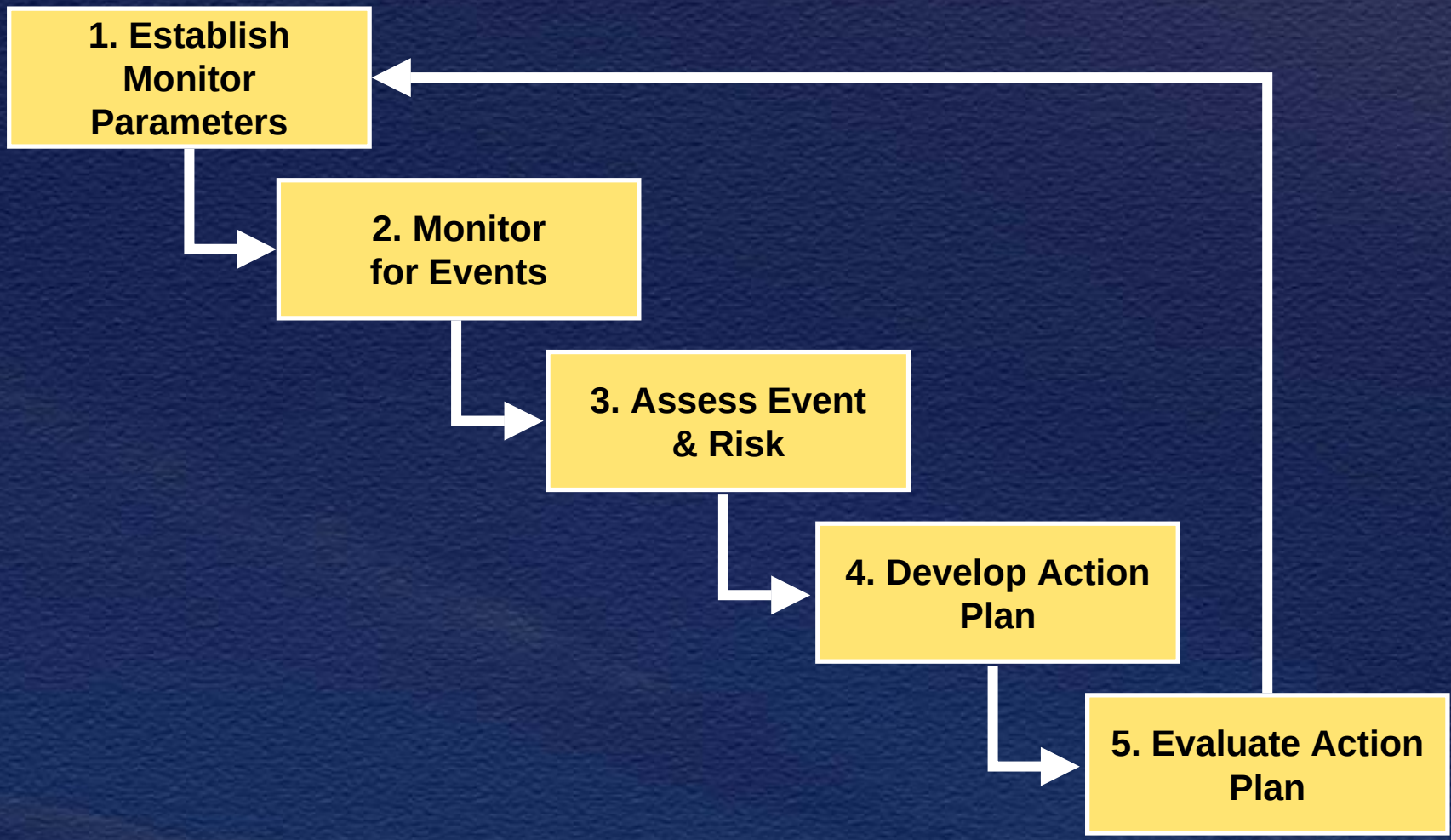
- USAir Flight 427
  - Service history supported FAA concerns
  - ETEB review identified new failure modes
- American Airlines Flight 587
  - Pilot use of rudder
- Alaska Airlines Flight 261
  - Changes made without sufficient data or analysis
- TWA Flight 800
  - Re-examine underlying design philosophy

Ongoing Assessment Process

SAE ARP5150, *Safety Assessment of Transport Airplanes in Commercial Service*

- Well established process
- Accepted by industry
- Established guidelines, methods, and tools for ongoing safety assessments

ARP5150 Five Step Process



Safety Issue 3: Ongoing Safety Assessments

NTSB

ARP5150 Benefits

- Provide feedback and coordination mechanisms
- Establish basis for collecting data to validate assumptions
- Prompt timely reviews
- Support ongoing assessment of safety-critical systems

NTSB