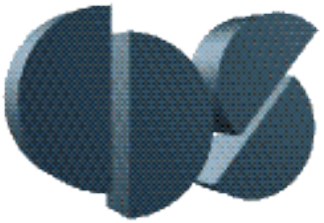
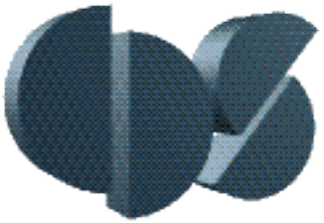



Agenda:

| | |
|---|---|
| 1:00 | Overview of the MuSyC Challenge Problem (Necmiye) |
| 1:15 | Review of Berkeley modeling and design-space exploration work (Pierluigi) |
| 1:40 | Review of Caltech correct-by-construction control synthesis work (Mumu) |
| 2:00 | Q&A |
| 2:30 | Next steps |
| 2:45 | Adjourn |

iCyPhy EPS Design Driver Telecon
4 February, 2013

# Aircraft Electric Power System Challenge Problem Overview

Necmiye Ozay, Caltech CDS

Joint work: John Finn, Quentin Maillet, Mostafiz Mozumdar, Richard Murray, Pierluigi Nuzzo, Robert Rogersten, Ufuk Topcu, Alberto S-Vincentelli, Mumu Xu (Caltech, Berkeley)

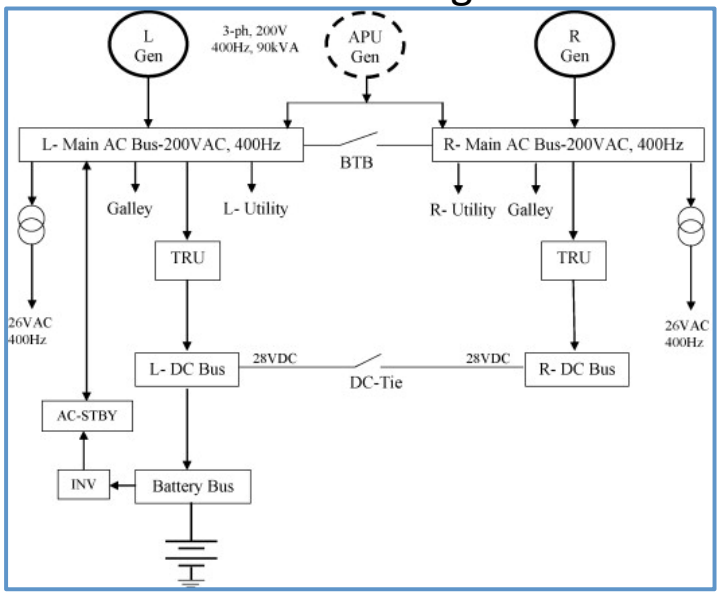
Thanks to: Rich Poisson of UTAS for feedback and discussions

iCyPhy EPS Design Driver Telecon
4 February, 2013

# Motivation

- Modern aircraft increasingly relies on electric power (traditionally, it was hydraulic, pneumatic, etc.)
- Complexity and safety-criticality of aircraft electric power systems (EPS) increased.

EPS for Boeing 767




Source: http://www.sciencedirect.com/science/article/pii/S0378779608002666

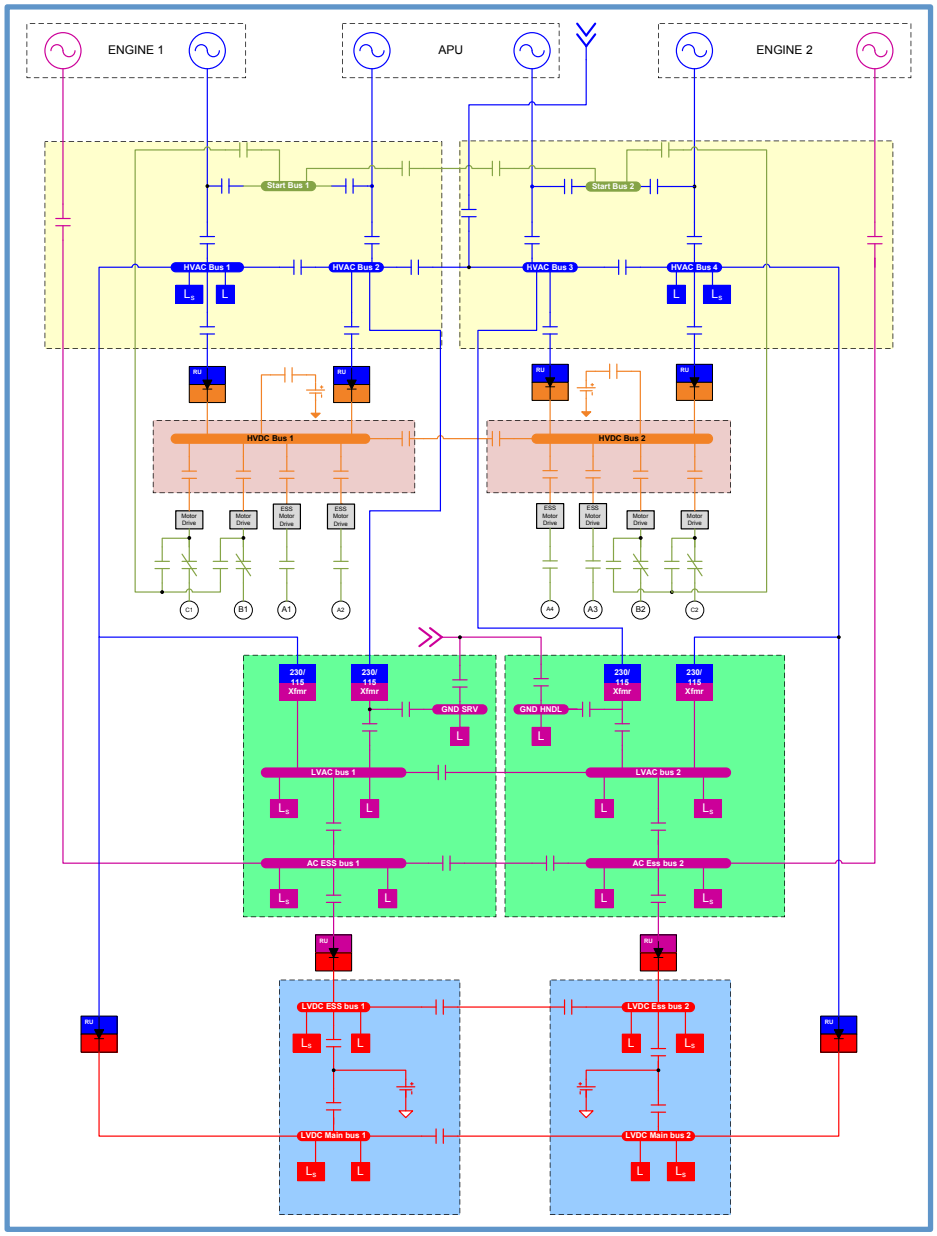



Figure courtesy of Rich Poisson, Hamilton-Sundstrand. Adapted from Honeywell Patent US 7,439,634 B2

# Motivation

- Aircraft EPS: a complex cyber-physical system
  - Large number of **heterogeneous** interacting components
  - Different failure modes
  - Sensing (for state estimation/ fault detection) and **embedded reactive controllers** (for accommodating faults)
- Want to design the topology and sensing-control protocols for it with **safety**, **reliability** and **performance** guarantees!

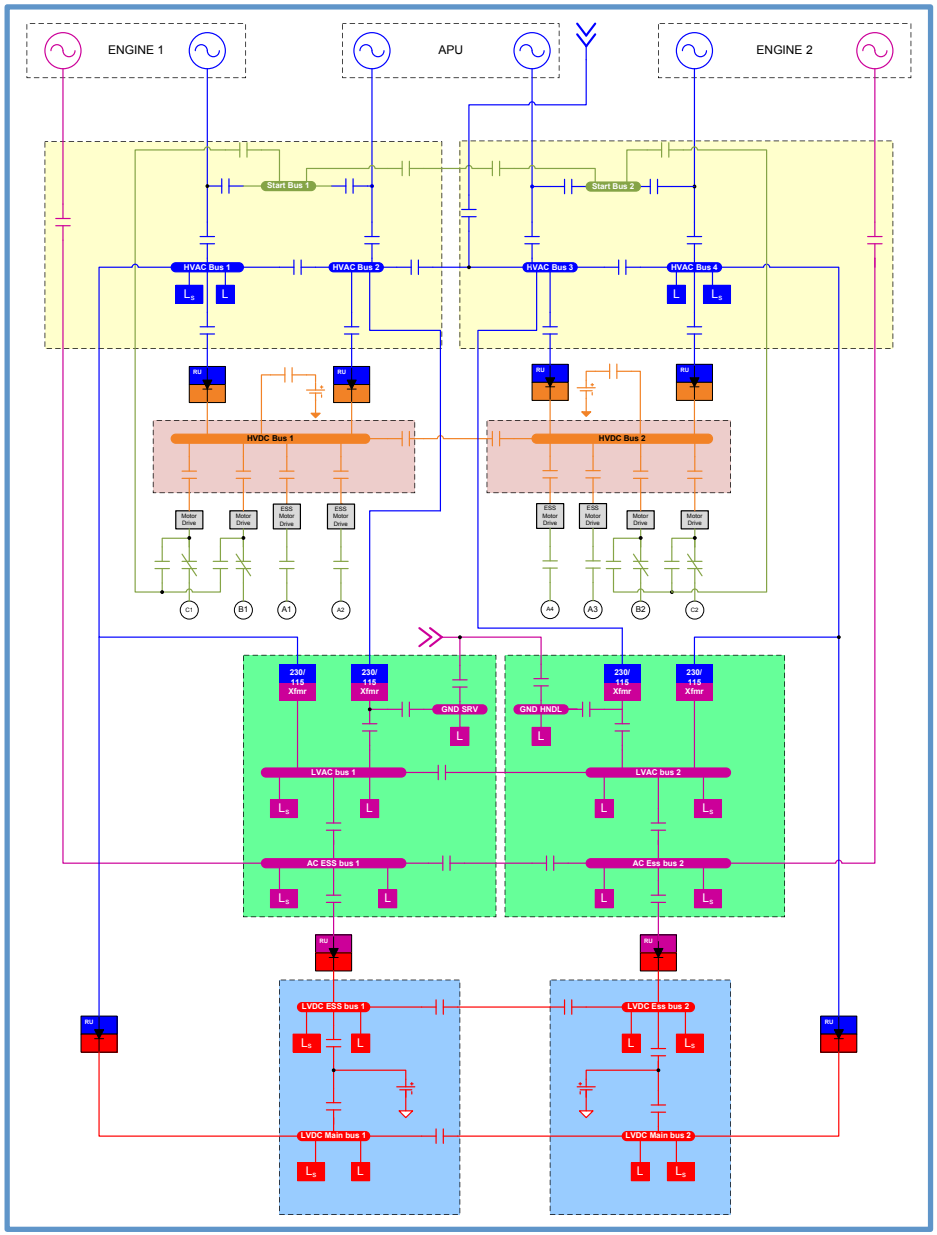



Figure courtesy of Rich Poisson, Hamilton-Sundstrand. Adapted from Honeywell Patent US 7,439,634 B2

# System Components

Single line diagram (SLD) or topology includes:

- Generators
- APUs
- External Power
- Batteries
- Loads
- Buses
  - Essential
  - Non-essential
- Contactors
- Transformers
- Rectifier Units
- Motor Drives

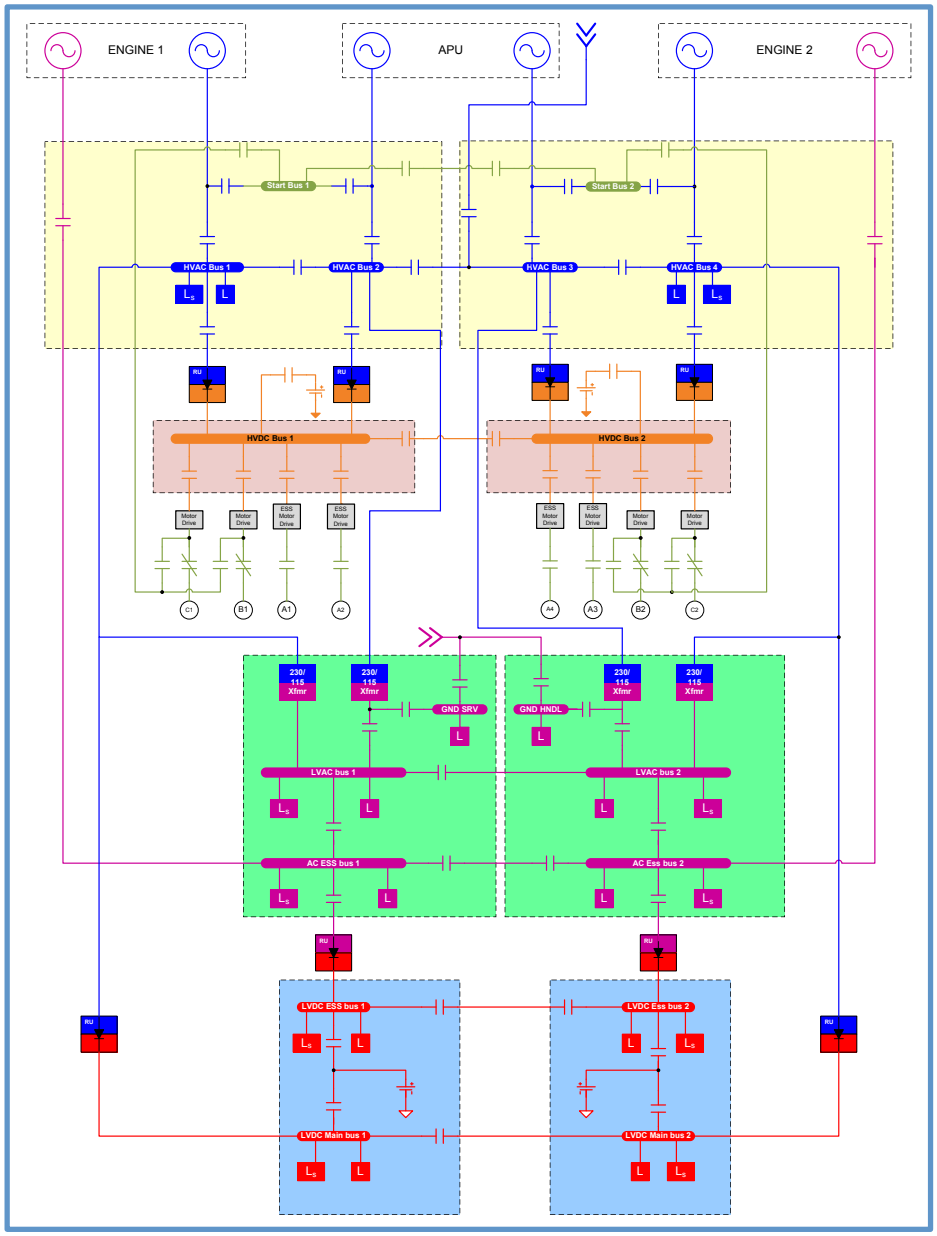
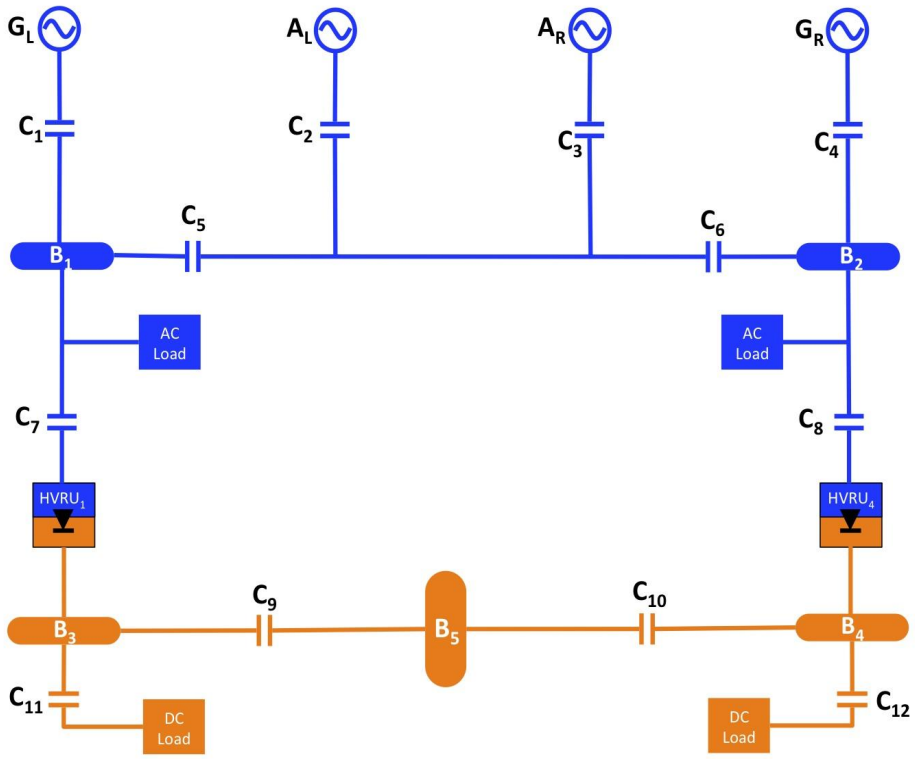



Figure courtesy of Rich Poisson, Hamilton-Sundstrand. Adapted from Honeywell Patent US 7,439,634 B2

# Overall Design Flow

- Given text based specifications:
  - Formalize requirements and associate them with system entities (e.g. components)
  - Find a ``feasible" topology (design-space exploration, topology synthesis)
  - Given the topology and specifications, **synthesize control protocol** with correctness guarantees
  - Export the controller to high fidelity models for simulation and further tests
  - Implement on hardware

# Simplified Challenge Problem




**REQUIREMENTS:**

1. No AC bus shall be simultaneously powered by more than one AC source.
2. The aircraft electric power system shall provide power with the following characteristics: 115 +/- 5 V (amplitude) and 400 Hz (frequency) for AC loads and 28 +/-2V for DC loads.
3. Buses shall be powered according to the priority tables.
4. AC buses shall not be unpowered for more than 50ms.
5. The overall system failure probability must be less than $10^{-9}$ per flight hour.
6. Never lose more than one bus for any single failure.
7. Total load must be within the capacity of the generator

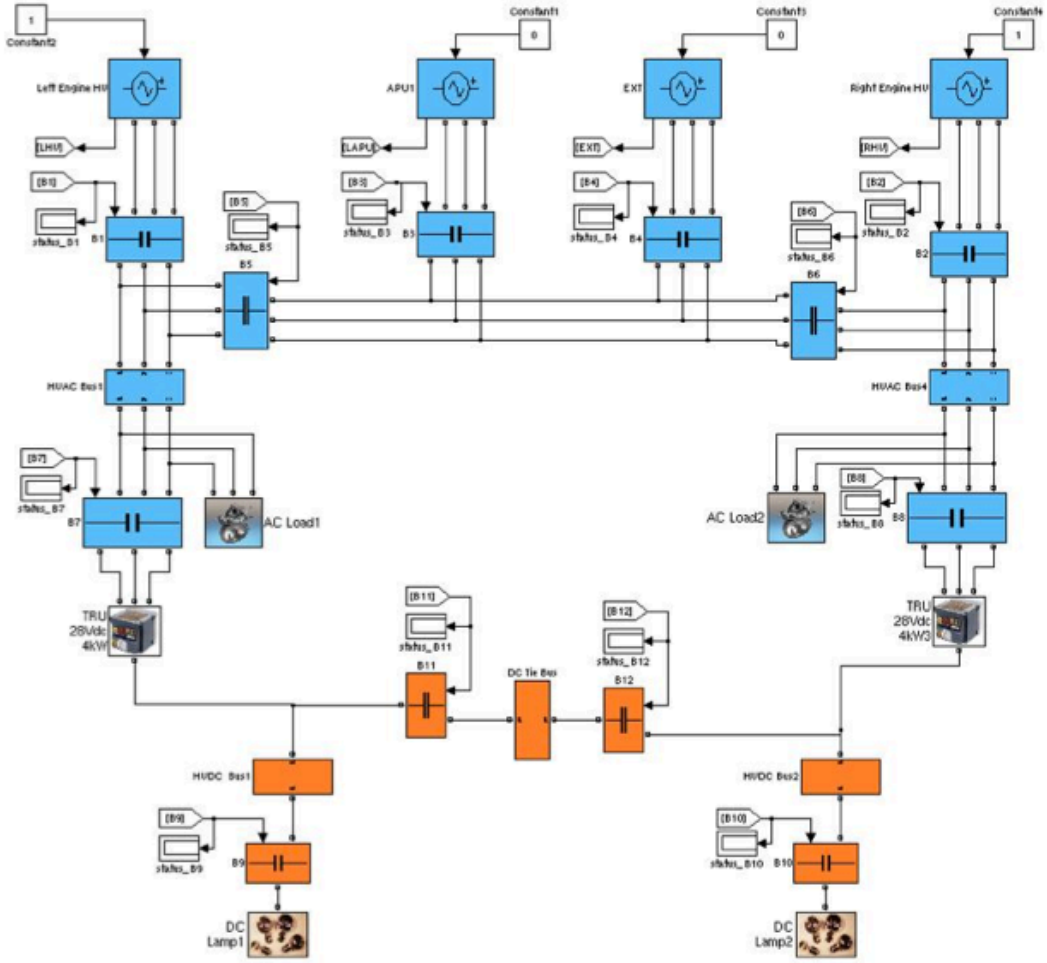
**Component models/specifications:**

1. Failure probabilities for contactors, generators, etc. (not much on failure modes)
2. Contactor closure times are between 15-25 ms and opening times are between 10-20 ms.

# System Components

Simulink model vs. full SLD:

- **Generators**
- APUs
- External Power
- Batteries
- **Loads**
- Buses
  - Essential
  - Non-essential
- **Contactors**
- Transformers
- **Rectifier Units**
- **Motor Drives**



# Goals (partly) achieved so far

- Demonstrated:
  - **requirement capture** (SySML, contracts, LTL)
  - **design space exploration** (topology synthesis based on reliability requirements)
  - **correct-by-construction control synthesis** (formalize the EPS control problem as a reactive synthesis problem and synthesize control logic),
  - **usability** (domain specific language for EPS control synthesis)
  - **integration with simulation tools** (import logic controller to simulink),
  - **CPS implementation** (hardware test-bed)

# Different Levels of Abstraction (Model Views)

| STATE \ TIME | untimed | discrete-time | continuous-time |
|---|---|---|---|
| discrete | | | |
| discrete & continuous | | | |

Fidelity increases -> Complexity increases

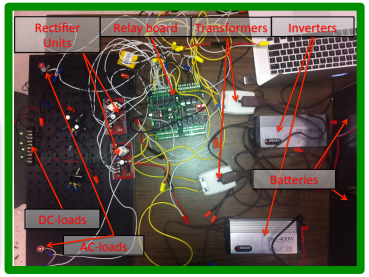
Actual System

Increase in complexity of models, verification and synthesis methods!

# Different Levels of Abstraction (Model Views)

| STATE \ TIME | untimed | discrete-time | continuous-time |
|---|---|---|---|
| discrete | synthesis (TuLiP) | | verification & synthesis (e.g. UPPAAL) |
| discrete & continuous | trivial abstractions | | simulation |

hardware test-bed




**Cyber-physical system**

- executable models in simulink
- simulation trace monitor (breach toolbox)