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

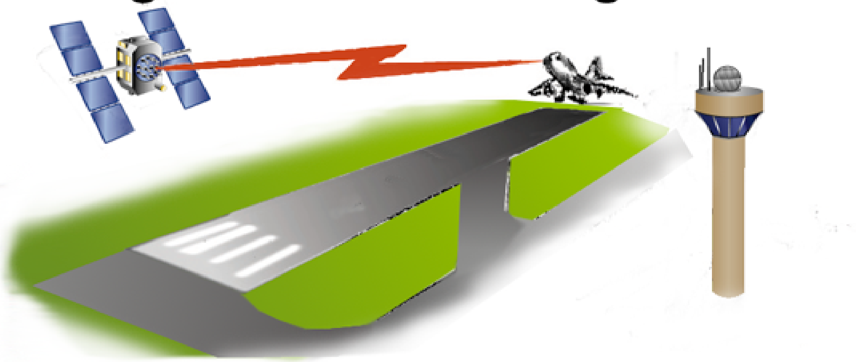
ILLINOIS

Mission and Strategic Goals

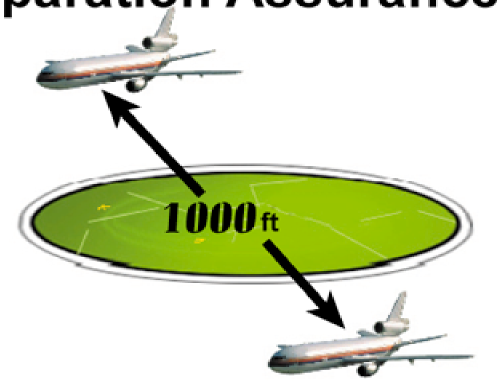
- **Mission**
  - **Provide a safe, efficient global aerospace system that contributes to national security.**
- **Strategic goals**
  - **Safety**
  - **Security**
  - **System efficiency**
- **Information Technology Drivers**
  - **Growth in aviation traffic**
  - **Need to reduce already low fatality rates**
  - **User demand for new and improved services**

U.S. National Airspace (NAS) System Services

Navigation and Landing Services



Separation Assurance



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)

Photo Copyright Michael Schmidt AIRLINERS.NET

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

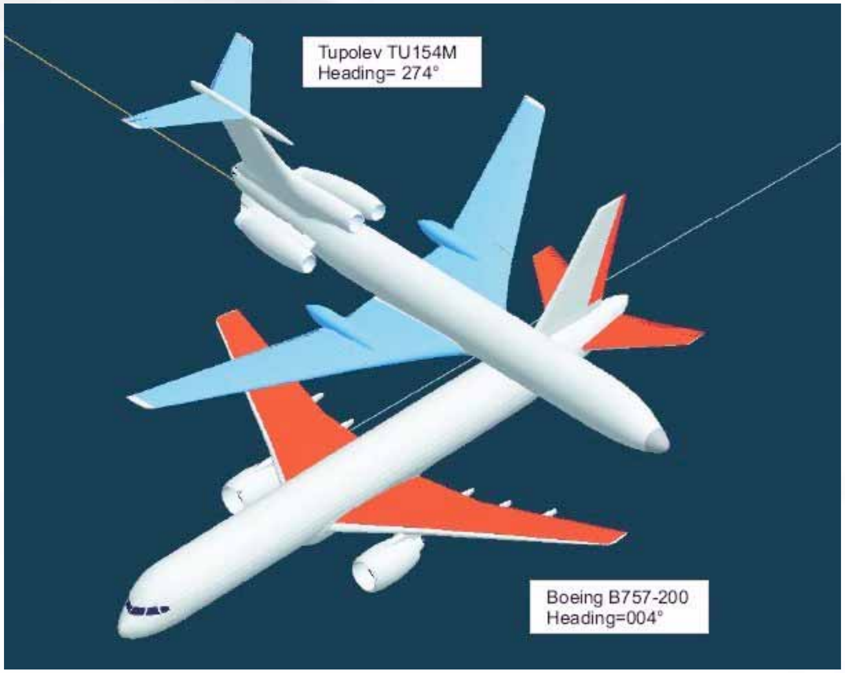
Toulouse, France (30 June 1994)

Airbus A330-321

Fatalities: 7:7

During takeoff, aircraft automatically transitioned to an automode with no pitch authority limitations

Überlingen, Germany (1 July 2002)



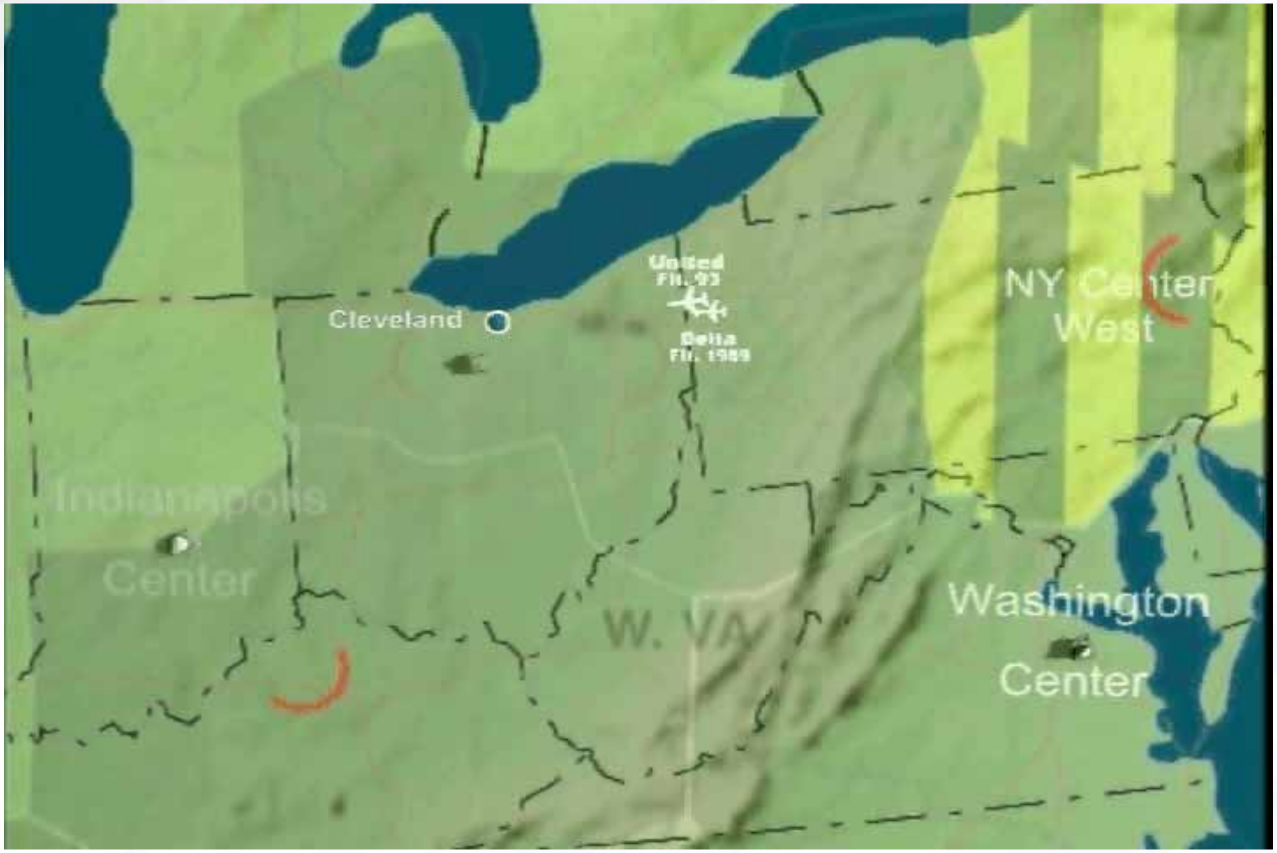
TU-154M/Boeing 757-23APF
Fatalities: 71:71

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)

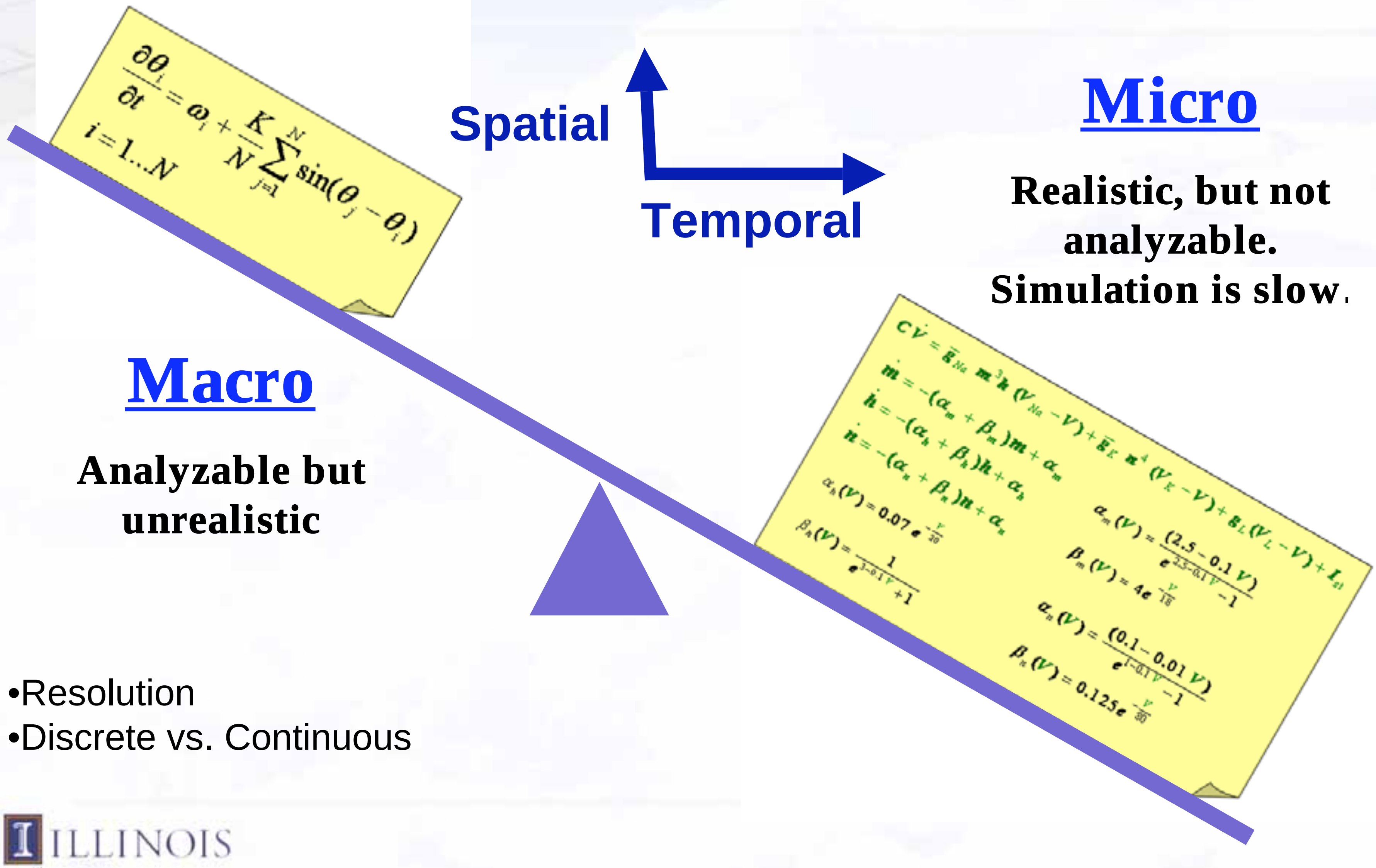


All traffic controlled by a single air traffic controller transmit on the same RF.

Outline

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

Issues of Scale


$\frac{\partial\theta_i}{\partial t} = \omega_i + \frac{K}{N}\sum_{j=1}^{N}\sin(\theta_j - \theta_i)$
$i = 1..N$
Spatial
Temporal
$C\dot{V} = \bar{g}_{Na}\, m^3 h\,(V_{Na} - V) + \bar{g}_K\, n^4\,(V_K - V) + g_L(V_L - V) + I_{st}$
$\dot{m} = -(\alpha_m + \beta_m)m + \alpha_m$
$\dot{h} = -(\alpha_h + \beta_h)h + \alpha_h$
$\dot{n} = -(\alpha_n + \beta_n)n + \alpha_n$
$\alpha_h(V) = 0.07\,e^{-\frac{V}{20}}$
$\beta_h(V) = \frac{1}{e^{3-0.1V}+1}$
$\alpha_m(V) = \frac{(2.5 - 0.1\,V)}{e^{2.5-0.1V}-1}$
$\beta_m(V) = 4e^{-\frac{V}{18}}$
$\alpha_n(V) = \frac{(0.1 - 0.01\,V)}{e^{1-0.1V}-1}$
$\beta_n(V) = 0.125e^{-\frac{V}{80}}$

Micro

Realistic, but not analyzable. Simulation is slow.

Macro

Analyzable but unrealistic

- Resolution
- Discrete vs. Continuous

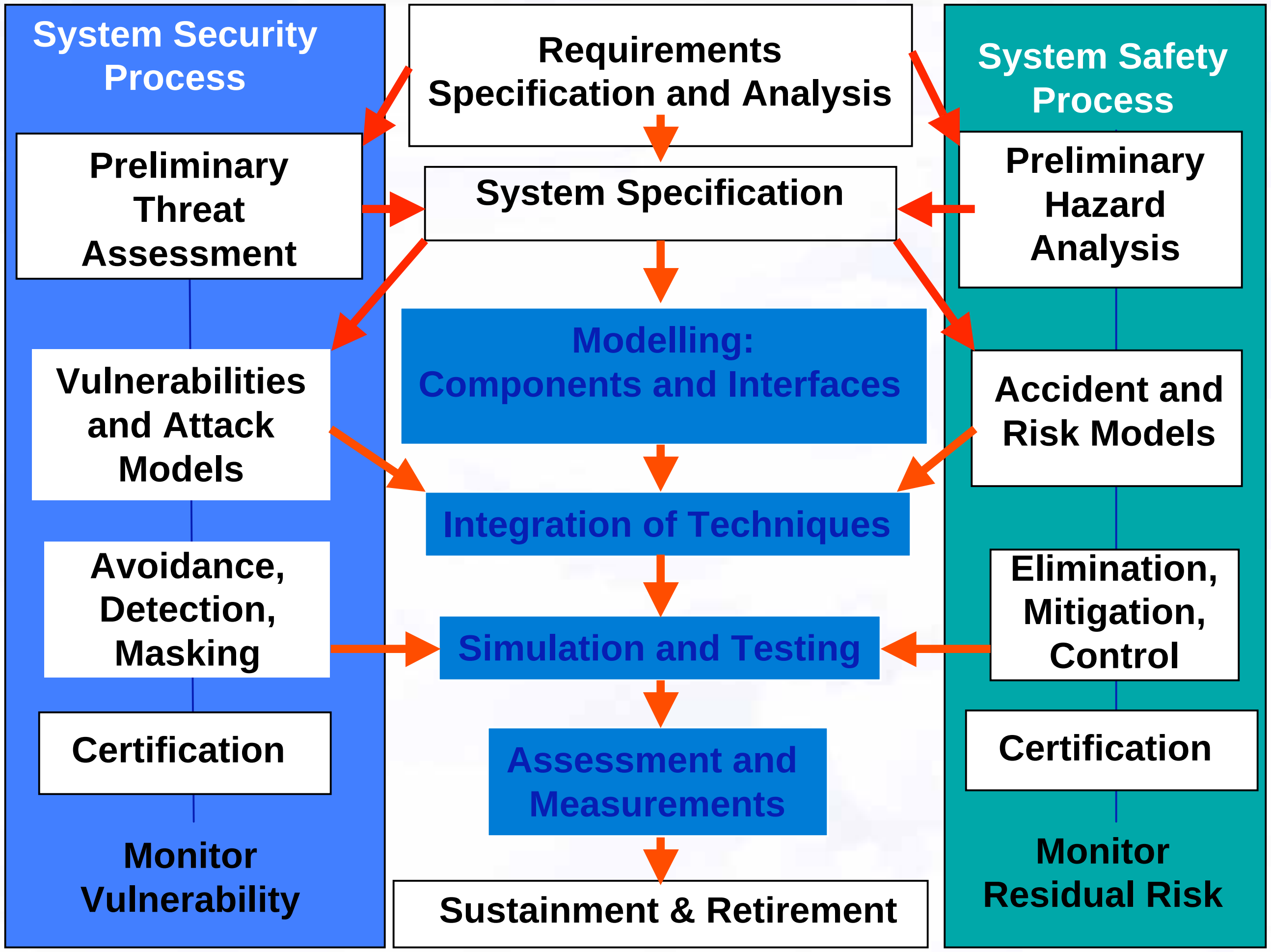
Multiple Qualities

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



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

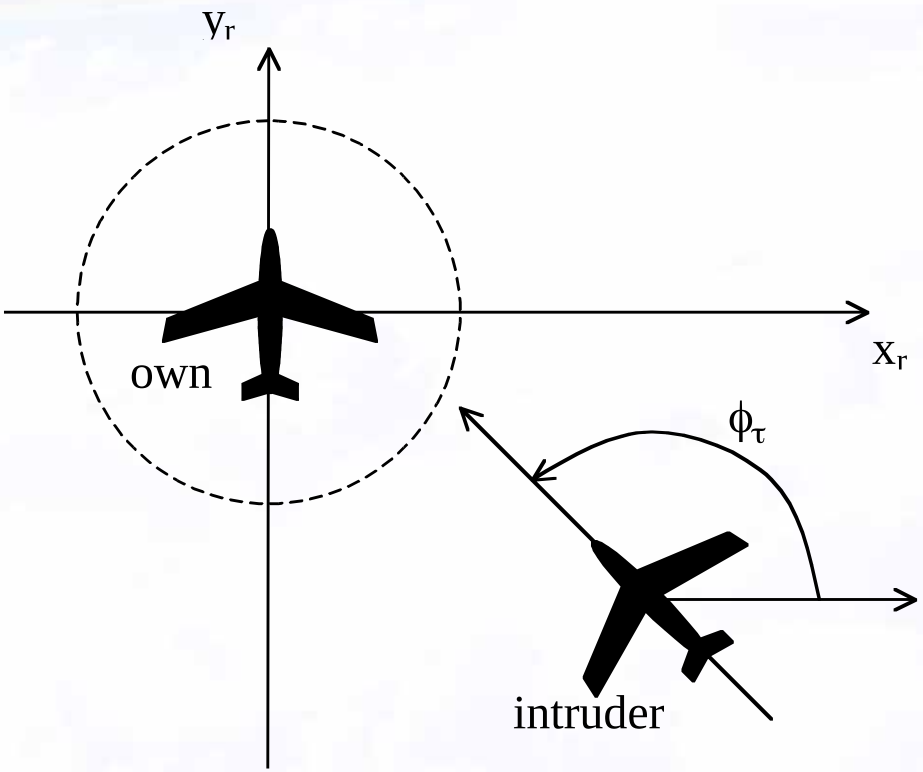
Accident and Risk Models

Elimination, Mitigation, Control

Certification

Monitor Residual Risk

Continuous Trajectory Description



$$\dot{x}_r = -v_1 + v_2 \cos\phi_r + \omega_1 y_r$$
$$\dot{y}_r = v_2 \sin\phi_r - \omega_1 x_r$$
$$\dot{\phi}_r = \omega_2 - \omega_1$$

$$x_r, y_r \in \Re^1$$
$$\phi_r \in [-\pi, \pi)$$
$$\omega_1 = [\underline{\omega}_1, \overline{\omega}_1] \subset \Re^1$$
$$\omega_2 = [\underline{\omega}_2, \overline{\omega}_2] \subset \Re^1$$

ILLINOIS

Discrete Conflict Definition for Continuous Trajectories

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

$$T = \left\{ (x_r, y_r) \in \Re, \phi_r \in [-\pi, \pi) \middle| x_r^2 + y_r^2 \leq 3^2 \right\}$$

- The aircraft are in conflict if:

$$(x_r, y_r, \phi_r) \in T$$

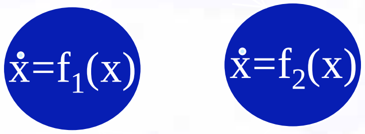
Related Work on Modeling

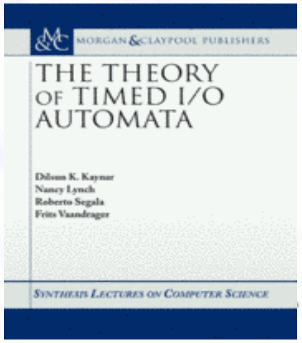
- Switched system: $x = f_{\sigma(t)}(x)$ [Branicky`98][Liberzon`03]
  - Switching signal $\sigma : P^+$�{1,2,3,..,N}
  - Discrete behavior is not modeled
- Hybrid automata [Alur, Henzinger, et al. `96]
  - Finite state machine + differential equations
- Hybrid I/O automata [Lynch, Segala,Vaandrager `05]
  - Typed variables (N, P, sets, sequences, maps)
  - Continuous evolution τ:[0,t] → 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

Daniel Liberzon

Switching in Systems and Control

Birkhäuser




M&C MORGAN & CLAYPOOL PUBLISHERS

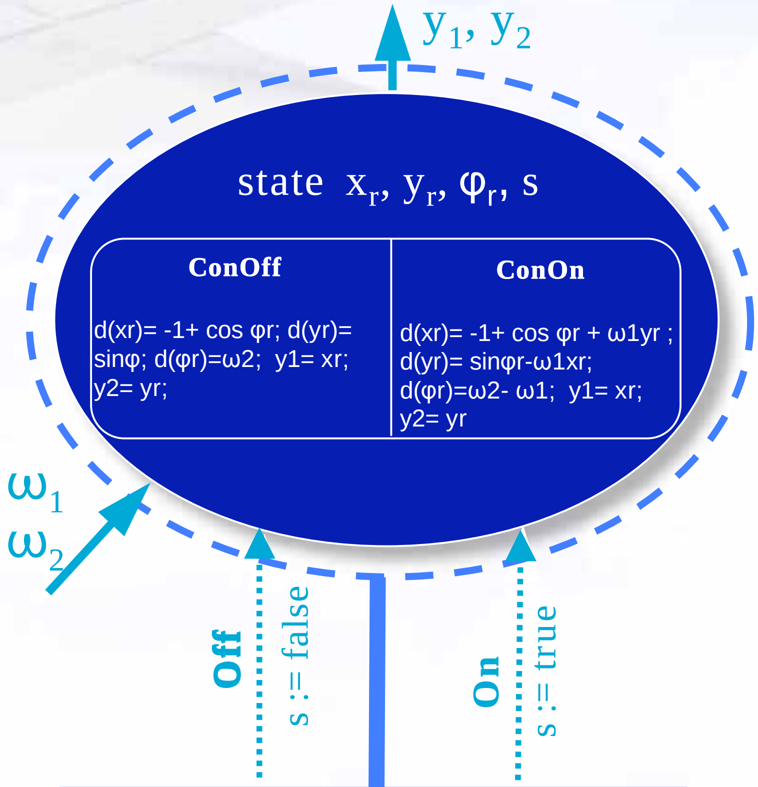
THE THEORY OF TIMED I/O AUTOMATA

Dilsun K. Kaynar
Nancy Lynch
Roberto Segala
Frits Vaandrager

SYNTHESIS LECTURES ON COMPUTER SCIENCE

ILLINOIS

HIOA Modeling Language


y_1, y_2
state x_r, y_r, φ_r, s
ConOff
d(xr)= -1+ cos φr; d(yr)= sinφ; d(φr)=ω2; y1= xr; y2= yr;
ConOn
d(xr)= -1+ cos φr + ω1yr ; d(yr)= sinφr-ω1xr; d(φr)=ω2- ω1; y1= xr; y2= yr
ω_1
ω_2
Off
s := false
On
s := true

Defines external interface of **H**

```
automaton H
 variables
   internal $x_r, y_r, \varphi_r$ :Real,s:Bool
   output $y_1, y_2$:Real
   input $\omega_1, \omega_2$:Real
 actions
   input conOn, conOff
 transitions
   On:  pre $x_r^2 + y_r^2 \le 3^2 + \Delta$, eff s:=true
   Off:  pre $x_r^2 + y_r^2 > 3^2$ , eff s:=false
 trajectories
   On: inv s evolve
    $d(x_r) = -1 + \cos\varphi_r + \omega_1 y_r$ ; $d(y_r) = \sin\varphi_r - \omega_1 x_r$;  $d(\varphi_r) = \omega_2 - \omega_1$;
    $y_1 = x_r$; $y_2 = y_r$;
   Off: inv ⌉s evolve
    $d(x_r) = -1 + \cos\varphi_r$; $d(y_r) = \sin\varphi$;  $d(\varphi_r) = \omega_2$;  $y_1 = x_r$; $y_2 = y_r$;
```

Defines a set of *trajectories* for **H**, i.e., functions from [0,t] to variable values

ILLINOIS

Semantics for HIOA

- An **execution** of **H** is a sequence

  $\alpha = \tau_0 a_1 \tau_1 a_2 \tau_2 \ldots$
- **Trace(α)** externally visible part of α
  - Input/output variables and actions
- Nondeterminism: multiple start states, uncertainties in transitions and dynamics

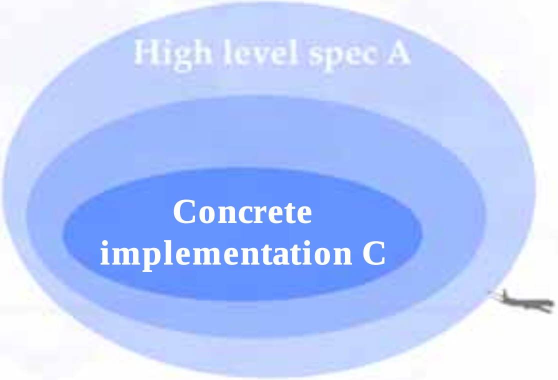
  Traces(H) set of all traces of **H**
- **C implements A** if Traces(**C**) ⊆ Traces(**A**)
  - **A** is an *abstraction* for **C**

Want to prove for HIOA under some composition ‖:

if F is invariant over H ^F is invariant over C → F is invariant over H‖C

Theorem: Given F is invariant over C and H, H‖C

∃A | traces(C)⊆ traces(A) and F is invariant over H‖A

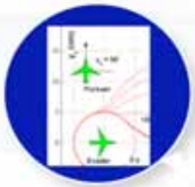


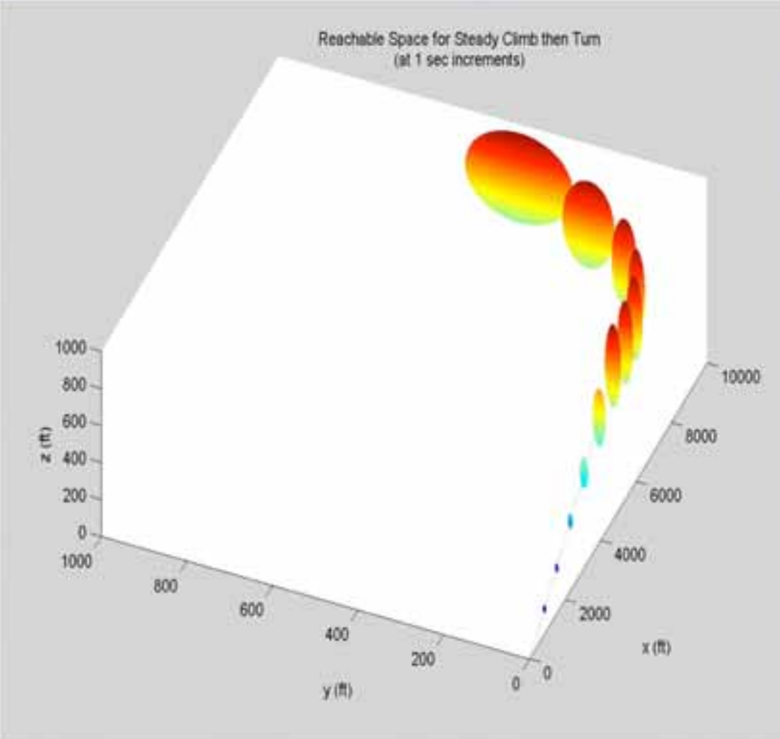
Outline

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

Multiple Properties and Composition

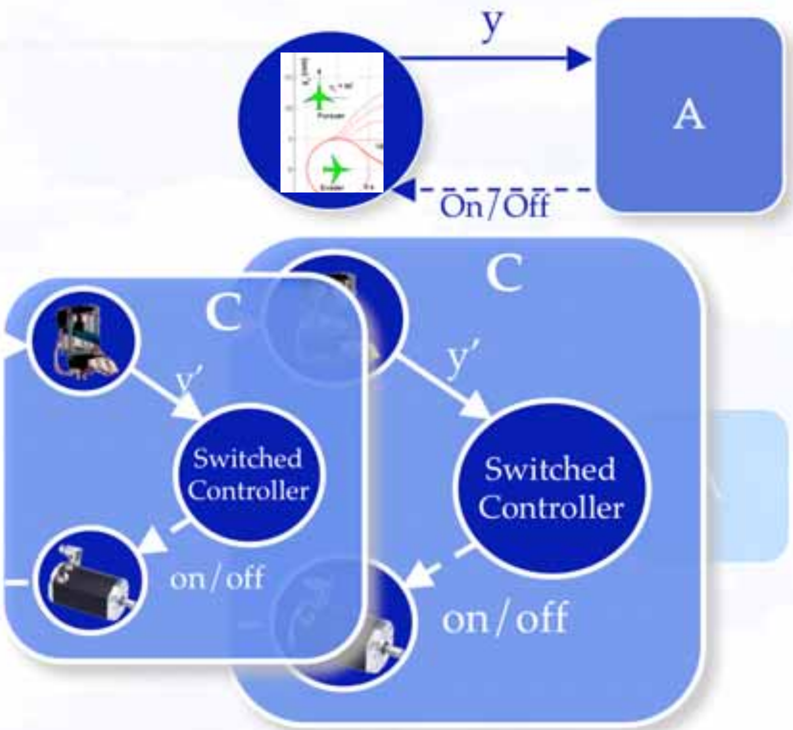
- Composition **H || A**
- Abstract supervisor **A** for ensuring that heading φ_1 is in safe range $[\varphi_{min}, \varphi_{max}]$
- Requirements dictate relative angular velocity must not exceed range $[\omega_{min}, \omega_{max}]$
- **Construct H||A** to achieve the desired invariant





Composition and Abstraction in Verification

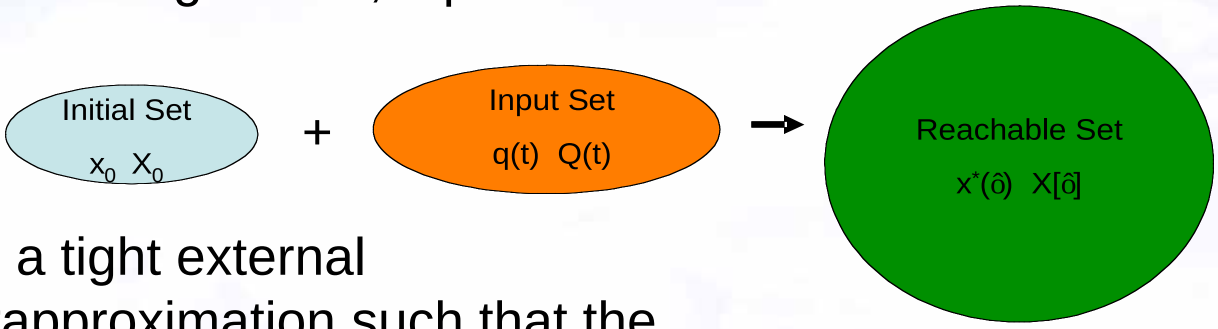
- To verify concrete system **H||C** it suffices to show that **C** implements **A**.
- To show **C** implements **A**
  simulation relation R on states of **C** and A, s.t. each **move** of **C**, is matched by **some sequence of moves** of **A** that preserve **R** and have the same trace behaviour
- 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 ω_1/alerts with resolution R at time t,
can we guarantee for all t: $x_r^2 + y_r^2 \le 3^2$

Reachable Sets: Ellipsoidal Overapproximations

- Problem:
  - Given Starting States, Inputs and Transition relations:



Initial Set

x_0 X_0

+

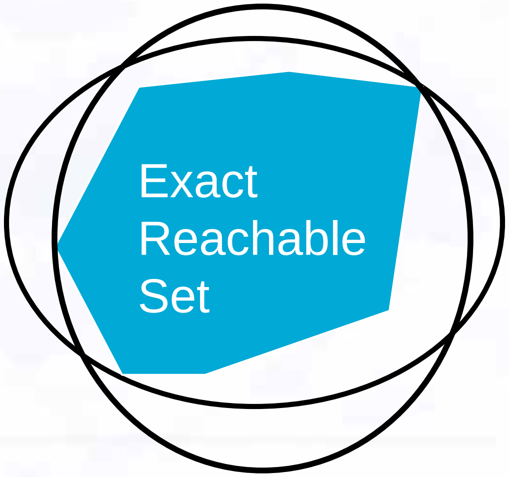
Input Set

q(t) Q(t)

Reachable Set

$x^*(ô)$ $X[ô]$

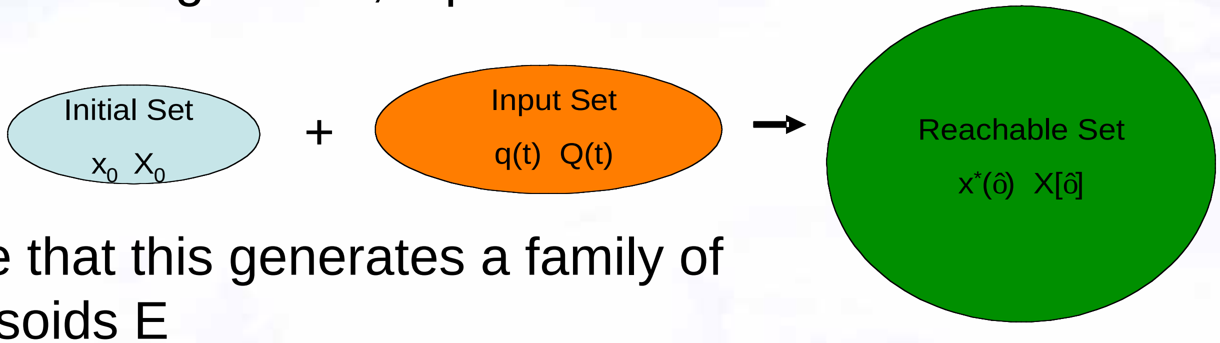
  - Find a tight external overapproximation such that the ellipsoid touches the exact reach set at two points at time t_1
    - Attempt to Verify Property
  - Refine the overapproximation using counter-examples to eliminate unreachable states



Exact Reachable Set

Reachable Sets: Ellipsoidal Overapproximations

- Problem:
  - Given Starting States, Inputs and Transition relations:



Initial Set

x_0 X_0

+

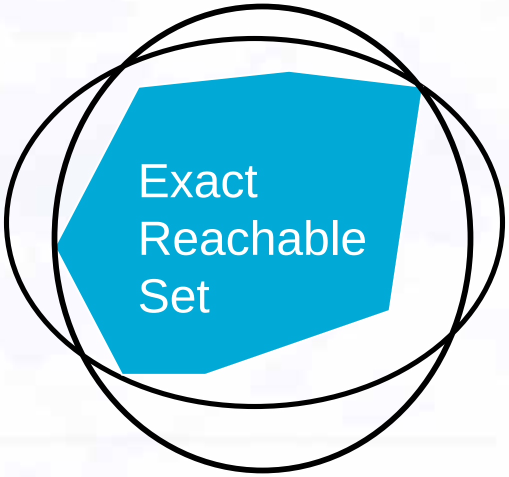
Input Set

q(t) Q(t)

Reachable Set

x^*(ô) X[ô]

  - 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



Exact Reachable Set

Approximate Solution

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

$$\varepsilon(q(t), Q(t)) = \{u : (u - q(t))^T Q^{-1}(t)(u - q(t)) \leq 1\}$$

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

Closed Form Solution

$$\dot{x}^* = A(t)x^* + q(t)$$

$$x^*(t_0) = x^0$$

$$X_+[t] = X_+(t \mid p(\cdot)) = \left(\int_{t_0}^{t} p(s)ds + p_0(t)\right)\left(\int_{t_0}^{t} p^{-1}(s)G(t,s)Q(s)G'(t,s)ds + p_0^{-1}(t)G(t,t_0)X^0X^{0\prime}(t,t_0)\right)$$

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

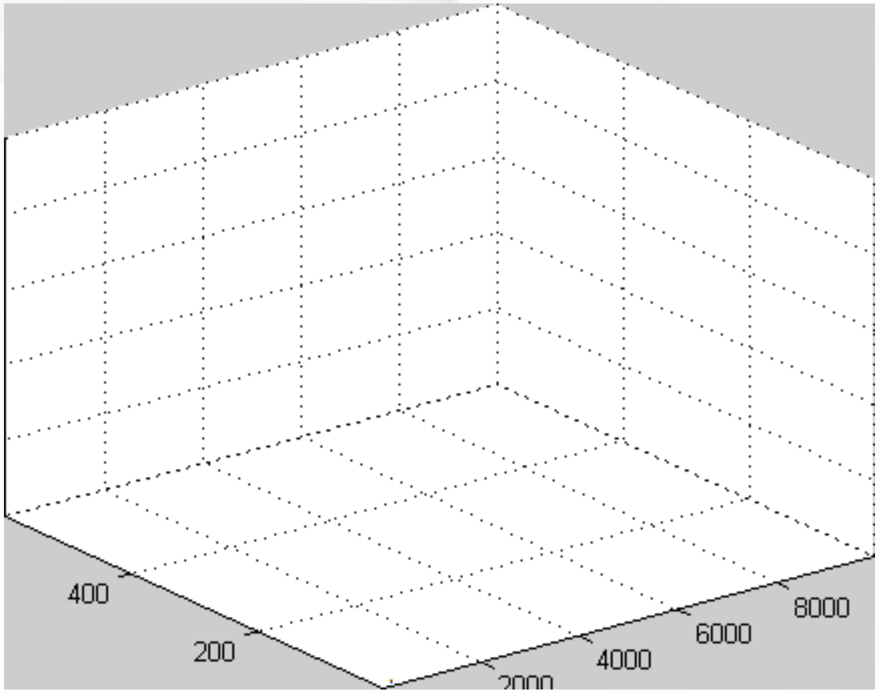
For tight external ellipsoid → *p(s)* must satisfy:

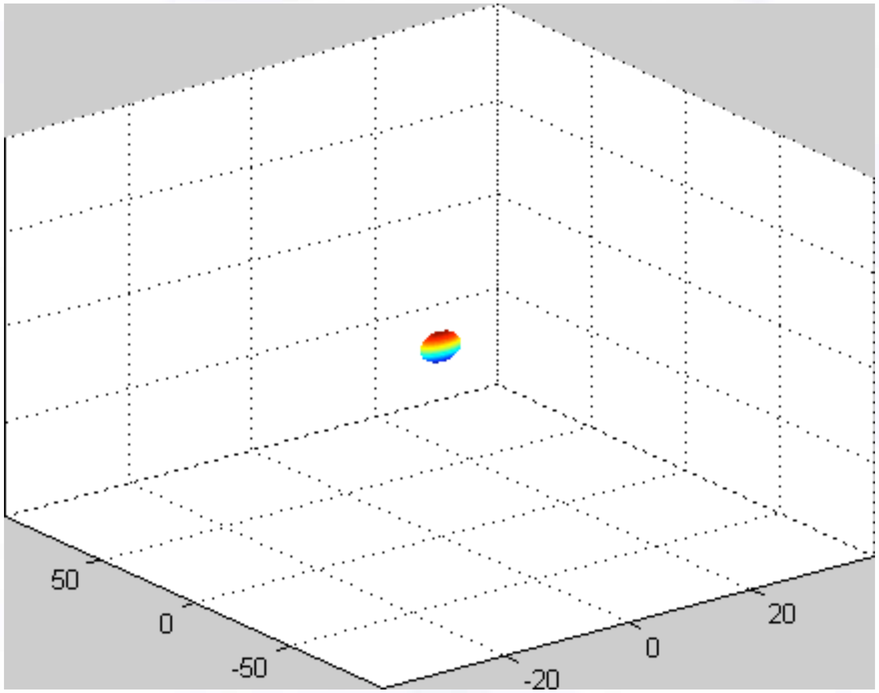
[illegible]

$$t_0 \le s \le t$$

[illegible]

Example: Boeing 747 in Steady Climbing Turn Resolution Maneuver





Summary of Verification Process

Given hybrid system represented by H, and controller C, for some $F=F_1 U F_2 U F_3 U \ldots U F_n$,

Verify H∥C has invariant set F

By construction:

- Create H∥A by overapproximating reachable set of H∥C
  - Select abstraction A_i such that F_i is satisfied, and Ai is optimal
  - $A = \bigcap_i A_i$
- Prove traces(C) ⊆ traces(A) → F invariant over H∥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

UAV movie

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

ILLINOIS

Thank You! Questions?

A Day in the Life of Global Air Traffic