Cooperative and Fractional Redundancy for Cost-Effective Mixed-Critical Flight Control Systems

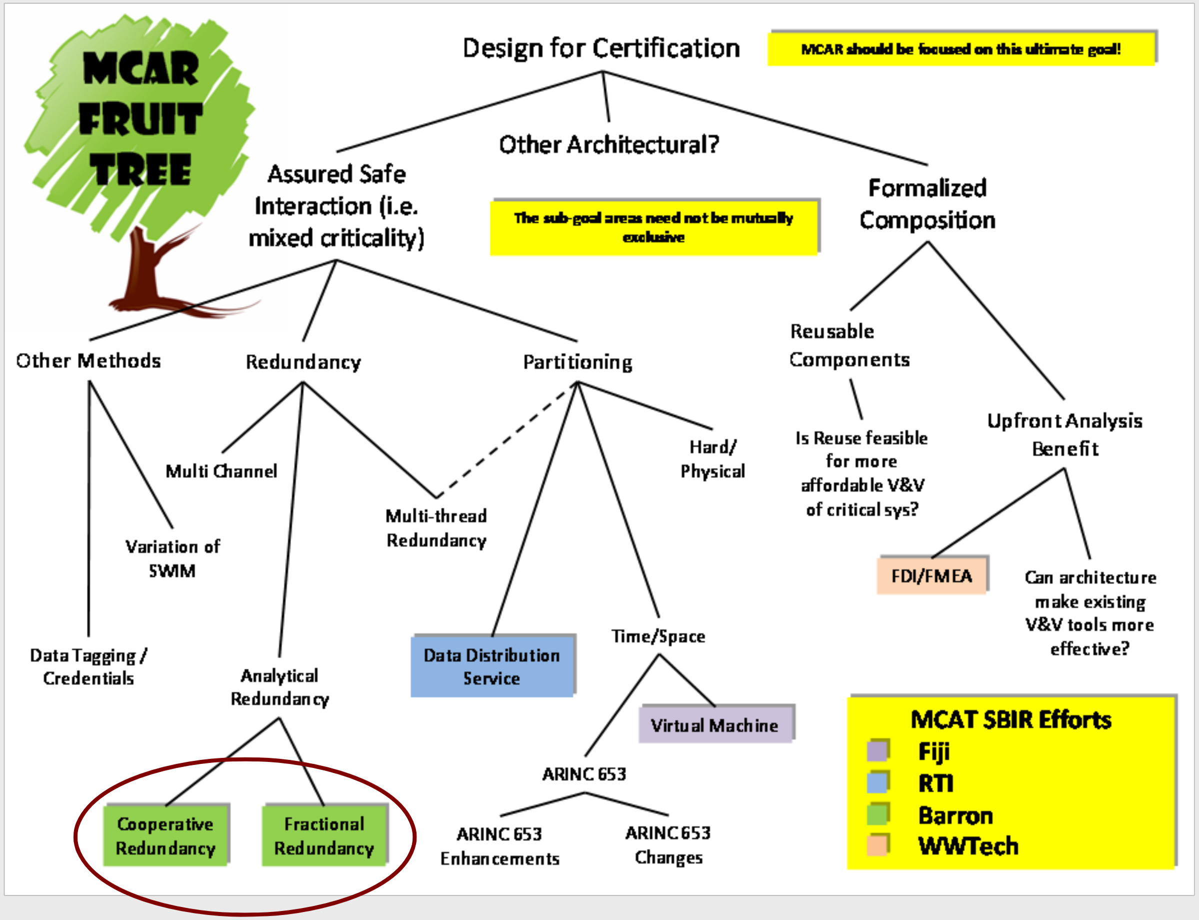
Air Force Contract No. FA8650-10-M-3027, SBIR Phase I

M. Anthony Aiello, John Schierman, Brian Dutoi, J.r Grohs, Michael DeVore
Barron Associates, Inc., Charlottesville, Virginia

Safe & Secure Software Systems Symposium (S5)
Dayton, Ohio
15-17 June, 2010

MCAT Program Background

- Mixed-Critical Architecture Technologies
  - Outgrowth of Mixed-Critical Architecture Requirements
  - Air Force Small-Business Innovative Research Project
  - Currently in Phase I
- Barron Associates a participant in MCAR
  - Part of the Lockheed Martin team
  - Helped define fault-tolerance-related future directions in response to the MCAR Fruit Tree

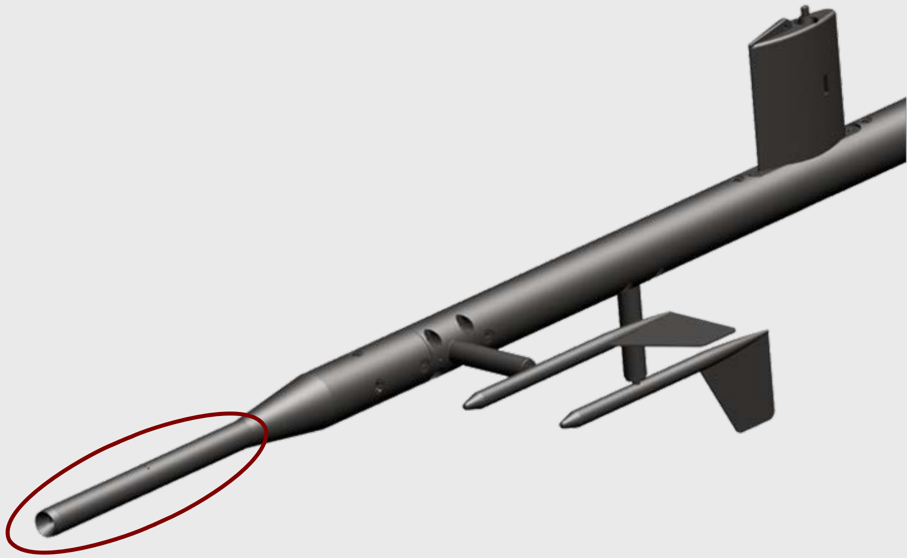


Barron Associates' Technologies

- Selected Technologies
  - Fractional Redundancy
  - Cooperative Redundancy
- Motivation
  - Reduce space, weight, and power by removing hardware replication
  - Maintain similar levels of reliability
- Approach
  - Fractional: leverage analytical redundancy
  - Cooperative: leverage data from an off-board source
    - Airfield
    - Wingman

Fractional Redundancy Example

- Consider the air data package
  - P_s: static pressure
  - P_t: total pressure
  - Alpha: angle of attack
  - Beta: sideslip angle
    - Depends on the package



- Assume a failure of P_s & P_t
  - Can no longer directly compute:
    - Airspeed
    - Mach number
    - Dynamic pressure
  - Has implications, e.g., for controller gain scheduling

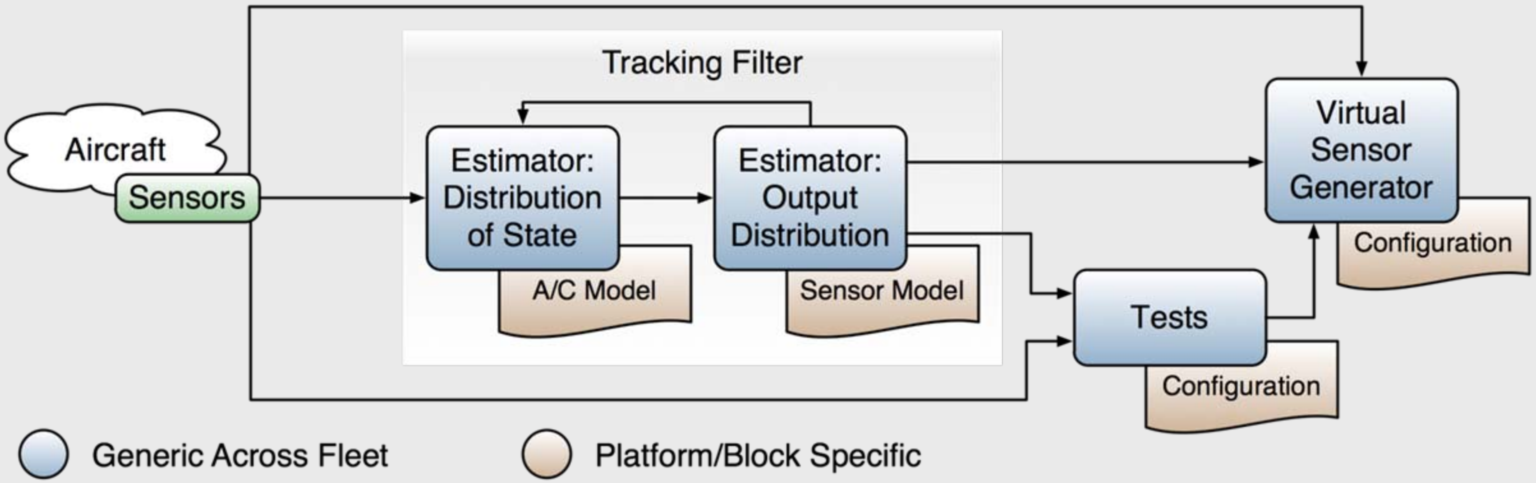
Image source: http://www.prweb.com/prfiles/2009/08/30/30740/4512.jpg

Fractional Redundancy: Example

- Still have some air data
  - Alpha
  - Beta
- Still have INS/GPS
  - Body angles
    - Pitch
    - Roll
    - Yaw
  - Inertial velocities
  - Altitude
- Still know effector positions

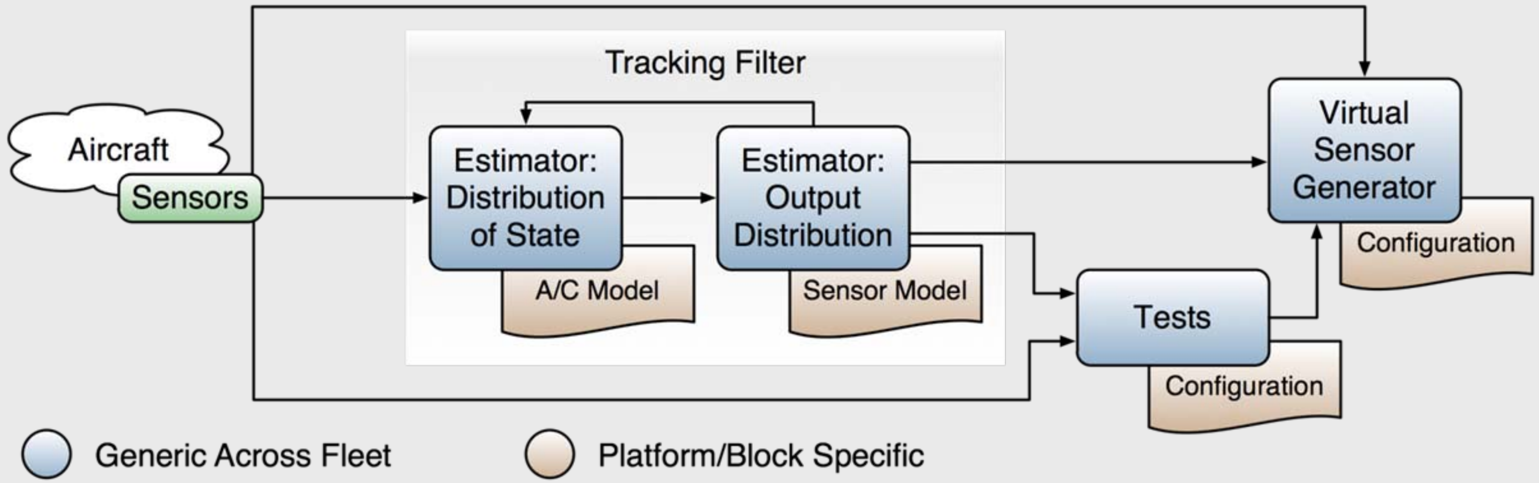
Fractional Redundancy: Approach

- Fuse available information to reconstruct missing air data
  - Based on a model that relates
    - Effector positions
    - Current state estimates
    - Healthy sensor inputs
  - Build virtual sensors for lost air data
- Caveats
  - Requires a high fidelity model
  - Yields low-frequency estimates only
- Model quality/completeness drives:
  - Fault detection and isolation capability
  - Virtual sensor quality



Fractional Redundancy: Approach

- Model-based analytical redundancy
  - Reduce total sensors
  - Provide similar levels of reliability
- Systematic vs. Ad-hoc design
  - Current approaches to analytical redundancy are ad hoc
    - Must be reexamined/rebuilt for each system
  - The computational components are reusable
  - The system model serves as configuration data
- An accurate, complete model will catch unknown-unknowns.



Fractional Redundancy: Dial-a-Redundancy

- Scales from simple to very complex

- Simple Example
  - Add a 4th axis to an INS
  - Cover a failure in any of the three, orthogonal axes

- Complex Example
  - Leverage end-game goal of IVHM
    - Sensors at many locations throughout the aircraft
    - Stress monitoring of surfaces and airframe
  - A model, e.g.,
    - Relating all of the sensors
    - Covering aeroelasticity
  - Detect and recover the failure of any or multiple sensors

Cooperative Redundancy: Example

- Some sensors poor choices for Fractional Redundancy

- Consider a failure of angle of attack
  - No longer directly observe wind direction
  - Observing wind magnitude more difficult
- Fractional Redundancy could reconstruct aero alpha
  - From INS data
  - Latch last known wind direction and magnitude
  - Changes in pitch are correlated to changes in alpha for constant wind

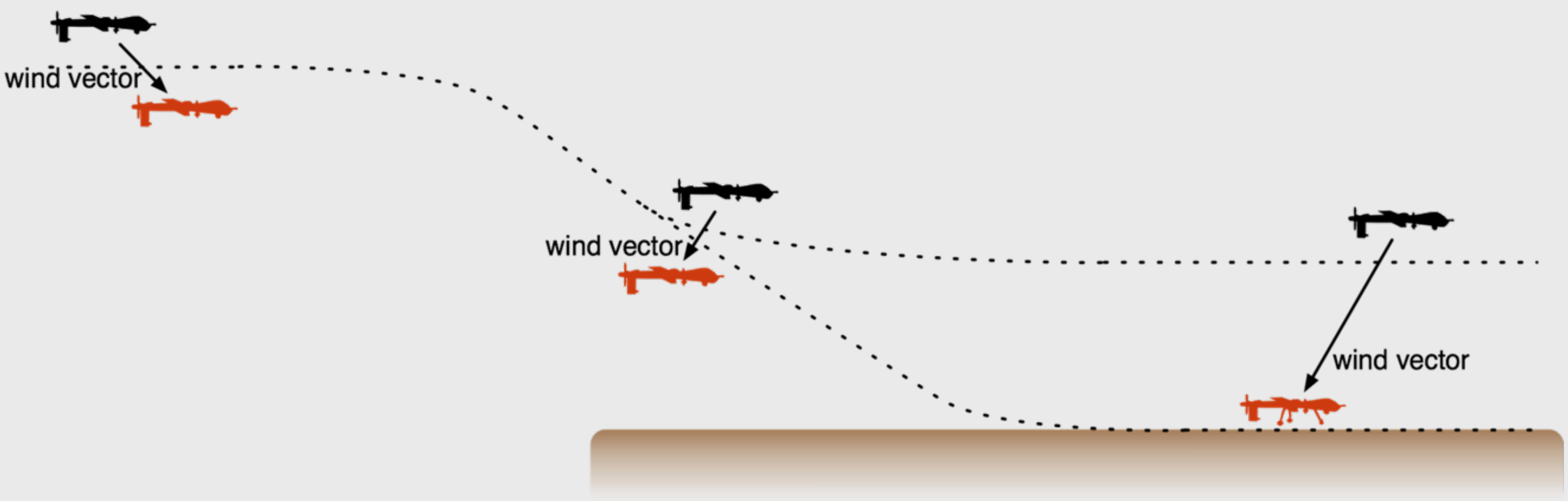
Image source: http://www.prweb.com/prfiles/2009/08/30/30740/4512.jpg

Cooperative Redundancy: Example

- Reconstructed aero alpha valid only while wind constant
  - Low-frequency approximation
- Winds are variable
  - Overall the estimate will be poor
  - Over time, it will grow worse
- Need to know how the airmass is moving
  - Get an estimate of wind from off board
  - E.g. a wingman

Cooperative Redundancy: Example

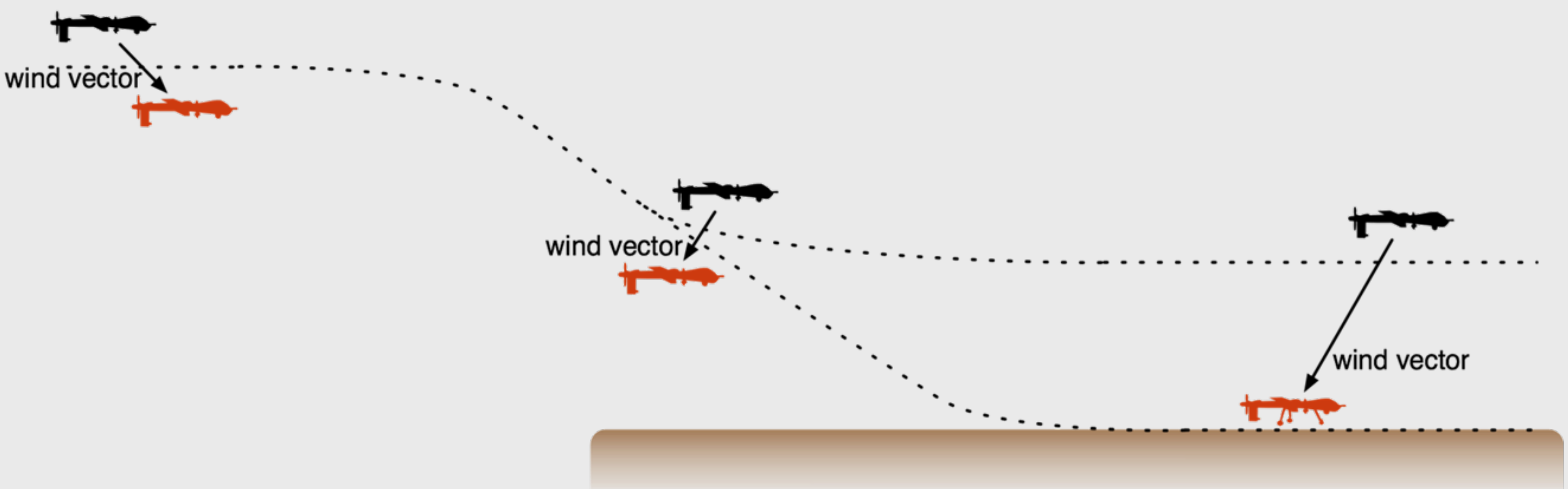
- Wingman sends
  - Difference between airspeed vector and inertial velocity vector
    - The estimated wind magnitude and direction
- Receiver reconstructs aero alpha
  - Biases inertial velocity vector with received wind direction and magnitude
    - Yields airspeed vector



Cooperative Redundancy: Key Features

- Supplement on-board data with off-board data
  - Reduce total sensors
  - Provide similar levels of reliability

- Effects not observable through analytical redundancy can be captured



Cooperative Redundancy: Mission Implications

- Multiple aircraft required for up-and-away flight
  - A ground station can provide off-board data for landing
  - A wingman required for other flight phases
- Impacts to multi-vehicle assignments
  - Each aircraft may be tasked with separate missions
  - One failure could tie up both aircraft
    - Healthy aircraft must stay near aircraft with failure
  - One failure scuttles two (or more) missions
- Offers potentially greater flexibility for mission planners
- Mission analysis required
  - Types of missions and roles part of design process
  - Ensure cooperative redundancy does not over-constrain roles

Summary

- Two novel approaches to fault tolerance
  - Fractional Redundancy
  - Cooperative Redundancy
- Fractional Redundancy
  - Leverages analytical redundancy
  - Model-based
- Cooperative Redundancy
  - Leverages off-board data
- Approaches are
  - Complementary
  - Synergistic

Questions

- BACKUPS

Cooperative Redundancy: Example

- Wingman sends
  - Difference between airspeed vector and inertial velocity vector
    - The estimated wind magnitude and direction
- Receiver reconstructs aero alpha
  - Biases inertial velocity vector with received wind direction and magnitude
    - Yields airspeed vector