Design and Analysis of Safety Critical Systems

Peter Seiler
University of Minnesota

MTA Sztaki
December 5, 2017
University of Minnesota

- Founded in 1851
- Campuses in Twin Cities, Duluth, Morris and Crookston.
- Twin Cities campus has 52,557 students (~7,200 in CSE).
First aeronautical engineering courses offered in 1926. Department founded in fall 1929 with 3 faculty members.

Aeronautical Engineering merged with the Department of Mechanics and Materials in 1958 to form current department.

17 regular faculty (6 systems, 6 fluids, 5 solids)

328 undergraduates, 17 MS, and 73 PhD students
Aerospace Systems

Demoz Gebre-Egziabher: Sensor fusion; design of multi-sensor systems for navigation

William Garrard: Dynamics and control of aerospace vehicles; parachute dynamics.

Peter Seiler: Robust control with applications to aerospace systems and wind energy

Yohannes Ketema: Dynamics; dynamics of active materials; stability of formations; orbital mechanics
Aerospace Systems

Richard Linares: *Orbital debris tracking, uncertainly quantification*

Maziar Hemati: *Control and optimization, primarily of fluid mechanical systems*

Derya Aksaray: *Control theory, formal methods, and machine learning with applications to autonomous systems.*

Ryan Caverly: *Robust control with applications to aerospace, mechanical and marine systems.*
Research Summary

Jordan Hoyt
Parul Singh
Sanjana Vijayshankar
Wind Energy

Raghu Venkataraman
Harish Venkataraman
Small UAVs

Abhineet Gupta
Aeroelasticity

Robust Control Design and Analysis

Chris Regan
Brian Taylor
Curt Olson
Fault Tolerance for Small UAVs
With: Raghu Venkataraman

Funding:
(NSF) CPS: Managing Uncertainty in the Design of Safety-Critical Aviation Systems
(MnDrive) Precision Agriculture: Robotics and Sensor Development for Revolutionary Improvements in the Global Food Supply and Reduced Environmental Impact in the Agriculture Industry.
Growth in Small UAVs

- **DJI Phantom 4**
  (Source: www.dji.com)

- **Trimble UX5**
  (Source: uas.trimble.com)

- **senseFly eBee**
  (Source: uncrate.com)

---

**Sentera Vireo**
- Donated to UMN in 2014
- Remote sensing applications, e.g. precision agriculture
Precision Agriculture

Remote sensing → Data analysis → Decision making → Actionable Information: Forecasting, Economics, Environment, UAS policy
Nominal mission

Lawnmower pattern contained within geo-fence perimeter

Flight Data From Aborted Mission

- Linkage to right elevon failed, i.e. “free float” [1].
- Autopilot attempted to control using left elevon.
- No active fault-tolerance
- Median size of US cropland = 1105 acres [2].

References
[1] Data courtesy of FourthWing Sensors, LLC.
Fault Tolerance: Commercial Aircraft

Boeing 787-8 Dreamliner
- 210-250 seats
- Length=56.7m, Wingspan=60.0m
- Range < 15200km, Speed< M0.89
- First Composite Airliner
- Honeywell Flight Control Electronics

Boeing 777-200
- 301-440 seats
- Length=63.7m, Wingspan=60.9m
- Range < 17370km, Speed< M0.89
- Boeing’s 1st Fly-by-Wire Aircraft
Fault Tolerance: Commercial Aircraft

Boeing 787-8 Dreamliner
- 210-250 seats
- Length=56.7m, Wingspan=60.0m
- Range < 15200km, Speed< M0.89
- First Composite Airliner
- Honeywell Flight Control Electronics

Boeing 777-200
- 301-440 seats
- Length=63.7m, Wingspan=60.9m
- Range < 17370km, Speed< M0.89
- Boeing’s 1st Fly-by-Wire Aircraft
777 Triple-Triple Architecture [Yeh, 96]

- Sensors x3
- Databus x3
- Triple-Triple Primary Flight Computers
- Actuator Electronics x4
777 Triple-Triple Architecture [Yeh, 96]

Left PFC

INTEL

AMD

MOTOROLA

Sensors x3  Databus x3  Triple-Triple Primary Flight Computers  Actuator Electronics x4
# Reliability Comparison

<table>
<thead>
<tr>
<th>Boeing 777</th>
<th>Reliability</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="Boeing 777" /></td>
<td>- &lt; $10^{-9}$ catastrophic failures per hour</td>
</tr>
<tr>
<td></td>
<td>- No single point of failure</td>
</tr>
<tr>
<td></td>
<td>- Protect against random &amp; common failures</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Design</th>
</tr>
</thead>
<tbody>
<tr>
<td>- Hardware Redundancy</td>
</tr>
<tr>
<td>- Dissimilar hardware and software</td>
</tr>
<tr>
<td>- Limited use of analytical redundancy [1]</td>
</tr>
<tr>
<td>- Fault Trees, etc to certify</td>
</tr>
</tbody>
</table>

---

**References**

## Reliability Comparison

<table>
<thead>
<tr>
<th>Boeing 777</th>
<th>Reliability</th>
<th>Design</th>
</tr>
</thead>
</table>
| ![Boeing 777](image) | • $< 10^{-9}$ catastrophic failures per hour  
• No single point of failure  
• Protect against random & common failures | • Hardware Redundancy  
• Dissimilar hardware and software  
• Limited use of analytical redundancy [1]  
• Fault Trees, etc to certify |

<table>
<thead>
<tr>
<th>Ultrastick 120</th>
<th>Reliability</th>
<th>Design</th>
</tr>
</thead>
</table>
| ![Ultrastick 120](image) | • ~0.8 failures/100 hrs [2]  
• Single points of failure | • Limited by size, weight, power, and cost (SWAPC) constraints |

### References
Key Questions

1. What is an appropriate level of reliability for small UAS?
   - FAA Modernization and Reform Act (1/12)
   - FAA 14 CFR Part 107 (8/16)

2. Can analytical redundancy be used to increase the reliability of small UAS?
   - Flight with a single aero surface [1]
   - Fault detection of actuator failures [2,3,4]

3. How can analytical methods be certified?
   - Probabilistic analysis methods and extended fault trees [5,6]

---

Key Questions

1. What is an appropriate level of reliability for small UAS?
   • FAA Modernization and Reform Act (1/12)
   • FAA 14 CFR Part 107 (8/16)

2. Can analytical redundancy be used to increase the reliability of small UAS?
   • Flight with a single aero surface [1]
   • Fault detection of actuator failures [2,3,4]

3. How can analytical methods be certified?
   • Probabilistic analysis methods and extended fault trees [5,6]

Final Goal

Takeoff

Nominal mission

Control surface fault

Safe landing

Fault tolerant control

Fault diagnosis

Time

Residual

Threshold
Flight With One Aero Surface

1. Ultrastick 120 [1]
Demonstrated closed-loop steady, level flight (2015).

2. Senior Design [2]
Team designed and built flying wing. Demonstrated ability to land by human pilot (2016).

3. Sentera Vireo

References

• Control input simultaneously excites longitudinal and lateral-directional motion
• No direct yaw control
System Identification

- Chirp excitations on elevator and aileron
- Identified frequency response from:
  - Elevator to pitch rate
  - Aileron to roll rate
- Grey-box modeling
  - Aero. Coeff. Initialized with using vortex-lattice method
  - Updated using flight data
- Plot shows aileron to roll rate
  - Dutch roll mode visible

![Graph showing frequency response and phase shift](image)
Single Surface Flight

- Right elevon stuck at 5 deg trailing edge up
- Flight divided into circle (set by user) and land phases
- The red plus sign is the target touch-down point
Glideslope Tracking
Fault Detection and Reconfiguration

Fault Detection and Reconfiguration

From Aerospace to Automotive....

Similar reliability concerns are now common in automotive applications due to rise of autonomous driving.
Performance Adaptive Aeroelastic Wing (PAAW)

- Goal: Suppress flutter, control wing shape and alter shape to optimize performance
  - Funding: NASA NRA NNX14AL36A
  - Technical Monitor: Dr. Jeffrey Ouellette
  - Two years of testing at UMN followed by two years of testing on NASA’s X-56 Aircraft
Aeroservoelasticity (ASE)

Efficient aircraft design

• Lightweight structures
• High aspect ratios

Source: www.flightglobal.com
Flutter

Source: NASA Dryden Flight Research
Classical Approach

Controller Bandwidth

Rigid Body Modes

Frequency Separation

Aeroelastic Modes

Flight Dynamics, Classical Flight Control

Flutter Analysis
Flexible Aircraft Challenges

Rigid Body Modes

Increasing wing flexibility

Aeroelastic Modes

Frequency
Flexible Aircraft Challenges

- Rigid Body Modes
- Aeroelastic Modes
- Coupled Rigid Body and Aeroelastic Modes

Integrated Control Design
Modeling and Control for Flex Aircraft

1. Parameter Dependent Dynamics
   - Models depend on airspeed due to structural/aero interactions
   - LPV is a natural framework.

2. Model Reduction
   - High fidelity CFD/CSD models have many (millions) of states.

3. Model Uncertainty
   - Use of simplified low order models OR reduced high fidelity models
   - Unsteady aero, mass/inertia & structural parameters
Current PAAW Aircraft

**mAEWing1**
10 foot wingspan
~14 pounds
Laser-scan replica of BFF 4 aircraft, >50 flights

**mAEWing2**
14 foot wingspan
~42 pounds
Half-scale X-56
Currently ground testing
mAEWing1 and 2
Open-Loop Flutter
Body Freedom Flutter
Comparison of BFF mode variation with airspeed I.D.’d from flight test data with theoretical predictions for Open Loop and H∞ controller; Marker descriptions – (X): theoretical poles, (◇): sys. I.D.’d open/closed loop poles.
Successful flight beyond flutter with 2 controllers!
Finite Horizon Robustness Analysis of LTV Systems Using Integral Quadratic Constraints

Peter Seiler
University of Minnesota

M. Moore, C. Meissen, M. Arcak, and A. Packard
University of California, Berkeley

MTA Sztaki
October 5, 2017
Issue: Few numerically reliable methods to assess the robustness of time-varying systems.
Goal: Assess the robustness of linear time-varying (LTV) systems on finite horizons.

Approach: Classical Gain/Phase Margins focus on (infinite horizon) stability and frequency domain concepts.

Instead focus on:

- Finite horizon metrics, e.g. induced gains and reachable sets.
- Effect of disturbances and model uncertainty (D-scales, IQCs, etc).
- Time-domain analysis conditions.
Nonlinear dynamics [MZS]:

\[ \dot{\eta} = f(\eta, \tau, d) \]

where

\[ \eta = [\theta_1, \dot{\theta}_1, \theta_2, \dot{\theta}_2]^T \]
\[ \tau = [\tau_1, \tau_2]^T \]
\[ d = [d_1, d_2]^T \]

\( \tau \) and \( d \) are control torques and disturbances at the link joints.

Nominal Trajectory (Cartesian Coords.)
Effect of Disturbances / Uncertainty

**Cartesian Coords.**

**Joint Angles**
Overview of Analysis Approach

Nonlinear dynamics:

\[ \dot{\eta} = f(\eta, \tau, d) \]

Linearize along a (finite –horizon) trajectory \((\bar{\eta}, \bar{\tau}, d = 0)\)

\[ \dot{x} = A(t)x + B(t)u + B(t)d \]

Compute bounds on the terminal state \(x(T)\) or other quantity \(e(T) = C x(T)\) accounting for disturbances and uncertainty.

Comments:

- The analysis can be for open or closed-loop.
- LTV analysis complements the use of Monte Carlo simulations.
Conclusions

• Fault tolerance for small UAVs
  • Commercial aircraft achieve high reliability with redundancy.
  • Model-based fault detection methods are an alternative that enables size, weight, power, and cost to be reduced.
  • Develop methods for analytical fault tolerance on small UAS and tools to certify the probabilistic performance.

• Modeling and control of flexible aircraft

• Robustness analysis of time-varying systems

http://www.aem.umn.edu/~SeilerControl/
Acknowledgements

• **US National Science Foundation**

• **NASA**

• **Eolos Consortium and Saint Anthony Falls Laboratory**
Backup
Modeling and Control for Wind Energy

Jen Annoni, Shu Wang, Daniel Ossmann, Parul Singh, Jordan Hoyt, Sanjana Vijayshankar
(with support from SAFL/EOLOS)
Clipper Liberty, 2012: Modern utility-scale turbine.

- Rosemount, MN.
- Diameter: 96m
- Power: 2.5MW
- Saint Anthony Falls Lab: [http://www.safl.umn.edu/](http://www.safl.umn.edu/)
Individual Blade Pitch Control

Goals:

• Reducing structural loads on the turbine to increase life time of turbine and components while keeping power production constant by adding an individual blade pitch controller.

Controller architecture

Implementation 2017

C96 Liberty research turbine

Ref: Ossmann, Theis, Seiler, ‘16 ASME DSCC, Best Energy Paper Award
1. Parameter Dependent Dynamics
   • Models depend on windspeed due to structural/aero interactions
   • LPV is a natural framework.

2. Model Reduction
   • High fidelity CFD/CSD models have many (millions) of states.

3. Model Uncertainty
   • Use of simplified low order models OR reduced high fidelity models
Minneapolis and St. Paul, Minnesota

- Twin Cities Population ~3.5 Million
- Average daily low/high in January is -15.4°C / -5.6°C
- Strong outdoor culture with many lakes and bike trails
Department History

John D. Akerman was first Department Head 1929 - 1957
- Born in Latvia late 1890’s
- Studied with Nikolai Joukowsky
- Acquainted with Igor Sikorsky

Jean and Jeanette Piccard performed pioneering research in high altitude ballooning (1930’s)

Akerman Tailless Aircraft

1930’s Cellophane Stratosphere Balloon Ascent in Memorial Stadium