# CPS: Embedded Fault Detection for Low-Cost, Safety-Critical Systems

Gary Balas, Jaideep Srivastava, Mats Heimdahl, Antonia Zhai, and Peter Seiler

University of Minnesota

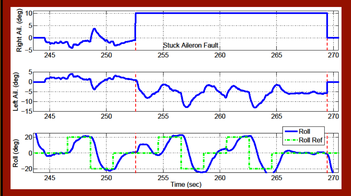
## Model-based Fault Detection

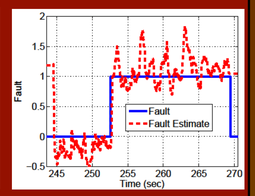
Synthesis of optimal, robust $H_\infty$ filters using convex optimization.

Ref: P. Seiler, B. Vanek, J. Bokor, and G. Balas, Robust $H_\infty$ filter design using frequency gridding, American Control Conference, 2011.

### UAV flight tests of model-based FDI

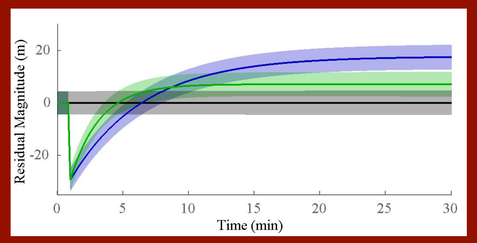
Ref: R. Pandita. Dynamic Flight Envelope Assessment with Flight Safety Applications. PhD thesis,University of Minnesota, 2010.




### Analysis of safety critical FDI

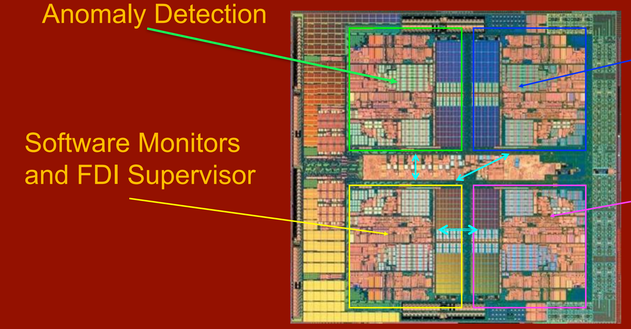
Ref: T.J. Wheeler, P. Seiler, A. K. Packard, and G.J. Balas, Performance analysis of fault detection systems, American Control Conference, 2011.

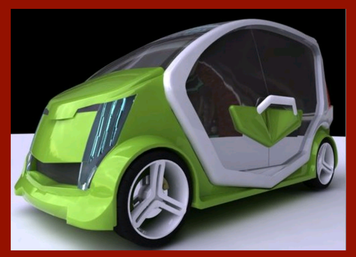


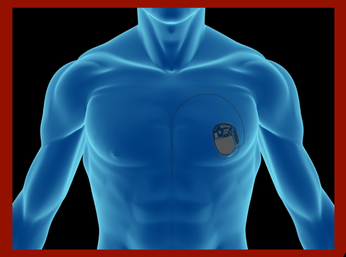

## Overview

Issue: Current safety critical systems rely mainly on physical redundancy but this increases system size, complexity and power consumption.

Objective: Develop algorithms and computing architectures that enable fault detection without relying on physical redundancy.



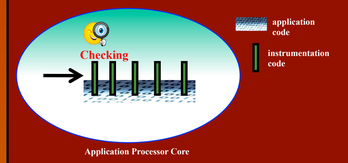





## Monitoring Software Execution HW and SW Support

**The Problem:**

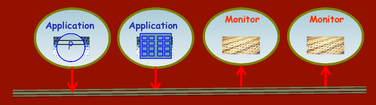
**Single-Core Program Monitor: Instrumentation-based**




**Performance overhead too high**

**The Solution:**

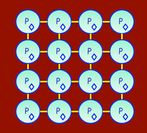
**Monitor software correctness with monitors executing on different cores than applications**



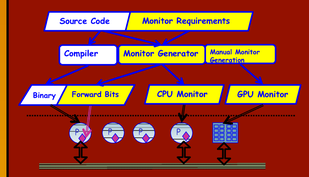

**Communications overhead could be significant**

**Fundamental Aspects of Efficient Multi-core Based Program Monitor**

- **Accelerate Information Extraction**
  - No instrumentation to the monitored code
  - Use generic hardware support Ex-Mon
- **Reduce Communication**
  - Reduce stress on the communication queue
  - Distill-based monitor generated by compiler support
- **Automatic Parallelization of Monitoring Tasks**
  - Distribute monitoring task on many cores or GPGPUs



**Current Compiler Infrastructure**




**Summary of Monitor Research**

| | On-Chip CPU | On-Chip GPU |
|---|---|---|
| Memory Bug Detection | ✔ | ✔ |
| Taint Propagation | ✔ | ✔ |
| Data Race Detection | ✖ | ✔ |

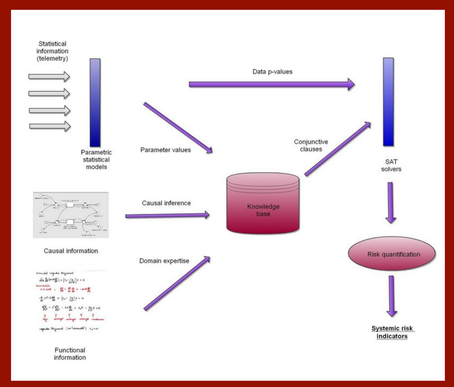
Challenges:
1. Communication bandwidth and latencies
2. Data dependences between consecutive events
3. Trade-off between accuracy and correctness
4. Recovery mechanisms

## Data Driven Anomaly Detection

Designed hybrid logic algorithm for detecting contextual anomalies in multivariate data from complex physical systems.

Method is complementary to model-based fault detection approaches. It also provides performance improvements for general anomaly detection in the form of intelligent dimensionality reduction.

**Hybrid-logic algorithm**

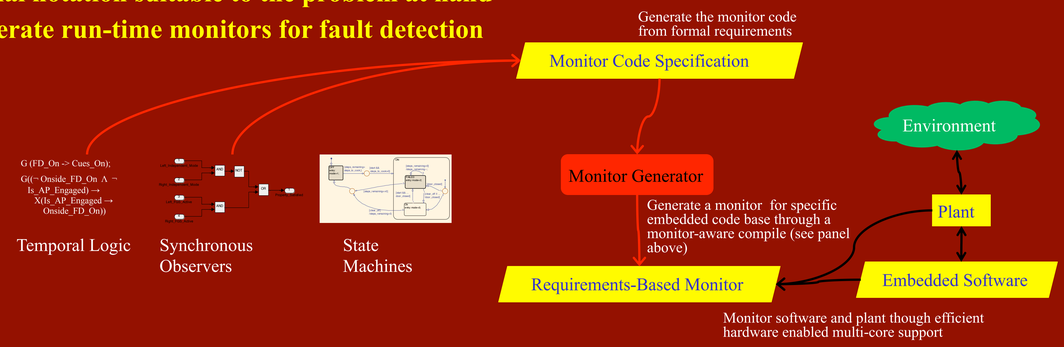



Ref: N. Srivastava and J. Srivastava. A hybrid-logic approach towards fault detection in complex cyber-physical systems, Proceedings of PHM, 2010 (to appear)

## Requirements-Based Fault Detection

- **Write system and software requirements in some formal notation suitable to the problem at hand**
- **Generate run-time monitors for fault detection**

**Auto Generate Run time Monitors for Multi Core Architecture**




Ref: G. He and A. Zhai, "Improving the Performance of Program Monitors with Compiler Support in Multi-Core Systems". Proc. The IEEE International Parallel & Distributed Processing Symposium (2010)"