25th anniversary
annual INCOSE
international symposium
Seattle, WA
July 13 - 16, 2015

# Methodology and Tools for Next Generation Cyber-Physical Systems: The iCyPhy Approach

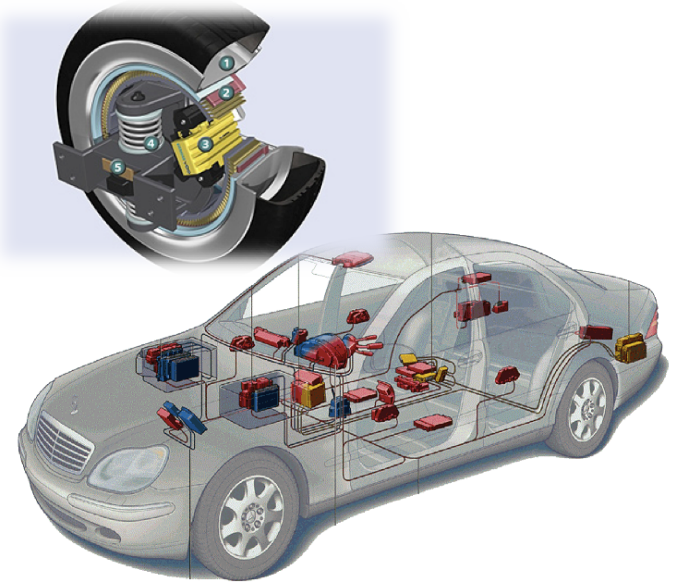
**Pierluigi Nuzzo***, Alberto L. Sangiovanni-Vincentelli*
and Richard M. Murray#

** Dep. Electrical Engineering and Computer Sciences, University of California, Berkeley*
*# Engineering and Applied Science, California Institute of Technology*

# Cyber-Physical Systems (CPS) in Our Life Today…

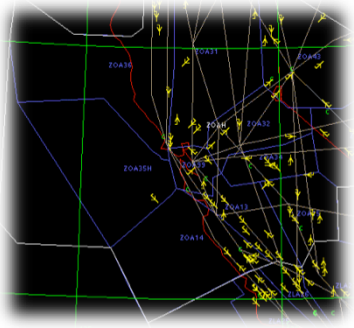
*Avionics*

*Automotive*

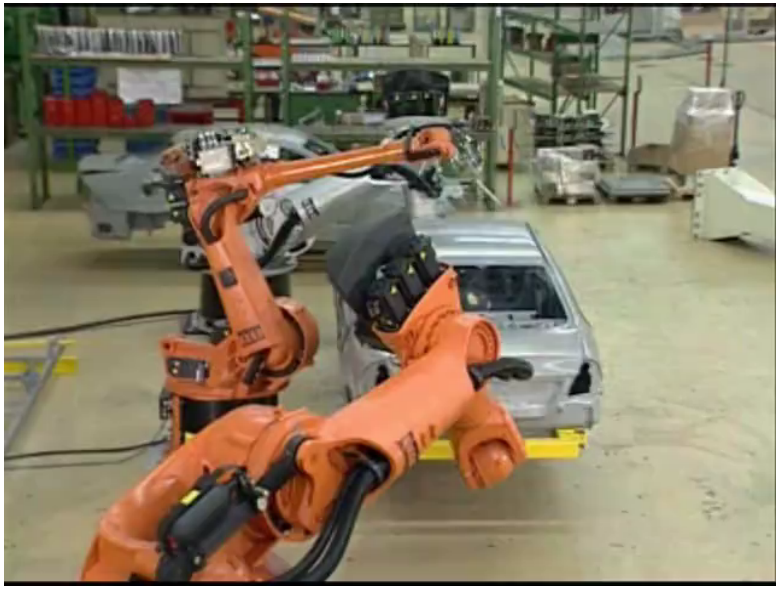


*Telecommunications*

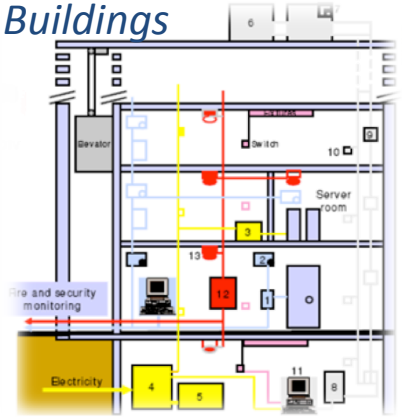
*Transportation (Air traffic control)*



*Factory automation*

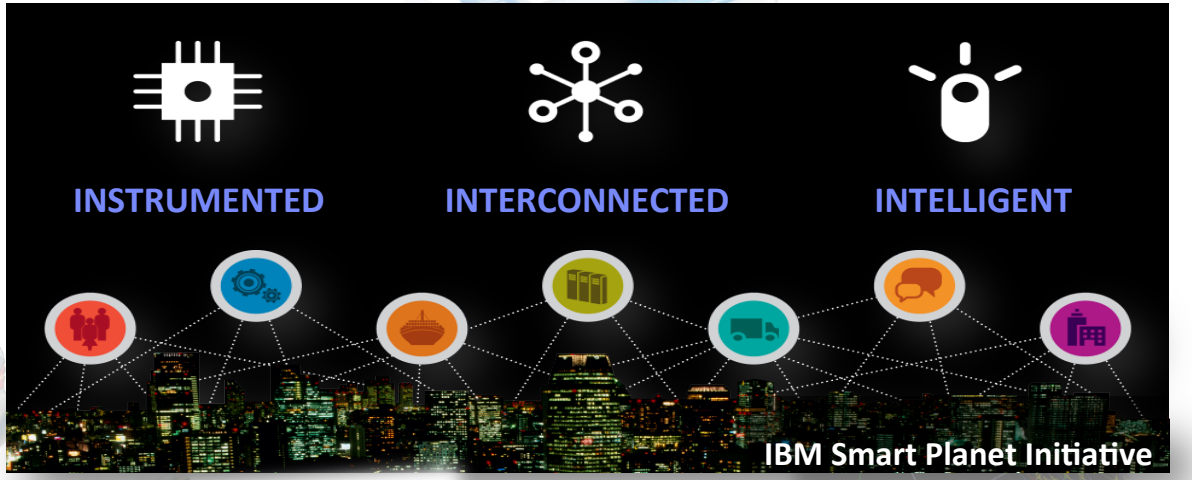


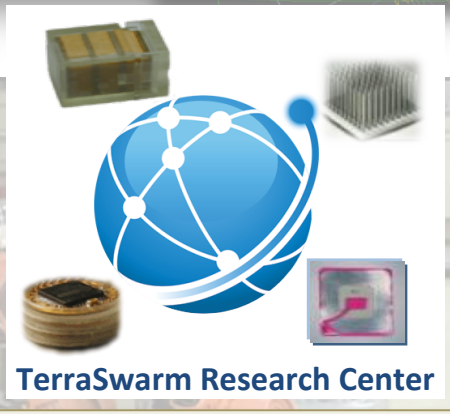
*Buildings*




*Power generation and distribution*

# …and in the Future



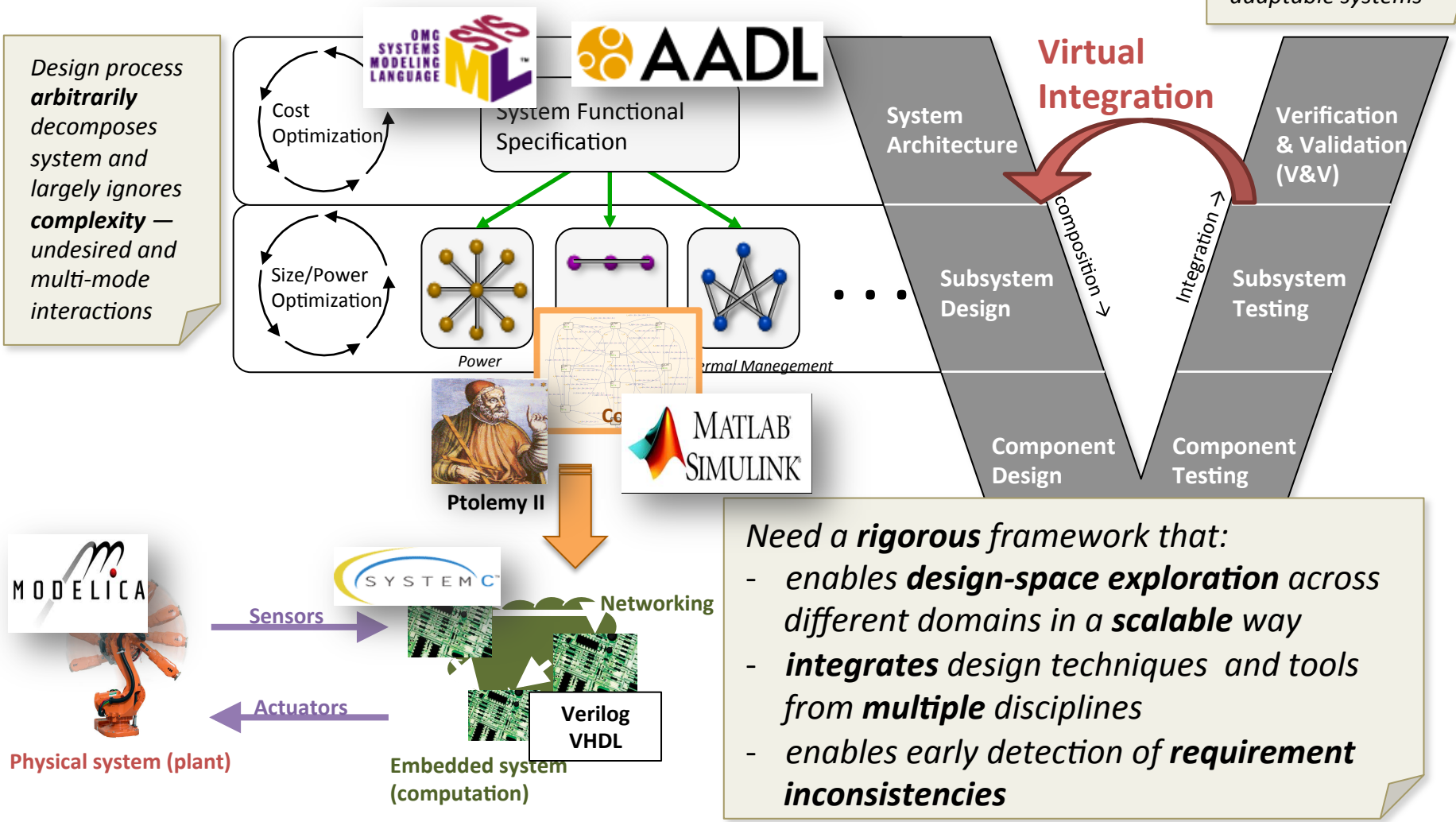

*"Enriched" input and output devices* ***on (and in) the body***
*and in the surrounding environment enable* ***real-life interaction***
*between humans and cyberspace*

# Methodology and Tools: The Challenge of Combining Heterogeneous Worlds

"Let's Get Physical: Computer Science Meets Systems", ETAPS Workshop, 2014

*Conventional V&V techniques do not **scale** to highly complex or adaptable systems*

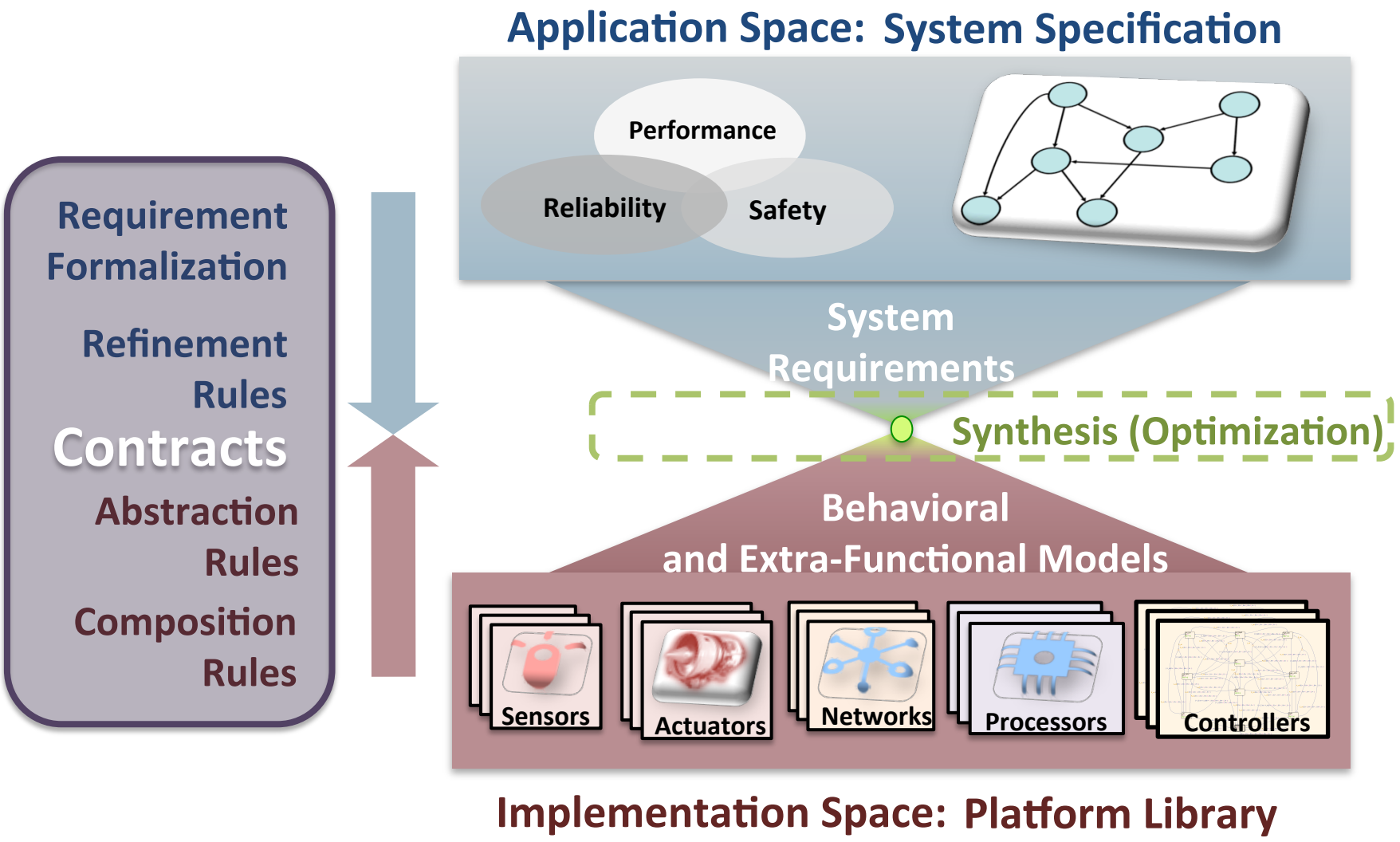
*Design process **arbitrarily** decomposes system and largely ignores **complexity** — undesired and multi-mode interactions*



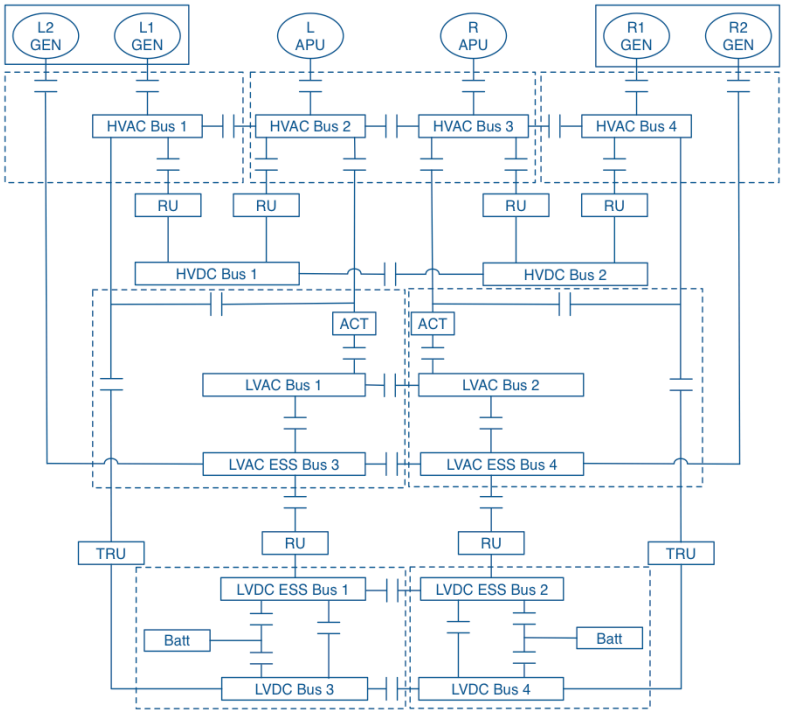

*Need a **rigorous** framework that:*

- *enables **design-space exploration** across different domains in a **scalable** way*
- ***integrates** design techniques and tools from **multiple** disciplines*
- *enables early detection of **requirement inconsistencies***

# The iCyPhy Approach: Platform-Based Design With Contracts



# Running Example: Electric Power System in "More-Electric" Aircraft




**Single Line Diagram modified from Honeywell Patent**

- Components: generators, loads, buses, contactors, transformers, rectifiers,…
- Design architecture and control under safety, reliability and real-time performance requirements
- Typical requirement:
  **A critical bus shall be unpowered for more than 70 ms with probability smaller than $10^{-9}$**

**"A Contract-Based Methodology for Aircraft Electric Power System Design," IEEE Access, 2014**

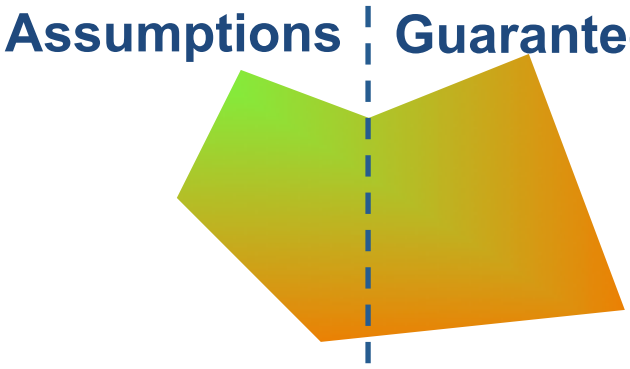
# Outline

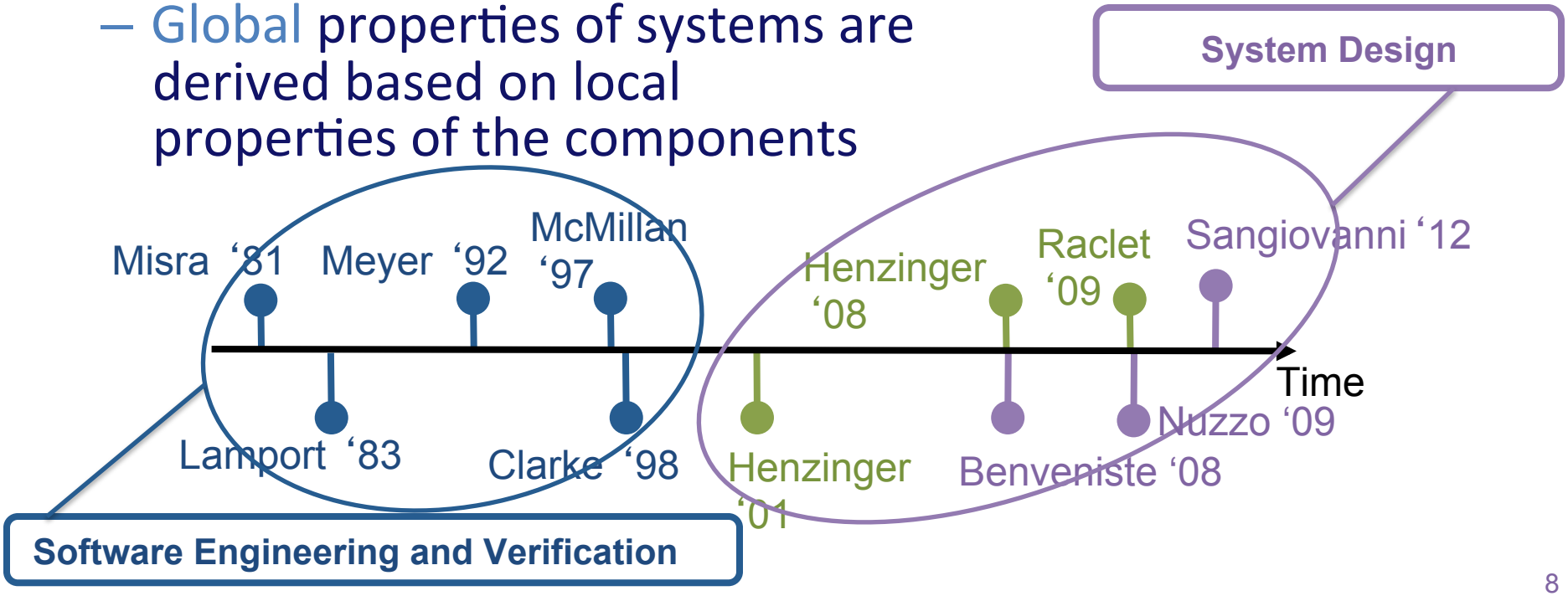
- Background on contracts
- Structure of the methodology
  - Requirement formalization
  - Library generation
  - Mapping specifications to implementations
- Design examples
  - Aircraft electric power system
  - Aircraft air management system

# Why Contracts?

Contracts are Assume-Guarantee pairs

- Component properties are guaranteed under a set of assumptions on the environment
- Global properties of systems are derived based on local properties of the components



# Assume/Guarantee (A/G) Contracts


$$\mathcal{C}_1 : \begin{cases} \text{variables:} & \begin{cases} \text{inputs:} & x, y \\ \text{outputs:} & z \end{cases} \\ \text{types:} & x, y, z \in \mathbb{R} \\ \text{assumptions:} & y \neq 0 \\ \text{guarantees:} & z = x/y \end{cases}$$

An **implementation** *M* **satisfies** a contract if $\boldsymbol{M \cap A \subseteq G}$

An **environment** *E* **satisfies** a contract if $\boldsymbol{E \subseteq A}$

Set $V = I \cup O$ of **variables**
Set *A* of **assumptions**
Set *G* of **guarantees**

(*A*, *G*) is **compatible** iff *A*

(*A*, *G*) is **consistent** iff *G*

**Composition**

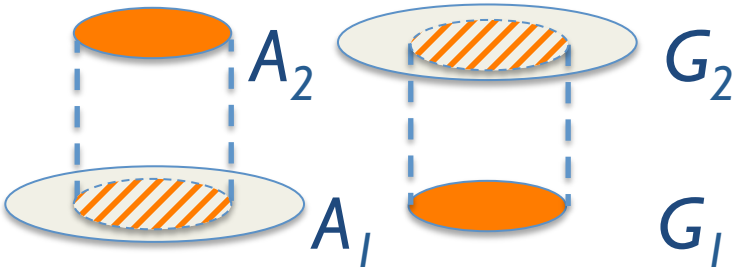
$A = (A_1 \cap A_2) \cup \neg G_1 \cup \neg G_2$
$G = G_1 \cap G_2$

# Assume/Guarantee (A/G) Contracts


$$\mathcal{C}_1 : \begin{cases} \text{variables:} & \begin{cases} \text{inputs:} & x, y \\ \text{outputs:} & z \end{cases} \\ \text{types:} & x, y, z \in \mathbb{R} \\ \text{assumptions:} & y \neq 0 \\ \text{guarantees:} & z = x/y \end{cases}$$

**Refinement**

$A_1$ $A_2$
$G_1$ $G_2$

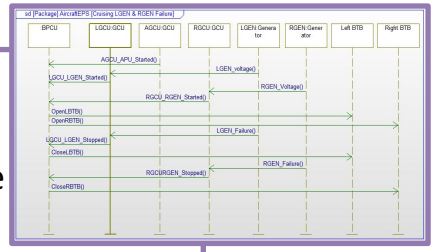



**Conjunction**

$A = A_1 \cup A_2$
$G = G_1 \cap G_2$

# Contracts for Formalizing, Analyzing and Propagating Requirements

1.Reliability
2. Safety
3. Performance
4. Cost (e.g. energy, weight,…)



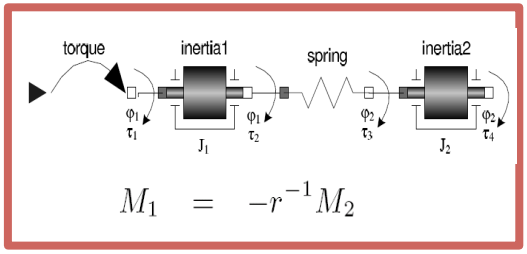
Structure and **formalize**
- Component/Environment
- Functional/Safety/Timing

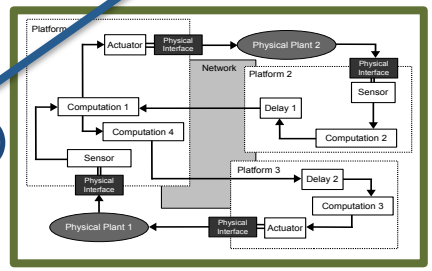
**Requirements**

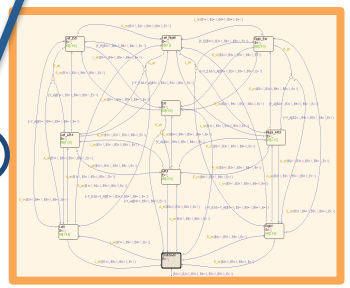
**Conjunction**: Satisfy?

**Refinement**: Satisfy? Replace?

**Composition**: Compatible?



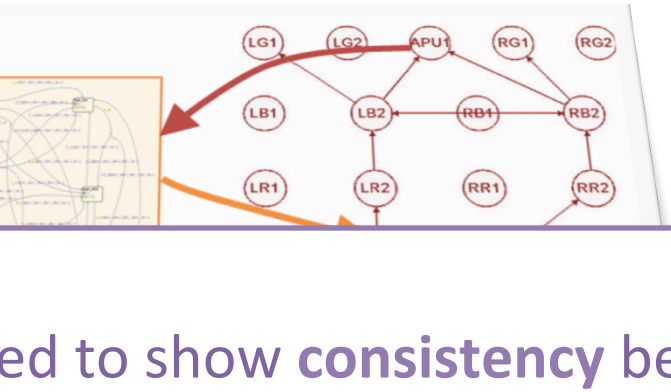



**Physical system** | **Embedded system** | **Controller**

# Horizontal and Vertical Contracts

- Horizontal contracts deal with components at the same level of abstraction
- A component can express assumptions and guarantees w.r.t. another level of abstraction [Nuzzo, et al., IEEE Sensors J. '12]




**Discrete Level Assumptions**

Actuation delay

Worst case execution time

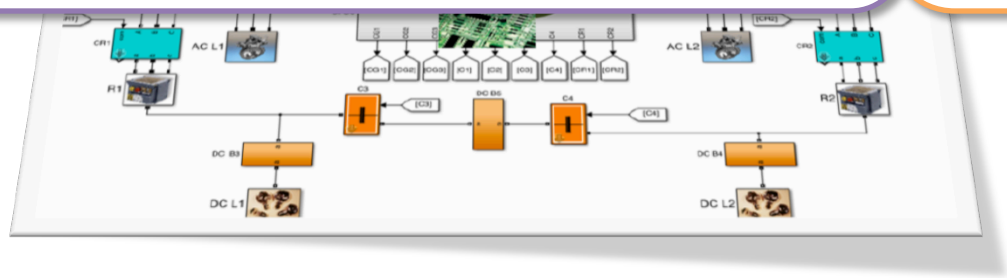
Sensor accuracy

Need to show **consistency** between Discrete and Continuous levels

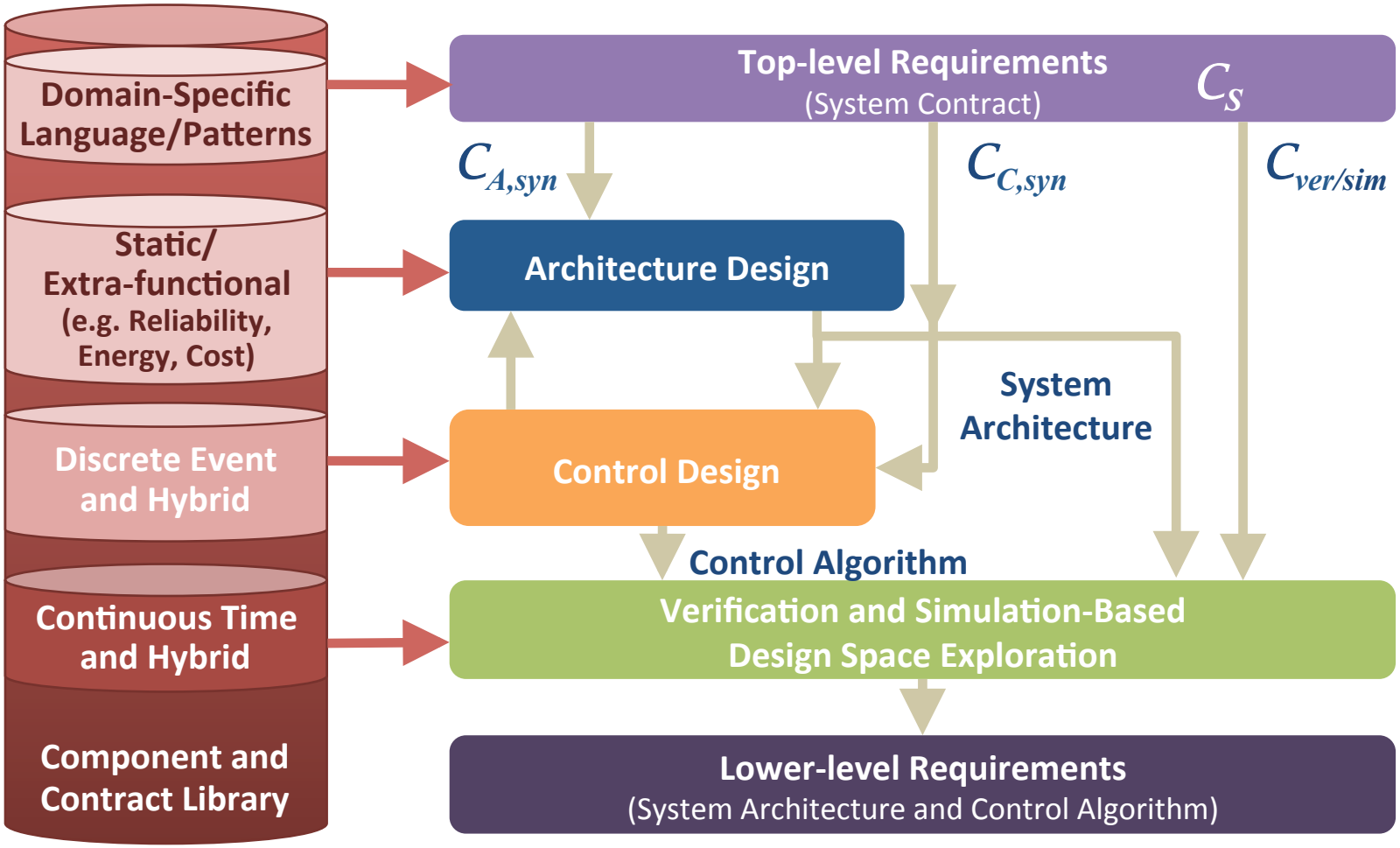
**Continuous Level Assumptions**

Reaction time

Resource usage

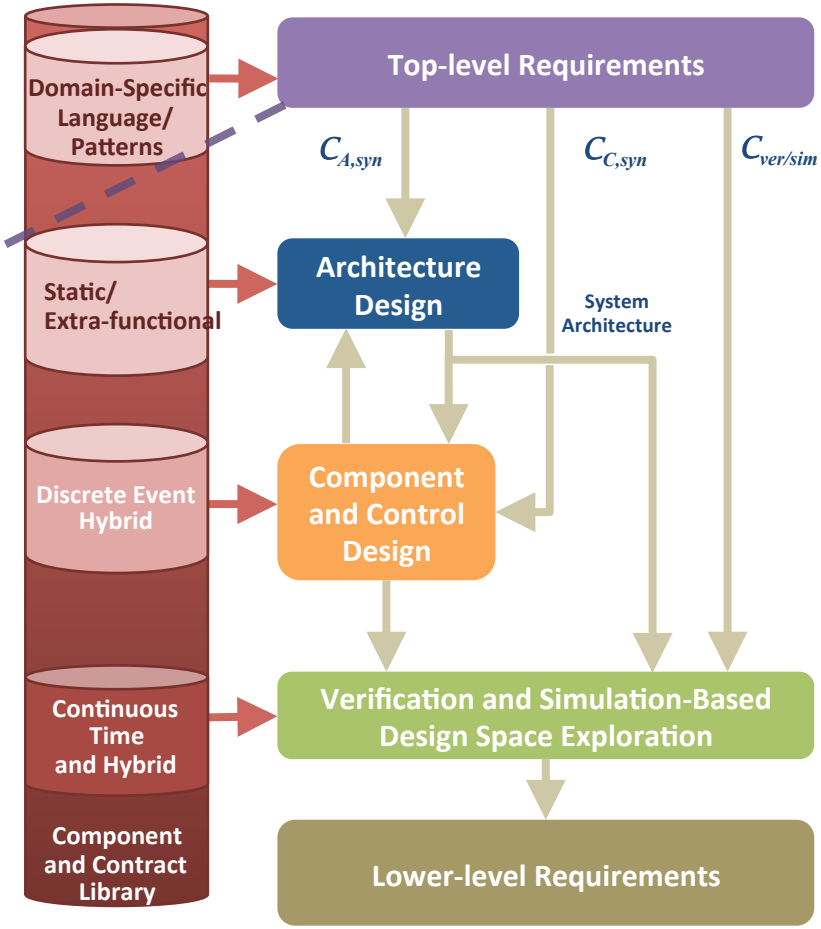


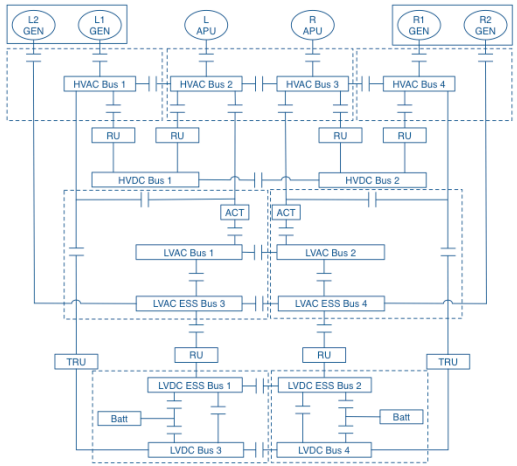
# The Structure of the Methodology

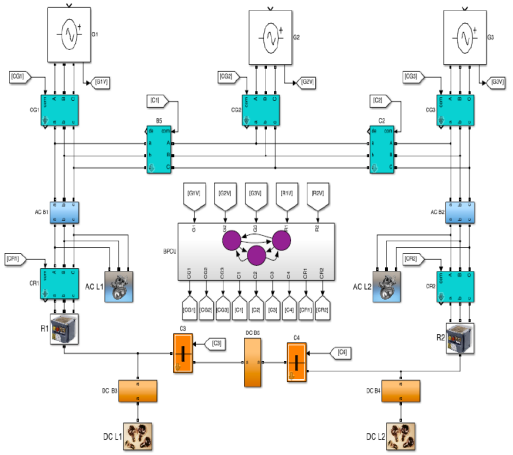


# Electrical Power Distribution System Methodology and Tools

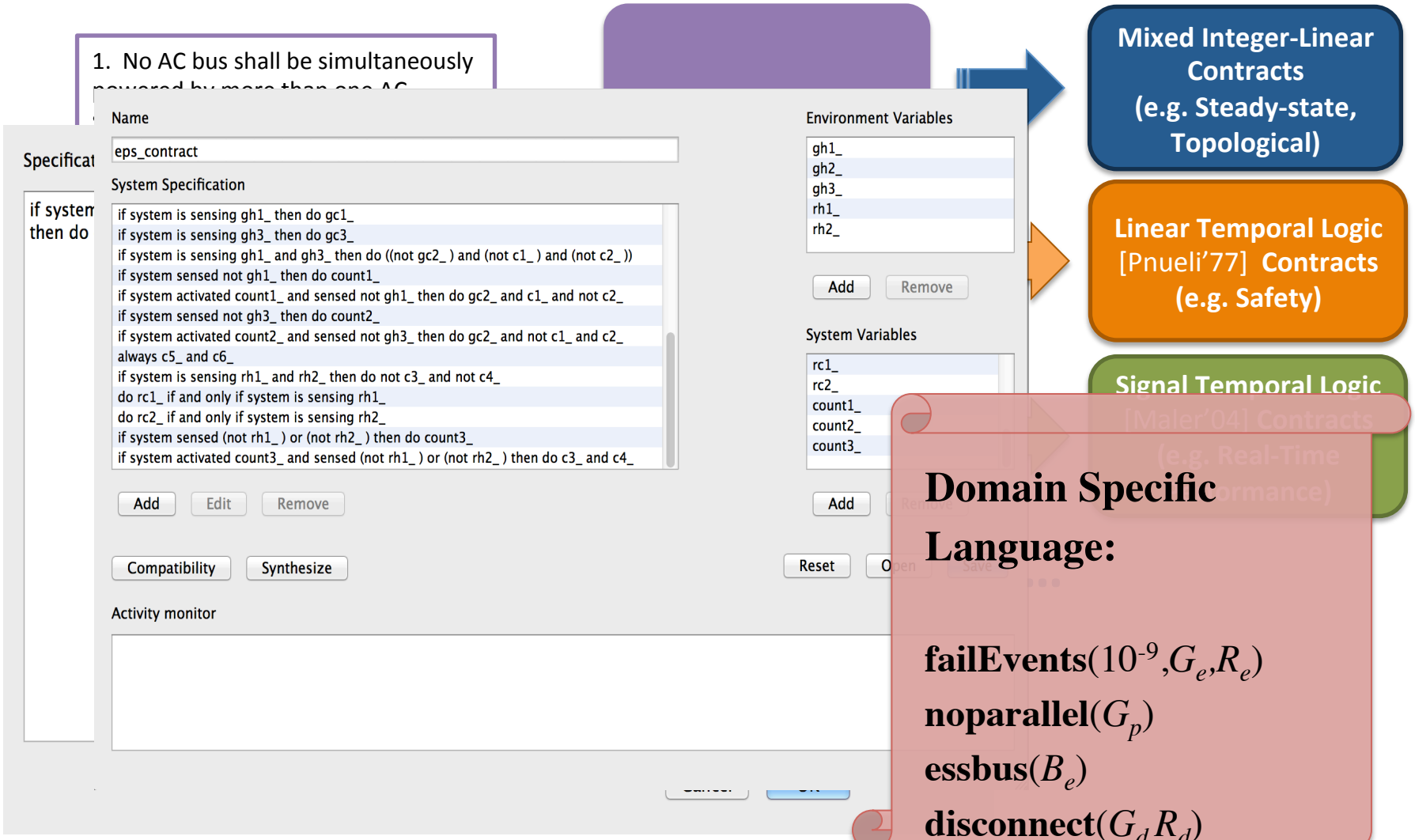
$$\Box\{(\tilde{c}=1\wedge c=0\wedge(x_C<T_{c_{min}}))\rightarrow (\bigcirc c=0\wedge\bigcirc x_C=x_C+\delta)\},$$
$$\Box\{(\tilde{c}=1\wedge c=0\wedge(x_C\geq T_{c_{min}}))\rightarrow (\bigcirc c=1\vee\bigcirc x_C=x_C+\delta)\},$$
$$\sum_{i=1}^{n_{rec}} M_{i,j}^{rd}\geq\sum_{i=1}^{n_{load}} M_{j,i}^{dl},\quad \sum_{i=1}^{n_{rec}} M_{i,j}^{rd}\geq\sum_{i=1}^{n_{dcb}} M_{j,i}^{dd}$$
$$\Box_{[\tau_i,\infty)}(\Diamond_{[0,t_{max}]}(\mid V_{DC}(t)-V_d\mid<\epsilon))$$



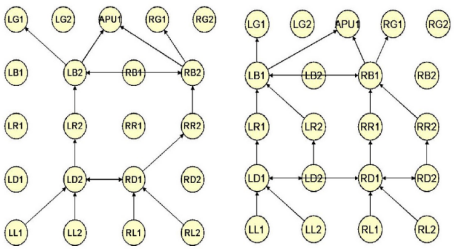



# Capturing and Formalizing Requirements as Contracts

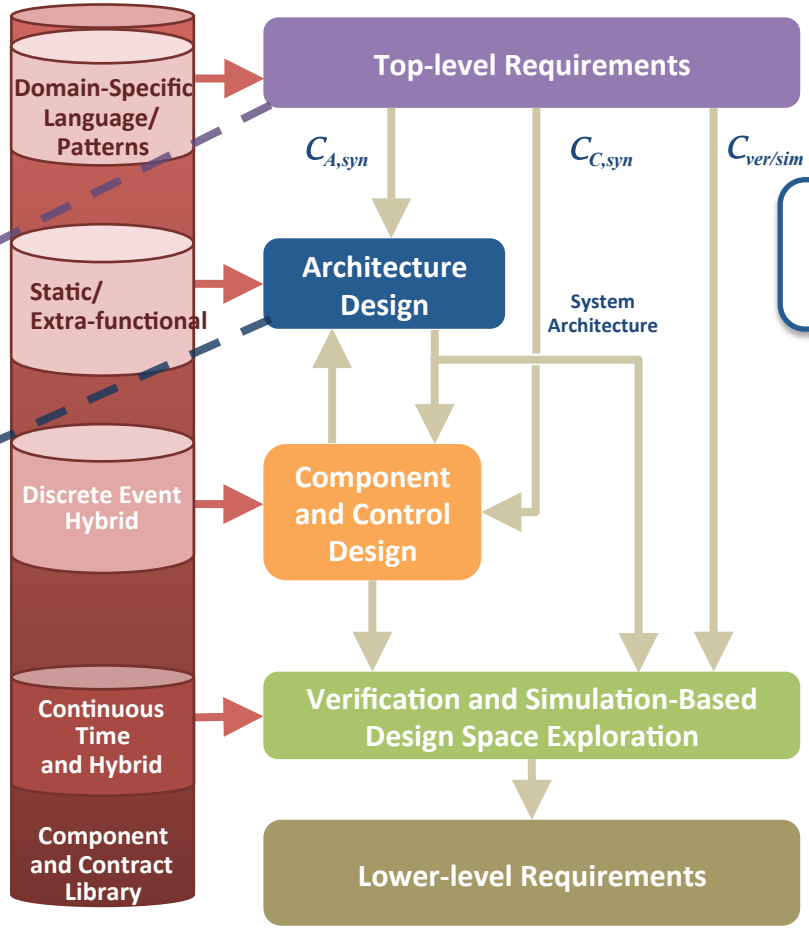


# Electrical Power Distribution System Methodology and Tools: Architecture

$$\square\{(\tilde{c}=1 \wedge c=0 \wedge (x_C < T_{c_{min}})) \rightarrow (\bigcirc c=0 \wedge \bigcirc x_C = x_C + \delta)\},$$
$$\square\{(\tilde{c}=1 \wedge c=0 \wedge (x_C \geq T_{c_{min}})) \rightarrow (\bigcirc c=1 \vee \bigcirc x_C = x_C + \delta)\},$$
$$\sum_{i=1}^{n_{rec}} M_{i,j}^{rd} \geq \sum_{i=1}^{n_{load}} M_{j,i}^{dl}, \quad \sum_{i=1}^{n_{rec}} M_{i,j}^{rd} \geq \sum_{i=1}^{n_{dcb}} M_{j,i}^{dd}$$
$$\square_{[\tau_i,\infty)}(\Diamond_{[0,t_{max}]}(\mid V_{DC}(t) - V_d \mid < \epsilon))$$




Minimize cost, weight, number of components subject to connectivity (electrical,…) and reliability constraints




**Interconnection**

$$\sum_{i=1}^{n_{acb}} M_{i,j}^{br} \geq \sum_{i=1}^{n_{dcb}} M_{j,i}^{rd}$$

**Power Flow/ Electrical**

**Reliability**

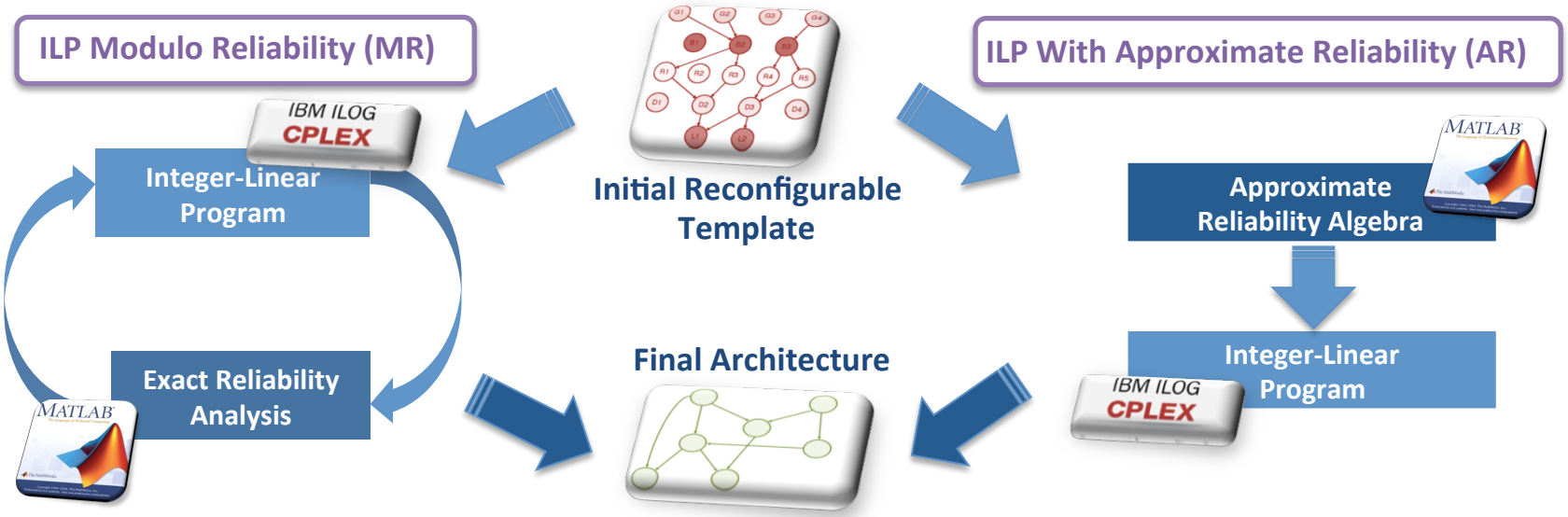
$$r = \mathbb{P}(F) = \mathbb{P}\left(\bigcup_{k=1}^{m} F_k\right)$$

ARCHEX

**Component Attributes:**
- Reliability (Fault models)
- Cost
- Type (function/role in system)

[DATE'15]

# ARCHEX: Harnessing the Complexity of Symbolic Reliability Computations




ILP-MR: Combines ILP solver with exact reliability analysis (lazy)

- Mo
  inc
- Exa

ILP-AR: Generates monolithic ILP instances (eager), albeit of a larger size

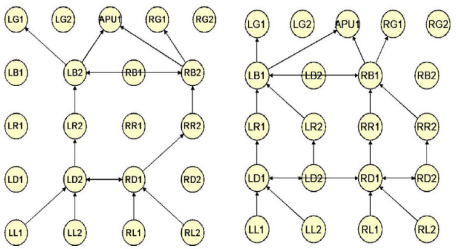
- Computes linear symbolic reliability constraints in polynomial

etical

Generate in **a few minutes** power system architectures with up to 50 graph nodes

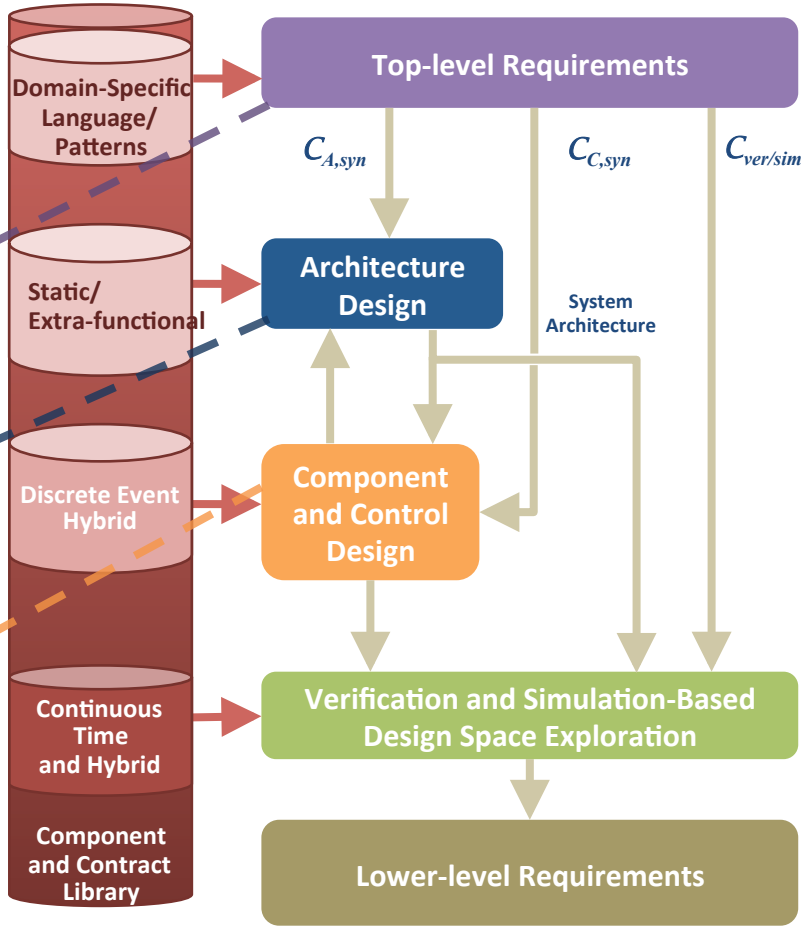
# Electrical Power Distribution System Methodology and Tools: Control

$$\Box\{(\tilde{c}=1 \wedge c=0 \wedge (x_C < T_{c_{min}})) \rightarrow (\bigcirc c=0 \wedge \bigcirc x_C = x_C + \delta)\},$$
$$\Box\{(\tilde{c}=1 \wedge c=0 \wedge (x_C \geq T_{c_{min}})) \rightarrow (\bigcirc c=1 \vee \bigcirc x_C = x_C + \delta)\},$$
$$\sum_{i=1}^{n_{rec}} M_{i,j}^{rd} \geq \sum_{i=1}^{n_{load}} M_{j,i}^{dl}, \quad \sum_{i=1}^{n_{rec}} M_{i,j}^{rd} \geq \sum_{i=1}^{n_{dcb}} M_{j,i}^{dd}$$
$$\Box_{[\tau_i,\infty)}(\Diamond_{[0,t_{max}]}(\mid V_{DC}(t) - V_d \mid < \epsilon))$$









# Control Synthesis from Temporal Logic Contracts

$G_C$

**Power Flow**

$$\square\left\{\bigwedge_{i\in\mathcal{I}}(e_i=1)\rightarrow\bigwedge_{i\in\mathcal{G}}(P_{e_i}\geq\sum_{B\in\mathcal{B}}l_{i,B})\right\}$$

**No Paralleling AC sources**

$$\square\bigwedge_{i,j\in\mathcal{G}}\left\{\neg\bigwedge_{C\in p_{i,j}}(c=1)\right\}$$

**Centralized and distributed controllers for different topologies: 4-113 states, 0.5-2 s**

TuLiP

**TL Specification & Architecture**

**Control Synthesis**

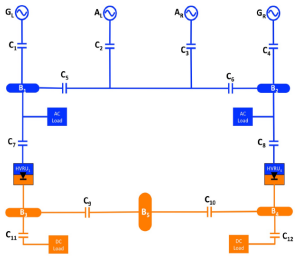

$A_C$

**LTL Behavioral Models**

**Environment Assumptions: Possible Failure Configurations**

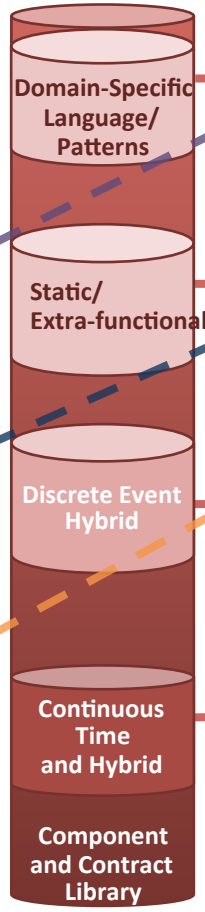
$$\mathcal{E}_S=\left\{\mathbf{e}_{\mathcal{I}'}\,|\,\mathcal{I}'\in h(r_S)\right\}$$

**Architecture**



# Electrical Power Distribution System Methodology and Tools: Control

$$\Box\{(\tilde{c}=1\wedge c=0\wedge(x_C<T_{c_{min}}))\rightarrow (\bigcirc c=0\wedge\bigcirc x_C=x_C+\delta)\},$$
$$\Box\{(\tilde{c}=1\wedge c=0\wedge(x_C\geq T_{c_{min}}))\rightarrow (\bigcirc c=1\vee\bigcirc x_C=x_C+\delta)\},$$
$$\sum_{i=1}^{n_{rec}} M_{i,j}^{rd}\geq\sum_{i=1}^{n_{load}} M_{j,i}^{dl},\quad \sum_{i=1}^{n_{rec}} M_{i,j}^{rd}\geq\sum_{i=1}^{n_{dcb}} M_{j,i}^{dd}$$
$$\Box_{[\tau_i,\infty)}(\Diamond_{[0,t_{max}]}(\mid V_{DC}(t)-V_d\mid<\epsilon))$$




Top-level Requirements

$C_{A,syn}$ $C_{C,syn}$ $C_{ver/sim}$

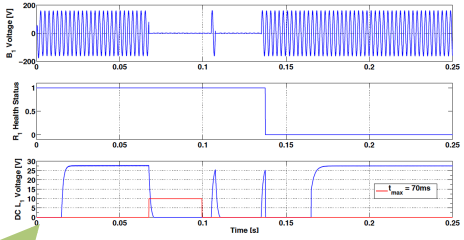
Architecture Design

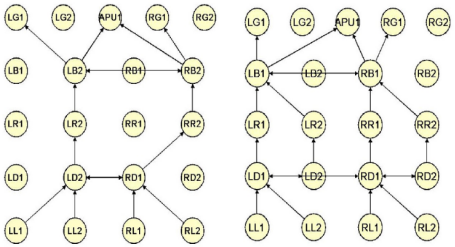
System Architecture

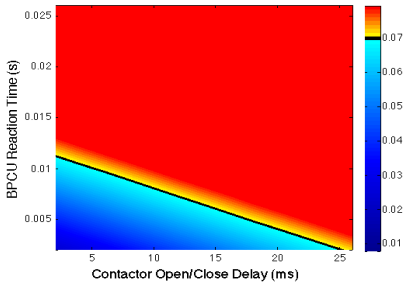
Component and Control Design

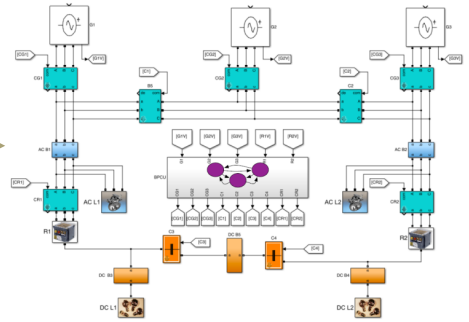
Verification and Simulation-Based Design Space Exploration

Lower-level Requirements







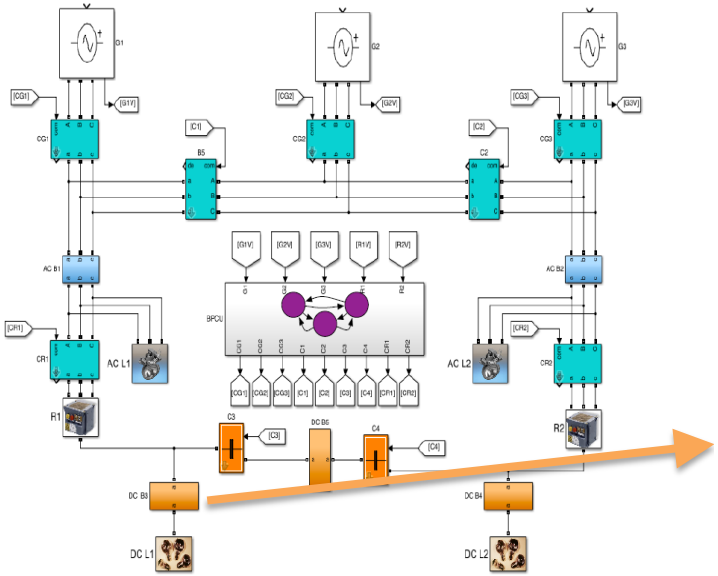



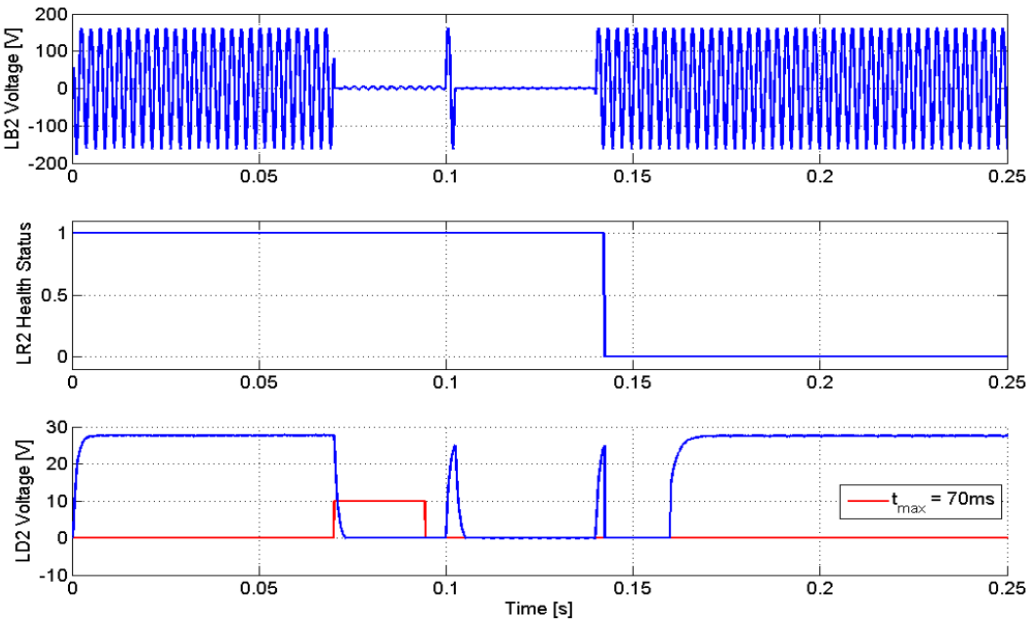
# Control Design: Monitoring STL Contracts

**Real-Time Performance Requirement**

$$\square_{[0,t_{max}]}\neg(|V_{LD2}(t) - V_d| < \delta)$$

MATLAB SIMULINK
BREACH Toolbox [Verimag]






Real-time requirement violation at the DC bus due to a two-generator fault followed by a rectifier fault (worst case scenario)

# Control Design:
# Optimizing Real-Time Performance

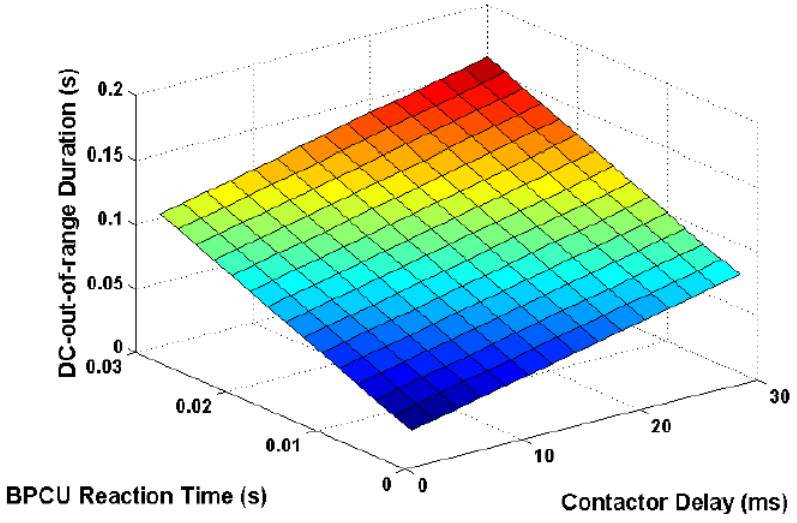
$$\min_{\boldsymbol{\kappa}\in\mathcal{K},\boldsymbol{\tau}\in\mathcal{T},\boldsymbol{\pi}\in\Pi} \quad C(\boldsymbol{\kappa},\boldsymbol{\tau},\boldsymbol{\pi})$$

Model/Formula Parameters

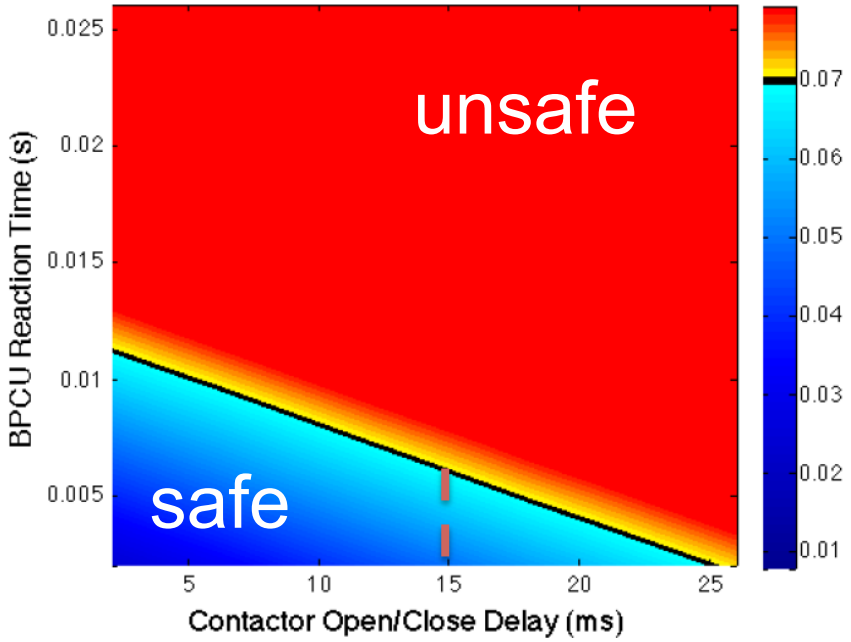
$$\text{s.t.} \begin{cases} \mathcal{F}(\boldsymbol{s},\boldsymbol{\kappa}) = 0 \\ \boldsymbol{s} \models \varphi_s(\boldsymbol{\tau},\boldsymbol{\pi}) \qquad \forall \boldsymbol{s} \quad \text{s.t.} \quad \boldsymbol{s} \models \varphi_e \end{cases}$$

Behavioral Model

STL Contracts



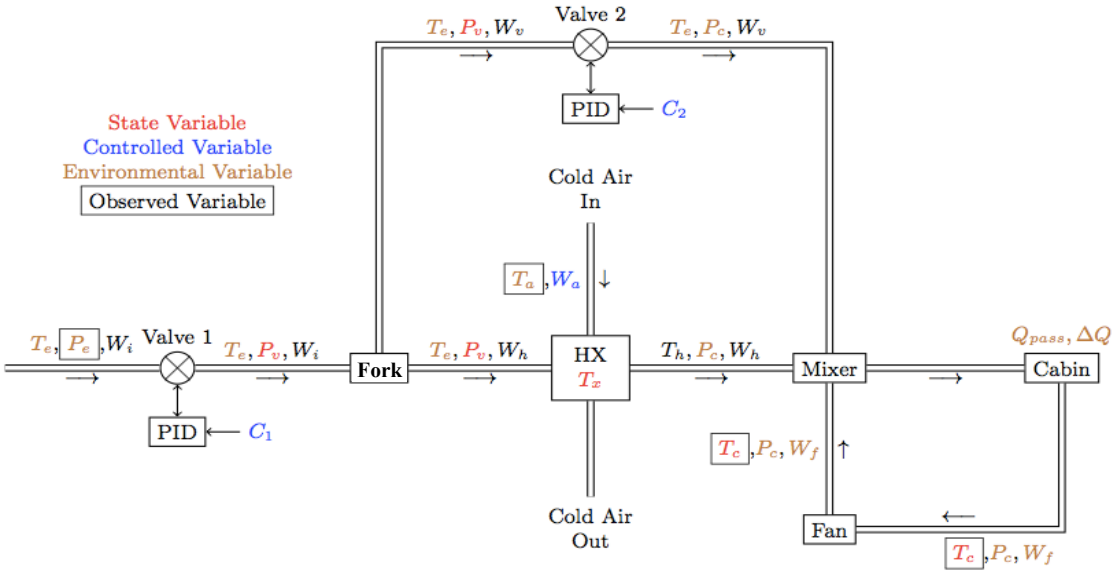

Duration of the violation of the DC bus requirement




Controller reaction times and contactor delays in the blue region satisfy the requirement

~4 hours for a 13x13 point grid

# Aircraft Air Management System




- Design architecture and control to
  - Supply desired pressure and fresh air to cabin at comfortable temperature and humidity
  - Be resilient to faults, e.g. freezing or warping of components

- Pressurization and Air Conditioning Kit
  - Valve 1 controls the flow rate into the system
  - Valve 2 controls fraction of inflow that is cooled in the heat exchanger (HX) by the cold mass flow

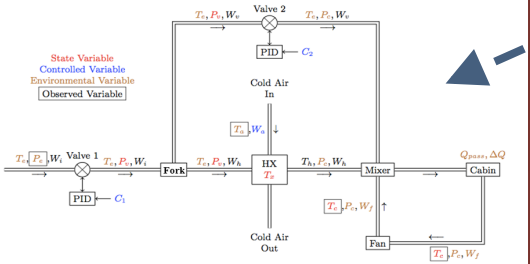
# Air Management System Methodology and Tools

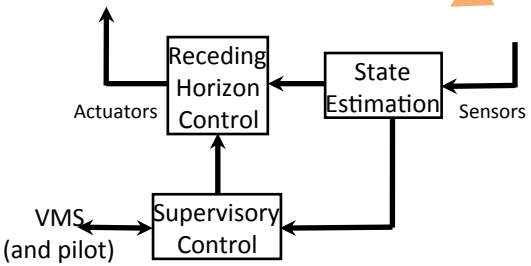
$$\Diamond_{[0,15min]} 291 \leq T_c \leq 298$$

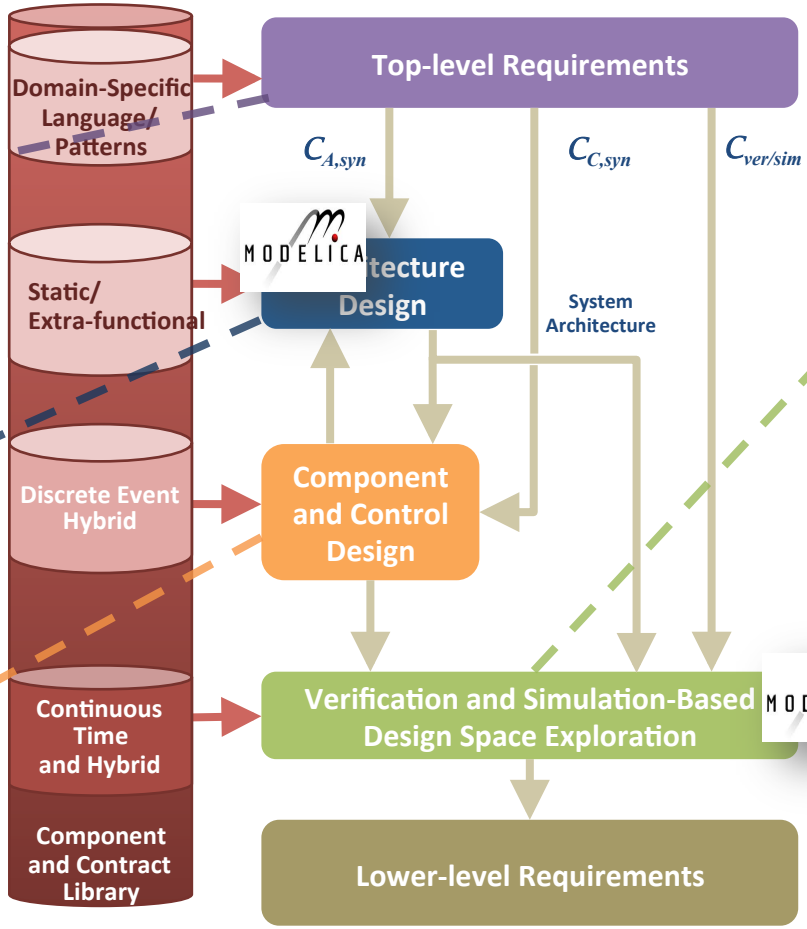
$$\Box_{[0,\infty)} T_x \geq 273$$

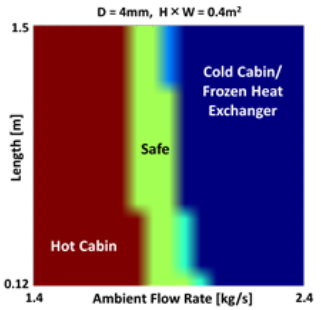
$$(C_{mat} == Al \rightarrow \Box_{[0,\infty)} T_{comp} \leq 450K)$$

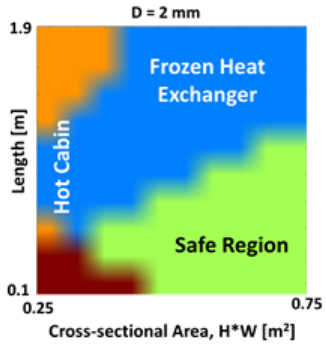
$$(C_{mat} == steel \rightarrow \Box_{[0,\infty)} T_{comp} \leq 800K)$$



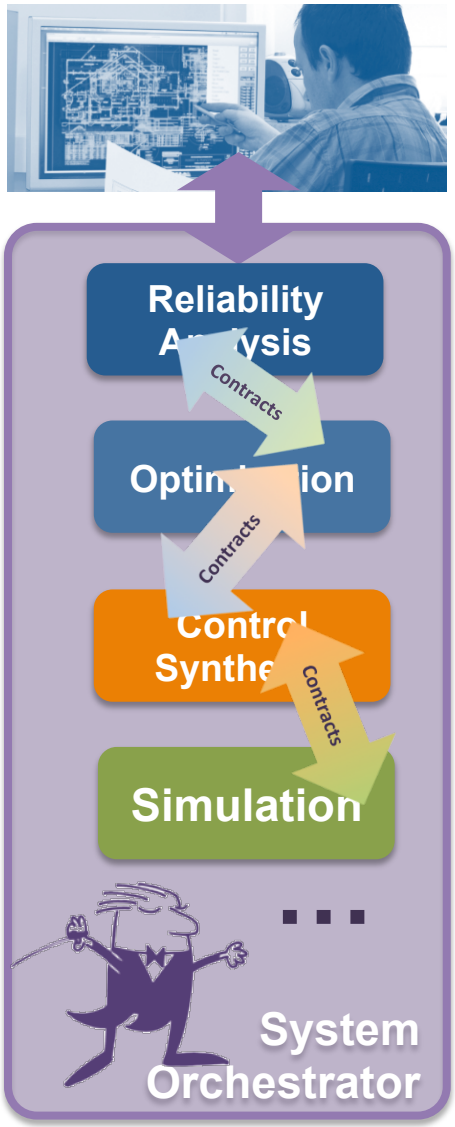




6.5 min for 1251 configurations on an Intel Xeon 3.59GHz with 24GB RAM

# Moving Forward: Towards an Integrated Framework for System Design

- Presented methodology for complex CPS design
  - Meet-in-the middle process (platform-based design)
  - Compositional and hierarchical (A/G contracts)
  - Two examples of industrial relevance
- Next steps
  - More tools for "usable" requirement formalization
  - More scalable contract analysis algorithms
  - Improved control synthesis algorithms for optimality, scalability and support for richer specification languages



# Thank you