Robustness Analysis of Safety-Critical Systems

Gary Balas[1], Peter Seiler[1], and Andrew Packard[2]

[1]University of Minnesota

[2]University of California, Berkeley

National Workshop on Transportation CPS

Session IV: Model-Based Design, Validation, and Verification

January 24, 2014

Themes: Model Based Design, V&V

performance
computing
Engineering
attacks
vehicle
VALIDATION
CONTROL
requirements
research
FORMAL
DYNAMICS
problem
model
PROVIDE
SOFTWARE
challenges
analysis
assurance
behavior
information
NEED
FEATURES
DESIGN
approach
DEVELOPMENT
UNCERTAINTY
safety
INTEGRITY
methods
VERIFICATION
tools
new
components
time
generation
abstraction
functions
critical
NETWORK
properties
LEVEL
example
COMPLEX
interactions
operation
DATA
BASED
order

(Word cloud made from Session IV position papers with tagxedo.com)

Boeing 787 Dreamliner

(Image Copyright: H. Michael Miley)

Observations:

- Extreme reliability
- Model-based Design
- Requirements development
- Distributed manufacturers
- Multi-rate system

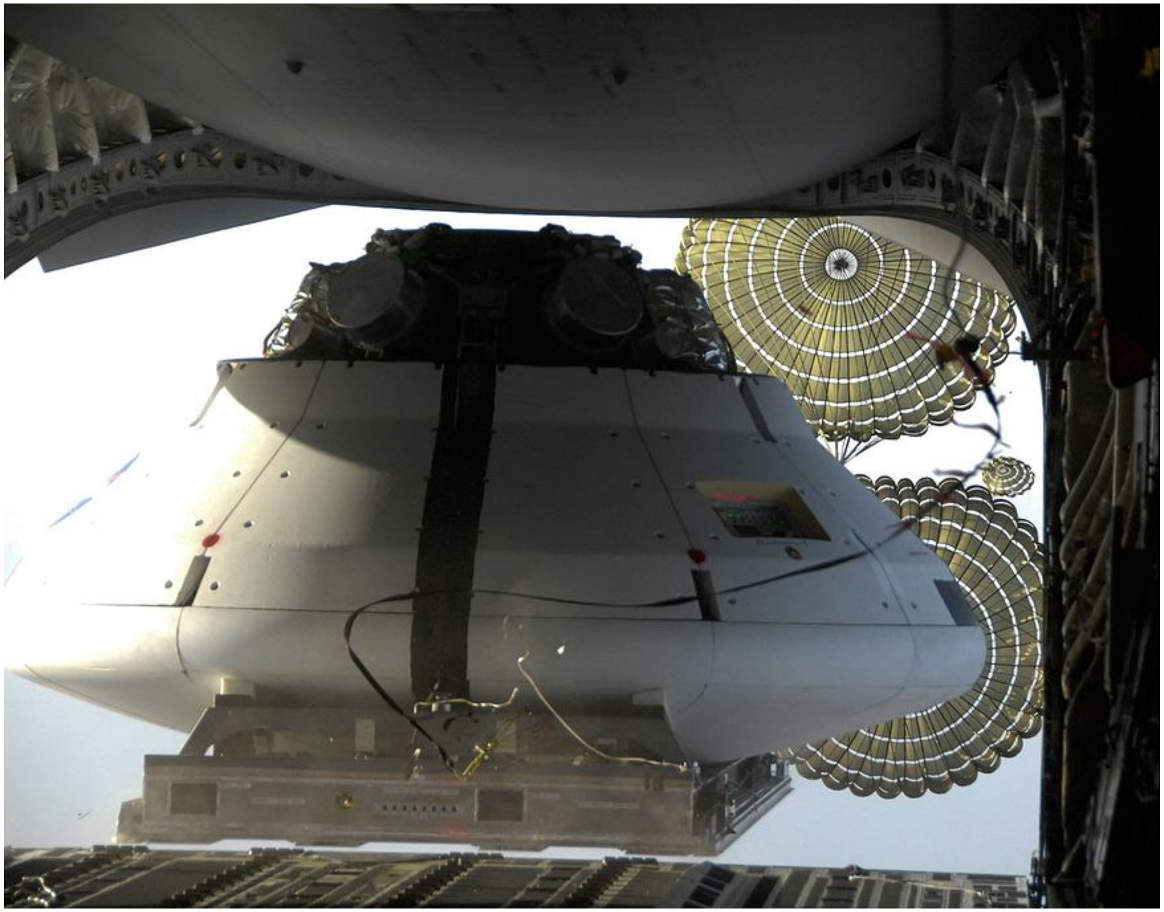
Automotive Active Safety

(Image Copyright: T. Wang)

Observations:

- Model-based Design
- Environmental uncertainty
- Human-machine interface
- Probabilistic errors in sensor fusion

NASA Orion Crew Exploration Vehicle



(Image Copyright: NASA)

Observations:

- Nonlinear effects
- Dynamic uncertainty
- Use of describing functions and Monte Carlo Sims

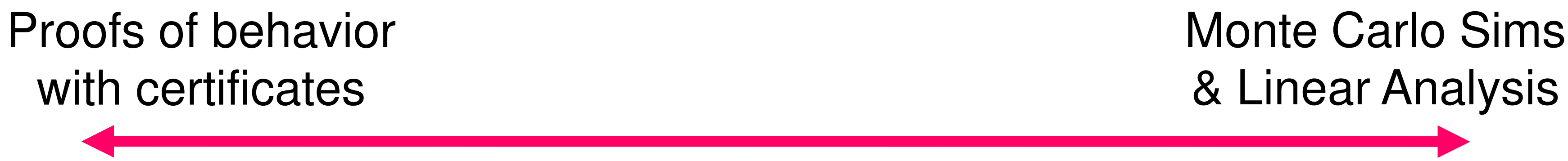
What We Do Well: Linear Analysis

- **Nominal:** Linear systems described by ordinary differential equations (ODEs) or difference eqns (DEs)
  - Metrics: Freq. & time responses, classical stability margins, variance due to stochastic inputs
  - 1000 states, 100's of inputs
- **Uncertainty:** Linear ODEs with rational dependence on parametric and/or dynamic uncertainty
  - "Known" unknowns
  - Metrics: Induced gains, generalized stability margins
  - 100's of states, 10's of inputs, 10's of uncertainties
  - Computational complexity issues
- **High quality software exists for these problems.**

Validation with Linear Analysis

- Ex: Gain-scheduled flight controls
  - Q: How much time delay can be tolerated?
  - A: (answers a different question) Here’s a scatter plot of delay margins at 1000 trim conditions throughout envelope

- Why was linear analysis so useful in the past?
  - Domain-specific expertise exists to interpret linear analysis and assess relevance
  - Fast, defensible answers on high-dimensional systems



Proofs of behavior with certificates

Monte Carlo Sims & Linear Analysis

What could we do well?

- Systems that are gain-scheduled (time-varying) and/or depend on a few nonlinear elements (e.g. saturation)
  - Systems with and without uncertainty
  - Metrics: Induced gains, generalized stability margins
  - 10’s of states, 10’s of inputs, 2-3 uncertainties, 2-3 parameters
- Well-developed theory and “beta” code for both classes

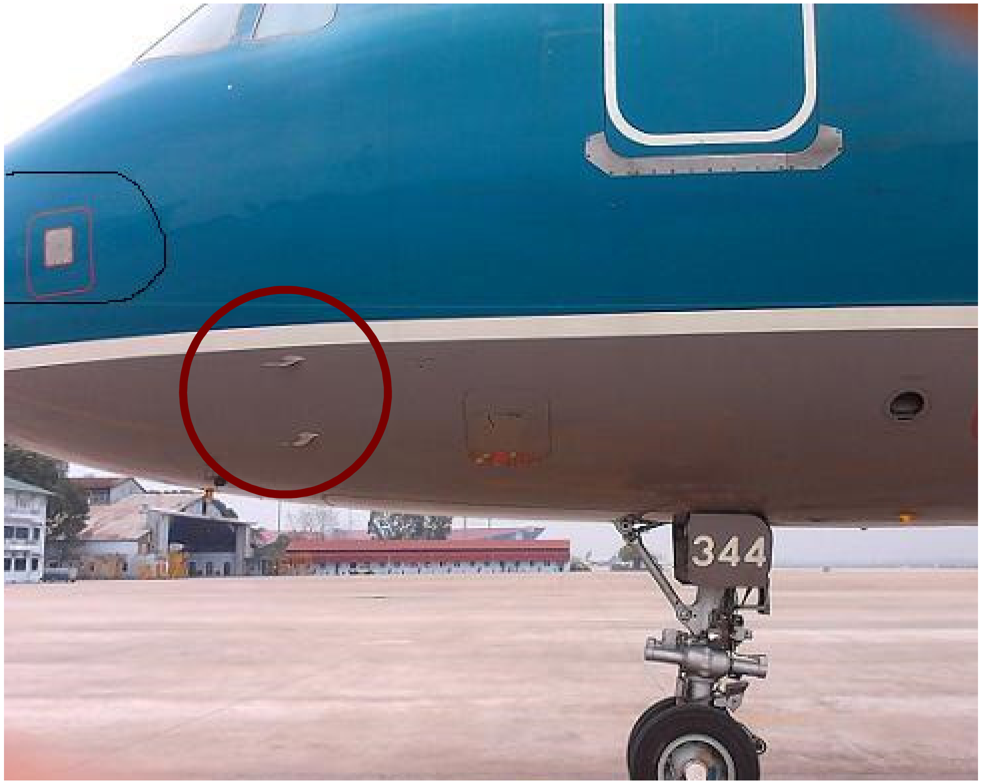
- Questions:
  - Are numerical methods valued?
  - What is the path to commercialization path from theory to SW useful for the practicing engineer?

Some issues for current/future CPS

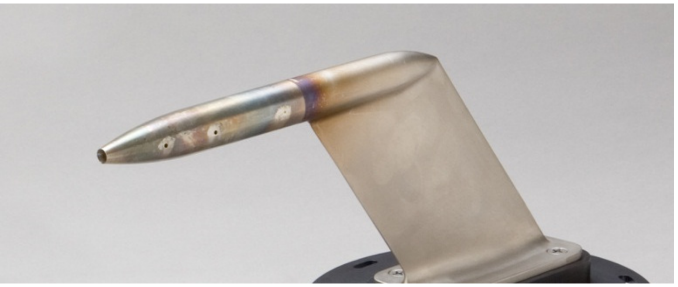
- Strongly nonlinear dynamics
- Hybrid systems
- Large-scale systems (Except linear systems)
- Uncertainty: Unknown unknowns
- Need for tools that cut-across domains (SW/HW)
- Specific time domain performance criteria

These issues limit our ability to certify the performance of novel algorithms for CPS

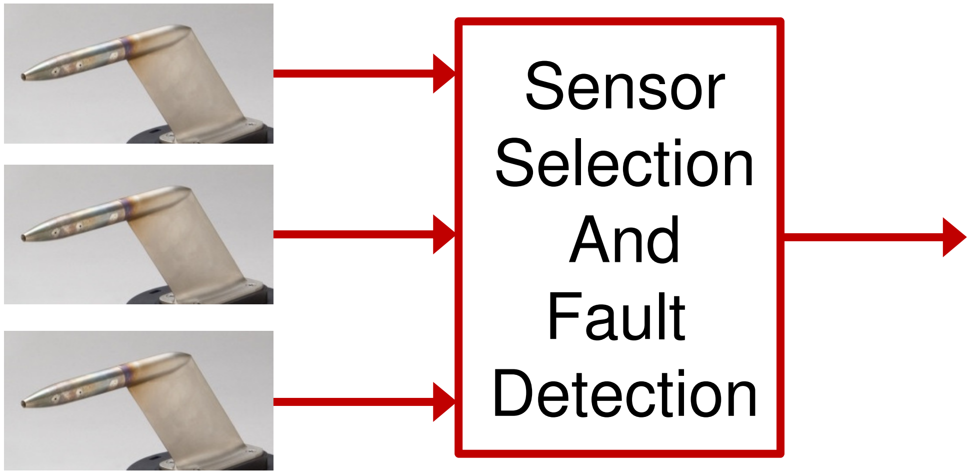
Example: Shift to Analytical Redundancy



Freeman, Seiler, Balas, “Air data system fault modeling and detection”, 2013



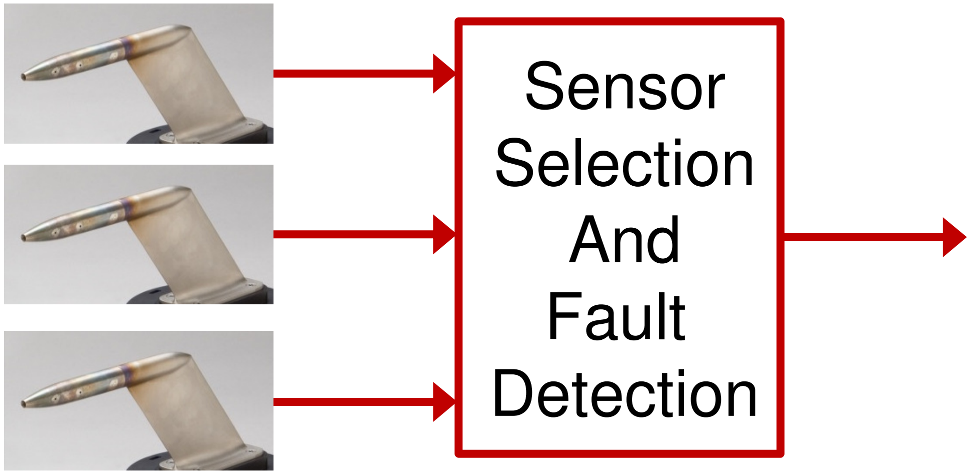
Example: Shift to Analytical Redundancy



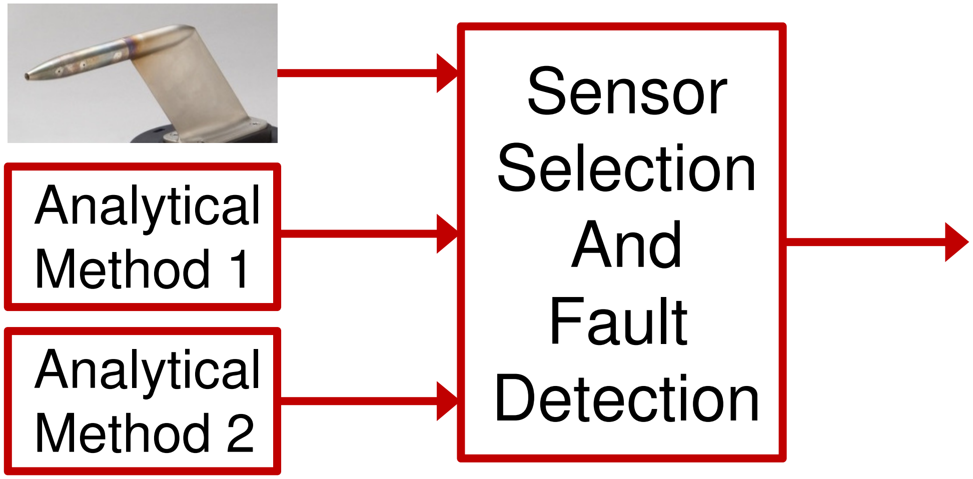
Sensor Selection And Fault Detection

Architecture reliability can be easily assessed from sensor failure rates

Example: Shift to Analytical Redundancy



Architecture reliability can be easily assessed from sensor failure rates



Comments:

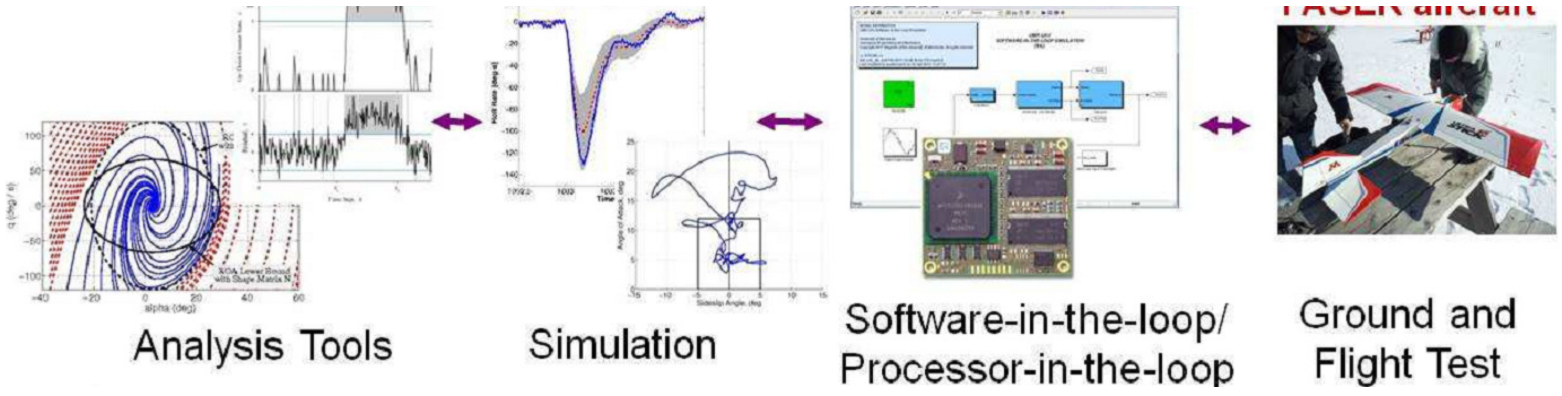
1. Analytical methods introduce new failure modes
2. Is there a benefit for algorithmic dissimilarity?

Certification of Novel Algorithms

- How do we certify algorithms that are nonlinear, stochastic, etc?
  - Probabilistic algorithm errors
    - [*Koopman,Wagner*], [*Heimdahl,Rayadurgam,Seiler,Balas*]
  - New performance metrics are likely required
    - [*Belcastro*]
  - Can we gain "trust" in the algorithm by fielding it with limited authority?
    - [*Seiler,Gebre-Egziabher,Rife,Guyer*]
    - Comment Yesterday: We don't V&V Pilots. We trust them based on training/experience.

Compositional Analysis

- Passivity/Lyapunov specifications on components
  - [*Antsaklis, Gupta, Wang*], [*Balas, Seiler, Packard*]
- Integration of simulations and more rigorous methods
  - [*Jin, Deshmukh, Kapinski, Ueda, Butts*]
- Correctness by design
  - *[Bhatt, Madl, Oglesby, Owre, Shankar, Tiwari], [Heimdahl, Rayadurgam, Seiler, Balas], [Kulkarni]*



Analysis Tools ↔ Simulation ↔ Software-in-the-loop/ Processor-in-the-loop ↔ Ground and Flight Test

Education in Model-Based Design

- Challenge: How do we train engineers in model-based design, validation and verification?
  - Are there specific education issues for transportation CPS?
- Key Issues: [Taken from *Pattipati, Pattipati, Ghimire*]
  - How to teach top-down thinking needed for a successful system design engineer using case/project-based learning?
  - Multi-domain Modeling
  - Formal Methods for Requirements, Verification & Validation
  - MBD-based Design Flows for Coordinated, Standardized and Measurable Design Process