Reactive Synthesis for Aircraft Electric Power Systems

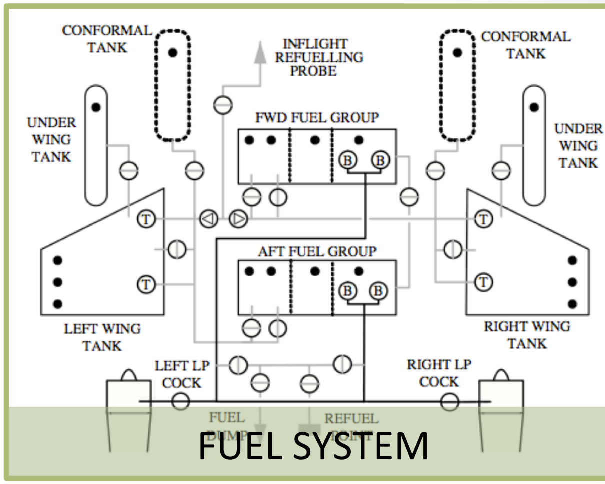
Mumu Xu
Ufuk Topcu, Richard M. Murray

August 1, 2012

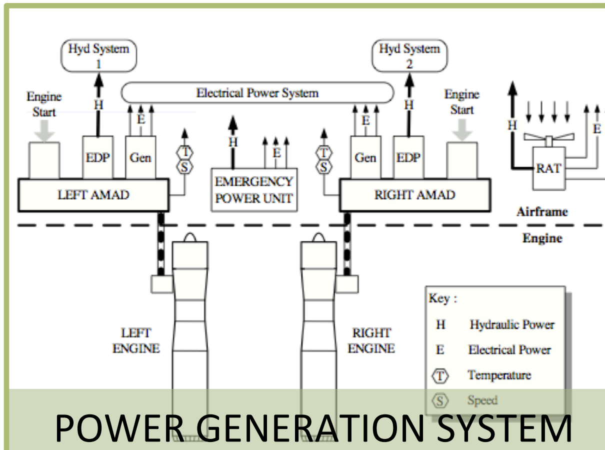
ENGINEERING RESILIENT SYSTEMS

Motivation

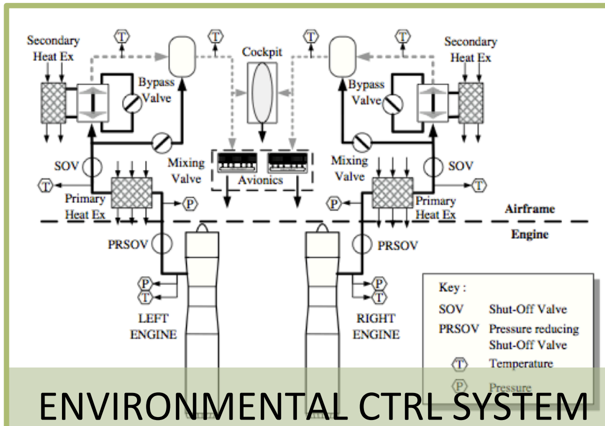
- Hydraulic, Pneumatic, Electric
- Fault-tolerant, reliable, autonomous
- Systematic methods for design based
  - formal specifications
  - verification and validation of complex systems
- Increasing complexity
  - VMS systems designed for verification
  - Need structure to allow verification tools to be applied
  - Synthesizing "correct-by-construction" design protocols



FUEL SYSTEM



POWER GENERATION SYSTEM



ENVIRONMENTAL CTRL SYSTEM

Electric Power System

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

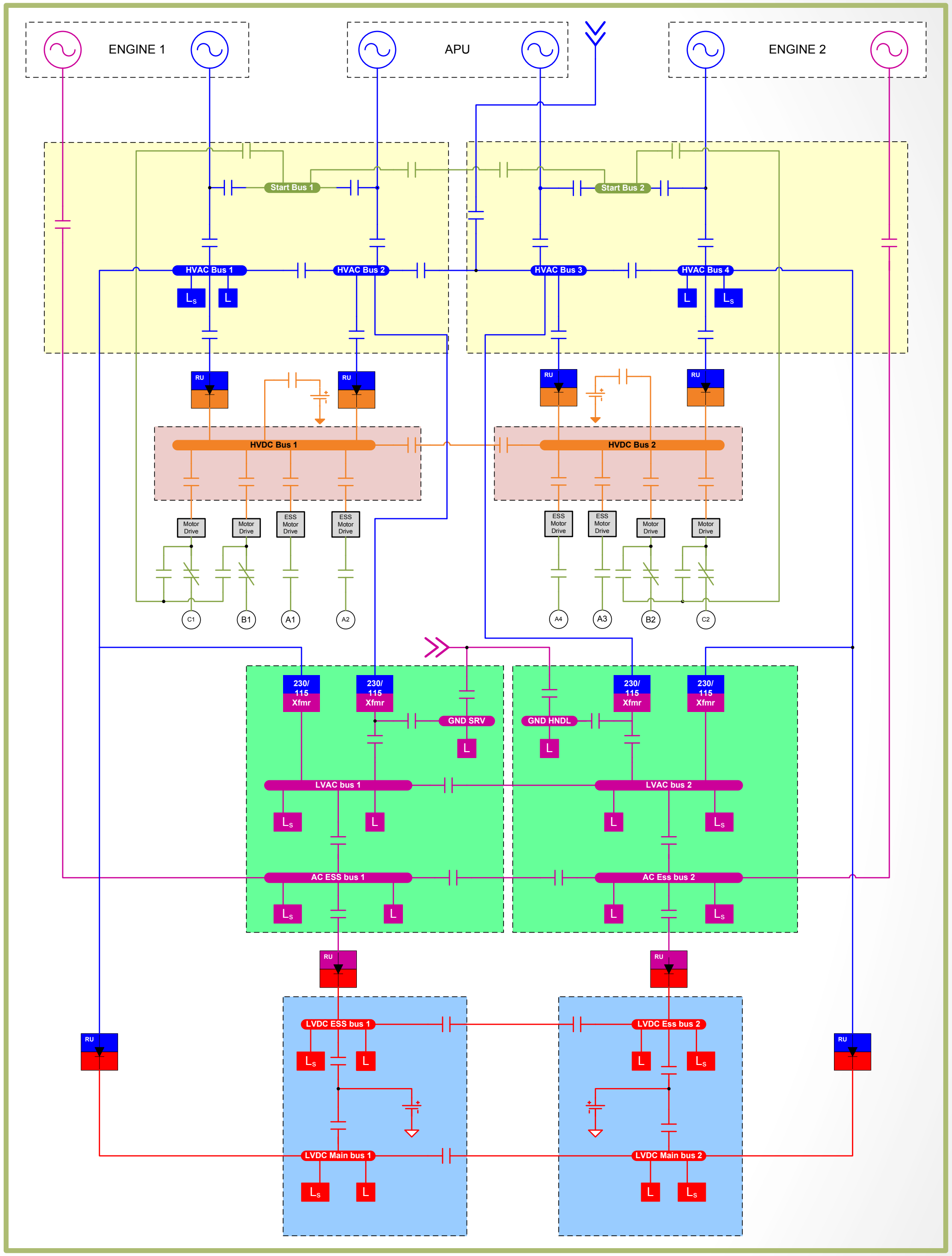


Figure courtesy of Rich Poisson, Hamilton-Sundstrand. Adapted from Honeywell Patent US 7,439,634 B2

Problem Description

- Specifications: text-based to formal language
  - Safety
    - Non-paralleling
    - Essential loads must be powered
    - Contactor opening and closing times
  - Reliance
    - Priority Tables
  - Performance
    - Probability of failure

Priority	Bus 1	Bus 2	Bus 3	Bus 4
1	G_L	A_L	A_R	G_R
2	G_R	G_L	G_R	G_L
3	A_L	G_R	G_L	A_R
4	A_R	A_R	A_L	A_L

Given system specifications, design a control protocol that ensures the controlled system satisfies the specifications.

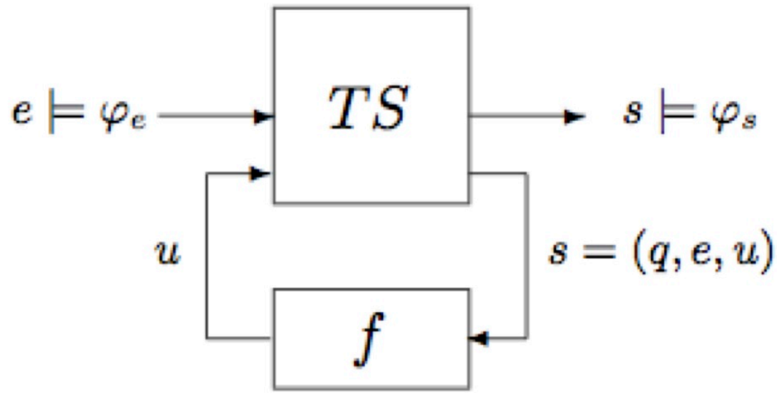
Reactive Synthesis

Given:

Open transition system

$$TS = (Q, I, \mathcal{A}_{uc}, \mathcal{A}_c, R_{nom})$$

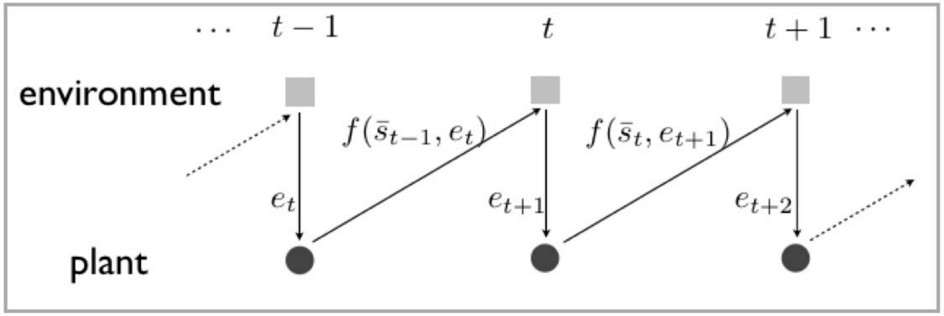
- Q finite set of states,
- $I \subseteq Q$ set of initial states,
- $\mathcal{A}_{uc}$ set of uncontrollable input actions
- $\mathcal{A}_c$ set of controllable input actions
- $R_{nom} \subseteq Q \times \mathcal{A} \times Q$ transition relation



Assume-guarantee type temporal logic specification

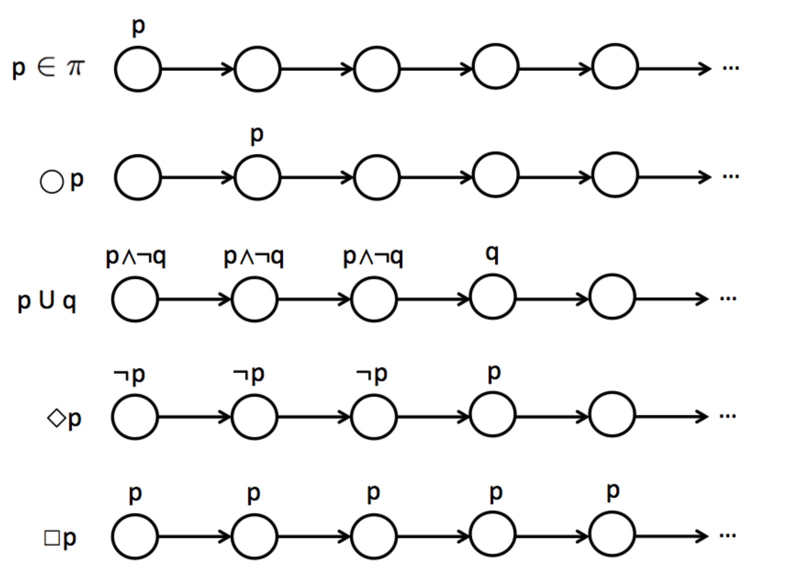
$$\varphi = \varphi_e \rightarrow \varphi_s$$

Compute: A strategy $f : (q_0, e_0, u_0, \cdots, q_{i-1}, e_{i-1}, u_{i-1}, q_i, e_i) \mapsto u_i$ with $(q_i, e_i, u_i, q_{i+1}) \in R_{nom}, \ \forall i \geq 0$ such that any controlled execution satisfies the specification.



Formal Specification and Synthesis

- Linear Temporal Logic
  - Safety
  - Progress
  - Response



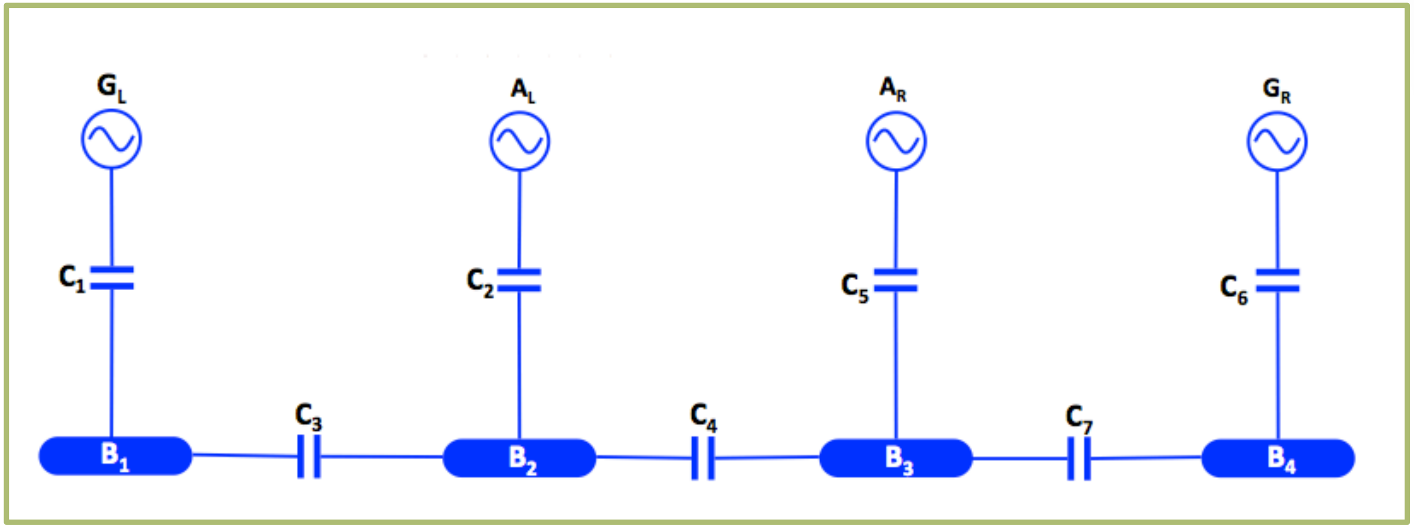
- GR(1) Reactive Synthesis

$$\varphi = (\varphi_e \rightarrow \varphi_s)$$

$$\varphi_\alpha := \varphi_{\text{init}}^\alpha \wedge \bigwedge_{i \in I_1^\alpha} \Box \varphi_{1,i}^\alpha \wedge \bigwedge_{i \in I_2^\alpha} \Box \Diamond \varphi_{2,i}^\alpha$$

TuLiP

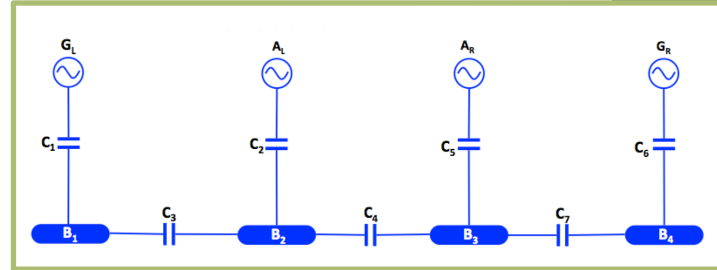
Electric Power System



- Variables
  - Environment: G_L, A_L, A_R, G_R (healthy, unhealthy)
  - Controlled: C_1- C_7 (closed, open)
  - Dependent: B_1- B_4 (powered, unpowered)

Given any admissible environment actions, determine all sets of contactor configurations (and transitions) such that system will satisfy all specifications

Formal Specifications



- Environment Assumption

$$\square\{(G_L = 1) \vee (A_L = 1) \vee (A_R = 1) \vee (G_R = 1)\}$$

1. **Direction – no parallel**
2. **Intention – time**

- Power Status of Buses

$$\square\{((C_1 = 1) \ \wedge \ (G_L = 1)) \rightarrow (B_1 = 1)\}$$
$$\square\{((B_2 = 1) \ \wedge \ (C_3 = -1)) \rightarrow (B_1 = 1)\}$$
$$\square\{\neg((C_1 = 1) \ \wedge \ (G_L = 1)) \vee ((B_2 = 1) \ \wedge \ (C_3 = -1)) \rightarrow (B_1 = 0).\}$$

- No Paralleling of AC Sources

$$\square\{\neg(G_L = 1) \rightarrow \neg(\tilde{C}_3 = 1)\}$$
$$\square\{\neg(((G_L = 1) \ \wedge \ (B_2 = 1)) \vee ((B_3 = 1) \ \wedge \ (B_2 = 1))) \rightarrow \neg(\tilde{C}_3 = -1) \ \}$$
$$\square\{\neg((C_2 = 1) \ \wedge \ (C_3 = 1))\}$$
$$\square\{\neg((C_2 = 1) \ \wedge \ (C_4 = -1))\}$$
$$\square\{\neg((C_3 = 1) \ \wedge \ (C_4 = -1))\}$$

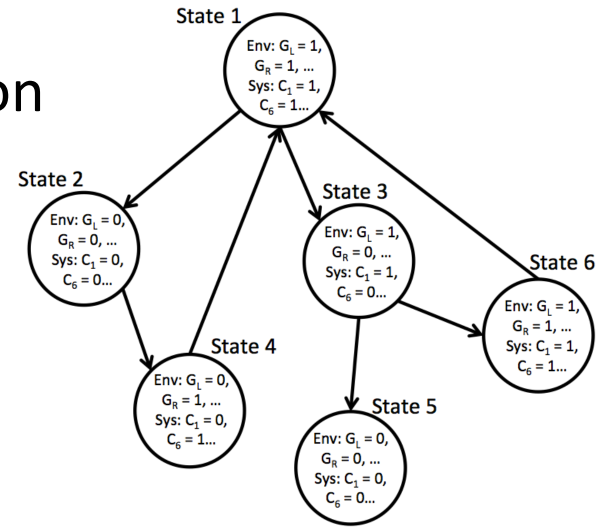
- Essential Buses

$$\square\{(B_1 = 0) \rightarrow (\bigcirc t_1 = t_1 + 1)\}$$
$$\square\{(B_1 = 1) \rightarrow (\bigcirc t_1 = 0)\}$$
$$\square\{t_1 \leq 5\}$$

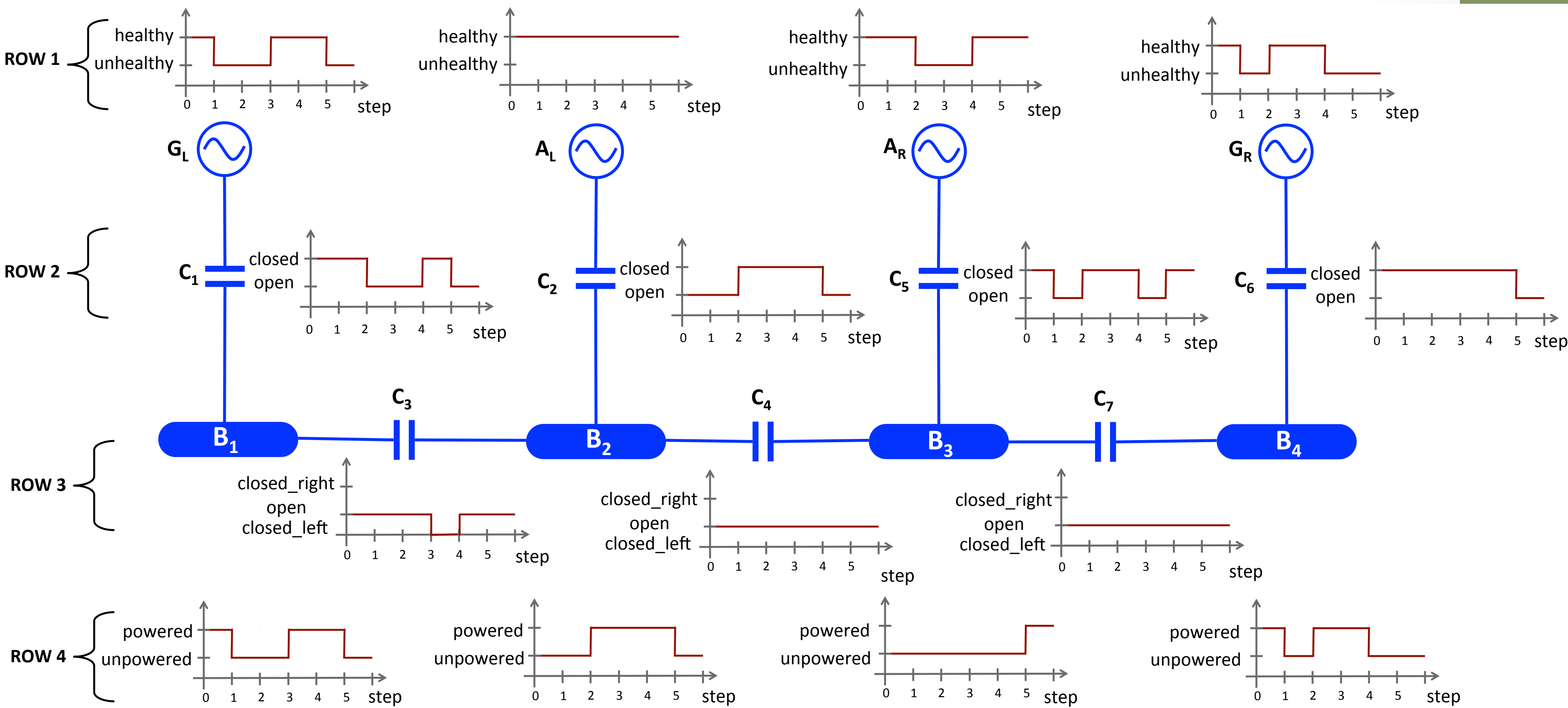
- Disconnect Unhealthy Buses

$$\square\{(G_L = 0) \rightarrow (\tilde{C}_1 = 0)\}$$
$$\square\{((G_L = 0) \ \wedge \ (A_L = 1)) \rightarrow (\tilde{C}_2 = 1)\}$$

Automaton



"Simulation"



Summary/Ongoing Work

- Single-line diagram of an electric power system
- Converted text-based requirements into formal specification language
- Synthesized central and distributed controllers
  - Timing and interface constraints

- Implementation of cost function vs. priority tables
- Scalability: synthesize for entire system (large-scale)
- Better integration with time
  - Timed temporal logic
  - "On-the-fly" synthesis

Acknowledgements

- Rich Poisson (Hamilton-Sundstrand)
- Multi-Scale Systems Center (MuSyC)
- The Boeing Corporation
- Necmiye Ozay (Caltech)