Design for Autonomy: A New Paradigm in System Reliability, Availability and Maintainability

George J. Vachtsevanos

Professor Emeritus

Georgia Institute of Technology

and

Kimon P. Valavanis

John Evans Professor

University of Denver

Autonomy

A system is called “autonomous” if:

- It can monitor its own performance.
- It can detect, isolate and identify incipient failures of its critical components.
- It can predict the remaining useful life of failing components.
- It can take appropriate corrective action to safeguard its integrity for the duration of the emergency.

Basic Ingredients for "Design for Autonomy"

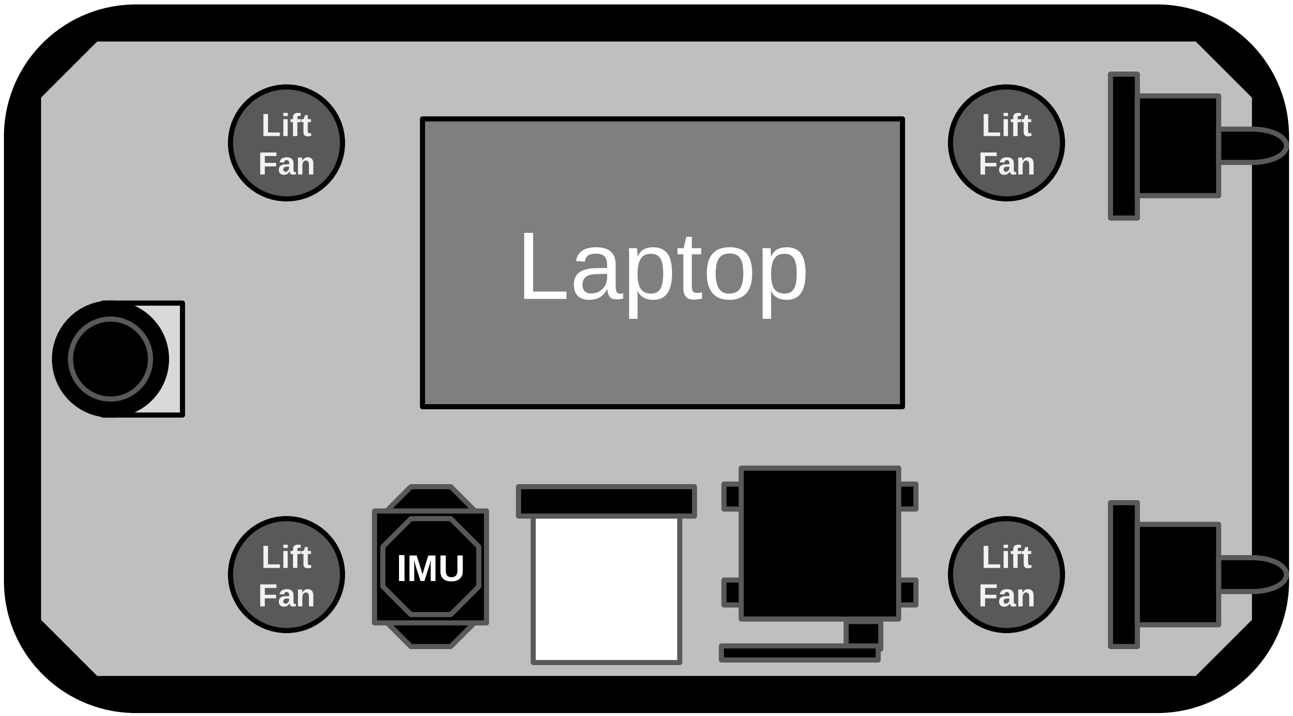
- Advanced System Design Concepts—Design for Fault Tolerance
- Sensing Strategies
- Modern Control Technologies
- Reasoning Strategies
- A Hybrid Hardware/Software Framework

Georgia Tech: The Past

Georgia Tech: New Autonomous Systems Developments

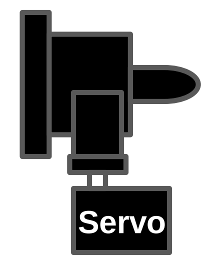
Hovercraft Layout

SICK LMS111 LIDAR



E-flite BL32 Brushless Motor

E-Flite Delta-V 15 Ducted Fan



Cooling Fan

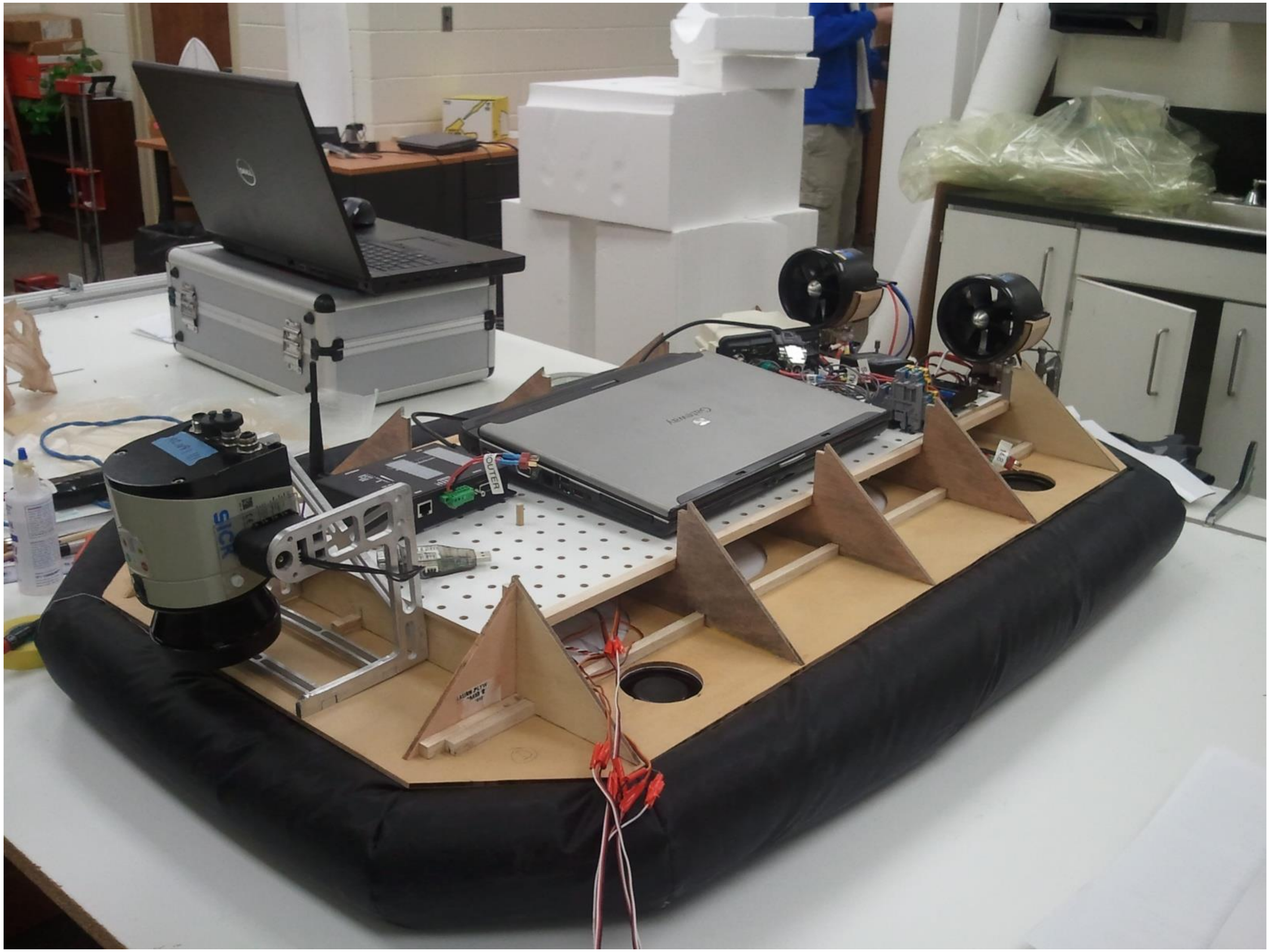
MicroStrain 3DM-GX1 IMU

Novatel OEMStar

MicroHard 2.4GHz Router

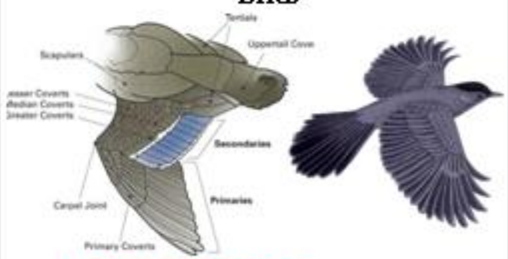
360° Servo

Hovercraft Layout – Front



Micro Air Vehicle Concept

BIRD



A. *Complex co-ordination*: Many muscles
B. *Larger wing-span* for long flight times
C. *Not recommended* for closed-quarter flight

HUMMINGBIRD

A. *Good Contender* for a design
B. *Not power efficient and short flight time*
C. *Complex Wing mechanisms* implementation

BUTTERFLY

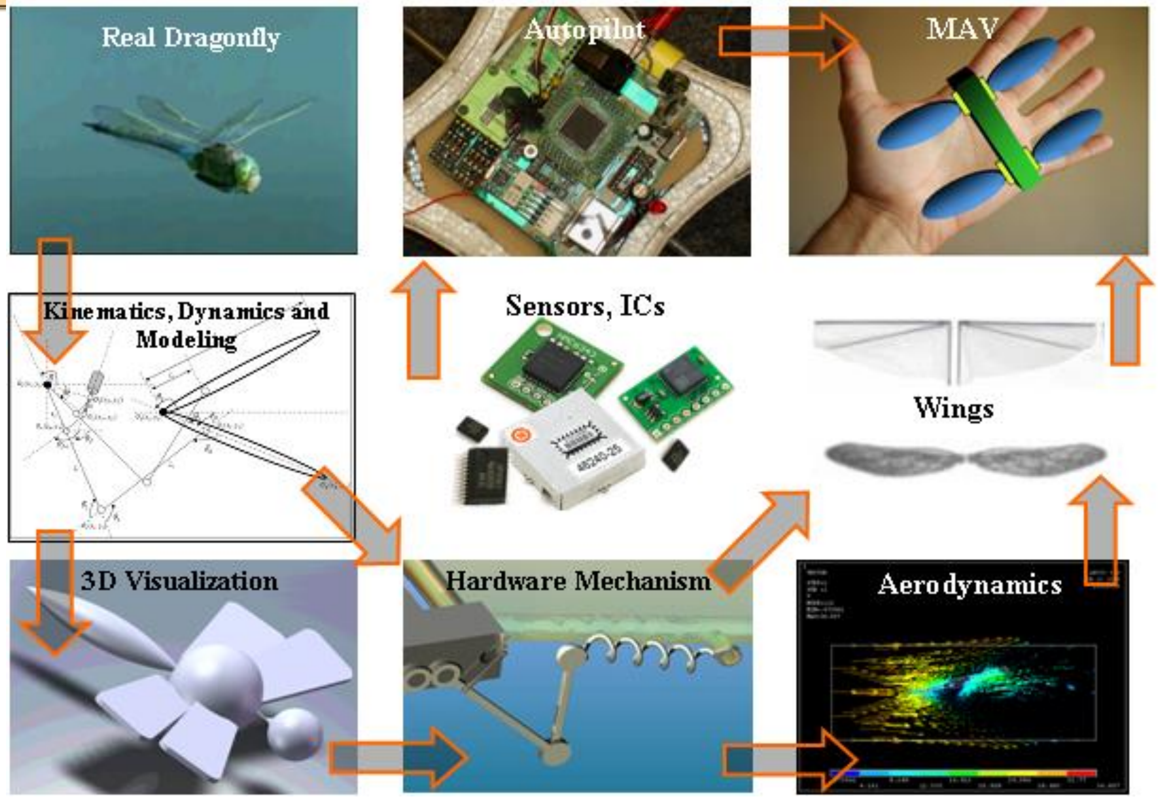
A. *Excellent contender* for a MAV
B. *Long flight times*
C. *Slow dynamics*, *low agility*
D. *Low controllability*

DRAGONFLY – THE DESIGN CHOICE

A. Four sets of wings provide *maximum Lifting power*
B. The Wings resonate synchronously, sustaining *super-long flight times*
C. Four wings give it unparalleled *agility and maneuverability*

D. Only *one actuator per wing*
E. *Simpler controls*
F. *Relatively less complex* parts - tolerance to damage

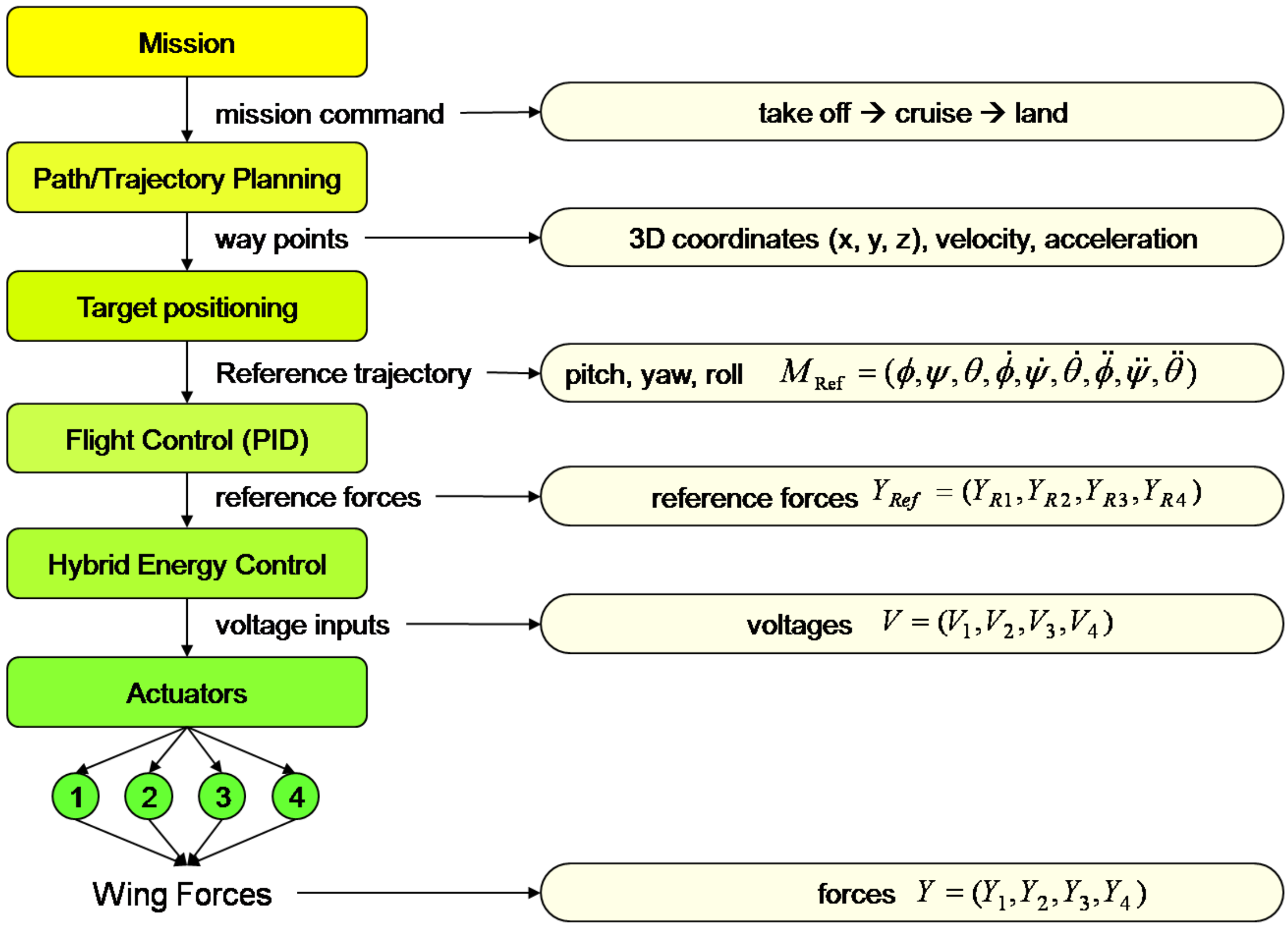
Program Objectives Dragonfly → MAV



- Actuation Mechanism
  - Re-Use of Elastic Energy
  - Simple, Robust Construction
- Control Design Methodology
  - Wing Control
  - MAV Attitude Control
  - Simpler Control Methodology
- Modeling and Simulations
- Prototype Construction
  - Sensors, CPU, Communication
  - Wing Design
  - Hardware – In – Loop Sim

Controls

Control Hierarchy



$$\text{Safety/Reliability} = \frac{1}{\textbf{Prob}(\text{failure})}$$

Design for Autonomy

Design for autonomy requires game changing technologies that synergistically contribute to an **integrated integrity management architecture** that may reduce significantly the operator engagement, while improving attributes of vehicle safety, durability and reliability.

Fundamental ingredients for autonomy

- Risk
- Confidence
- Uncertainty Management
- Fault-Tolerant Control

Risk and Confidence: Modeling Tools

- Risk Models
  - How do we model risk?
  - What does it mean to model risk?
  - Risk strategies/management

- Candidate Models
  - *Monte Carlo*
  - Dynamic Nonlinear/Stochastic
  - *Response Surface Models*
  - Fuzzy/Neuro-fuzzy, etc.
  - Empirical Models

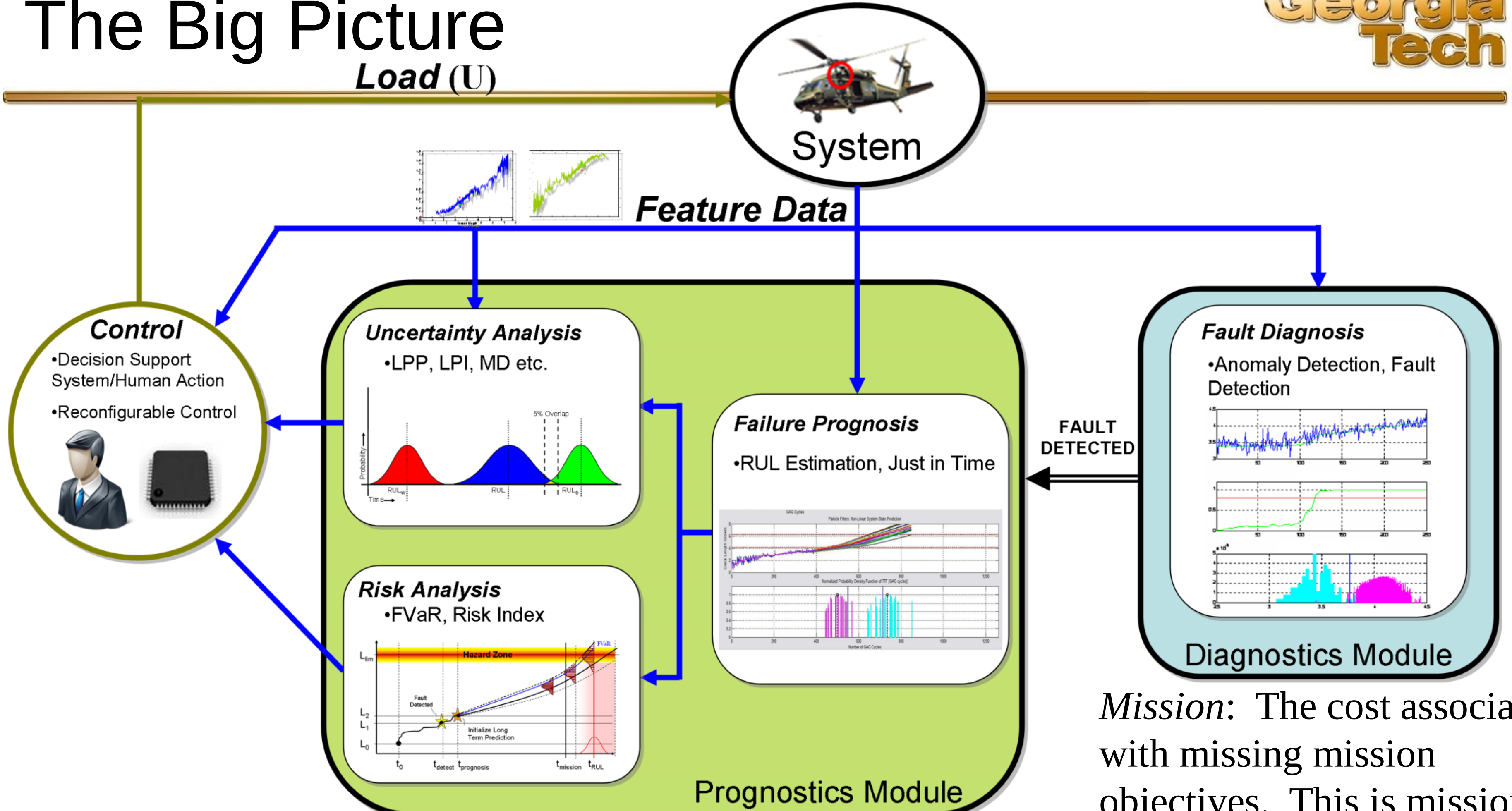
Data! Data! Data!

- Lack of “good” data
- Data quality
- Data processing/data mining strategies.
- Data availability

Integrity Management-The Enabling Technologies

- System Integrity Management is viewed as the maintenance of the operational response of high-valued assets in the presence of the adverse events.
- Design for autonomy, assuring that systems operate with high confidence.
- Emphasis on Prognostics and Health Management.

The Big Picture

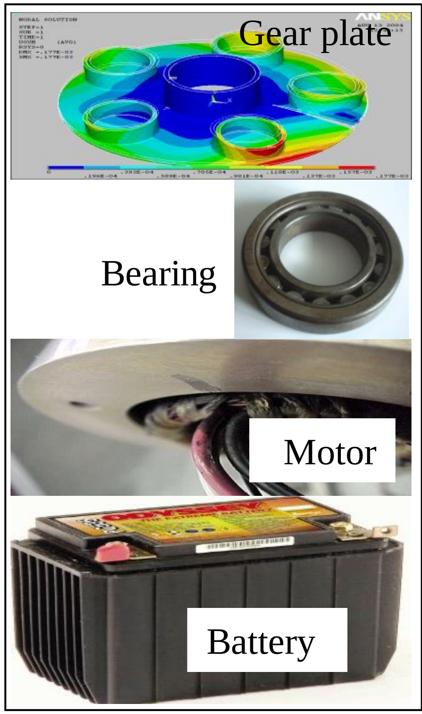


Mission: The cost associated with missing mission objectives. This is mission dependent and possibly subjective.

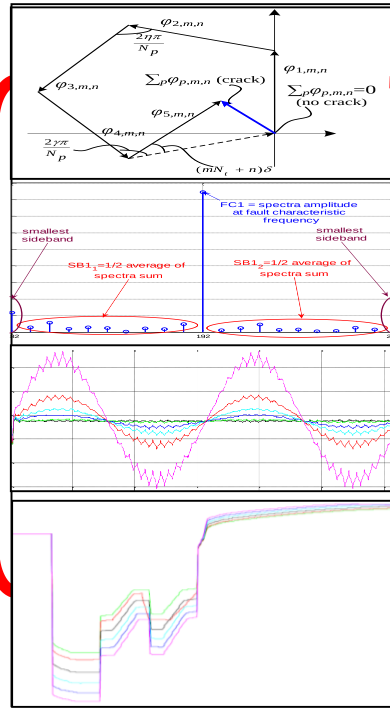
1) Choose U to Minimize a Cost Function: $J = \alpha FVaR + \beta Mission$

2) This U is called U_{opt}. The Uncertainty metrics provide a bound around U_{opt} where the system operator may adjust U and still ensure system reliability and sub-optimal operating conditions.

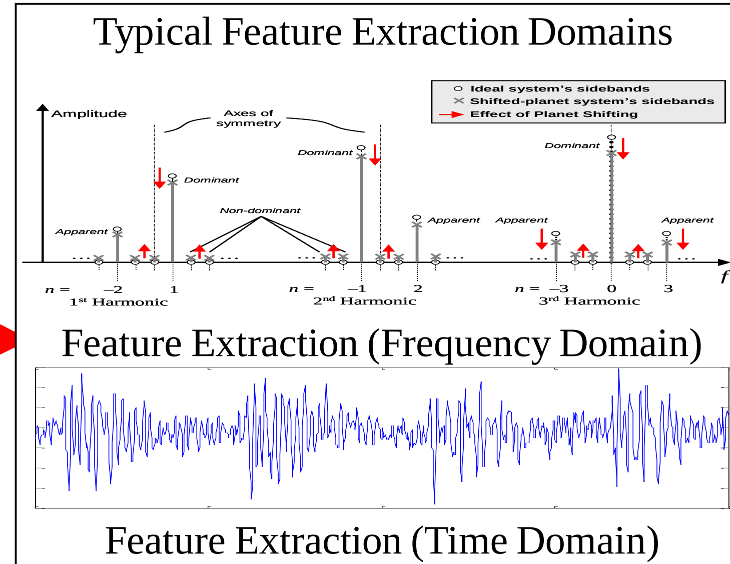
Understanding the Physics of Failure Mechanisms



Various Systems

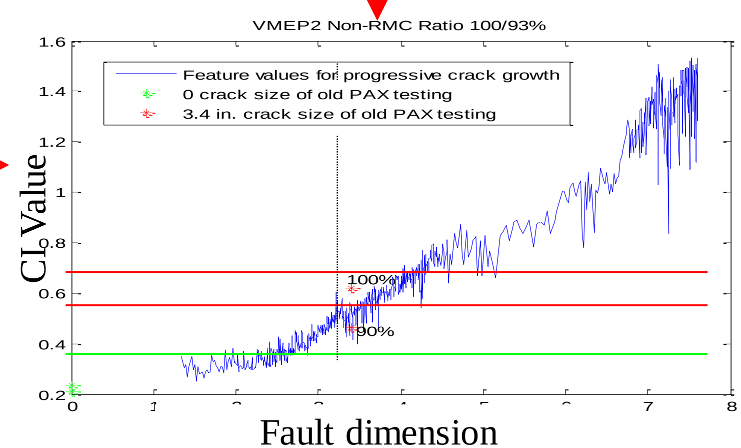


Failure Mechanism



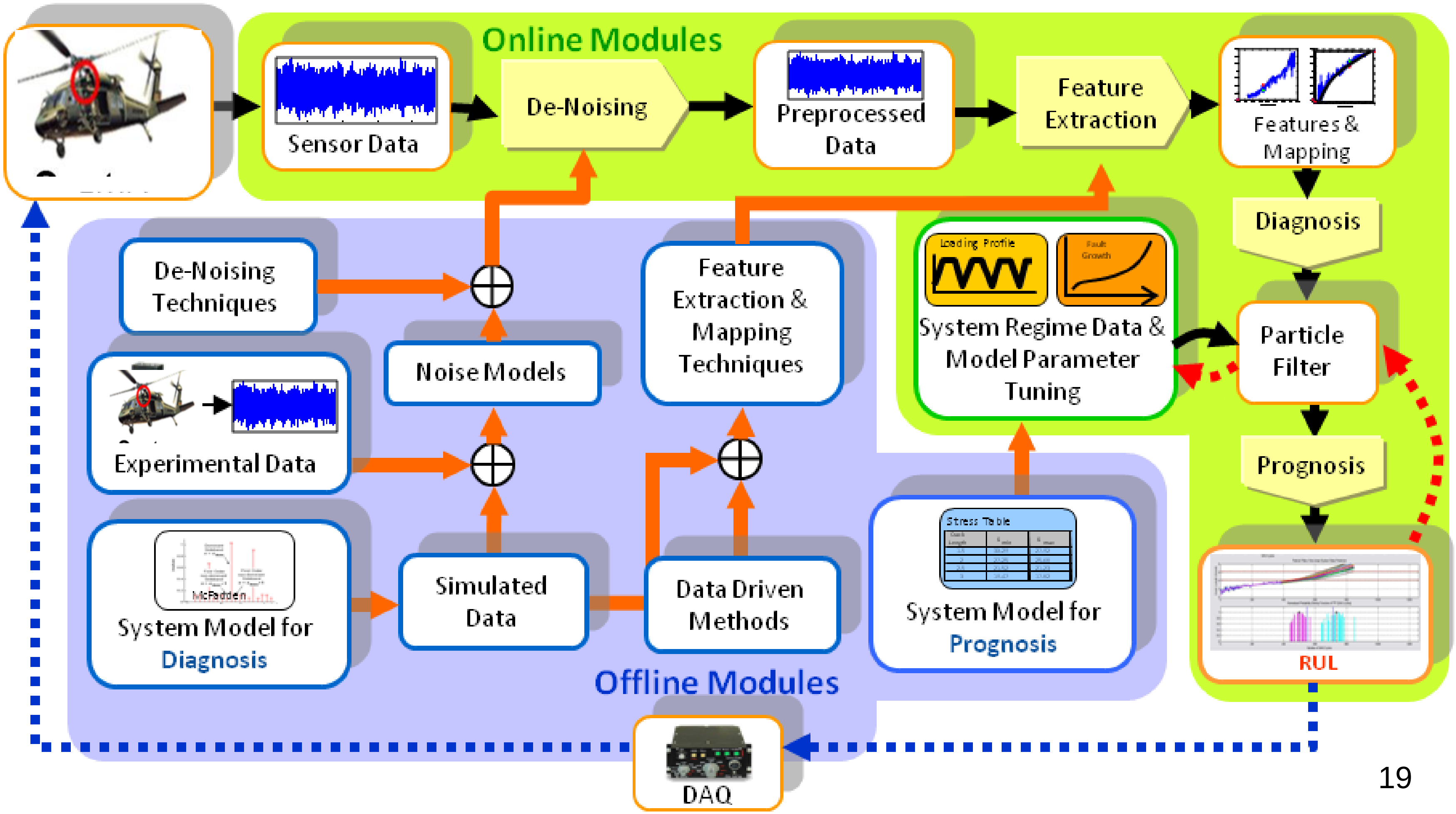
CI Value

Ground Truth Fault Dimension



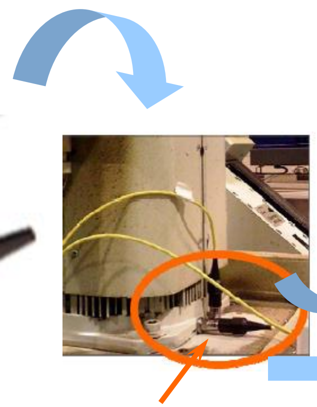
- Optimum Feature Selection
- Mapping of Features vs. Fault Dimension
- Utility in Diagnosis / Prognosis

Background: Prognostics and Health Management Architecture



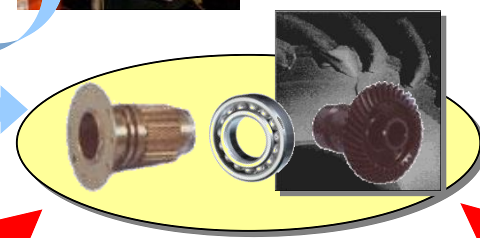
A Systems Engineering Process to Integrity Management

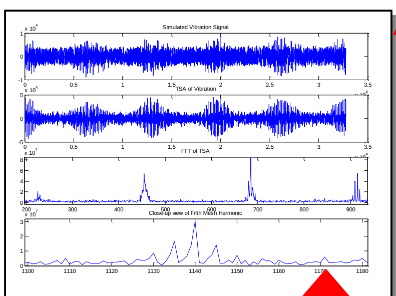
Testing, Modeling, and Reasoning Architecture – The Enabling Technologies for CBM



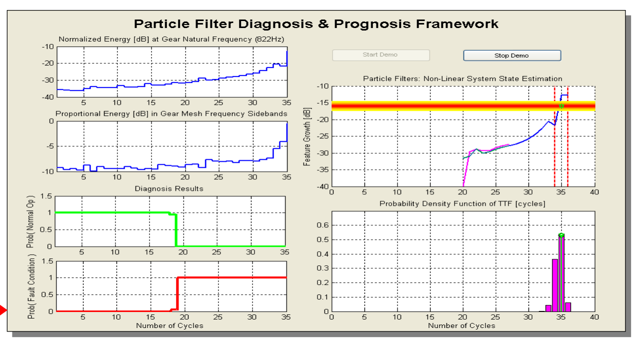
CBMi

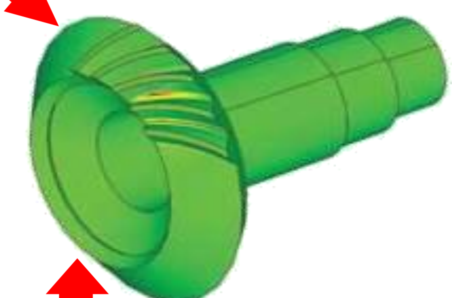
- Prevent unscheduled maintenance
- Assist the maintainer/manager in making intelligent decisions about the health status of critical equipment/facilities





Testing/
Seeded Fault Data





Modeling

Reasoning Architecture for Diagnosis-Prognosis

An Anomaly Detection Framework

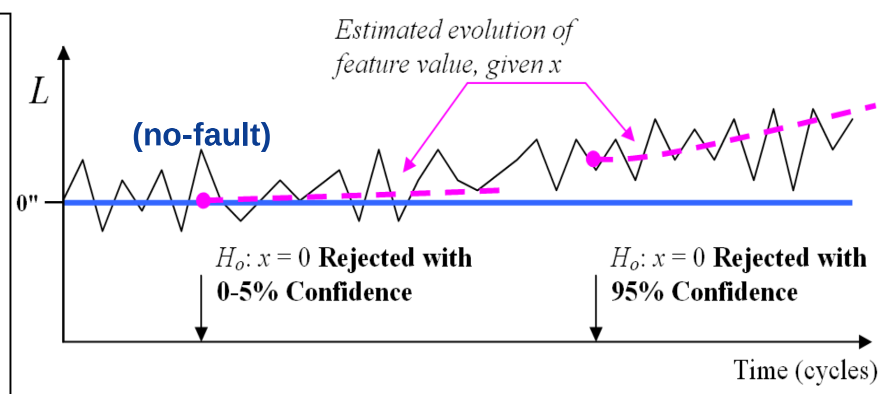
➢ The implementation Philosophy:

- Initially, noisy accelerometer measurements suggest that the fault hypothesis (crack, for example) is rejected. Confidence in fault being detected ~ 0-5%.
- A fault (crack) is initiated and its evolution is tracked via a model.

$$L(k+1) = L(k) + C \cdot (\Delta K)^{x} + w(k)$$

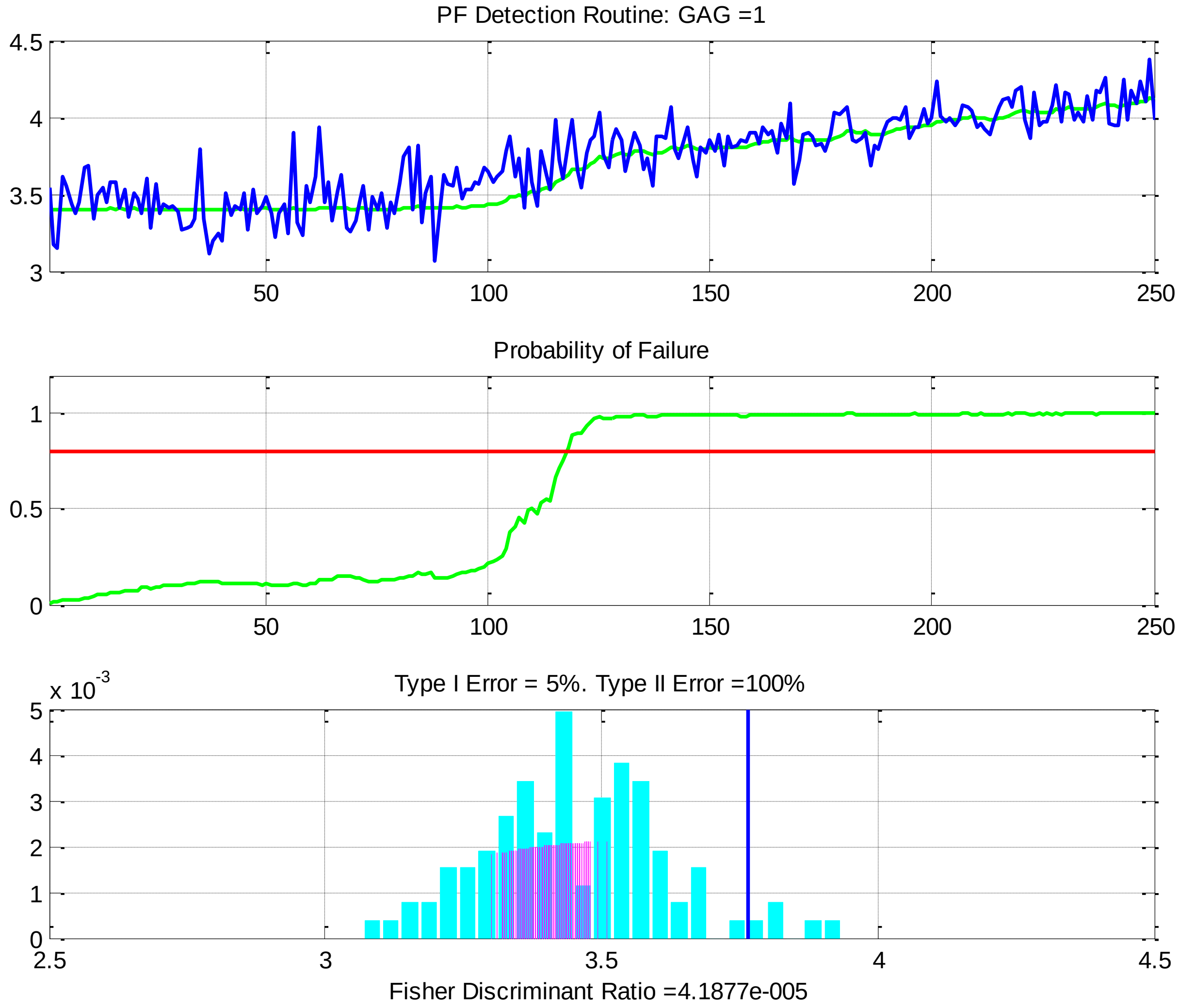
where:

$L(k)$: Crack length at time instant k
C: Material related coefficient
ΔK: Stress variation due to load profile
$w(k)$: white noise signal



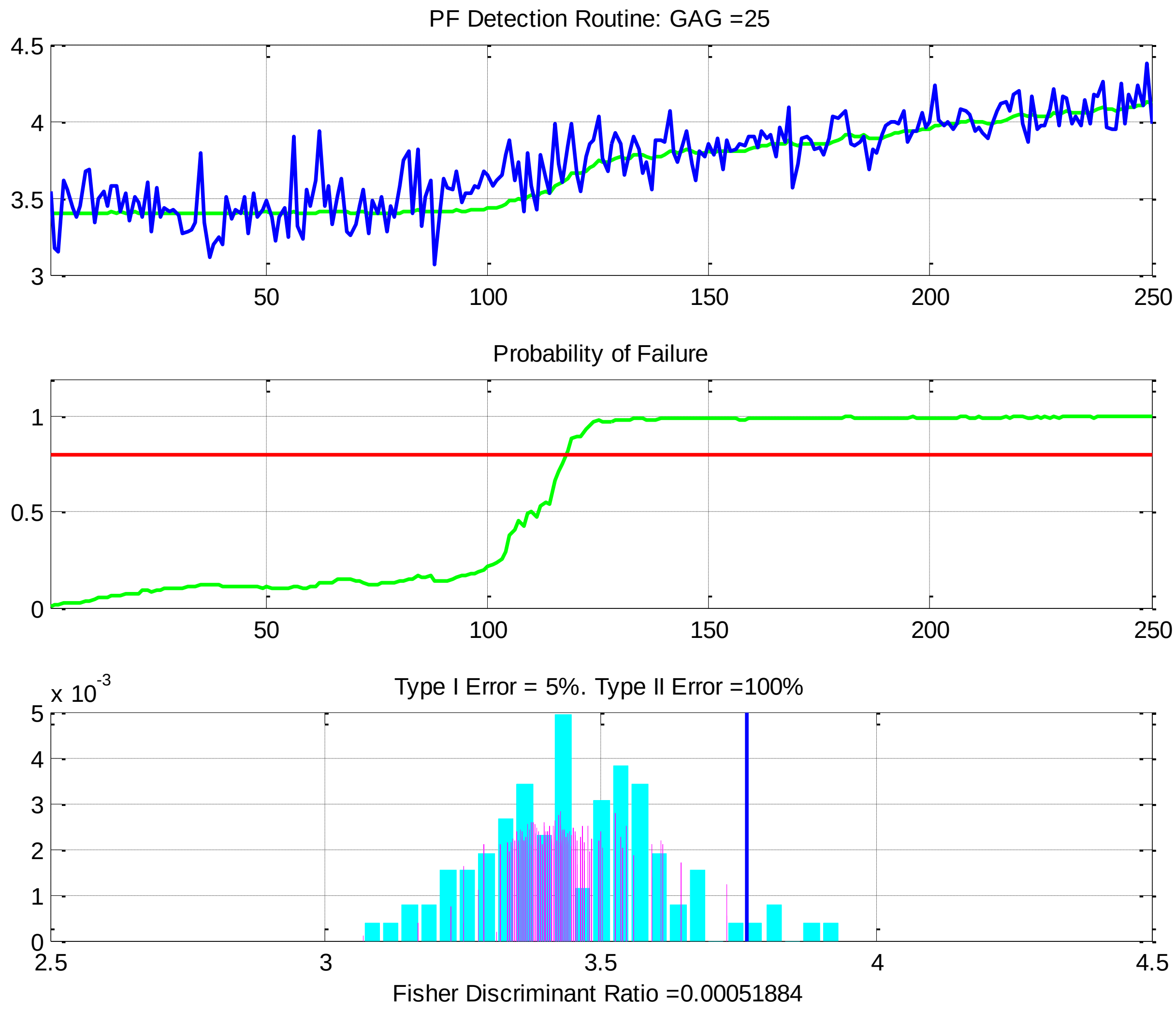
Particle Filtering-FDI Framework

Detection Results: Type I Error = 5%



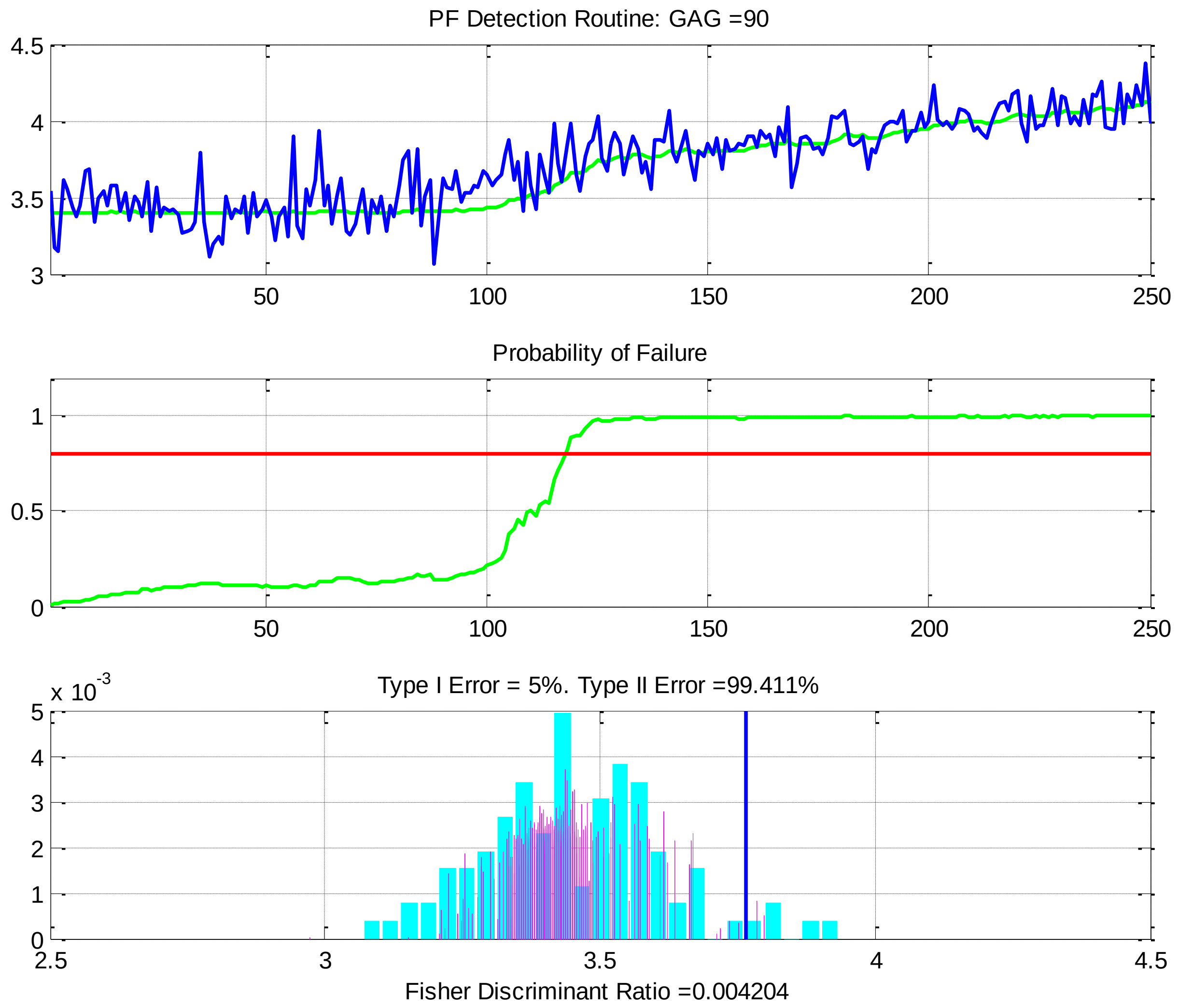
Particle Filtering FDI Framework

Detection Results: Type I Error = 5%



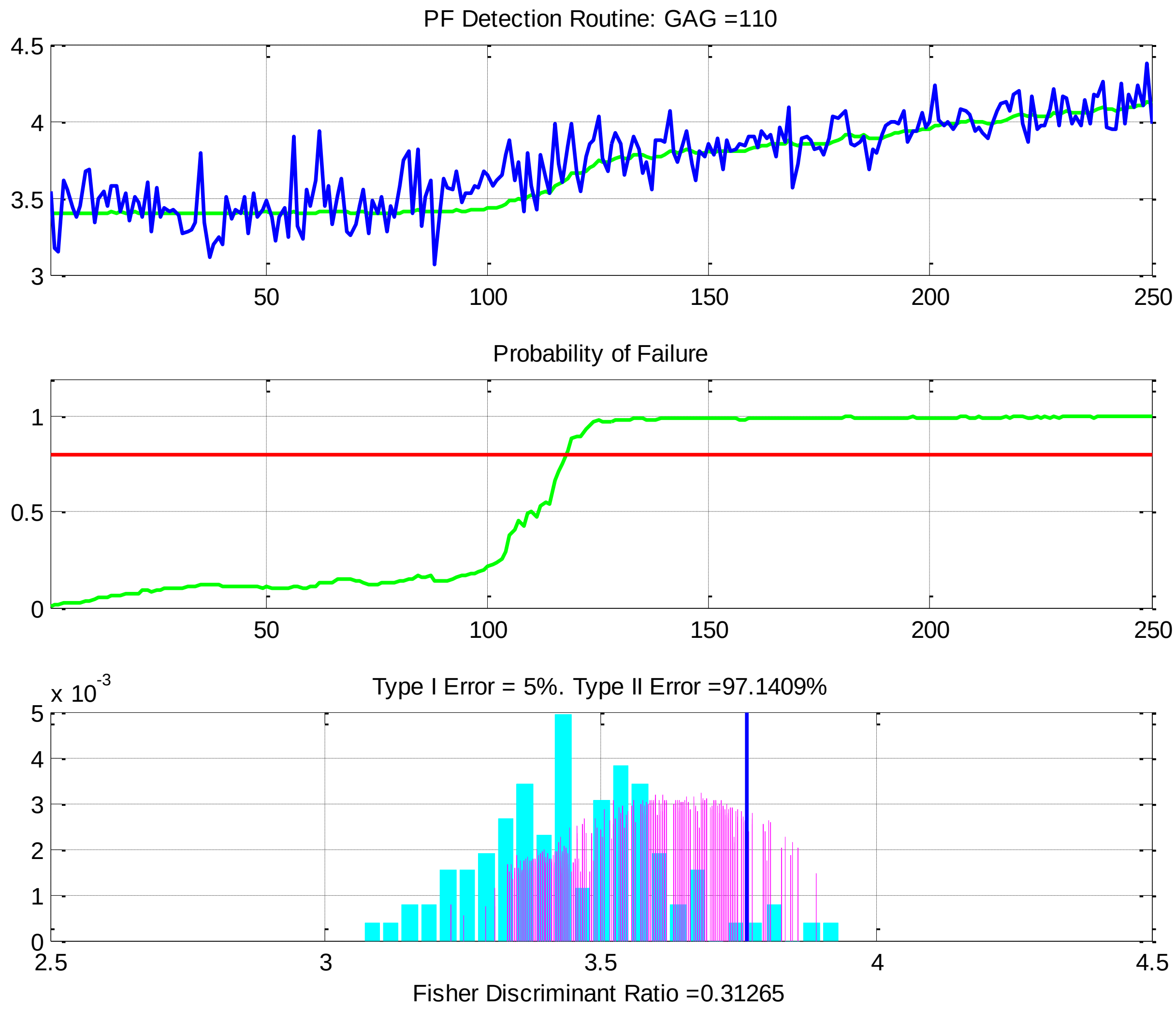
Particle Filtering-FDI Framework

Detection Results: Type I Error = 5%



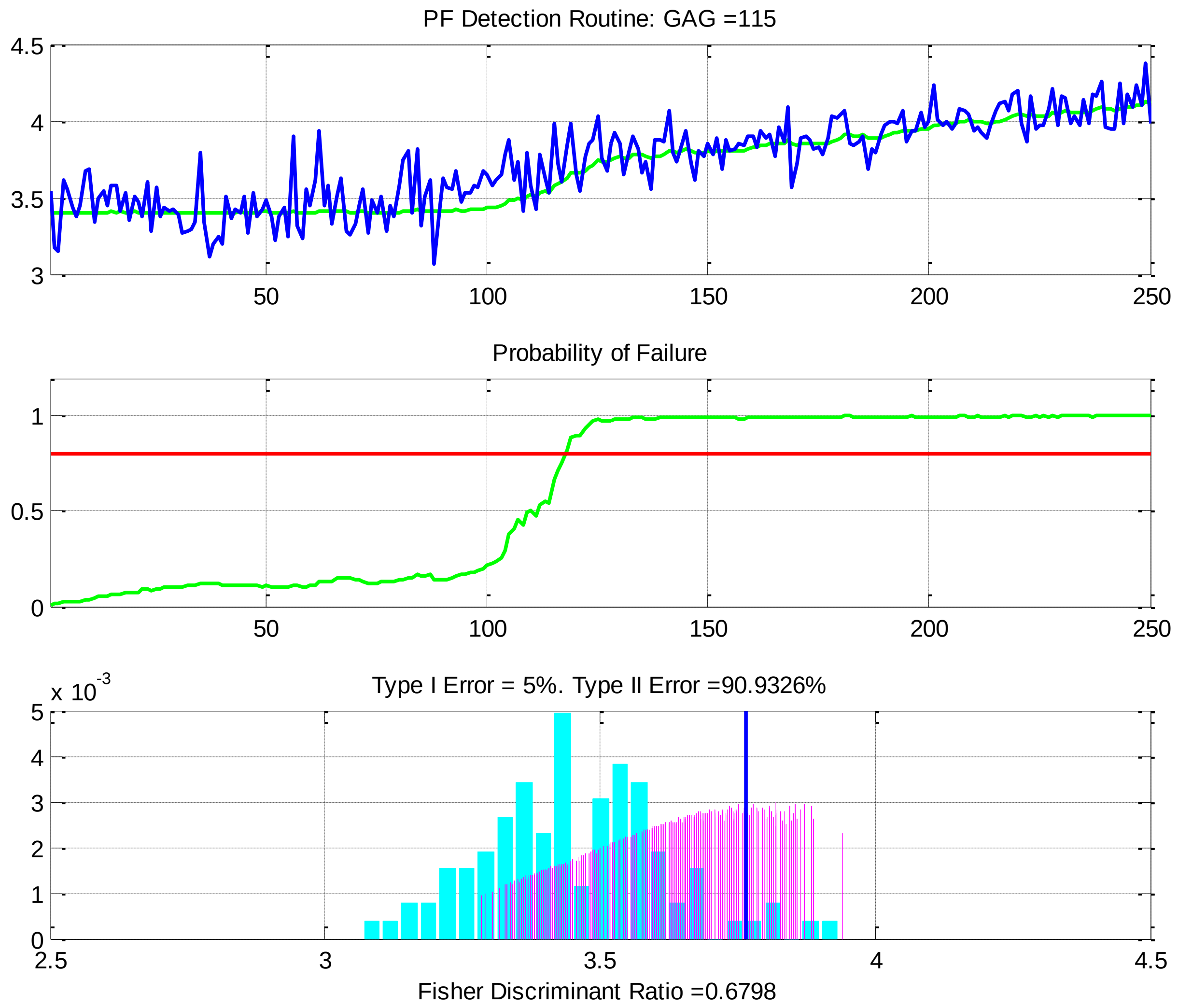
Particle Filtering-FDI Framework

Detection Results: Type I Error = 5%



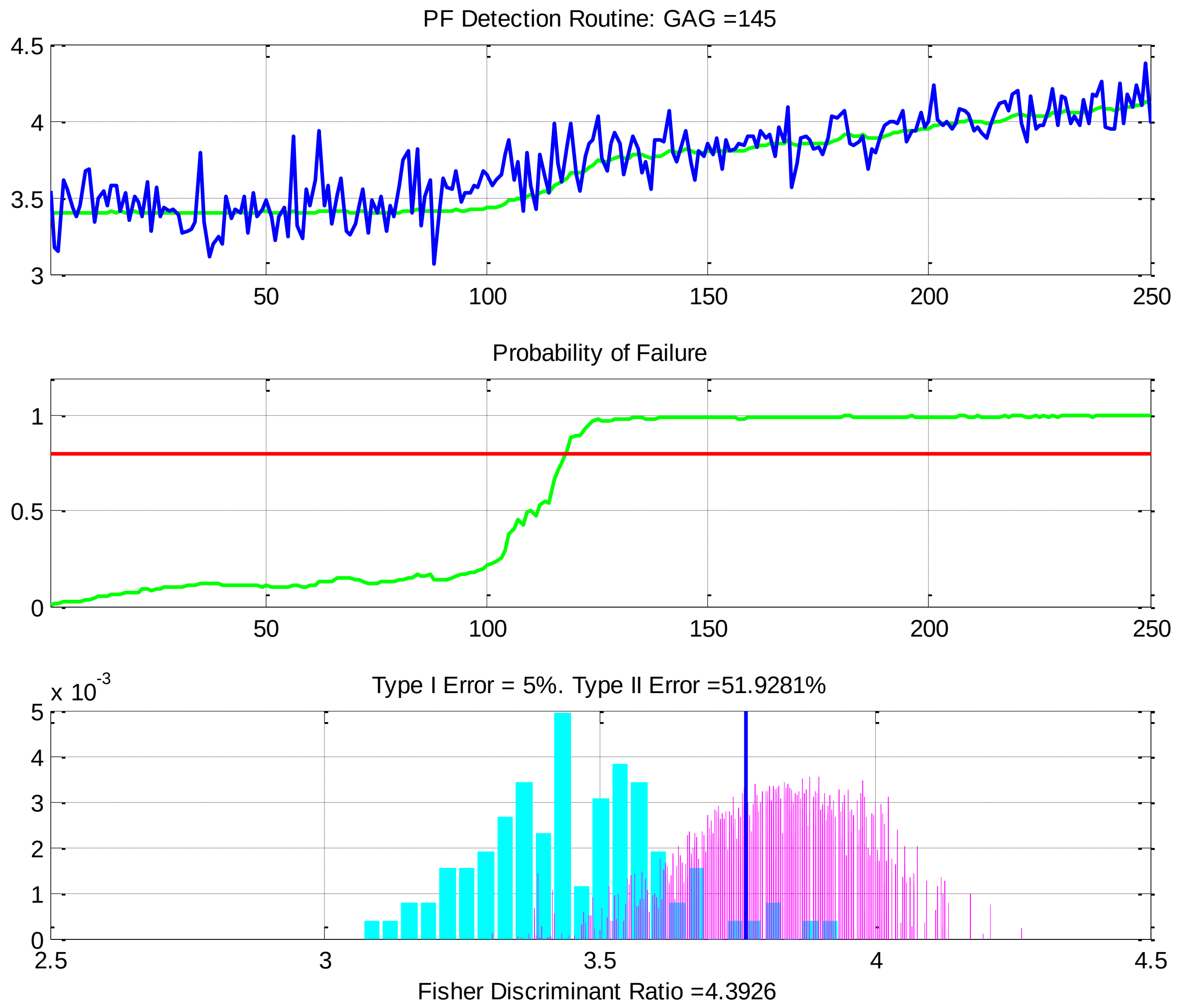
Particle Filtering-FDI Framework

Detection Results: Type I Error = 5%



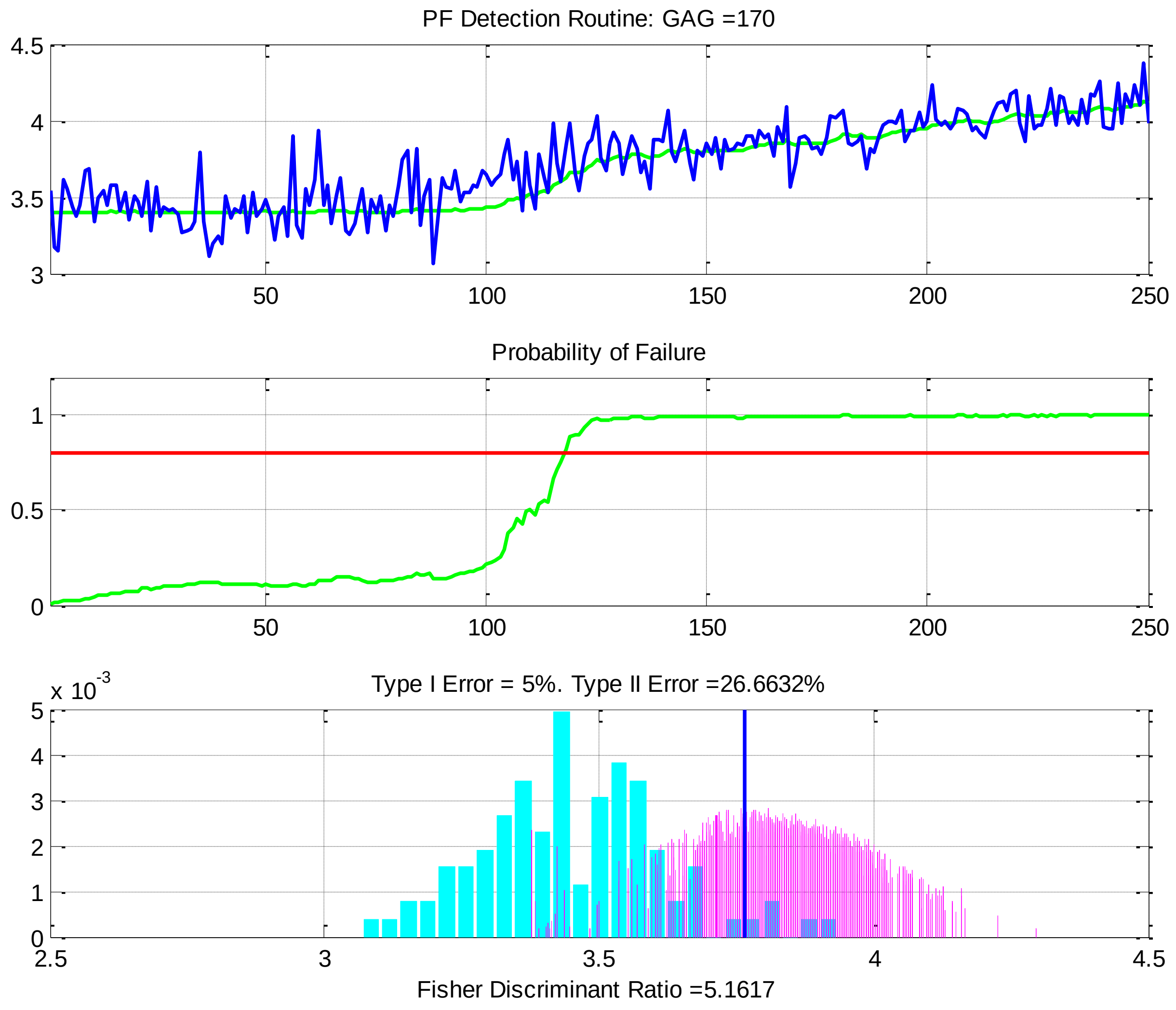
Particle Filtering-FDI Framework

Detection Results: Type I Error = 5%



Particle Filtering-FDI Framework

Detection Results: Type I Error = 5%

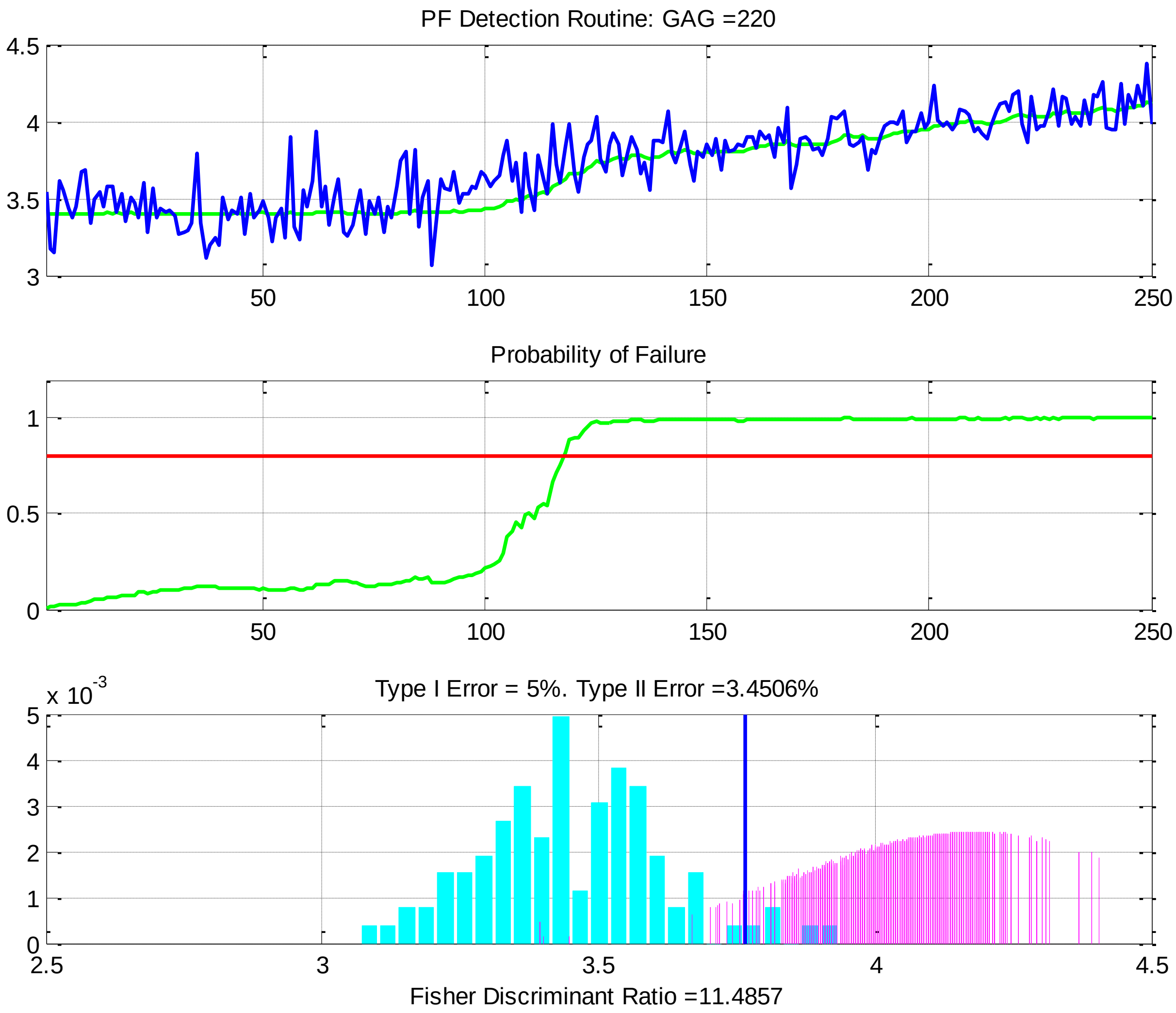


Particle Filtering-FDI Framework

Detection Results: Type I Error = 5%

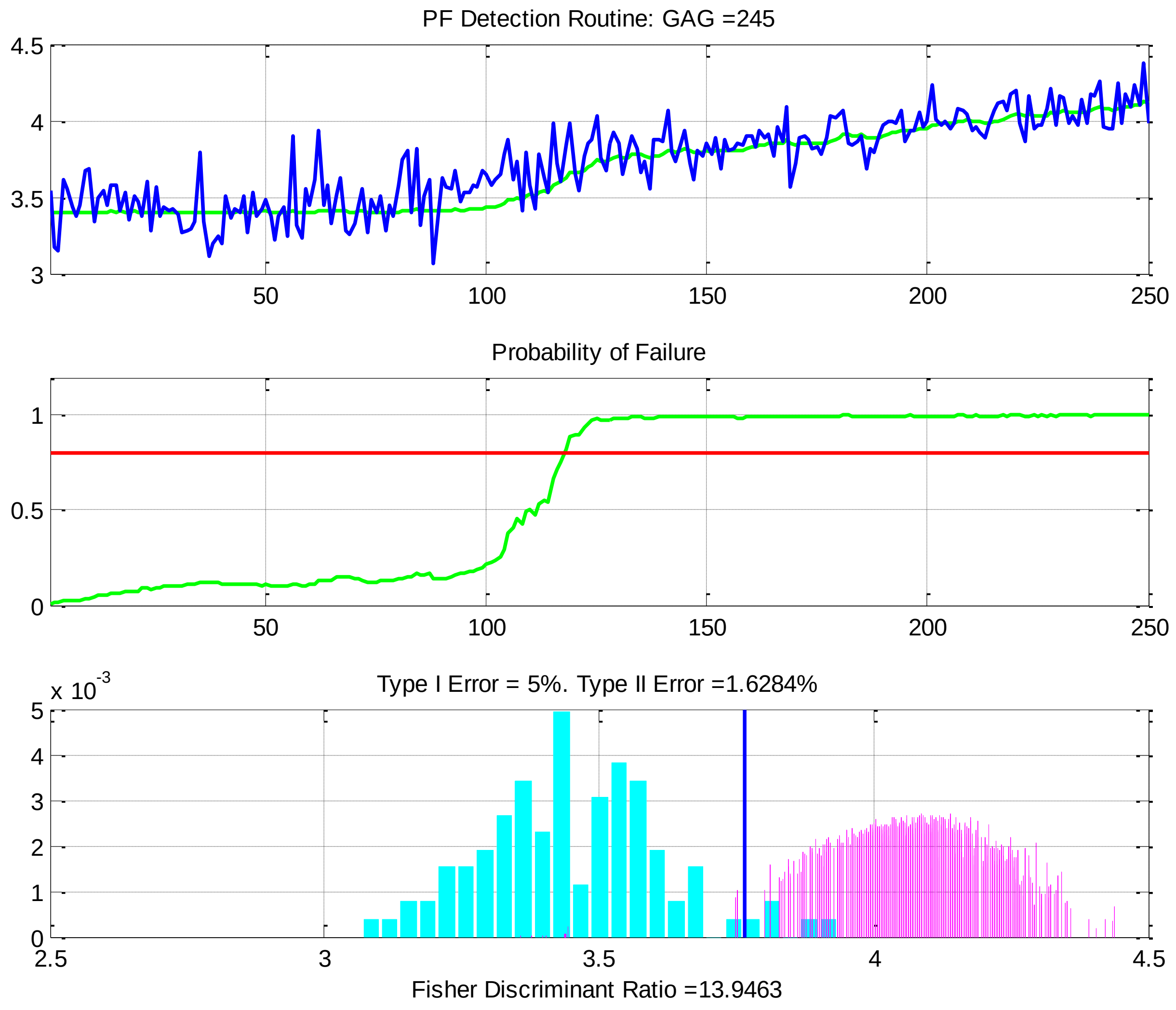
Particle Filtering-FDI Framework

Detection Results: Type I Error = 5%



Particle Filtering-FDI Framework

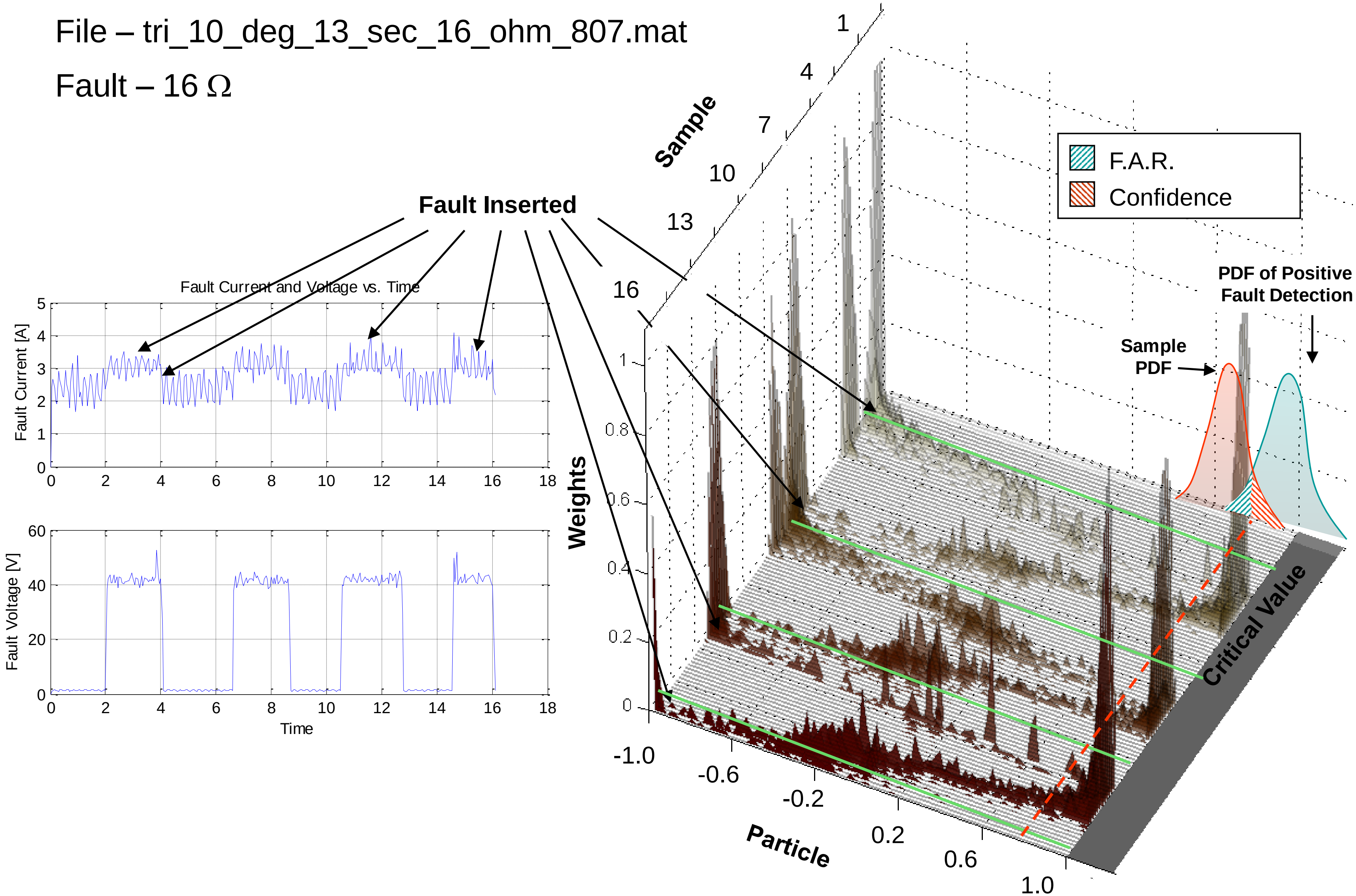
Detection Results: Type I Error = 5%



Particle Filter Results – Fault

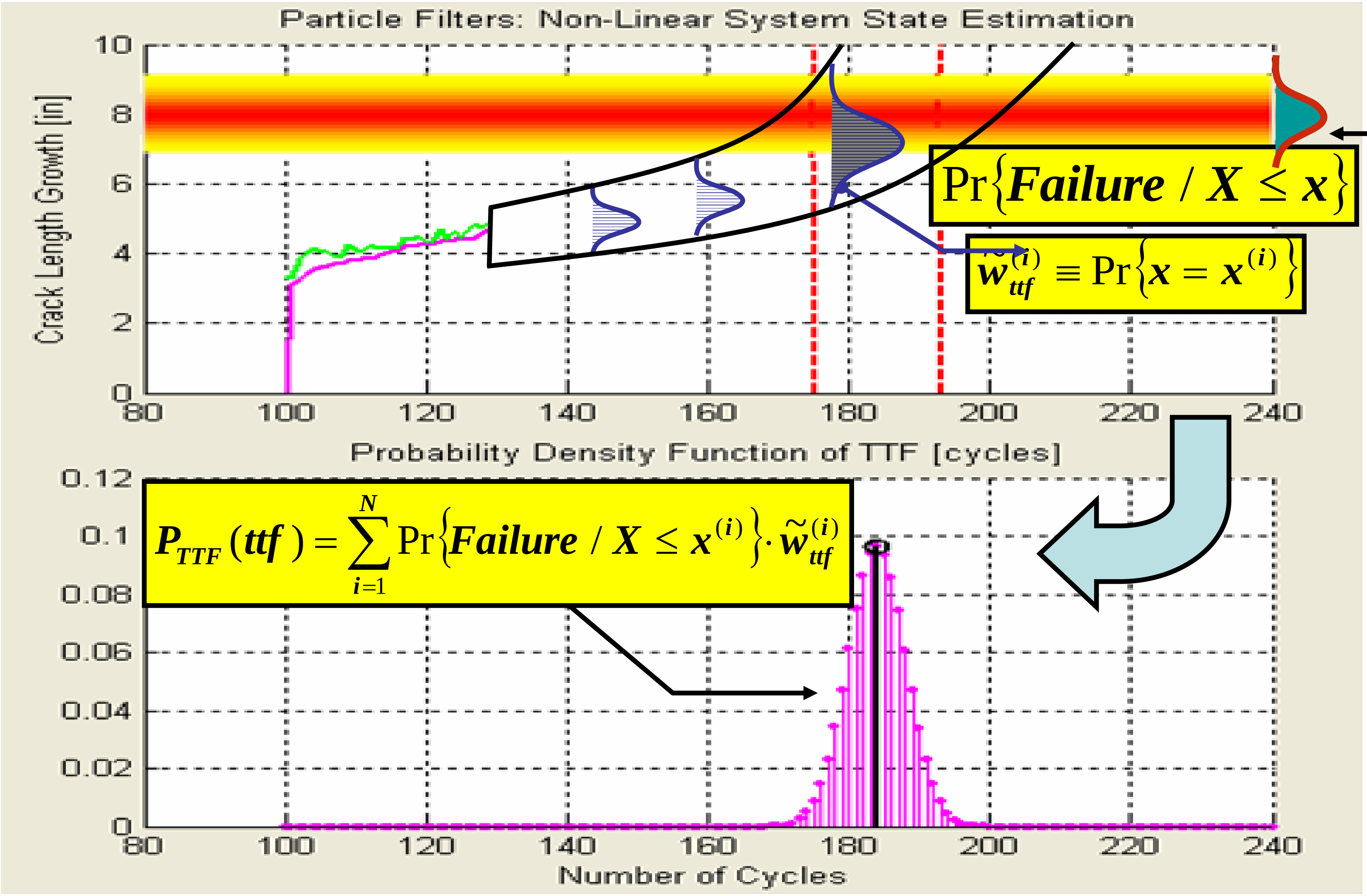
File – tri_10_deg_13_sec_16_ohm_807.mat

Fault – 16 Ω



Failure Prognosis

- Objective
  - Estimation of Remaining Useful Life of a failing component/system
  - Determine time window over which optimal maintenance or corrective action must be performed without compromising the system’s operational integrity
- Prognosis vs. Trending
- Prediction in the presence of uncertainty
- Prognosis from “birth” or “usage-based” vs. “heatlt-based” or, real-time prognosis
- The customer base:
  - The maintainer
  - The fleet commander/process manager
  - The designer



Particle Filters: Non-Linear System State Estimation
Crack Length Growth [in]
$\Pr\{Failure / X \le x\}$
$\tilde{w}_{ttf}^{(i)} \equiv \Pr\{x = x^{(i)}\}$
Probability Density Function of TTF [cycles]
$P_{TTF}(ttf) = \sum_{i=1}^{N} \Pr\{Failure / X \le x^{(i)}\} \cdot \tilde{w}_{ttf}^{(i)}$
Number of Cycles

Risk and Confidence

- Risk = 1/Distance between current state and a critical safe envelope, assuming certain operating conditions.
- Risk: Probability of system failure or probability of loss of control for a chosen strategy.

Risk indicators

- **Fault Value at Risk (FVaR)**

- The $FVaR(t, t_{prognosis})$ is the maximum increase in fault dimension $l(t)$ that can occur within time t after the time of prognosis $t_{prognosis}$.

- The FVaR at the confidence level α is given by the smallest number $l(t)$ such that the probability that the damage (degradation, fault dimension) $L(t)$ exceeds $l(t)$ is not larger than $(1- \alpha)$, i.e.

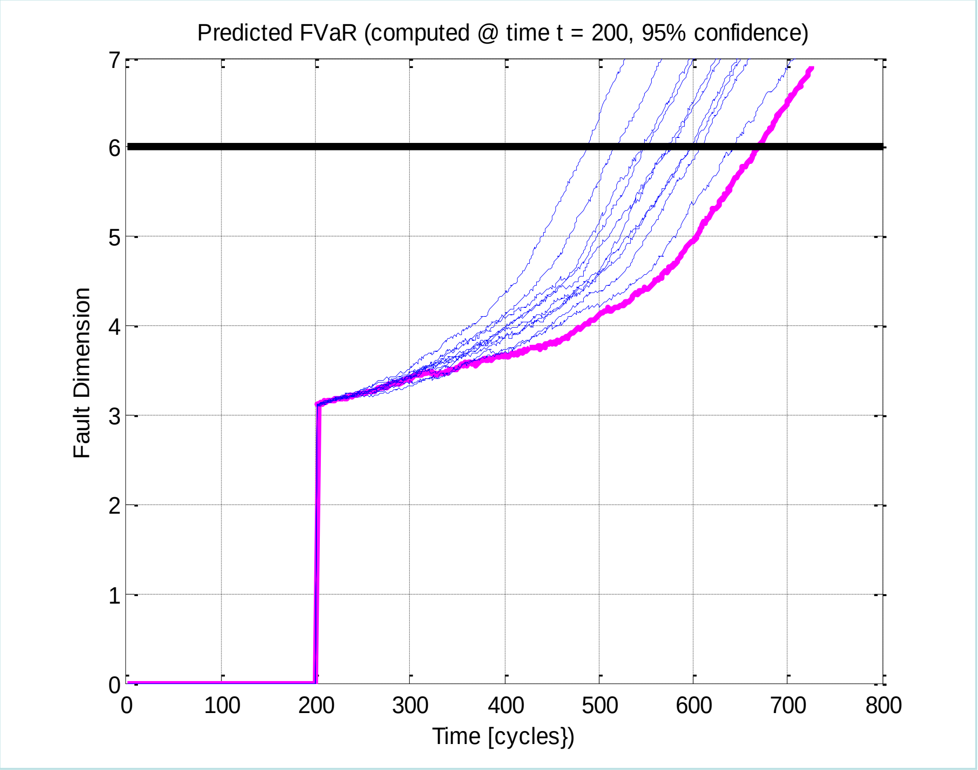
$$FVaR(t, t_{prognosis}) = \inf\left(l(t) \in \Re : P\left\{ L(t) > l(t) \mid y_{t_{prognosis}} \right\} \leq 1 - \alpha \right)$$

Online computation of Risk Indicators

- Within a PF-based prognosis framework:

$$FVaR(t,t_{prognosis}) \Leftrightarrow \alpha = 0.95 = \int_{-\infty}^{FVaR(t,t_{prognosis})} \hat{p}(x_t^1 \mid y_{t_{prognosis}})dx_t^1$$

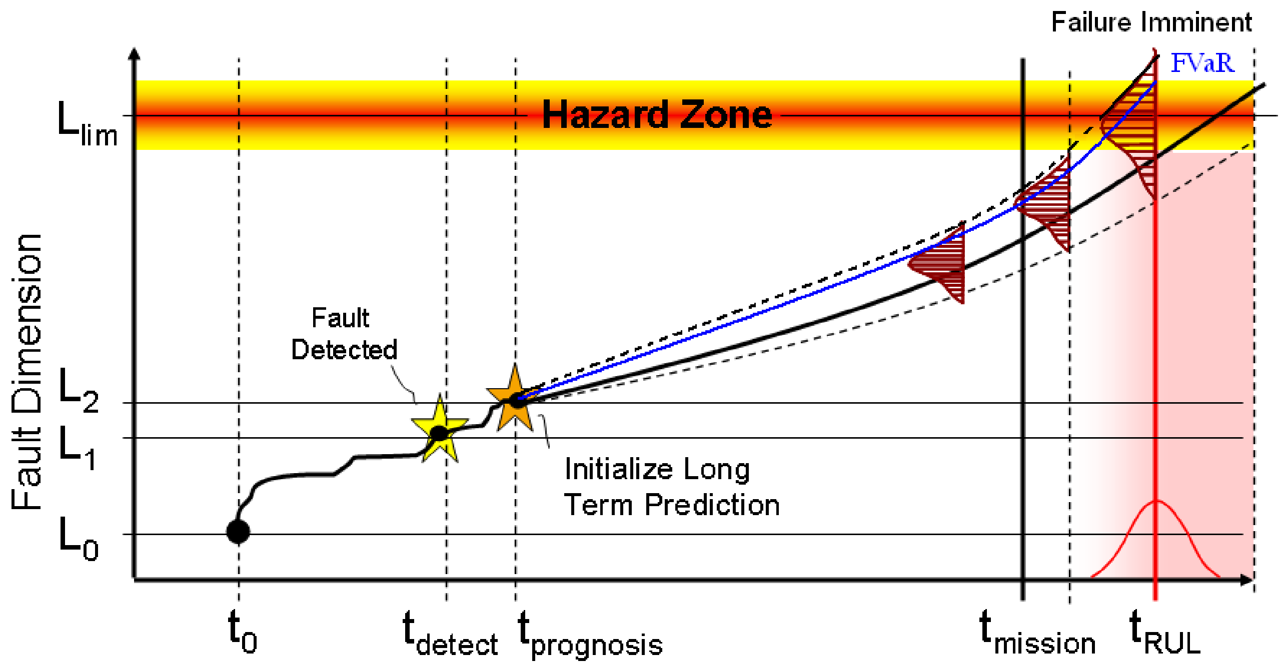
- It can be computed online, based on the current PF estimate of the state vector.
- Requires the definition of a borderline condition for the operation of the system.
- Different load conditions will lead to dissimilar FVaR functions



Confidence: Necessary ingredient for action

$$\alpha = \int_{-\infty}^{FVaR(t_{future},t_{prognosis})} \hat{p}(x_{t_{future}} \mid y_{t_{prognosis}})dx_{t_{future}}$$

α: degree of confidence specified by the user



FVaR predicted from time $t_{prognosis}$

An Example:

Consider an a/c component fault

The system has 12 hr FVaR of fault dimension at 95% confidence level means:

> We are 95% confident that a change in the fault dimension (damage) in 12 hrs will not result in an increase of 10 units in the fault dimension.

Or:

> There is a 5% confidence level that damage will increase by 10 units or more in 12 hrs.

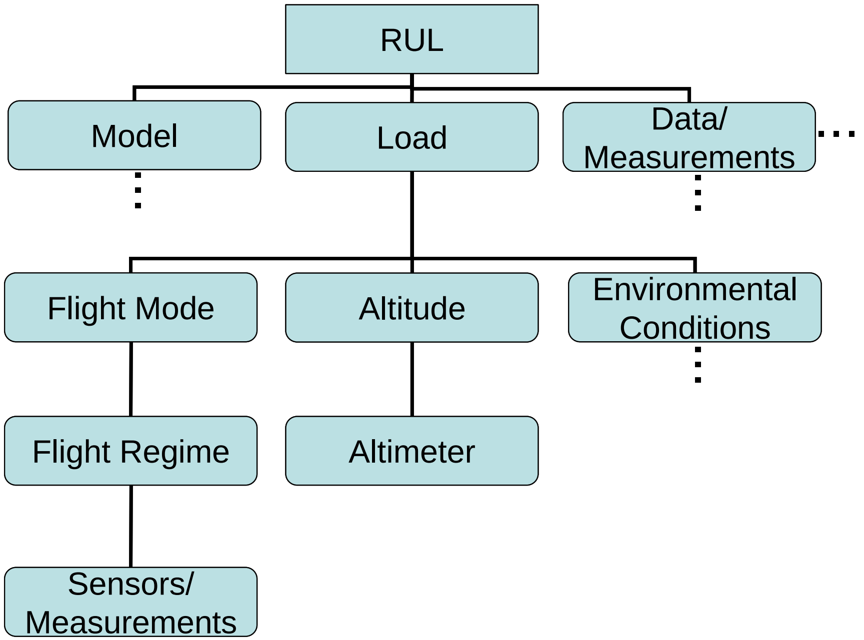
Risk Control

- Change risk profile through proactive maintenance and upgrade
- Take corrective action with acceptable risk
    - Quantify <u>risk</u> and <u>uncertainty</u>
    - Essential link between failure prognosis and reconfigurable control

Uncertainty Representation and Management

Sources of uncertainty – the uncertainty tree

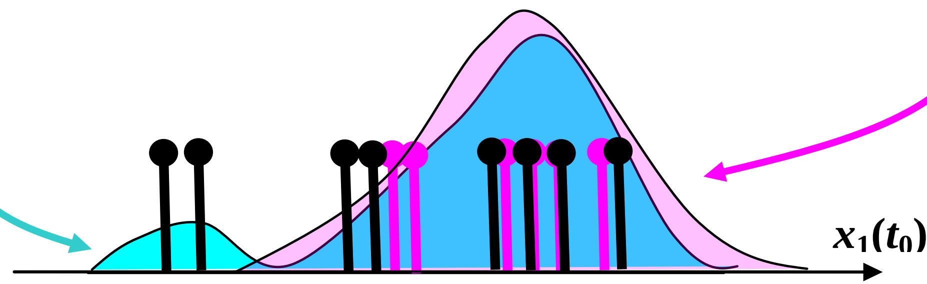
- A graphical depiction of the variable dependence in uncertainty analysis.
- Technique suitable for combining multiple sources of uncertainty for a single variable.
- Useful also for design of experiments.
- A tool for relating uncertainties: root-sum-square.



Risk-Sensitive Particle Filtering – A Novel Approach to Estimate Scarce Event (Fault Evolution)

$$\boxed{q_t(\tilde{x}_{0:t} \mid x_{0:t-1}) = p(\tilde{x}_t \mid x_{t-1}) = f_t(\tilde{x}_t \mid x_{t-1})}$$

$$\boxed{q\left(\tilde{d}_t, \tilde{x}_t \mid \tilde{d}_{0:t-1}^{(i)}, x_{0:t-1}^{(i)}, y_{1:t}\right) = \gamma_t \cdot r(d_t) \cdot p\left(d_t, \tilde{x}_t \mid y_{1:t}\right)}$$



Where:

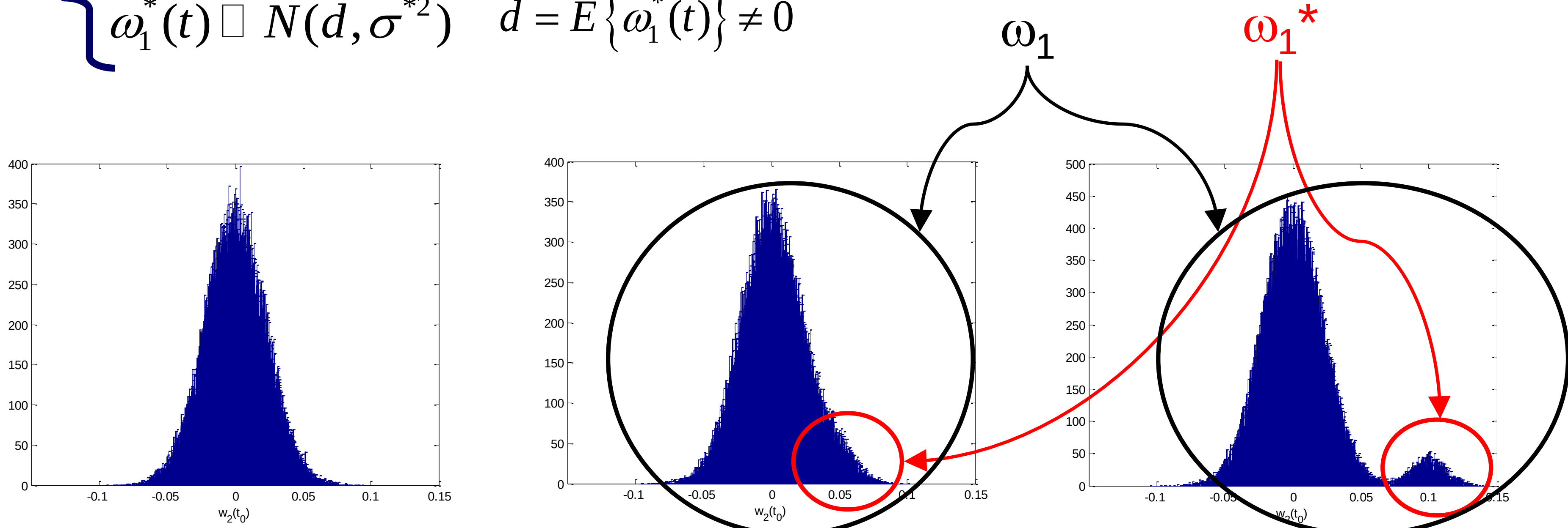
- d_t is a set of discrete-valued states representing fault modes
- x_t is a set of continuous-valued states that describe the evolution of the system
- $r(\mathrm{d}_t)$ is a is a positive risk function
- γ_t is a normalizing constant

Proposed Approach

$$\begin{cases} x_1(t+1) = x_1(t) + C\cdot x_2(t)\cdot(a - b\cdot t + t^2)^m + \omega_1(t) \\ x_2(t+1) = x_2(t) + \omega_2(t) \end{cases}$$

$$\omega_1(t) \sim N(0, \sigma^{*2})$$

$$\begin{cases} \omega_1(t) \sim \delta\cdot\omega_1'(t) + (1-\delta)\cdot\omega_1^*(t) \\ \omega_1^*(t) \sim N(d, \sigma^{*2}) \qquad d = E\left\{\omega_1^*(t)\right\} \neq 0 \end{cases}$$



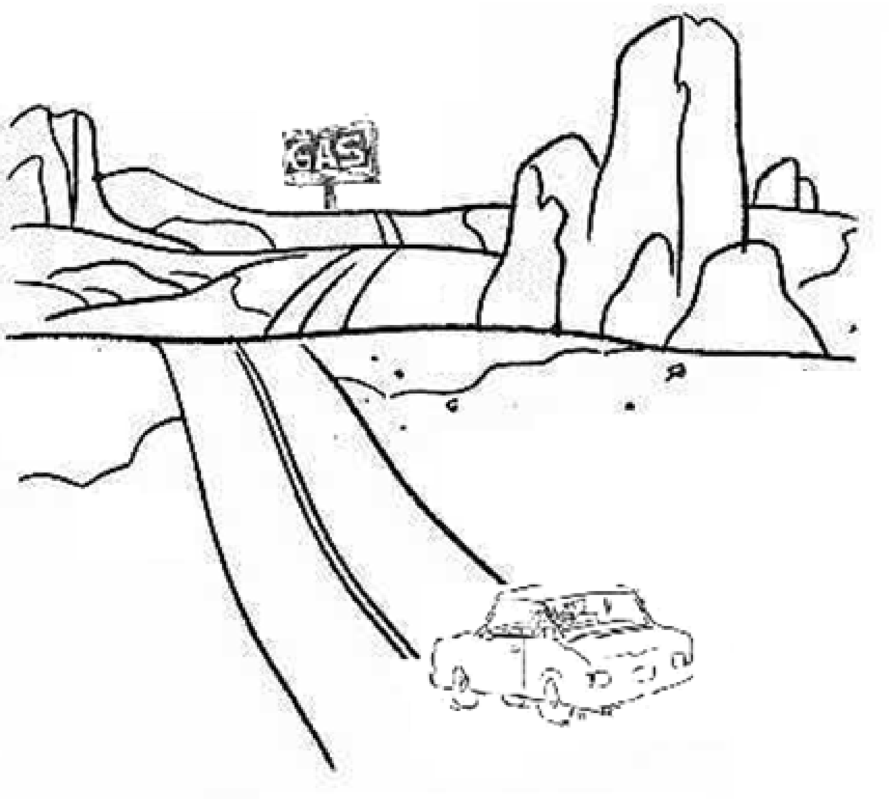
RSPF Kernel **$E\{\omega_1{}^*\} = 0.00$** | **RSPF Kernel** **$E\{\omega_1{}^*\} = 0.05$** | **RSPF Kernel** **$E\{\omega_1{}^*\} = 0.10$**

Fault – Tolerant Control

(Fault Mitigation, Fault Accommodation, Reconfigurable Control)

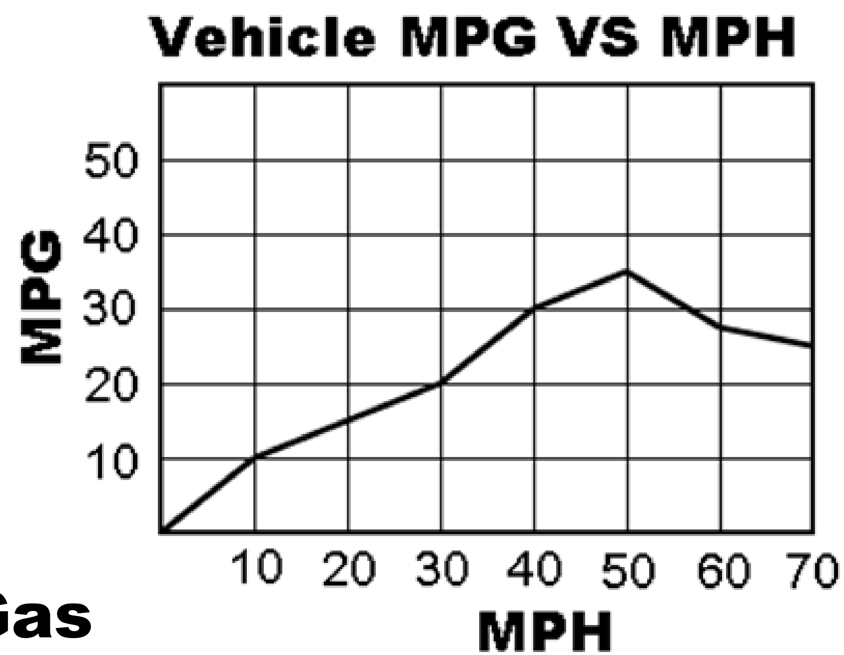
The Caveat: With Prognostic Information

The Link between PHM and Control



We have 1 GAL left in the tank

THE NEAREST STATION IS
30 MI AWAY!!!



Can We Make It To The Gas Station?

Motivation

Previous and Current Initiatives

Timeline

1980's — 1990s — 2000s — Present — Future

Military fixed wing aircraft programs

AVIATION SAFETY PROGRAM NASA /FAA

NASA Aviation Safety Program

Integrated Resilient Aircraft Control

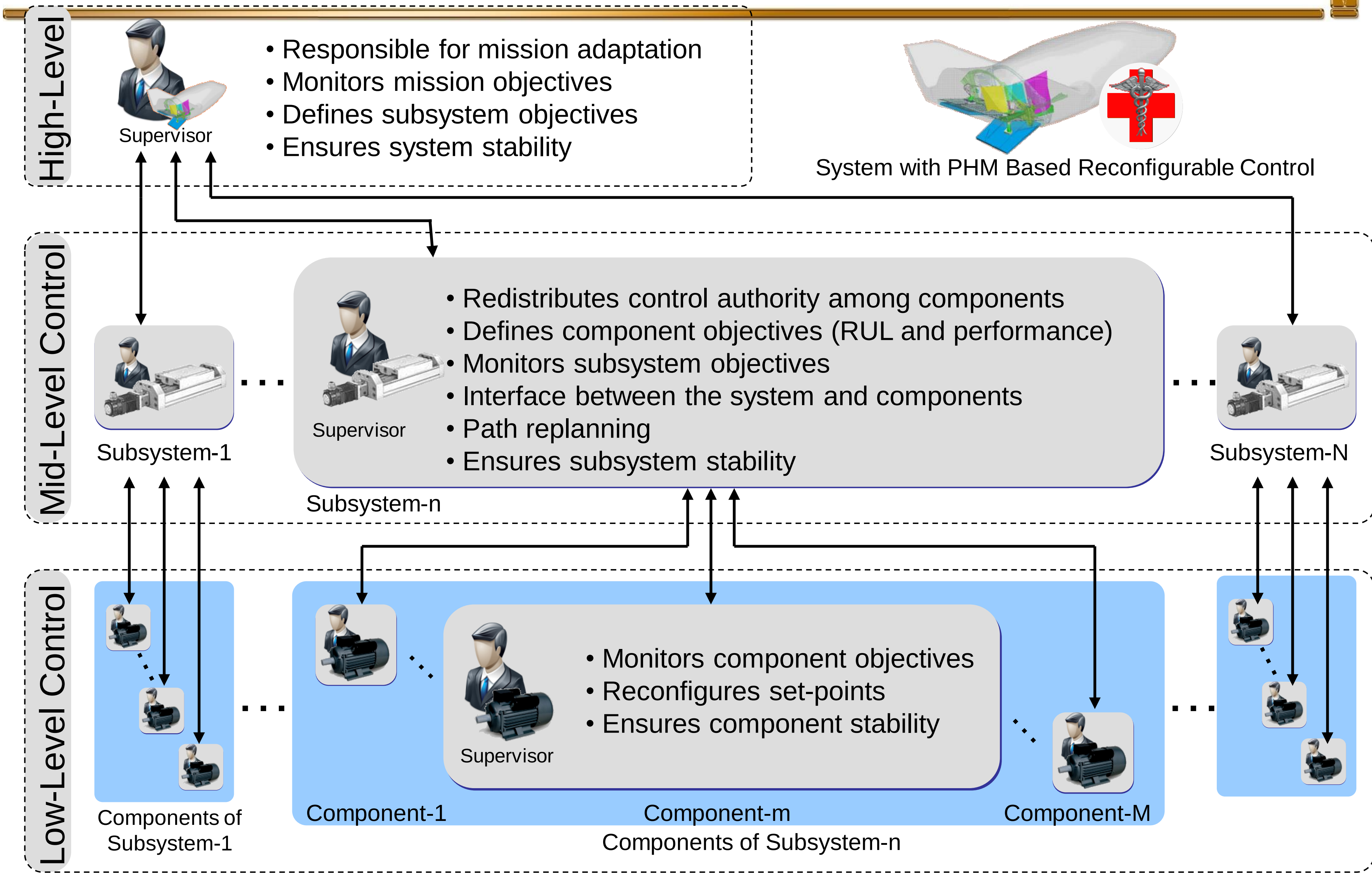
IVHM HTD

Integrated Vehicle Health Management

- Prognostic Center of Excellence
- Integrated Flight Deck Project
- Aircraft Aging Durability Project
- Fundamental Aeronautics
- Exploration Systems Mission Directorate
- Joint Army Navy NASA Air Force Initiative

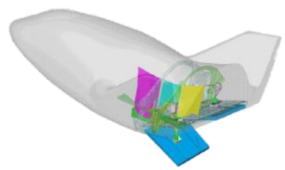
Reconfigurable Control Architecture

Functional Relation in the Hierarchy



The Control Architecture

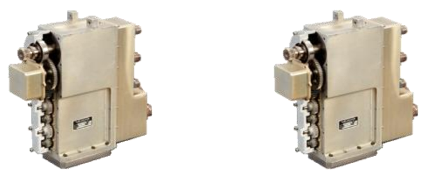
High Level



Vehicle

- System level
- Monitors mission objectives
- Mission adaptation (eg. path replanning)

Mid Level



Control Surface Actuators

- Sub-system level
- Redistributes control authority
- Ensures vehicle stability

Low Level

Brushless-DC Motors

- Component level
- Reconfigures set-points
- Ensures minimum performance

Timeline

1980's | 1990s | 2000s | Present | Future

Military fixed wing aircraft programs

NASA Aviation Safety Program

Collective goals:

- Improve safety and reliability
  - Early fault detection
  - Failure prediction
  - Fault mitigation
- Reduce maintenance costs
- Reduce system down-time

Health Management

ter of

Deck

urability

ronautics

ems

ate

NASA

ve

The Control Architecture

Introduction

– The Big Question –

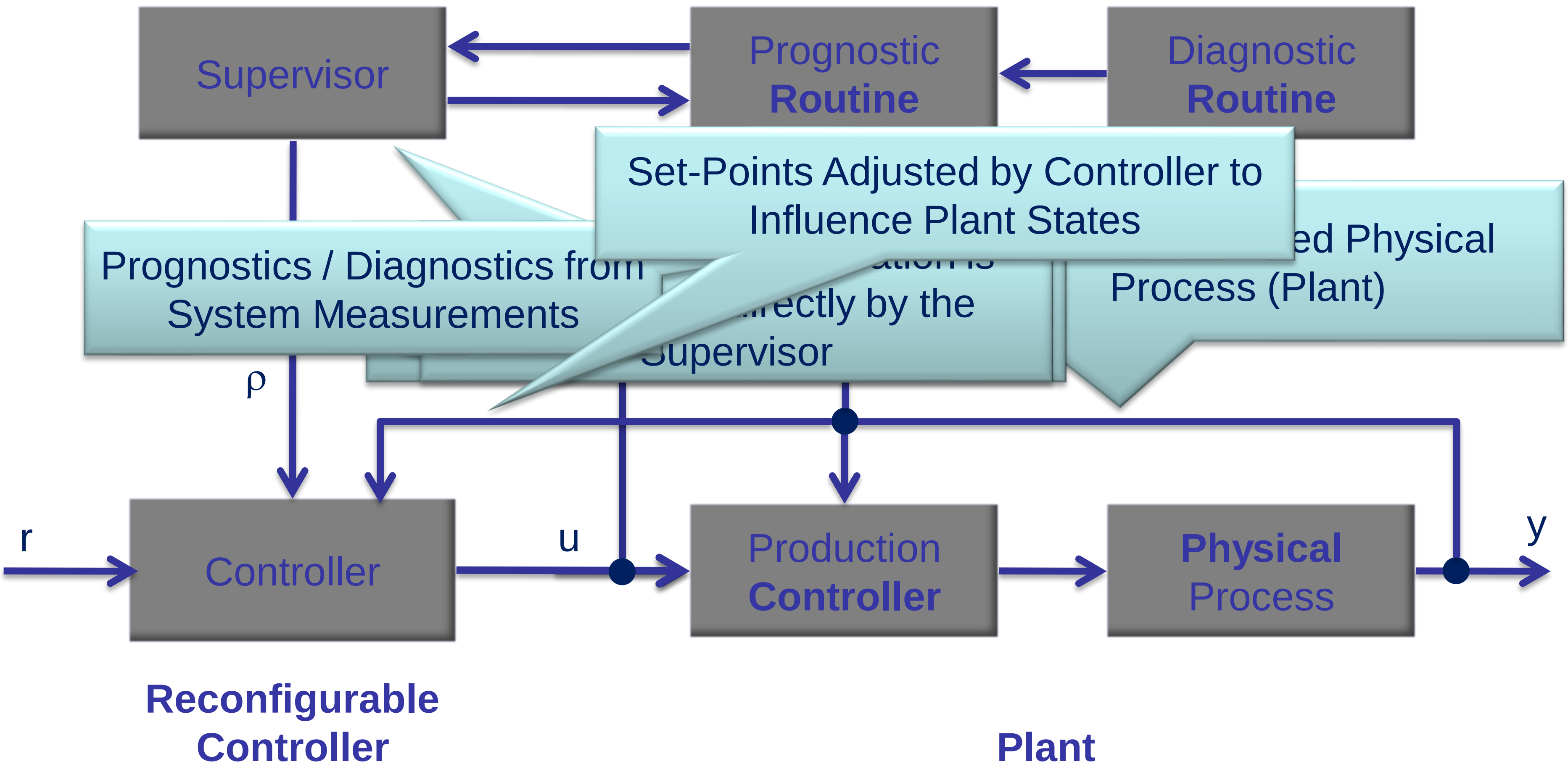
Can remaining useful life (RUL) be increased by reducing performance?

Health vs. Performance

- How is RUL related to performance?
- How can performance be reduced?
- What are the factors?
  - Application
  - Operating conditions

Architecture Dependent

The Control Architecture
Reconfigurable Control Architecture



The Control Architecture

Optimization Criteria for MPC

Health

vs.

Performance

Assumptions

RUL Related States

vs.

Tracking Error

Adaptation parameter ρ adjusts cost

- The cost function:

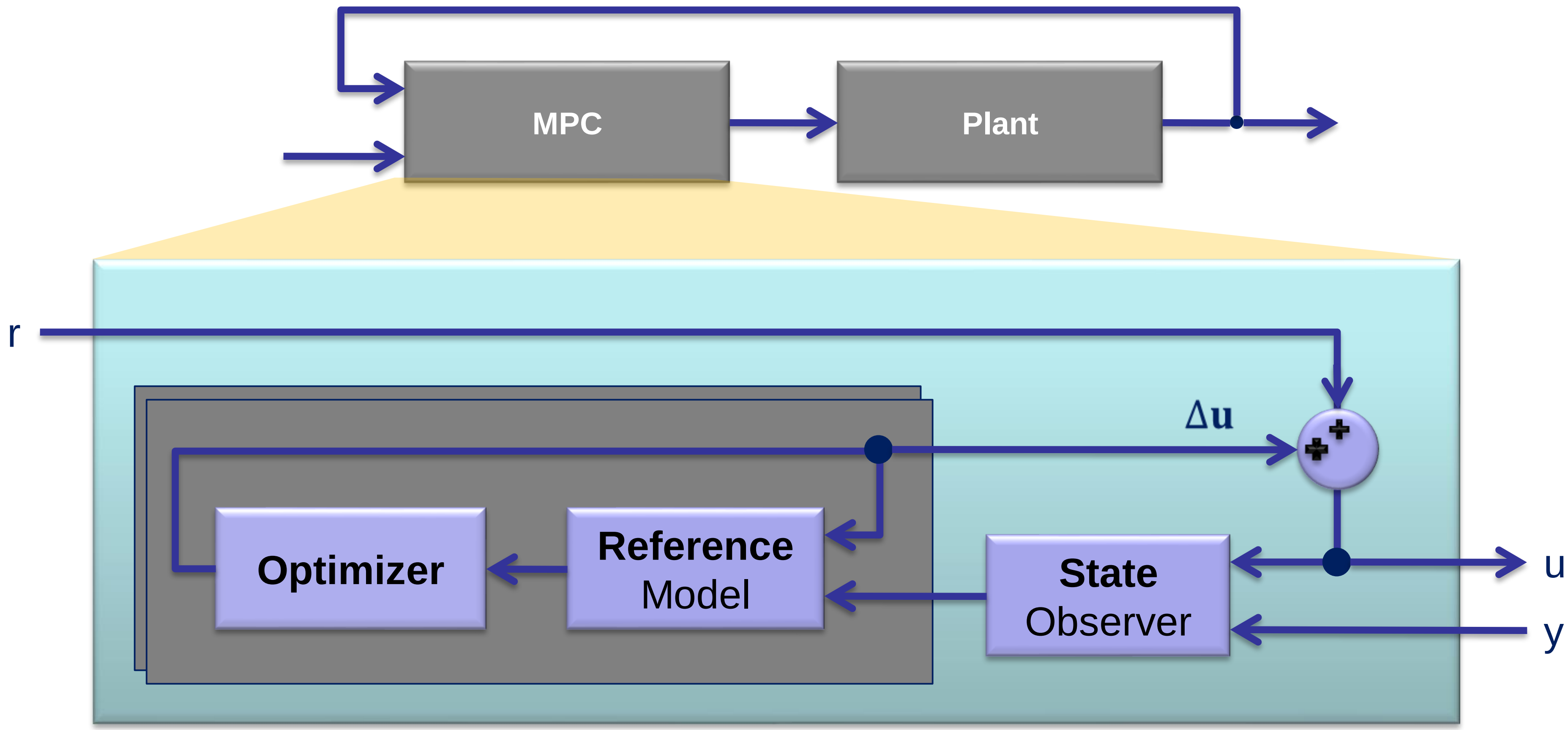
$$J = \min_{\Delta \mathbf{u}} \int_{t_0}^{t_0+T} [(\mathbf{x} - \mathbf{x}^{\star})^{\top} (\ \mathbf{Q})(\mathbf{x} - \mathbf{x}^{\star}) + \Delta \mathbf{u}^{\top} \mathbf{R} \Delta \mathbf{u}] dt$$

- Subject to the constraints,

$$\begin{cases} \Delta \mathbf{u}_{\min} \leq \Delta \mathbf{u}(t) \leq \Delta \mathbf{u}_{\max} \\ \mathbf{u}_{\min} \leq \mathbf{u}(t) \leq \mathbf{u}_{\max} \end{cases}$$

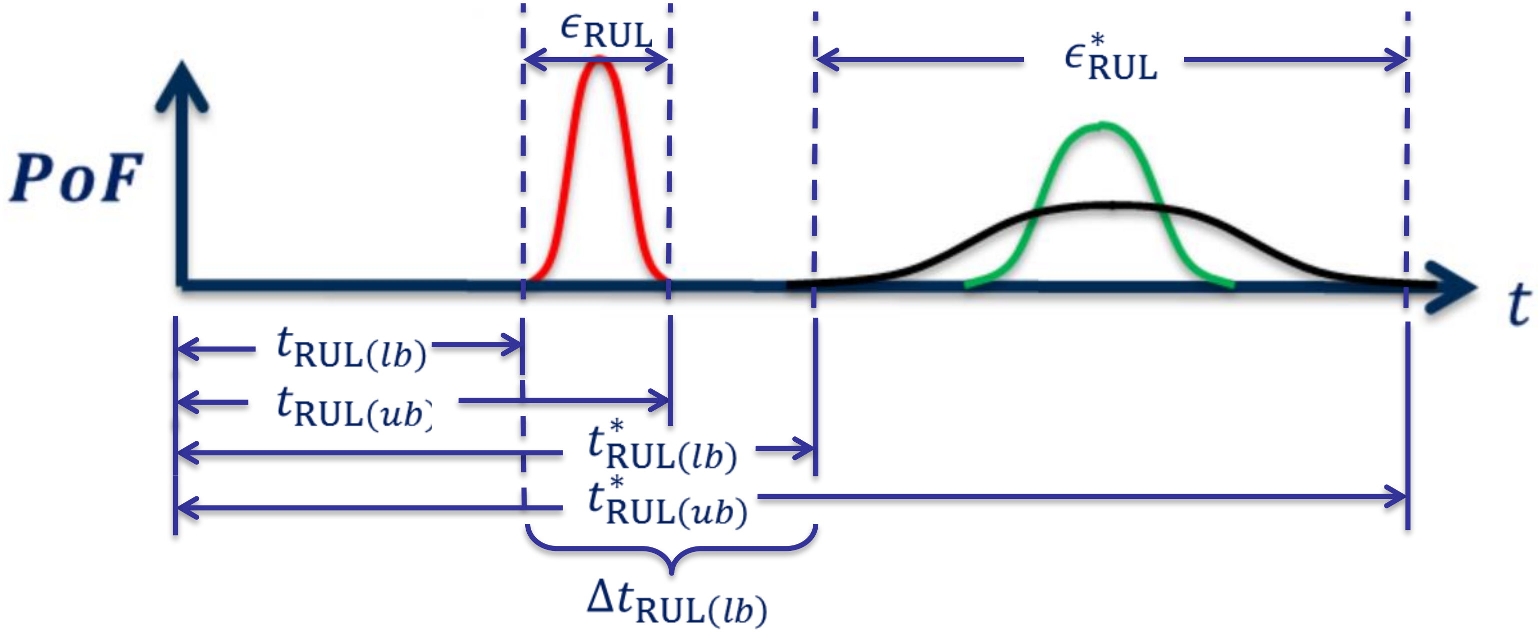
Stability and Uncertainty Analysis

<u>Composite system</u> – Plant coupled with MPC controller



Stability and Uncertainty Analysis

Measurements



Definition (RUL Gain)

The resulting RUL gained after reconfiguration,

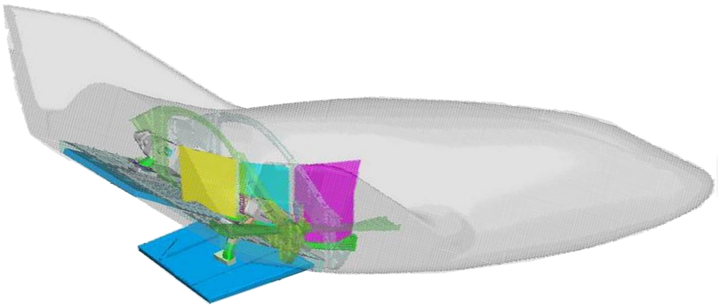
$$\Delta t_{\text{RUL}(lb)} \triangleq t^{\star}_{\text{RUL}(lb)} - t_{\text{RUL}(lb)}$$

Definition (Confidence Interval)

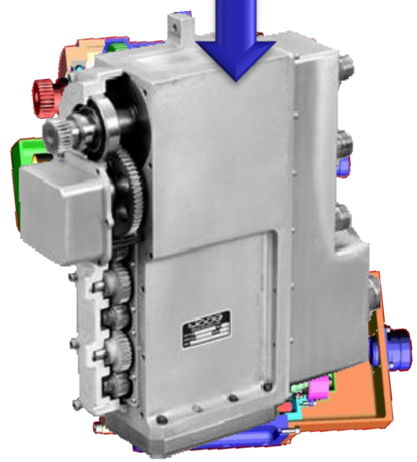
The confidence interval width of the reconfigured RUL,

$$\epsilon^{*}_{\text{RUL}} \triangleq t^{\star}_{\text{RUL}(ub)} - t^{\star}_{\text{RUL}(lb)}$$

Example Application
Electro-Mechanical Actuator



System
X38 Crew Re-entry Vehicle



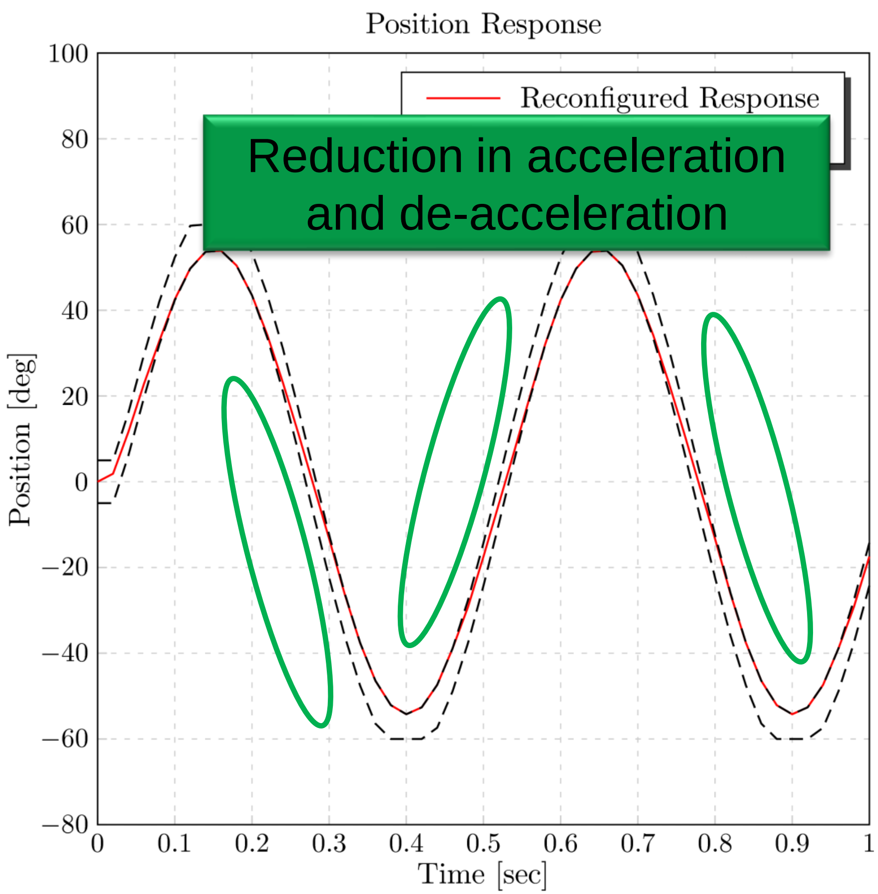
Sub-System
Electro-Mechanical Actuator (EMA)

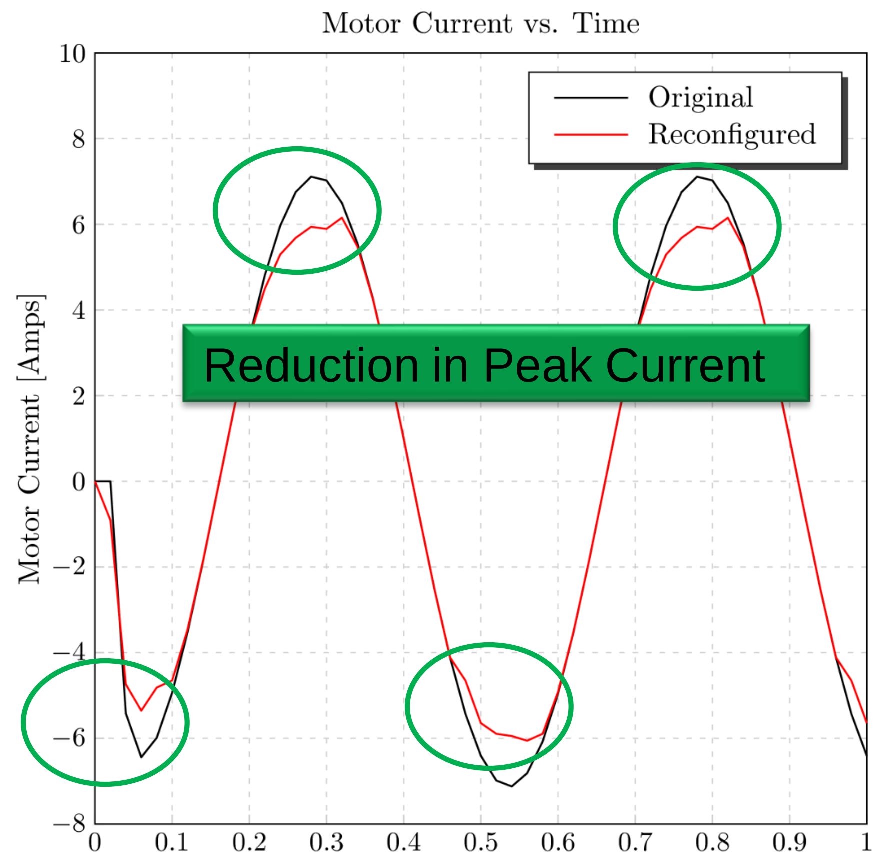
Fault Mode
Winding Insulation

Component
Brushless DC Motor

Example Application
Reconfiguration Feasibility

- Consider worst case: $\rho \gg 1$, $\mathbf{Q} = \text{diag}([1\ 0\ 0\ 0\ 0])$ and $\mathbf{R} = 1$.
- Deterministic with no external load ($\mathbf{v} \equiv \mathbf{0}$).
- Simulated case: $p = 5$ and $\eta = 0.19$ (implies feasibility)

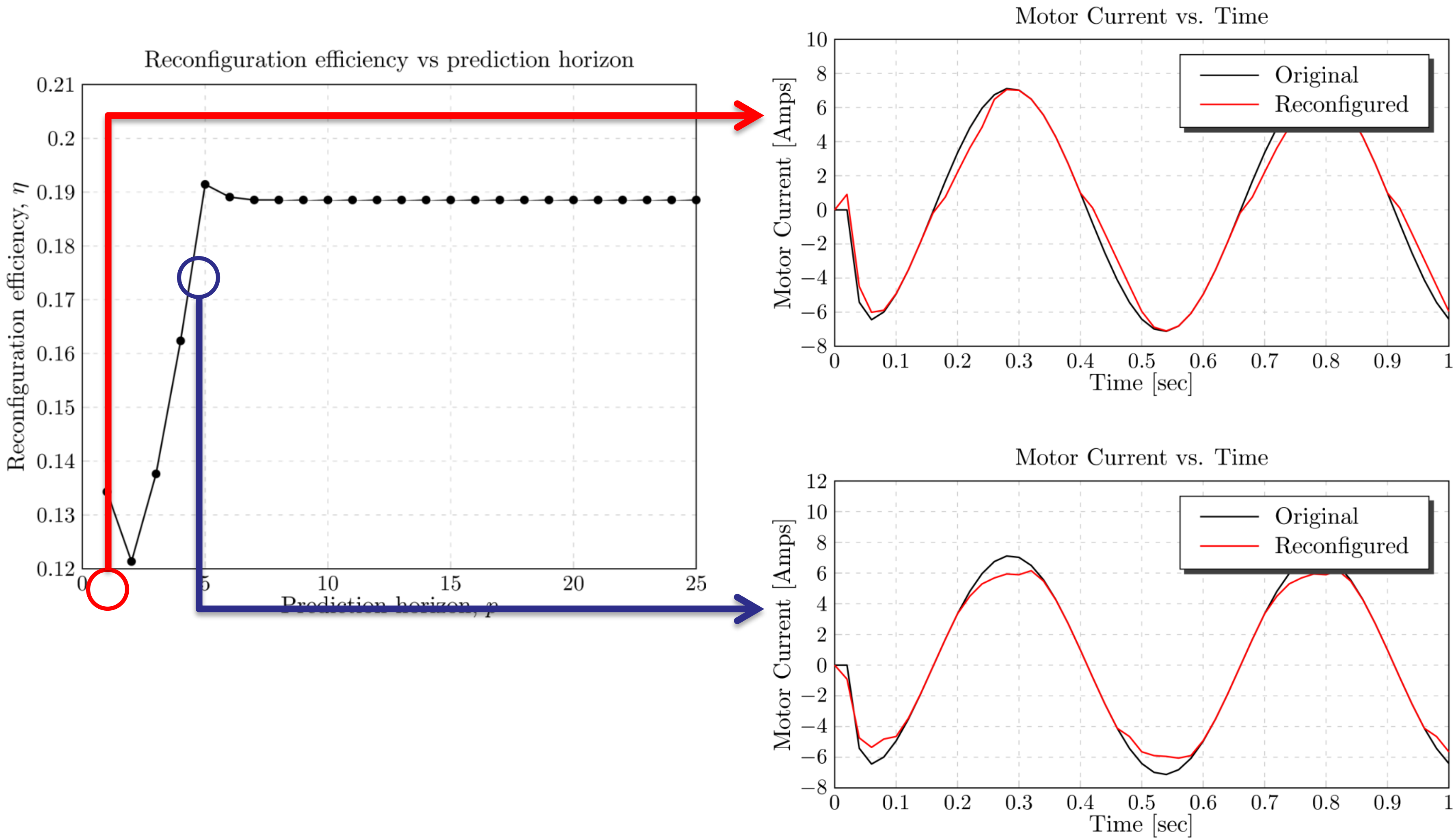




Example Application

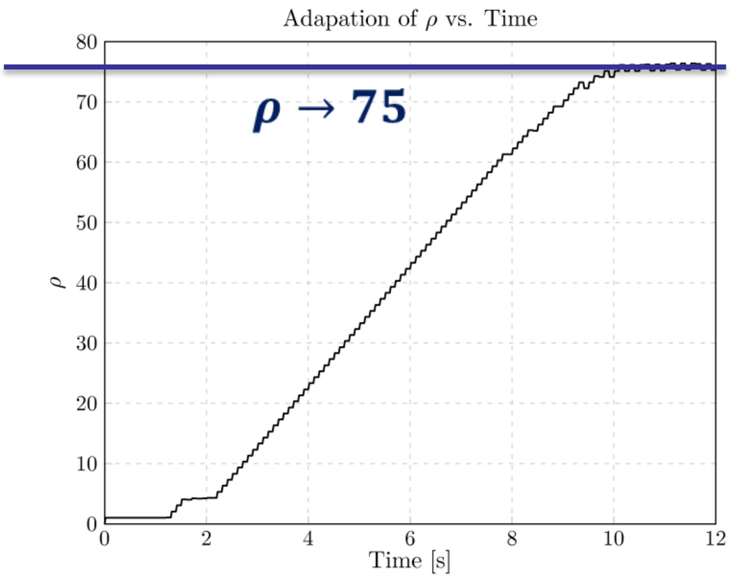
Prognostic Horizon

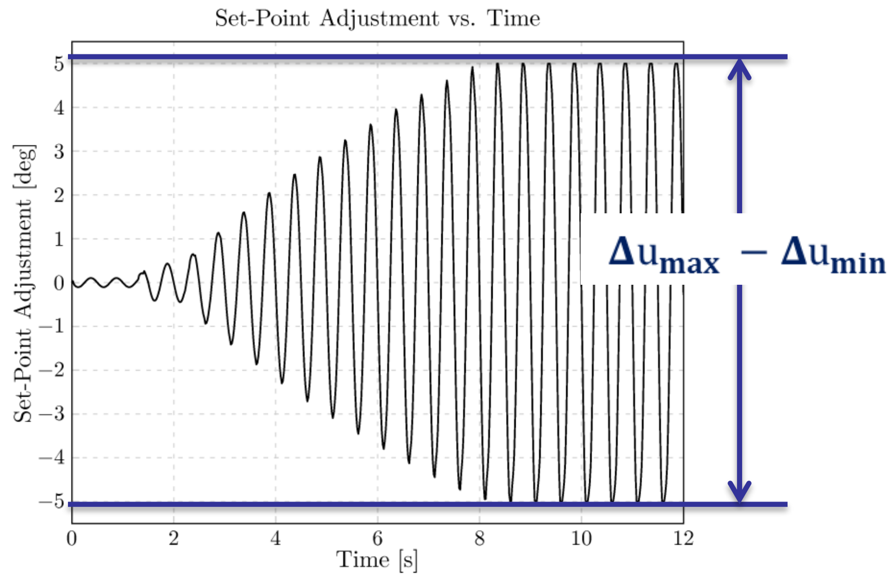
- Reconfiguration for different horizons, p.

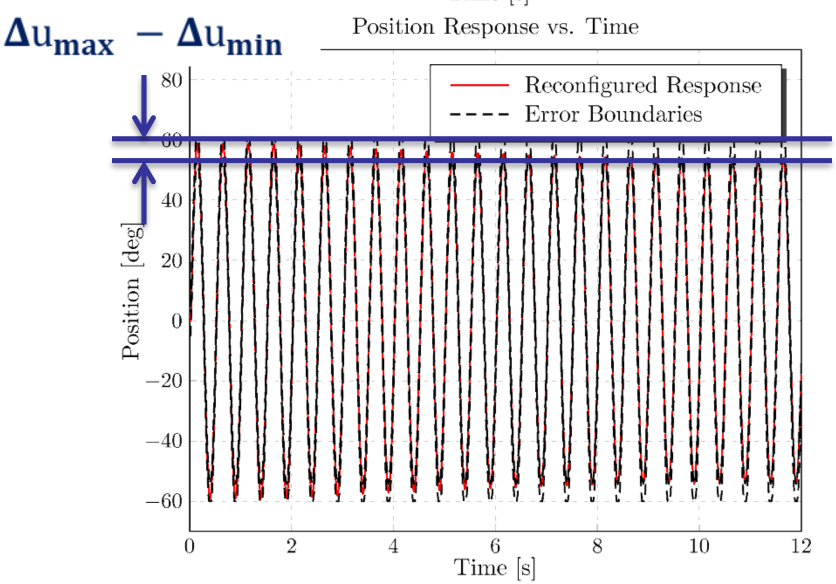


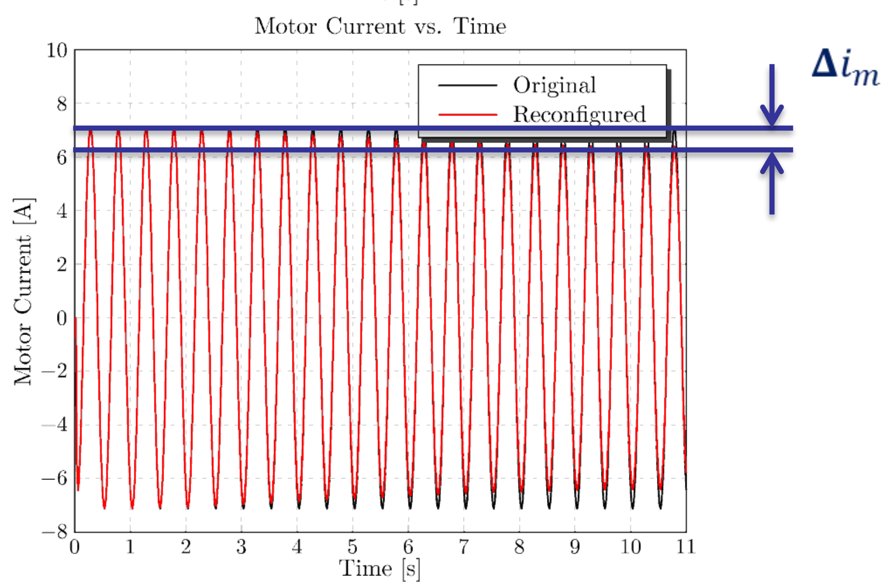
Example Application

Adaptation Parameter Dependence (Example)



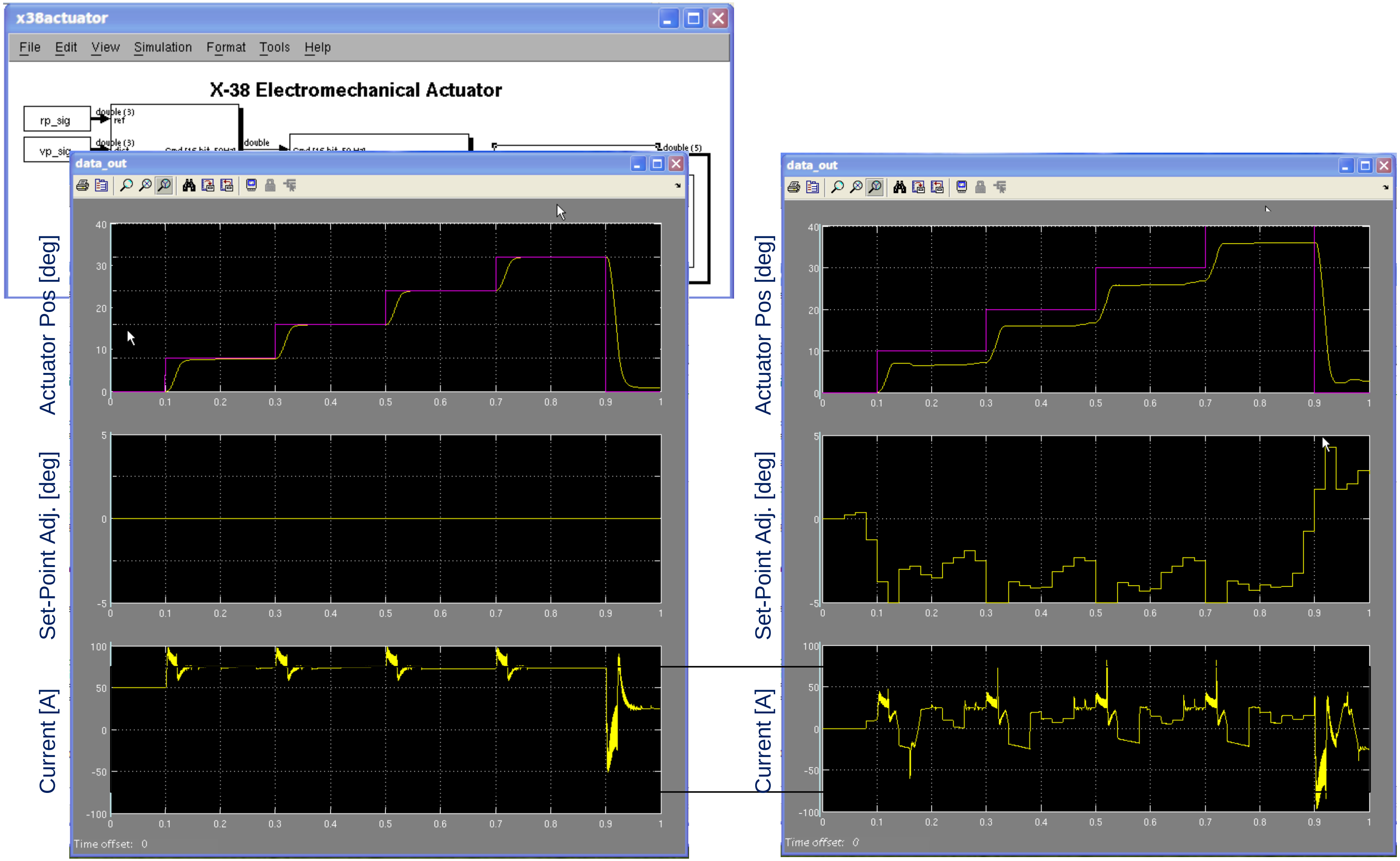






Example Application

Non-Linear System / Demonstrate Feasibility



Tech Transfer Issues

- Generic Aspects of the Technology
- Possible Candidate Platforms: UGVs, UAVs, UUVs, other Unmanned Systems
- Advanced Aircraft and Spacecraft
- Complex Industrial Processes

Potential Benefits

- Design and Development of High Confidence Systems
- Reduced Operator Workload
- Improved Safety and Reliability
- Reduced Maintenance Costs
- Other

Where do we go from here?

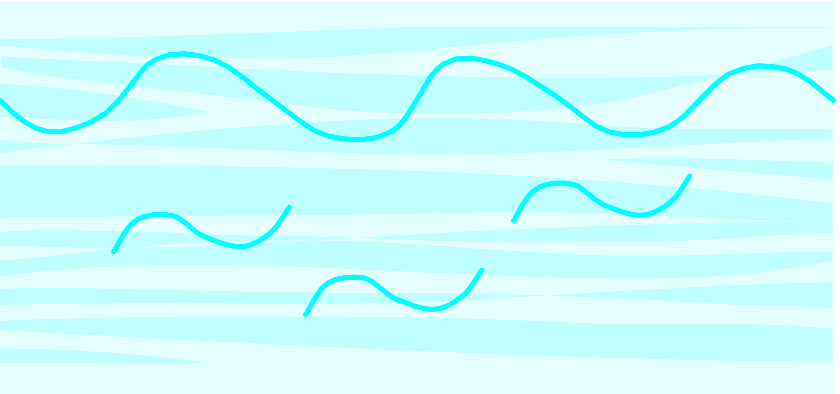
- Improved coupling between design and control
- The human-system interface
- Testing and evaluation
- The uncertainty issue
- Probabilistic design methods

The Problem


Drive System


Source: Sahrmann (2004)
5 in


Source: Sahrmann (2004)

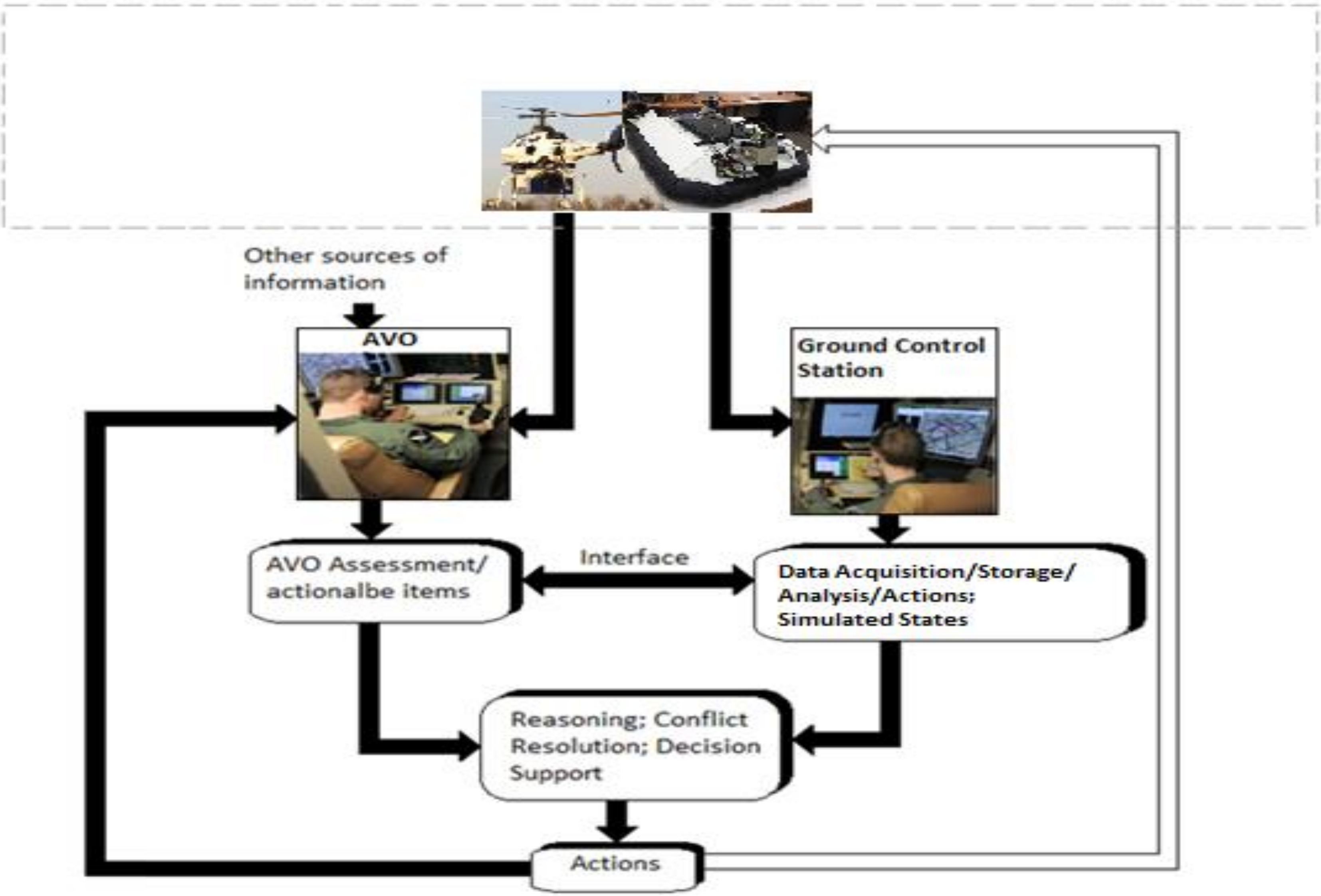


The Human-Machine Interface

MQ-9 Reaper AVOs

AVO: “he’s been more overcome by the torrent of information pouring in during a drone flight than he was in the cockpit”

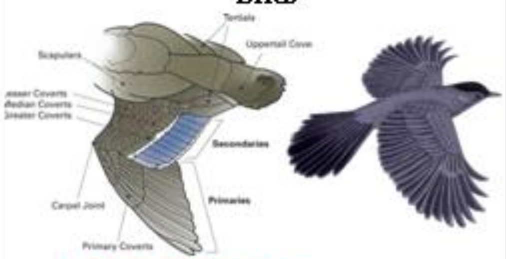
The Human-Machine Interface



Georgia Tech: Autonomous Systems Developments

Micro Air Vehicle Concept

BIRD



A. ***Complex co-ordination***: Many muscles
B. ***Larger wing-span*** for long flight times
C. ***Not recommended*** for closed-quarter flight

HUMMINGBIRD

A. ***Good Contender*** for a design
B. ***Not power efficient and short flight time***
C. ***Complex Wing mechanisms*** implementation

BUTTERFLY

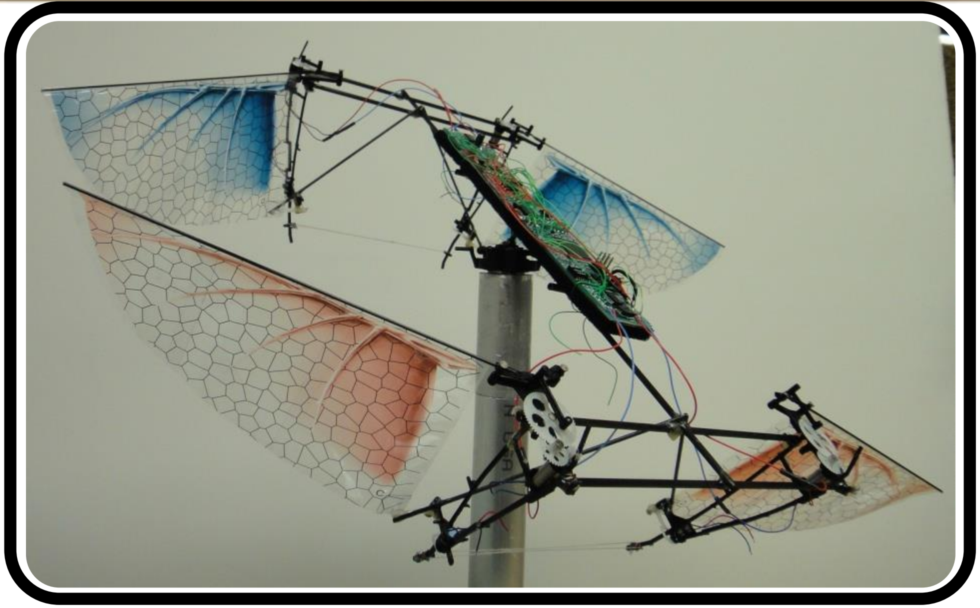
A. ***Excellent contender*** for a MAV
B. **Long flight times**
C. ***Slow dynamics***, *low agility*
D. ***Low controllability***

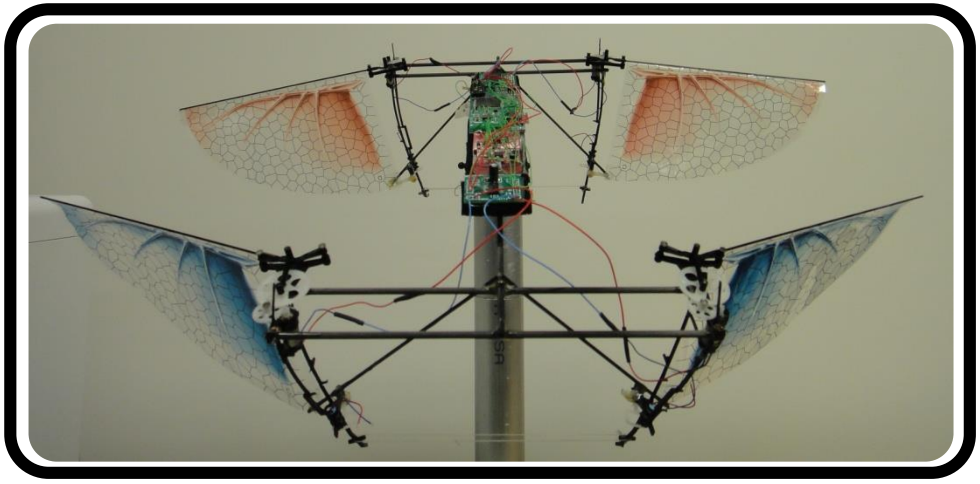
DRAGONFLY – THE DESIGN CHOICE

A. Four sets of wings provide ***maximum Lifting power***
B. The Wings resonate synchronously, sustaining ***super-long flight times***
C. Four wings give it unparalleled ***agility and maneuverability***

D. Only ***one actuator per wing***
E. ***Simpler controls***
F. ***Relatively less complex*** parts - tolerance to damage

QV: Quad Wing Design



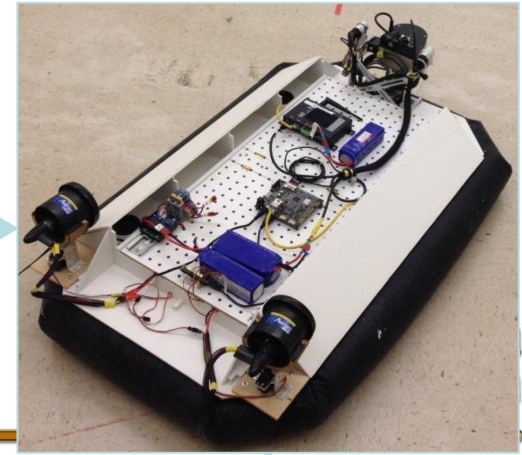


Control System

Control Laws:
*LQR
*Dynamic Inversion
*Adaptive
*Backstepping

Actuator (Motor) Command

Plant



Navigation System

Sensors:
*LIDAR
*IMU
*Camera

Measuring
Estimating
Filtering

Position
Velocity
Acceleration

Guidance System

Mission:
*Trajectory Tracking
*Path Following (Waypoints following)
*Stabilization

Guidance Command
Guidance Law

Tech Transfer Issues

- Generic Aspects of the Technology
- Possible Candidate Platforms: UGVs, UAVs, UUVs, other Unmanned Systems
- Advanced Aircraft and Spacecraft
- Complex Industrial Processes

Where do we go from here?

- Improved coupling between design, health management and fault-tolerant control
- The human-system interface
- The uncertainty issue
- Probabilistic design methods

Design and Development of High Confidence Systems