Certification and Avionics

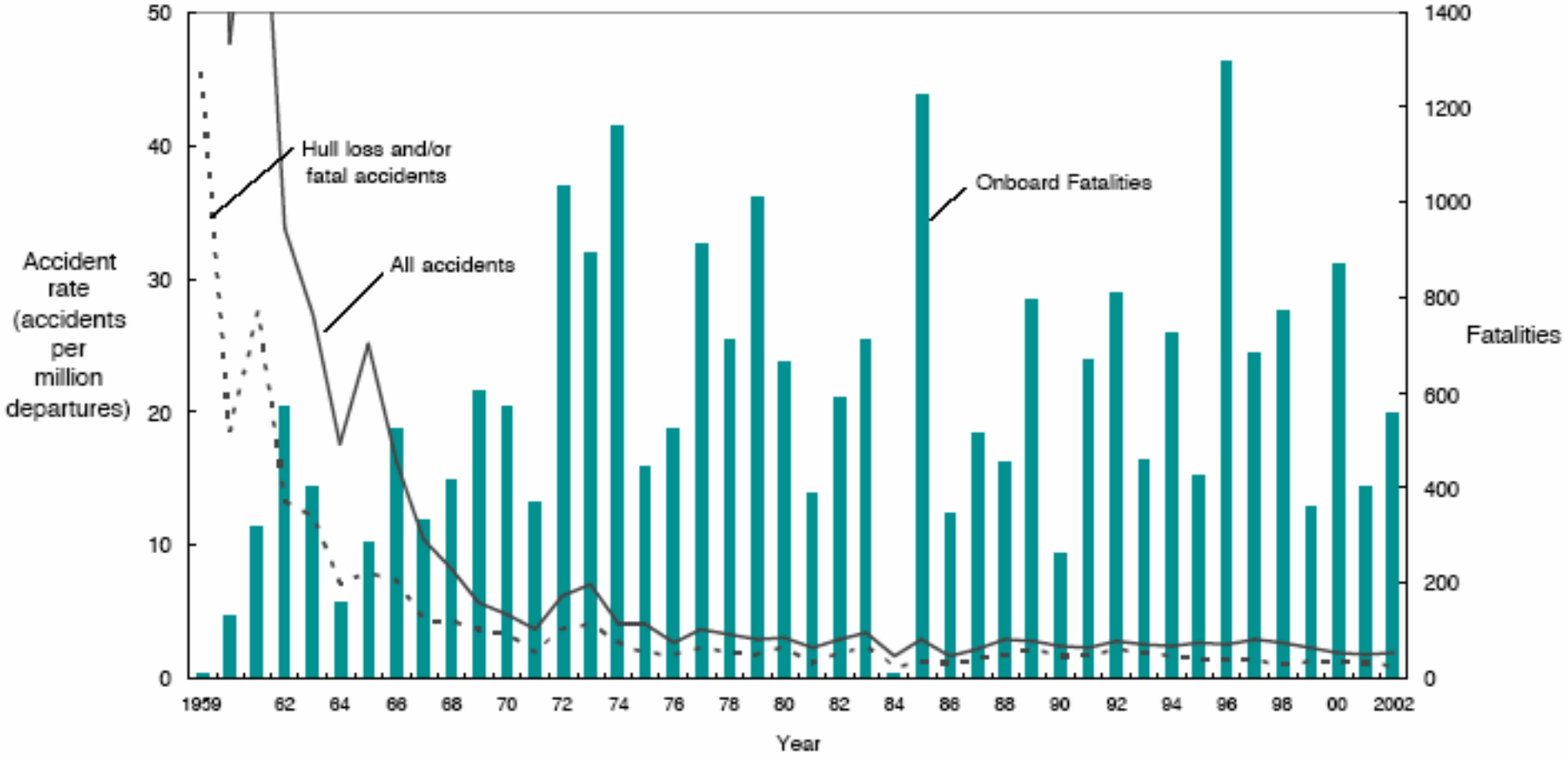
Prof. R. John Hansman
MIT International Center for Air Transportation

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

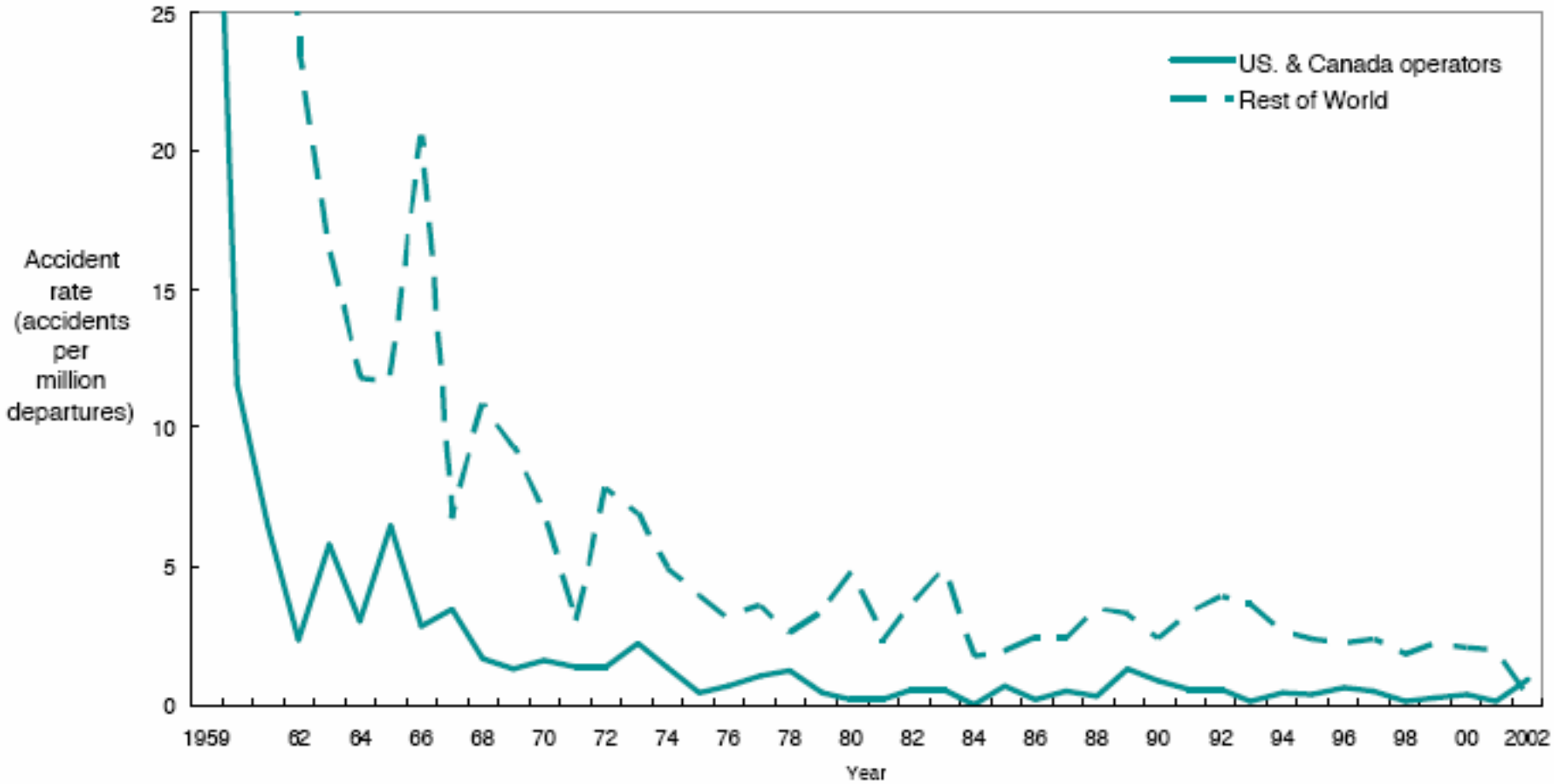
All Accidents - Worldwide Commercial Jet Fleet - 1959 through 2002



(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

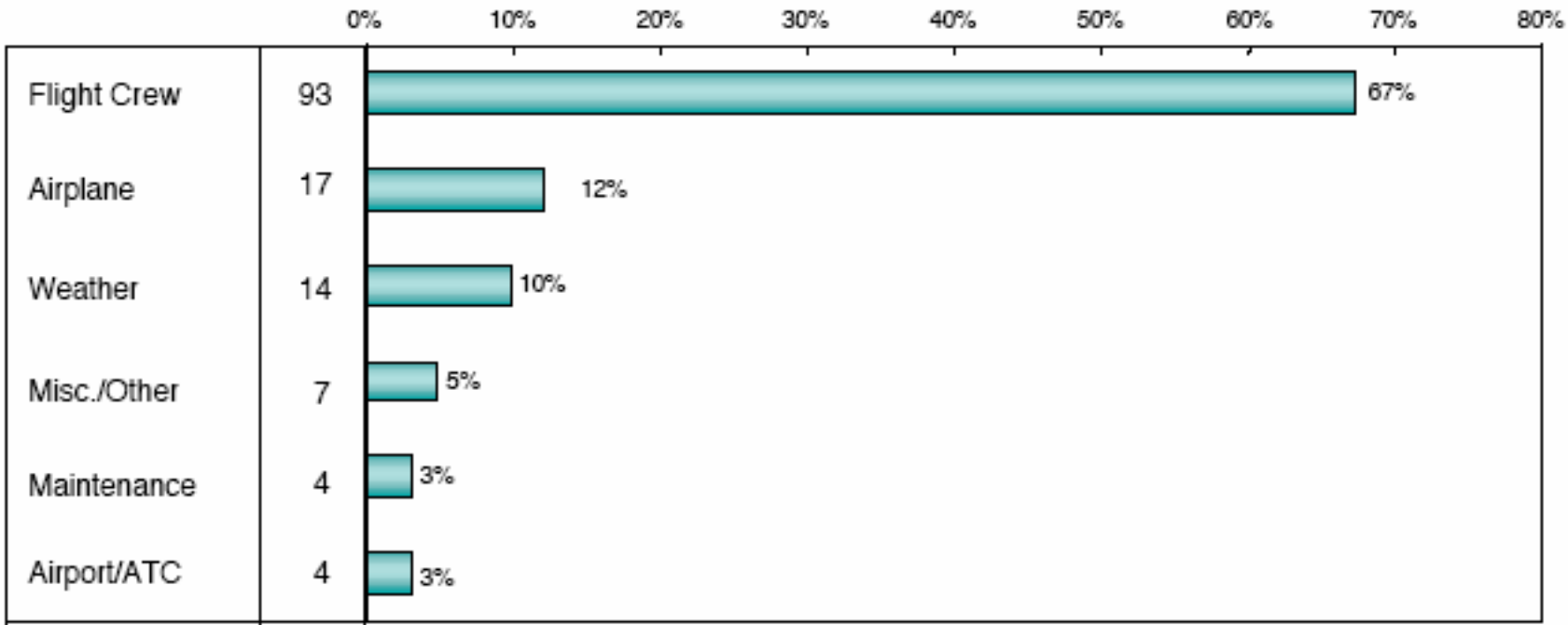


(Courtesy of Boeing Corporation. Used with permission.)

BOEING

Accidents by Primary Cause*

Hull Loss - Worldwide Commercial Jet Fleet - 1993 through 2002



Total with known causes	139
Unknown or awaiting reports	59
Total	198

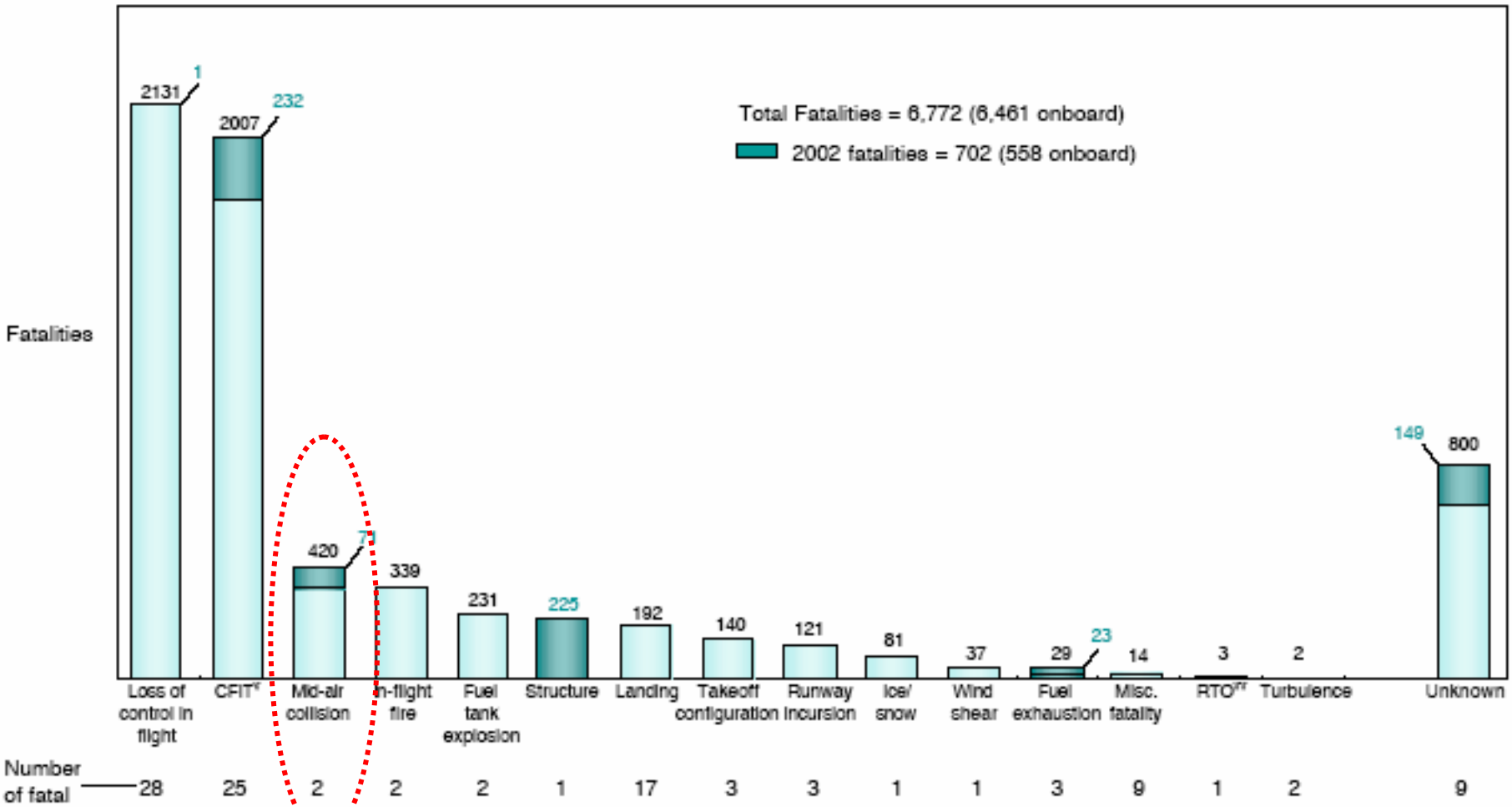
*As determined by the investigating authority, percent of accidents with known causes.

(Courtesy of Boeing Corporation. Used with permission.)

BOEING

Fatalities by Accident Category

Fatal Accidents - Worldwide Commercial Jet Fleet - 1993 Through 2002



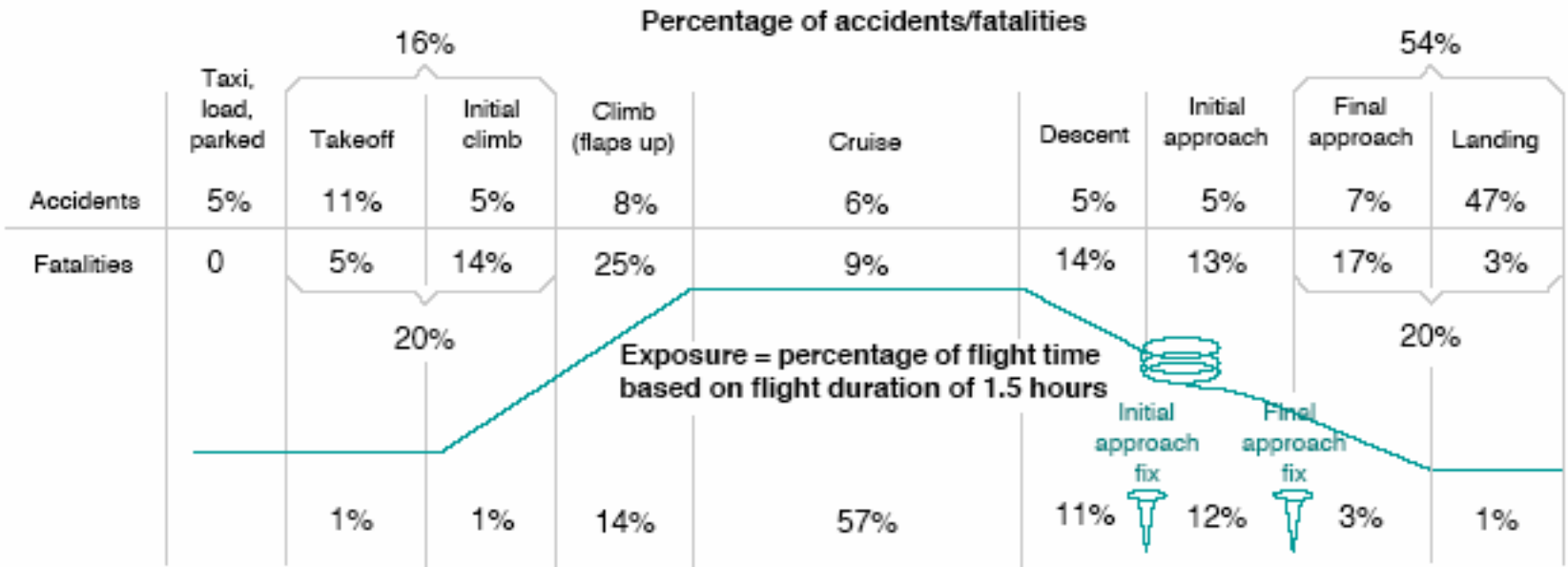
Note: Accidents involving multiple, non-onboard fatalities are included
Accidents involving single, non-onboard fatalities are excluded
Fatalities/accidents are placed in one category only.

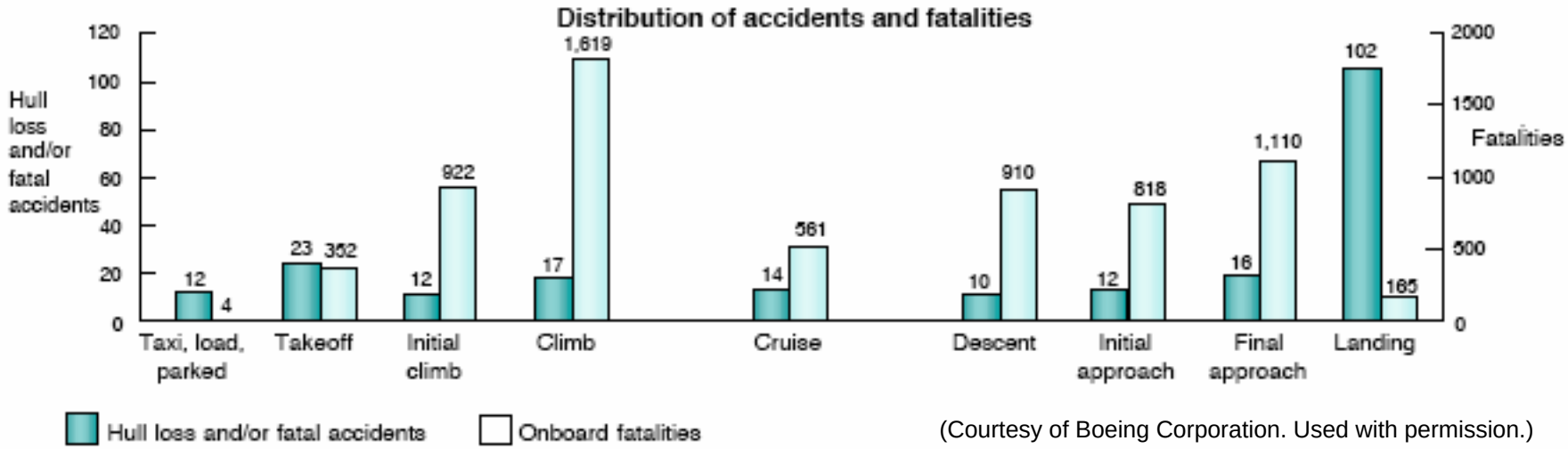
* CFIT = Controlled Flight Into Terrain
** RTO = Refused Takeoff

BOEING

Accidents and Onboard Fatalities by Phase of Flight

Hull Loss and/or Fatal Accidents - Worldwide Commercial Jet Fleet - 1993 - 2002

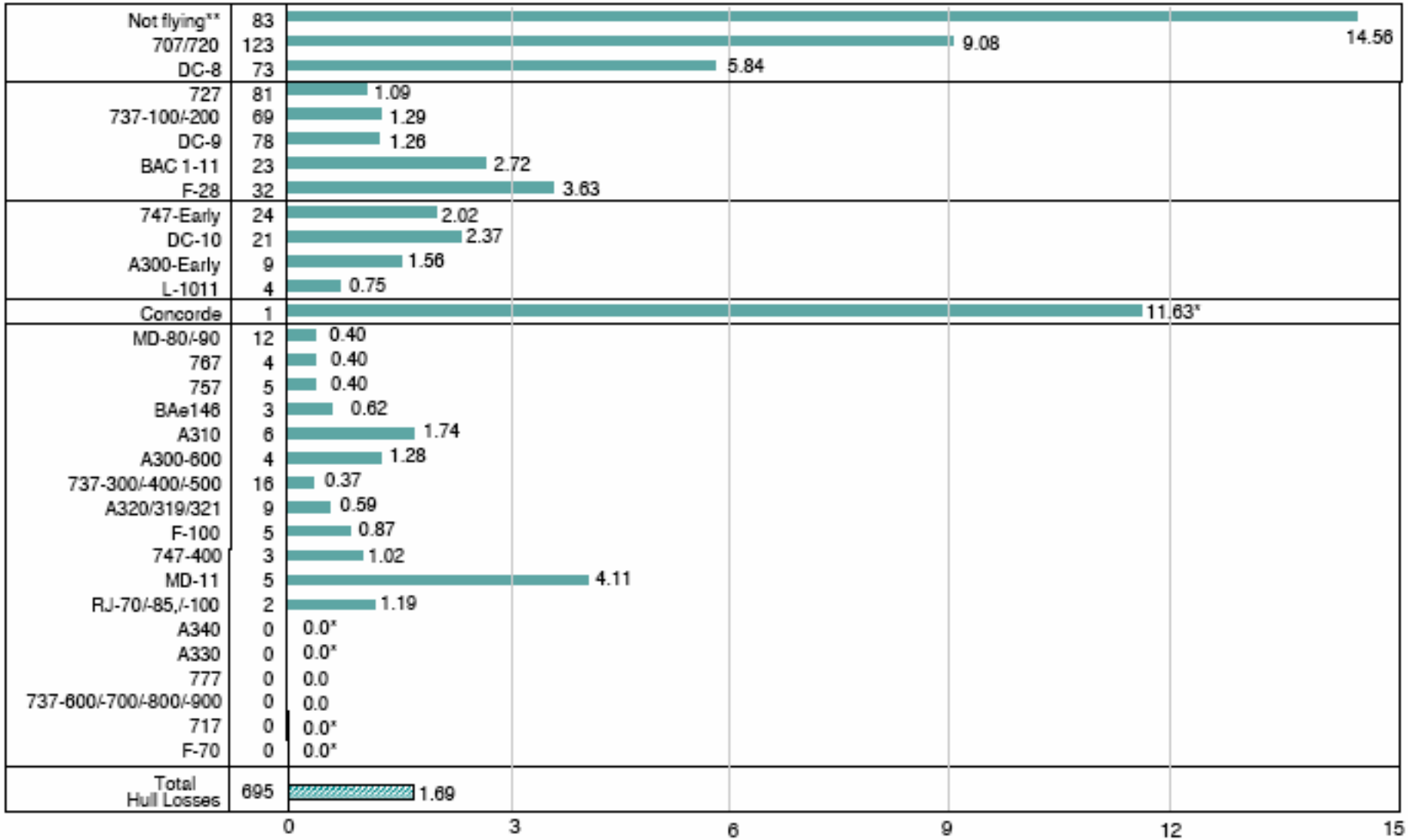




(Courtesy of Boeing Corporation. Used with permission.)

Accident Rates by Airplane Type

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



(Courtesy of Boeing Corporation. Used with permission.)

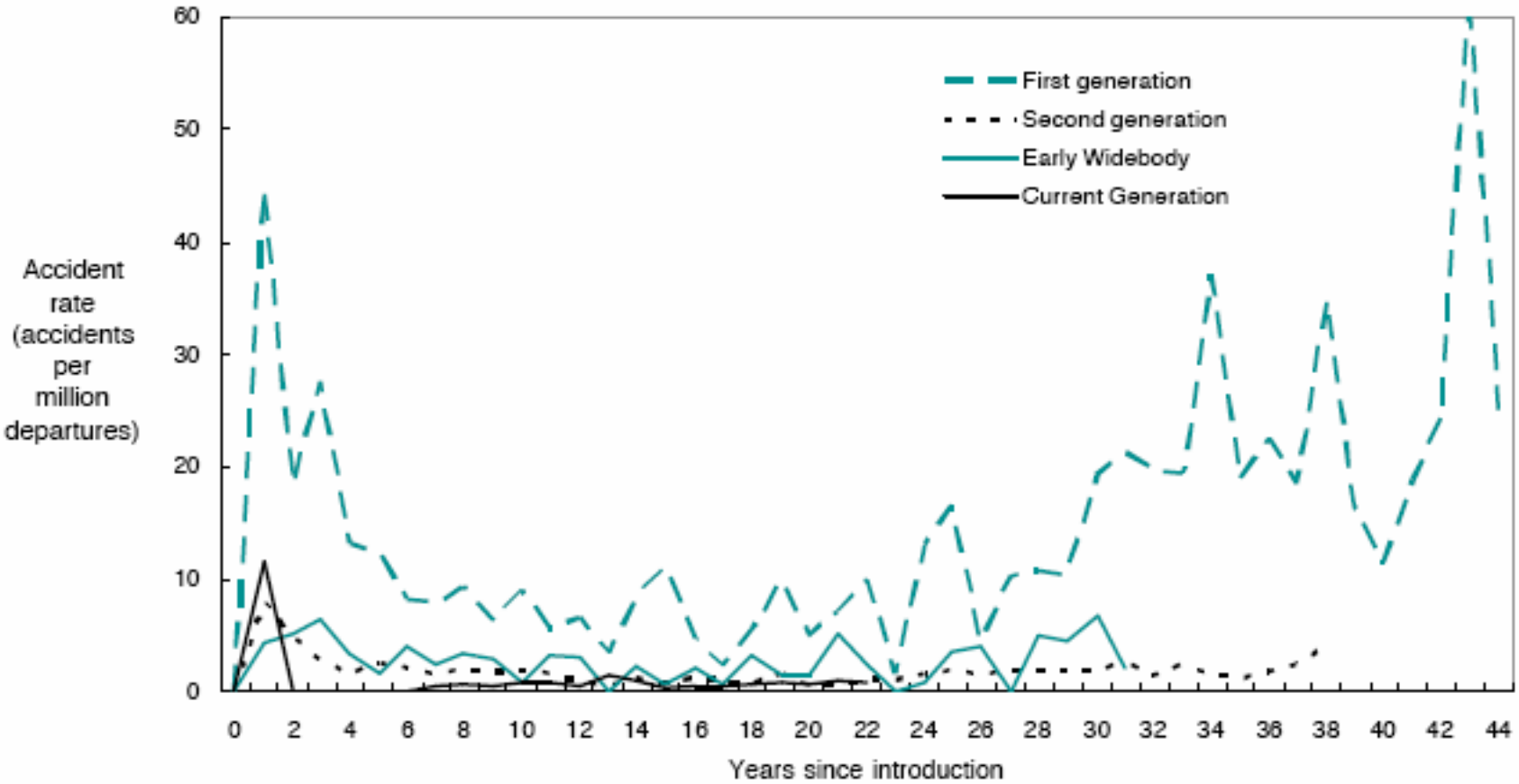
** The Comet, CV880/990, Caravelle, Trident & VC-10 are no longer in commercial service, and are combined in the "Not Flying" bar.

* These types have accumulated fewer than 1 million departures.

BOEING

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

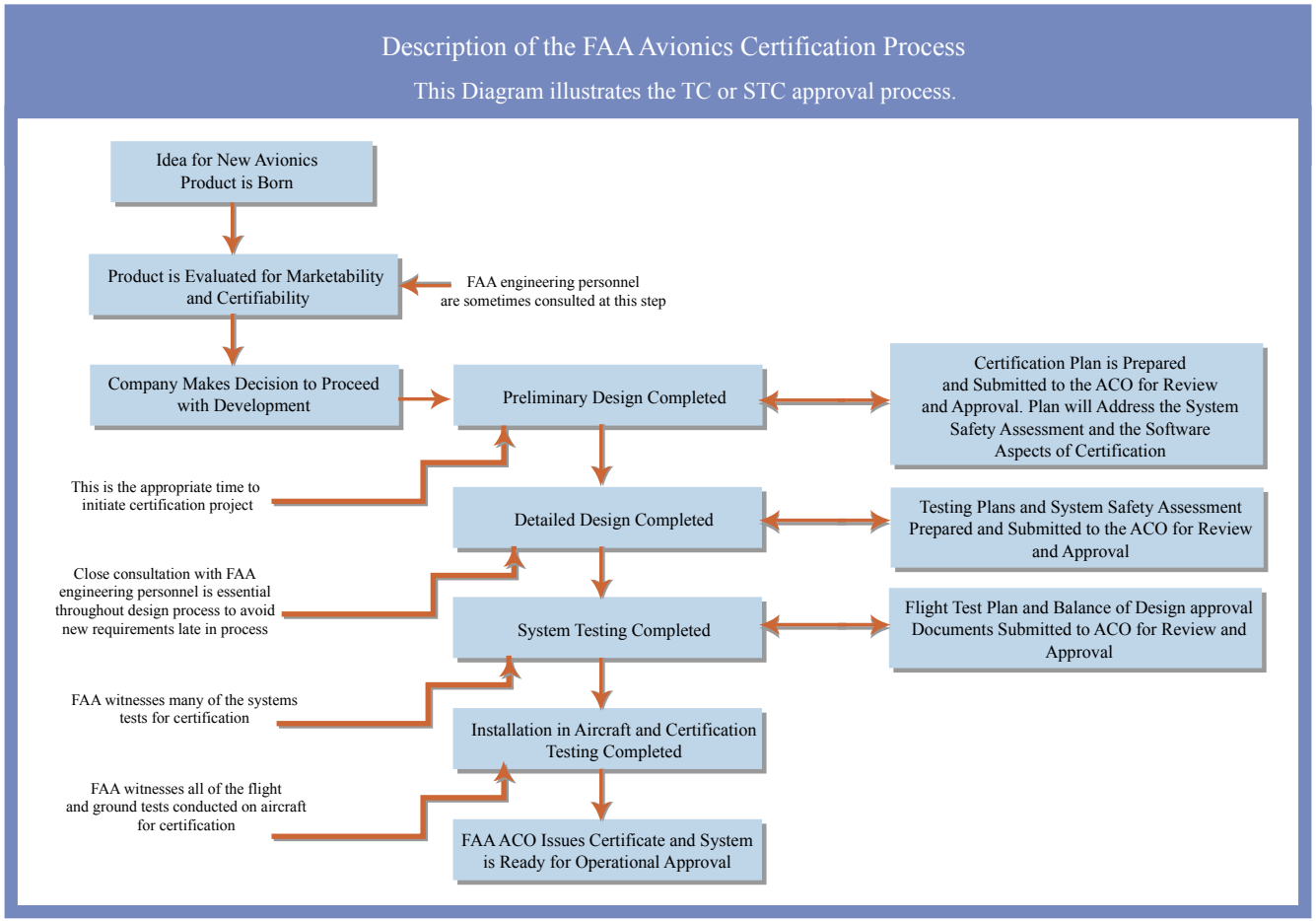
Certification

- **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

- **http://www.airweb.faa.gov/Regulatory_and_Guidance_Library/rgWebcomponents.nsf/HomeFrame?OpenFrameSet**


Description of the FAA Avionics Certification Process
This Diagram illustrates the TC or STC approval process.
Idea for New Avionics Product is Born
Product is Evaluated for Marketability and Certifiability
FAA engineering personnel are sometimes consulted at this step
Company Makes Decision to Proceed with Development
Preliminary Design Completed
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
This is the appropriate time to initiate certification project
Detailed Design Completed
Testing Plans and System Safety Assessment Prepared and Submitted to the ACO for Review and Approval
Close consultation with FAA engineering personnel is essential throughout design process to avoid new requirements late in process
System Testing Completed
Flight Test Plan and Balance of Design approval Documents Submitted to ACO for Review and Approval
FAA witnesses many of the systems tests for certification
Installation in Aircraft and Certification Testing Completed
FAA witnesses all of the flight and ground tests conducted on aircraft for certification
FAA ACO Issues Certificate and System is Ready for Operational 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

	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	
		Reasonably Probable
10E-5		
		Remote
10E-7	Improbable	
		Extremely Remote
10E-9		
	Extremely Improbable	Extremely Improbable

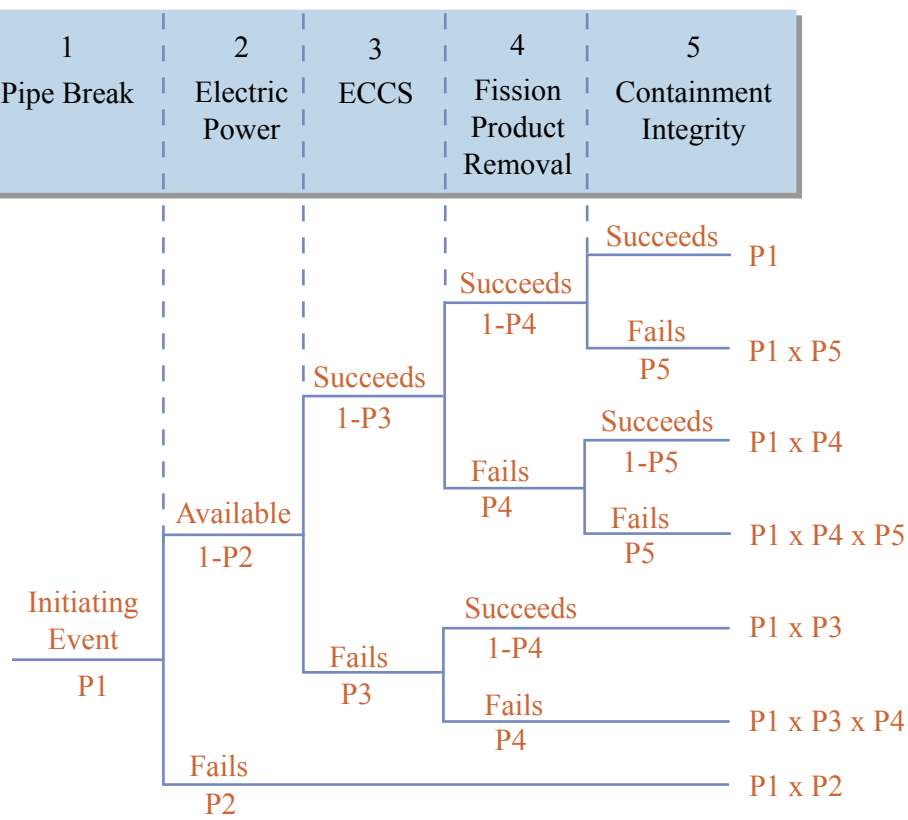
What is the correct unit of exposure : Flight hour, Departure, Failure

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

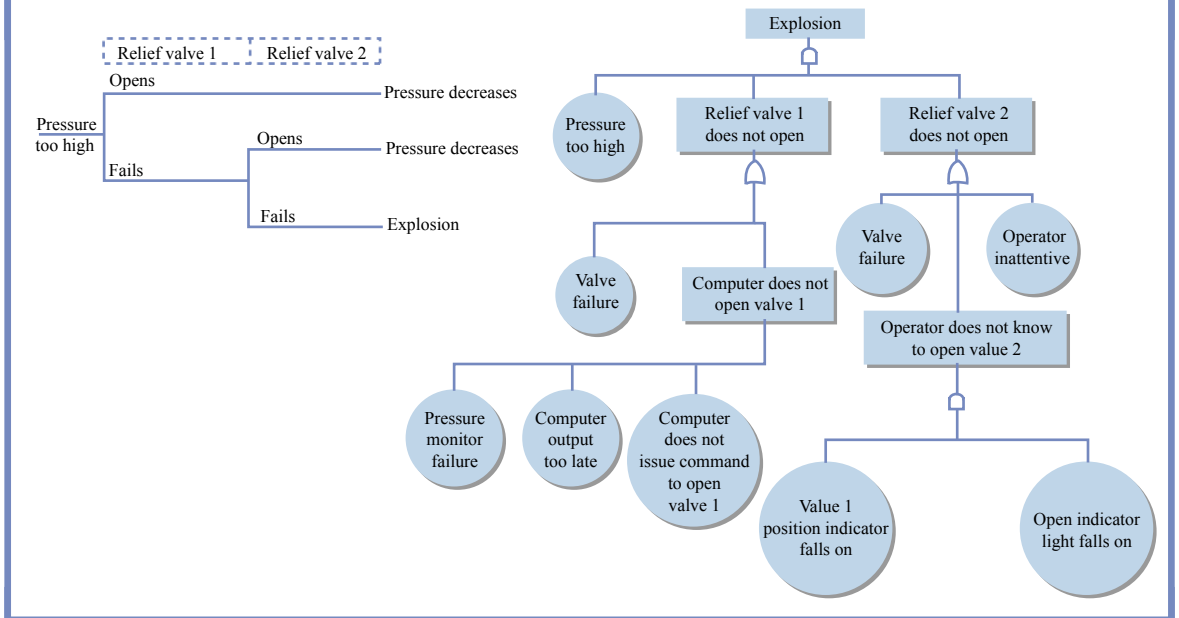
A reduced event tree for a loss of coolant accident.



Adapted from: Leveson, Nancy. *Safeware*: *System Safety and Computers*. Addison-Wesley, 1995.

Fault Tree and Event Tree Examples From : Leveson

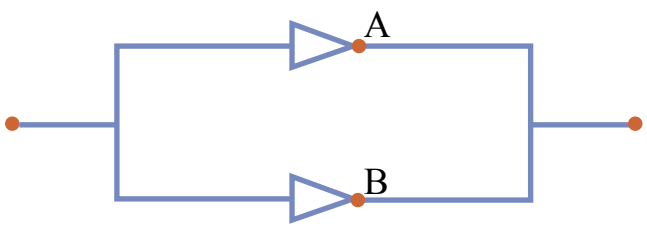
A fault tree and event tree comparison.



Adapted from: Leveson, Nancy. *Safeware*: *System Safety and Computers*. Addison-Wesley, 1995.

Failure Modes and Effects Analysis

FMEA for a system of two amplifiers in parallel.



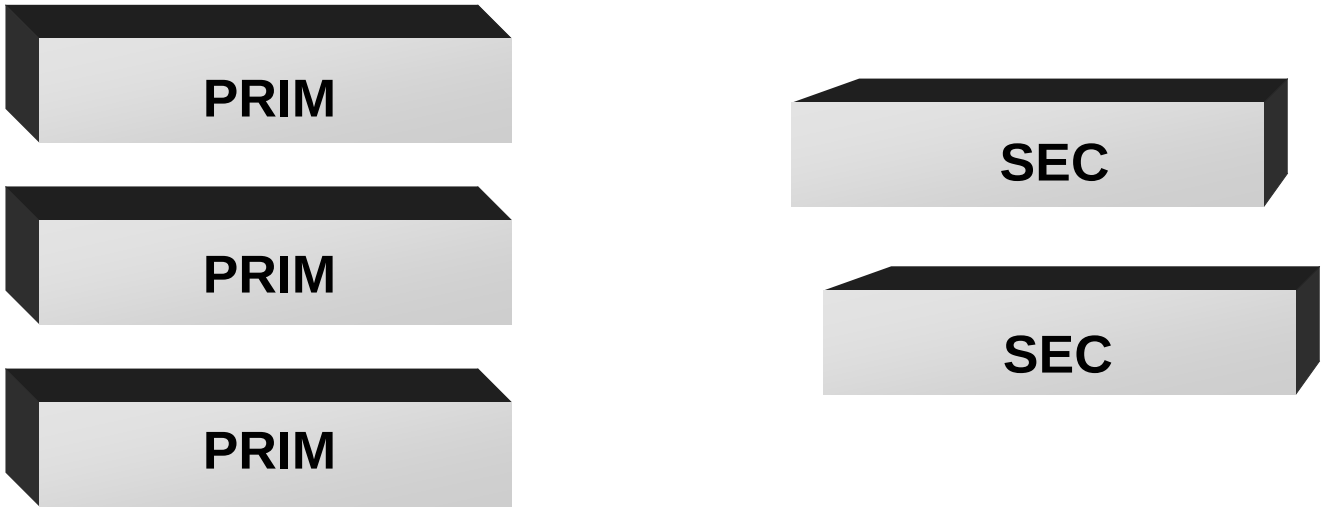
Critical	Failure probability	Failure mode	% Failure by mode	Effects	
				Critical	Noncritical
A	1×10^{-3}	Open	90		x
		Short	5	5×10^{-5}	
		Other	5	5×10^{-5}	
B	1×10^{-3}	Open	90		x
		Short	5	5×10^{-5}	
		Other	5	5×10^{-5}	

Adapted from: Leveson, Nancy. *Safeware*: *System Safety and Computers.* Addison-Wesley, 1995.

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

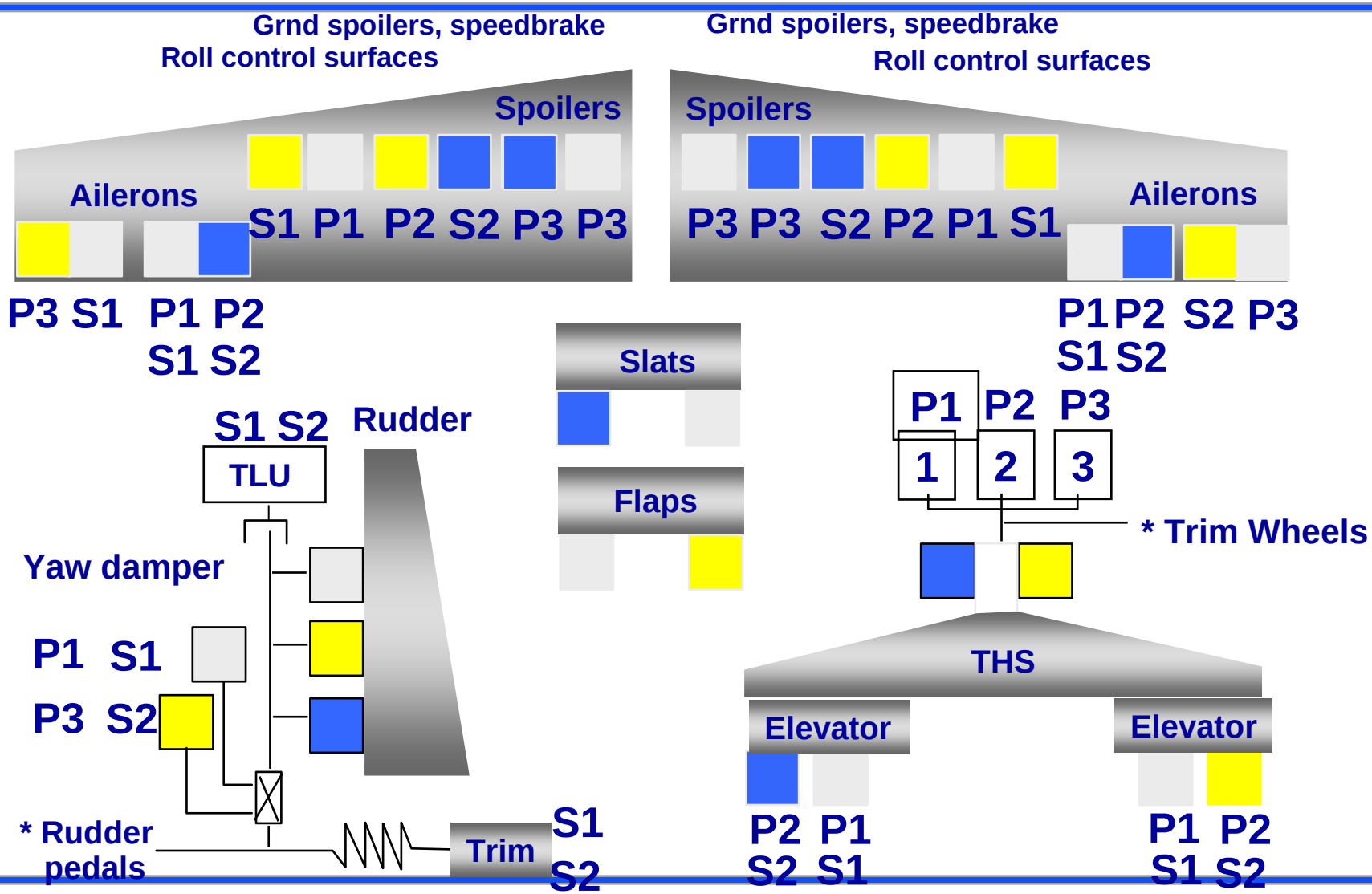
Fly-by-wire - A330/A340



- 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

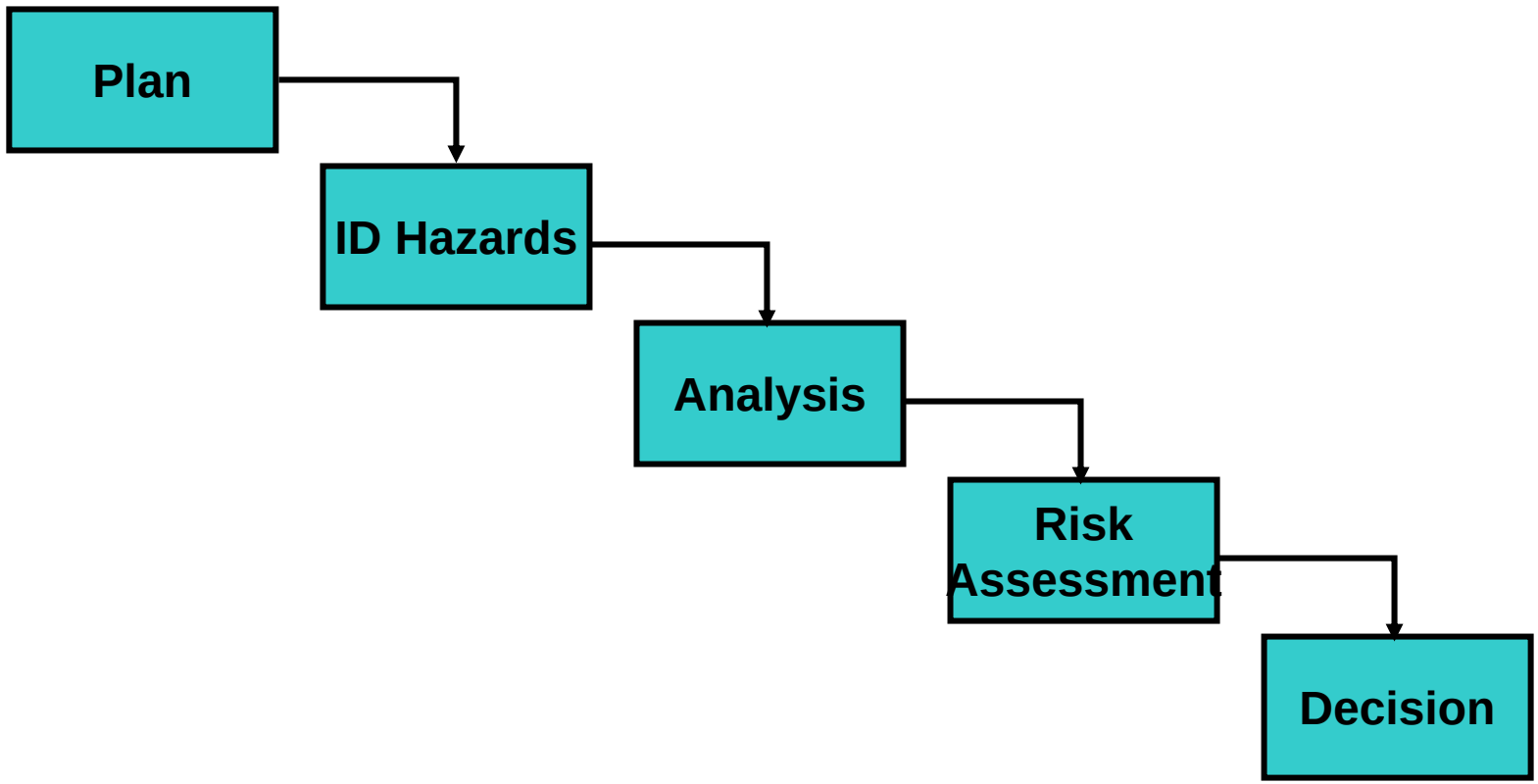
Computer / hydraulic actuator arrangement



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

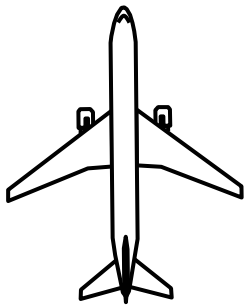
- **MTBF**
  - Mean Time Between Failure
- **MTBUR**
  - Mean Time Between Unscheduled Replacement
- **Dispatch Reliability**
  - Conditional Airworthiness
  - Minimum Equipment List

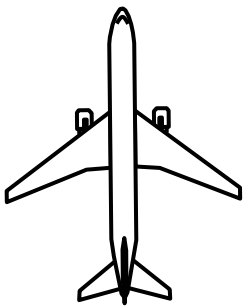
- **Relates to Life Cycle Costs**

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)
  - Airworthiness Directives, Service Difficulty Reports
- **Parts Inventory**
  - Parts Tracking
  - Commonality
    - Glass Cockpits
    - F16 Tail

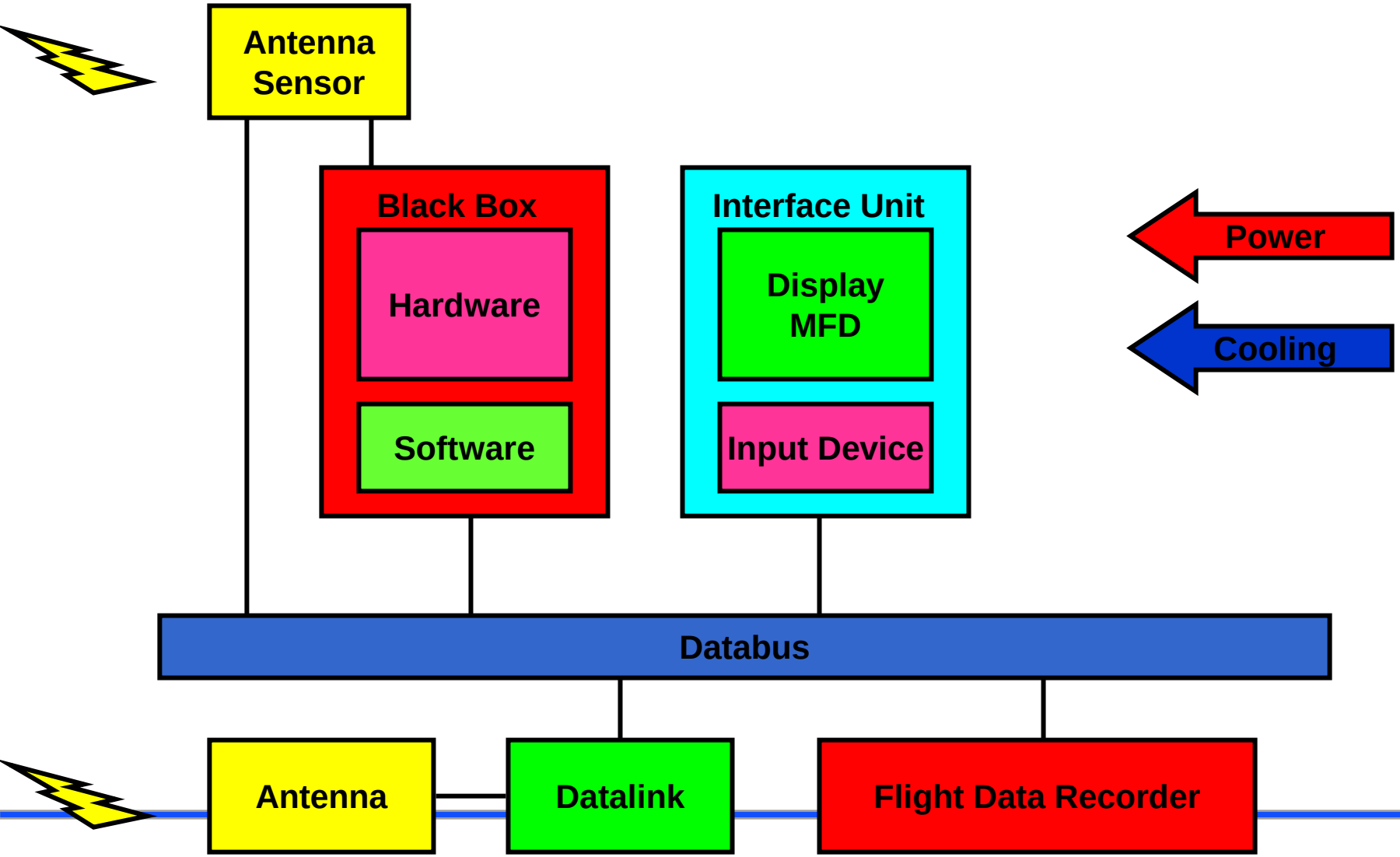
What are the Key Technologies for Formation Flight





- **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?**

Generic Avionic System

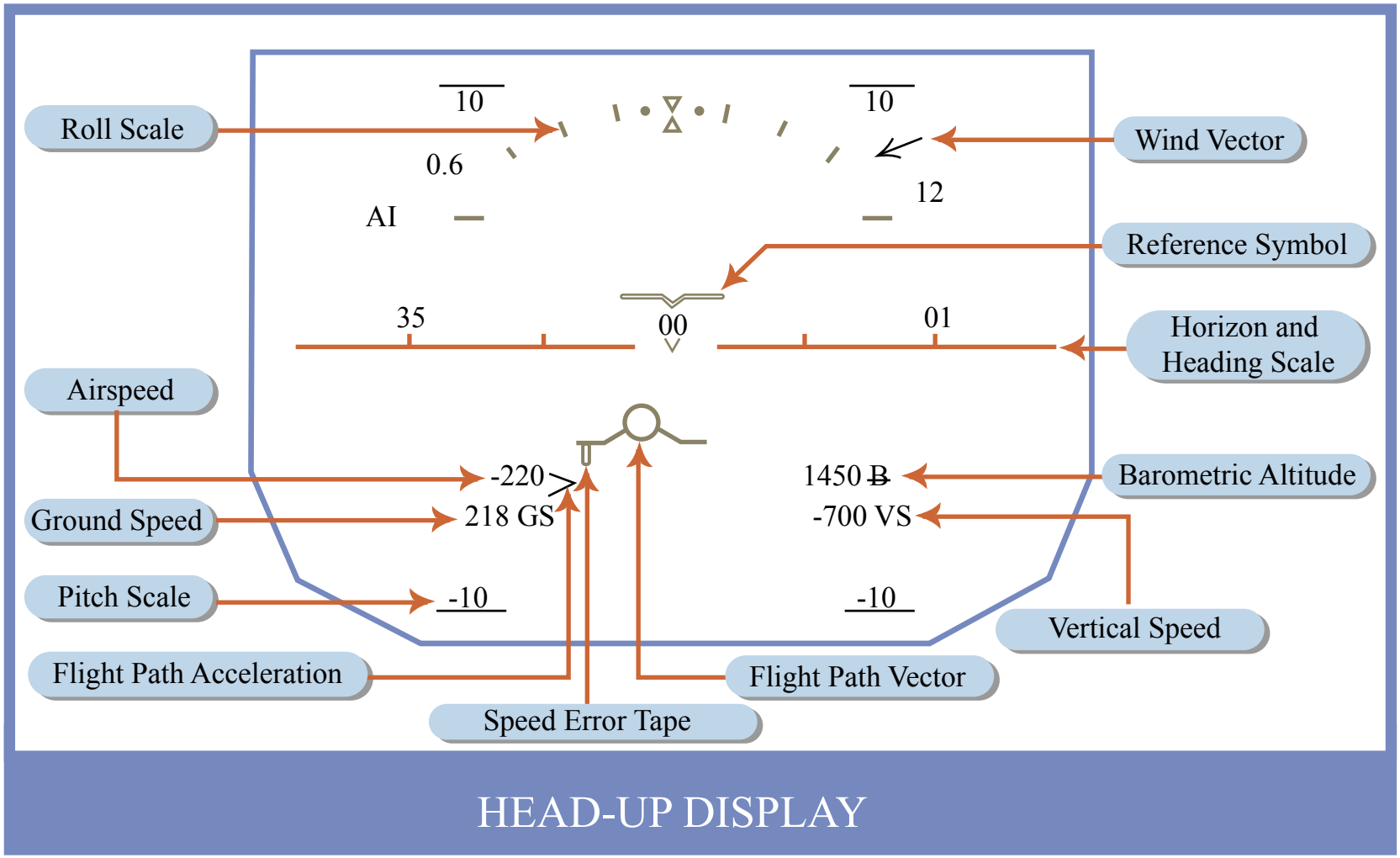


Avionics Components

- **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 (α)
- Angle of Sideslip (β)



HEAD-UP DISPLAY