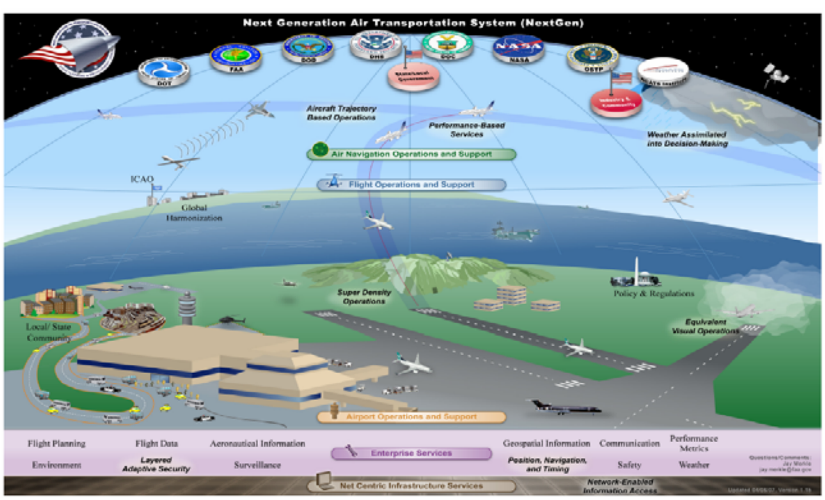
MIT International Center for Air Transportation

Safety Approval of New Operational Systems

Roland E. Weibel, PhD
rweibel@gmail.com

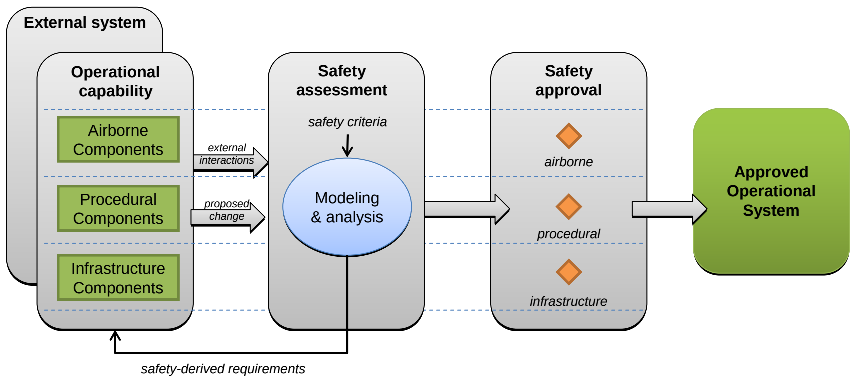
MIT Global Airline Industry Consortium Meeting
MIT, October 29, 2009

Motivation: New Operational Systems Envisioned



from: Joint Planning and Development Office, Concept of Operations for the Next Generation Air Transportation System, Version 3.0, October 2009

Safety Assessment and Approval of New Operational Systems

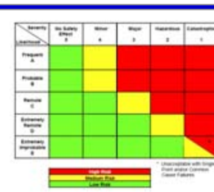


- **Safety assessment required before approval and implementation of most new operational systems in air transportation**
- **Decisions made in safety assessment significantly influence cost and performance of new operational systems**
- **Research conducted to understand expected challenges in safety assessment of new operational systems**

Systems-Level Safety Assessment Approaches

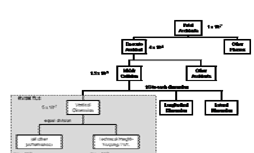
Risk Matrix

Risk ranking defined by severity and likelihood of each hazard in an operational system



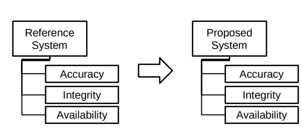
Target Level of Safety

Risk threshold defined for a single hazard decomposed from an overall accident rate target



Reference System

Performance of reference system characterized by several factors, which are required in the proposed system



Case Studies Analyzed

- Instrument Landing System, ILS (1961): Glideslope guidance to aircraft landing in poor visibility
- North Atlantic Organized Track System, NAT OTS (1966-1981): Air traffic routes with aircraft separated by self-reported position
- Traffic Alert & Collision Avoidance System, TCAS (1993): Onboard avionics displaying surrounding traffic and providing midair collision avoidance
- Precision Runway Monitor, PRM (1981): High update rate radar used to separate aircraft on closely-spaced approaches
- European Reduced Vertical Separation Minima, EUR RVSM (2002): Reduction in vertical separation from 3,000 to 1,000 ft enabled by improved altimetry precsion
- Automatic Dependent Surveillance, Broadcast, ADS-B (pending): Broadcast of aircraft-derived position & other states for multiple applications
- Unmanned Aircraft Systems, UAS (pending): Aircraft without onboard flight crew

Case Studies Analyzed

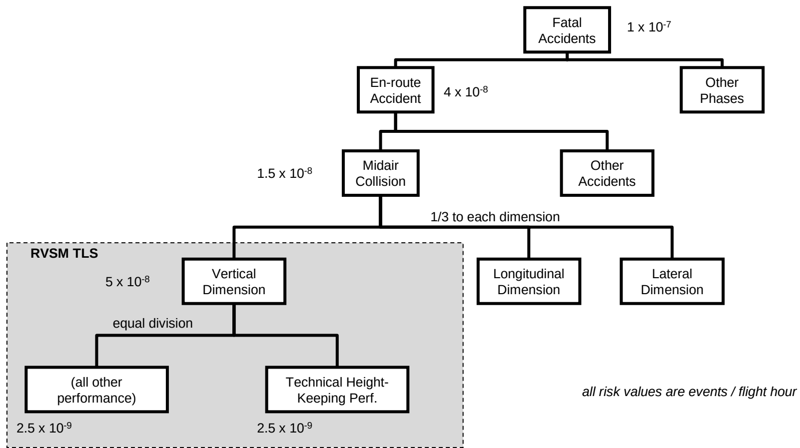
No	Case	Implemented	Assessment Approach
1	Instrument Landing Systems (ILS)	1961	TLS
2	North Atlantic Organized Track System (NAT OTS)	1966-1981	TLS
3	Traffic Alert and Collision Avoidance System (TCAS)	1993	TLS (Risk Ratio)
4	Precision Runway Monitor (PRM)	1997	TLS
5	Automatic Dependent Surveillance, Broadcast (ADS-B) Alaska Capstone	1999	Risk Matrix
6	EUR Reduced Vertical Separation Minima (RVSM)	2002	Risk Matrix TLS
7	Automatic Dependent Surveillance, Broadcast (ADS-B) System-Wide Deployment	(pending)	Risk Matrix TLS Reference System
8	Unmanned Aircraft Systems (UAS)	(pending)	Risk Matrix TLS Reference System

Implemented Changes (rows 1–6)

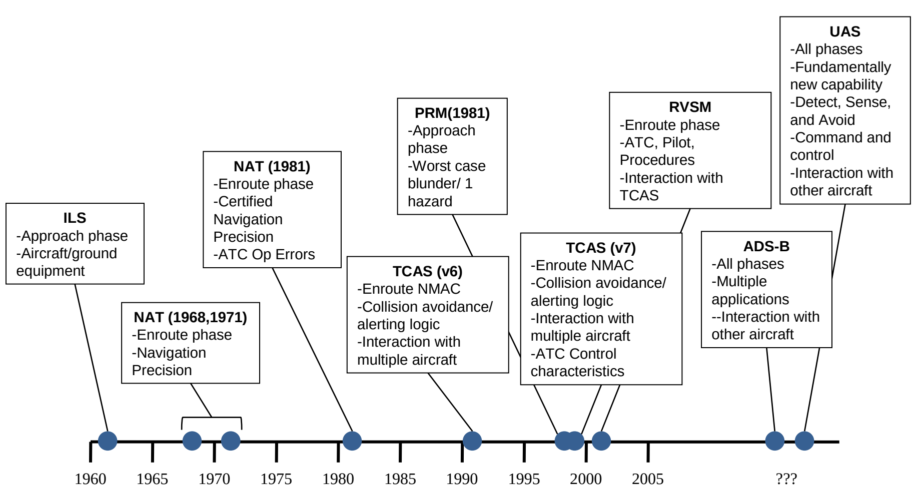
Pending Changes (rows 7–8)

Three Assessment Approaches

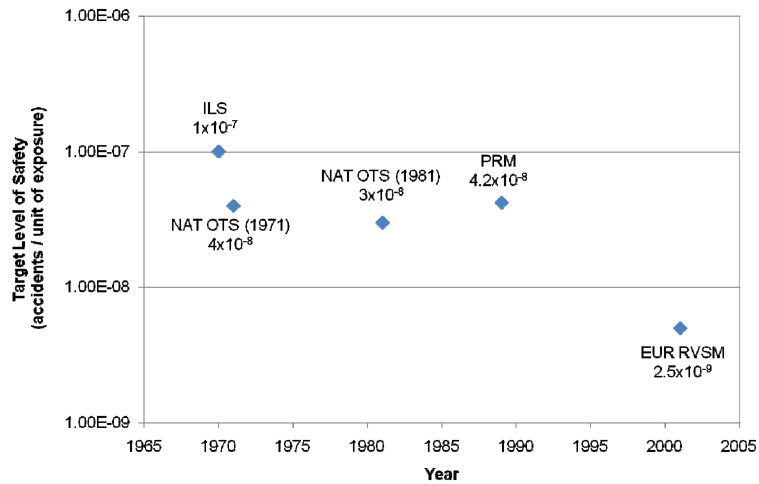
EUR RVSM Risk Budget Limiting Scope of Analysis



Increasing Scope of Analysis



Increasing Safety Performance Demands from TLS in Reviewed Cases



Factors Driving Increased Scope of Safety Assessment

- **High safety performance demands**
  - Increased evaluation of more hazards
  - Increased fidelity of models and use of data
- **Increased scale of changes**
  - Large number of conditions evaluated
- **Fundamentally new types of operation**
  - Reduced similarity to current safety experience
- **Interactions between systems**
  - Legacy system performance limiting acceptable operations
  - Coupling in interaction between systems in failure conditions

Analysis of NextGen Operational Improvement Approval Risk

Code	Definition & Basis
(Not Applicable) ○	No operational approval required Non-operational or process improvements (e.g. scheduling, security, environment, SMS, etc.)
Green (G)	Minimal risk of operational approval No significant safety impact or depends on approved capabilities or operations already approved
Green/Yellow (GY)	Minor risk of operational approval Similar application/operation already approved, or minor safety impacts
Yellow (Y)	Major risk of operational approval Large changes, but limited to one domain (e.g. airborne, ATC, etc.) and hazardous or major safety consequences
Red (R)	Significant risk of operational approval Large amount of analysis required, limited operational experience with concept, or significant change in roles (human/automation)

119 Proposed Operational Improvements Assessed from NextGen Integrated Work Plan (2008) based on summary descriptions

Example of OI Analysis

347	Air Traffic Control Surveillance Service in Non-Radar Areas (ADS-B)	R
348	Reduce Separation - High Density Terminal, Less Than 3-miles	R
349	Automation Support for Mixed Environments	G
350	Flexible Routing	GY
351	Flexible Airspace Management	GY
352	Automated Clearance Delivery and Frequency Changes	Y
353	Reduced Oceanic Separation - Altitude Change Pair-Wise Maneuvers	GY
354	Reduced Oceanic Separation - Co-Altitude Pair-Wise Maneuvers	Y
355	Delegated Responsibility for Horizontal Separation	R
356	Delegated Separation - Pair-Wise Maneuvers	R
358	Trajectory Flight Data Management	Y
359	Self-Separation Airspace - Oceanic	R
360	Automation-Assisted Trajectory Negotiation	Y
361	Resource Planning	G
362	Self-Separation Airspace Operations	R
363	Delegated Separation - Complex Procedures	R

365	Advanced Management of Airspace for Special Use	G
366	Dynamic Airspace Reclassification	G
368	Flow Corridors - Level 2 Dynamic	Y
369	Automated Negotiation/Separation Management	R
370	Trajectory-Based Management - Full Gate-To-Gate	Y
381	GBAS Precision Approaches	Y
400	Wake Turbulence Mitigation: Departures - Wind-Based Wake Procedures	Y
401	Wake Turbulence Mitigation: Arrivals - Wind-Based Wake Procedures	Y
402	Wake Turbulence Mitigation: Departures - Dynamic Wind Procedures	Y
403	Wake Turbulence Mitigation: Arrivals - Dynamic Wind Procedures	Y
406	NAS Wide Sector Demand Prediction and Resource Planning	G
408	Provide Full Flight Plan Constraint Evaluation with Feedback	G
409	Net-Centric Virtual Facility	R
410	Automated Virtual Towers	R
2010	Net-Enabled Common Weather Information Infrastructure	GY
2020	Net-Enabled Common Weather Information - Level 1 Initial Capability	GY
2021	Net-Enabled Common Weather Information - Level 2 Adaptive Control/Enhanced Forecast	GY
2022	Net-Enabled Common Weather Information - Level 3 Full NextGen	GY

Approval Challenges in NextGen OIs

Code	Number of OIs	Percent of OIs
NA	53	45%
G	19	16%
GY	11	9%
Y	21	18%
R	15	13%
[redacted]		

Conclusions

- **Safety assessment will be key capability to achieve future operational changes**
- **Increased demands for safety assessment quality can be expected**
  - Emphasis on structured approaches can expand the scope of analysis
  - Obtaining operational data will be a critical capability to qualitatively and quantitatively characterize safety behavior
- **Significant challenges in safety approval of new operational systems can be expected**
  - Risk that increased scope can lead to intractability of analysis
    - Long time scales of change
    - Risk of failure to close safety case
  - Risk that tractability may limit changes to functionally similar capabilities

Questions?

- Thesis available at http://dspace.mit.edu >> air transportation research