Assuring Emergent Properties Under Composition: A Case Study of the U.S. National Airspace System

Natasha Neogi
52nd IFIP Workgroup 10.4 Meeting
Edinburgh, Scotland
June 29, 2007
Outline

- US National Airspace System
- Accident Analysis
- Models and Languages
- Proof Strategies and Techniques
- Future Directions
Outline

- US National Airspace System
  - Introduction
  - Motivation
- Accident Analysis
- Models and Languages
- Proof Strategies and Techniques
- Future Directions
Mission and Strategic Goals

- **Mission**
  - Provide a safe, efficient global aerospace system that contributes to national security.

- **Strategic goals**
  - Safety
  - Security
  - System efficiency

- **Information Technology Drivers**
  - Growth in aviation traffic
  - Need to reduce already low fatality rates
  - User demand for new and improved services
U.S. National Airspace (NAS) System Services

Navigation and Landing Services

Separation Assurance

1000 ft

Traffic Management

Aviation Information
Mandate

Each day, manage 30,000 commercial flights to safely move 2,000,000 passengers

- ~ 500 FAA Managed Air Traffic Control Towers
- ~ 180 Terminal Radar Control Centers
- 20 Enroute Centers
- ~ 60 Flight Service Stations
- ~ 40,000 Radars, NAVAIDs, Radios, etc.
A Crisis Looming in Air Transportation

- Exponential growth in demand but system not scalable
- US economy and quality of life highly dependent on air transportation
- Exacerbated by environmental, fuel, and security concerns
- Problem of national and international significance (Commission on the Future of the United States Aerospace Industry, JPDO, NGATS, NRC, SESAME/SESAR)
Unique Environment

- Safety and security are highest priorities
  - Airplanes can't stop in flight and corrupted messages can pose a dangerous situation
  - Most access/authentication systems not appropriate
  - Self-inflicted DOS not an option
- Mixed Equipage and Backwards Compatibility
- International - 187 ICAO members
- NAS diversity uses physical separation and redundant systems
- Unlike DoD, Confidentiality is not primary concern, Integrity and Availability are critical

Increasingly automated, information driven system results in accidents due to complex, unpredictable interactions
Outline

- The National Airspace System
- Accident Analysis
- Models and Languages
- Proof Strategies and Techniques
- Future directions
Warsaw, Poland (14 September 1993)

Airbus A320-200
Fatalities 2:70

A320 doesn’t allow for manual application of braking when Full Flaps configuration set until touchdown recorded
Nagoya, Japan (26 April 1994)

Airbus 300B4-622R
Fatalities: 264:271

A300 autopilot designed not to disconnect using standard control column force below α-deck
Toulouse, France (30 June 1994)

**Airbus A330-321**

Fatalities: 7:7

During takeoff, aircraft automatically transitioned to an automode with no pitch authority limitations
Überlingen, Germany (1 July 2002)

TU-154M/Boeing 757-23APF
Fatalities: 71:71

It is not required to notify the ATC prior to responding to a TCAS RA.
Cleveland, Ohio (Denial of Service)

Boeing 767-300J
Fatalities: 0:66
Cleveland, Ohio (11 September 2001)

All traffic controlled by a single air traffic controller transmit on the same RF.
Outline

- Introduction
- Accident Analysis
- Model and Language
  - Modelling Issues
  - Hybrid Systems
- Proof Techniques
- Future Directions
Issues of Scale

**Macro**
Analyzable but unrealistic

- Resolution
- Discrete vs. Continuous

**Micro**
Realistic, but not analyzable. Simulation is slow.

Spatial

Mathematical equations and formulas are used to illustrate the concepts of spatial and temporal resolution in modelling. The page also mentions issues related to resolution and the distinction between discrete and continuous models.
Approach:
• Build in Safety/Security from system inception

Broader Context:
• Methodology applies to safety critical high confidence critical infrastructure systems
• Can be used for mobile, real-time systems

Multiple Qualities

System Security Process
- Preliminary Threat Assessment
- Vulnerabilities and Attack Models
- Avoidance, Detection, Masking
- Certification
- Monitor Vulnerability

Requirements Specification and Analysis
- System Specification
- Modelling: Components and Interfaces
- Integration of Techniques
- Simulation and Testing
- Assessment and Measurements
- Sustainment & Retirement

System Safety Process
- Preliminary Hazard Analysis
- Accident and Risk Models
- Elimination, Mitigation, Control
- Certification
- Monitor Residual Risk
Continuous Trajectory Description

\[ \xi_r = -v_1 + v_2 \cos \phi_r + \omega_1 y_r \]
\[ \xi_r = v_2 \sin \phi_r - \omega_1 x_r \]
\[ \phi_r = \omega_2 - \omega_1 \]

\[ x_r, y_r \in \mathbb{R}^1 \]
\[ \phi_r \in [-\pi, \pi) \]
\[ \omega_1 = [\omega_1, \bar{\omega}_1] \subset \mathbb{R}^1 \]
\[ \omega_2 = [\omega_2, \bar{\omega}_2] \subset \mathbb{R}^1 \]
Discrete Conflict Definition for Continuous Trajectories

- Consider the protected zone around the own aircraft to be defined by the three mile cylindrical block:

\[ T = \{(x_r, y_r) \in \mathbb{R}, \phi_r \in [-\pi, \pi], x_r^2 + y_r^2 \leq 3^2\} \]

- The aircraft are in conflict if:

\[ (x_r, y_r, \phi_r) \in T \]
Related Work on Modeling

- **Switched system**: \( x = f_{\sigma(t)}(x) \) \[Branicky`98\][Liberzon`03]
  - Switching signal \( \sigma : \mathbb{P}^+ \rightarrow \{1,2,3,\ldots,N\} \)
  - Discrete behavior is not modeled

- **Hybrid automata** [Alur, Henzinger, et al. `96]
  - Finite state machine + differential equations

- **Hybrid I/O automata** [Lynch, Segala, Vaandrager `05]
  - Typed variables (\( N, P, \) sets, sequences, maps)
  - Continuous evolution \( \tau: [0,t] \rightarrow X; \) Discrete transitions
  - Closed under composition

- **Hazard Hybrid I/O automaton (HHA)** [Neogi, Lynch, Leveson `07]
  - Continuous evolution specified by differential & algebraic equations, stopping conditions, invariance conditions
  - Abstraction based on reachable set overapproximation wrt invariant properties

---

\[ \dot{x} = f_1(x) \quad \dot{x} = f_2(x) \]
HIOA Modeling Language

automaton H

variables
  internal \( x_r, y_r, \phi_r : \text{Real} \), \( s : \text{Bool} \)
  output \( y_1, y_2 : \text{Real} \)
  input \( \omega_1, \omega_2 : \text{Real} \)

actions
  input conOn, conOff

transitions
  On: pre \( x_r^2 + y_r^2 \leq \Delta \), eff \( s := \text{true} \)
  Off: pre \( x_r^2 + y_r^2 > \Delta \), eff \( s := \text{false} \)

trajectories
  On: inv \( s \) evolve
    \( d(x_r) = -1 + \cos \phi_r + \omega_1 y_r \), \( d(y_r) = \sin \phi_r - \omega_1 x_r \), \( d(\phi_r) = \omega_2 - \omega_1 \), \( y_1 = x_r \), \( y_2 = y_r \)
  Off: inv \( \neg s \) evolve
    \( d(x_r) = -1 + \cos \phi_r \), \( d(y_r) = \sin \phi_r \), \( d(\phi_r) = \omega_2 \), \( y_1 = x_r \), \( y_2 = y_r \)

Defines external interface of H

Defines a set of trajectories for H, i.e., functions from \([0,t]\) to variable values
Semantics for HIOA

- An **execution** of $H$ is a sequence
  \[ \alpha = t_0 a_1 t_1 a_2 t_2 \ldots \]
- **Trace($\alpha$)** externally visible part of $\alpha$
  - Input/output variables and actions
- Nondeterminism: multiple start states, uncertainties in transitions and dynamics
- **Traces($H$)** set of all traces of $H$
- **C implements** $A$ if $\text{Traces}(C) \subseteq \text{Traces}(A)$
  - $A$ is an *abstraction* for $C$

Want to prove for HIOA under some composition $\parallel$:

if $F$ is invariant over $H$\(^{\parallel} F$ is invariant over $C \rightarrow F$ is invariant over $H\parallel C$

**Theorem:** Given $F$ is invariant over $C$ and $H$, $H\parallel C$

\[ \exists A \mid \text{traces}(C) \subseteq \text{traces}(A) \text{ and } F \text{ is invariant over } H\parallel A \]
Outline

- Introduction
- Accident Analysis
- Modelling and Language
- Proof Techniques
  - Abstraction and Composition
  - Reachability Theory
- Future Directions
Multiple Properties and Composition

- **Composition** $H \parallel A$
- Abstract supervisor $A$ for ensuring that heading $\phi_1$ is in the safe range $[\phi_{\text{min}}, \phi_{\text{max}}]$
- Requirements dictate relative angular velocity must not exceed range $[\omega_{\text{min}}, \omega_{\text{max}}]$
- **Construct** $H\parallel A$ to achieve the desired invariant
Composition and Abstraction in Verification

- To verify concrete system $H || C$ it suffices to show that $C$ implements $A$.

- To show $C$ implements $A$, a simulation relation $R$ on states of $C$ and $A$, s.t. each move of $C$, is matched by some sequence of moves of $A$ that preserve $R$ and have the same trace behaviour.

- Abstraction constructed inductively by using the invariant properties to be verified → Examine reachable behaviour

For a given controller/decision aid, $C$, that applies some input $\omega$ or alerts with resolution $R$ at time $t$, can we guarantee for all $t$: $x_r^2 + y_r^2 \leq 3^2$
Reachable Sets: Ellipsoidal Overapproximations

- **Problem:**
  - Given Starting States, Inputs and Transition relations:
    - Initial Set $x_0 X_0$
    - Input Set $q(t) Q(t)$
    - Reachable Set $x^*(\omega) X[\omega]$

- Find a tight external overapproximation such that the ellipsoid touches the exact reach set at two points at time $t_1$
  - Attempt to Verify Property
- Refine the overapproximation using counter-examples to eliminate unreachable states
Reachable Sets: Ellipsoidal Overapproximations

- **Problem:**
  - Given Starting States, Inputs and Transition relations:
    - Note that this generates a family of ellipsoids $E$
    - For well behaved $F_i$, each quality represents a manifold in the state space
    - Pick the $E_i$ s.t. its projection on the manifold formed by $F_i$ is optimal wrt to the associated metric space
Approximate Solution

- Initial Set and Input/Control Set can be bounded by and described by ellipsoids

$$\mathcal{S}((x(t), Q(t))) = \{u : (u - g(t))^T Q^{-1} (u - g(t)) \leq 1\}$$
Closed Form Solution

\[
\dot{x} = A(t)x + g(t)
\]

\[
x(t_0) = x_0
\]

Any choice of positive, integrable \( p(s) \) will yield an external approximation ellipsoid.

For tight external ellipsoid \( \Rightarrow p(s) \) must satisfy:

\[
\begin{align*}
\mathbb{E}[x(t) x(t)^T] - \mathbb{E}[x(t_0) x(t_0)^T] & \leq \int_{t_0}^{t} \int_{t_0}^{s} \mathbb{E}[(x(s) - x(t)) (x(s) - x(t))^T] ds \, ds \\
\mathbb{P}[\|x(t_0)\| < \|x(t)\|] & \leq \frac{\int_{t_0}^{t} \int_{t_0}^{s} \mathbb{E}[(x(s) - x(t)) (x(s) - x(t))^T] ds \, ds}{\int_{t_0}^{t} \int_{t_0}^{s} \mathbb{E}[(x(s) - x(t)) (x(s) - x(t))^T] ds \, ds}
\end{align*}
\]
Example: Boeing 747 in Steady Climbing Turn Resolution Maneuver
Summary of Verification Process

Given hybrid system represented by $H$, and controller $C$, for some $F=F_1 \cup F_2 \cup F_3 \cup \ldots \cup F_n$, Verify $H \parallel C$ has invariant set $F$

By construction:

- Create $H \parallel A$ by overapproximating reachable set of $H \parallel C$
- Select abstraction $A_i$ such that $F_i$ is satisfied, and $A_i$ is optimal
- $A = \bigcup A_i$
- Prove $\text{traces}(C) \subseteq \text{traces}(A) \Rightarrow F$ invariant over $H \parallel C$
Outline

- The National Airspace System
- Accident Analysis
- Models and Languages
- Proof Strategies and Techniques
- Future Directions
Scaled/UAV Testbed

- Inject/Insert Errors to cause misbehaviour
  - Evaluate detection coverage
  - Measure Performance and Latency
- Verify timing assumptions under varying operational/environmental conditions
  - Error rate and type
  - Communications
  - Power consumption
  - Malicious events
- Discover incorrect/missing requirements that have not been traced to implementation
Air Transportation Vision

A distributed air transportation system with
- Information-rich airspace
- Scalable/increased capacity
- Safe, secure operation
- Reduced environmental impact

That incorporates
- Human-centered automation
- Accommodation for new vehicles
- Shared situational awareness
- Distributed vehicle state and health, traffic, weather, and airport information
- Agile systems for safety, security, capacity, and environment
Thank You! Questions?

A Day in the Life of Global Air Traffic