Avionic Systems

Advanced Research Into Methodology for Design of Distributed Embedded Systems

ARTIST
Embedded Systems: Industrial Applications
Rome, Italy

Clas A. Jacobson
Chief Scientist, Controls, UTC
JacobsCA@utrc.utc.com

November 12, 2008

United Technologies

UTC Power

Carrier

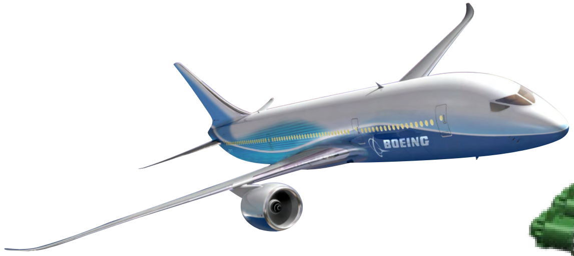
Pratt & Whitney

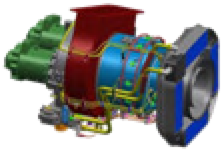
Building Systems

Aerospace Systems

Power Systems

Otis





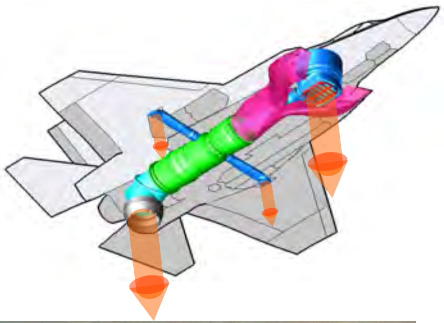
Hamilton Sundstrand

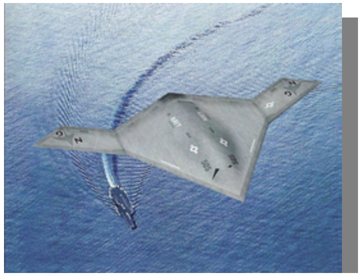
UTC Fire & Security

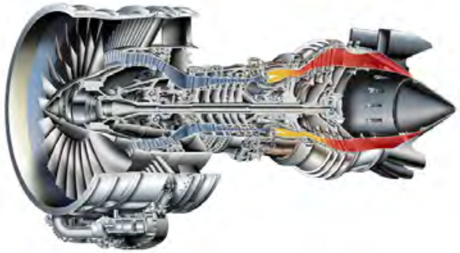
Pratt and Whitney Products

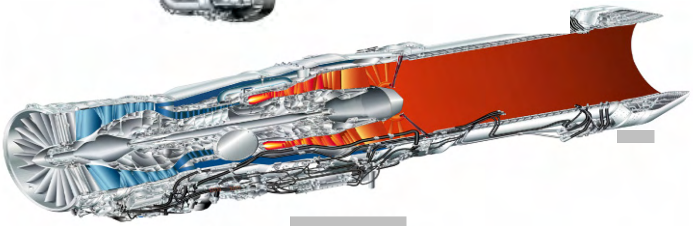
Pratt & Whitney
A United Technologies Company

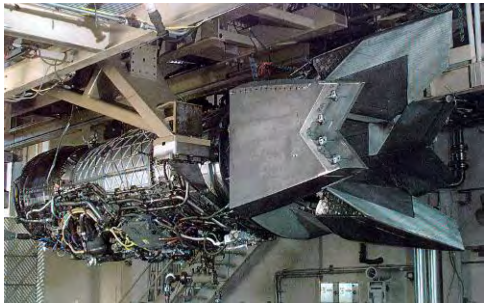
Military Engines

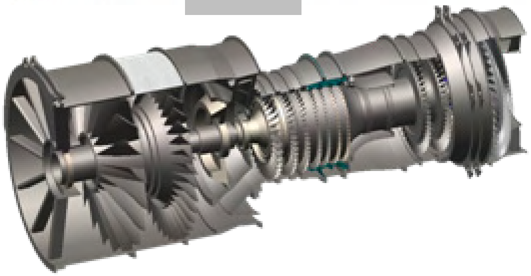








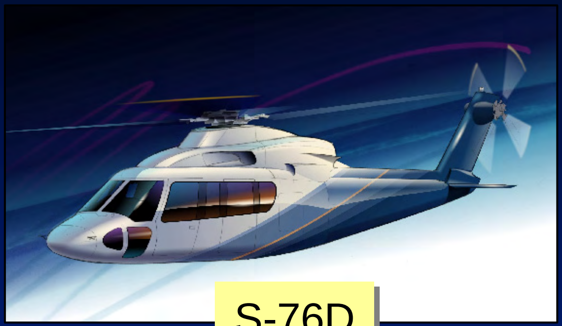




Commercial Engines

SIKORSKY PRODUCT LINE

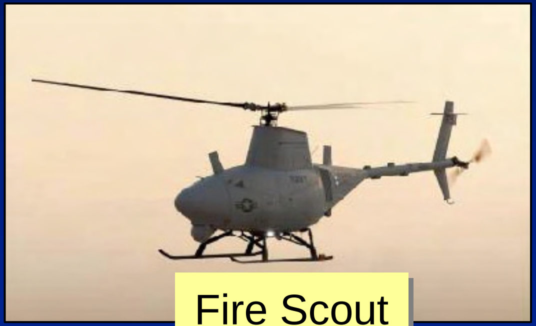

UH-60M


S-76D


CH-53K


MH-60R


S-92


Fire Scout

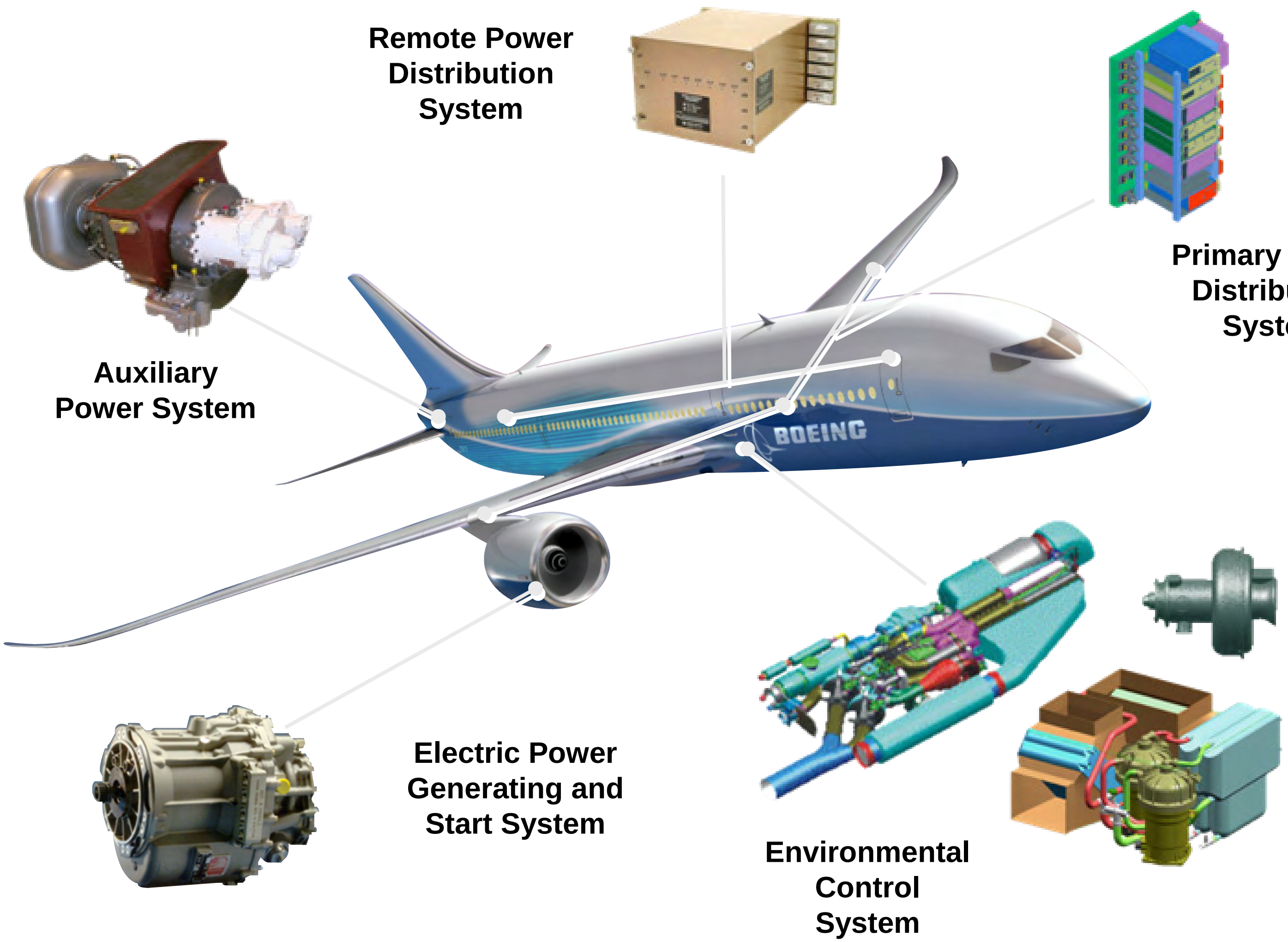

MH-60S


H-92


X2 Technology

Boeing 787: Hamilton Sundstrand

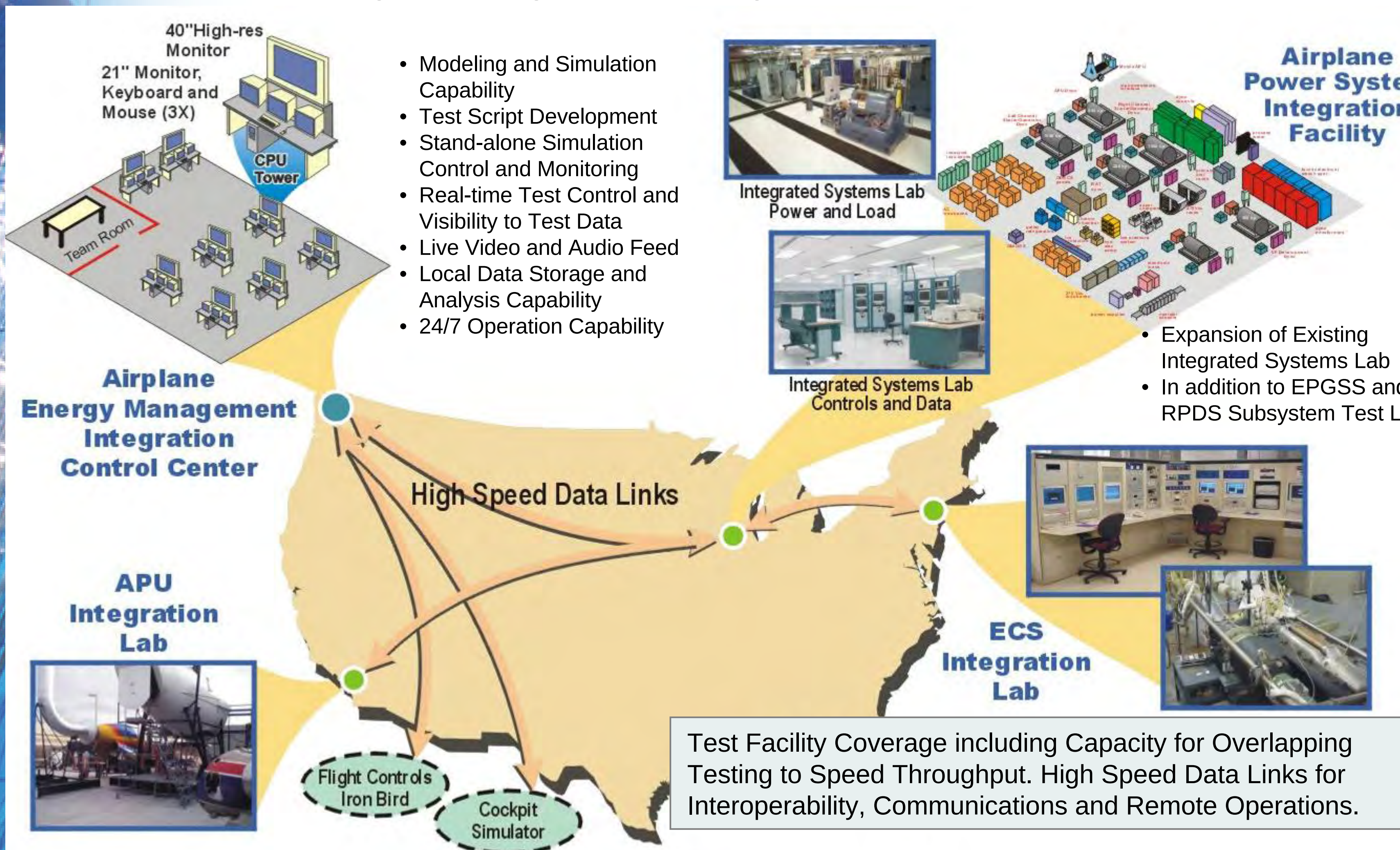
Complete Power, Fuel and Thermal Management Solutions



Benefit: Decreased weight, increased efficiency
Risk: Fragility, inadequacy of design processes

The Integration Environment

Airplane Energy Management Integration Environment (AEMIE)



- Modeling and Simulation Capability
- Test Script Development
- Stand-alone Simulation Control and Monitoring
- Real-time Test Control and Visibility to Test Data
- Live Video and Audio Feed
- Local Data Storage and Analysis Capability
- 24/7 Operation Capability

- Expansion of Existing Integrated Systems Lab
- In addition to EPGSS and RPDS Subsystem Test Labs

Test Facility Coverage including Capacity for Overlapping Testing to Speed Throughput. High Speed Data Links for Interoperability, Communications and Remote Operations.

DOD Issues in Integrated Systems: 2008

One area where the committee believes that new research would benefit DoD is the management of engineering risk in unprecedented large and ultra-scale systems. Such systems have engineering risks associated with early design commitments related to system functionality, non-functional attributes, and architecture. The research would focus on ways to mitigate these engineering risks at early stages of the process through new approaches to early validation, modeling, and architectural analysis.

ftware Research Needs and Priorities: A Letter Report

Preliminary Observations on DoD Software Research Needs and Priorities

A Letter Report

Committee on Advancing Software-Intensive Systems Producibility

ence and Telecommunications Board
ngineering and Physical Sciences

NATIONAL RESEARCH COUNCIL
OF THE NATIONAL ACADEMIES

THE NATIONAL ACADEMIES PRESS
Washington, D.C.
www.nap.edu

The third area, which is just as important as the first two, is the reduction of requirements-related risk in unprecedented systems without too great a sacrifice in systems capability. The challenge in this area has two parts. First, how can consequences of early commitments related to functional or nonfunctional requirements be understood at the earliest possible time during development? And, second, how can we make "requirements" more flexible over a greater portion of the system life cycle? The committee believes that the most useful research for DoD would look at ways to achieve early validation—for example, through modeling, protoptying, and simulation — and also look at how iterative development cycles can be supported more effectively and, from the standpoint of risk in program management, more safely.

The second area where DoD has leading demand and could benefit from technological advancement is software quality assurance for defense systems. Software assurance encompasses reliability, security, robustness, safety, and other quality-related attributes. Defense systems often include commercial off-the-shelf components and may involve global development—global sourcing is a reality for major commercial software products and, additionally, for commercial custom software and service provisioning. The needed research would focus on new ways for producers and consumers to create (and validate) a body of technical evidence to support specific claims in support of an overall judgment of fitness.

KEY POINTS

Defense control systems are increasing in complexity at a rate that is outpacing the current capabilities of design methodologies to address. *The issues of complexity are heterogeneity, scale and subsystem interactions;*

The elements of the control systems as communication, computation and the physical systems are increasingly integrated which leads to an inability to separate functional elements and flow down subsystem requirements. *This lack of capability to set requirements affects current programs in cost, schedule and performance;*

The lack of a rigorous, scalable design methodology that includes integration of communication and control is a barrier to meeting the requirements of future defense needs;

Enabling technology in the form of Platform-Based Design is being developed that introduces layers of abstractions to cope with the increase in complexity. *There are investable tools that address the issues in the design of defense systems to enable higher levels of functionality;*

INABILITY TO FLOW DOWN REQUIREMENTS IN INCREASINGLY COMPLEX SYSTEMS

Fly-by-Wire Systems

Black Hawk Experience

Exponential complexity increase: 10x computations, 100x communications, 4x thermal dissipation increase every 5 years

Compressed development schedules

Requirements to improve handling quality (to level 1), increase maintainability (64x), and reduce weight

Communication bandwidth, latency, control and reliability issues when moving from physical to fly-by-wire domain

Aircraft Power Systems

787 Experience

Verification of performance and safety of logic for 100k + fault conditions

Certification of closed loop control over networks of multiple types in an uncertain environment

Instabilities caused by interactions between components discovered in hardware tests

Multivariate optimization of competing requirements

- Weight, stability, thermal management, efficiency, reliability, …

Validation of requirements flow-down

DESIGN METHODOLOGY

Cannot meet required functionality: exponentially increasing requirements

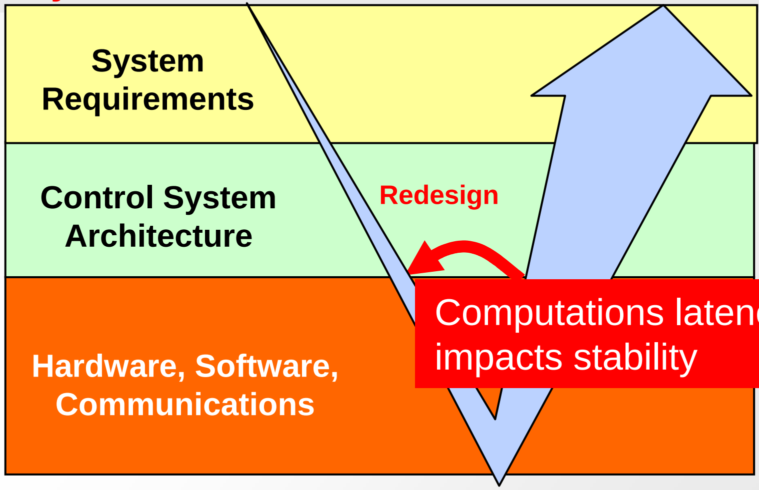
Complex, cyber-physical system with multiple overlapping time scales…

Today

Separated flight control, navigation, communications, diagnostics

Suboptimal use of computational resources

Computations and communications at maximum capacity



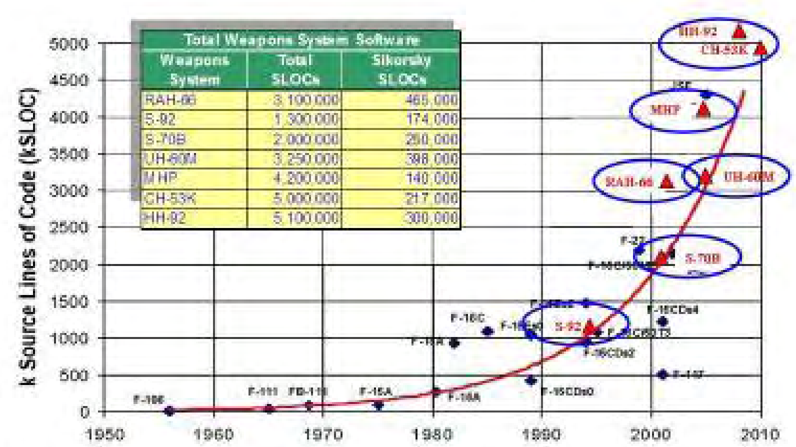
Future challenge…

Unmanned Flight

High resolution sensor data fusion

Advanced Control Algorithms

INCREASINGLY COMPLEX SYSTEMS DEVELOPED UNDER COST AND SCHEDULE CONTRAINTS



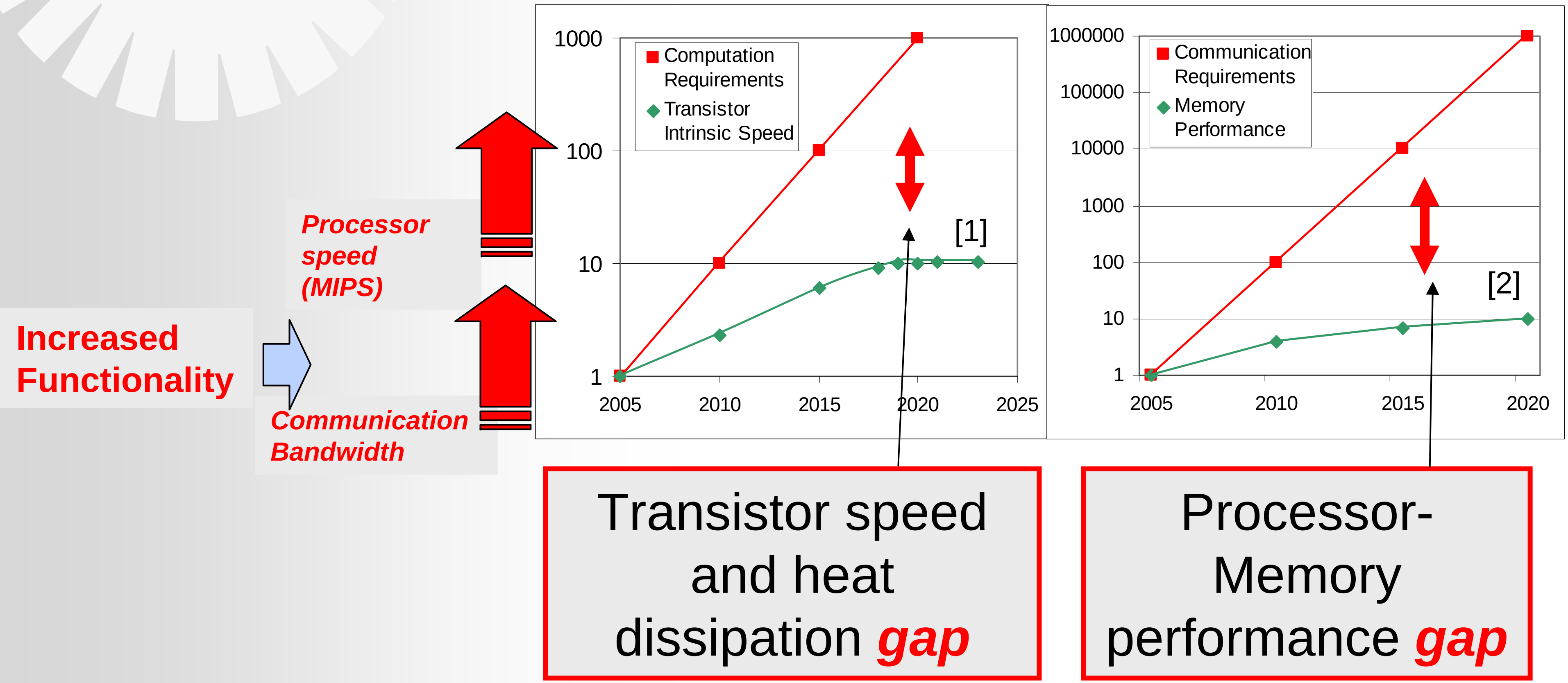
Total Weapons System Software		
Weapons System	Total SLOCs	Sikorsky SLOCs
RAH-66	3,100,000	465,000
S-92	1,300,000	174,000
S-70B	2,000,000	250,000
UH-60M	3,250,000	398,000
MHP	4,200,000	140,000
CH-53K	5,000,000	217,000
HH-92	5,100,000	300,000

- 100 Lines of Code per man-month
- Compressed schedules

TECHNOLOGY BARRIERS

Current design paradigm will not continue to work:

Increasing clock speed and communication bandwidth is no longer scalable

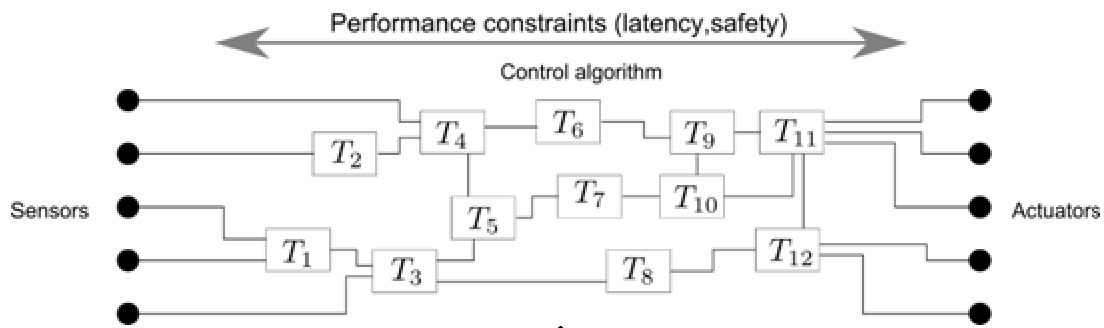


[1] International Technology Roadmap of Semiconductors, 2007

[2] David Patterson, Thomas Anderson et al., *A Case for Intelligent RAM : IRAM*

NEED OF AN ARCHITECTURAL CHANGE

Distributed Computation as Key Enabling Technology



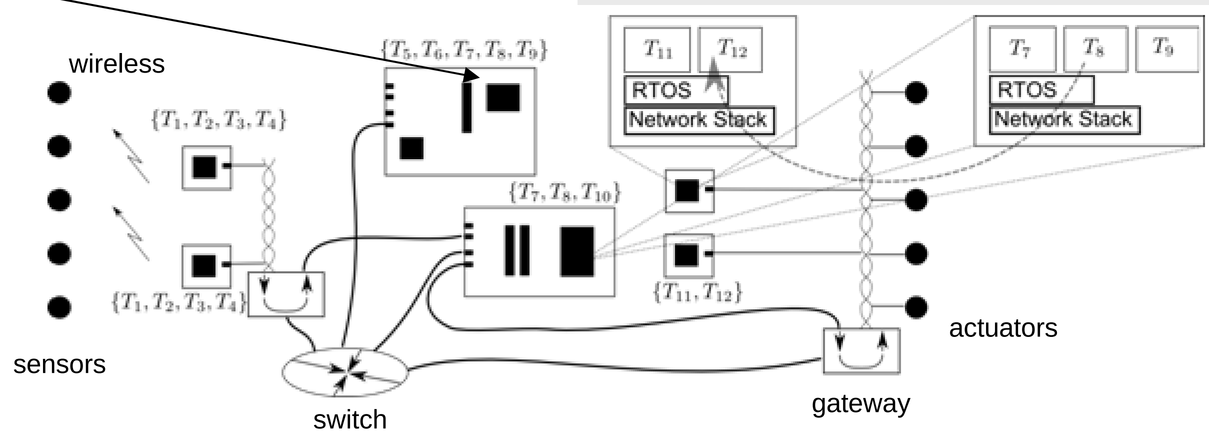
Exploit concurrency in the control algorithm

Q: How do we bridge the semantic gap?

A: Modeling & Optimization Tools (seed project)

Distribute I: Multi-core processors *provide computing power while containing heat dissipation*

Distribute II: Network architectures:
reduce bandwidth requirements by using local processing



NOVEL DESIGN METHODOLOGY

Meet-in-the-middle, synthesis driven, multiple abstraction layers

Key Elements

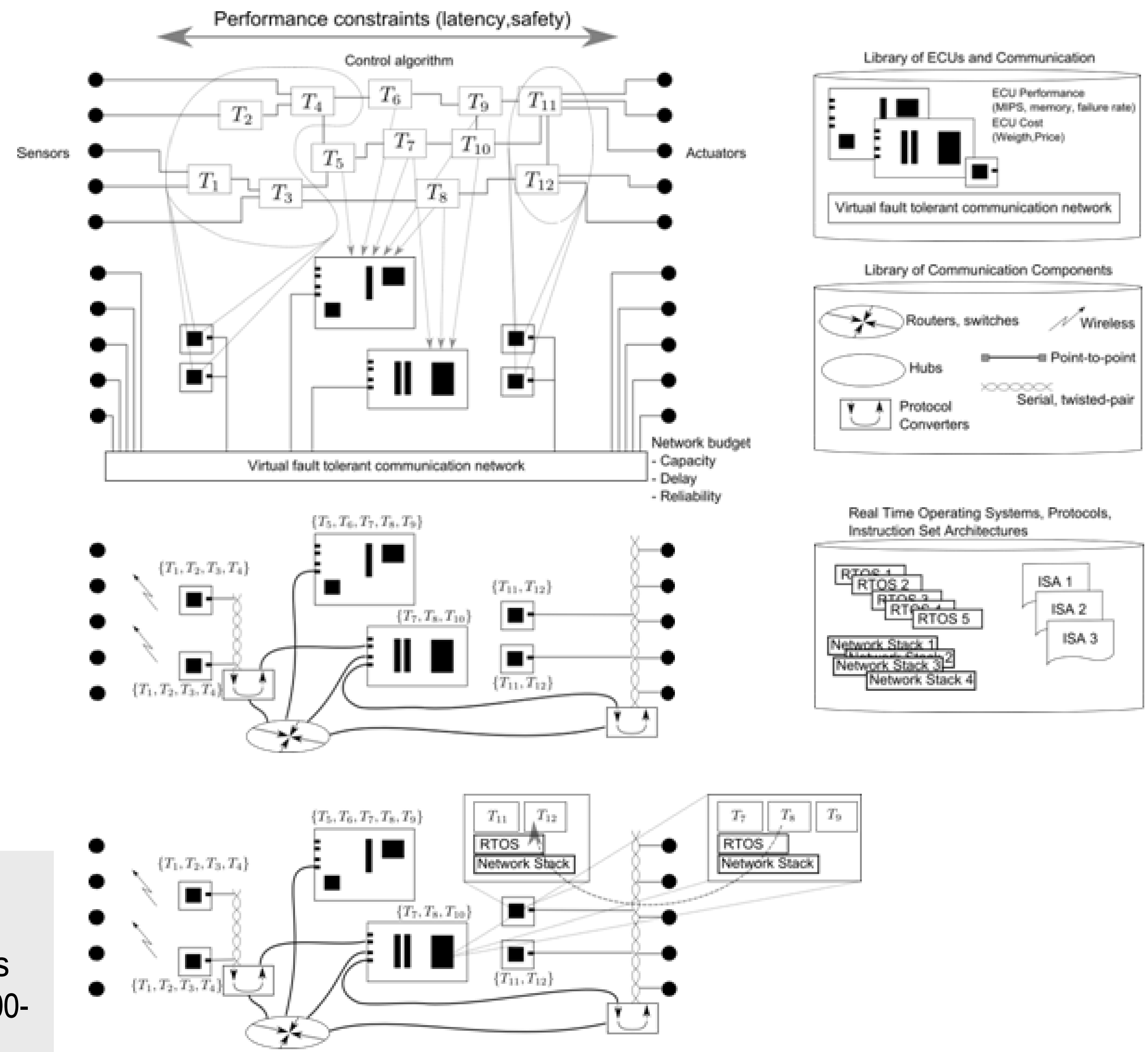
Design exploration of distributed architectures

Performance and safety driven mapping of tasks to distributed architecture

Automatic synthesis of fault tolerant communication networks

Software synthesis: Automatic generation of tasks and distributed RTOS

Project focuses on distributed implementation: extending the scope to designing concurrent control algorithms offers path to close gaps completely (100-1000X in latency/computational speed)

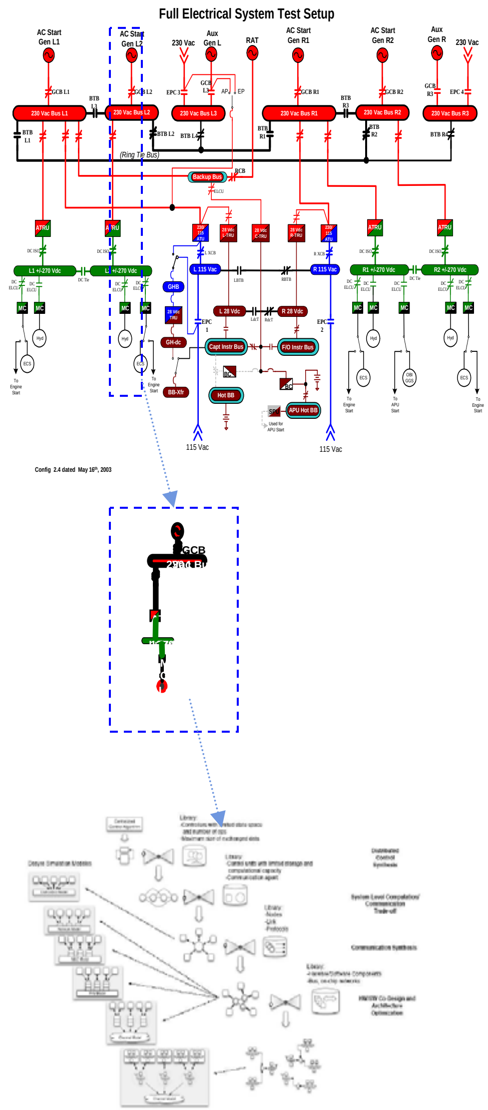


Electric Power – Current and Desired States

- Architecture selected by modification of prior design
- System stability verified in hardware test
- Control logic verified using hardware test

- Detailed dynamic models too slow for analysis
- Stability and Power Quality verified in hardware test
- Inefficient Uncertainty Quantification using Monte Carlo

- Software and communications verified by hardware test



Model that can take a set of requirements and flow them down to component level

- Optimal architecture from model-based exploration tool
- Robust stability guaranteed by analysis
- Control logic verified using models

- Accurate & fast models enable simulations and analysis
- Stability and Power Quality guaranteed by analysis
- Polynomial Chaos and QMC1000x faster than MC

- Automatic code generation and verification
- Correct by construction communications design