Certification and Avionics

Prof. R. John Hansman

MIT International Center for Air Transportation
Safety

- **Safety Targets/Standards**
  - Civil Air Carrier: FAR Part 25, FAR Part 121 (JAR)
  - Civil General Aviation: FAR Part 23, FAR Part 91
  - Military: Mil Spec

- **Safety Components**
  - Vehicle Airworthiness
  - Training and Operating Procedures
  - Maintenance
  - Culture
    - Quality Management Processes
    - Incident Reporting
    - Accident Investigation
  - Liability

- **Design Philosophy**
  - Fail Safe
  - Fail Operational
Accident Rates and Fatalities by Year
All Accidents - Worldwide Commercial Jet Fleet - 1959 through 2002

(Courtesy of Boeing Corporation. Used with permission.)
U.S.A. and Canadian Operators Accident Rates
Hull Loss and/or Fatal accidents - Worldwide Commercial Jet Fleet - 1959 through 2002

(Courtesy of Boeing Corporation. Used with permission.)
# Accidents by Primary Cause*

**Hull Loss - Worldwide Commercial Jet Fleet - 1993 through 2002**

<table>
<thead>
<tr>
<th>Cause</th>
<th>Count</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Flight Crew</td>
<td>93</td>
<td>67%</td>
</tr>
<tr>
<td>Airplane</td>
<td>17</td>
<td>12%</td>
</tr>
<tr>
<td>Weather</td>
<td>14</td>
<td>10%</td>
</tr>
<tr>
<td>Misc./Other</td>
<td>7</td>
<td>5%</td>
</tr>
<tr>
<td>Maintenance</td>
<td>4</td>
<td>3%</td>
</tr>
<tr>
<td>Airport/ATC</td>
<td>4</td>
<td>3%</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Category</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total with known causes</td>
<td>139</td>
</tr>
<tr>
<td>Unknown or awaiting reports</td>
<td>59</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td>198</td>
</tr>
</tbody>
</table>

*As determined by the investigating authority, percent of accidents with known causes.

(Courtesy of Boeing Corporation. Used with permission.)
Fatalities by Accident Category

Total Fatalities = 6,772 (6,461 onboard)
- 2002 fatalities = 702 (558 onboard)

- Loss of control in flight: 2131
- CFIT (controlled flight into terrain): 2007
- Mid-air collision: 420
- In-flight fire: 77
- Fuel tank explosion: 339
- Structure: 231
- Landing: 225
- Takeoff configuration: 192
- Runway incursion: 140
- Ice/snow: 121
- Wind shear: 81
- Fuel exhaustion: 37
- Misc. fatal: 29
- RTO (Refused Takeoff): 23
- Turbulence: 14
- Unknown: 149
- Total: 800

Note: Accidents involving multiple, non-onboard fatalities are included. Accidents involving single, non-onboard fatalities are excluded. Fatalities/accidents are placed in one category only.

(Courtesy of Boeing Corporation. Used with permission.)
Accidents and Onboard Fatalities by Phase of Flight
Hull Loss and/or Fatal Accidents - Worldwide Commercial Jet Fleet - 1993 - 2002

Percentage of accidents/fatalities

<table>
<thead>
<tr>
<th>Phase of Flight</th>
<th>Accidents</th>
<th>Fatalities</th>
</tr>
</thead>
<tbody>
<tr>
<td>Taxi, load, parked</td>
<td>5%</td>
<td>0%</td>
</tr>
<tr>
<td>Takeoff</td>
<td>11%</td>
<td>5%</td>
</tr>
<tr>
<td>Initial climb</td>
<td>16%</td>
<td>14%</td>
</tr>
<tr>
<td>Climb (flaps up)</td>
<td>8%</td>
<td>25%</td>
</tr>
<tr>
<td>Cruise</td>
<td>6%</td>
<td>9%</td>
</tr>
<tr>
<td>Descent</td>
<td>5%</td>
<td>14%</td>
</tr>
<tr>
<td>Initial approach</td>
<td>5%</td>
<td>13%</td>
</tr>
<tr>
<td>Final approach</td>
<td>7%</td>
<td>17%</td>
</tr>
<tr>
<td>Landing</td>
<td>47%</td>
<td>3%</td>
</tr>
</tbody>
</table>

Exposure = percentage of flight time based on flight duration of 1.5 hours

Distribution of accidents and fatalities

Hull loss and/or fatal accidents

- Taxi, load, parked: 12, 4
- Takeoff: 23, 302
- Initial climb: 12, 17
- Climb: 1,619
- Cruise: 14, 561
- Descent: 10, 910
- Initial approach: 12, 818
- Final approach: 16, 1,110
- Landing: 102, 185

(Courtesy of Boeing Corporation. Used with permission.)
### Accident Rates by Airplane Type

**Hull Loss Accidents - Worldwide Commercial Jet Fleet - 1959 through 2002**

<table>
<thead>
<tr>
<th>Airplane Type</th>
<th>Hull Losses</th>
<th>Rate Per Million Departures</th>
</tr>
</thead>
<tbody>
<tr>
<td>Not flying**</td>
<td>695</td>
<td>1.69</td>
</tr>
<tr>
<td>707/720</td>
<td>123</td>
<td>5.84</td>
</tr>
<tr>
<td>DC-8</td>
<td>73</td>
<td>1.09</td>
</tr>
<tr>
<td>727</td>
<td>81</td>
<td>1.29</td>
</tr>
<tr>
<td>737-100-200</td>
<td>69</td>
<td>1.26</td>
</tr>
<tr>
<td>DC-9</td>
<td>78</td>
<td>2.72</td>
</tr>
<tr>
<td>BAC 1-11</td>
<td>23</td>
<td>3.63</td>
</tr>
<tr>
<td>F-28</td>
<td>32</td>
<td>2.02</td>
</tr>
<tr>
<td>747-Early</td>
<td>24</td>
<td>1.56</td>
</tr>
<tr>
<td>DC-10</td>
<td>21</td>
<td>0.75</td>
</tr>
<tr>
<td>A300-Early</td>
<td>9</td>
<td>0.40</td>
</tr>
<tr>
<td>L-1011</td>
<td>4</td>
<td>0.40</td>
</tr>
<tr>
<td>MD-80-90</td>
<td>12</td>
<td>4.00</td>
</tr>
<tr>
<td>767</td>
<td>4</td>
<td>0.40</td>
</tr>
<tr>
<td>757</td>
<td>5</td>
<td>0.40</td>
</tr>
<tr>
<td>BAe146</td>
<td>3</td>
<td>0.62</td>
</tr>
<tr>
<td>A310</td>
<td>6</td>
<td>1.74</td>
</tr>
<tr>
<td>A300-800</td>
<td>4</td>
<td>1.28</td>
</tr>
<tr>
<td>737-300-400/500</td>
<td>16</td>
<td>0.37</td>
</tr>
<tr>
<td>A320/319/321</td>
<td>9</td>
<td>0.59</td>
</tr>
<tr>
<td>F-100</td>
<td>5</td>
<td>0.87</td>
</tr>
<tr>
<td>747-400</td>
<td>3</td>
<td>1.02</td>
</tr>
<tr>
<td>MD-11</td>
<td>5</td>
<td>1.19</td>
</tr>
<tr>
<td>RJ-70/85/100</td>
<td>2</td>
<td>4.11</td>
</tr>
<tr>
<td>A340</td>
<td>0</td>
<td>0.0</td>
</tr>
<tr>
<td>A330</td>
<td>0</td>
<td>0.0</td>
</tr>
<tr>
<td>777</td>
<td>0</td>
<td>0.0</td>
</tr>
<tr>
<td>737-600/700/800/900</td>
<td>0</td>
<td>0.0</td>
</tr>
<tr>
<td>717</td>
<td>0</td>
<td>0.0</td>
</tr>
<tr>
<td>F-70</td>
<td>0</td>
<td>0.0</td>
</tr>
</tbody>
</table>

(Courtesy of Boeing Corporation. Used with permission.)

**Hull Loss Accident Rate Per Million Departures**

**The Comet, CV880/990, Caravelle, Trident & VC-10 are no longer in commercial service, and are combined in the "Not Flying" bar.**

* These types have accumulated fewer than 1 million departures.
Accident Rates by Years Following Introduction
Hull Loss and/or Fatal accidents - Worldwide Commercial Jet Fleet - 1959 through 2002

(Courtesy of Boeing Corporation. Used with permission.)
Certification

- **Civil**
  - Certificate of Airworthiness (i.e. Certification)
    - Guarantee to the public that the aircraft is airworthy to some standard
  - Operational Approval
    - Operating Certificate
      - Equipment
      - Procedures
      - Training

- **Military**
  - Procurement

- **Space**
  - Man Rated
Certification

- Aircraft Certificate of Airworthiness
  - Standard Type Certificate (STC)
  - Categories
    - Air Carrier
    - Normal
    - Utility
    - Experimental
    - Rotorcraft
    - LTA
    - Others
Certification

• Component Certificate of Airworthiness
  - Engines
  - Propellers
  - Parts
  - Instruments

• Component (Parts & Instruments) Standards
  - Technical Service Order (TSO)
  - Minimum Operational Performance Specification (MOPS)

• Software Standards
  - RTCA DO-178B

• Continued Airworthiness
  - Inspections
  - Maintenance
• Airline Operating Certificate - Part 121
  □ Procedures
  □ Training
  □ Airports
  □ Aircraft
  □ Management
Federal Aviation Regulations

• Part 1 - DEFINITIONS AND ABBREVIATIONS
• Part 11 - GENERAL RULEMAKING PROCEDURES
• Part 21 - CERTIFICATION PROCEDURES FOR PRODUCTS AND PARTS
• Part 23 - AIRWORTHINESS STANDARDS: NORMAL, UTILITY, ACROBATIC, AND COMMUTER CATEGORY AIRPLANES
• Part 25 - AIRWORTHINESS STANDARDS: TRANSPORT CATEGORY AIRPLANES
• Part 27 - AIRWORTHINESS STANDARDS: NORMAL CATEGORY ROTORCRAFT
• Part 29 - AIRWORTHINESS STANDARDS: TRANSPORT CATEGORY ROTORCRAFT
• Part 31 - AIRWORTHINESS STANDARDS: MANNED FREE BALLOONS
• Part 33 - AIRWORTHINESS STANDARDS: AIRCRAFT ENGINES
• Part 34 - FUEL VENTING AND EXHAUST EMISSION REQUIREMENTS FOR TURBINE ENGINE POWERED AIRPLANES
• Part 35 - AIRWORTHINESS STANDARDS: PROPELLERS
• Part 36 - NOISE STANDARDS: AIRCRAFT TYPE AND AIRWORTHINESS CERTIFICATION

Description of the FAA Avionics Certification Process
This Diagram illustrates the TC or STC approval process.

1. **Idea for New Avionics Product is Born**
   - This is the appropriate time to initiate certification project.

2. **Product is Evaluated for Marketability and Certifiability**
   - Close consultation with FAA engineering personnel is essential throughout design process to avoid new requirements late in process.
   - FAA witnesses many of the system tests for certification.

3. **Company Makes Decision to Proceed with Development**
   - FAA witnesses all of the flight and ground tests conducted on aircraft for certification.

4. **Preliminary Design Completed**
   - FAA engineering personnel are sometimes consulted at this step.

5. **Detailed Design Completed**

6. **System Testing Completed**

7. **Installation in Aircraft and Certification Testing Completed**

8. **FAA ACO Issues Certificate and System is Ready for Operational Approval**

9. **Certification Plan is Prepared and Submitted to the ACO for Review and Approval**
   - Plan will Address the System Safety Assessment and the Software Aspects of Certification.

10. **Testing Plans and System Safety Assessment Prepared and Submitted to the ACO for Review and Approval**

11. **Flight Test Plan and Balance of Design approval Documents Submitted to ACO for Review and Approval**
• Advisory Circular AC 25.1309-1A
  □ System Design and Analysis
• Fail Safe
• Fail Operational
• Preliminary Hazard Analysis
• Functional Hazard Assessment
• Depth of Analysis Flowchart
  □ Complex System
### Probability vs. Consequences

<table>
<thead>
<tr>
<th></th>
<th>Probable</th>
<th>Improbable</th>
<th>Extremely Improbable</th>
</tr>
</thead>
<tbody>
<tr>
<td>Catastrophic Accident</td>
<td>Red</td>
<td>Red</td>
<td>Yellow</td>
</tr>
<tr>
<td>Adverse Effect On Occupants</td>
<td>Yellow</td>
<td>Yellow</td>
<td>Green</td>
</tr>
<tr>
<td>Airplane Damage</td>
<td>Green</td>
<td>Green</td>
<td>Green</td>
</tr>
<tr>
<td>Emergency Procedures</td>
<td>Yellow</td>
<td>Yellow</td>
<td>Green</td>
</tr>
<tr>
<td>Abnormal Procedures</td>
<td>Yellow</td>
<td>Yellow</td>
<td>Green</td>
</tr>
<tr>
<td>Nuisance</td>
<td>Green</td>
<td>Green</td>
<td>Green</td>
</tr>
<tr>
<td>Normal</td>
<td>Green</td>
<td>Green</td>
<td>Green</td>
</tr>
</tbody>
</table>
## Descriptive Probabilities

<table>
<thead>
<tr>
<th>Probability (per unit of exposure)</th>
<th>FAR</th>
<th>JAR</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Probable</td>
<td>Frequent</td>
</tr>
<tr>
<td>10E-3</td>
<td></td>
<td>Reasonably Probable</td>
</tr>
<tr>
<td>10E-5</td>
<td>Improbable</td>
<td>Remote</td>
</tr>
<tr>
<td>10E-7</td>
<td></td>
<td>Extremely Remote</td>
</tr>
<tr>
<td>10E-9</td>
<td>Extremely Improbable</td>
<td>Extremely Improbable</td>
</tr>
</tbody>
</table>

What is the correct unit of exposure: Flight hour, Departure, Failure
Safety Analysis

• Preliminary Hazard Analysis

• Fault Tree Analysis
  □ Top Down Search - Presumes Hazards Known
  □ System Definition
  □ Fault Tree Construction
  □ Qualitative Analysis
  □ Quantitative Analysis

• Event Tree Analysis
  □ Bottom Up “Forward” Search - Identifies possible outcomes

• Failure Modes and Effects Analysis
  □ Probabilistic “Forward” Search
  □ Requires Failure Probability Estimates
  □ Requires Assumed Failures from PHA or Historical Data
  □ “Target Level of Safety”
Event Tree Example
From: Leveson

A reduced event tree for a loss of coolant accident.

Fault Tree and Event Tree Examples From: Leveson

FMEA for a system of two amplifiers in parallel.

<table>
<thead>
<tr>
<th>Critical</th>
<th>Failure probability</th>
<th>Failure mode</th>
<th>% Failure by mode</th>
<th>Effects</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>$1 \times 10^{-3}$</td>
<td>Open</td>
<td>90</td>
<td>Critical $5 \times 10^{-5}$ Noncritical $x$</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Short</td>
<td>5</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Other</td>
<td>5</td>
<td></td>
</tr>
<tr>
<td>B</td>
<td>$1 \times 10^{-3}$</td>
<td>Open</td>
<td>90</td>
<td>Critical $5 \times 10^{-5}$ Noncritical $x$</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Short</td>
<td>5</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Other</td>
<td>5</td>
<td></td>
</tr>
</tbody>
</table>

Reliability Architectures

• Analysis Values often of Questionable Integrity

• Drives Failure Mitigation Approaches

• Avoid Single String Failure
  □ Cannot guarantee 10E-9

• Redundancy
  □ Dual Redundant for Passive Failures
    • e.g. Wing Spar
  □ Triple Redundancy for Active Systems
    • 777 Fly By Wire
      ↓ Sensors
      ↓ Processors
      ↓ Actuators
      ↓ Data Bus
    • A320 Reliability Architecture by Comparison
• Flight Control computers are dual channel
  – one for control and one for monitoring
• Each processor has a different vendor for hardware & software
  – software for each processor coded in a different language
FBW - A330/A340 flight control architecture

Computer / hydraulic actuator arrangement

Grnd spoilers, speedbrake
Roll control surfaces

Spoilers

Ailerons

S1 P1 P2 S2 P3 P3

P3 S1 P1 P2 S1 S2

S1 S2

Rudder

TLU

Yaw damper

* Rudder pedals

* Trim Wheels

Grnd spoilers, speedbrake
Roll control surfaces

Spoilers

Ailerons

P1 P2 S2 P3

S1 S2

P1 P2 S2 P3

Elevator

Elevator

S1 P1 P2 S1 S2

P2 P1 S2 S1

P1 P2
Additional Issues

- Conventional vs. New Technologies/Configurations
- Problem with Software and Complex Systems
- Emergent Behavior
- Air-Ground Coupling Issues
FAA 8040.4 Safety Analysis Process

Plan → ID Hazards → Analysis → Risk Assessment → Decision
Operational Reliability

- **MTBF**
  - Mean Time Between Failure

- **MTBUR**
  - Mean Time Between Unscheduled Replacement

- **Dispatch Reliability**
  - Conditional Airworthiness
  - Minimum Equipment List

- Relates to Life Cycle Costs
Maintenance

- Scheduled Maintenance
  - Periodic (e.g. Annual)
  - On Time (Time Between Overhaul) (TBO)
  - Progressive (Inspection Based e.g. Cracks)
  - Conditional (Monitoring Based e.g. Engines - ACARS)
  - Heavy Maintenance Checks

- Unscheduled
  - “Squawks” = Reported Anomalies
    - Logbook Entries (ACARS)
  - Line Replacement Units (LRU)
  - Airworthiness Directives, Service Difficulty Reports

- Parts Inventory
  - Parts Tracking
  - Commonality
    - Glass Cockpits
    - F16 Tail
What are the Key Technologies for Formation Flight

- Communications
- Navigation
- Surveillance
- Control (Station Keeping)
  - Intent States
  - String Stability
- Vehicle Configuration
  - Aero/Performance
  - Control
- Propulsion
- Degree of Autonomy
- Flight Criticality
  - Hardware
  - Software
- Low Observability
- Others?
Avionics Components

- Black Box (LRU)
- Power (440 AC or 28V DC)
- Cooling
- Databus (AIRINC 429, 629, IEEE486,...)
  - Databus Interface
- Antenna and or Sensors
- Display Head
  - MFD
  - Dedicated Display
Air Data

- Barometric Altitude
- Airspeed
- Mach Number
- Vertical Speed
- Total Air Temperature (TAT)
- Static Air Temperature (SAT)
- Angle of Attack ($\alpha$)
- Angle of Sideslip ($\beta$)
HEAD-UP DISPLAY

- Roll Scale
- Wind Vector
- Reference Symbol
- Horizon and Heading Scale
- Barometric Altitude
- Airspeed
- Ground Speed
- Pitch Scale
- Flight Path Acceleration
- Vertical Speed
- Flight Path Vector
- Speed Error Tape