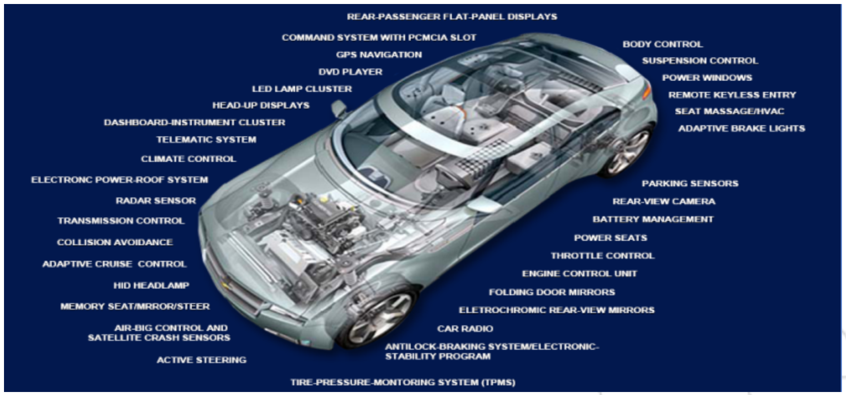
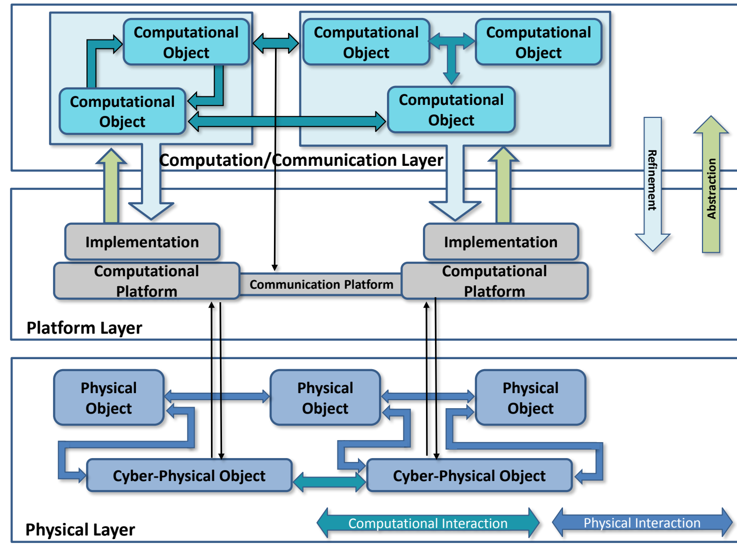
Model-Based Design and Verification of Automotive CPS

Xenofon Koutsoukos

2014 National Workshop on Transportation Cyber-Physical Systems

System Integration





- Implemented components are connected and system-level properties are verified/tested
  - **High risk** – many fundamental problems surface during system integration
  - **Ad-hoc** – 'making it work somehow' attitude
  - **Fundamental problem:** *limited composability and compositionality in heterogeneous systems lead to lack of constructivity in system design*

Scientific Challenge: Foundations for Correct-by-Construction Design

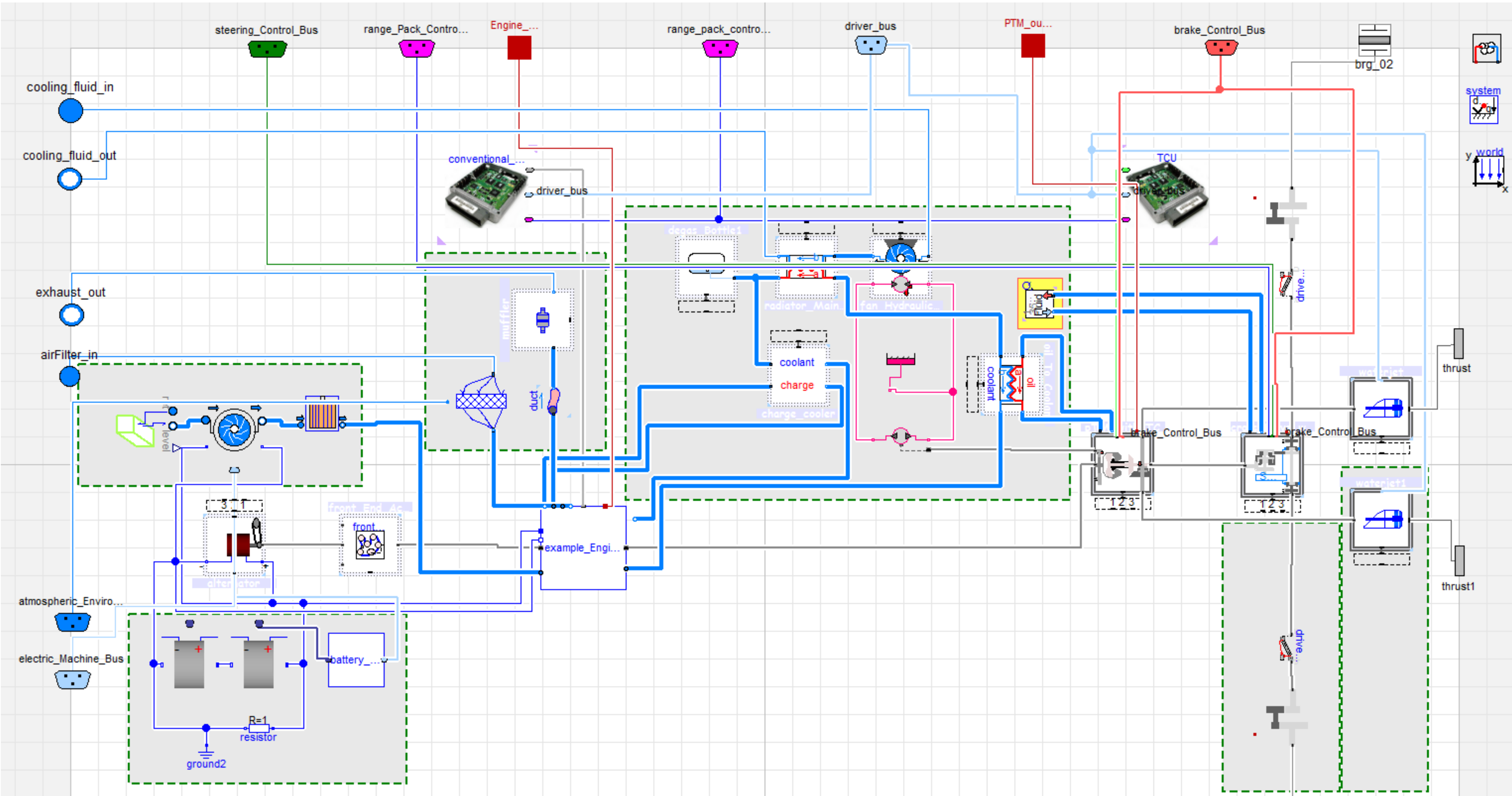
Goal: extend the limits of "correct-by-construction" design:

- **in *broad sense*: model- based design process that leads to manufacturable CPS products with desired properties**
- in *narrow sense*: use architectures that guarantee certain properties

Three major challenges in CPS to advance correct-by construction:

1. Multi-modeling with abstractions for modeling cross-domain interactions
2. Composition in heterogeneous domains
3. Validation and Verification

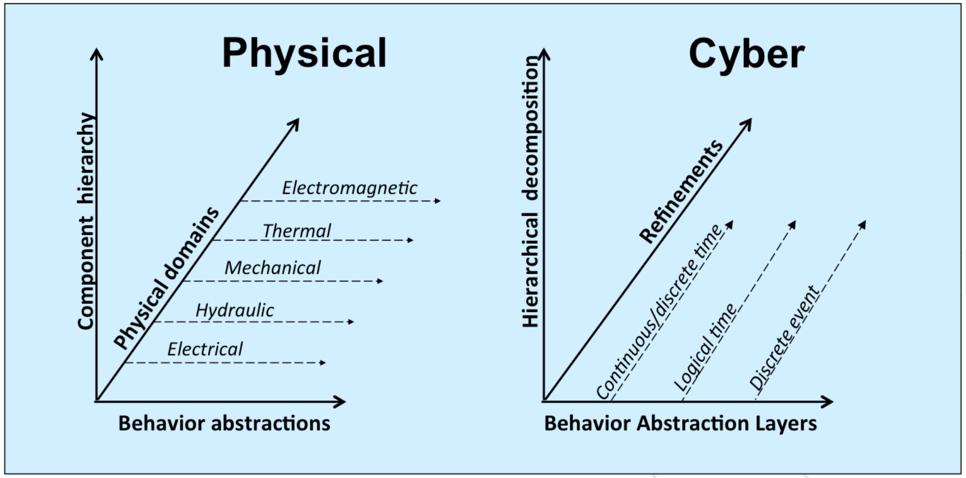
Drivetrain Model in Modelica



Components: Engine, Drive Shaft, Transmission, Final Drive, Air filter, Fuel-Pump, Fuel-Tank, Batteries, Alternator, Coolant System, Hydraulic Reservoir, Hydraulic Pump, ECU, TCU, …

[DARPA AVM Program]

Heterogeneity, Complexity, and Scale



Imperative Code

```
block Sigmoid_Between_Limits
  "y = sigmoid(u) with y very close to 0 at u = u_low and very close to 1 at u = u_high"
  extends Modelica.Blocks.Interfaces.SISO;
  import C2M2L_Ext.Math.Logistic;
  //import C2M2L_Ext.Math.der_Logistic;
  parameter Real u_low = 0 "Value of u at which y should be very close to 0";
  parameter Real u_high = 1 "Value of u at which y should be very close to 1";
  parameter Real sharpness = 10
    "Higher values give a sharper transition and less deviation at u=u_low and u=u_high.  Default 10 gives 0.7% deviation.";
protected
  parameter Real mid_point = (u_high + u_low) * 0.5;
  parameter Real scale = u_high - u_low;
equation
  assert(u_high > u_low, "Sigmoid_Between_Limits: u_high must be greater than u_low");
  y = Logistic(sharpness * (u - mid_point) / scale);
  a;
end Sigmoid_Between_Limits;
```

Original Model

Number of components: 1535 (MSL)
Variables: 14608
Constants: 323 (321 scalars)
Parameters: 5131 (15576 scalars)
Unknowns: 9154 (9911 scalars)
Differentiated variables: 341 scalars
Equations: 8449
Nontrivial : 7275

Simplified Model

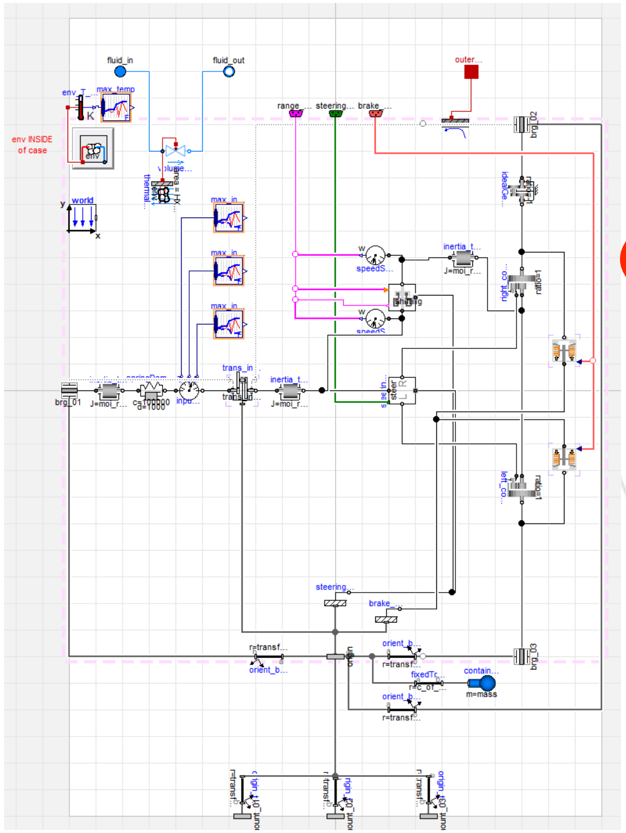
Constants: 4438 scalars
Free parameters: 7437 scalars
Parameter depending: 17496 scalars
Continuous-time states: 103 scalars
Time-varying variables: 2476 scalars
Alias variables: 5249 scalars
Assumed default initial conditions: 78
Number of mixed real/discrete systems of equations: 15
Sizes of linear systems of equations: {31, 22, …}
Sizes after manipulation of the linear systems: {22, 12, …}
Sizes of nonlinear systems of equations: {70, 40, …}
Sizes after manipulation of the nonlinear systems: {7, 6, …}

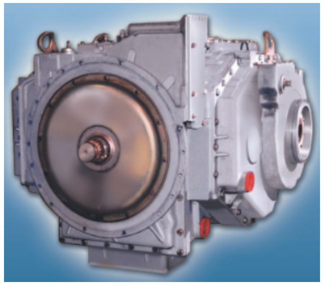
System Requirements

- Payload, towing load effects to dynamic behavior
- Operation in various environmental conditions
  - Altitude, temperature, …
- Mobility
  - Operation profile, acceleration, speed, lateral stability, …
- Brakes
  - Stopping distance, stopping time, …
- Grade and slope operations
- Operational range
- Electronic stability control, suspension, transmission, tires, power generation and management
  - Dynamic behavior, time to raise lower adjustable height transmission, …

The vehicle shall meet all performance targets for all load conditions without exceeding component manufacturers limits [JLTV FoV]

Example: Transmission Limits





SPECIFICATIONS

Gross Input Power — kW (hp) 895 (1200)
1118 (1500)

Gross Input Torque — N•m (lb-ft)
- 1200 hp 5484 (4045)
- 1500 hp 5995 (4422)

Maximum Turbine Torque —
- lb-ft (N•m) 7442 (5489)

Rated Input Speed — rpm 2100

Maximum Input Speed — rpm. 2200

Weight, Dry (approx) — kg (lb)
- Transmission 1694 (3735)
- Engine/Transmission Coupling 108 (238)

Gears
- Type .... Straight spur planetary
- Forward/Reverse....................... 7F/0R

Transmission Speed Ratios

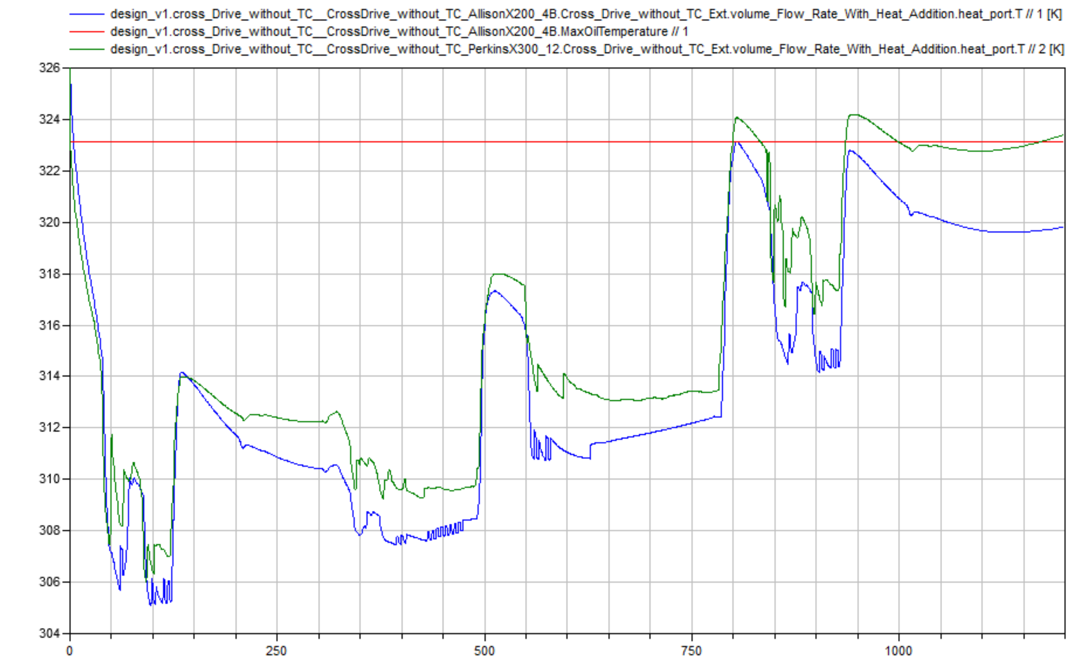
OIL SYSTEM

Cat Transmission/Drive Train Oil-4 (TDTO) or equivalent

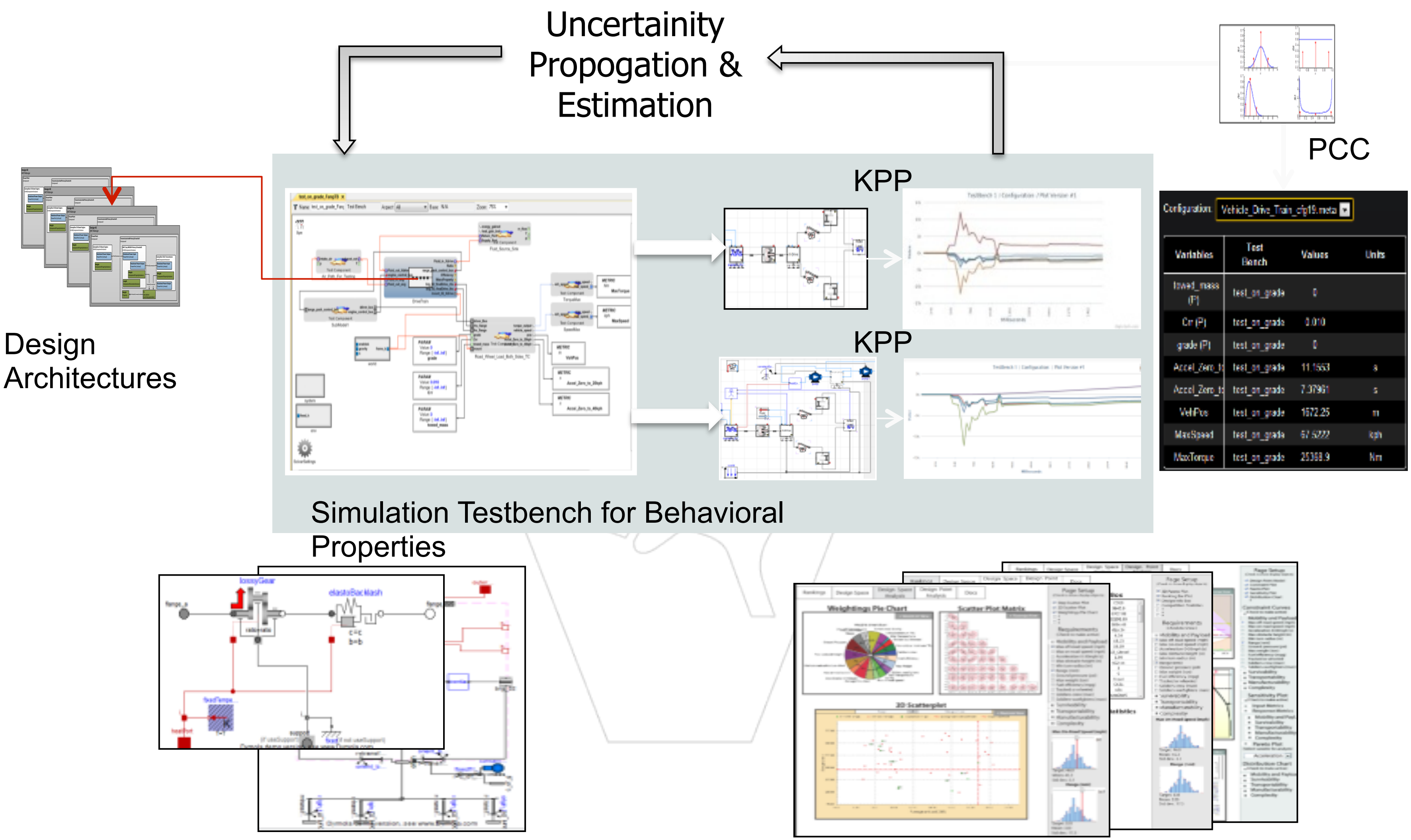
Oil temperatures
- Continuous — 90°C (195°F)
- Maximum operating — 99°C (210°F)

Hydraulic fill capacity — approx. 114 L (30 gal) subject to cooler size, lines, and installation — initial fill may be greater

Filter type — 6 micron synthetic, cartridge remote mount



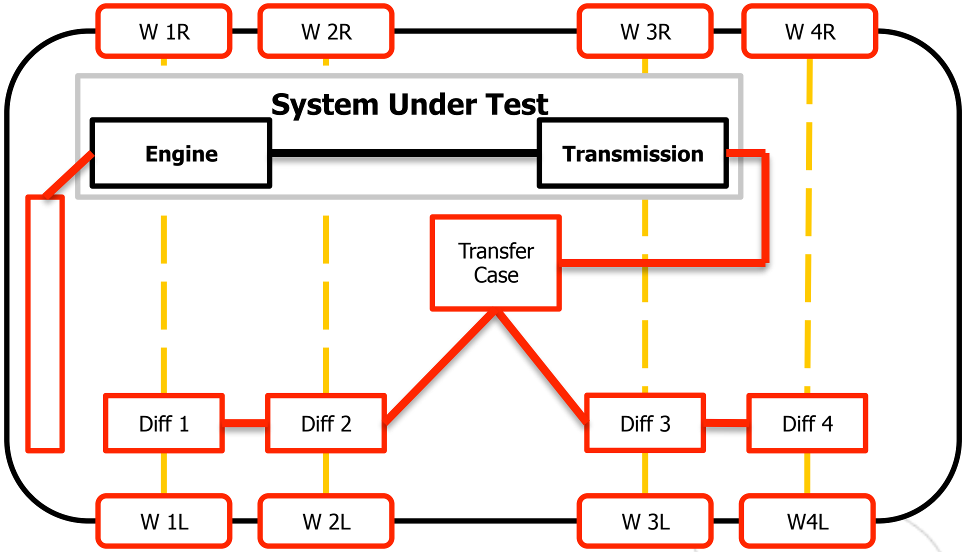
Simulation-based Analysis



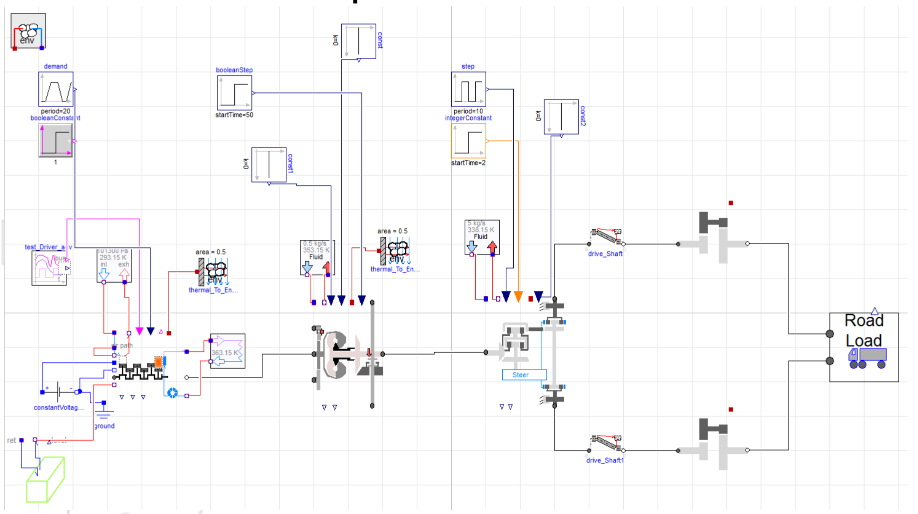
Multiple Fidelity Behavior Models

Multiple Physics Domains

Hybrid System Verification



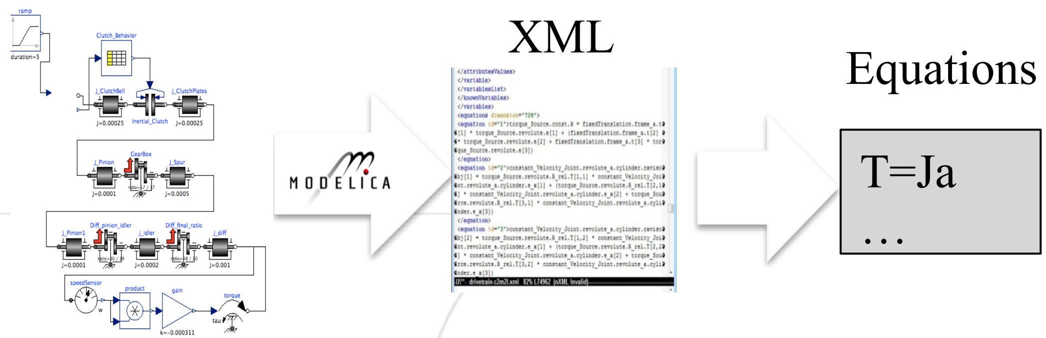
Simplified model



- Problem 1: Determine the range of grades where gears provably do not chatter
- Problem 2: Determine the range for input that guarantees that the engine RPM is bounded
  - Inputs: throttle position and grade of the road

[HybridSAL – Ashish Tiwari (SRI)]

Automated Model Translation



- Modelica2HybridSAL translator
- Piecewise-linear and piecewise-constant approximations
- Identify modes and differential equations for each mode
- 43 continuous variables but 89 discrete variables
- Conditions
  - modes in the plant
  - discrete controller
  - if time < startTime then ...
  - if x < 0 then …
  - if abs(x - 1) < 1e-10 then ...

- Simulation models are not appropriate for formal verification
  - Imperative code
    - Vectorized interpolation (friction and torque maps)
  - Code for numerical stability
    - regRoot
  - Initialization
    - initial()

Formal Verification Challenges

- Complexity and scalability
- Models appropriate for formal verification
- Translation of design requirements to formal verification requirements
- Software tools and integration with modeling and simulation tools
- Usability
- Integration in the design flow: Design space exploration, guidance to the designer

Model Validation

- Model-based design relies on the credibility of predictive modeling
  - Computational models are used to predict system behavior which is not tested experimentally

- Verified properties are properties of the models
  - Dealing with modeling uncertainty is essential
    - Probabilistic uncertainty
    - Epistemic uncertainty

- Model validation is crucial
  - Fidelity-to-data
  - Robustness-to-uncertainty (and lack of knowledge)
  - Prediction confidence