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


No accidents were noted in the following principal categories:
- AMAN Abrupt Maneuver
- ADRM Aerodrome
- ATM Air Traffic Management
- CABIN Cabin Safety Events
- EVAC Evacuation
- F-POST Fire/Smoke (Post-Impact)
- GCOL Ground Collision
- ICE Icing
- LALT Low Altitude Operations
- RS-A Runway Incursion – Aircraft
- SEC Security Related
- TURB Turbulence Encounter

For a complete description go to:
http://www.internationalstandards.org/

Note: Principal categories as assigned by CAST.
Fatal Accidents and Onboard Fatalities by Phase of Flight

Percentage of accidents/fatalities

<table>
<thead>
<tr>
<th>Phase of Flight</th>
<th>Fatal Accidents</th>
<th>Onboard Fatalities</th>
</tr>
</thead>
<tbody>
<tr>
<td>Taxi, load/unload</td>
<td>12%</td>
<td>0%</td>
</tr>
<tr>
<td>Initial climb</td>
<td>11%</td>
<td>12%</td>
</tr>
<tr>
<td>Climb (flaps up)</td>
<td>8%</td>
<td>17%</td>
</tr>
<tr>
<td>Cruise</td>
<td>12%</td>
<td>14%</td>
</tr>
<tr>
<td>Descent</td>
<td>9%</td>
<td>19%</td>
</tr>
<tr>
<td>Initial approach</td>
<td>5%</td>
<td>6%</td>
</tr>
<tr>
<td>Final approach</td>
<td>10%</td>
<td>10%</td>
</tr>
<tr>
<td>Landing</td>
<td>9%</td>
<td>11%</td>
</tr>
</tbody>
</table>

Exposure
(Percentage of flight time estimated for a 1.5 hour flight)

<table>
<thead>
<tr>
<th>Phase of Flight</th>
<th>&lt;1%</th>
<th>1%</th>
<th>1%</th>
<th>14%</th>
<th>57%</th>
<th>11%</th>
<th>12%</th>
<th>3%</th>
<th>1%</th>
</tr>
</thead>
<tbody>
<tr>
<td>Taxi, load/unload</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Initial climb</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Climb (flaps up)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cruise</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Descent</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Initial approach</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Final approach</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Landing</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Distribution of fatal accidents and onboard fatalities

Boeing

2007 STATISTICAL SUMMARY, JULY 2008
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)

![Graph showing the history of safety targets from 1965 to 2005. The graph includes the following points:

- UK CAA ILS Requirement: 1x10^-7 accidents/approach
- NAT Track Spacing: 1x10^-7 midairs/hr
- NAT Track Spacing: 2x10^-8 midairs/hr
- Precision Runway Monitor: 4x10^-8 accidents/approach
- EU RVSM: 2.5x10^-9 accidents/hr]
## Approaches to Setting the Target Level of Safety

<table>
<thead>
<tr>
<th>Approach</th>
<th>Description</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Parity</strong></td>
<td>TLS set equal to the current accident rate</td>
<td>Precision Runway Monitor (PRM)</td>
</tr>
<tr>
<td><strong>Extrapolation/Risk Ratio</strong></td>
<td>TLS set by fixed improvement in risk, or continuance of extrapolated risk reduction</td>
<td>North Atlantic Longitudinal Spacing, TCAS</td>
</tr>
<tr>
<td><strong>Homeostasis</strong></td>
<td>TLS calculated to maintain constant annual accident frequency</td>
<td>Mineta Commission, SESAR targets</td>
</tr>
<tr>
<td><strong>Absolute</strong></td>
<td>TLS set regardless of accident frequencies</td>
<td>ATO Safety Management System</td>
</tr>
</tbody>
</table>
Continued Target Reductions in Accident Rates

2008 AVS Business Plan

- 16% reduction in GA & nonsched. Pt. 135 accident rate
- 17% reduction in GA fatalities per year
- 80% reduction in airline fatal accident rate
- 50% reduction in commercial fatalities
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

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)

**ATC-Based Applications**
- Surveillance
- Separation procedures
- Trajectory-based operations

**Cockpit-Based Applications**
- Self-separation
- Equivalent VFR operations
- Traffic & runway awareness
- Airspace, weather, terrain awareness
- Precision Navigation

**Air Vehicle Component**
- Avionics Integration
- ADS-B Out
  - Position & intent broadcast from aircraft to ground or other aircraft
- ADS-B In
  - Information transmitted from ground to the aircraft

**Ground Component**
- ATC Integration
- Radar Tracks

**Global Navigation Satellite System**

**Operation Procedures**
- Aircraft Cockpit
- ATC

**Other Aircraft**
- Air to Air
- Air to Ground
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 exceedance 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

- Accidents
- Incidents
- Unsafe Acts
- Latent Conditions

Measures

- Midair collision rates
- Accident Rates
- Runway Collisions
- Loss of Separation
- Ground Incursions
- Near-accidents
- Operational Errors
- Operational Deviations
- Pilot Deviations

Decreasing Signal Strength Toward Root Causes

Modified from H.W. Heinrich, *Industrial Accident Prevention*, 1931
Confidence Intervals on Rate of Rare Event

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

\[
f_x(x | \lambda, t) = \frac{(\lambda)^x e^{-\lambda}}{x!}
\]

\[
g(\lambda | x, t) = \frac{(\lambda t)^x e^{-\lambda t}}{x!}
\]

- $x =$ no. of events
- $t =$ observation time
- $\lambda =$ true event rate
- $t = 10^8$ hours

![Graph showing probability of $x$ Events in 100 million hours vs. True rate $\lambda$ (accidents/hr)]
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
  - Performance
  - 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

<table>
<thead>
<tr>
<th>Severity</th>
<th>No Safety Effect</th>
<th>Minor</th>
<th>Major</th>
<th>Hazardous</th>
<th>Catastrophic</th>
</tr>
</thead>
<tbody>
<tr>
<td>Likelihood</td>
<td>5</td>
<td>4</td>
<td>3</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>Frequent A</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Probable B</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Remote C</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Extremely Remote D</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Extremely Improbable E</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

* Unacceptable with Single Point and Common Cause Failures

From SMS:
- High Risk - Unacceptable
- Medium Risk - Minimum Acceptable
- Low Risk - Target

Simplified Set of States Required to Achieve Operational Capability

Certification Process

- General Air/Ground Integrated System
- Airborne Operational Capability
- Procedural Operational Capability
- System Operational Capability

Avionics Spec.
- Designed Avionics
- Certified Avionics
- Installed Equipment
- Certified Installation
- Operationa l Approval
- Airborne Operational Capability

Airborne Elements
- Designed Procedures (Airborne)
- Operating Spec.
- Trained Pilot
- Operationa l Approval
- Procedural Operational Capability
- System Operational Capability

Operations/Applications Spec
- Designed Procedures (Airborne)
- Operating Spec.
- Trained Controller
- Operationa l Approval
- Procedural Operational Capability
- System Operational Capability

Shared Procedures
- Designed Procedures (Control)
- Published Procedures
- Operationa l Approval
- Procedural Operational Capability
- System Operational Capability

Ground/ATC Elements
- Designed Equipment
- Approved Equipment
- Acquired Equipment
- Verified Equipment
- In-Service Decision
- Ground Infrastructure Capability

Infrastruct. Spec.
- Designed Infrastruct.
- Approved Infrastruct.
- Deployed Infrastruct.
- In-Service Decision
- Ground Infrastructure Capability

Acquisition Process
Level of Requirements for Future Functionality

- overspecification for requirement B
- underspecification from requirement 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
CNS/ATM Software Assurance Based on Risk

<table>
<thead>
<tr>
<th>SEVERITY</th>
<th>LIKELIHOOD OF OCCURRENCE</th>
<th>AL 6/E</th>
<th>AL 5/D</th>
<th>AL 3/C</th>
<th>AL 2/B</th>
<th>AL 1/A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Extremely Improbable</td>
<td>Extremely Remote</td>
<td>AL 6</td>
<td>AL 5</td>
<td>AL 4</td>
<td>AL 4</td>
<td>AL 3</td>
</tr>
<tr>
<td>Extremely Improbable</td>
<td>Frequent</td>
<td>AL 6/E</td>
<td>AL 5/D</td>
<td>AL 3/C</td>
<td>AL 2/B</td>
<td>AL 1/A</td>
</tr>
<tr>
<td>Extremely Improbable</td>
<td>Probable (Note: 2)</td>
<td>AL 6/E</td>
<td>AL 5/D</td>
<td>AL 3/C</td>
<td>AL 2/B</td>
<td>AL 1/A</td>
</tr>
<tr>
<td>No Safety Effect</td>
<td>Minor</td>
<td>AL 6/E</td>
<td>AL 5/D</td>
<td>AL 3/C</td>
<td>AL 2/B</td>
<td>AL 1/A</td>
</tr>
</tbody>
</table>

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).

## DO-178B Software Design Assurance Levels (DALs)

<table>
<thead>
<tr>
<th>Level</th>
<th>Failure condition</th>
<th>Objectives</th>
<th>With independence</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>Catastrophic</td>
<td>66</td>
<td>25</td>
</tr>
<tr>
<td>B</td>
<td>Hazardous</td>
<td>65</td>
<td>14</td>
</tr>
<tr>
<td>C</td>
<td>Major</td>
<td>57</td>
<td>2</td>
</tr>
<tr>
<td>D</td>
<td>Minor</td>
<td>28</td>
<td>2</td>
</tr>
<tr>
<td>E</td>
<td>No effect</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

- **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

- Human
- Software
- Hardware
- Environment
Accidents by Primary Cause*

<table>
<thead>
<tr>
<th>Cause</th>
<th>Count</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Flight Crew</td>
<td>74</td>
<td>55%</td>
</tr>
<tr>
<td>Airplane</td>
<td>23</td>
<td>17%</td>
</tr>
<tr>
<td>Weather</td>
<td>17</td>
<td>13%</td>
</tr>
<tr>
<td>Misc./Other</td>
<td>10</td>
<td>7%</td>
</tr>
<tr>
<td>Airport/Air Traffic Control</td>
<td>6</td>
<td>5%</td>
</tr>
<tr>
<td>Maintenance</td>
<td>4</td>
<td>3%</td>
</tr>
<tr>
<td><strong>Total with known causes</strong></td>
<td><strong>134</strong></td>
<td></td>
</tr>
<tr>
<td>Unknown or awaiting reports</td>
<td>49</td>
<td></td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td><strong>183</strong></td>
<td></td>
</tr>
</tbody>
</table>

*As determined by the investigating authority, percent of accidents with known causes.
Mode Awareness is becoming a serious issue 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

Functional Analysis → Automation Model

Automation Model is derived from Functional Analysis, operator and expert user input.

Training material is derived from Automation Model. Training Representation is created.

Training Material → Software Specification

Software specification is derived from Training Material.

Software Specification → Software

Software is certified against Automation Model.

System is certified against Automation Model.

Configuration Management verifies and maintains consistency with Automation Model.

Configuration Management → Certification

Certification

Iterative Human-Centered Prototype Evaluation Stage
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

Type of Analysis

Decision Aspects

Expert Appraisal

- approval decision
  - mitigations to reach sufficient safety
    - standards for evaluation
      - abstraction to potential hazards & effects
        - system description

Hazard Analysis

- approval decision
  - mitigations to reach sufficient safety
    - hazard likelihood & effects
      - categorization of potential hazards
        - system description

Modeling & Quantification

- approval decision
  - safety standard
    - mitigation design
      - hazard likelihood & effects
        - abstraction
          - system description

Standard Compliance

- compliance decision
  - compliance evidence
    - standards for evaluation
      - system description
Confidence Intervals on Rate of Rare Event

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

\[
f_x(x | \lambda, t) = \frac{(\lambda)^x e^{-\lambda}}{x!}
\]

\[
g(\lambda | x, t) = \frac{(\lambda t)^x e^{-\lambda t}}{x!}
\]

- \( x \) = no. of events
- \( t \) = observation time
- \( \lambda \) = true event rate
- \( t = 10^8 \) hours
Addressing Multiple Hazards in System

Dominant Hazard Case

Multiple Equal Hazards

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