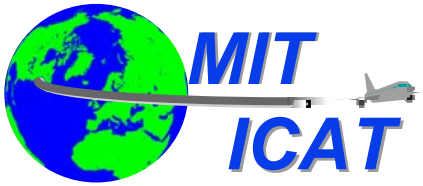
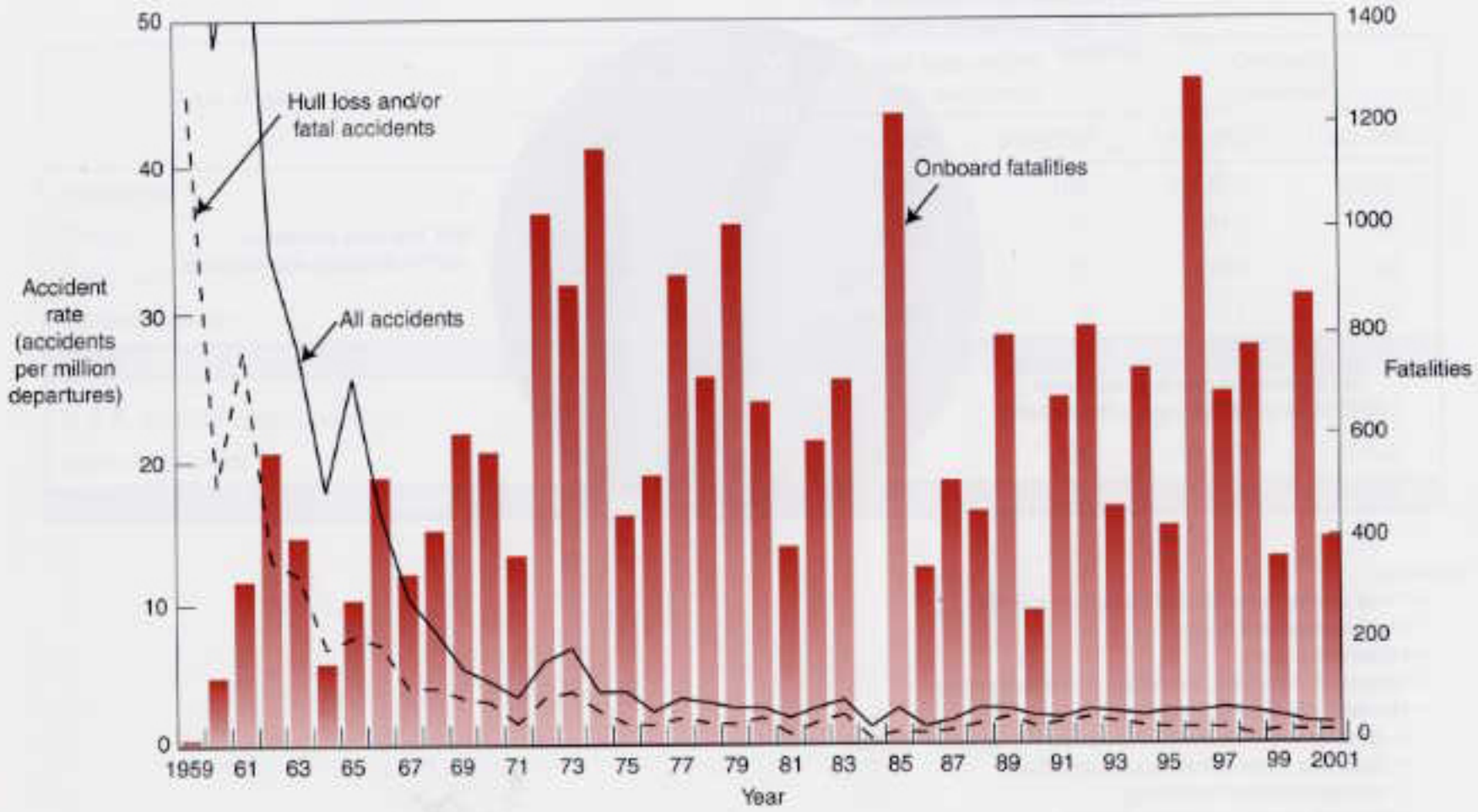


Safety, Reliability, Certification, Maintenance

Prof. R. John Hansman
MIT International Center for Air Transportation

Accident Rates and Fatalities by Year

Worldwide Commercial Jet Fleet — 1959 Through 2001



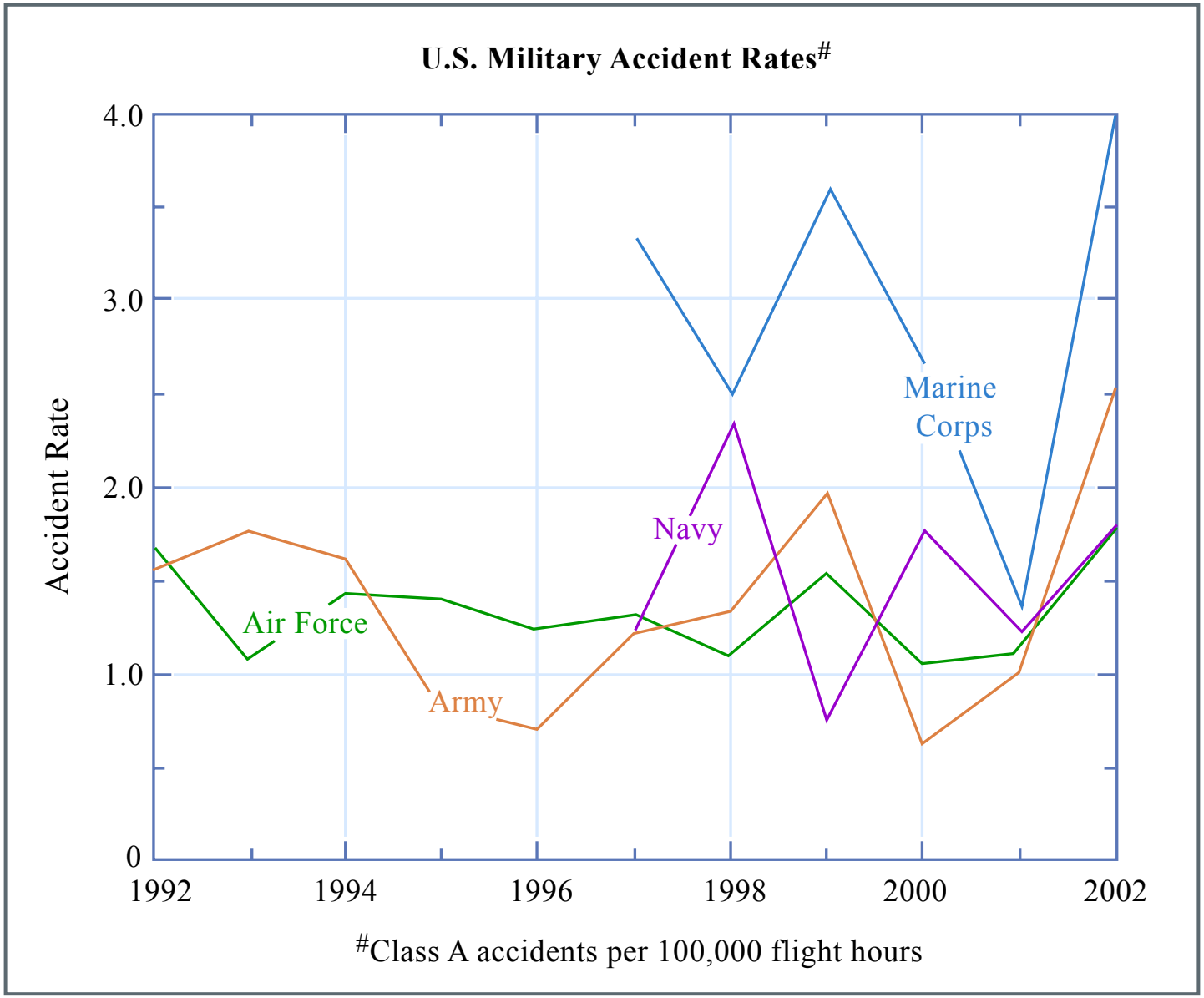
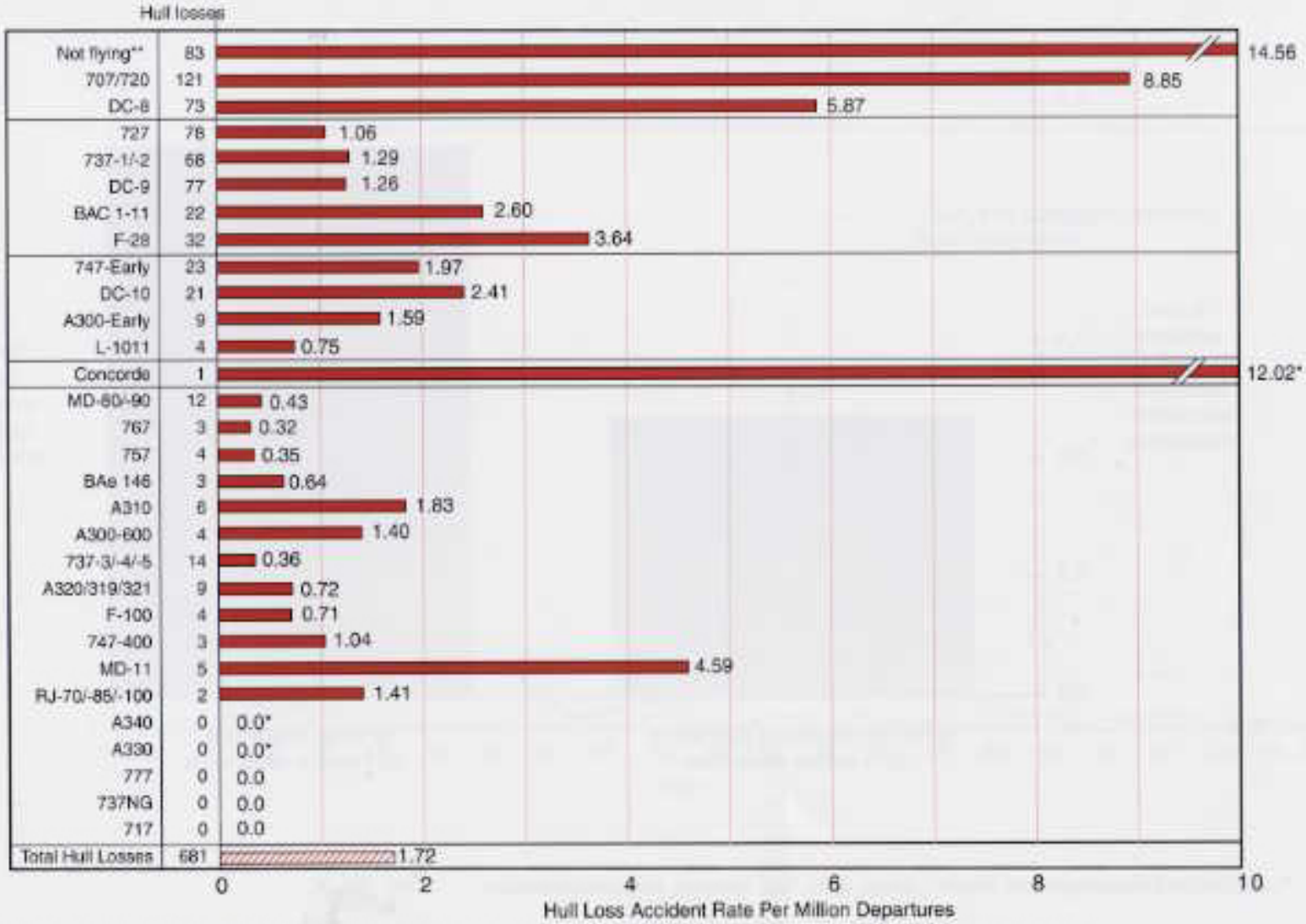


Figure by MIT OCW. Adapted from: Aviation Week 10/02.

Accident Rates by Airplane Type

Hull Loss Accidents — Worldwide Commercial Jet Fleet — 1959 Through 2001



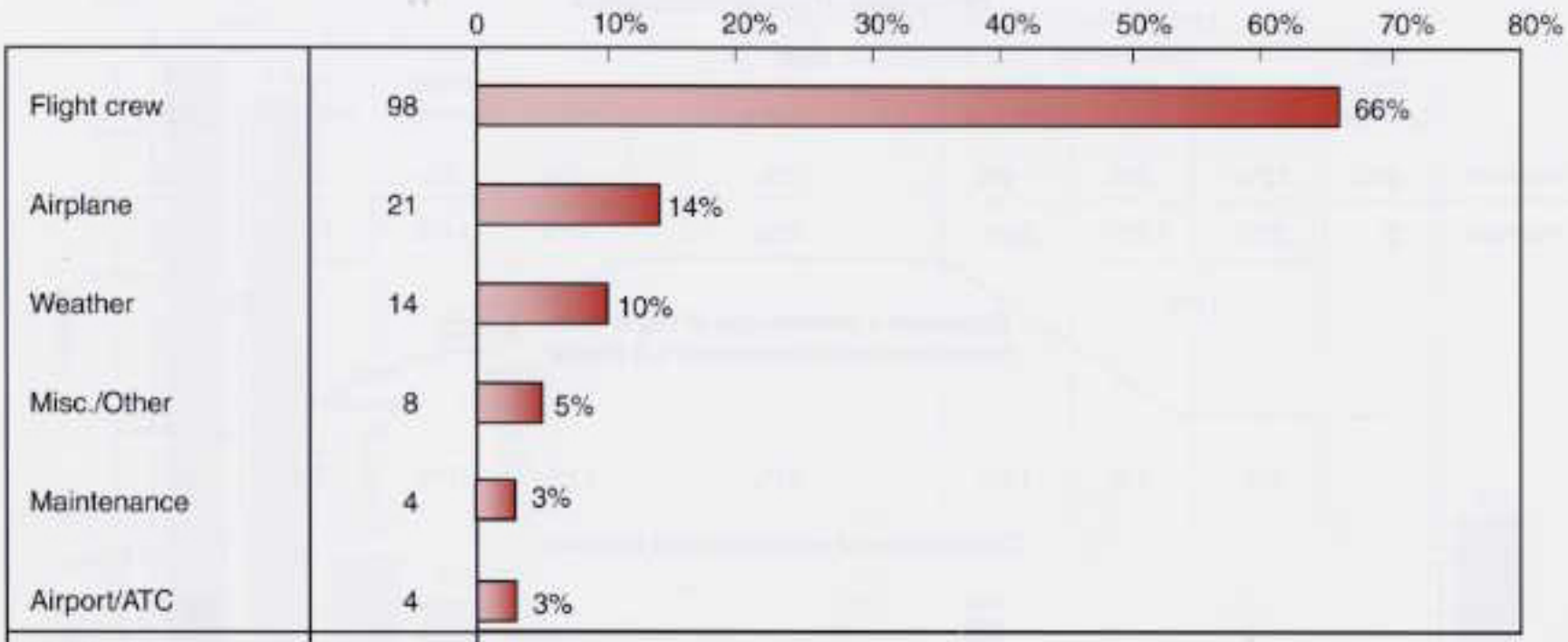
** The Comet, CV-880/-990, Caravelle, Mercure, Trident & VC-10 are no longer in commercial service, and are combined in the "Not Flying" bar.

* These types have accumulated fewer than 1 million departures.

BOEING

Accidents by Primary Cause*

Hull Loss Accidents — Worldwide Commercial Jet Fleet — 1992 Through 2001

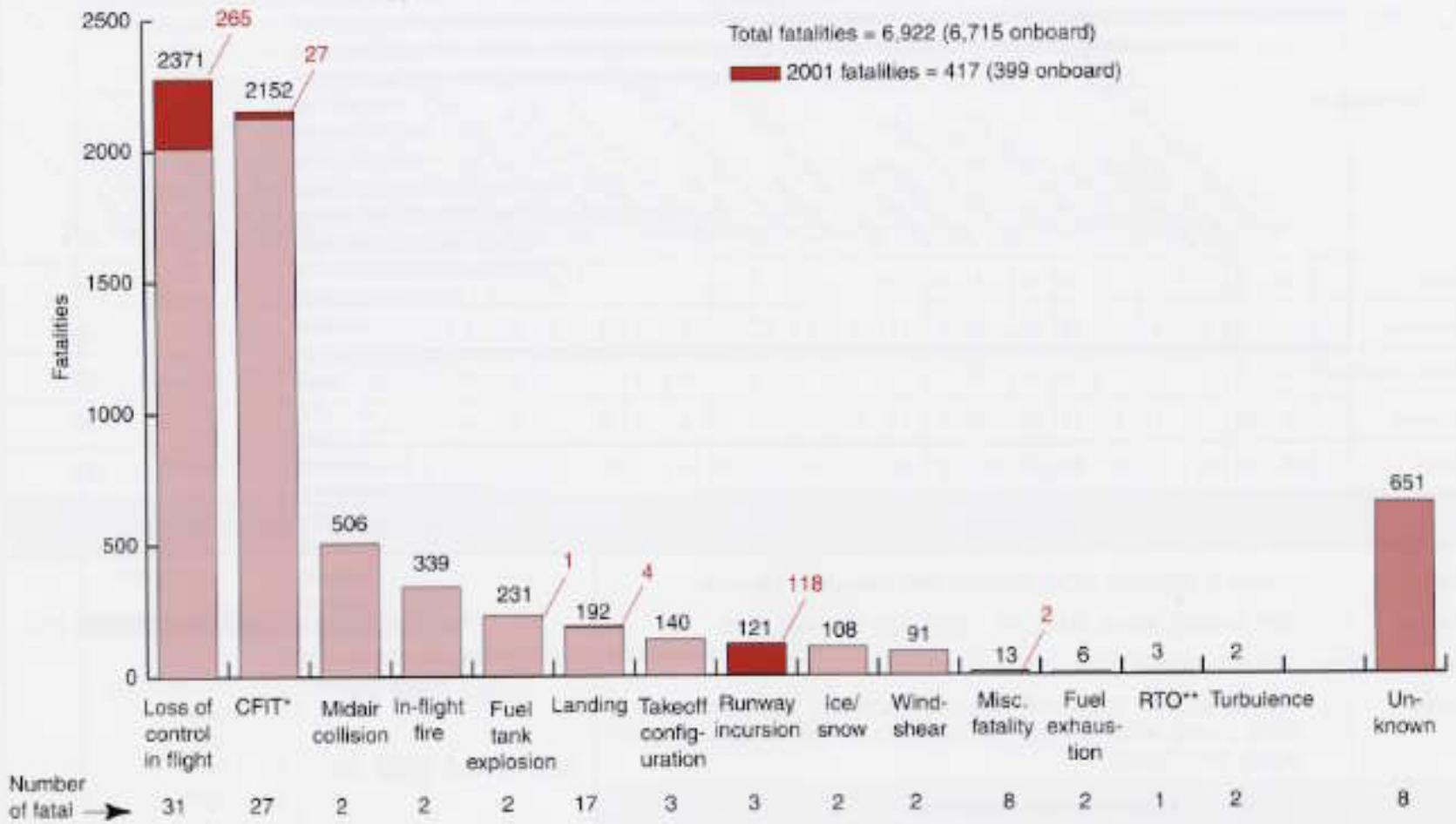


Flight crew	98
Airplane	21
Weather	14
Misc./Other	8
Maintenance	4
Airport/ATC	4
Total with known causes	149
Unknown or awaiting reports	61
Total	210

*As determined by the investigative authority.

Fatalities by Accident Categories

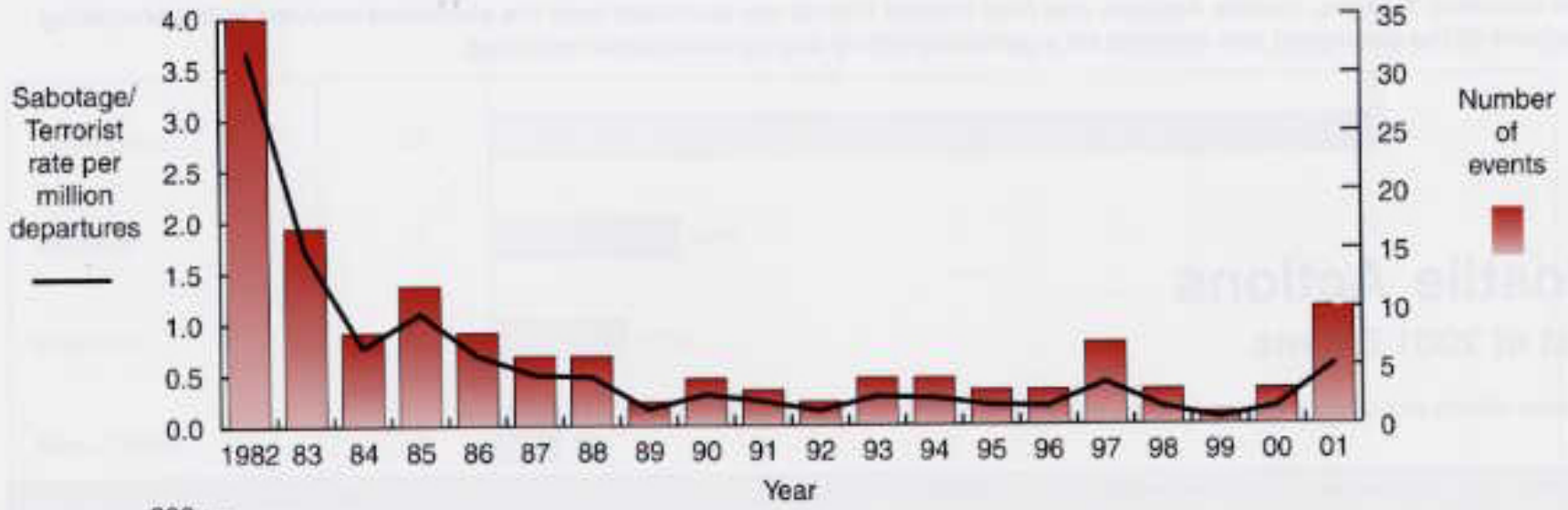
Fatal Accidents — Worldwide Commercial Jet Fleet — 1992 Through 2001

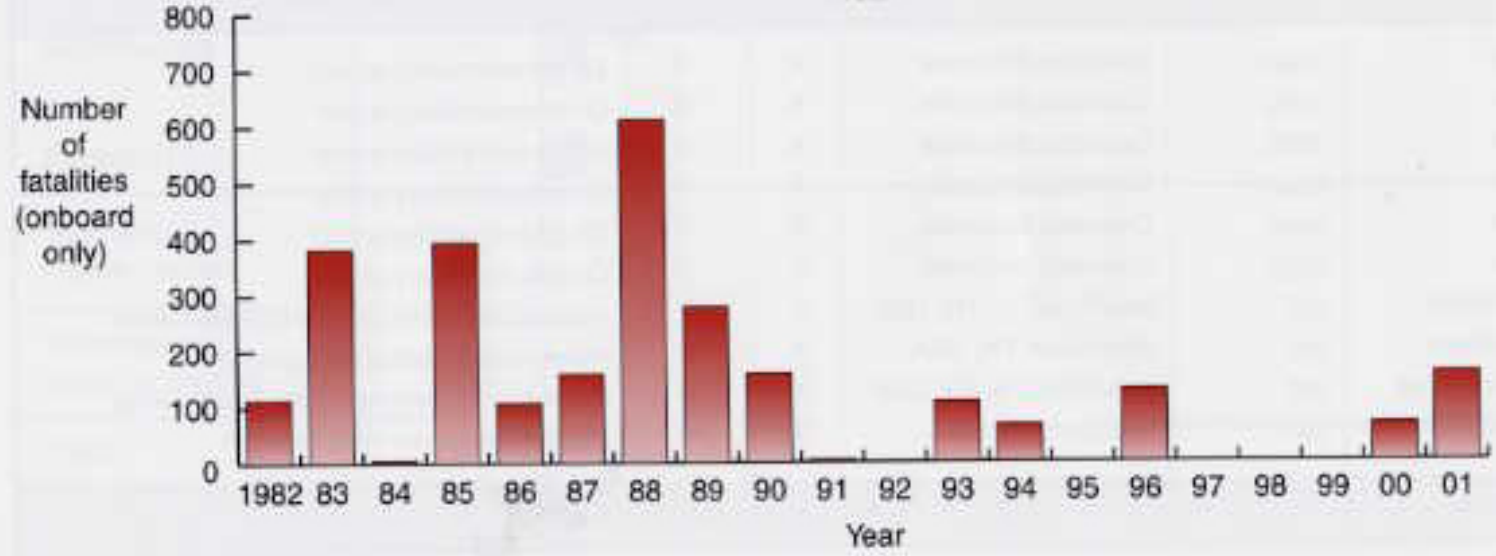


BOEING

Hostile Actions

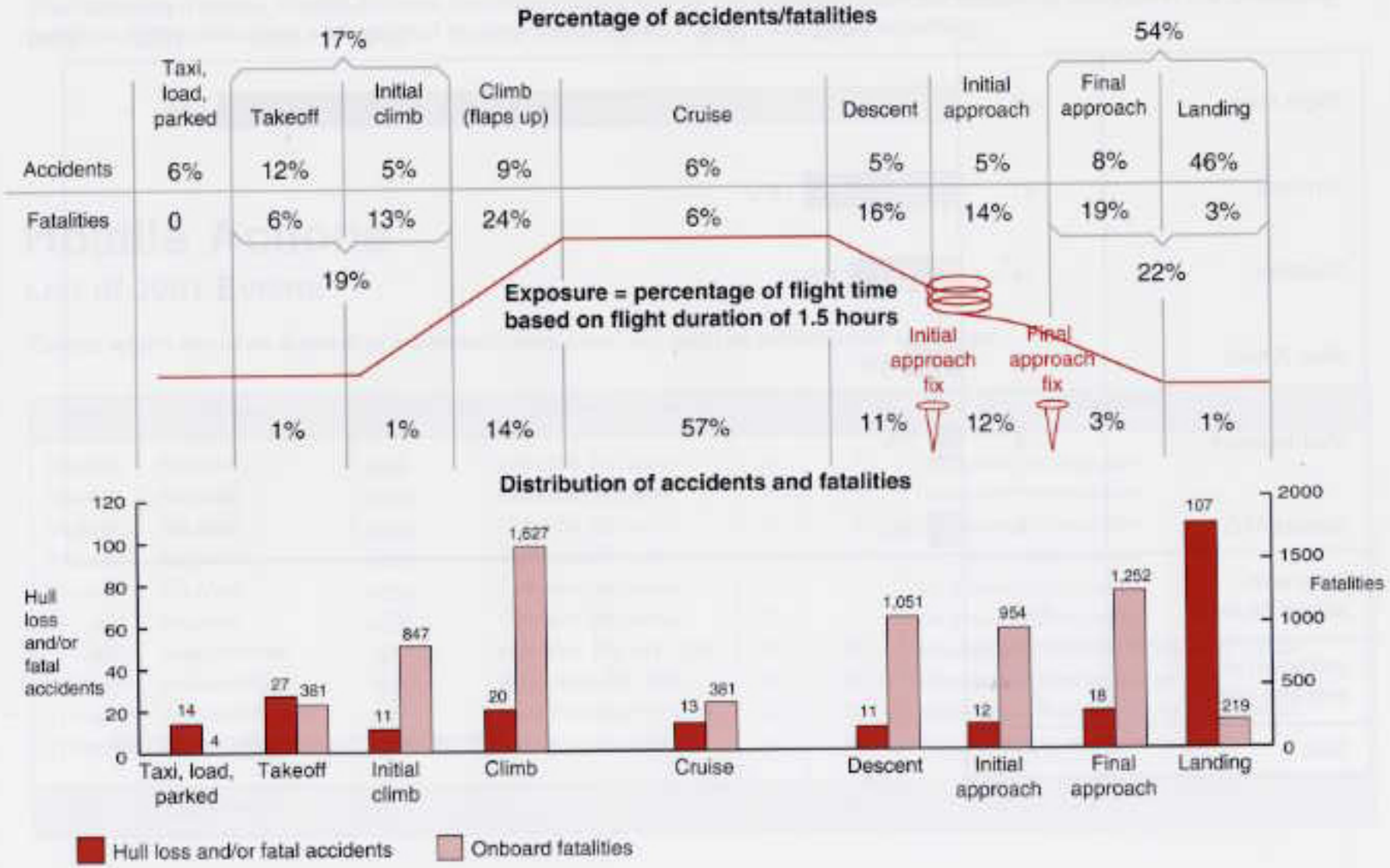
Worldwide Commercial Jet Fleet — 1982 Through 2001





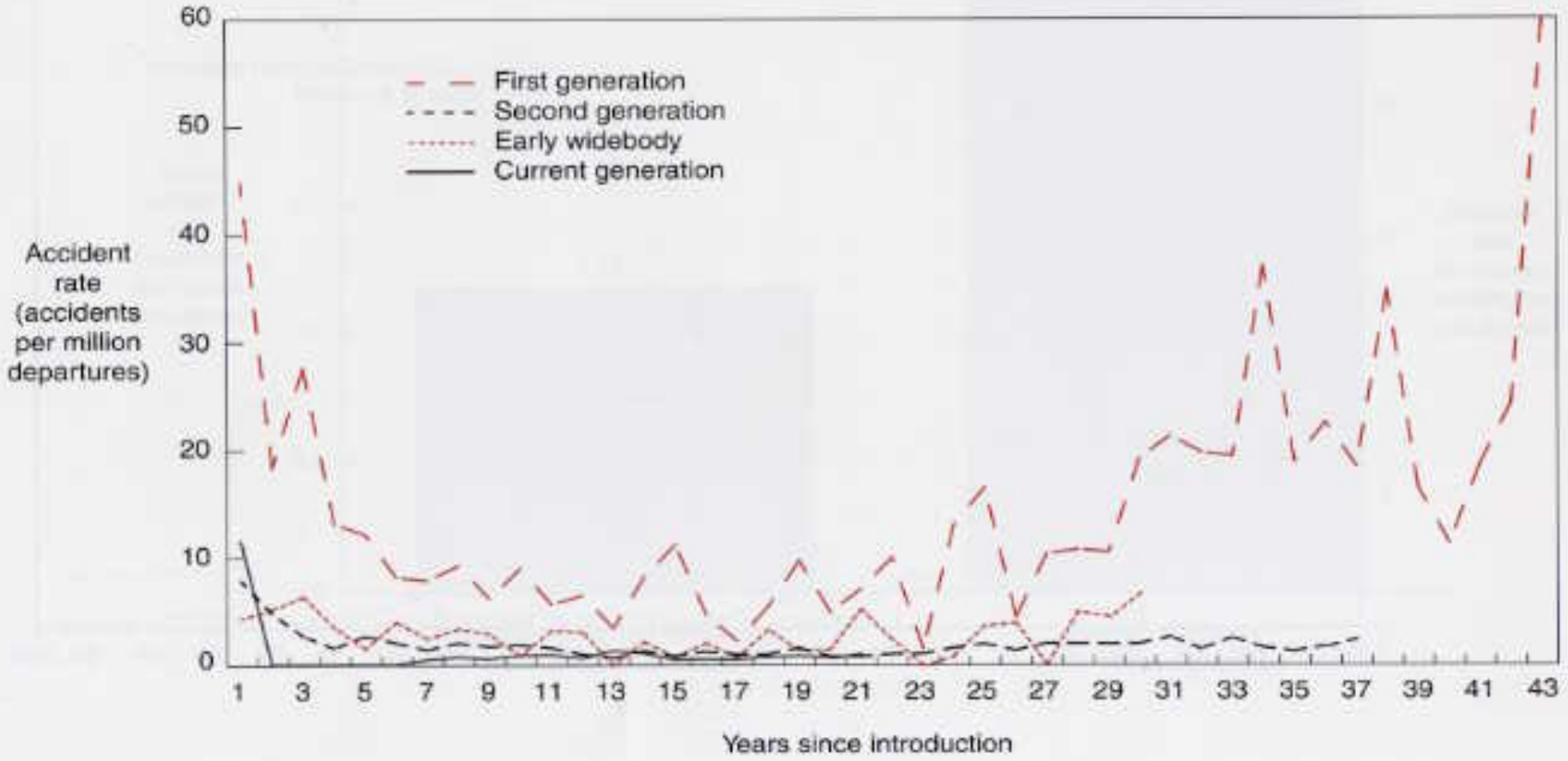
Accidents and Onboard Fatalities by Phase of Flight

Hull Loss and/or Fatal Accidents — Worldwide Commercial Jet Fleet — 1992 through 2001



Accident Rates by Years Following Introduction

Hull Loss and/or Fatal Accidents – Worldwide Commercial Fleet – 1959 Through 2001



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

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

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

- http://www.faa.gov/regulations_policies/

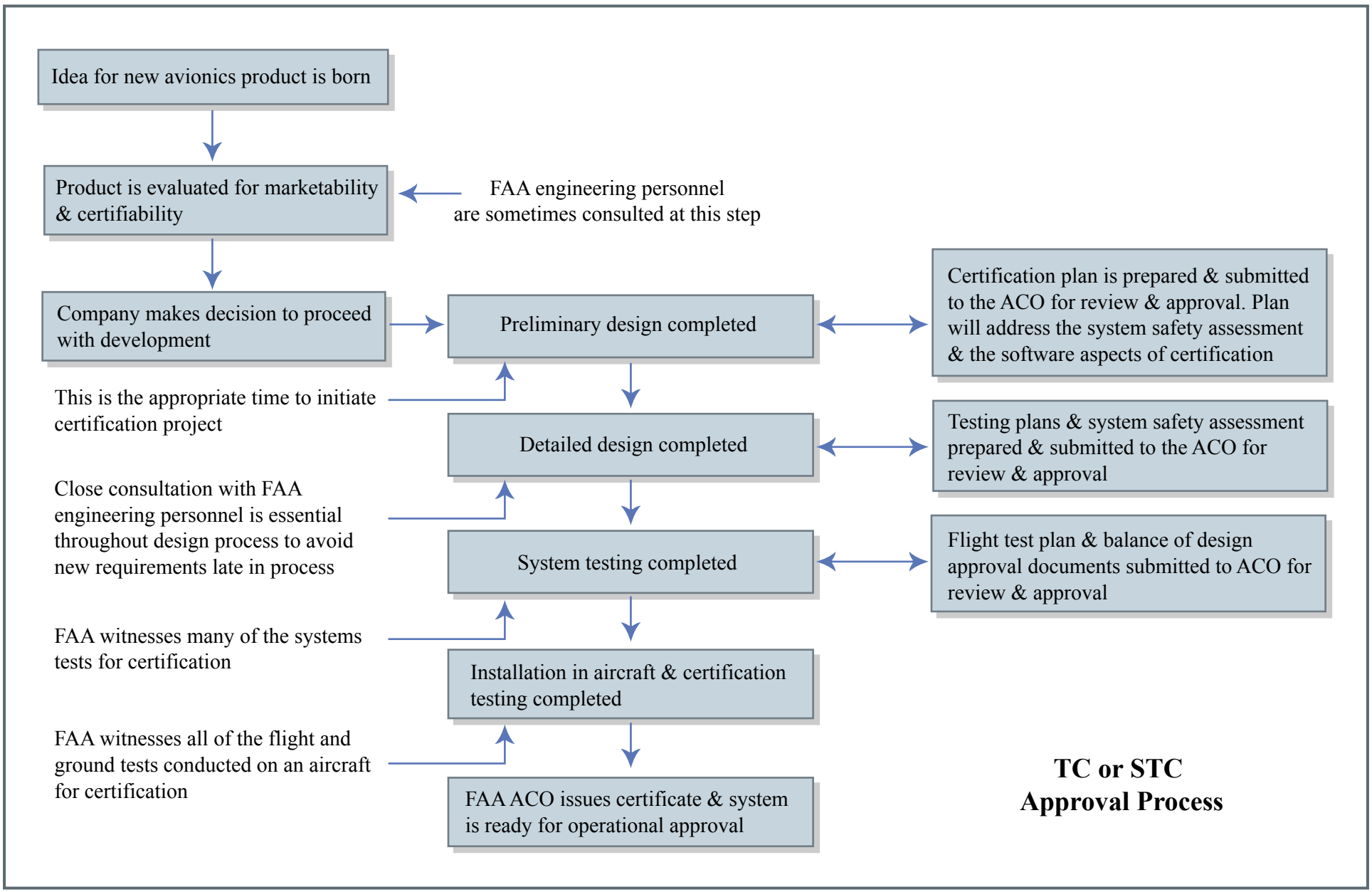
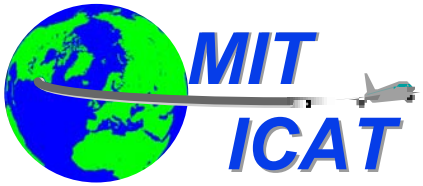


Figure by MIT OCW.

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



	Probable	Improbable	Extremely Improbable
Catastrophic Accident			
Adverse Effect On Occupants			
Airplane Damage			
Emergency Procedures			
Abnormal Procedures			
Nuisance			
Normal			

Descriptive Probabilities

Probability (per unit of exposure)	FAR	JAR
1		Frequent
10E-3	Probable	
10E-5		Reasonably Probable
10E-7	Improbable	Remote
10E-9		Extremely Remote
	Extremely Improbable	Extremely Improbable

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

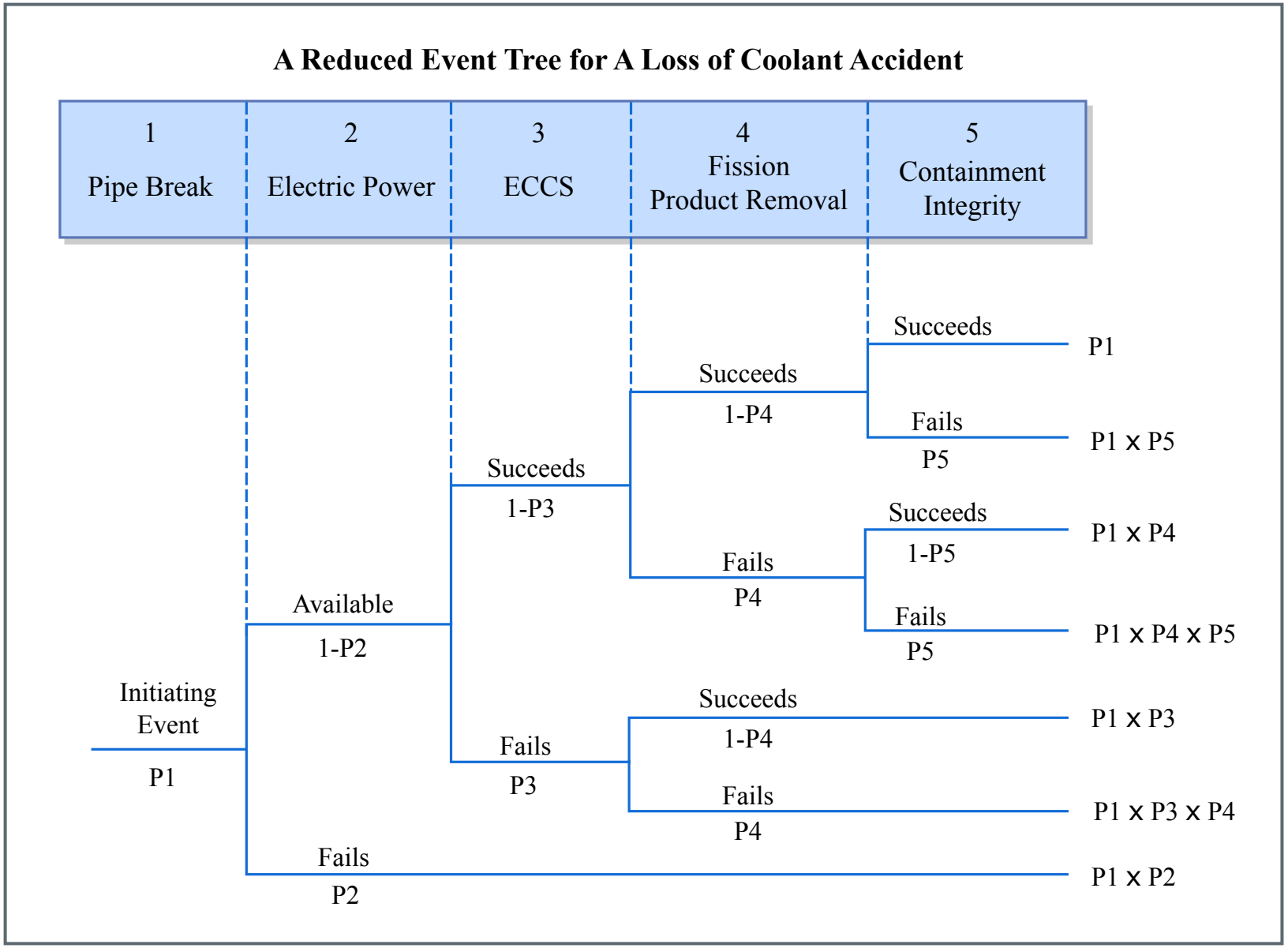
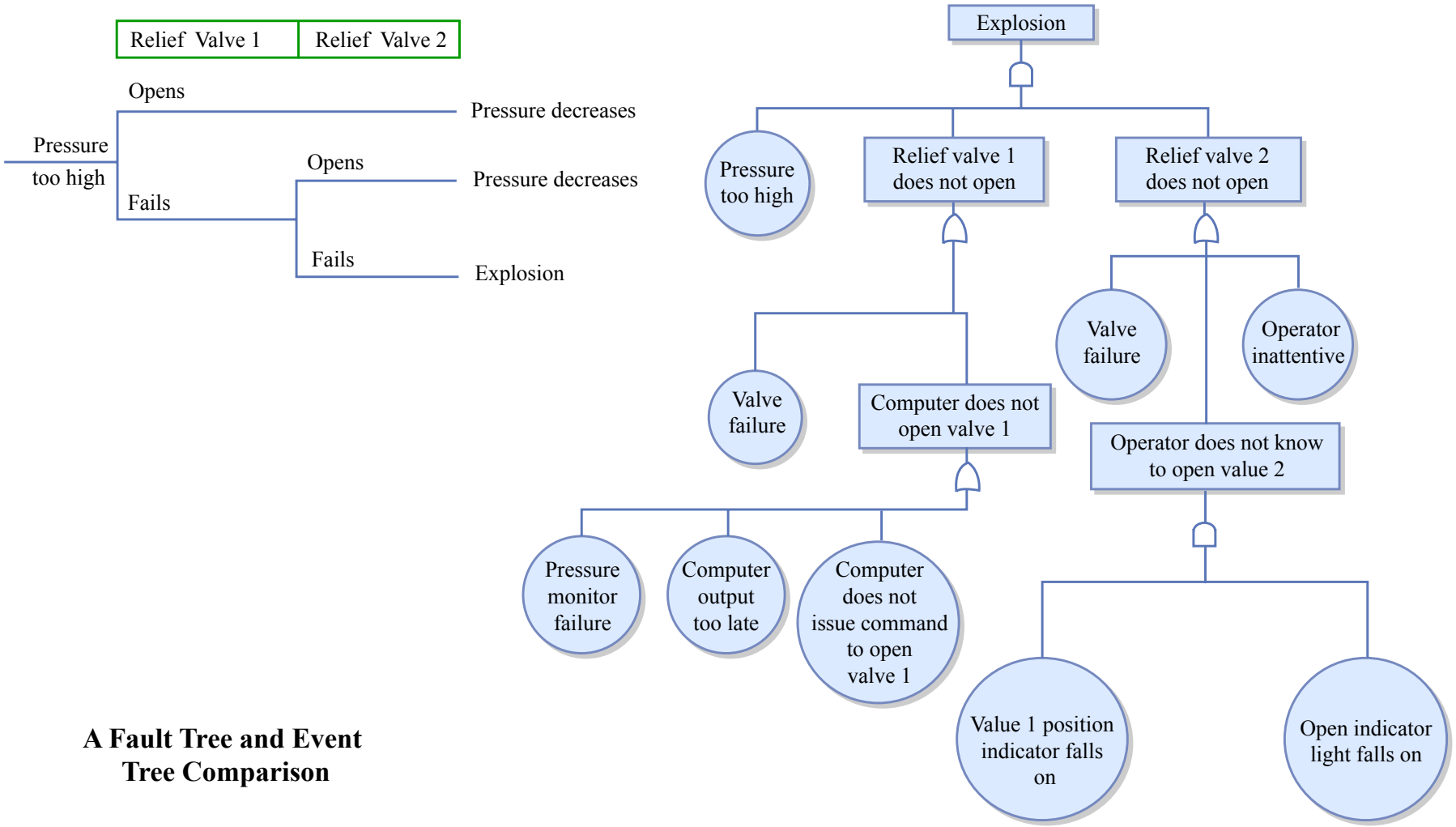


Figure by MIT OCW.

Fault Tree and Event Tree Examples
From : Leveson

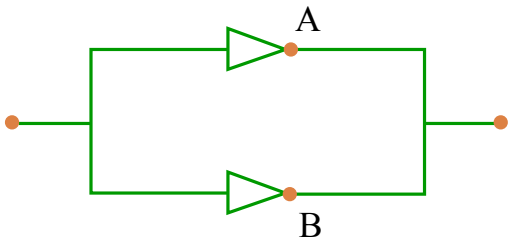


A Fault Tree and Event Tree Comparison

Figure by MIT OCW.

Failure Modes and Effects Analysis

FMEA FOR A SYSTEM OF TWO AMPLIFIERS IN PARALLEL



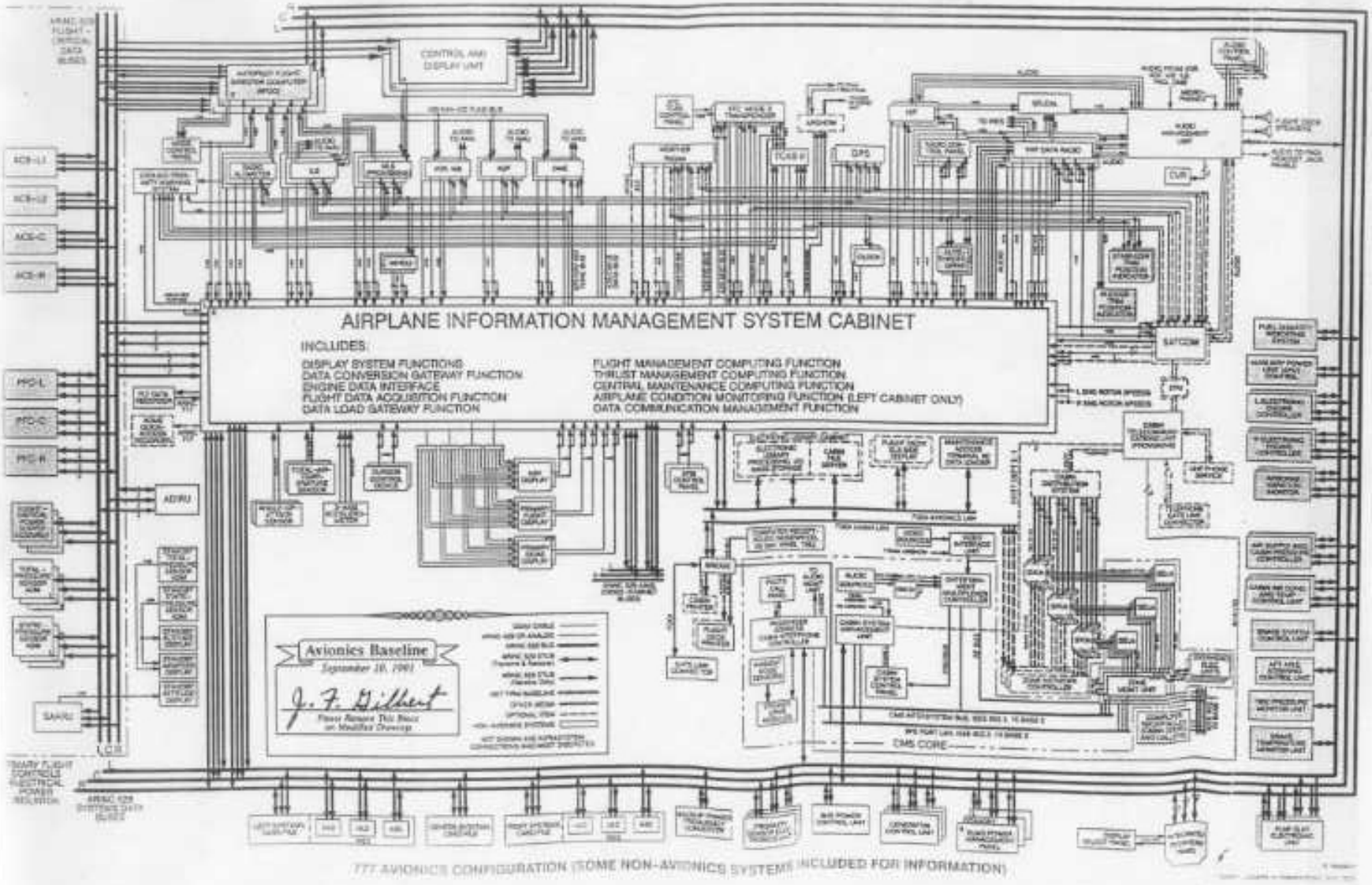
Critical	Failure probability	Failure mode	Failures by mode (%)	Effects	
				Critical	Noncritical
A	1×10^{-3}	Open	90		x
		Short	5	5×10^{-5}	
		Other	5	5×10^{-5}	
B	1×10^{-3}	Open	90		x
		Short	5	5×10^{-5}	
		Other	5	5×10^{-5}	

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

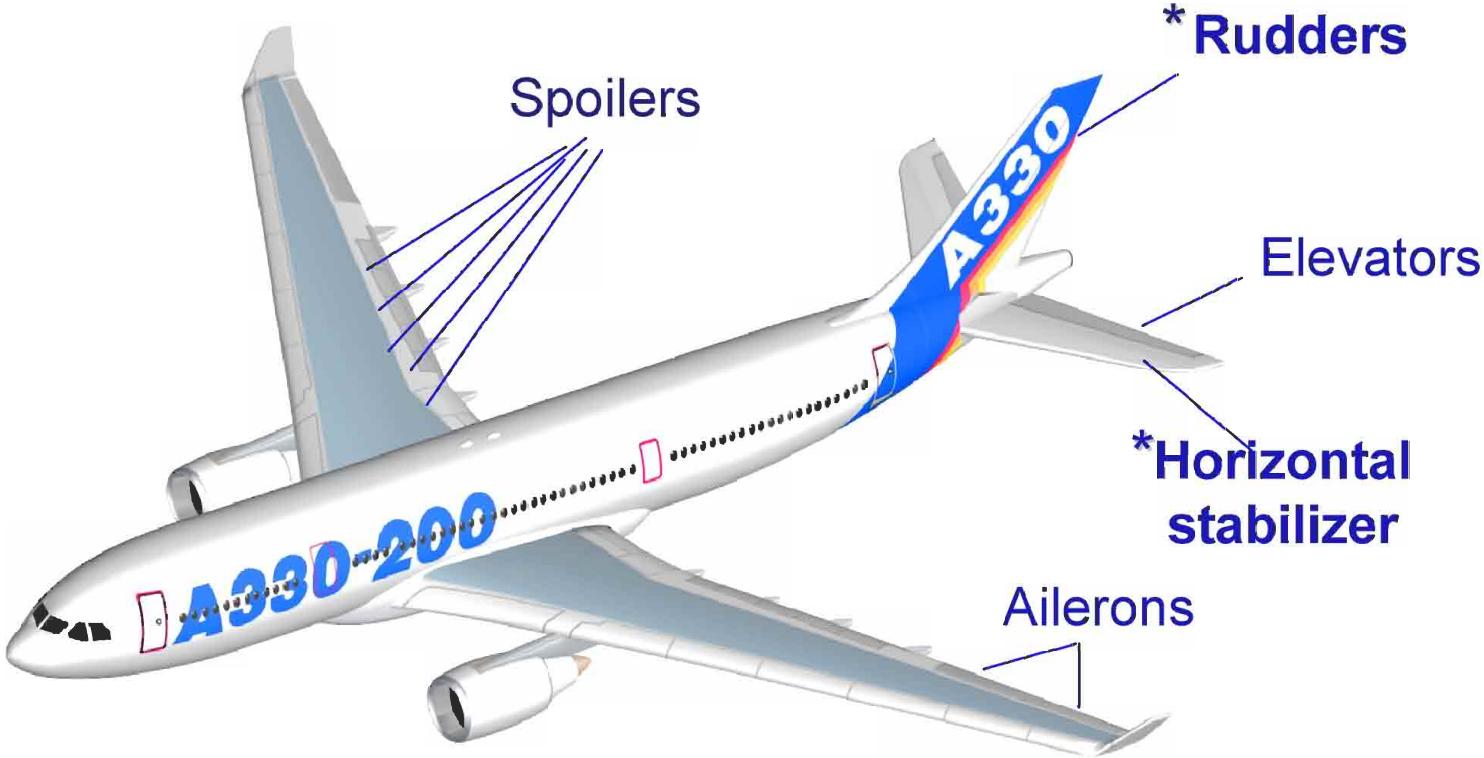
B777 Avionics Architecture



777 AVIONICS CONFIGURATION (SOME NON-AVIONICS SYSTEMS INCLUDED FOR INFORMATION)

A330 A340
Fly-by-wire - control surfaces

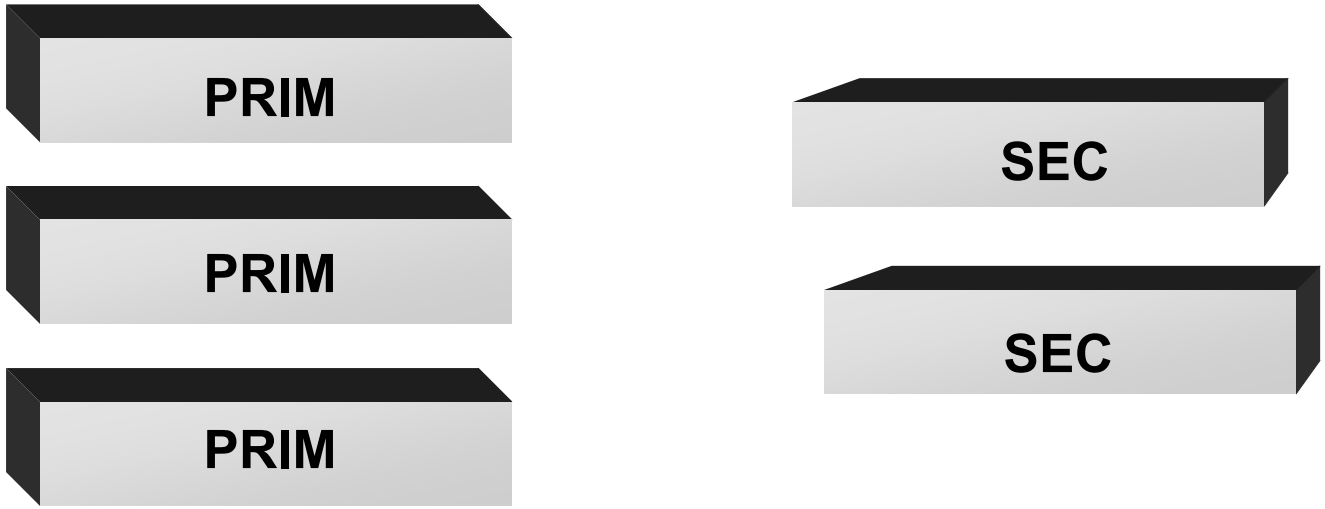
Electrically controlled, hydraulically actuated



Identical for the A340

*Rudder & Horizontal stabilizer have back-up mechanical control

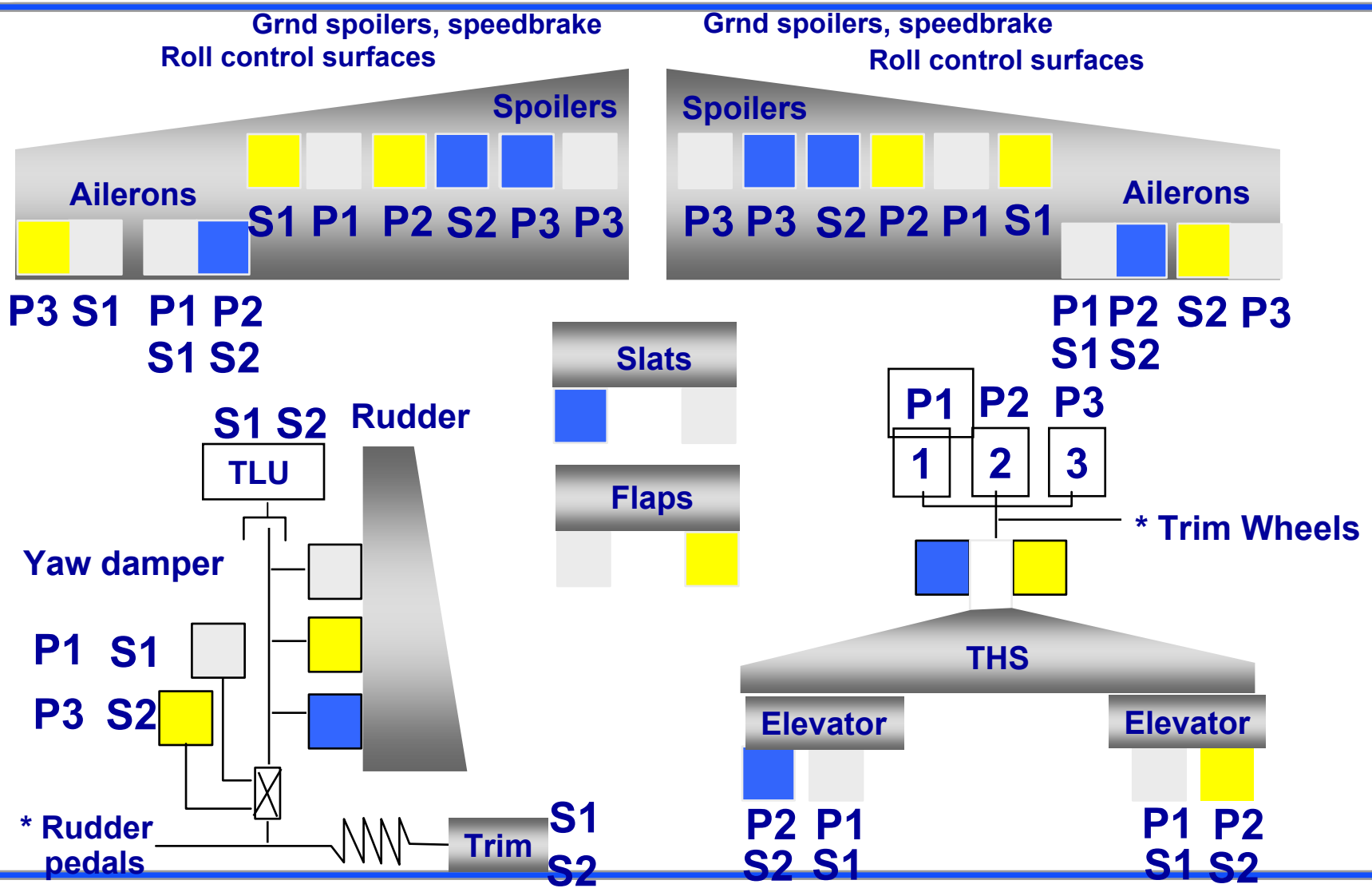
Fly-by-wire A330/A340

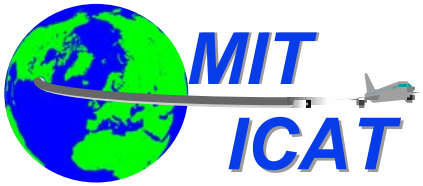


- Flight Control computers are dual channel
  - one for control and one for monitoring
- Each processor has a different vendor for hardware & software
  - software for each processor coded in a different language

FBW-A330/A340 flight control architecture

Computer / hydraulic actuator arrangement

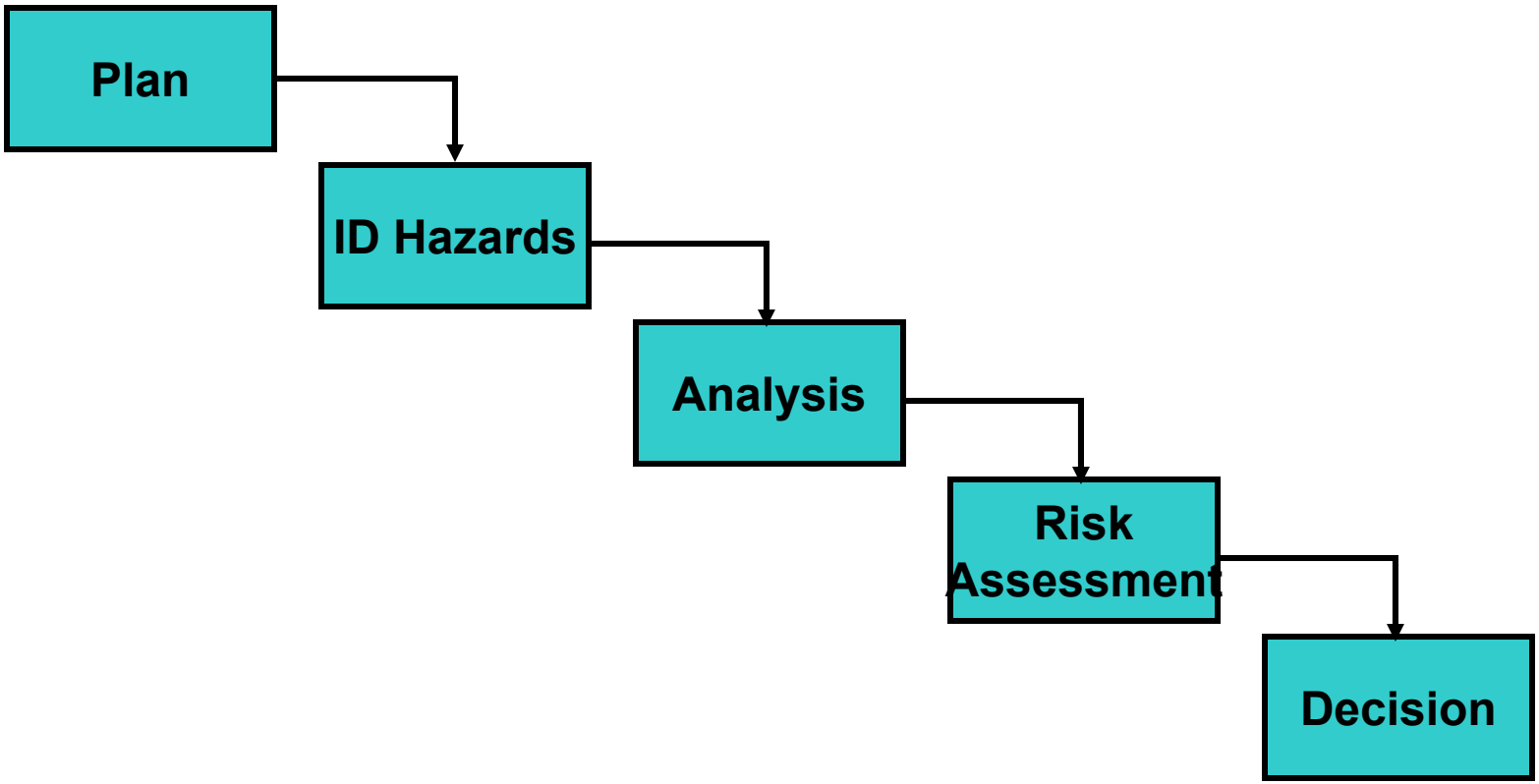




Additional Issues

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

FAA 8040.4 Safety Analysis Process



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 month (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 month according to cycles/flying time etc.
- **IL-check** is made every 48 month and include 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 month.

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