Safety, Reliability, Certification, Maintenance

Prof. R. John Hansman

MIT International Center for Air Transportation
Accident Rates and Fatalities by Year

- Hull loss and/or fatal accidents
- All accidents
- Onboard fatalities

Accident rate (accidents per million departures)

Year

1959 61 63 65 67 69 71 73 75 77 79 81 83 85 87 89 91 93 95 97 99 2001

Fatalities
U.S. Military Accident Rates

Accident Rate

#Class A accidents per 100,000 flight hours

Figure by MIT OCW. Adapted from: Aviation Week 10/02.
Accident Rates by Airplane Type


**The Comet, CV-880/-990, Caravelle, Mercure, 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.*
Accidents by Primary Cause*

<table>
<thead>
<tr>
<th>Category</th>
<th>Count</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Flight crew</td>
<td>98</td>
<td>66%</td>
</tr>
<tr>
<td>Airplane</td>
<td>21</td>
<td>14%</td>
</tr>
<tr>
<td>Weather</td>
<td>14</td>
<td>10%</td>
</tr>
<tr>
<td>Misc./Other</td>
<td>8</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>
<tr>
<td>Total with known causes</td>
<td>149</td>
<td></td>
</tr>
<tr>
<td>Unknown or awaiting reports</td>
<td>61</td>
<td></td>
</tr>
<tr>
<td>Total</td>
<td>210</td>
<td></td>
</tr>
</tbody>
</table>

*As determined by the investigative authority.
Fatalities by Accident Categories


Total fatalities = 6,922 (6,715 onboard)
2001 fatalities = 417 (399 onboard)

Number of fatal accidents
112 Total

Note: Accidents involving multiple non-onboard fatalities are included. Accidents involving single, non-onboard fatalities are excluded.

* CFIT  Controlled flight into terrain
** RTO  Refused takeoff
Hostile Actions

Sabotage/Terrorist rate per million departures

Number of events

Number of fatalities (onboard only)
Accidents and Onboard Fatalities by Phase of Flight
Hull Loss and/or Fatal Accidents — Worldwide Commercial Jet Fleet — 1992 through 2001

Percentage of accidents/fatalities

- **Accidents**
  - Taxi, load, parked: 6%
  - Takeoff: 12%
  - Initial climb: 5%
  - Climb (flaps up): 9%
  - Cruise: 6%
  - Descent: 5%
  - Initial approach: 5%
  - Final approach: 8%
  - Landing: 46%

- **Fatalities**
  - Taxi, load, parked: 0
  - Takeoff: 6%
  - Initial climb: 13%
  - Climb (flaps up): 24%
  - Cruise: 6%
  - Descent: 16%
  - Initial approach: 14%
  - Final approach: 19%
  - Landing: 3%

**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: 14
  - Takeoff: 27
  - Initial climb: 847
  - Climb: 1,627
  - Cruise: 13
  - Descent: 11
  - Initial approach: 12
  - Final approach: 18
  - Landing: 219

- Onboard fatalities:
  - Taxi, load, parked: 4
  - Takeoff: 318
  - Initial climb: 954
  - Climb: 2,252
  - Cruise: 107
  - Descent: 11
  - Initial approach: 12
  - Final approach: 18
  - Landing: 219

**Note:** Hull loss and/or fatal accidents vs. Onboard fatalities.
Accident Rates by Years Following Introduction

Accident rate (accidents per million departures)

Years since introduction
Safety

- **Safety Targets/Standards**
  - Civil Air Carrier: FAR Part 25, FAR Part 121
  - 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
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
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
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 ENGINEPOWERED AIRPLANES
- Part 35 - AIRWORTHINESS STANDARDS: PROPELLERS
- Part 36 - NOISE STANDARDS: AIRCRAFT TYPE AND AIRWORTHINESS CERTIFICATION

- [http://www.faa.gov/regulations_policies/](http://www.faa.gov/regulations_policies/)
Idea for new avionics product is born

Product is evaluated for marketability & certifiability

FAA engineering personnel are sometimes consulted at this step

Company makes decision to proceed with development

This is the appropriate time to initiate certification project

Close consultation with FAA engineering personnel is essential throughout design process to avoid new requirements late in process

FAA witnesses many of the systems tests for certification

FAA witnesses all of the flight and ground tests conducted on an aircraft for certification

Certification plan is prepared & submitted to the ACO for review & approval. Plan will address the system safety assessment & the software aspects of certification

Testing plans & system safety assessment prepared & submitted to the ACO for review & approval

Flight test plan & balance of design approval documents submitted to ACO for review & approval

Preliminary design completed

Detailed design completed

System testing completed

Installation in aircraft & certification testing completed

FAA ACO issues certificate & system is ready for operational approval

TC or STC Approval Process

Figure by MIT OCW.
Safety Analysis

- 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 Graph

<table>
<thead>
<tr>
<th></th>
<th>Probable</th>
<th>Improbable</th>
<th>Extremely Improbable</th>
</tr>
</thead>
<tbody>
<tr>
<td><em>Catastrophic Accident</em></td>
<td>Red</td>
<td>Red</td>
<td>Yellow</td>
</tr>
<tr>
<td><em>Adverse Effect On Occupants</em></td>
<td>Red</td>
<td>Yellow</td>
<td>Yellow</td>
</tr>
<tr>
<td><em>Airplane Damage</em></td>
<td>Red</td>
<td>Yellow</td>
<td>Green</td>
</tr>
<tr>
<td><em>Emergency Procedures</em></td>
<td>Yellow</td>
<td>Green</td>
<td>Green</td>
</tr>
<tr>
<td><em>Abnormal Procedures</em></td>
<td>Yellow</td>
<td>Green</td>
<td>Green</td>
</tr>
<tr>
<td><em>Nuisance</em></td>
<td>Green</td>
<td>Green</td>
<td>Green</td>
</tr>
<tr>
<td><em>Normal</em></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>Frequent</td>
<td>Reasonably Probable</td>
</tr>
<tr>
<td>10E-3</td>
<td>Probable</td>
<td>Remote</td>
</tr>
<tr>
<td>10E-5</td>
<td>Improbable</td>
<td>Extremely Remote</td>
</tr>
<tr>
<td>10E-7</td>
<td>Extremely Improbable</td>
<td>Extremely Improbable</td>
</tr>
<tr>
<td>10E-9</td>
<td>Extremally 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”
A Reduced Event Tree for A Loss of Coolant Accident

1. Pipe Break
2. Electric Power
3. ECCS
4. Fission Product Removal
5. Containment Integrity

Initiating Event: P1

- Fails P2
  - Fails P4
    - Fails P5

- Available 1-P2
  - Succeeds 1-P3
    - Succeeds 1-P4
      - Fails P5
    - Fails P5

- Succeeds 1-P4
  - Succeeds 1-P5
    - Fails P5
  - Fails P5

Figure by MIT OCW.
Fault Tree and Event Tree Examples
From: Leveson

A Fault Tree and Event Tree Comparison

- Pressure too high
- Relief Valve 1 opens
- Pressure decreases
- Relief Valve 2 opens
- Pressure decreases
- Explosion

- Relief valve 1 does not open
- Relief valve 2 does not open
- Valve failure
- Operator inattentive
- Computer does not open valve 1
- Operator does not know to open value 2
- Pressure monitor failure
- Computer output too late
- Computer does not issue command to open valve 1
- Value 1 position indicator falls on
- Open indicator light falls on

Figure by MIT OCW.
## Failure Modes and Effects Analysis

### FMEA for a System of Two Amplifiers in Parallel

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

Figure by MIT OCW. Adapted from: Leveson.
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
A330 A340
Fly-by-wire - control surfaces

Electrically controlled, hydraulically actuated

Spoilers

*Rudders
Elevators
*Horizontal stabilizer
Ailerons

Identical for the A340
*Rudder & Horizontal stabilizer have back-up mechanical control
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

Grd spoilers, speedbrake
Roll control surfaces

Ailerons
Spoilers

S1 P1 P2 S2 P3 P3

Rudder

Slats

Flaps

* Trim Wheels

Yaw damper

* Rudder pedals

Trim

Elevator

THS

* Trim Wheels

Elevator

TLU
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)
  - Parts Inventory
    - F16 Tail
    - Glass Cockpits
Logbook Entries

- Pilot: Test flight OK, except autoland very rough.
- Mechanic: Autoland not installed on this aircraft.
- Pilot: No. 2 propeller seeping prop fluid.
- Mechanic: No. 2 propeller seepage normal. Nos. 1, 3 and 4 propellers lack normal seepage.
- Pilot: Something loose in cockpit.
- Mechanic: Something tightened in cockpit.
- Pilot: Autopilot in altitude-hold mode produces a 200-fpm descent.
- Mechanic: Cannot reproduce problem on ground.
- Pilot: DME volume unbelievably loud.
- Mechanic: DME volume set to more believable level.
- Pilot: Friction locks cause throttle levers to stick.
- Mechanic: That's what they're there for!
- Pilot: IFF inoperative.
- Mechanic: IFF always inoperative in OFF mode.
- Pilot: Suspected crack in windscreen.
- Mechanic: Suspect you're right.
- Pilot: Number 3 engine missing.
- Mechanic: Engine found on right wing after brief search.
- Pilot: Aircraft handles funny.
- Mechanic: Aircraft warned to straighten up, fly right, and be serious.
Typical Check Cycles

- **Ramp-check** before every flight

- **A-check** is done every 350-650 hours and includes more detailed check of electronics and systems as well as a cabin/haul check

- **B-check** is done every 5 months (1000 hours) and is basically an extended A-check.

- **C-check** is a detailed inspection of the aircraft’s structure as well as systems carried out every 8-18 months according to cycles/flying time etc.

- **IL-check** is made every 48 months and includes detailed inspection and service of structure, wings etc. as well as very extensive tests and service carried out on electronics, hydraulics etc. Recommended improvements are also done.

- **D-check** is almost a total dismantle and rebuilding of the aircraft. Almost every part is checked. D-check is made every 72 months.
Airworthiness Directives

- **Airworthiness Directives**
  - Based on identified hazards
  - Time to compliance

- **Service Bulletins**
Servicing

- Fueling
- Loading
  - Payload
  - Stores
- Servicing
  - Food
  - Water
  - Oxygen
  - Oil
  - Hydraulics
  - Air
- Cleaning
- Arming
Transition training / CCQ

100%

25 days

9 days

8 days

8 days

3 days

1 day

Full Transition Training

A320 to A340

A320 to A330

A330/A340 to A320

A330 to A340

A340 to A330