Safety Management Challenges for Aviation Cyber Physical Systems

Prof. R. John Hansman & Roland Weibel

MIT International Center for Air Transportation

rjhans@mit.edu, weibel@mit.edu

Challenges

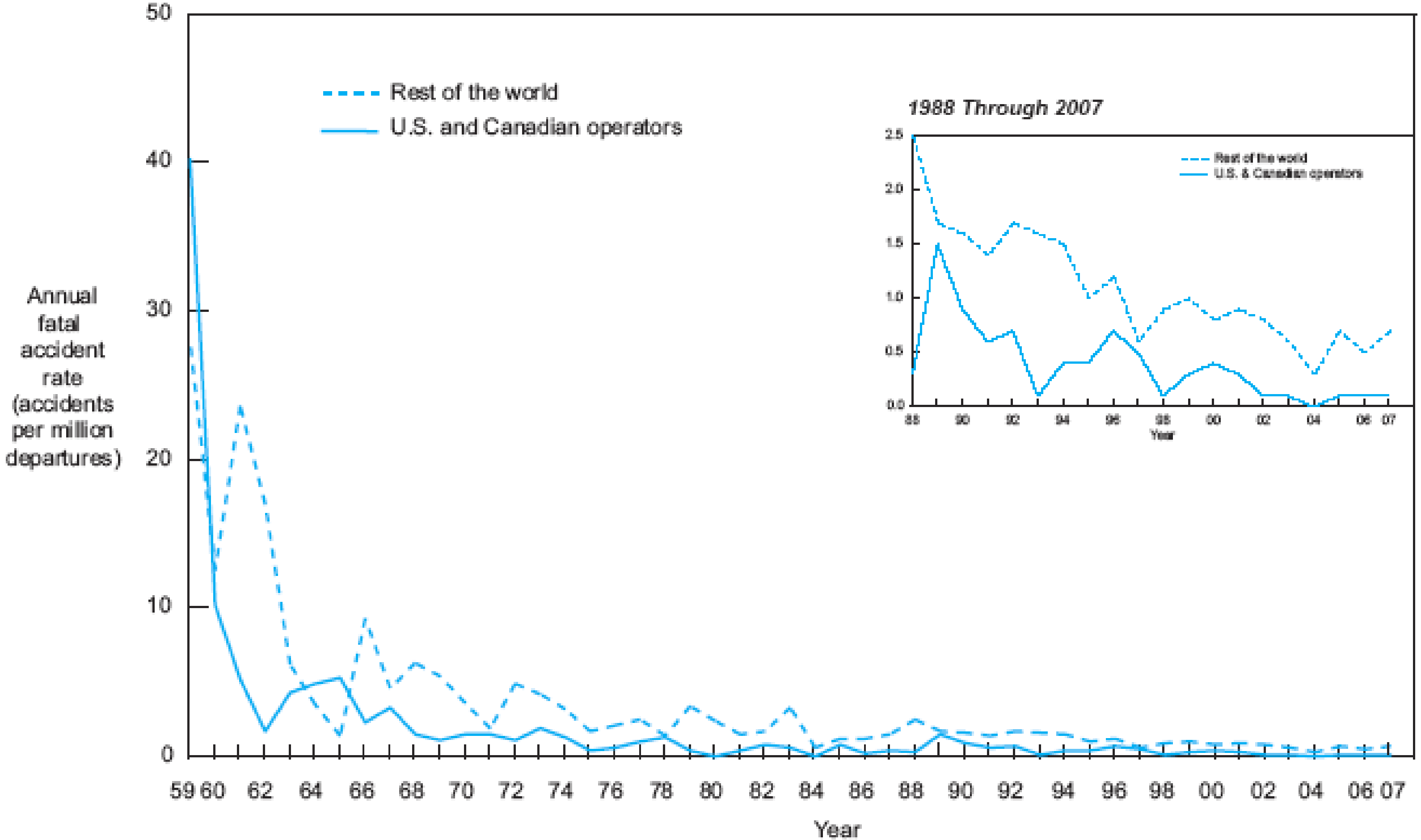
- **Target Level of Safety Expectations**
- **System Complexity**
- **Prognostic vs Forensic Data Analysis**
- **Safety Assurance and Operational Approval**
  - New Systems and Procedures
  - Standards
- **Software Development and Certification**
- **High Confidence Human-Systems Integration**

Challenges

- Target Level of Safety Expectations
- System Complexity
- Prognostic vs Forensic Data Analysis
- Safety Assurance and Operational Approval
  - New Systems and Procedures
  - Standards
- Software Development and Certification
- High Confidence Human-Systems Integration

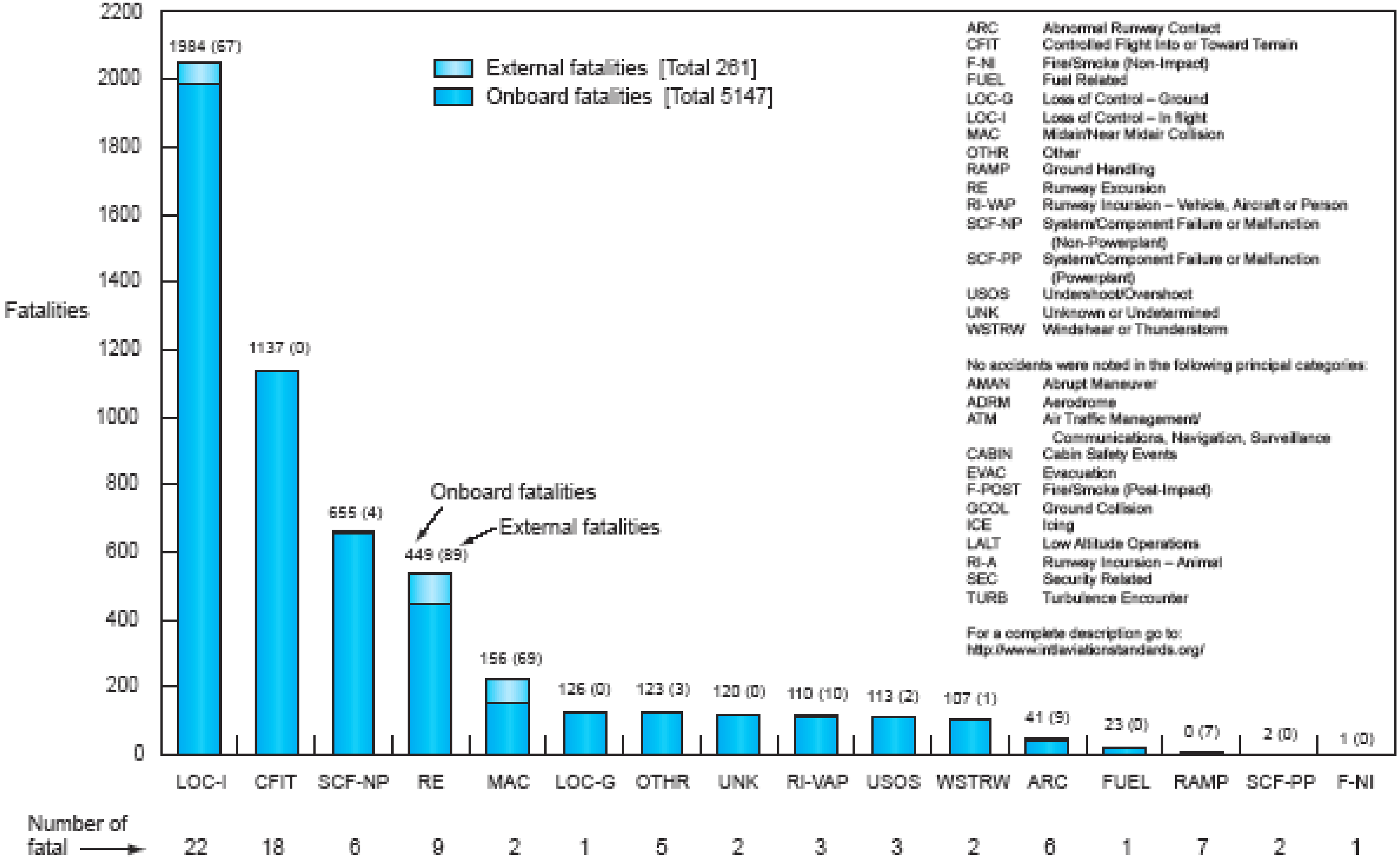
U.S. and Canadian Operators Accident Rates by Year

Fatal Accidents – Worldwide Commercial Jet Fleet – 1959 Through 2007



Fatalities by CAST/ICAO Common Taxonomy Team (CICTT) Aviation Occurrence Categories

Fatal Accidents – Worldwide Commercial Jet Fleet – 1998 Through 2007

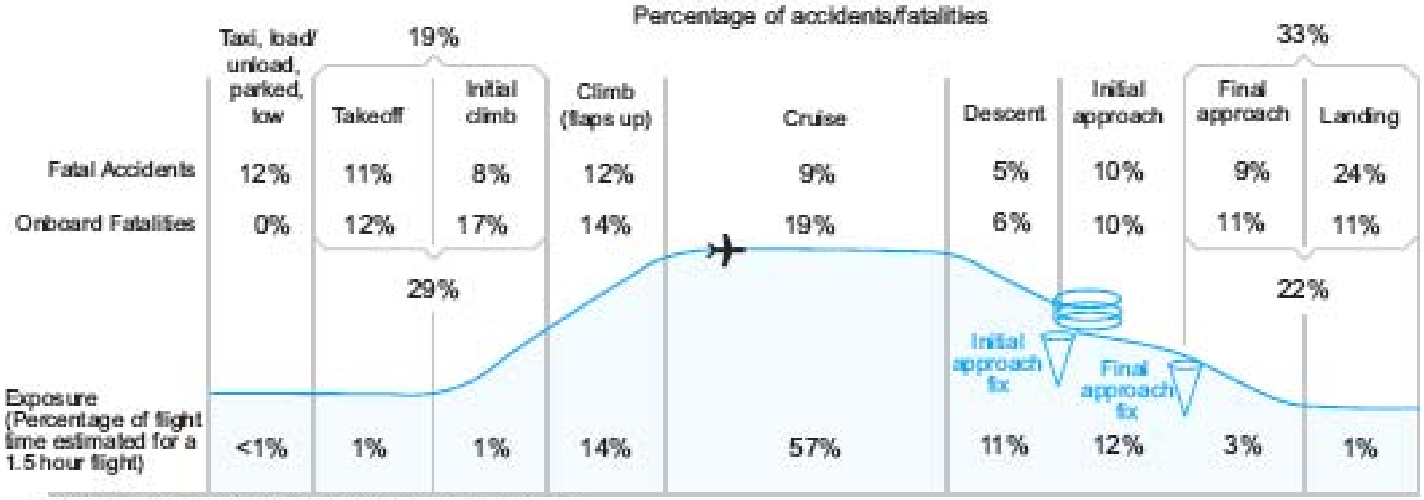


Note: Principal categories as assigned by CAST.

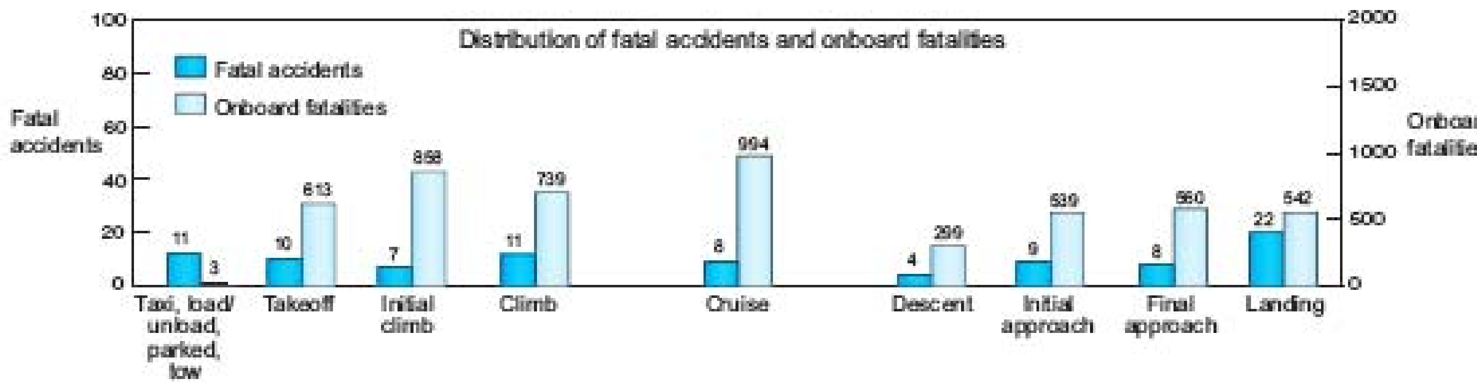
BOEING

Fatal Accidents and Onboard Fatalities by Phase of Flight

Worldwide Commercial Jet Fleet – 1998 Through 2007

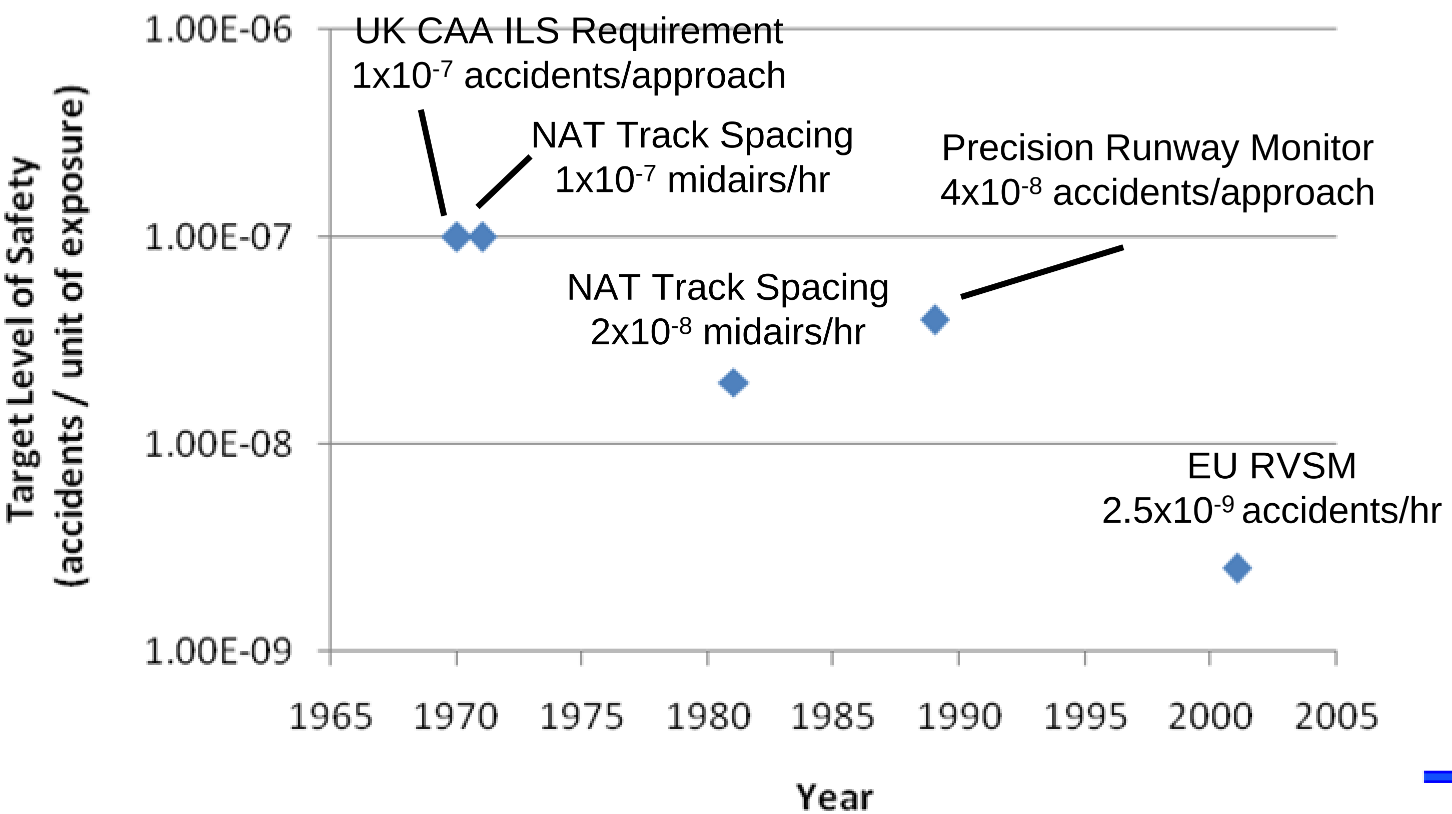


Percentages may not sum to 100% due to numerical rounding.



Increasing Stringency Of Safety Standards

- **Safety targets and assessment process reviewed for past changes**
  - CAA ILS Requirements
  - EU Reduced Vertical Separation Minimums (RVSM)
  - North Atlantic Track (NAT) Separation – (2 cases)
  - Precision Runway Monitor (PRM)



Approaches to Setting the Target Level of Safety

<u>Parity</u>: TLS set equal to the current accident rate

Example: Precision Runway Monitor (PRM)

<u>Extrapolation/Risk Ratio</u>: TLS set by fixed improvement in risk, or continuance of extrapolated risk reduction

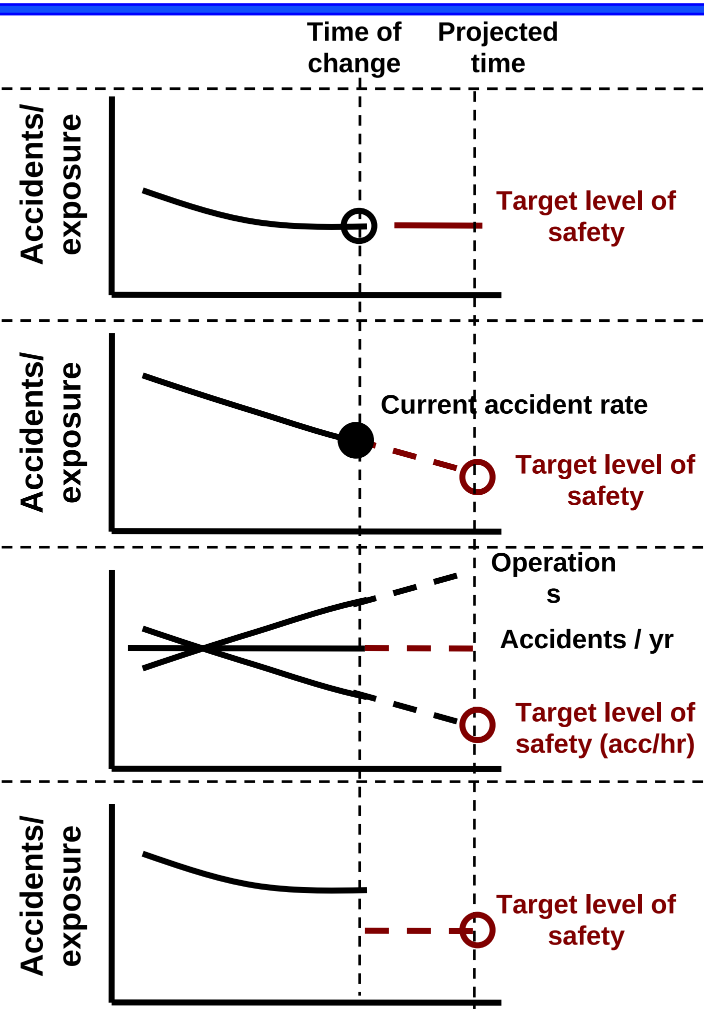
Examples: North Atlantic Longitudinal Spacing, TCAS

<u>Homeostasis</u>: TLS calculated to maintain constant annual accident frequency

Examples: Mineta Commission, SESAR targets

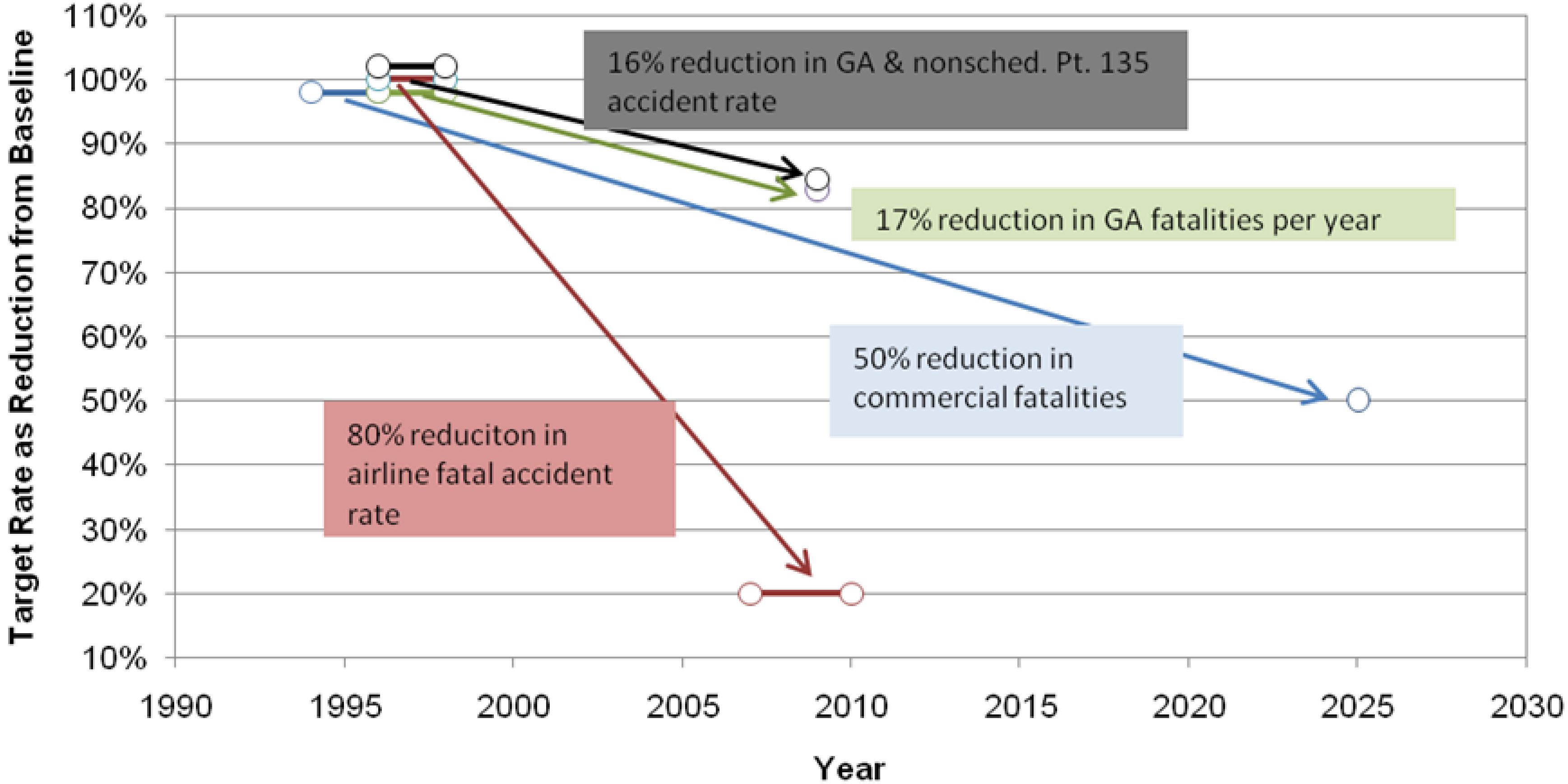
<u>Absolute</u>: TLS set regardless of accident frequencies

Examples: ATO Safety Management System

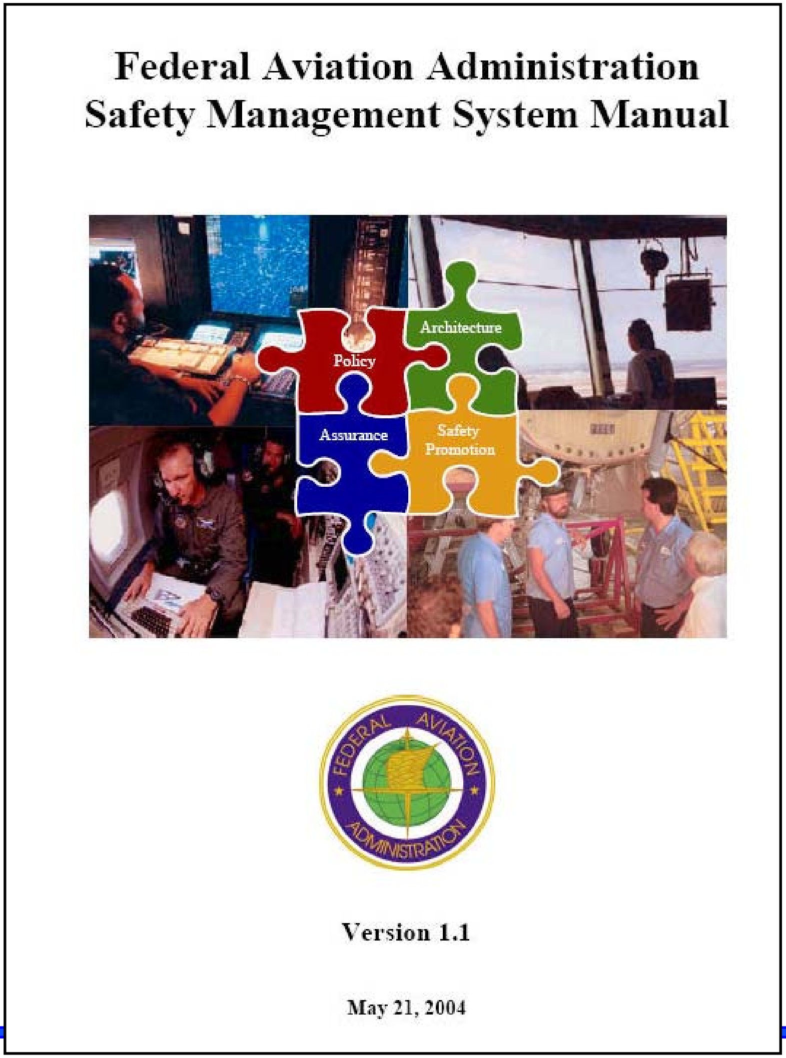


Continued Target Reductions in Accident Rates

2008 AVS Business Plan

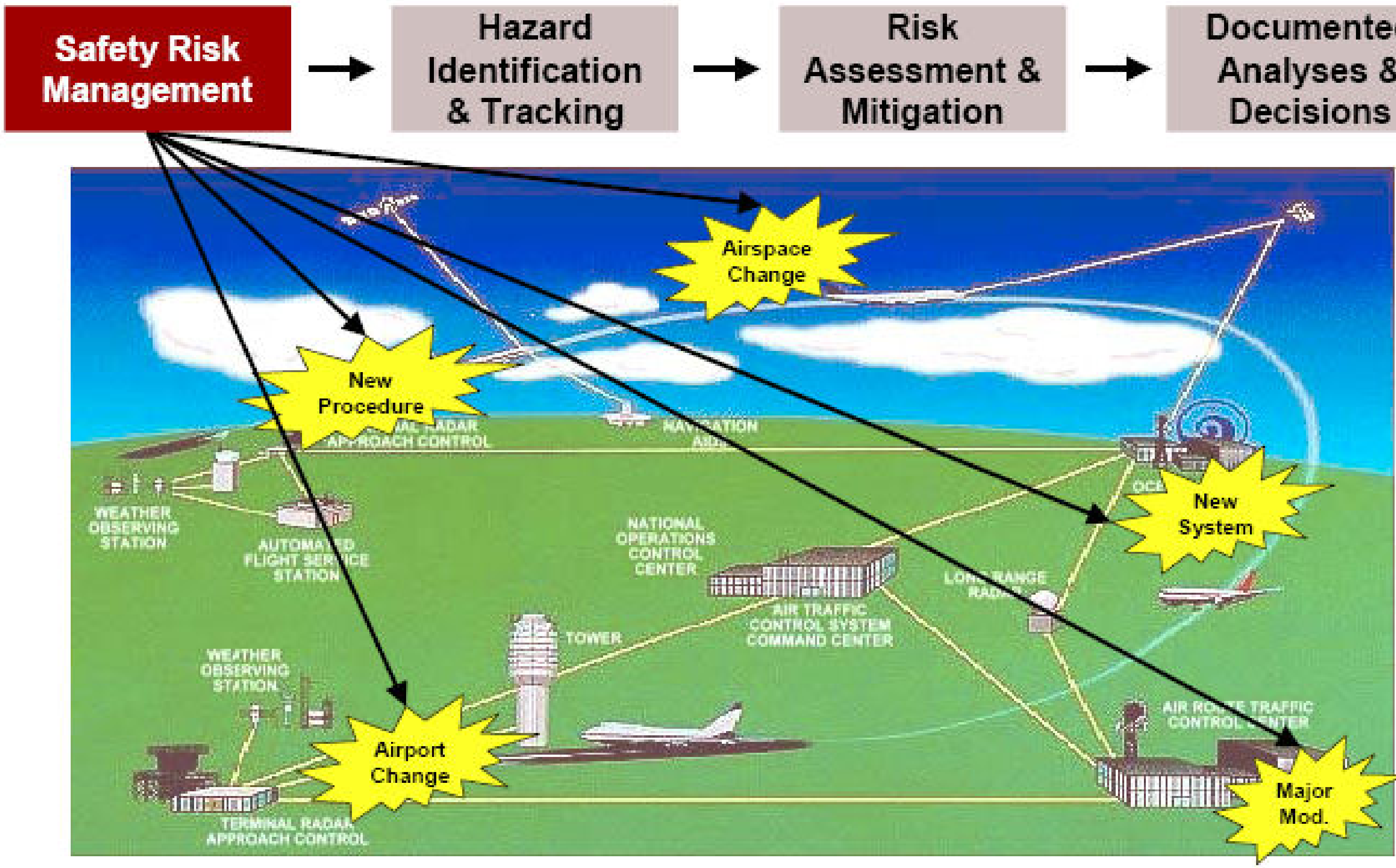


Safety Risk Management



- FAA Safety Management System (SMS)
- Documented Guidelines for Performing Safety Risk Management
- Primarily Directed to ATO Personnel
- Stated Applicability to all systems related to ATC, navigation, and acquisition
- Purpose of Risk Management: A structured process to examine potential causes of accidents and prioritize requirements to mitigate risk to an acceptable level

NAS Change Areas for Analysis of Safety Impacts

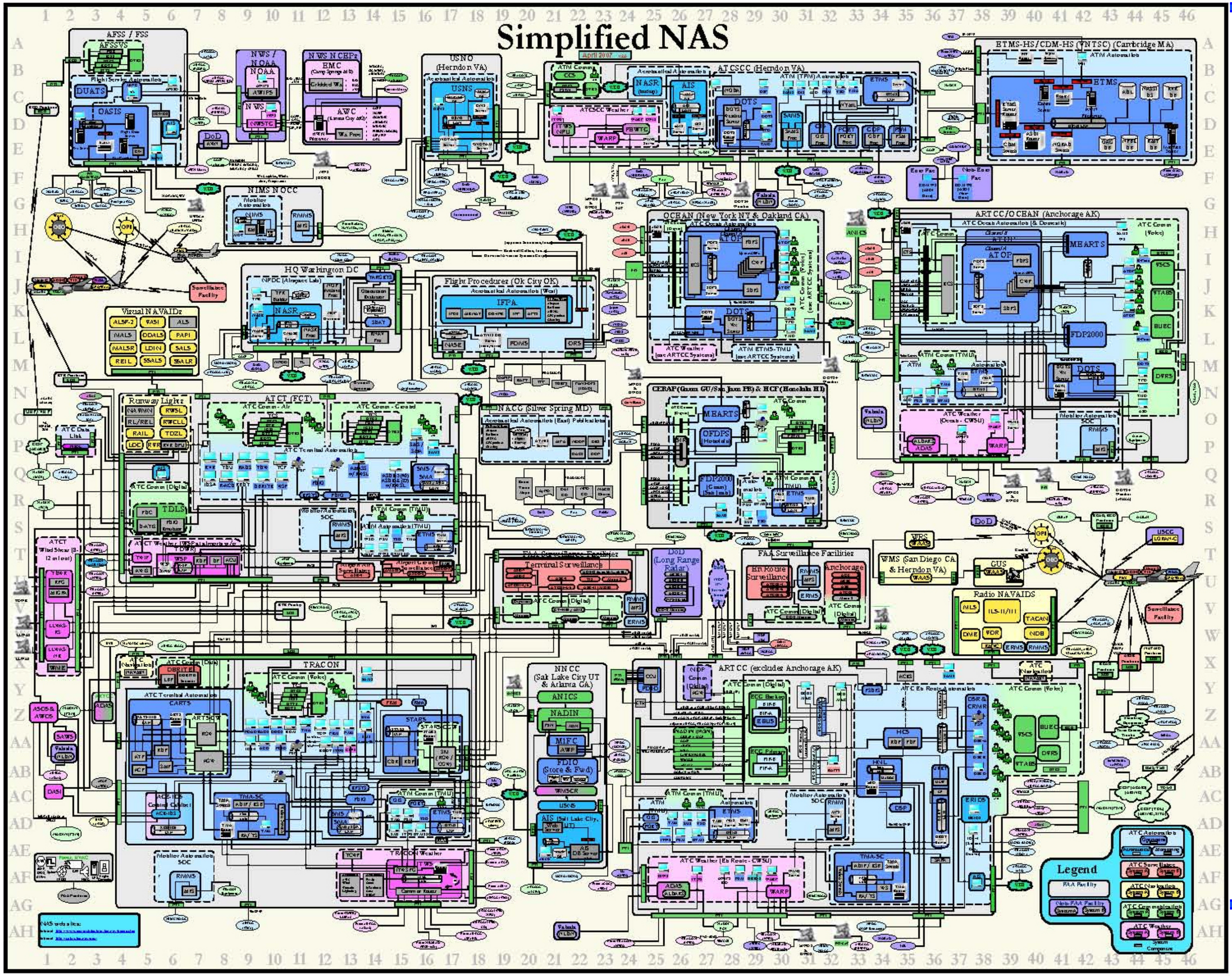


Source: FAA Safety Management System Manual, Version 1.1, May 21, 2004, p. 10.

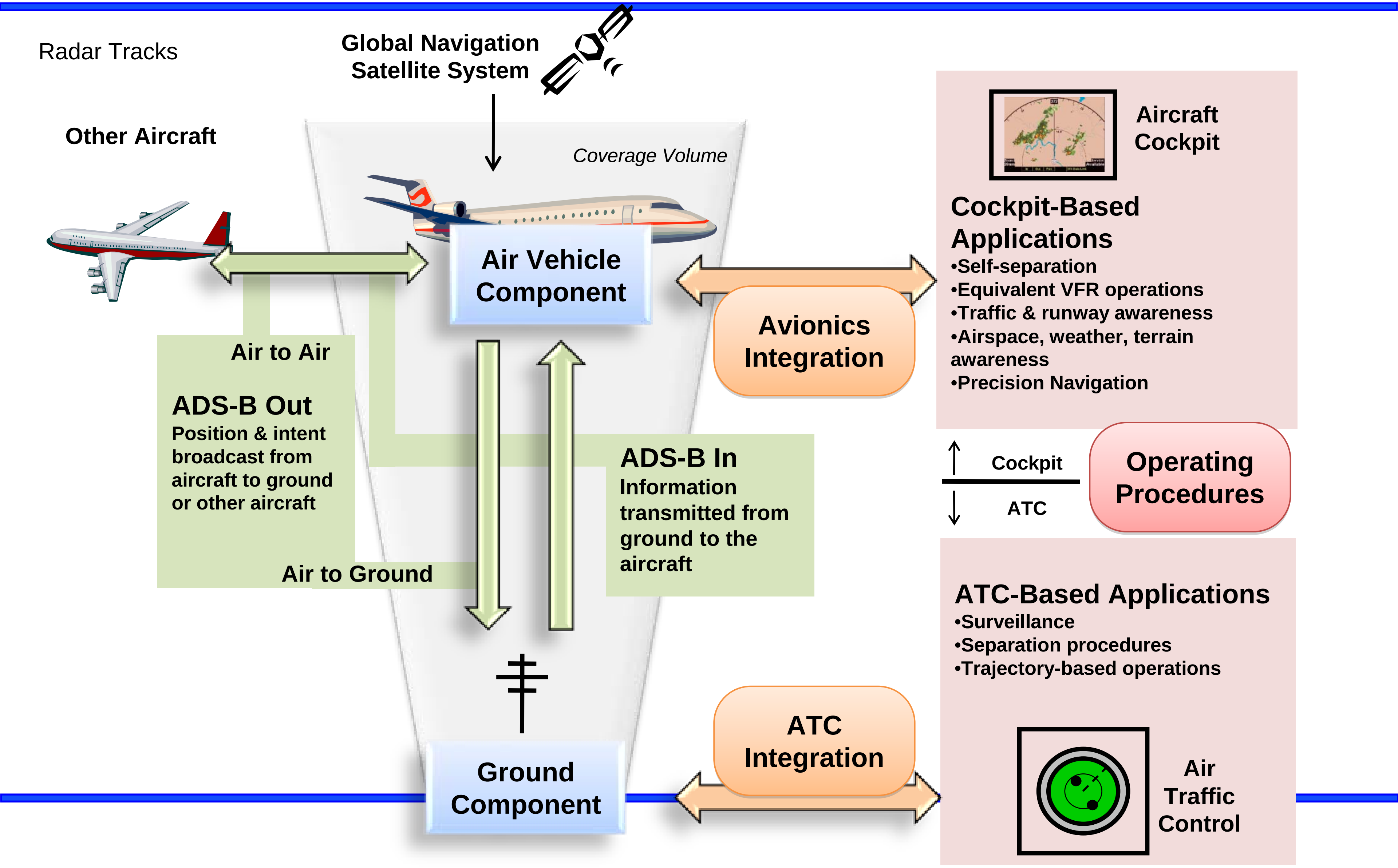
Challenges

- **Target Level of Safety Expectations**
- **System Complexity**
- **Prognostic vs Forensic Data Analysis**
- **Safety Assurance and Operational Approval**
  - New Systems and Procedures
  - Standards
- **Software Development and Certification**
- **High Confidence Human-Systems Integration**

System Complexity
“Simplified” NAS Architecture



Distributed Air-Ground Systems (eg ADS-B)



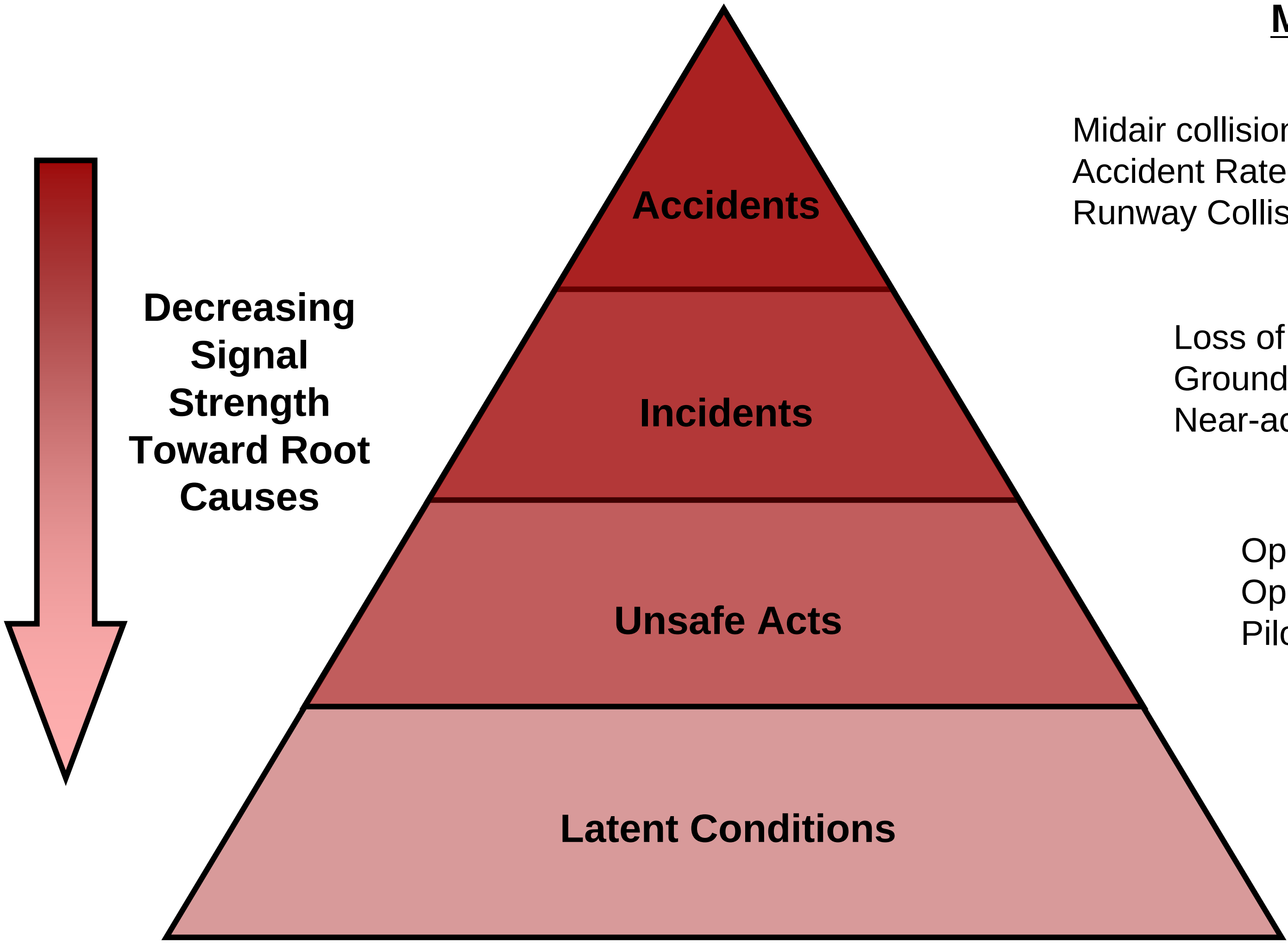
Challenges

- **Target Level of Safety Expectations**
- **System Complexity**
- **Prognostic vs Forensic Data Analysis**
- **Safety Assurance and Operational Approval**
  - New Systems and Procedures
  - Standards
- **Software Development and Certification**
- **High Confidence Human-Systems Integration**

Need for New Approaches to Data Analysis

- **Forensic vs Prognostic Approaches**
- **As safety improves, signals of accident causes weaken**
  - "Paradox of Almost Totally Safe Transportation Systems" – Rene Amalberti
- **Current data approaches are generally based on simple excedance parameters**
  - FOQA – envelope exceedance
  - Operations certificate – procedural non-compliance
- **Current data mining methods are not prognostic**
  - Require hypothesis or identified problem
  - Forensic: after-accident investigation

Accidents and Precursors



Measures

Midair collision rates
Accident Rates
Runway Collisions

Loss of Separation
Ground Incursions
Near-accidents

Operational Errors
Operational Deviations
Pilot Deviations

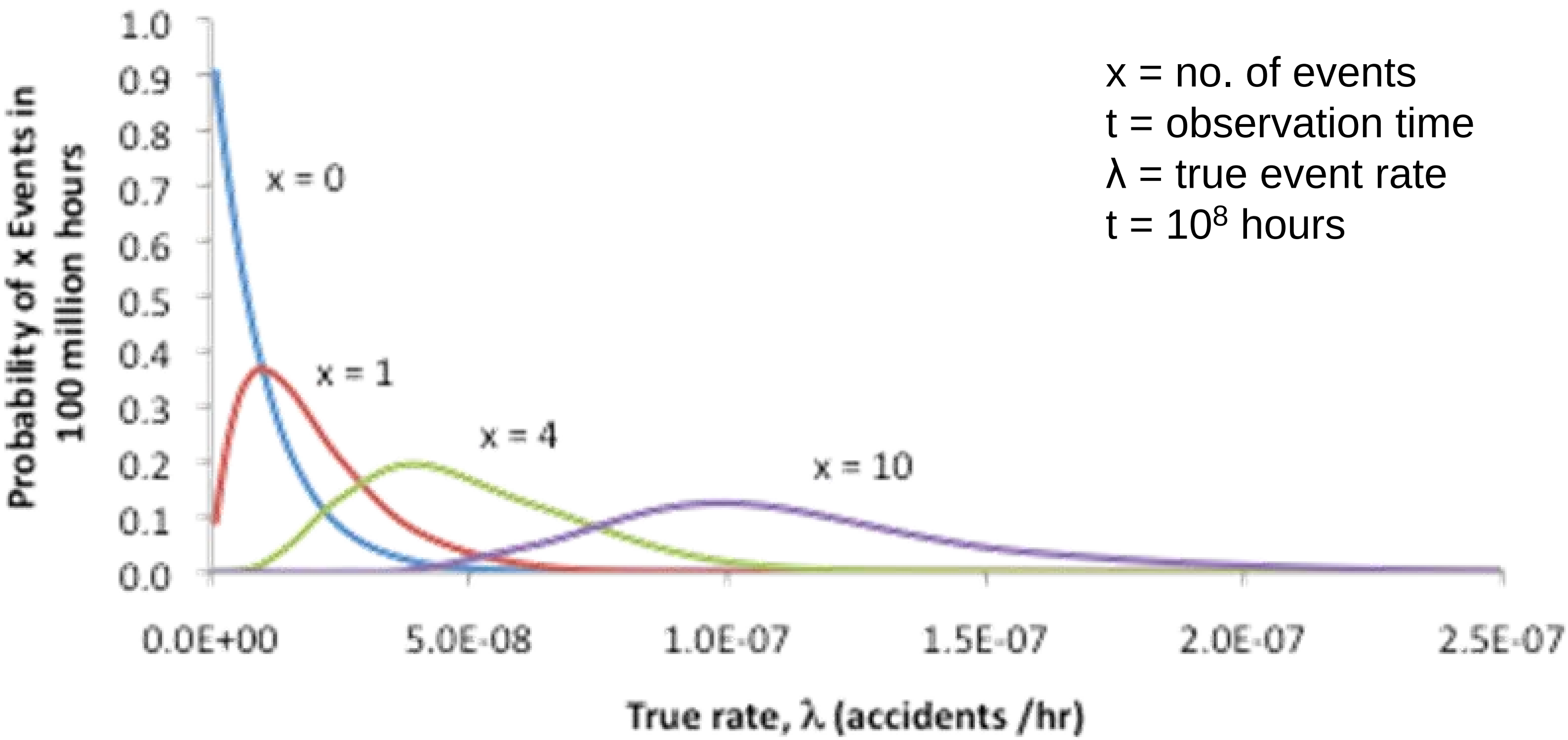
???

Confidence Intervals on Rate of Rare Event

- **Poisson Distribution**: probability *f* of observing *x* events over time *t* if true rate is *λ*
- **Alternate formulation** (after applying Bayes rule): given *x* observed events over time *t*, what is distribution *g* of true rate *λ*?

$$f_X(x \mid \lambda, t) = \frac{(\lambda)^x e^{-\lambda}}{x!}$$

$$g(\lambda \mid x, t) = \frac{(\lambda t)^x e^{-\lambda t}}{x!}$$



x = no. of events
t = observation time
λ = true event rate
t = 10^8 hours

Need for New Approaches to Data Analysis

- **Forensic vs Prognostic Approaches**
- **As safety improves, signals of accident causes weaken**
  - “Paradox of Almost Totally Safe Transportation Systems” – Rene Amalberti
- **Current data approaches are generally based on simple excedance parameters**
  - FOQA – envelope exceedance
  - Operations certificate – procedural non-compliance
- **Current data mining methods are not prognostic**
  - Require hypothesis or identified problem
  - Forensic: after-accident investigation

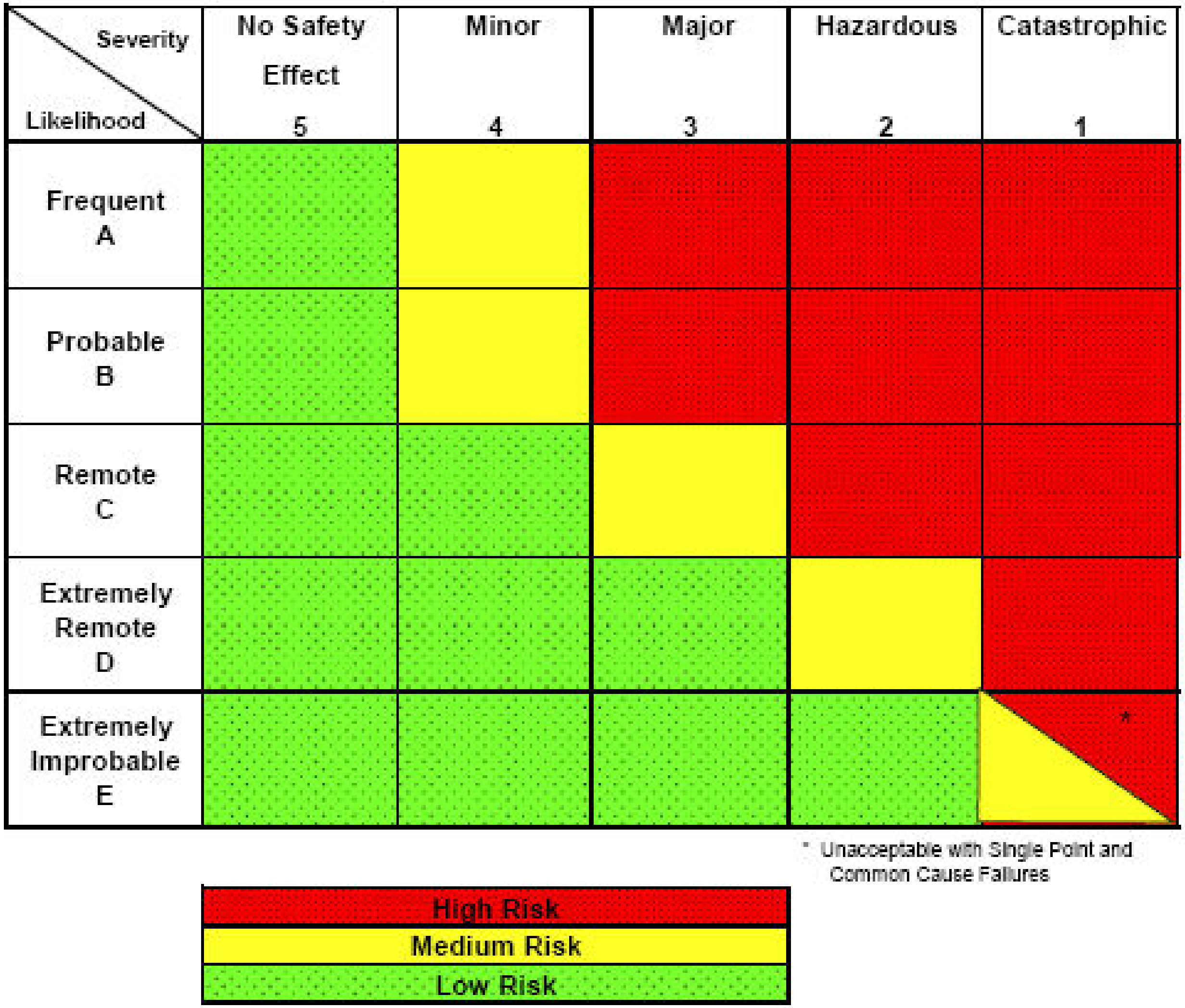
Increasing Set of Potential Data Sources (Multiple Formats)

- **Flight Data Recorder (CVR)**
  - 300 to 1000 states
  - 1/5 to 30 hz
- **Other Electronic Recordings**
  - GPS, FMS, Instrumentation
- **Cockpit Voice Recorder (CVR)**
- **Air Ground Communications**
  - Voice, Data
- **Trajectory Data**
  - Radar, Multilateration, ADS-B
- **Self Reports**
  - Pilots, Controllers, Mechanics
  - ASAS, NASA ASRS
- **Accident, Incident Reports**
- **Dispatch and Weather Data**
- **Maintenance Data**
  - Performance Tracking Data
  - Logbook writeups
- **Aircrew Data**
  - Medical
  - Perfornece
  - Rest
- **Developmental Test Data**
- **Video**
- **Oversight**
  - Air Carrier Oversight (ATOS)

Challenges

- **Target Level of Safety Expectations**
- **System Complexity**
- **Prognostic vs Forensic Data Analysis**
- **Safety Assurance and Operational Approval**
  - New Systems and Procedures
  - Standards
- **Software Development and Certification**
- **High Confidence Human-Systems Integration**

Severity/Likelihood Measure of Risk



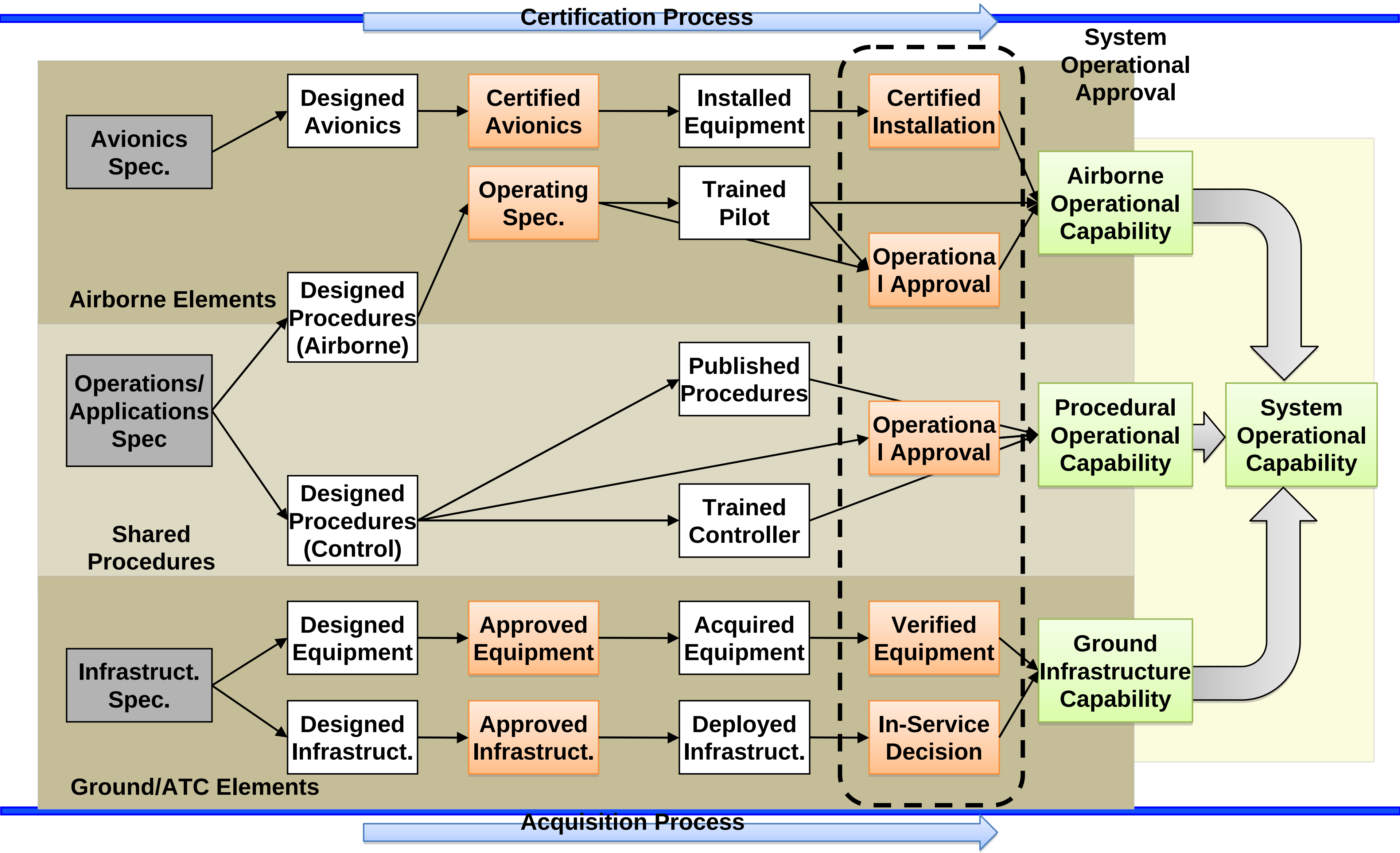
From SMS:

- **High Risk- Unacceptable**
- **Medium Risk- Minimum Acceptable**
- **Low Risk- Target**

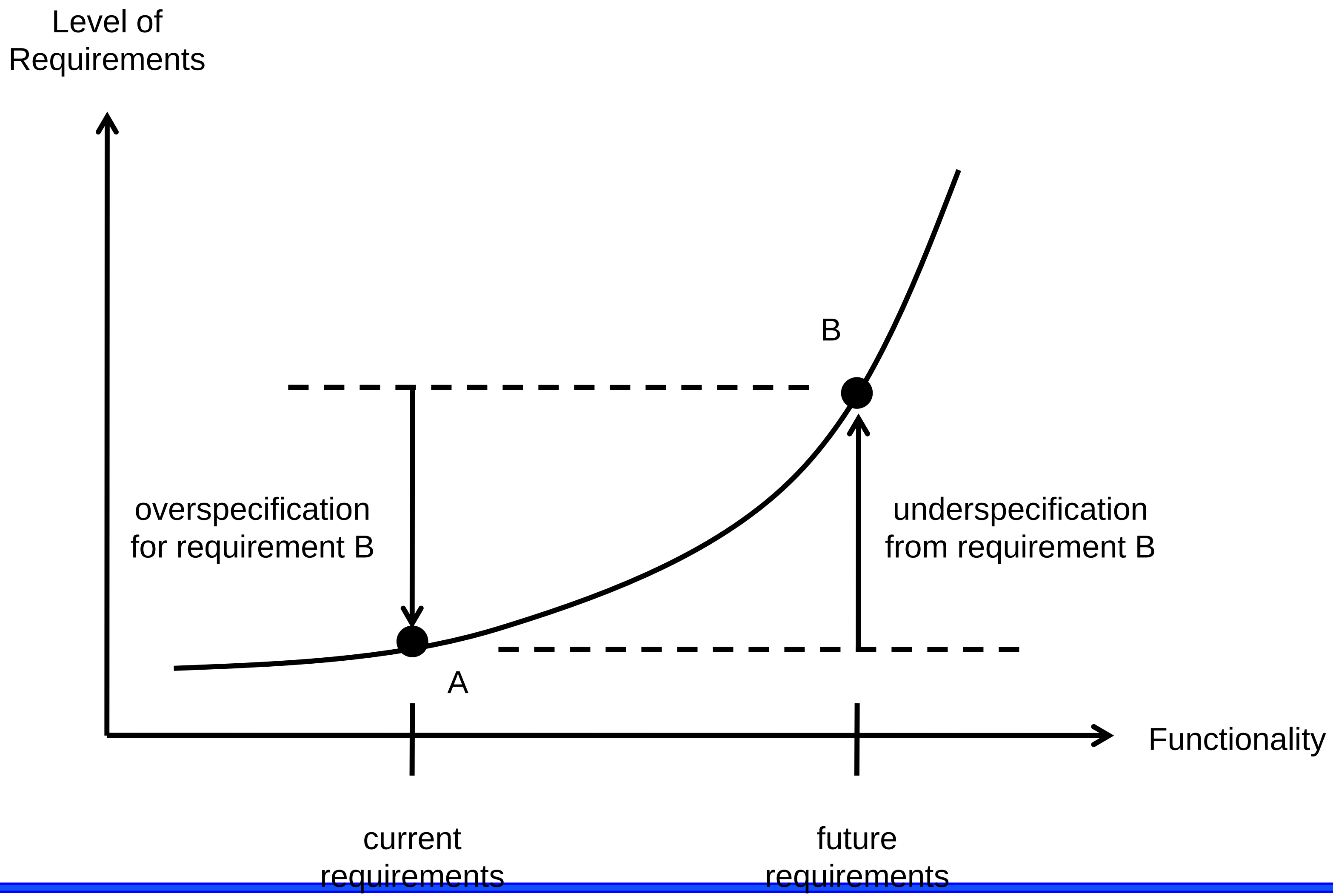
*Source: FAA Safety Management System Manual, Version 1.1, May 21, 2004, p. 45.

Simplified Set of States Required to Achieve Operational Capability

General Air/Ground Integrated System



Level of Requirements for Future Functionality



Challenges

- **Target Level of Safety Expectations**
- **System Complexity**
- **Prognostic vs Forensic Data Analysis**
- **Safety Assurance and Operational Approval**
  - New Systems and Procedures
  - Standards
- **Software Development and Certification**
- **High Confidence Human-Systems Integration**

CNS/ATM Software Assurance Based on Risk

CNS/ATM SWAL Assignment Matrix

LIKELIHOOD OF OCCURRENCE

SEVERITY

	No Safety Effect	Minor	Major	Hazardous	Catastrophic
Probable (Note: 2)	AL 6/E	AL 5/D	AL 3/C	AL 2/B	AL 1/A
Frequent	AL 6/E	AL 5/D	AL 3/C	AL 2/B	AL 1/A
Remote	AL 6	AL 5	AL 4	AL 3	AL 2
Extremely Remote	AL 6	AL 5	AL 4	AL 4	AL 3
Extremely Improbable	AL 6	AL 6	AL 5	AL 5	AL 4

- Software assurance is often used to control risk by mitigating anomalous software behavior.
- Software assurance provides the confidence and artifacts to ensure the system safety requirements implemented in software function as designed.

Note:

1. *Minimally recommended SW assurance levels based on system risk, any deviation must be pre-approved by the appropriate approval/certification authority.*
2. *DO-278 equates to DO-178B for SW whose functionality has a direct impact on aircraft operations (e.g., ILS, WAAS).*

From FAA System Safety Management Program Manual, December 2004, p.42

DO-178B Software Design Assurance Levels (DALs)

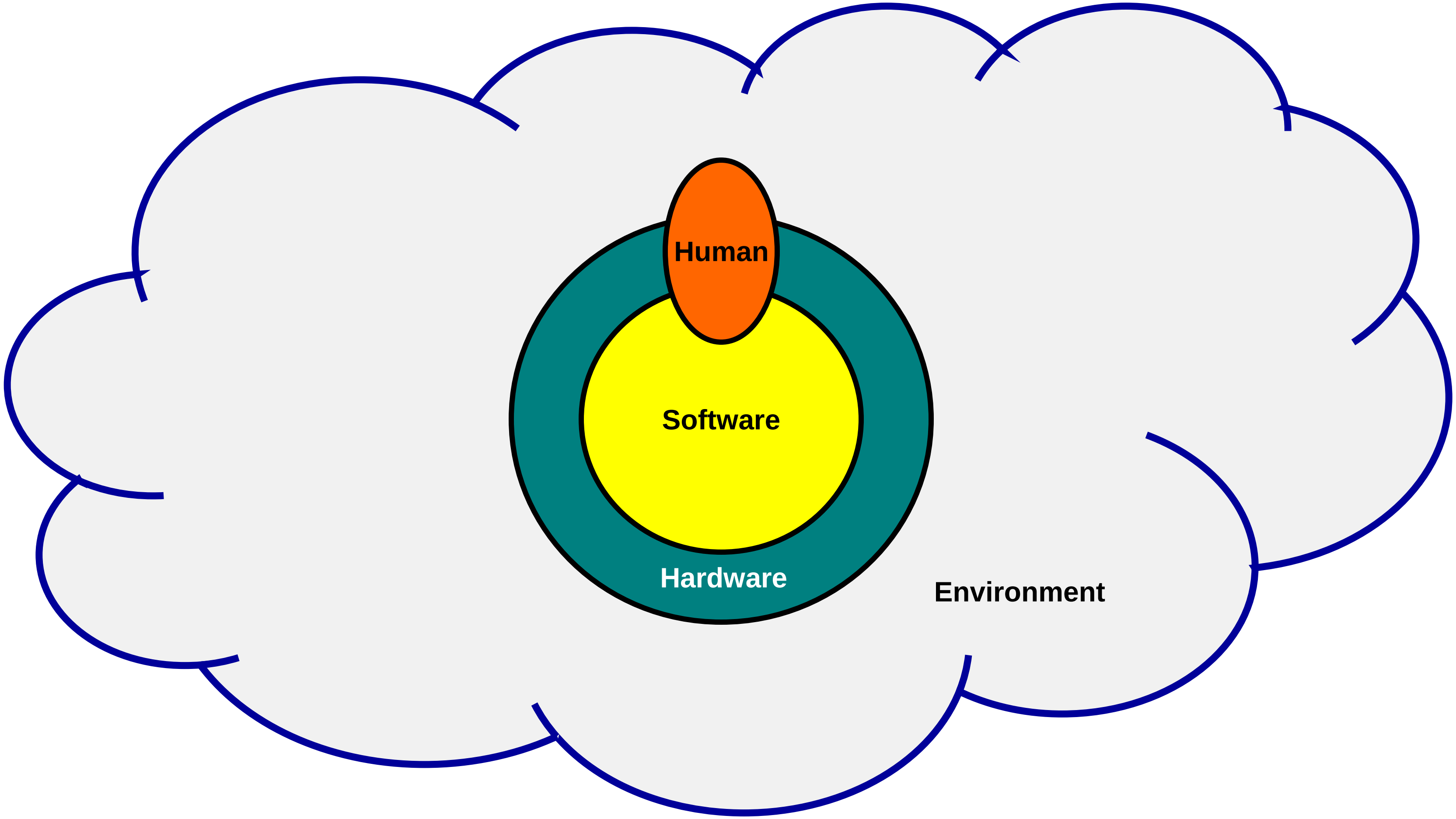
Level	Failure condition	Objectives	With independence
A	Catastrophic	66	25
B	Hazardous	65	14
C	Major	57	2
D	Minor	28	2
E	No effect	0	0

- **De facto standard for certification of safety-critical software systems**
- **Currently in update: DO-178C**

Challenges

- **Target Level of Safety Expectations**
- **System Complexity**
- **Prognostic vs Forensic Data Analysis**
- **Safety Assurance and Operational Approval**
  - New Systems and Procedures
  - Standards
- **Software Development and Certification**
- **High Confidence Human-Systems Integration**

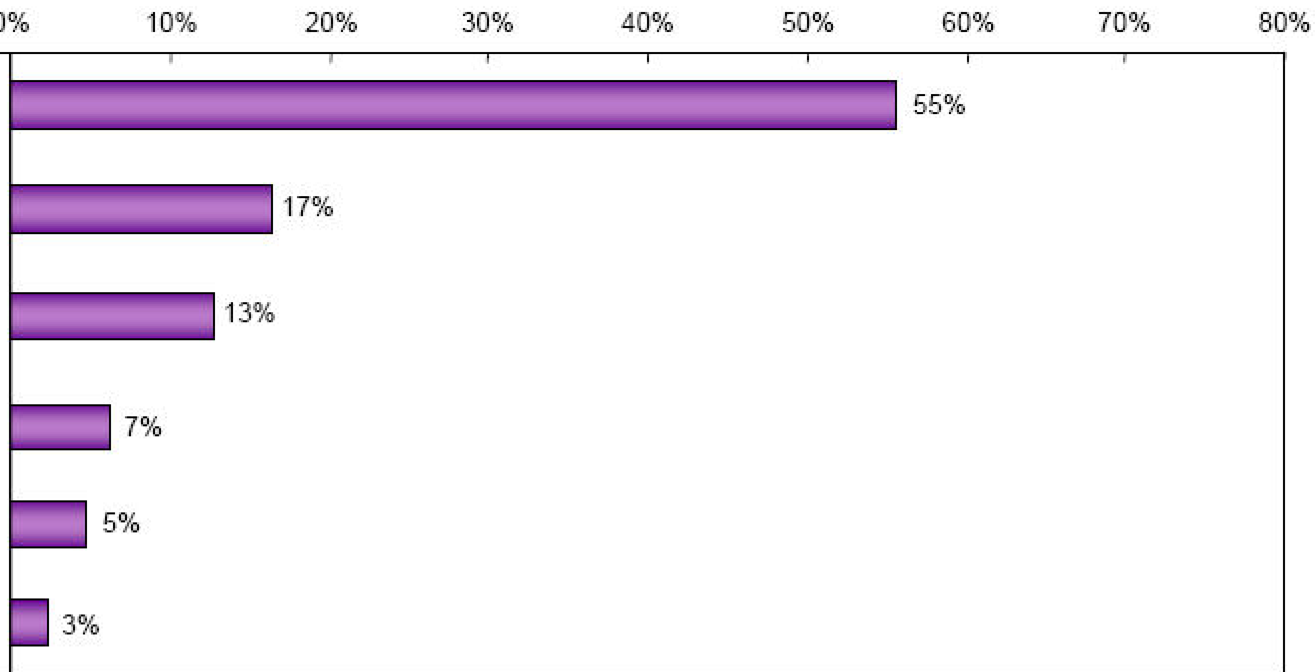
Need to Consider Entire System



Accidents by Primary Cause*

Hull Loss Accidents – Worldwide Commercial Jet Fleet – 1996 through 2005

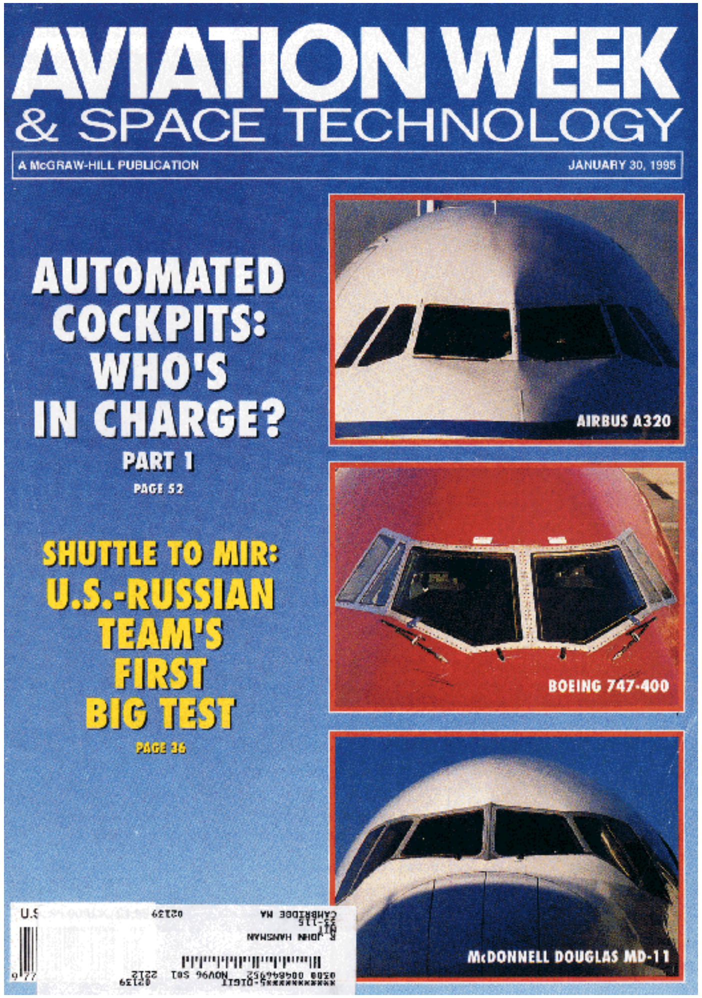
Flight Crew	74
Airplane	23
Weather	17
Misc./Other	10
Airport/Air Traffic Control	6
Maintenance	4
Total with known causes	134
Unknown or awaiting reports	49
Total	183



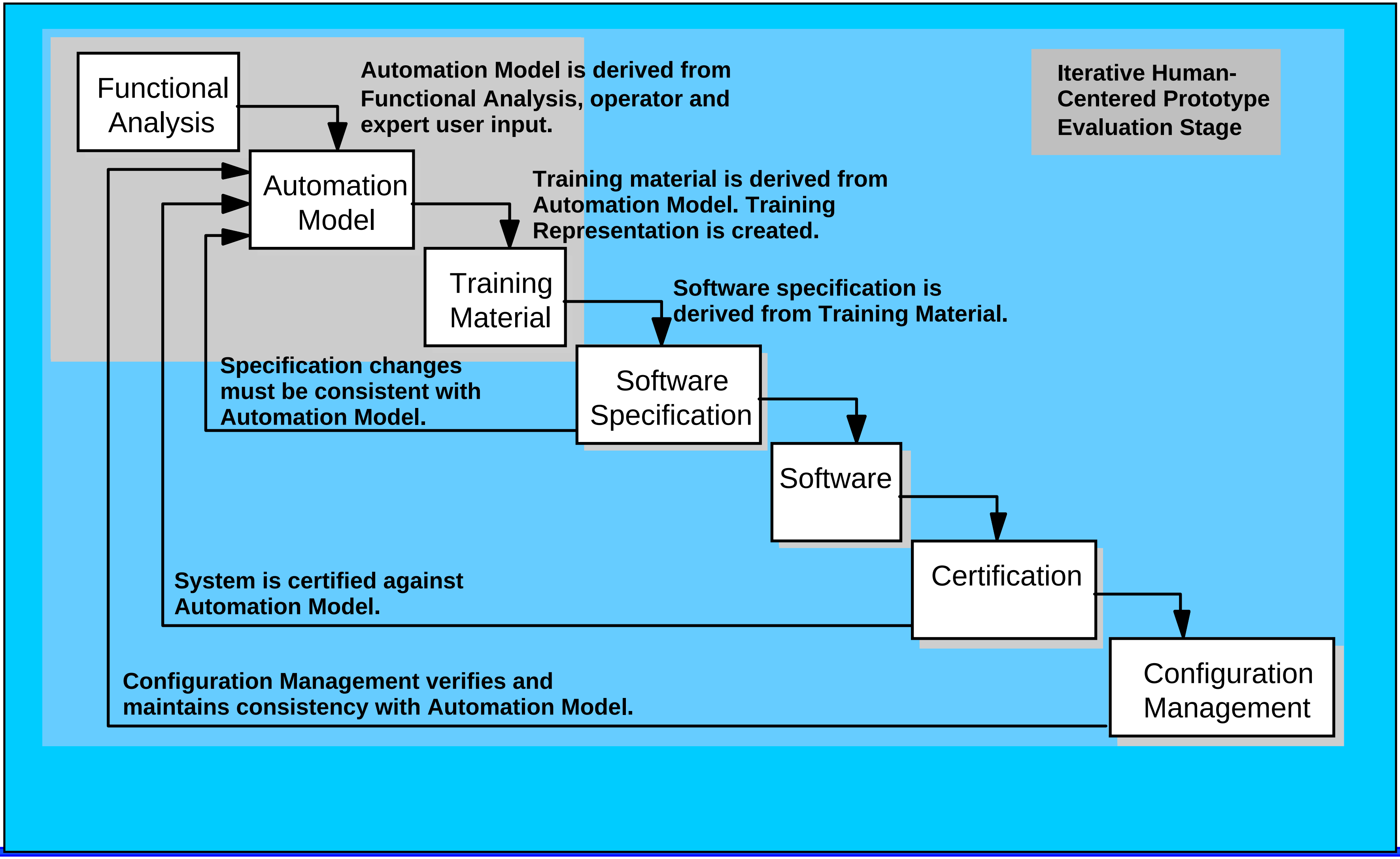
*As determined by the investigating authority, percent of accidents with known causes.

Mode Awareness

- ***Mode Awareness* is becoming a serious issues in Complex Automation Systems**
  - automation executes an unexpected action (commission), or fails to execute an action (omission) that is anticipated or expected by one or more of the pilots
- **Multiple accidents and incidents**
  - Strasbourg A320 crash: incorrect vertical mode selection
  - Orly A310 violent pitchup: flap overspeed
  - B757 speed violations: early leveloff conditions
- **Pilot needs to**
  - Identify current state of automation
  - Understand implications of current state
  - Predict future states of automation



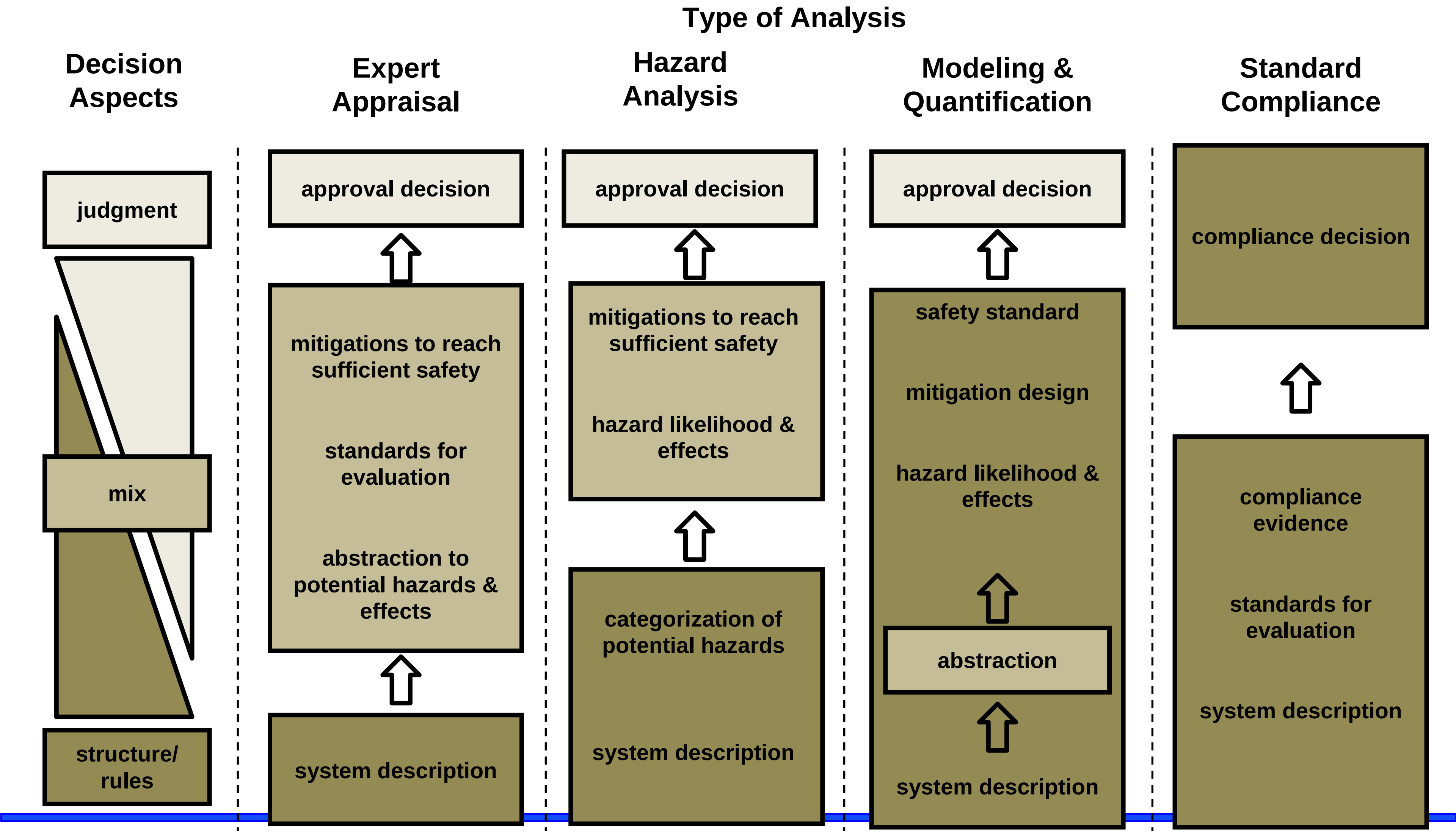
Operator Directed Process



Challenges

- **Target Level of Safety Expectations**
- **System Complexity**
- **Prognostic vs Forensic Data Analysis**
- **Safety Assurance and Operational Approval**
  - New Systems and Procedures
  - Standards
- **Software Development and Certification**
- **High Confidence Human-Systems Integration**

Spectrum of Judgment in Approval Process Steps

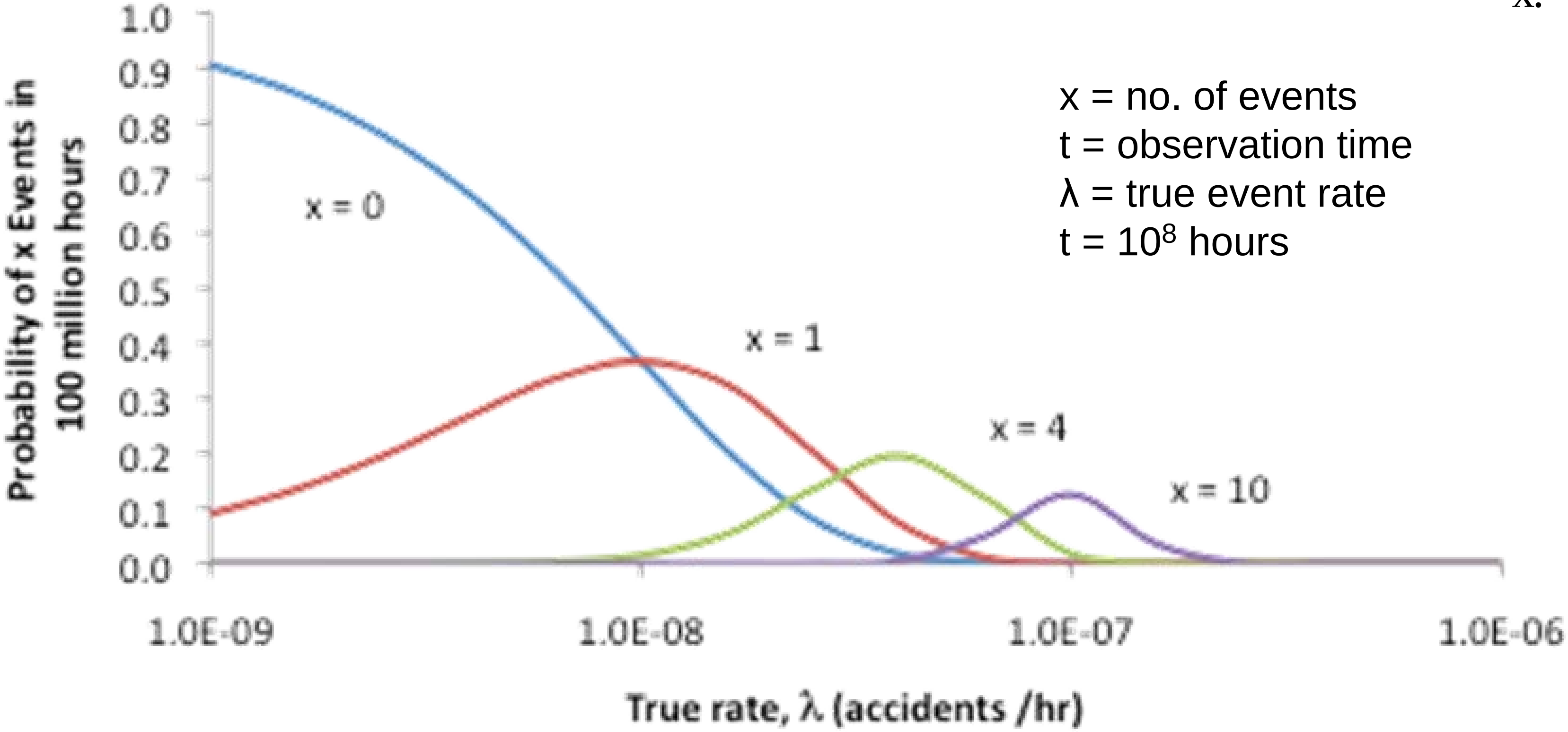


Confidence Intervals on Rate of Rare Event

- **Poisson Distribution**: probability *f* of observing *x* events over time *t* if true rate is *λ*
- **Alternate formulation** (after applying Bayes rule): given *x* observed events over time *t*, what is distribution *g* of true rate *λ*?

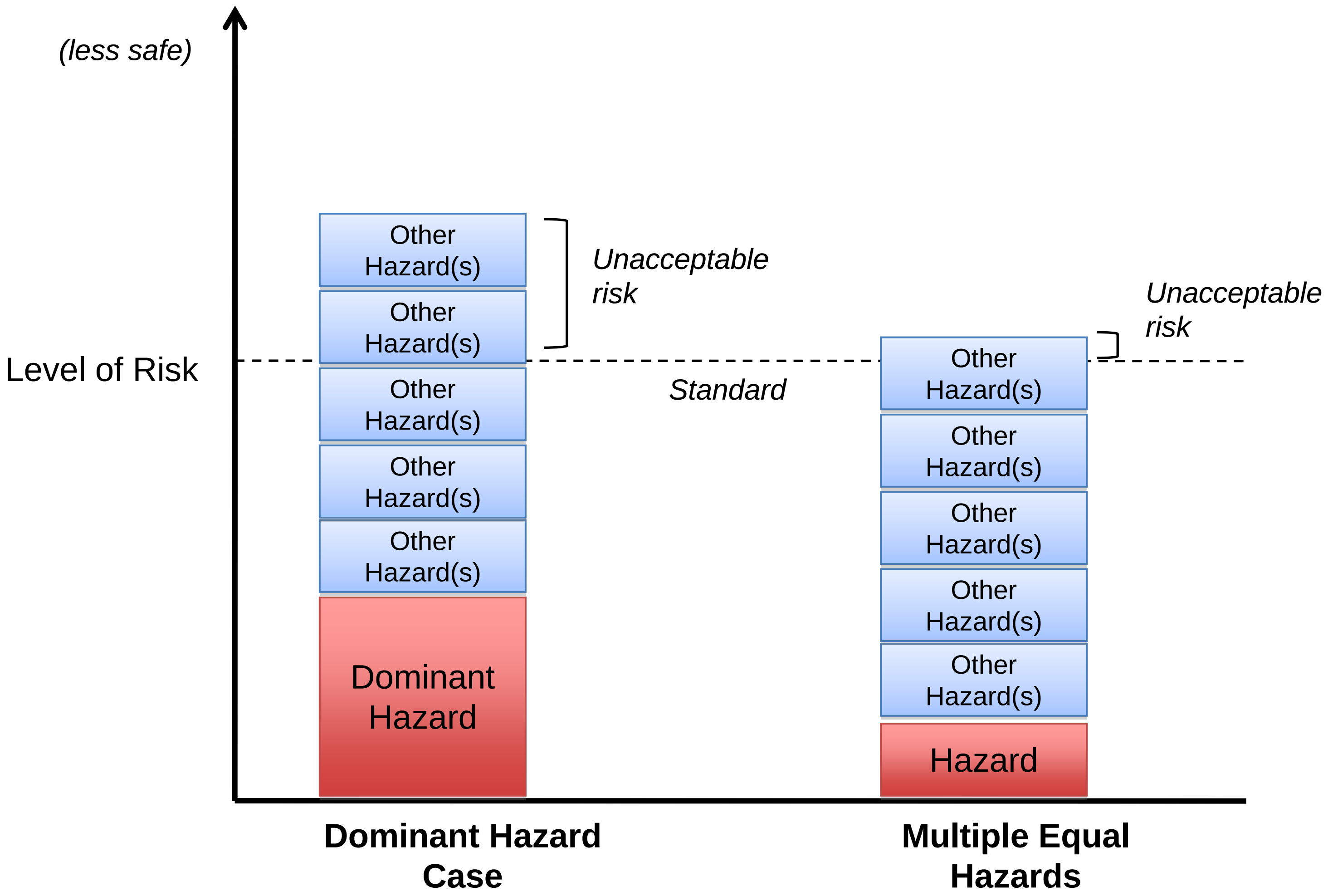
$$f_X(x \mid \lambda, t) = \frac{(\lambda)^x e^{-\lambda}}{x!}$$

$$g(\lambda \mid x, t) = \frac{(\lambda t)^x e^{-\lambda t}}{x!}$$



x = no. of events
t = observation time
λ = true event rate
t = 10^8 hours

Addressing Multiple Hazards in System



All hazards of equal severity, therefore likelihood combines to overall level of risk