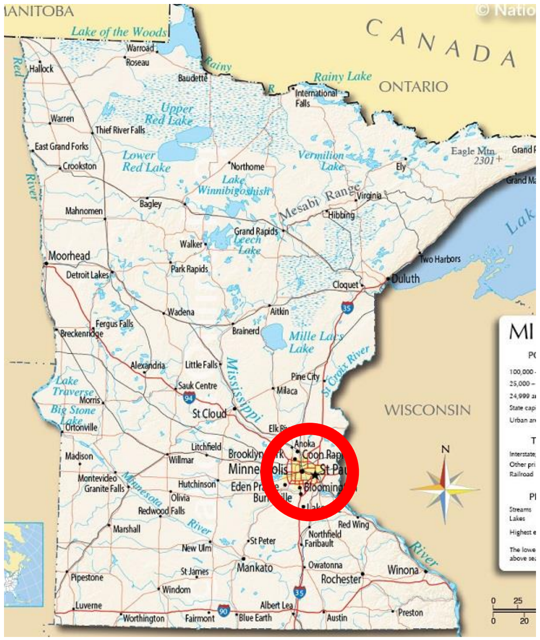
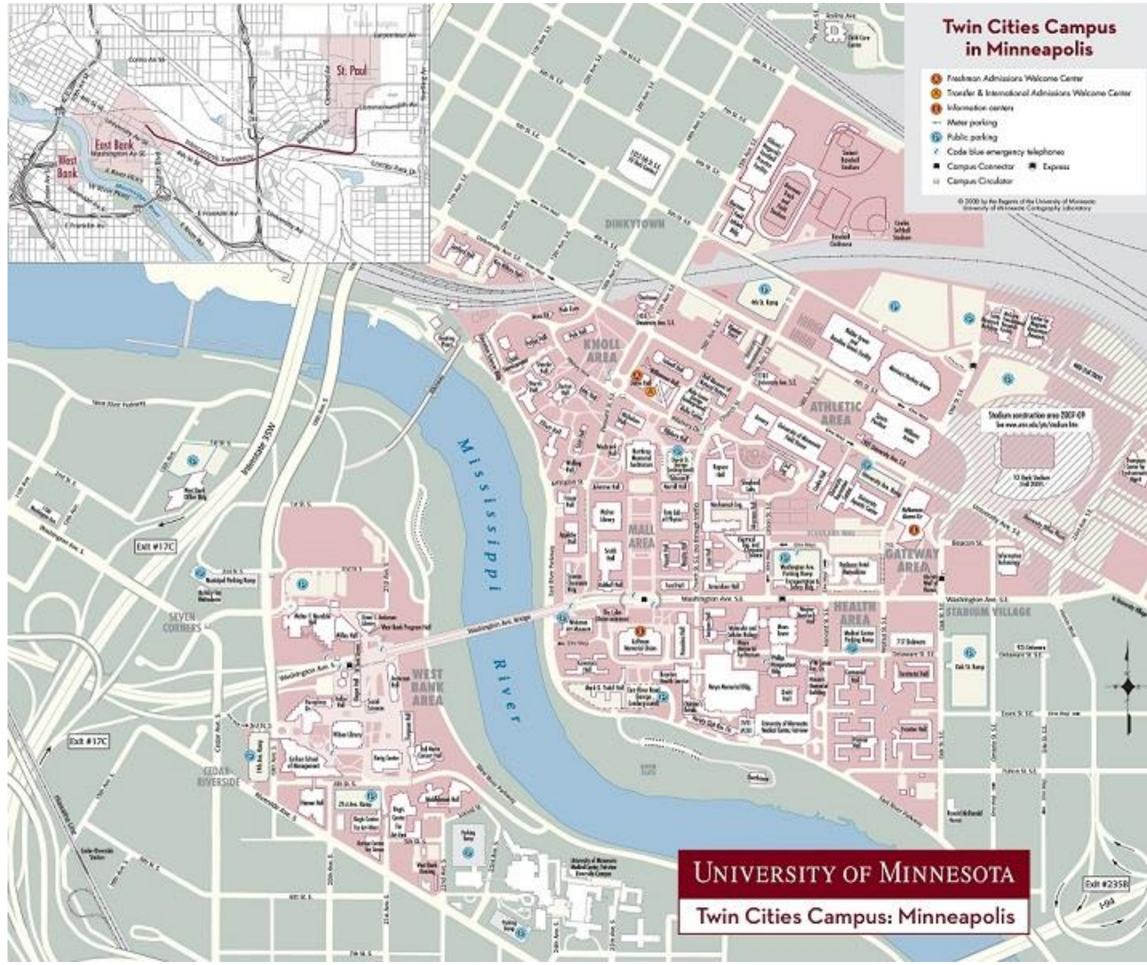
Design and Analysis of Safety Critical Systems

Peter Seiler
University of Minnesota

MTA Sztaki
December 5, 2017

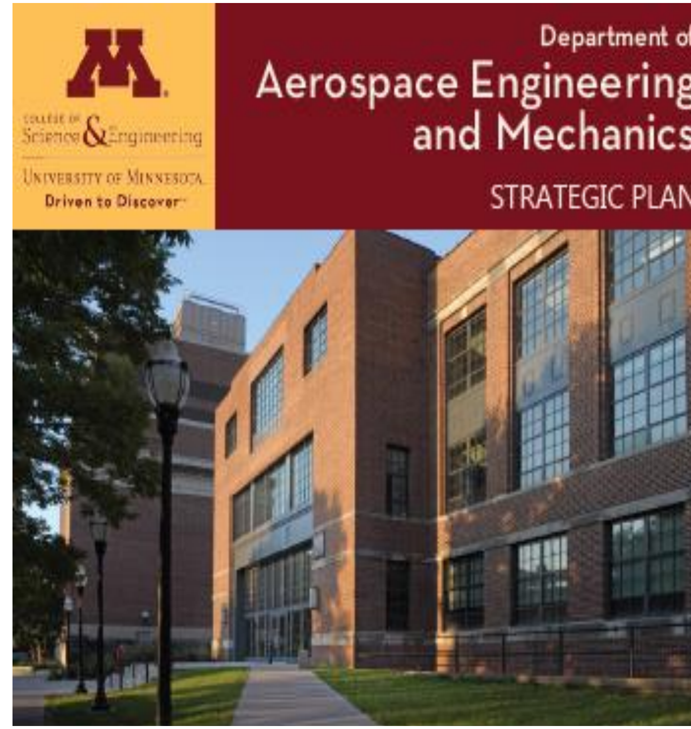
University of Minnesota





- Founded in 1851
- Campuses in Twin Cities, Duluth, Morris and Crookston.
- Twin Cities campus has 52,557 students (~7,200 in CSE).

Dept. of Aerospace Engineering & Mechanics

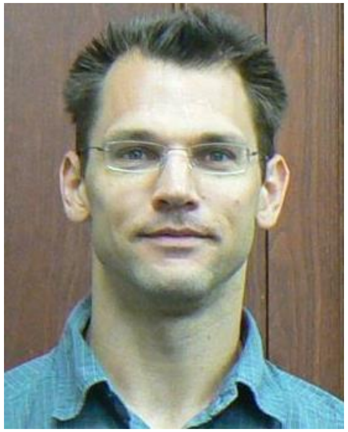


- First aeronautical engineering courses offered in 1926. Department founded in fall 1929 with 3 faculty members.
- Aeronautical Engineering merged with the Department of Mechanics and Materials in 1958 to form current department
- 17 regular faculty (6 systems, 6 fluids, 5 solids)
- 328 undergraduates, 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*

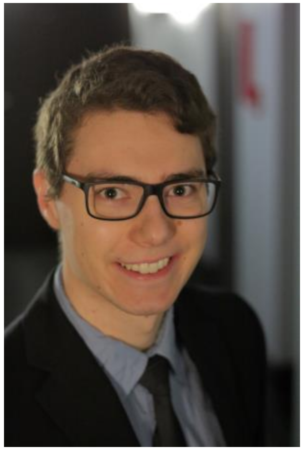
Yohannes Ketema: *Dynamics; dynamics of active materials; stability of formations; orbital mechanics*

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

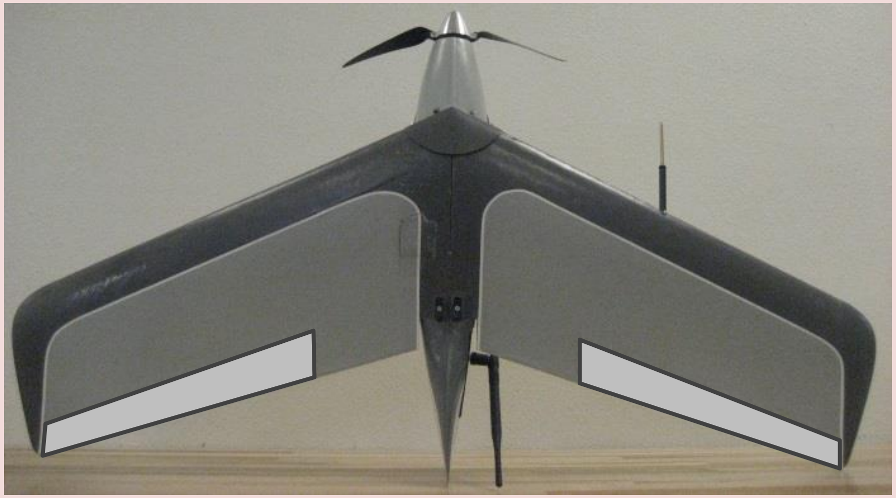
(MnDrive) Precision Agriculture: Robotics and Sensor Development for Revolutionary Improvements in the Global Food Supply and Reduced Environmental Impact in the Agriculture Industry.

Growth in Small UAVs

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

Trimble UX5
(Source: uas.trimble.com)

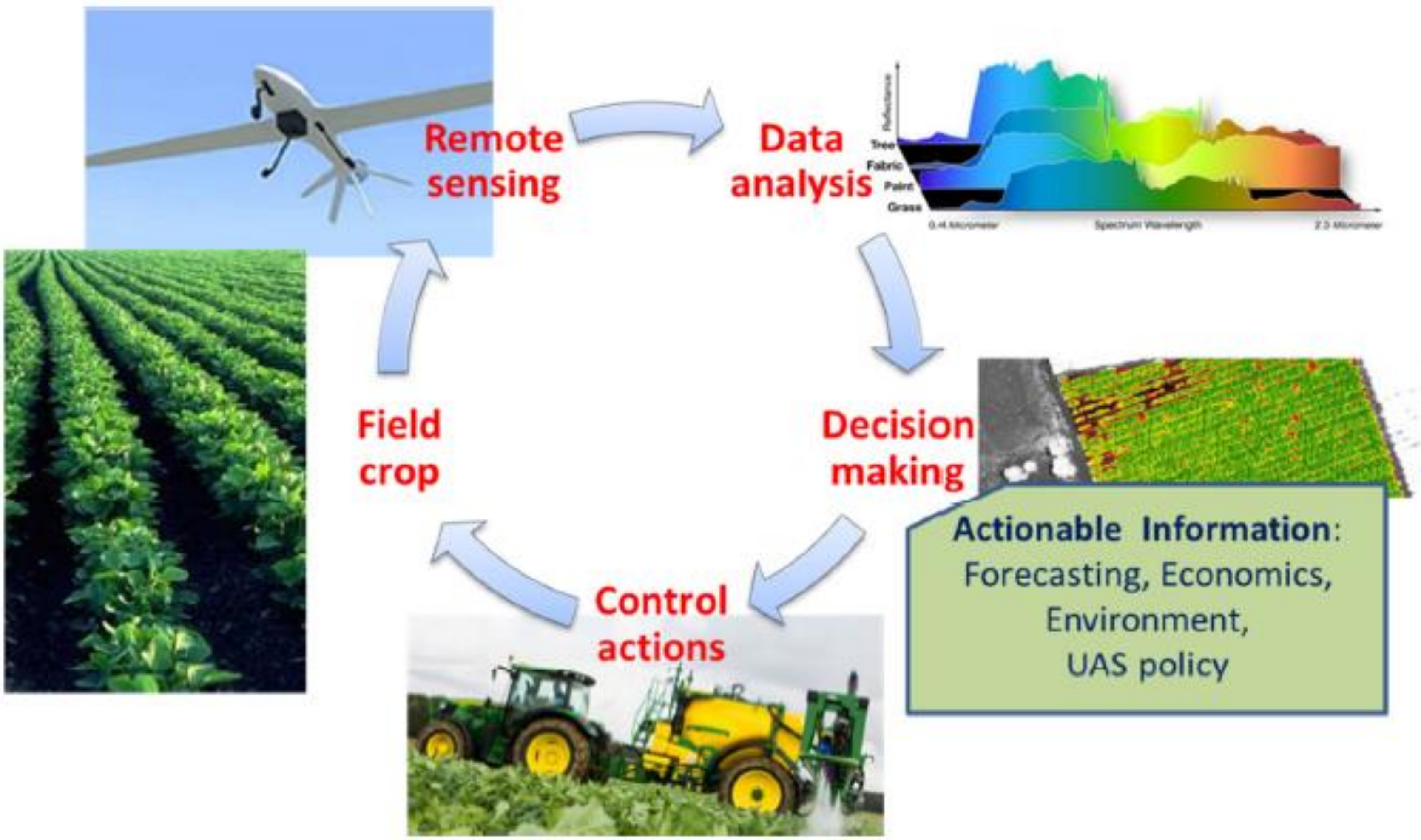
senseFly eBee
(Source: uncrate.com)



Sentera Vireo

- Donated to UMN in 2014
- Remote sensing applications, e.g. precision agriculture
- Mahon et al. “Research Flight Test Vehicle: Small Two Surface UAV,” UMN Technical Report, 2016.

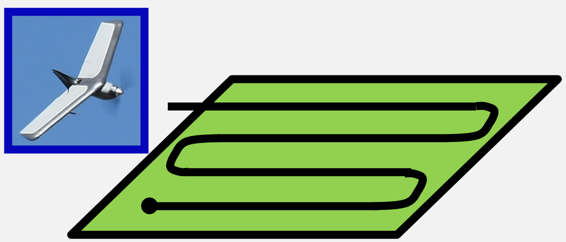
Precision Agriculture



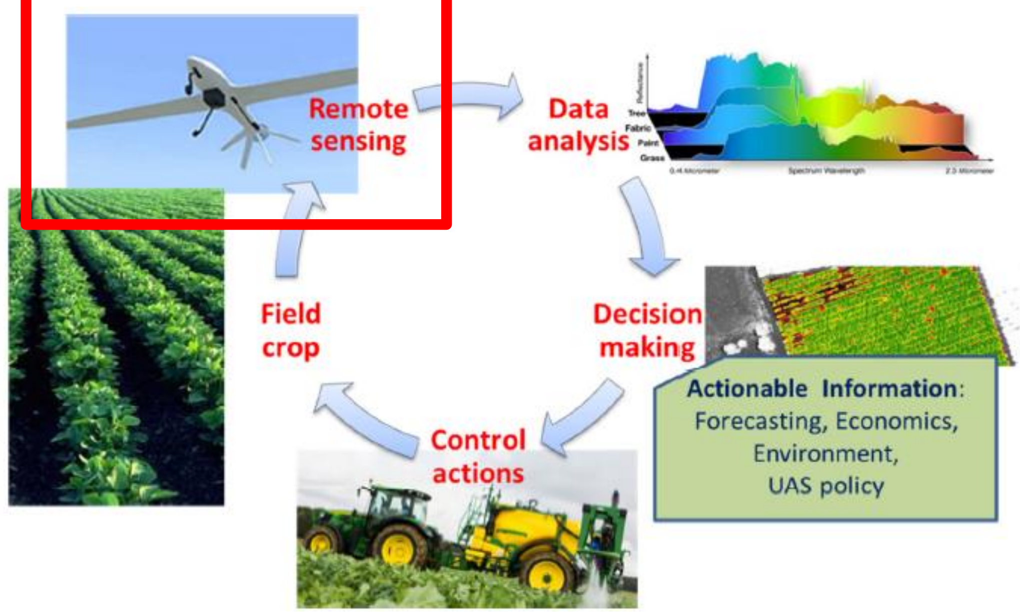
Precision Agriculture

Nominal mission

Lawnmower pattern contained within geo-fence perimeter

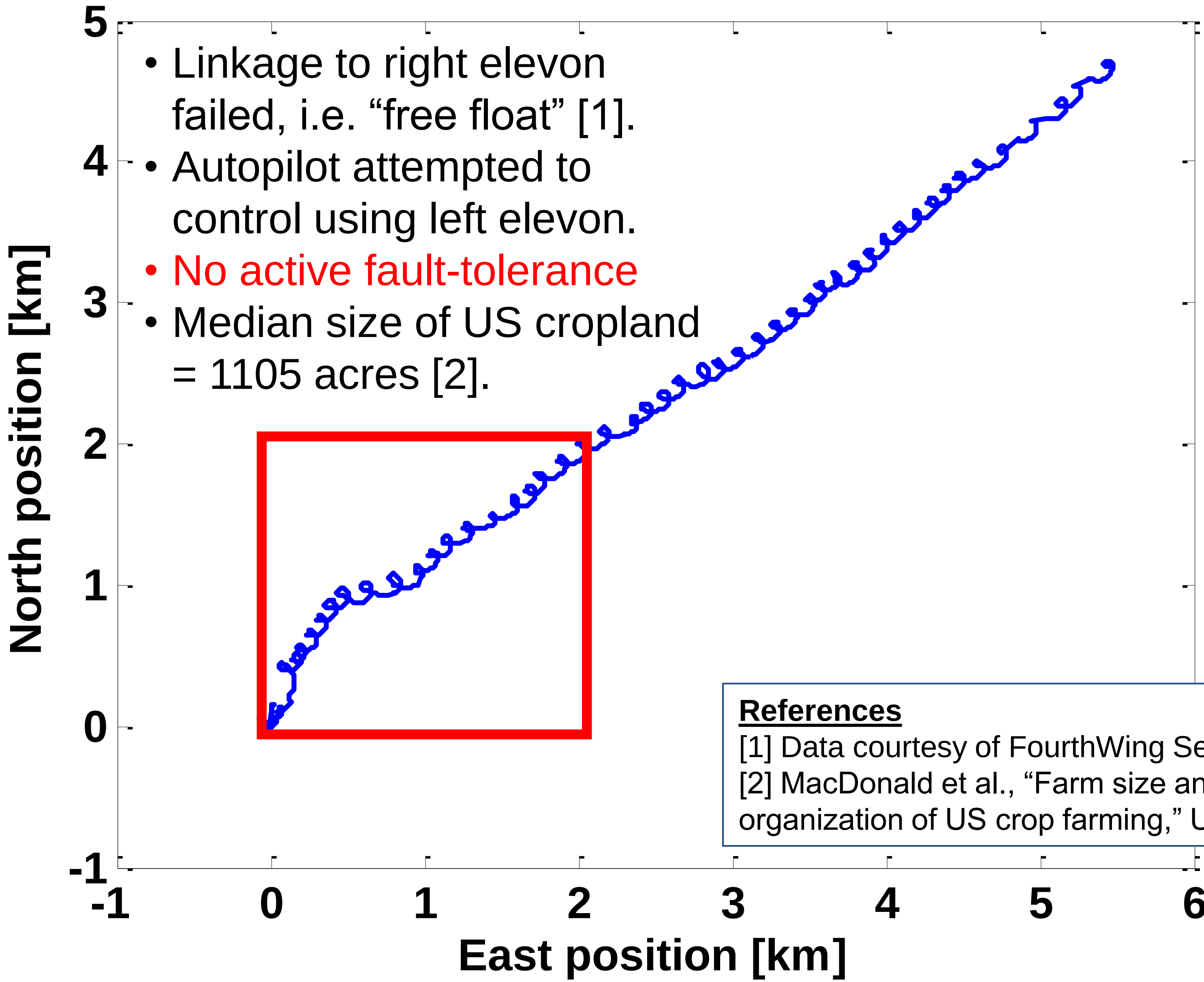


Atkins, "Autonomy as an enabler of economically-viable, beyond-line-of-sight, low-altitude UAS applications with acceptable risk," AUVSI, 2014.



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.
[2] MacDonald et al., “Farm size and the organization of US crop farming,” USDA, 2013.

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

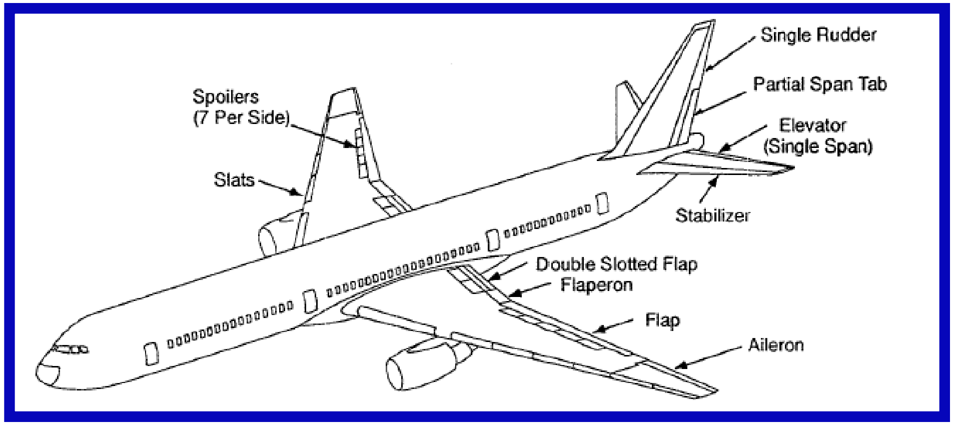
Boeing 777-200

- 301-440 seats
- Length=63.7m, Wingspan=60.9m
- Range < 17370km, Speed< M0.89
- Boeing's 1st Fly-by-Wire Aircraft
- Ref: Y.C. Yeh, "Triple-triple redundant 777 primary flight computer," 1996.

Fault Tolerance: Commercial Aircraft

Boeing 787-8 Dreamliner

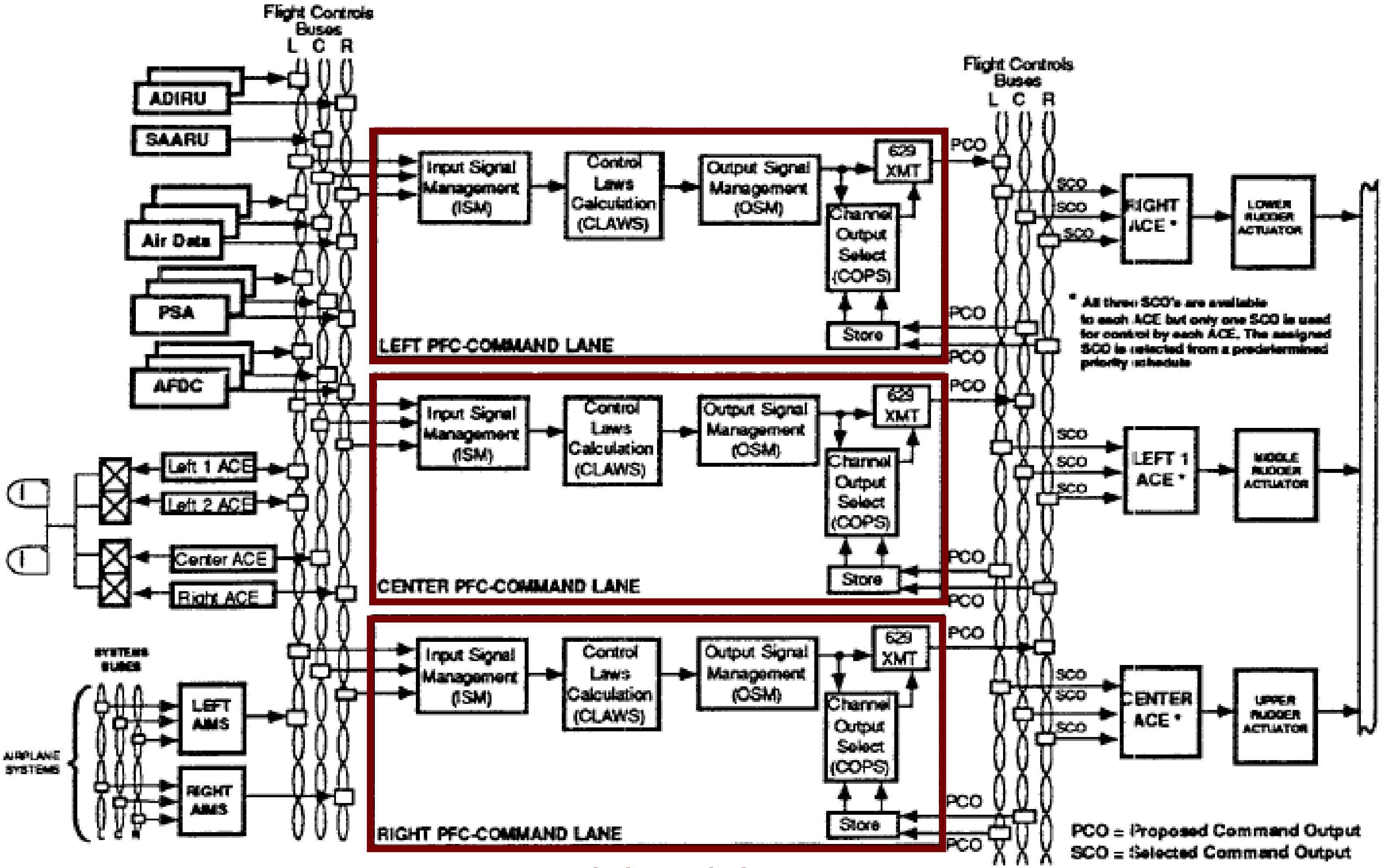
- 210-250 seats
- Length=56.7m, Wingspan=60.0m
- Range < 15200km, Speed< M0.89
- First Composite Airliner
- Honeywell Flight Control Electronics



Boeing 777-200

- 301-440 seats
- Length=63.7m, Wingspan=60.9m
- Range < 17370km, Speed< M0.89
- Boeing's 1st Fly-by-Wire Aircraft
- Ref: Y.C. Yeh, "Triple-triple redundant 777 primary flight computer," 1996.

777 Triple-Triple Architecture [Yeh, 96]



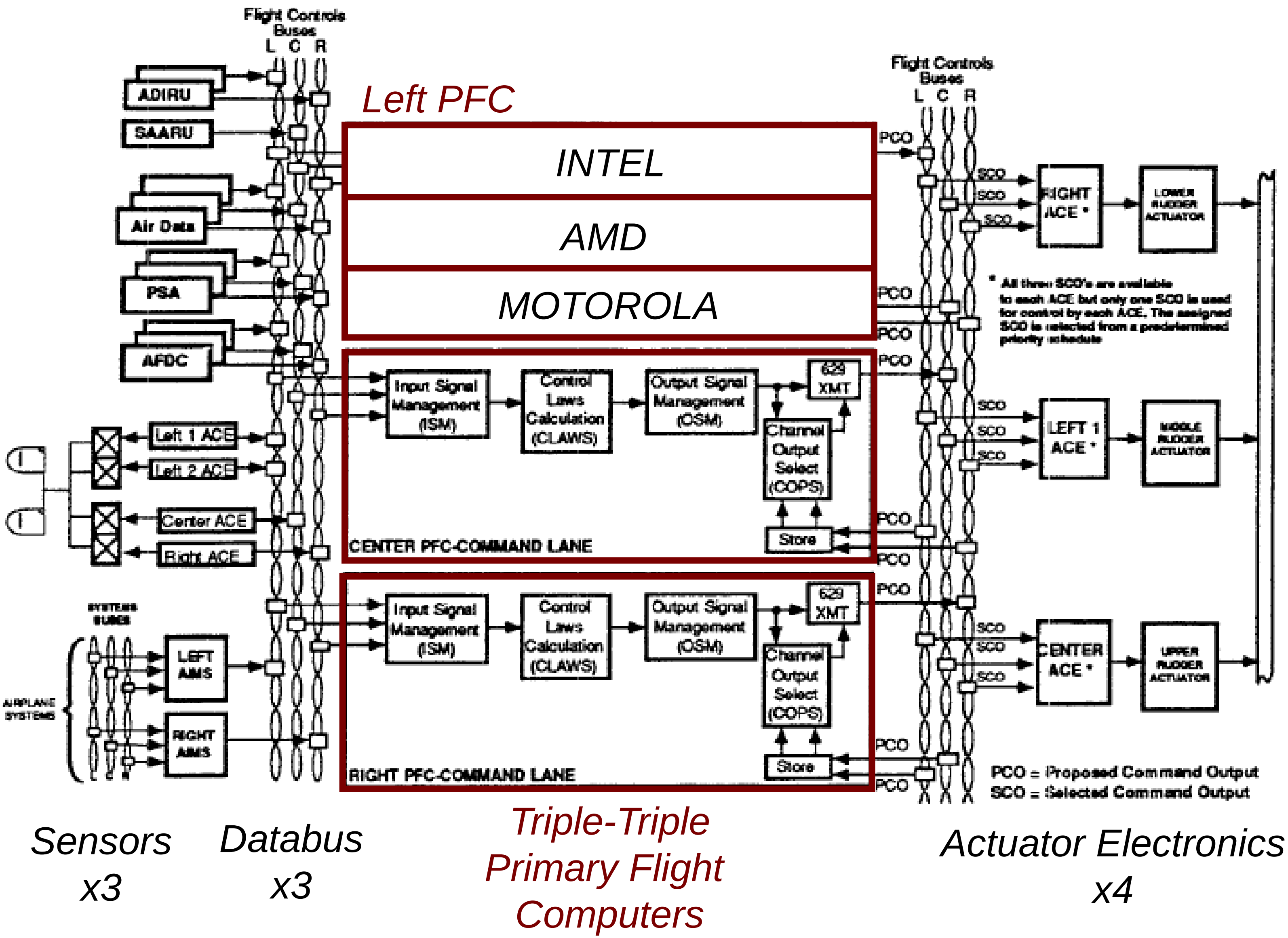
Sensors x3

Databus x3

Triple-Triple Primary Flight Computers

Actuator Electronics x4

777 Triple-Triple Architecture [Yeh, 96]



Reliability Comparison

Boeing 777

Reliability

- < 10^{-9} catastrophic failures per hour
- No single point of failure
- Protect against random & common failures

Design

- Hardware Redundancy
- Dissimilar hardware and software
- Limited use of analytical redundancy [1]
- Fault Trees, etc to certify

References

[1] Goupil, "Oscillatory failure case detection in the A380 electrical flight control system by analytical redundancy," Control Engineering Practice, 2010.

Reliability Comparison

Boeing 777

Reliability
- $< 10^{-9}$ catastrophic failures per hour
- No single point of failure
- Protect against random & common failures

Design
- Hardware Redundancy
- Dissimilar hardware and software
- Limited use of analytical redundancy [1]
- Fault Trees, etc to certify

Ultrastick 120

Reliability
- ~0.8 failures/100 hrs [2]
- Single points of failure

Design
- Limited by size, weight, power, and cost (SWAPC) constraints

References
[1] Goupil, "Oscillatory failure case detection in the A380 electrical flight control system by analytical redundancy," Control Engineering Practice, 2010.
[2] Amos et al., "UAV for Reliability Build," Technical Report, University of Minnesota, 2014.

Key Questions

Boeing 777

Ultrastick 120

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]

[1] Venkataraman & Seiler, Safe Flight Using One Aerodynamic Control Surface, AIAA, 2016.
[2] Venkataraman & Seiler, Model-Based Detection and Isolation of Rudder Faults for a Small UAS, AIAA, 2015.
[3] Lakshminarayan, et al, "Designing Reliability Into Small UAS Avionics“, Inside Unmanned Systems, 2016.
[4] Bauer, et al, “Fault Detection and Basic In-Flight Reconfiguration of a Small UAV…”, SafeProcess, 2018.
[5] Venkataraman, et al, Reliability Assessment of Actuator Architectures for Unmanned Aircraft, AIAA, 2016.
[6] Hu & Seiler, Pivotal decomposition for reliability analysis of fault tolerant control systems on UAVs, RESS, 2015.

Key Questions

Boeing 777

Ultrastick 120

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]

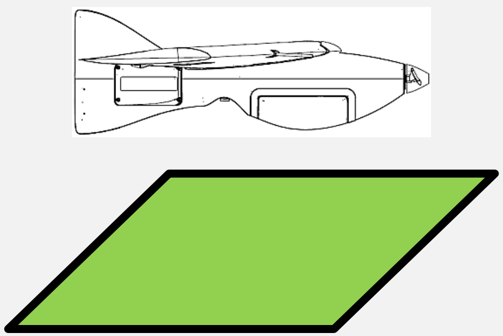
3. How can analytical methods be certified?

- Probabilistic analysis methods and extended fault trees [5,6]

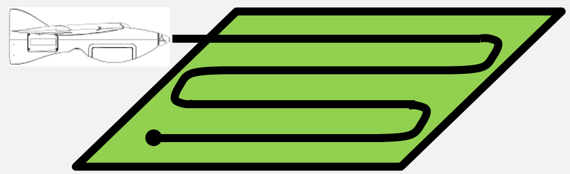
[1] Venkataraman & Seiler, Safe Flight Using One Aerodynamic Control Surface, AIAA, 2016.
[2] Venkataraman & Seiler, Model-Based Detection and Isolation of Rudder Faults for a Small UAS, AIAA, 2015.
[3] Lakshminarayan, et al, "Designing Reliability Into Small UAS Avionics", Inside Unmanned Systems, 2016.
[4] Bauer, et al, "Fault Detection and Basic In-Flight Reconfiguration of a Small UAV…", SafeProcess, 2018.
[5] Venkataraman, et al, Reliability Assessment of Actuator Architectures for Unmanned Aircraft, AIAA, 2016.
[6] Hu & Seiler, Pivotal decomposition for reliability analysis of fault tolerant control systems on UAVs, RESS, 2015.

Final Goal

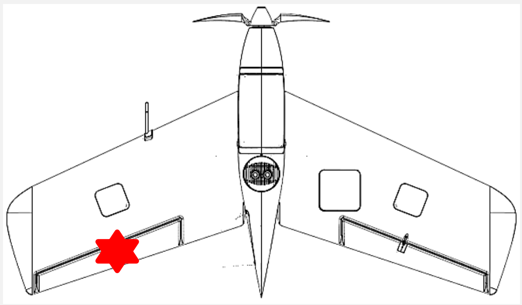
Takeoff



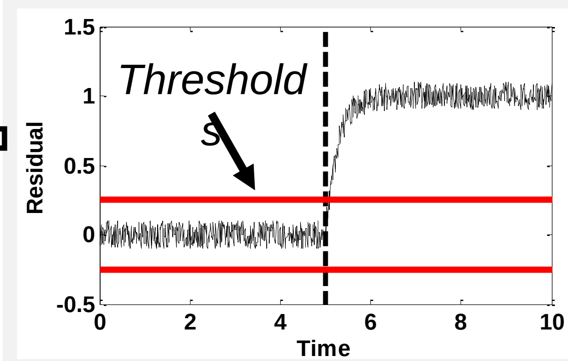
Nominal mission



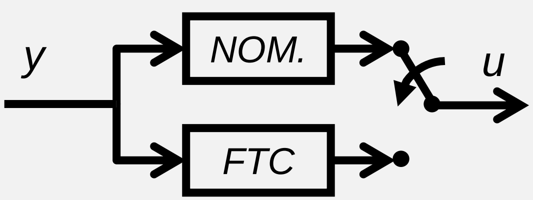
Control surface fault



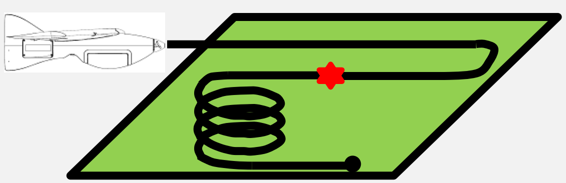
Fault diagnosis



Fault tolerant control



Safe landing



Flight With One Aero Surface

1. Ultrastick 120 [1]

Demonstrated closed-loop steady, level flight (2015).

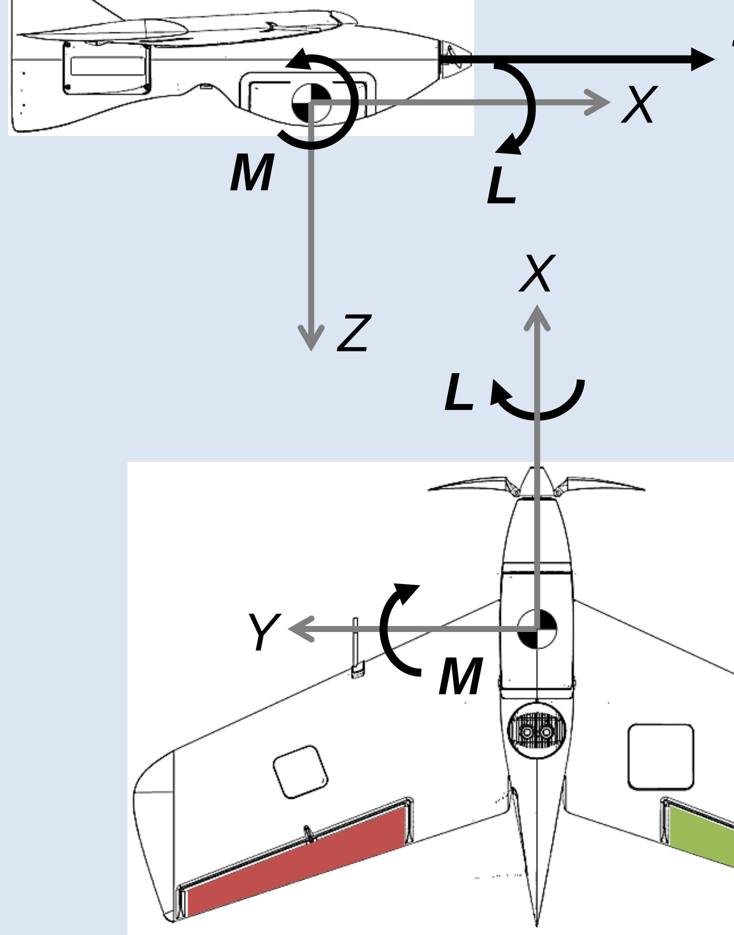
2. Senior Design [2]

Team designed and built flying wing. Demonstrated ability to land by human pilot (2016).

3. Sentera Vireo

Built avionics and performed first flights for sys id (2016). Plan to demonstrate closed-loop landing (2017).

Source: Sentera, LLC, 2016.



- *Control input simultaneously excites longitudinal and lateral-directional motion*
- *No direct yaw control*

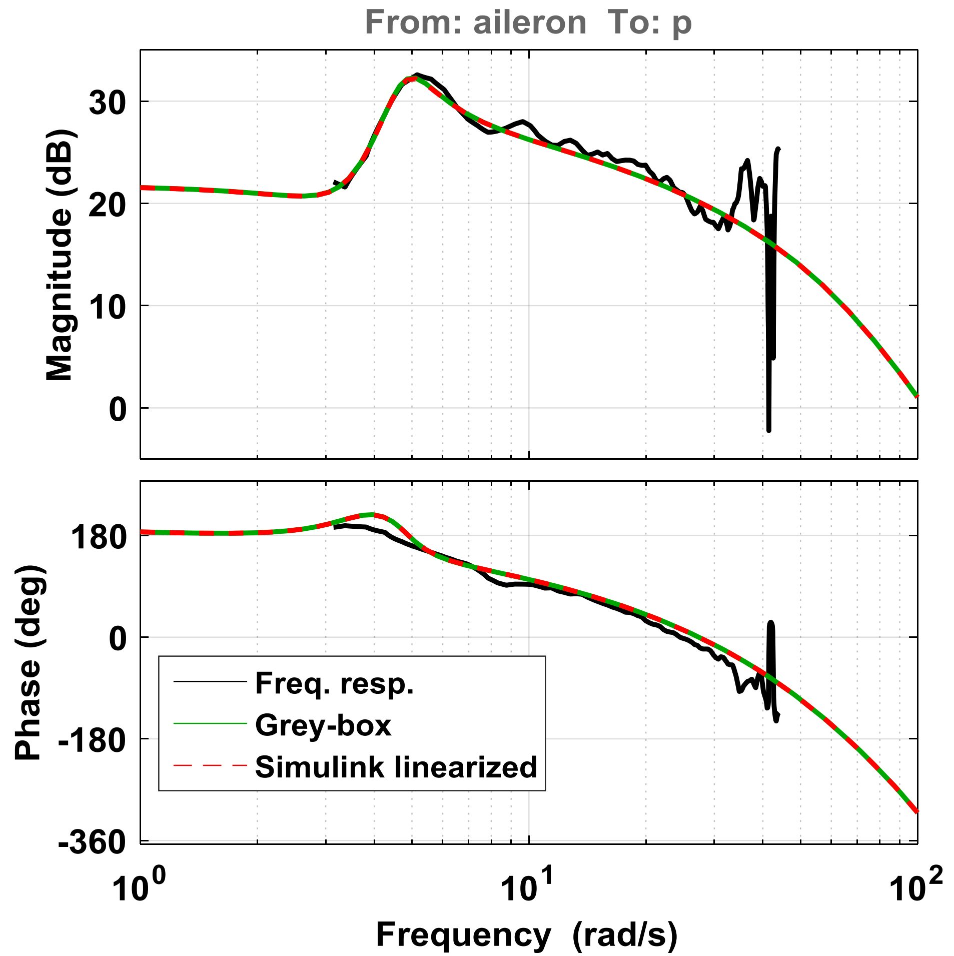
References

[1] Venkataraman & Seiler, AIAA 2016.

[2] Condron, et al, UMN Report, 2016.

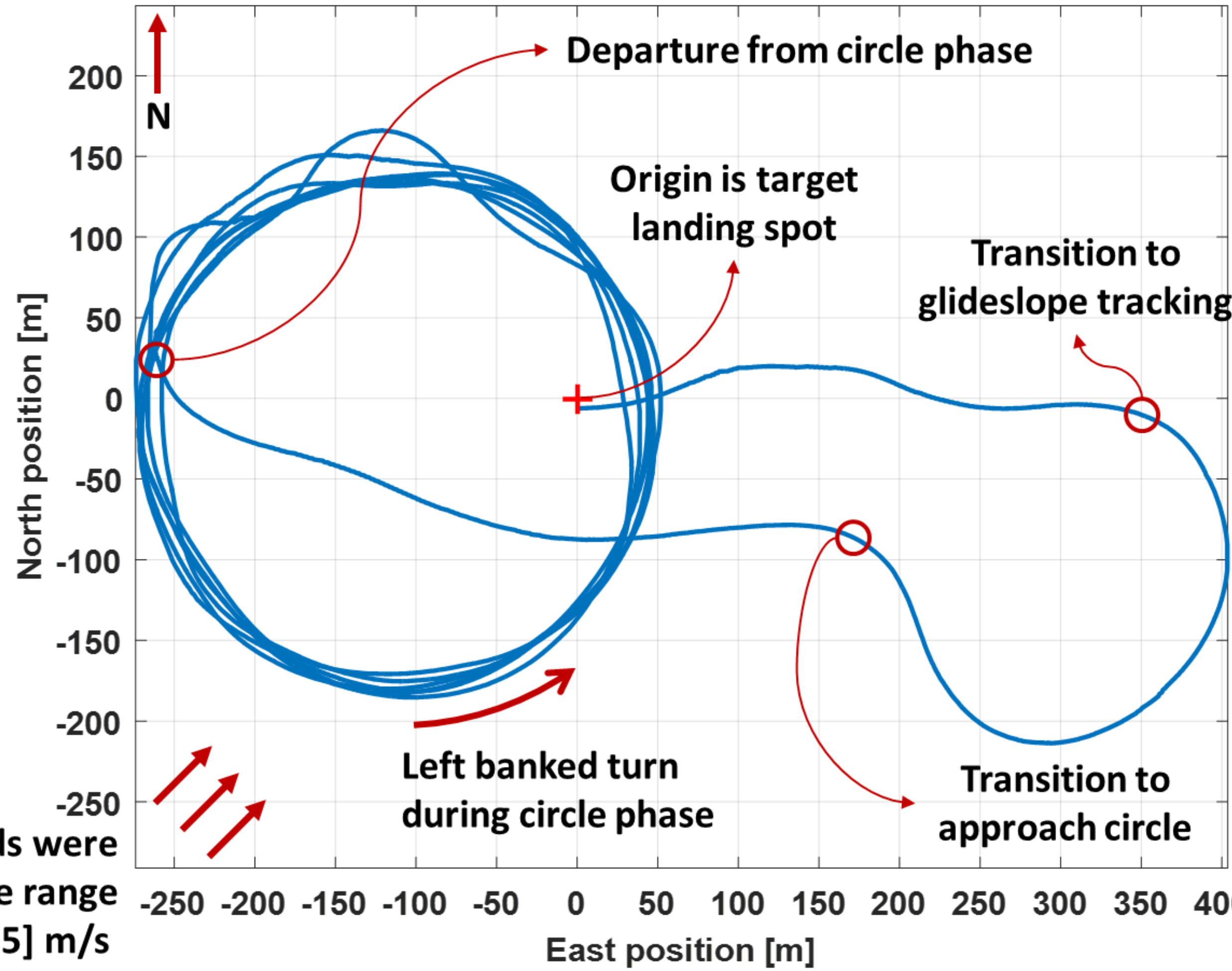
System Identification

- 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



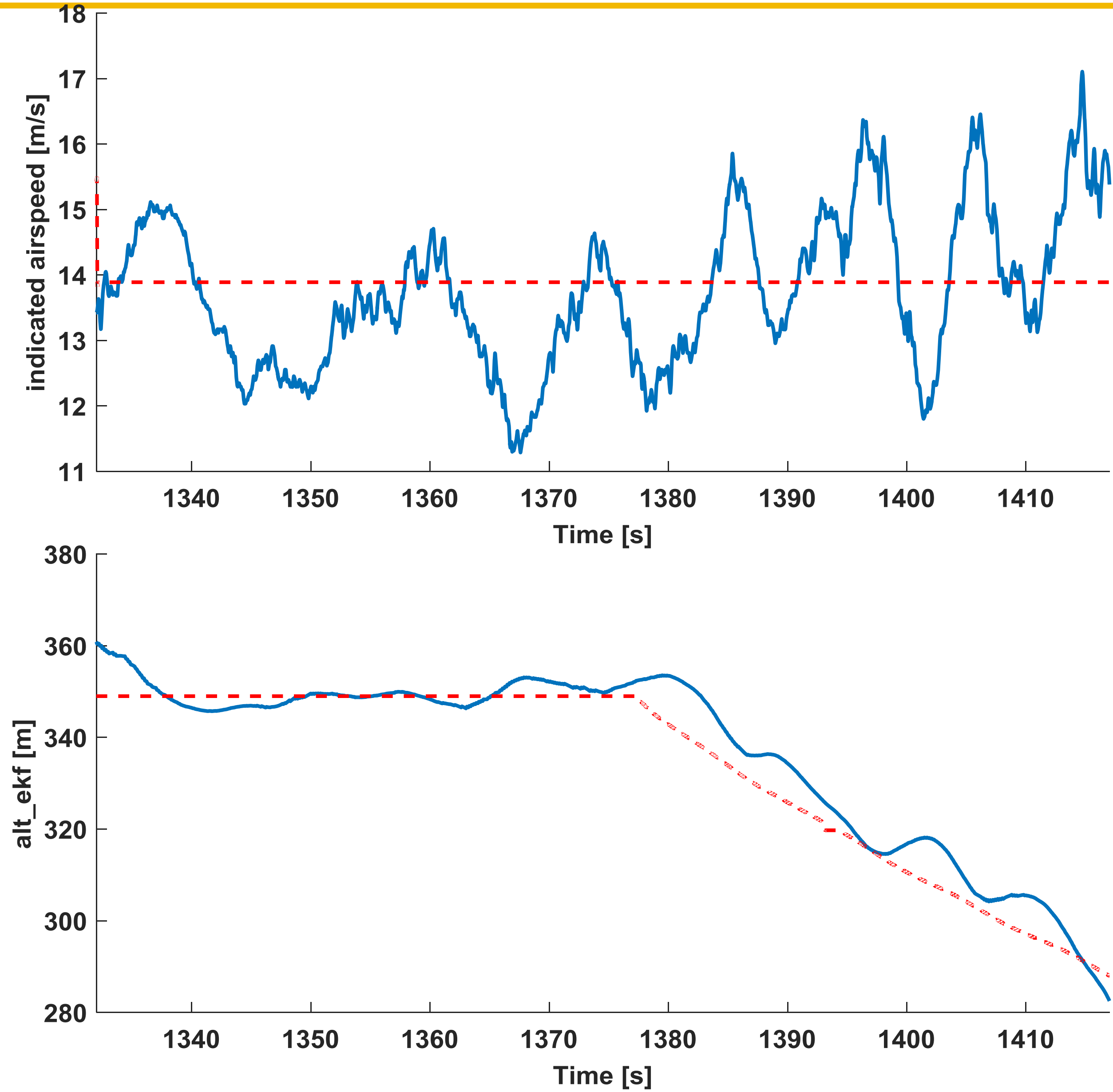
Single Surface Flight

- 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

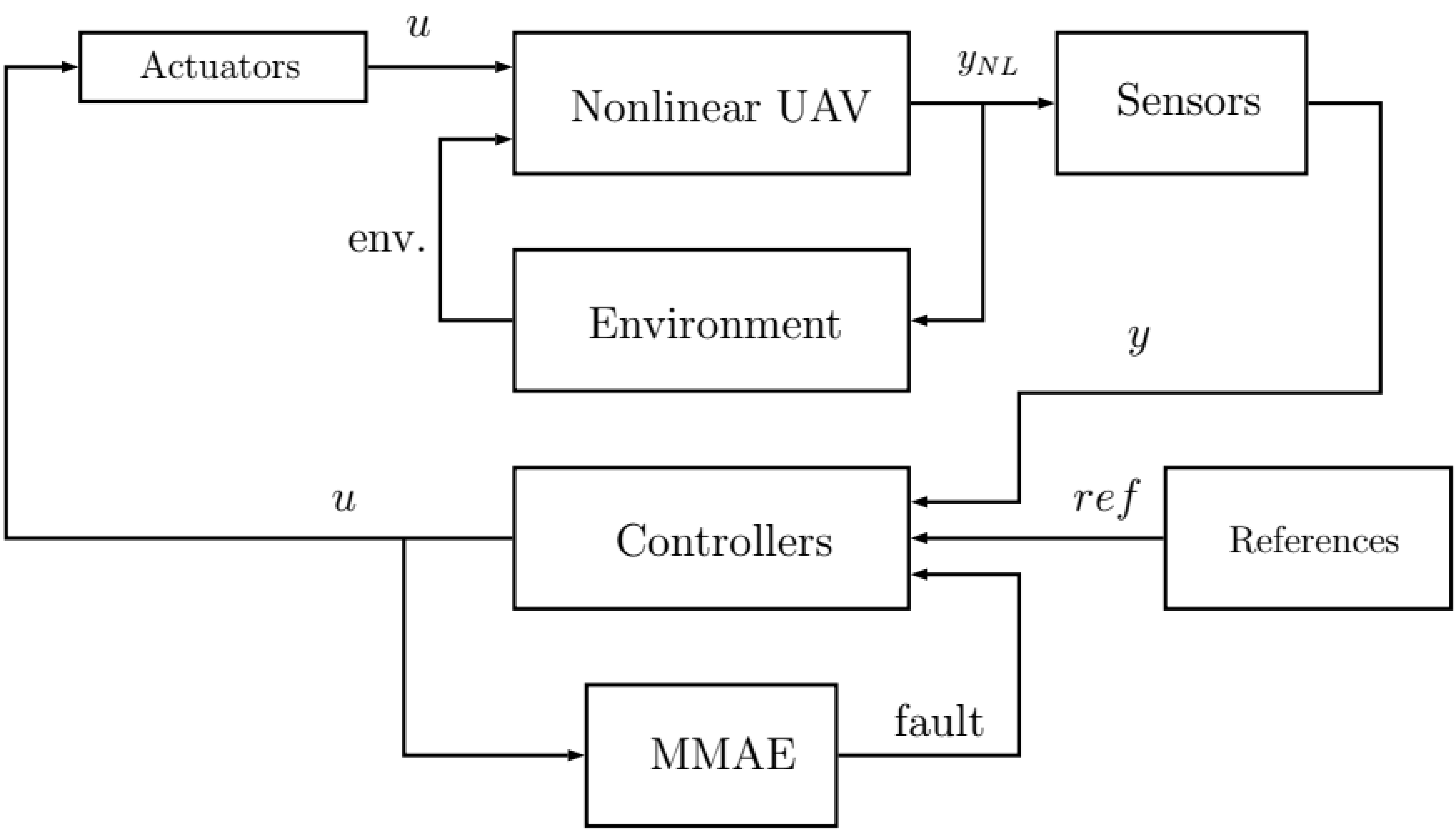


Winds were in the range [2.5, 5] m/s from SW.

Glideslope Tracking

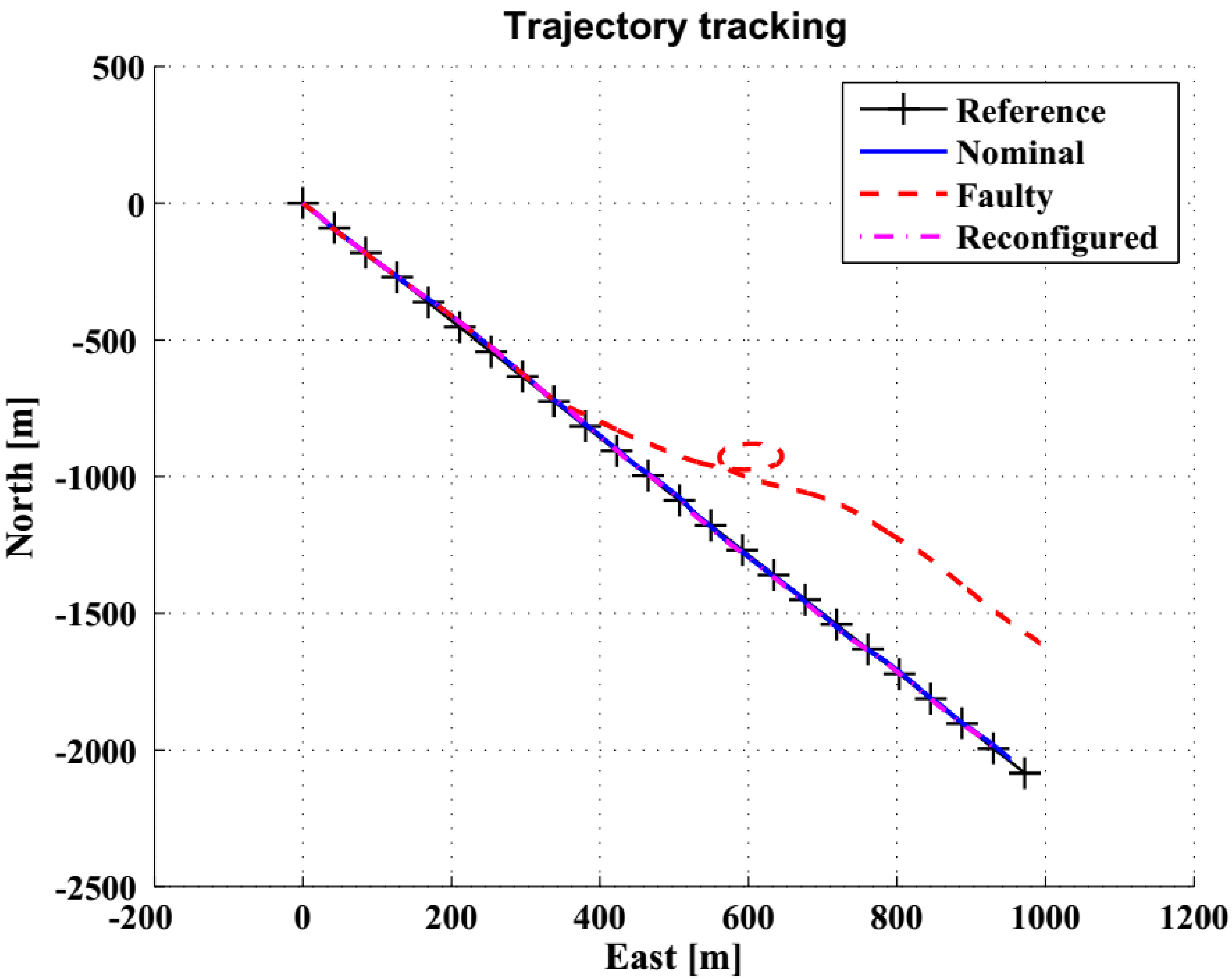


Fault Detection and Reconfiguration



Reference: Bauer, et al, "Fault Detection and Basic In-Flight Reconfiguration of a Small UAV Equipped with Elevons", SafeProcess, 2018.

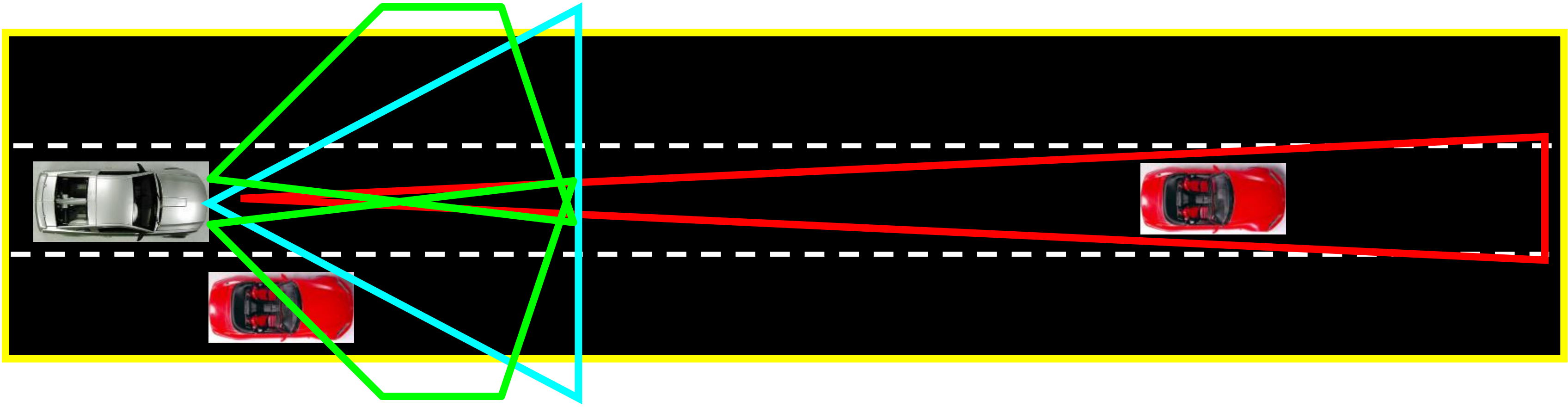
Fault Detection and Reconfiguration



Reference: Bauer, et al, "Fault Detection and Basic In-Flight Reconfiguration of a Small UAV Equipped with Elevons", SafeProcess, 2018.

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

Aurora FLIGHT SCIENCES

CMSoft

Schmidt & Associates

VirginiaTech Invent the Future®

LM BFF

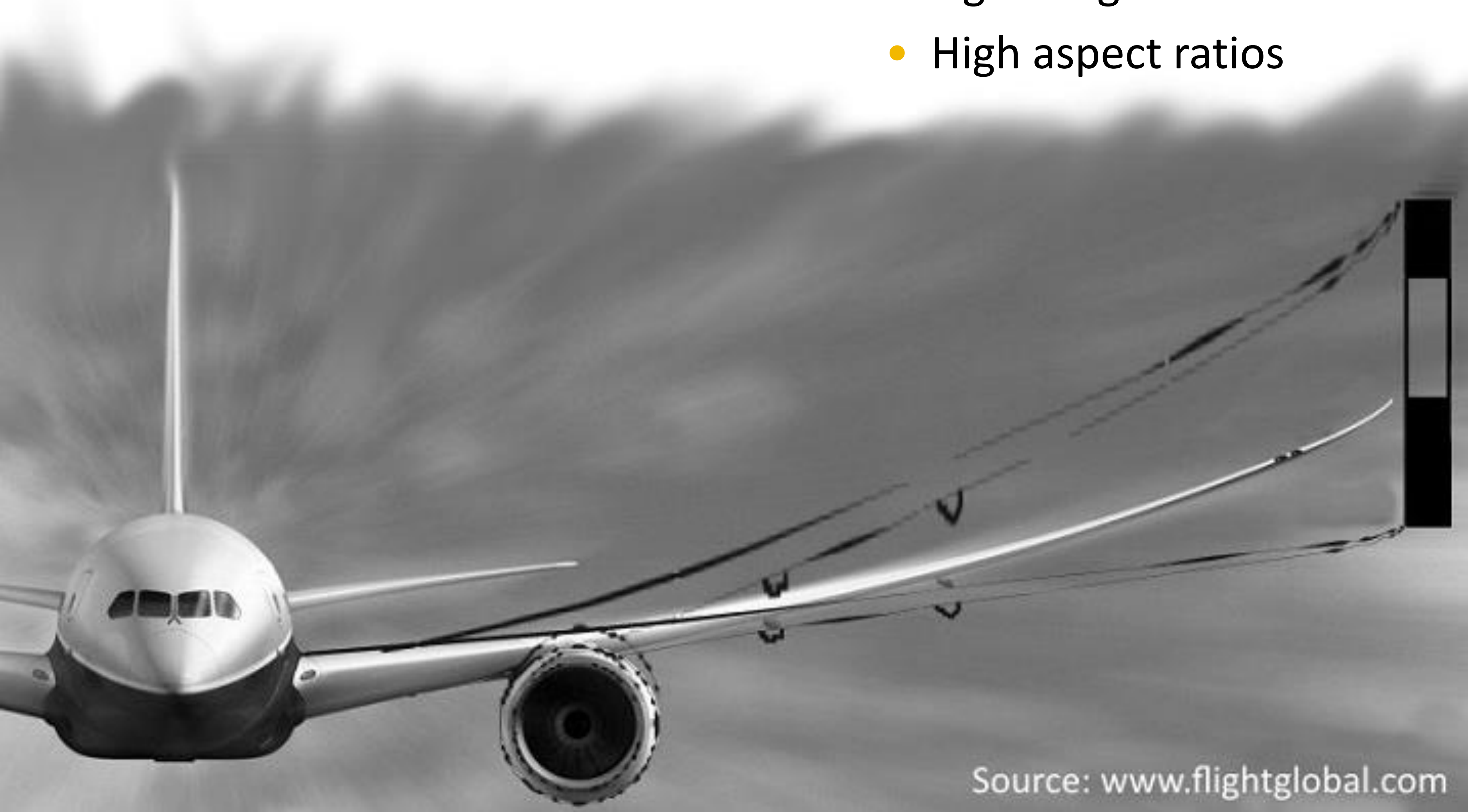
UMN Mini-Mutt

LM/NASA X-56

Aeroservoelasticity (ASE)

Efficient aircraft design

- Lightweight structures
- High aspect ratios

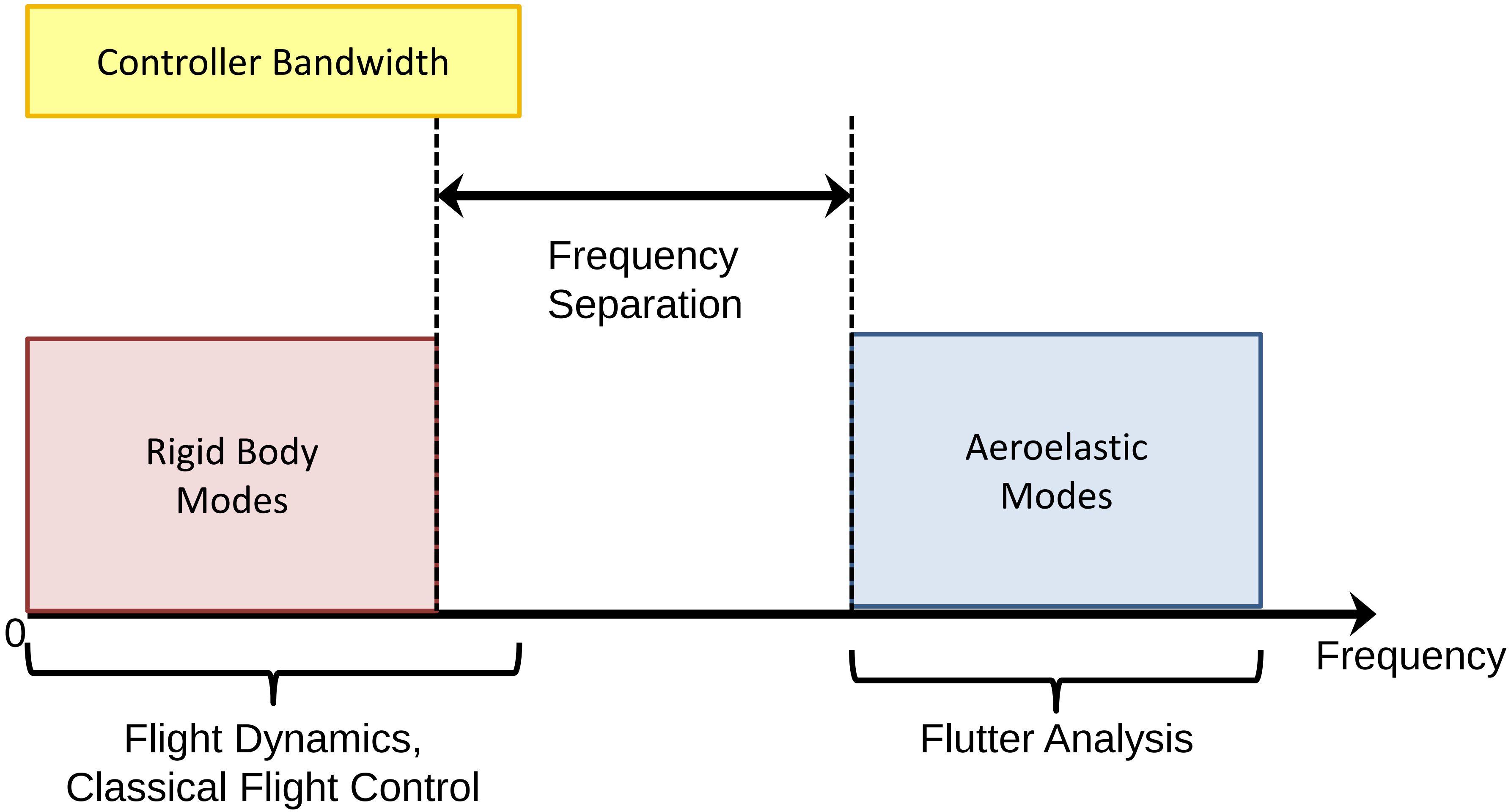


Source: www.flightglobal.com

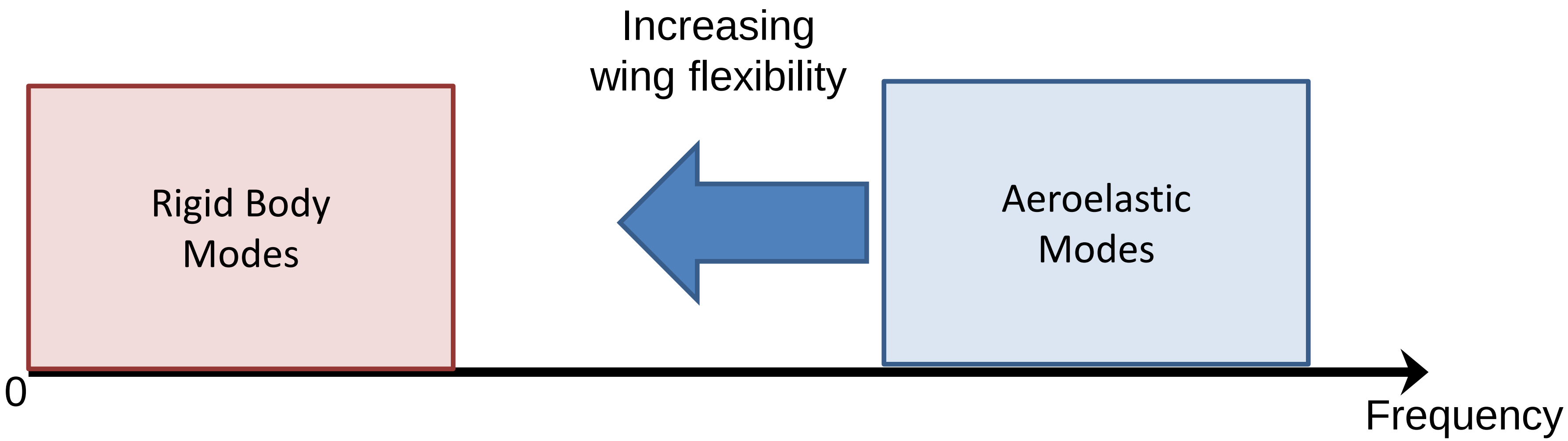
Flutter

Source: NASA Dryden Flight Research

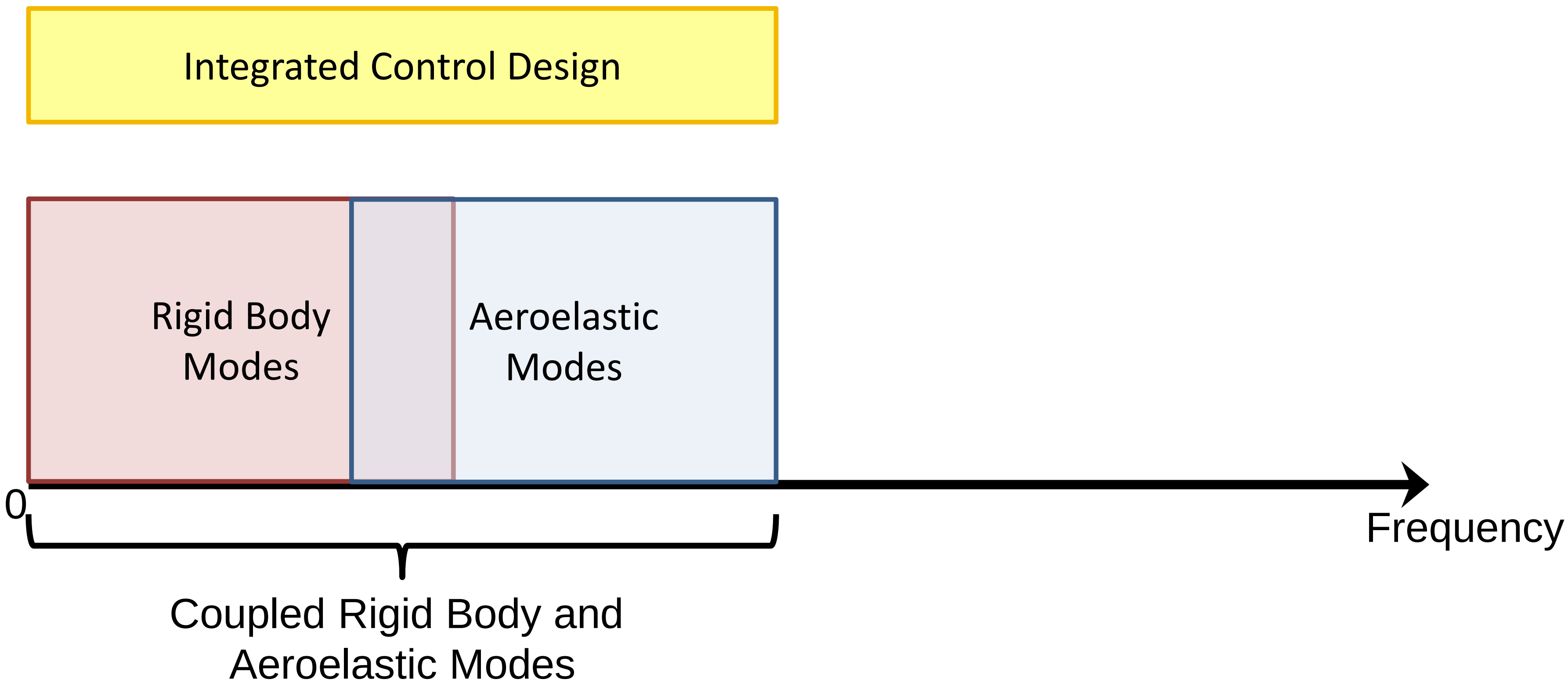
Classical Approach



Flexible Aircraft Challenges

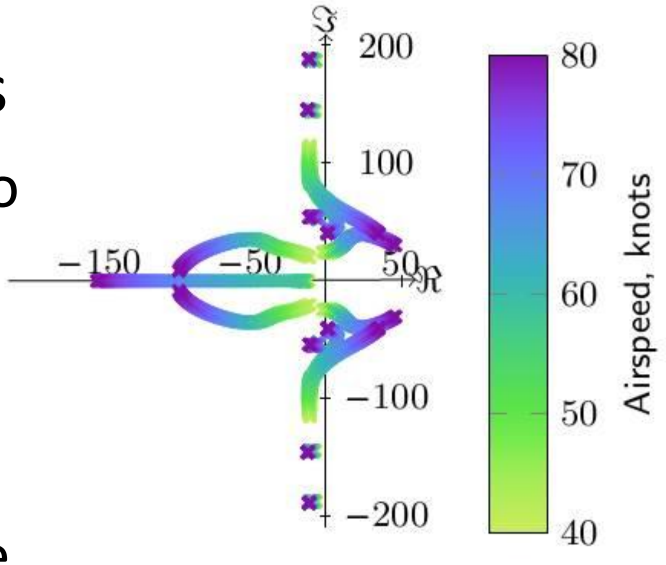


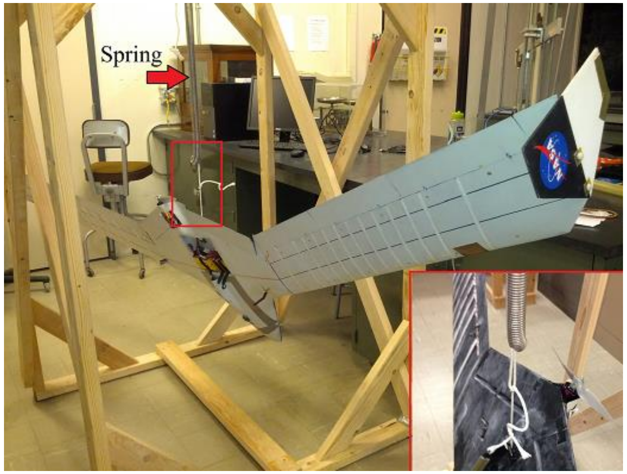
Flexible Aircraft Challenges



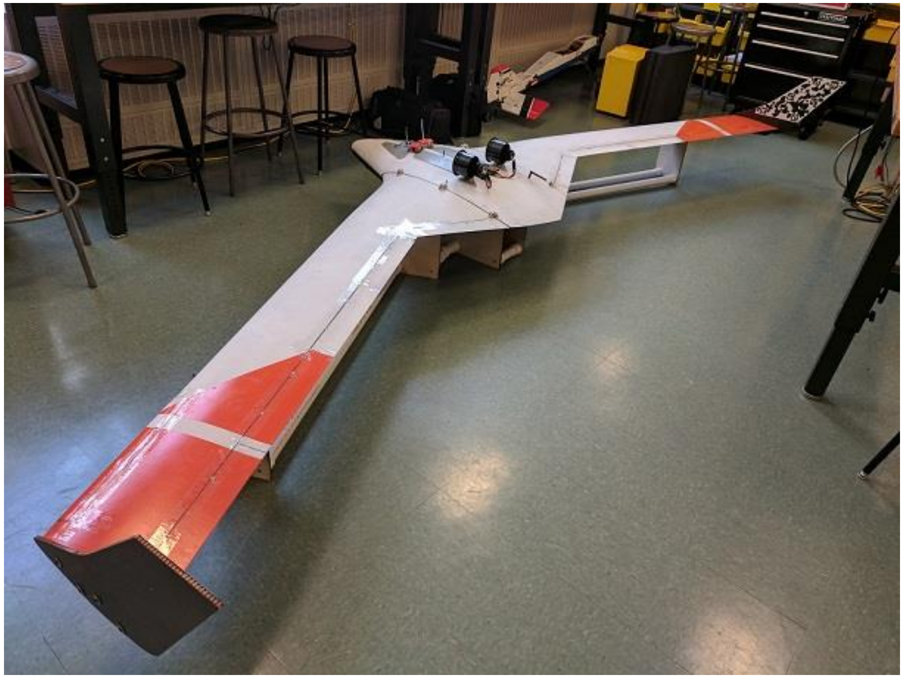
Modeling and Control for Flex Aircraft

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

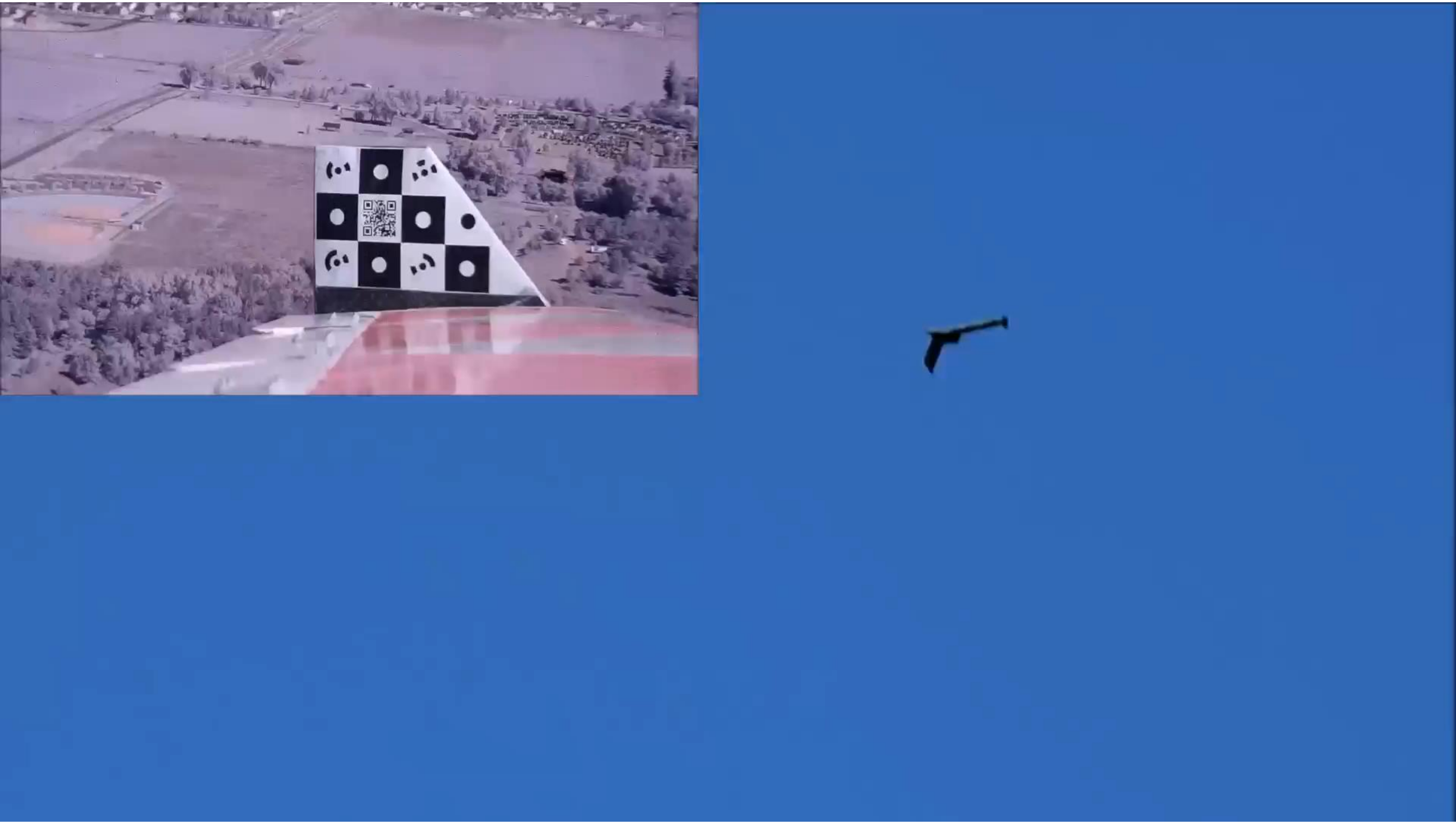


mAEWing1
10 foot wingspan
~14 pounds
Laser-scan replica of BFF
4 aircraft, >50 flights

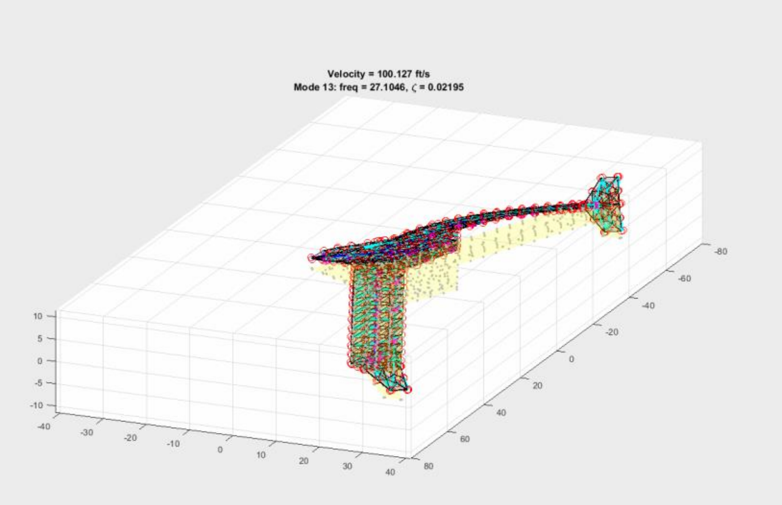
mAEWing2
14 foot wingspan
~42 pounds
Half-scale X-56
Currently ground testing

mAEWing1 and 2

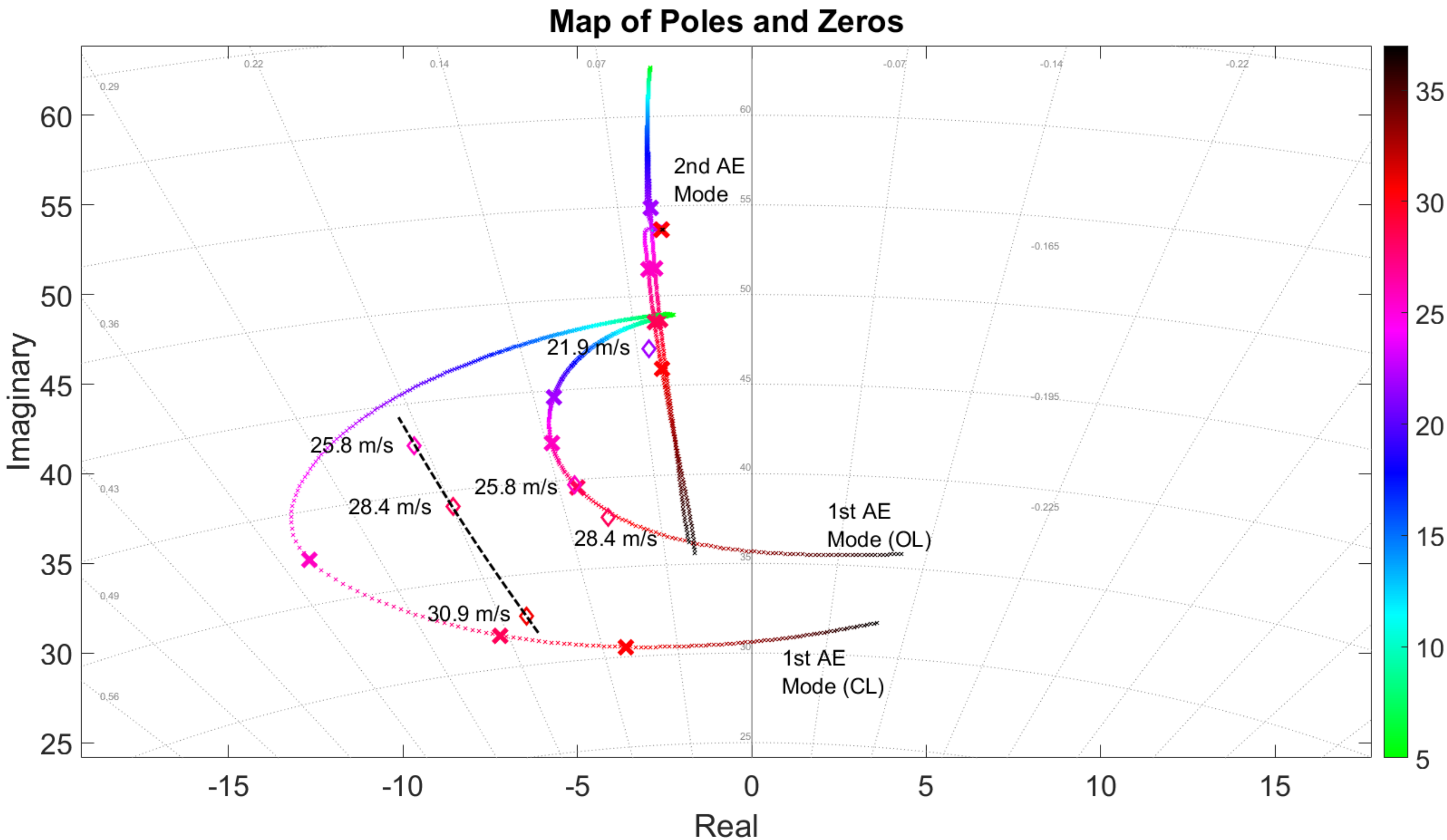
Open-Loop Flutter



Body Freedom Flutter

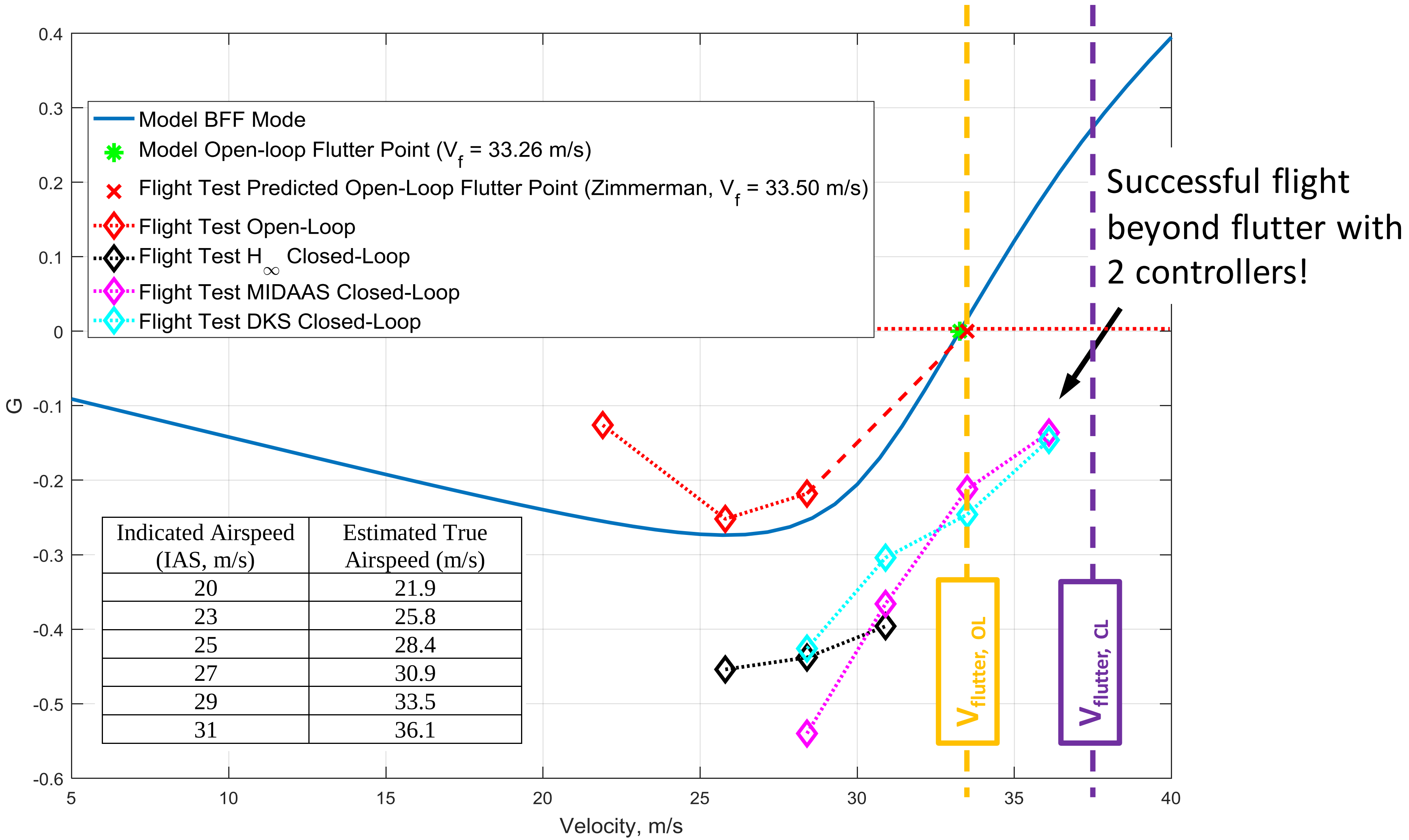


Pole Map for H-Inf Controller



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.

Flight Test Summary



Indicated Airspeed (IAS, m/s)	Estimated True Airspeed (m/s)
20	21.9
23	25.8
25	28.4
27	30.9
29	33.5
31	36.1

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

Time-Varying Systems

Wind Turbine
Periodic /
Parameter-Varying

Flexible Aircraft
Parameter-Varying

Vega Launcher
Time-Varying
(Source: ESA)

Robotics
Time-Varying
(Source: ReWalk)

Issue: Few numerically reliable methods to assess the robustness of time-varying systems.

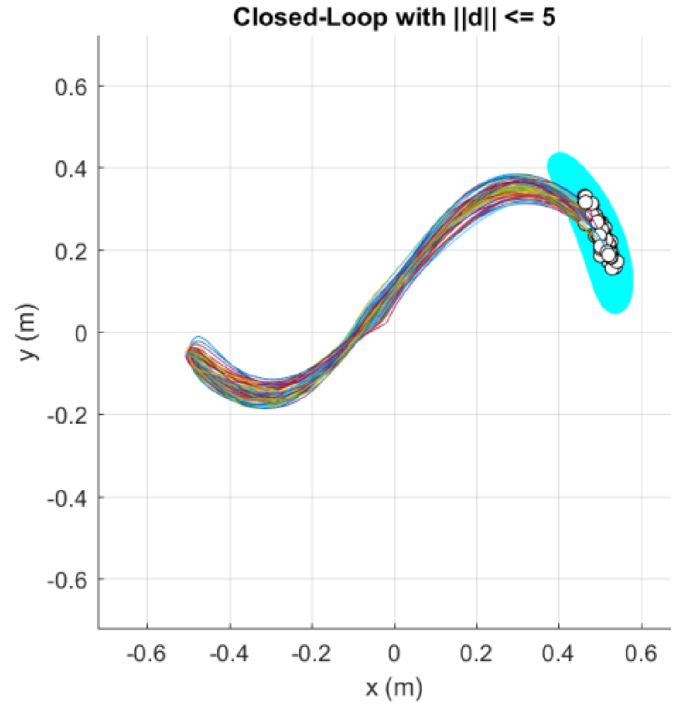
Analysis Objective

Goal: Assess the robustness of linear time-varying (LTV) systems on finite horizons.

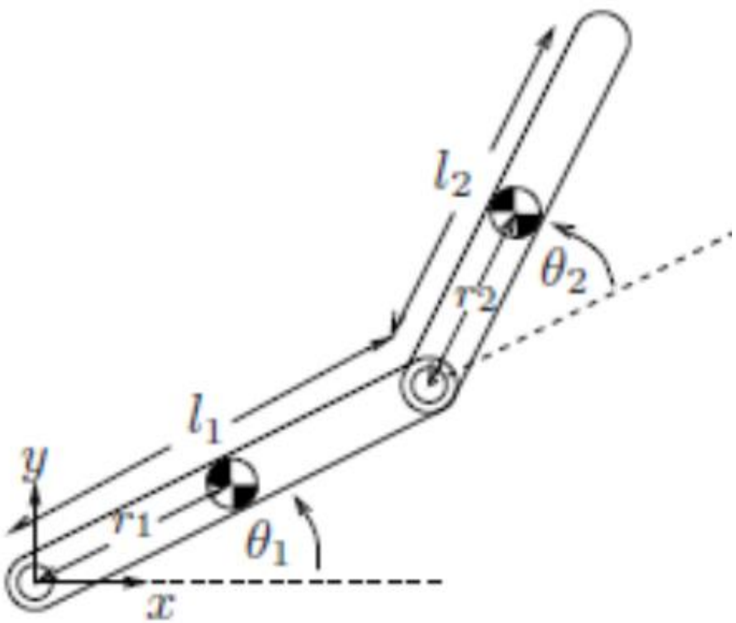
Approach: Classical Gain/Phase Margins focus on (infinite horizon) stability and frequency domain concepts.

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.



Two-Link Robot Arm



Two-Link Diagram [MZS]

Nonlinear dynamics [MZS]:

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

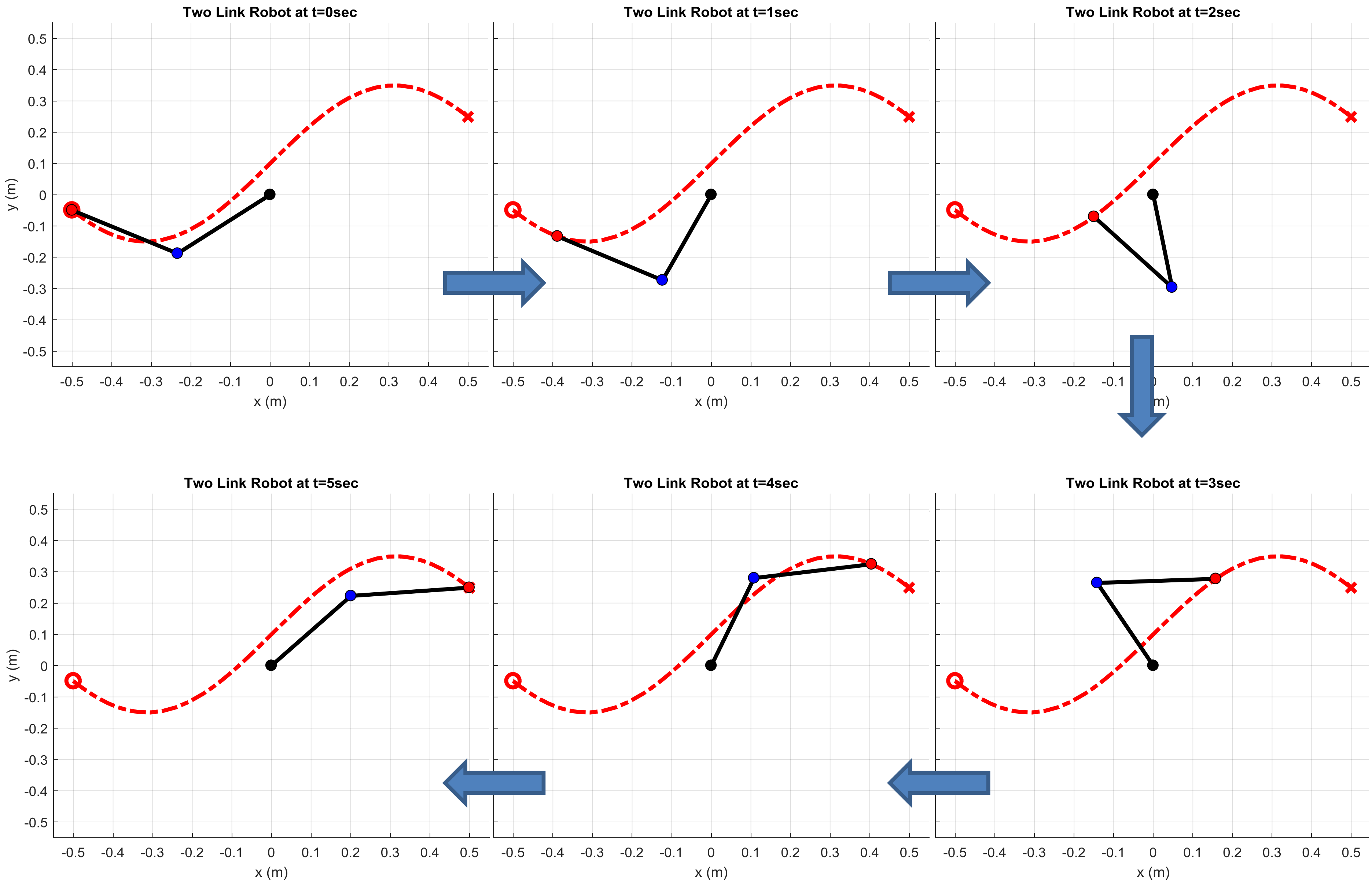
where

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

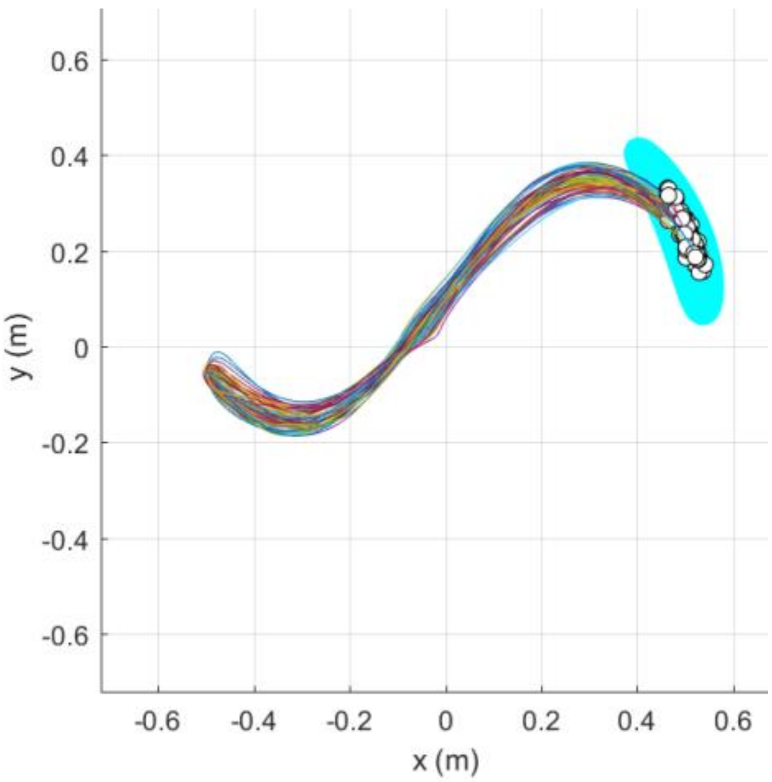
τ and d are control torques and disturbances at the link joints.

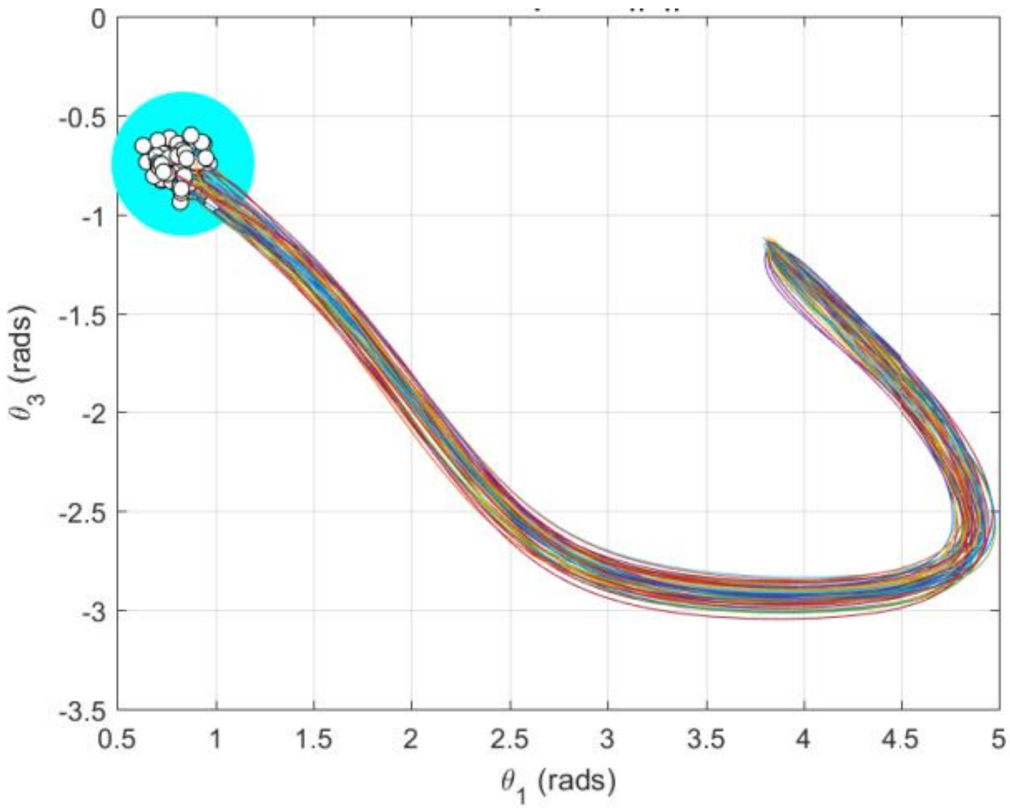
[MZS] R. Murray, Z. Li, and S. Sastry. *A Mathematical Introduction to Robot Manipulation*, 1994.

Nominal Trajectory (Cartesian Coords.)



Effect of Disturbances / Uncertainty





Cartesian Coords.

Joint Angles

Overview of Analysis Approach

Nonlinear dynamics:

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

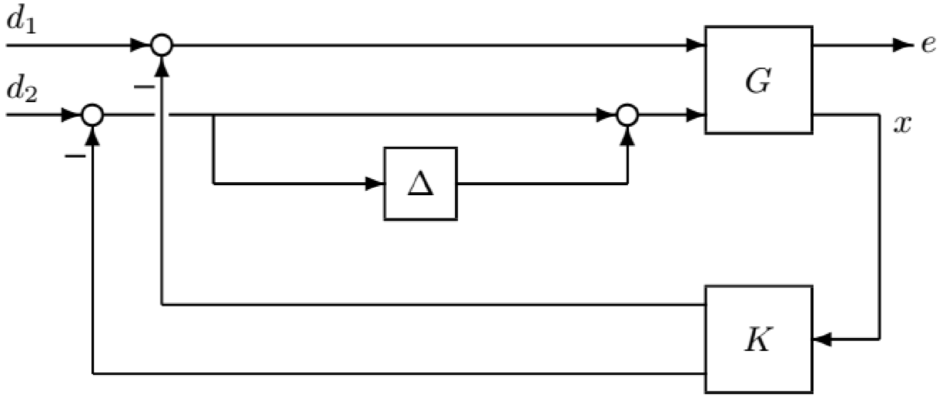
Linearize along a (finite –horizon) trajectory $(\bar{\eta}, \bar{\tau}, d = 0)$

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

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

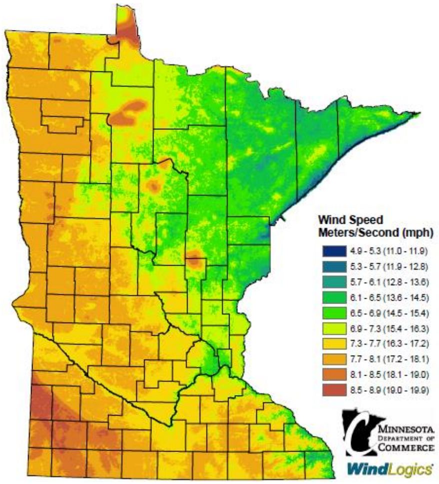
- US National Science Foundation
  - Grant No. NSF-CMMI-1254129: "CAREER: Probabilistic Tools for High Reliability Monitoring and Control of Wind Farms." Prog. Manager: J. Berg.
  - Grant No. NSF/CNS-1329390: "CPS: Breakthrough: Collaborative Research: Managing Uncertainty in the Design of Safety-Critical Aviation Systems". Prog. Manager: D. Corman.
- NASA
  - NRA NNX14AL36A: "Lightweight Adaptive Aeroelastic Wing for Enhanced Performance Across the Flight Envelope," Tech. Monitor: J. Ouelette.
  - NRA NNX12AM55A: "Analytical Validation Tools for Safety Critical Systems Under Loss-of-Control Conditions." Tech. Monitor: C. Belcastro.
  - SBIR contract #NNX12CA14C: "Adaptive Linear Parameter-Varying Control for Aeroservoelastic Suppression." Tech. Monitor. M. Brenner.
- Eolos Consortium and Saint Anthony Falls Laboratory
  - http://www.eolos.umn.edu/ & http://www.safl.umn.edu/

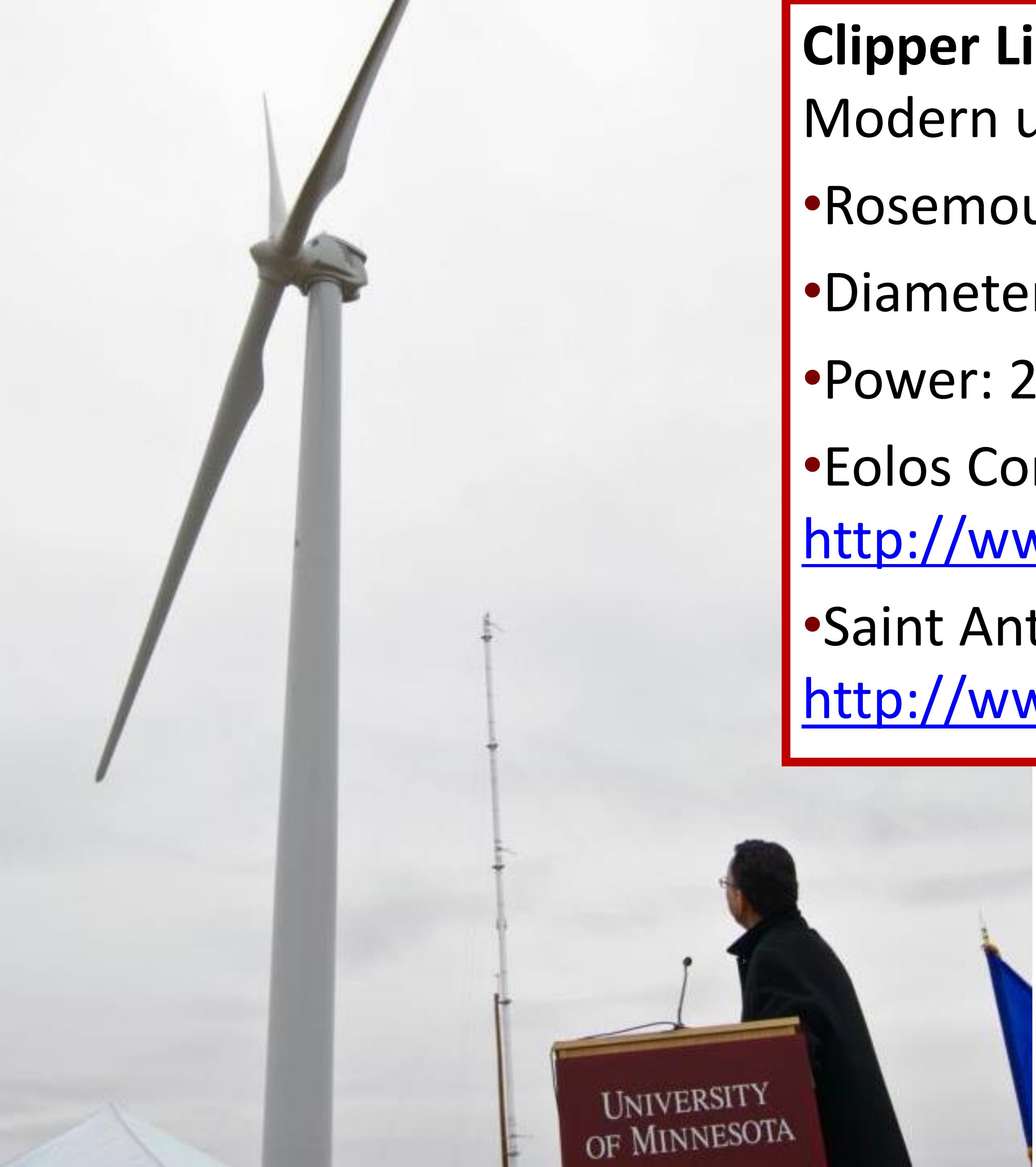
Backup

Modeling and Control for Wind Energy

Jen Annoni, Shu Wang, Daniel Ossmann, Parul Singh, Jordan Hoyt, Sanjana Vijayshankar

(with support from SAFL/EOLOS)





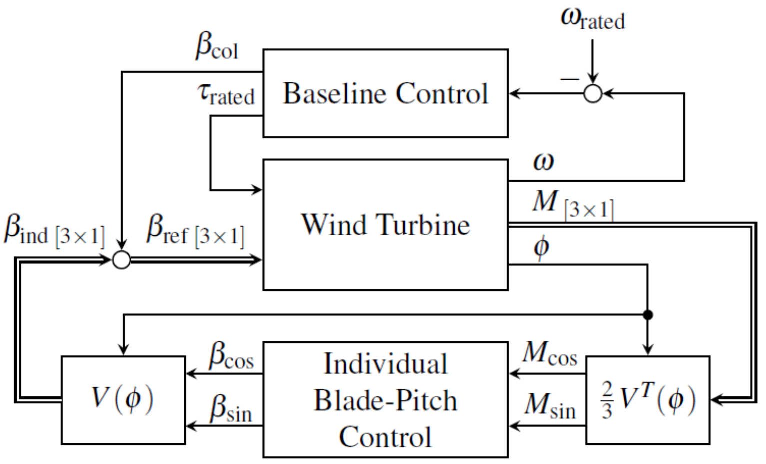
Clipper Liberty, 2012:
Modern utility-scale turbine.

- Rosemount, MN.
- Diameter: 96m
- Power: 2.5MW
- Eolos Consortium: http://www.eolos.umn.edu/
- Saint Anthony Falls Lab: 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

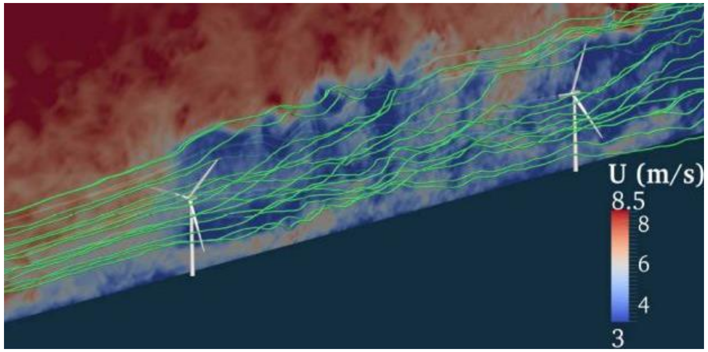
Ref: Ossmann, Theis, Seiler, '16 ASME DSCC, Best Energy Paper Award

Modeling and Control for Wind Farms

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

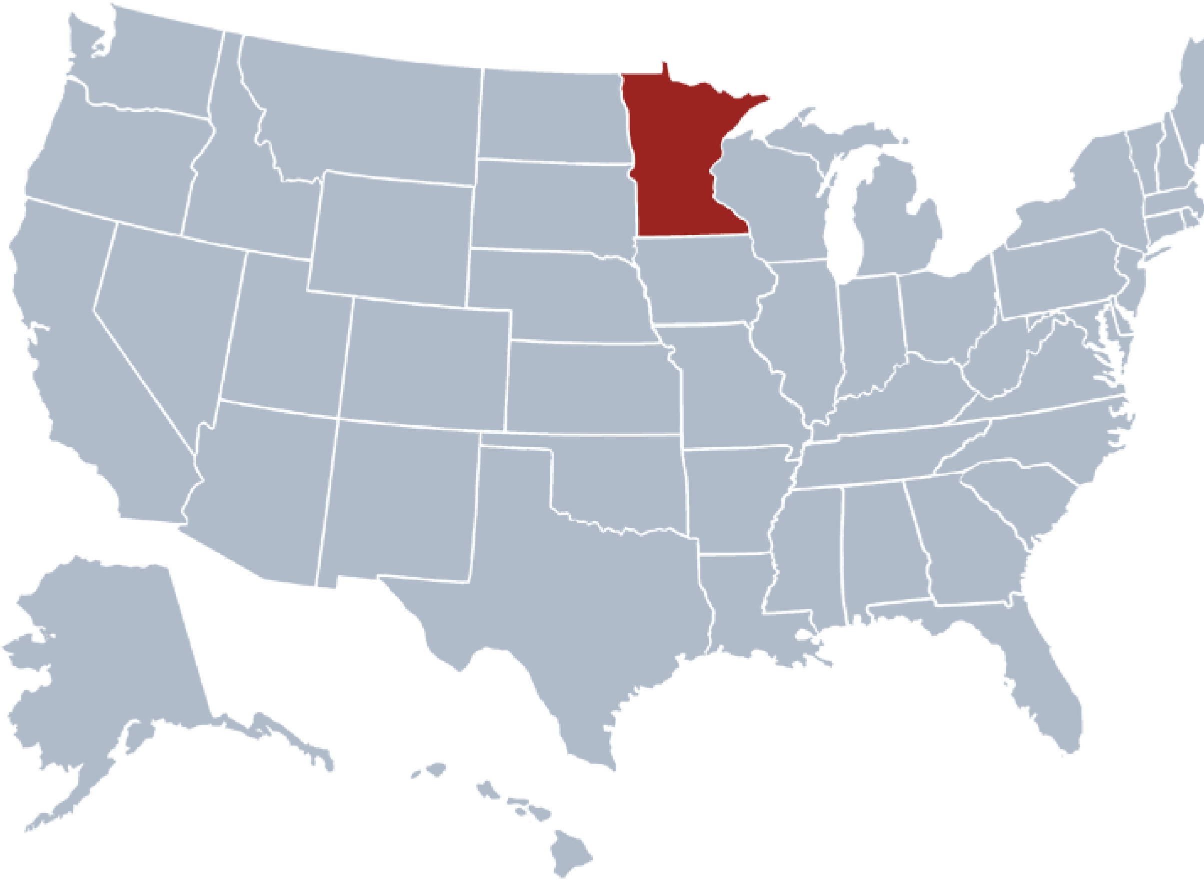
Eolos: http://www.eolos.umn.edu/

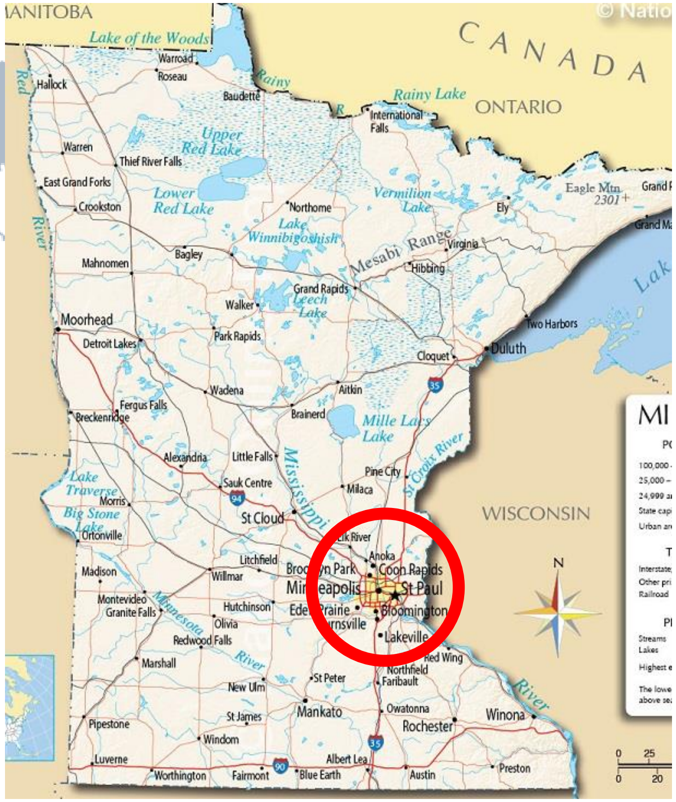
Saint Anthony Falls: http://www.safl.umn.edu/



Simulator for Wind Farm Applications, Churchfield & Lee
http://wind.nrel.gov/designcodes/simulators/SOWFA

Minneapolis and St. Paul, Minnesota





- Twin Cities Population ~3.5Million
- Average daily low/high in January is -15.4^{o}C / -5.6^{o}C
- Strong outdoor culture with many lakes and bike trails

Department History

Akerman Tailless Aircraft

John D. Akerman was first Department Head 1929 - 1957

- Born in Latvia late 1890's
- Studied with Niklolai Joukowsky
- Acquainted with Igor Sikorsky

1930's
Cellophane Stratosphere Balloon
Ascent in Memorial Stadium

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