Integrated Safety Envelopes

Built-in Restrictions of Navigable Airspace

Edward A. Lee
Professor, EECS, UC Berkeley

With thanks to:
Adam Cataldo (Berkeley)
David Corman (Boeing)
Peter Huber (Forbes Magazine)
Xiaojun Liu (Berkeley)
Per Peterson (Berkeley)
Shankar Sastry (Berkeley)
Claire Thomlin (Stanford)
Don Winter (Boeing)

NSF / OSTP Workshop on Information Technology Research for Critical Infrastructure Protection

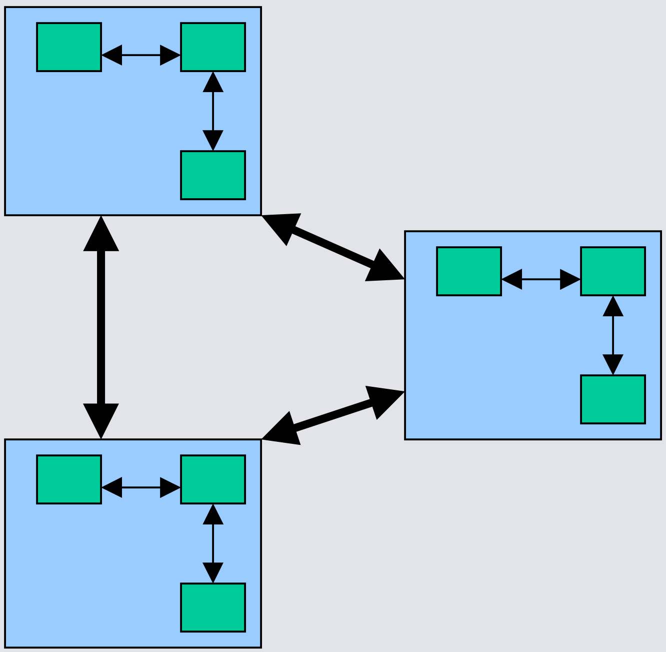
Sept. 19-20, 2002

The General Principle

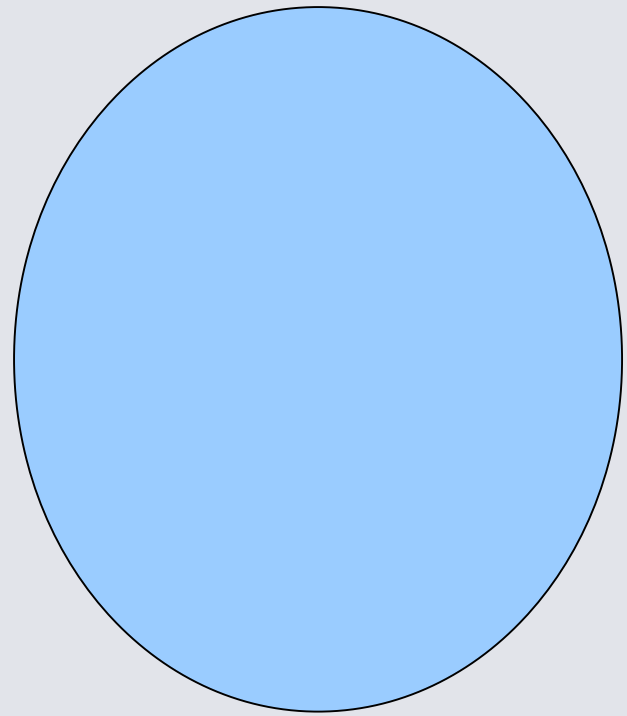
- Networked systems can impose safety envelopes
  - This is the intent of the air traffic control system
- Networks fail
  - E.g. Malicious pilots can ignore air traffic control directives
- Components can locally impose safety envelopes
  - Tighter envelopes may be required when networks fail
- Software-driven control systems enable imposition of safety envelopes at all levels of the network hierarchy
  - Air traffic control
  - Individual aircraft
  - Individual engine
  - Individual part

Principle:
Integrated Safety Envelopes

Flexible Networked Systems with Rich Functionality



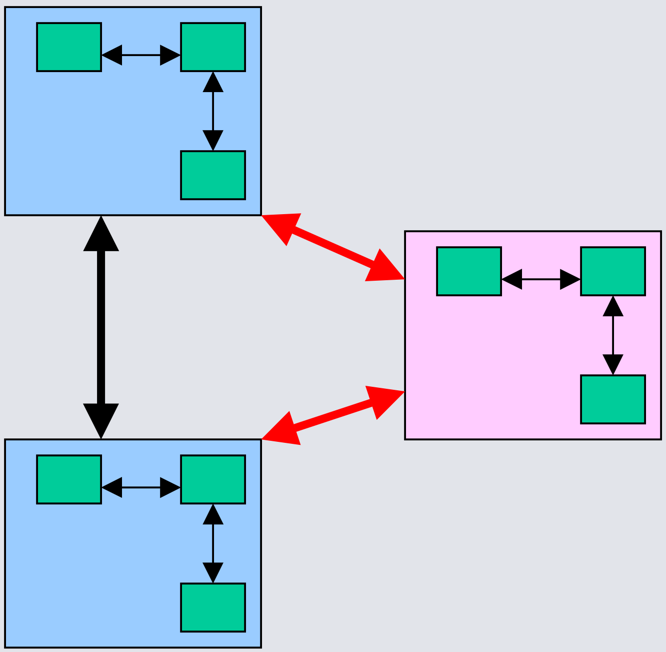
Networked embedded system…



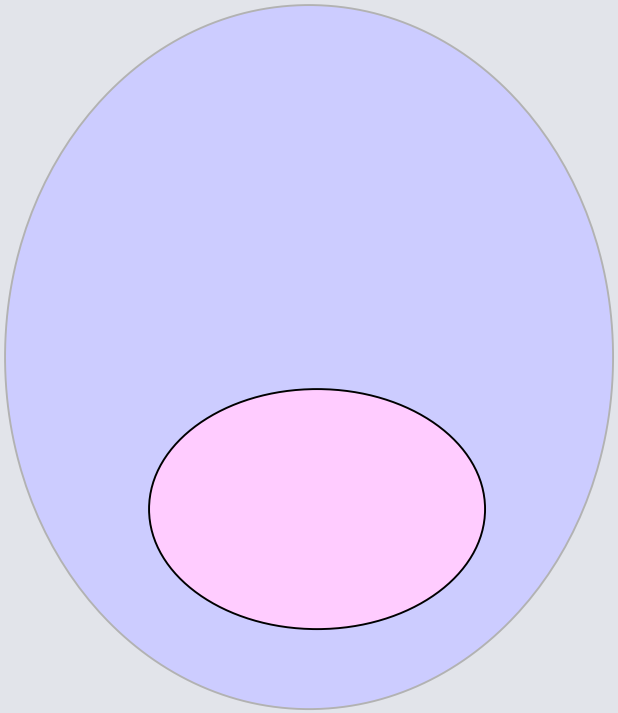
with a rich set of safe behaviors

Principle:
Integrated Safety Envelopes

Compromised Networked Systems Falls back to Less Functionality



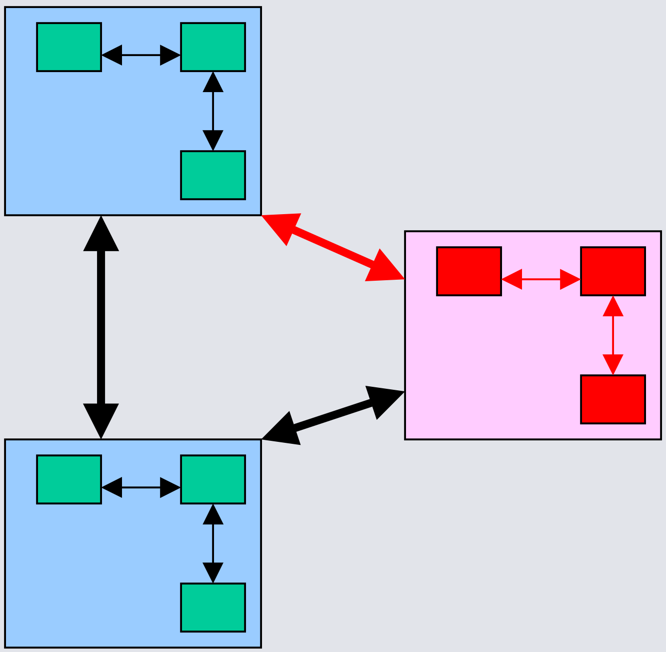
Compromised system…



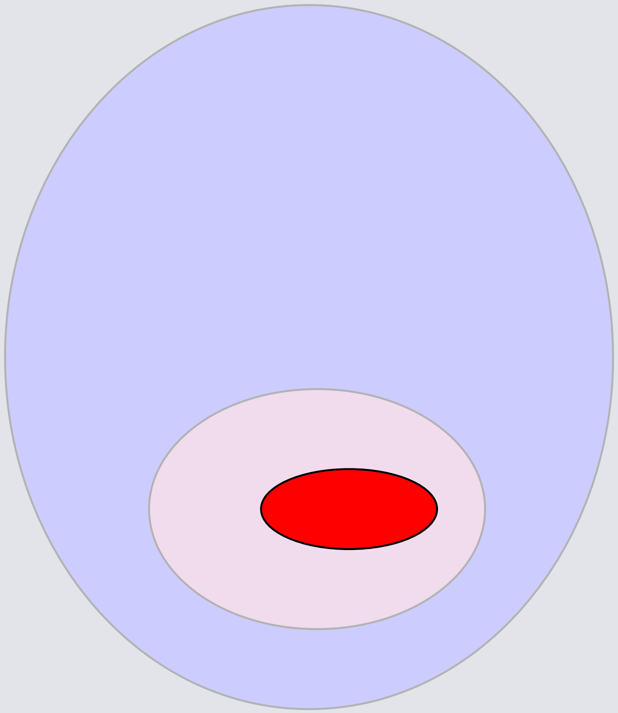
has fewer safe behaviors

Principle:
Integrated Safety Envelopes

Hierarchical Networked Systems With Locally Defined Safety Envelopes



Compromised subsystem…



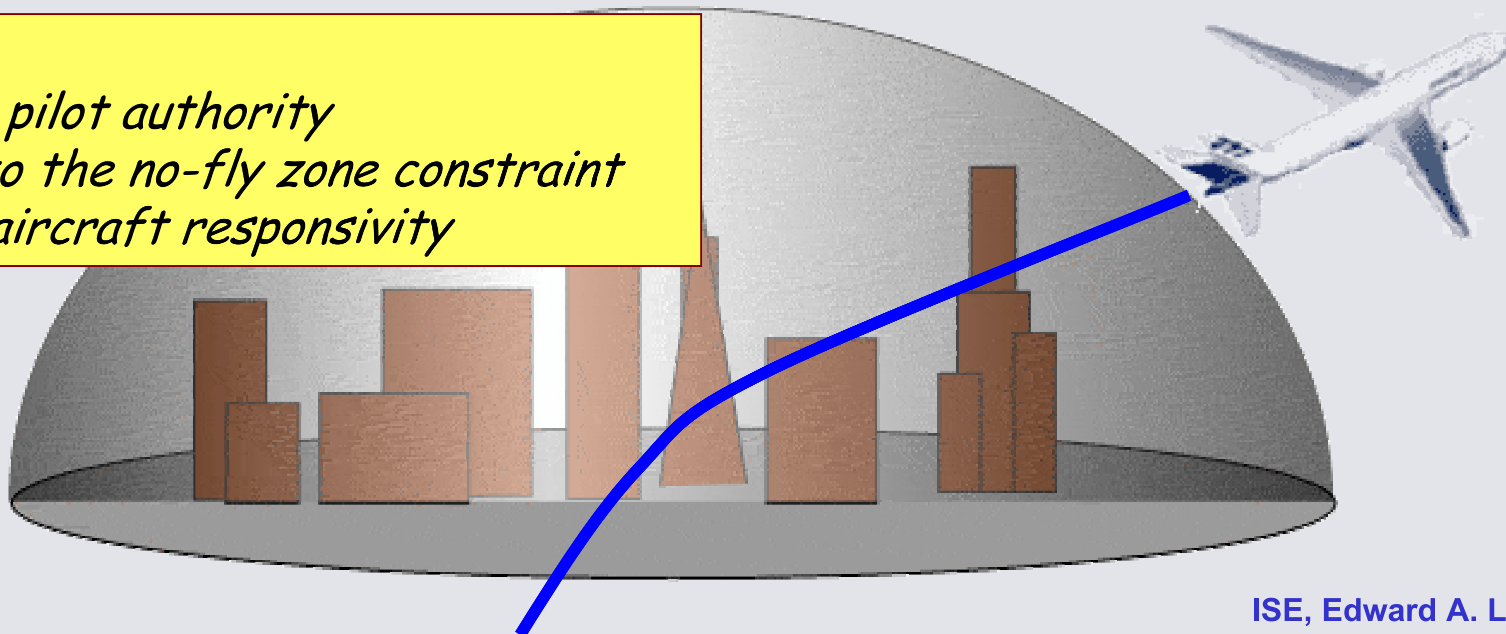
behavior within locally defined safety envelopes

Principle:
Integrated Safety Envelopes

Illustration of the Principle: Softwalls

- Enforce no-fly zones in the on-board avionics.
- Carry on-board a 3-D database with "no-fly-zones".
- Localization technology identifies aircraft position.
  - GPS + inertial navigation system
- System is not networked and not hackable.
- Improves aircraft safety
  - prevents controlled flight into terrain.

Principle:
- *Maximize pilot authority*
- *Subject to the no-fly zone constraint*
- *Maintain aircraft responsivity*



No-Fly Zone with Harsher Enforcement

There are already regions of space into which aircraft can't fly. The idea is to make some of these virtual.

Trajectory with Maximally Uncooperative Pilot

Assumptions:

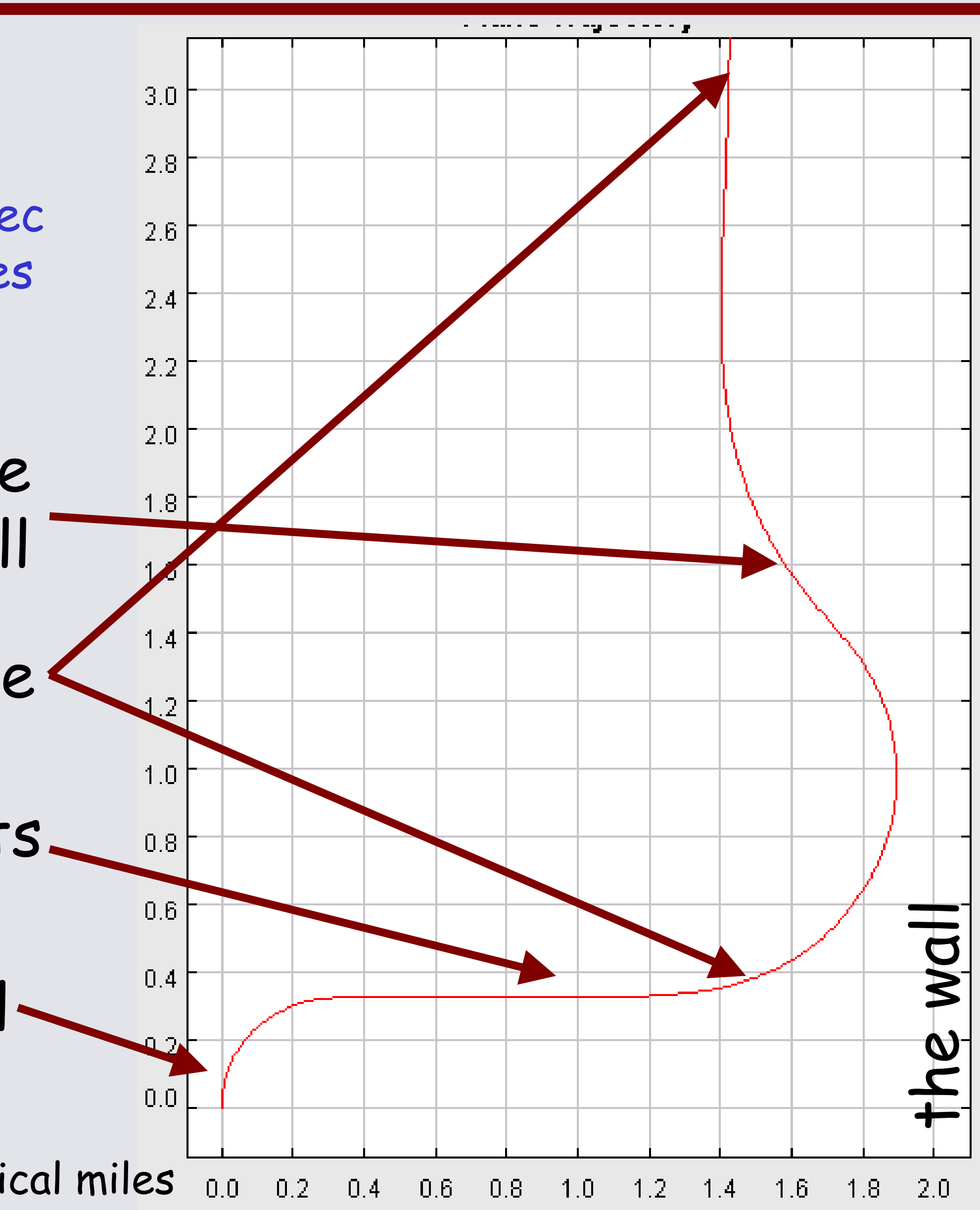
- speed: 0.1 miles/sec = 360 miles/hour
- Max rate of turn: M = $2\pi/20$ radians/sec
- min turning radius: speed/M = 0.32 miles

pilot regains steerage towards wall

pilot controls saturate

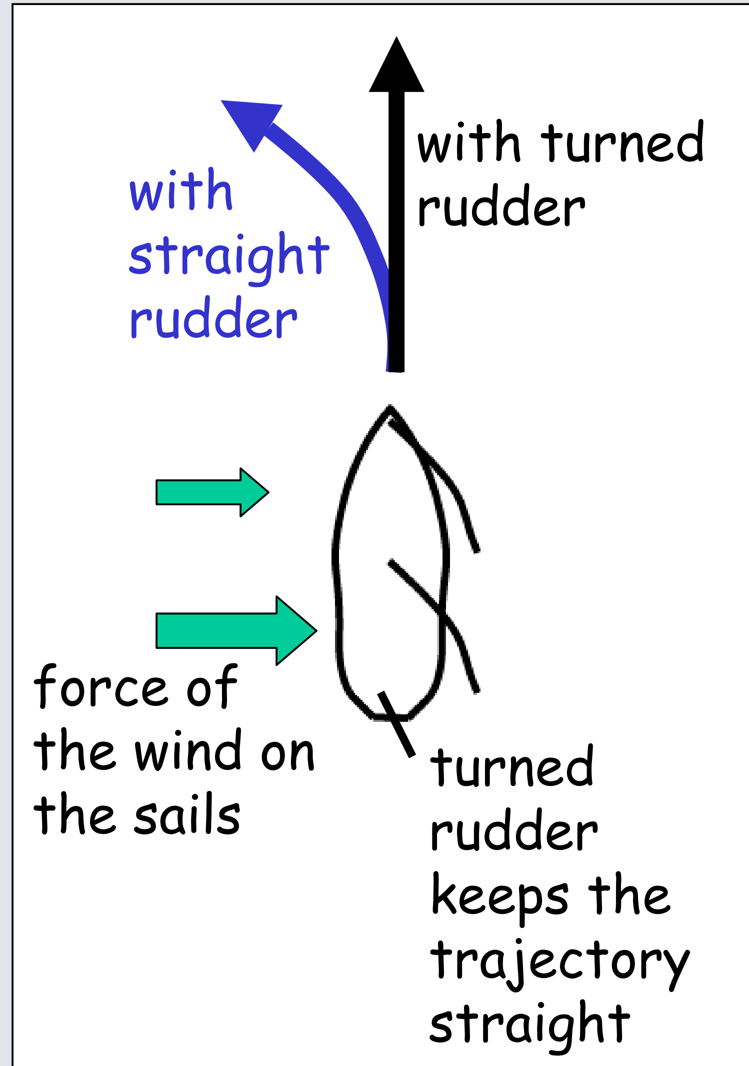
bias starts, pilot counteracts

pilot turns towards the wall



Aircraft is Diverted by a Blending Controller, which Combines a Bias with Pilot Directives

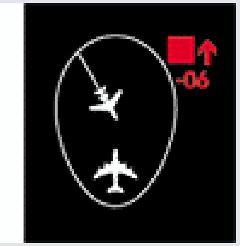
Sailing analogy: weather helm



Even with weather helm, the craft responds to fine-grain control as expected.

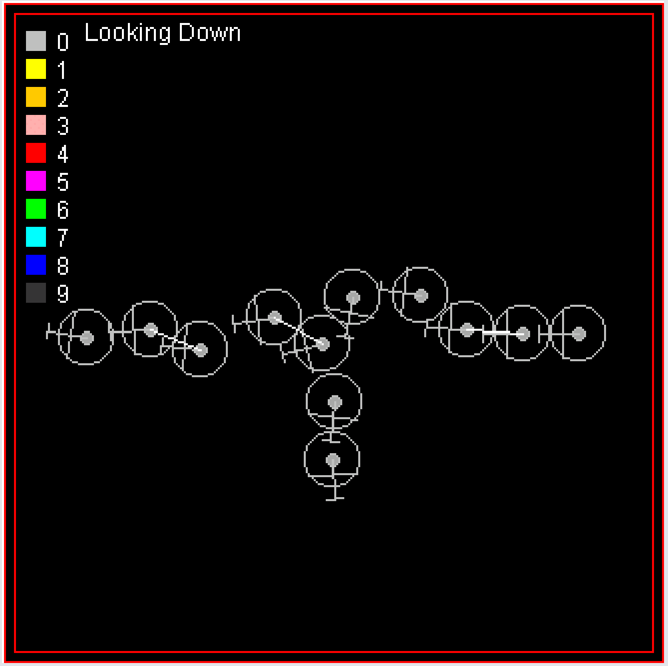
Related Methods

- Ground proximity warning systems
- Automatic ground avoidance systems
- TCAS & ACAS – collision avoidance
- Potential field methods for air-traffic control



Honeywell TCAS

These all share one feature: localization of safety envelopes.



Rockwell conflict resolution

Issues

- Reducing pilot authority is dangerous
  - reduces ability to respond to emergencies

Is There Any Aircraft Emergency Severe Enough to Justify Trying to Land on Fifth Ave?

Issues

- Reducing pilot authority is dangerous
  - reduces ability to respond to emergencies
- There is no override
  - switch in the cockpit

No-Fly Zone with Harsher Enforcement

There is no override in the cockpit that allows pilots to fly through this.

Issues

- Reducing pilot authority is dangerous
  - reduces ability to respond to emergencies
- There is no override
  - switch in the cockpit
- Localization technology could fail
  - GPS can be jammed

Localization Issues

GPS falls back to Inertial navigation

Accurate, robust localization technology is an essential technology.

"Localization" is the technology for reliably and accurately knowing the location of an object.

Issues

- Reducing pilot authority is dangerous
  - reduces ability to respond to emergencies
- There is no override
  - switch in the cockpit
- Localization technology could fail
  - GPS can be jammed
- Deployment could be costly
  - how to retrofit older aircraft?

Deployment

- Fly-by-wire aircraft
  - a software change
- Older aircraft
  - autopilot level?
- Phase in
  - prioritize airports

Issues

- Reducing pilot authority is dangerous
  - reduces ability to respond to emergencies
- There is no override
  - switch in the cockpit
- Localization technology could fail
  - GPS can be jammed
- Deployment could be costly
  - how to retrofit older aircraft?
- Deployment could take too long
  - software certification

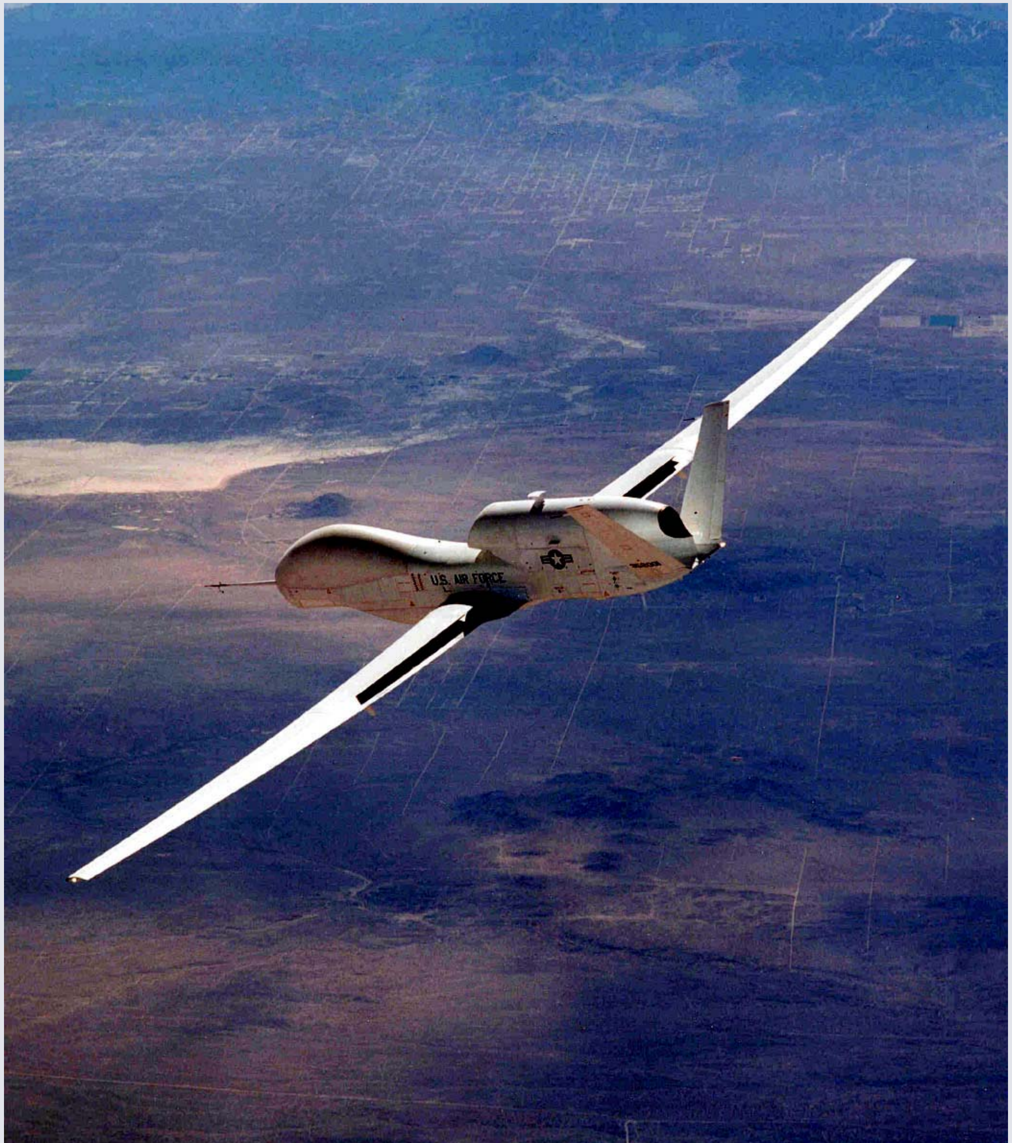
Softwalls Works When Air Traffic Control Fails

This seems largely orthogonal of air traffic control, and could complement safety methods deployed there. It is self-contained on a single aircraft. Improves robustness of any air traffic control system.

Issues

- Reducing pilot authority is dangerous
  - reduces ability to respond to emergencies
- There is no override
  - switch in the cockpit
- Localization technology could fail
  - GPS can be jammed
- Deployment could be costly
  - how to retrofit older aircraft?
- Deployment could take too long
  - software certification
- Fully automatic flight control is possible
  - throw a switch on the ground, take over plane

UAV Technology
(Unoccupied Air Vehicle)



e.g. Global Hawk
(Northrop Grumman)

Technology Support Working Group (TSWG), office of the Secretary of Defense, recommends against any partial control approach. Their feeling is that there is only one feasible strategy: a single trigger, either on-board or remote control, that would assume complete control and take the plane to a safe base.

Northrop Grumman has such a system in the Global Hawk UAV that some believe can be dropped-in to passenger airliners.

Potential Problems with Switching to Ground Control When Threat is Detected

- Human-in-the-loop delay on the ground
  - authorization for takeover
  - delay recognizing the threat
- Security problem on the ground
  - hijacking from the ground?
  - takeover of entire fleet at once?
- Requires radio communication
  - hackable
  - jammable

This does not follow the principle of *Integrated Safety Envelopes*

Integrated Safety Envelopes Research Agenda

- Defining hierarchical safety envelopes
  - Model-based design
- Fault and threat detection
  - On-line models
- Fault and threat isolation
  - Mode changes to impose safety envelopes
- Predictable mode transitions
  - Avoid emergent behavior, propagating effects
- Adapting existing systems
  - Models must include the phase-in transition
- Policy issues
  - Limiting authority

Conclusions

- Don't have to choose between large, centralized control, and decentralized, semi-autonomous actors.
  - Use both
  - Failures or threats $\Rightarrow$ tighter safety envelopes

- Need control algorithms that maintain safe operating parameters and maximize local authority subject to the safety constraints.