Ontological Reasoning for Consistency in the Design of Cyber-Physical Systems

CPPS'16

April 12th, 2016

Ken Vanherpen, Joachim Denil, István Dávid, Paul De Meulenaere, Pieter J. Mosterman, Martin Törngren, Ahsan Qamar, Hans Vangheluwe

CoSys-Lab
Constrained Systems Lab
University of Antwerp

MathWorks

KTH VETENSKAP OCH KONST

Ford

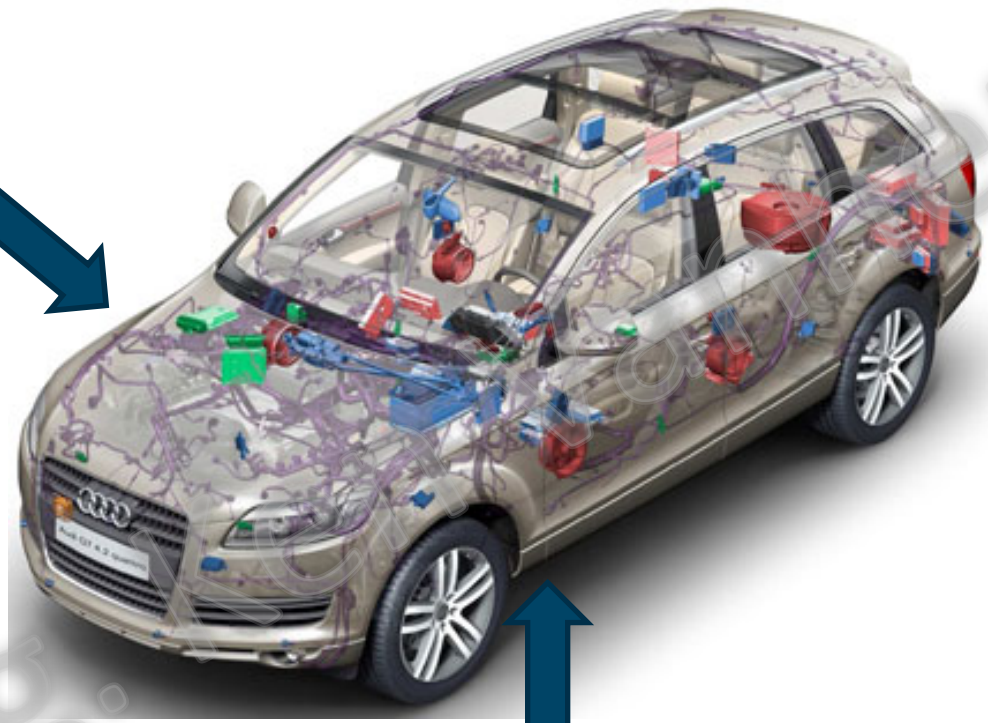
McGill UNIVERSITY

Introduction

Problem Statement

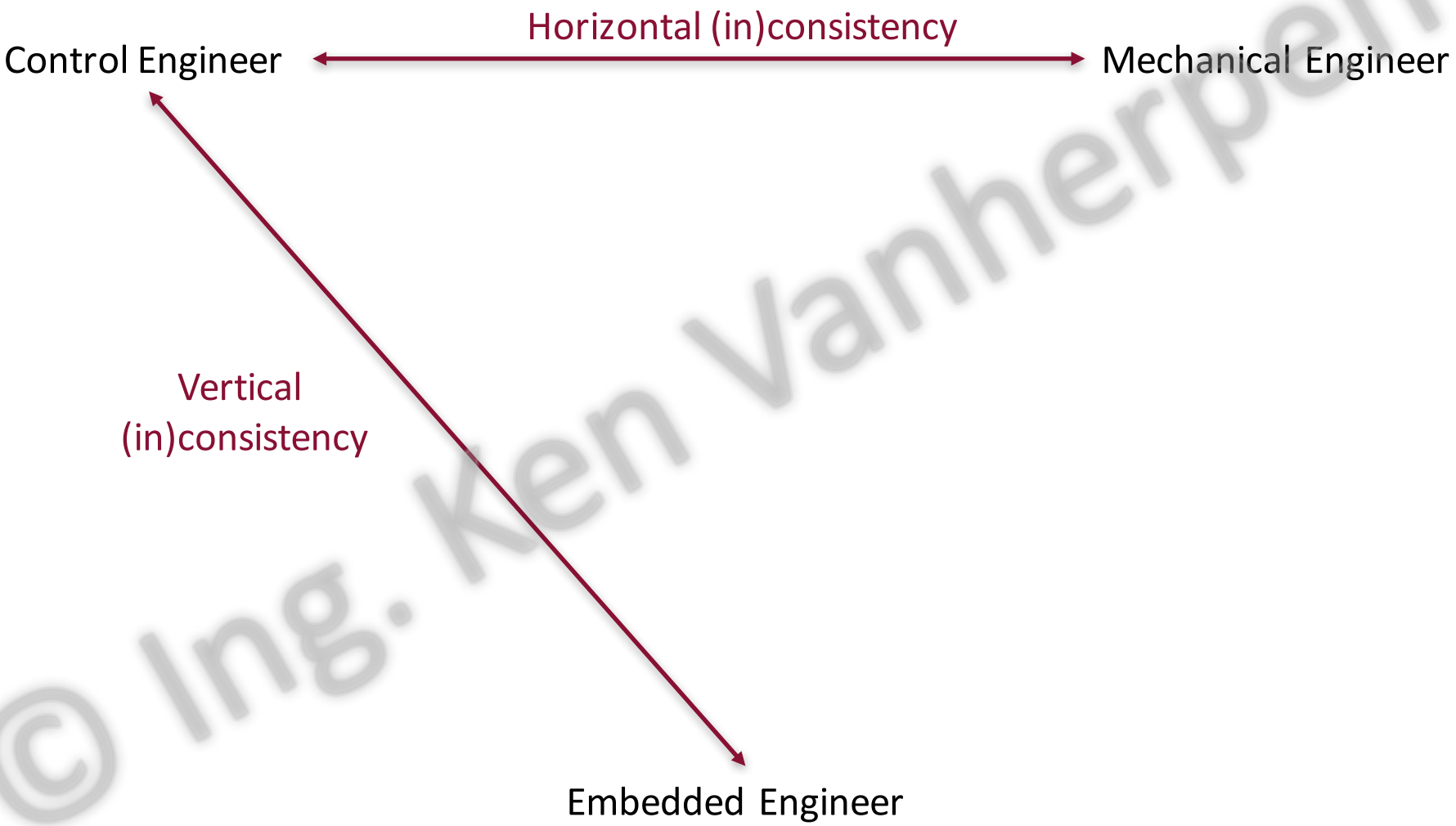
Control Engineer

Mechanical Engineer

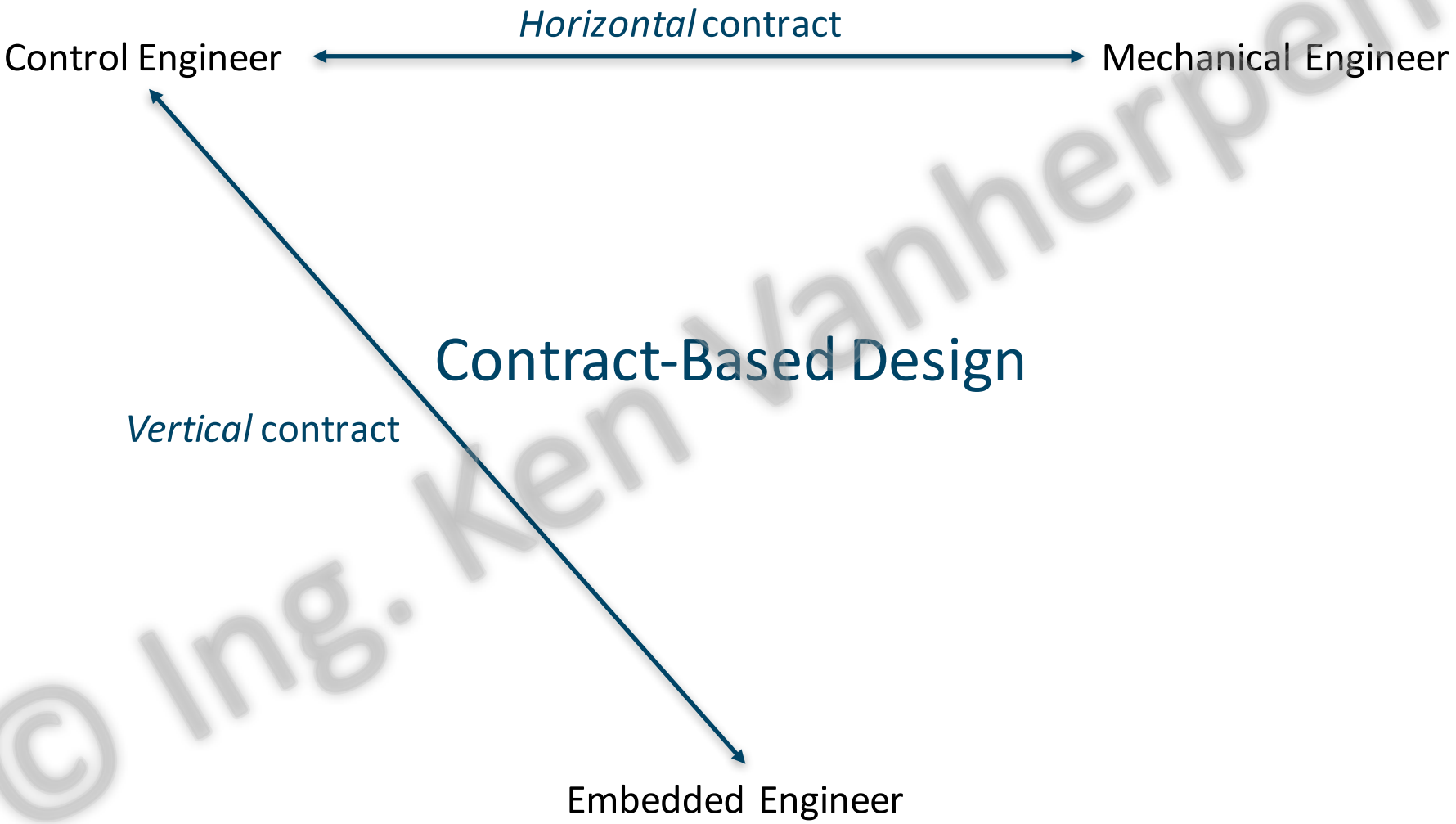


Embedded Engineer

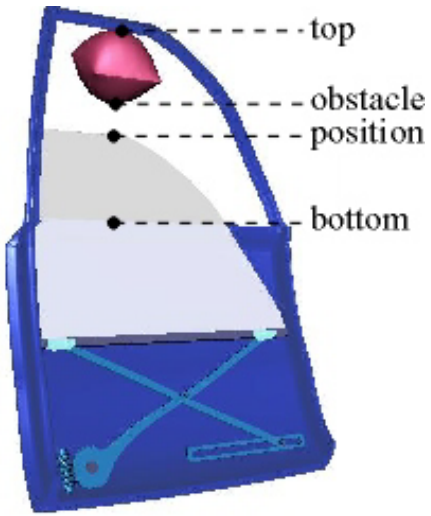
(In)Consistency



Current Solution – Contract-Based Design



Example – Power Window



Requirements[1,2]	Mech	Control	Embedded
An electrical motor will operate the power window.	x	x	x
The window has a width and a height of respectively 1057 mm and 768 mm.	x	x	
The power window can be operated by both driver and passenger. Priority is given to the driver.		x	x
The power window should start moving within 200 ms after a command is issued.			x
The power window shall be fully opened or closed within 4.5 s.	x		x
Detection of a clamped object when closing the window should lower the window by 100 mm.		x	x

[1] S.M. Prabhu, and P.J. Mosterman. Model-Based Design of a Power Window System: Modeling , Simulation , and Validation. In Society for Experimental Machines IMAC Conference, 2004
[2] National Highway Traffic Safety Administration. Federal Motor Vehicle Safety Standards; Power-Operated Window, Partition, and Roof Panel Systems. Docket No. NHTSA-2004-19032

Example – Power Window

- One functional requirement of the power window states that:

  Detection of a clamped object when closing the window should lower the window by 100 mm.

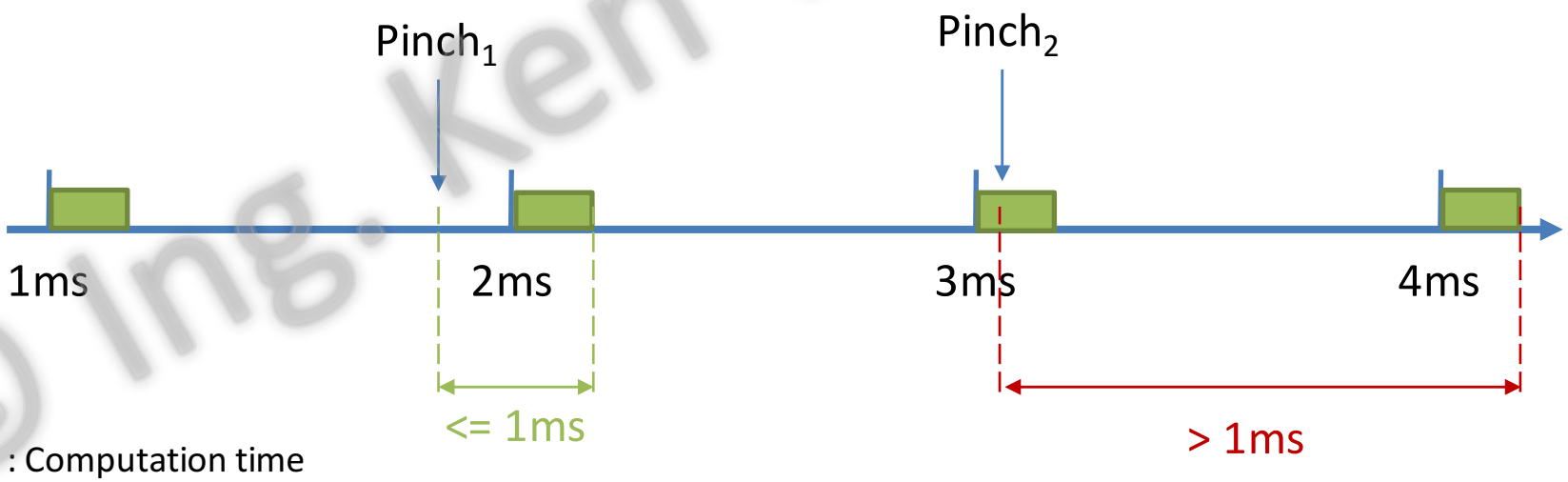
- Given this functional requirement, one may reason about **safety** and refines the above:
  - In the spatial dimension: if a clamped object is detected, the power window may continue to close for **maximum 0,2 mm**.
  - In the temporal dimension: given the dimensions of the window, safety can be guaranteed if the window will lower **within 1 ms.**

Naive Assumptions

… for the control engineer about the underlying platform:

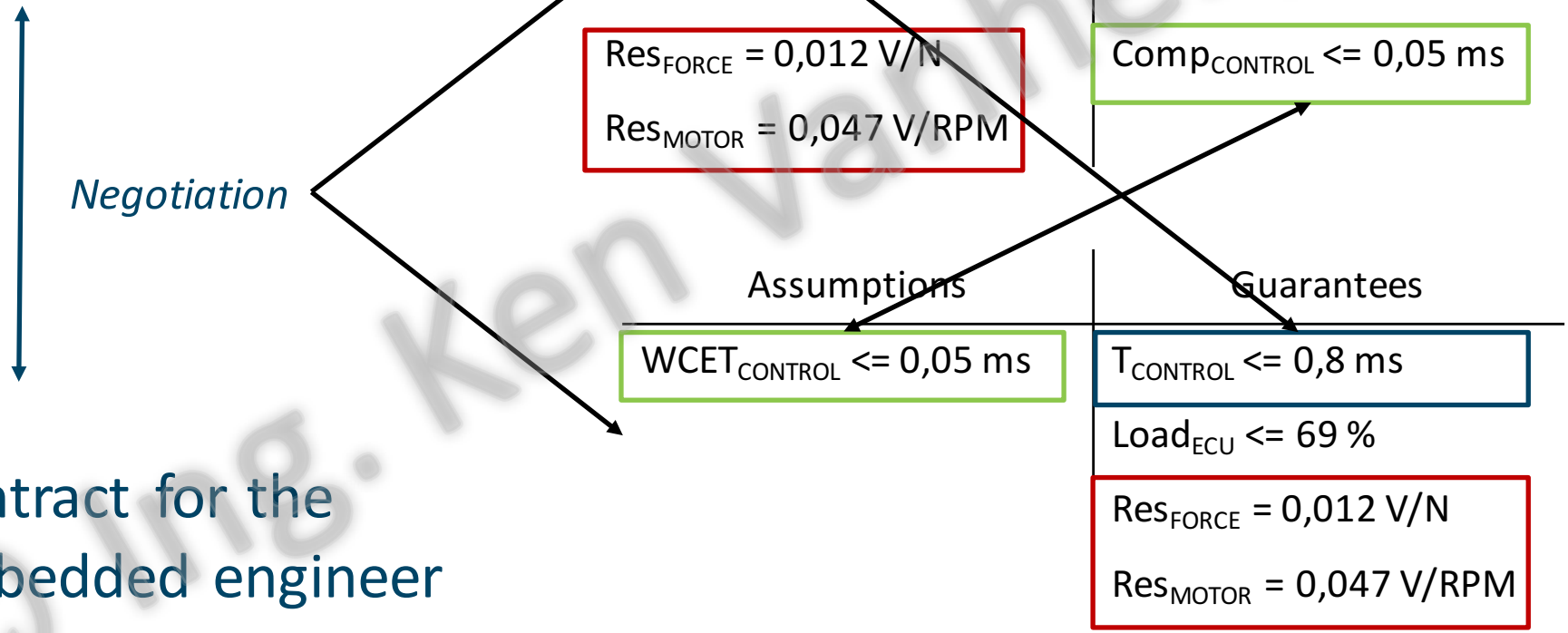
Assumptions	Guarantees
Sample time <= 1ms	Safety <= 0,2mm
	Reaction time <= 1ms

??Can this be guaranteed??



Example of a Vertical Contract

Contract for the control engineer



Contract for the embedded engineer

Contract-Based Design

Pros

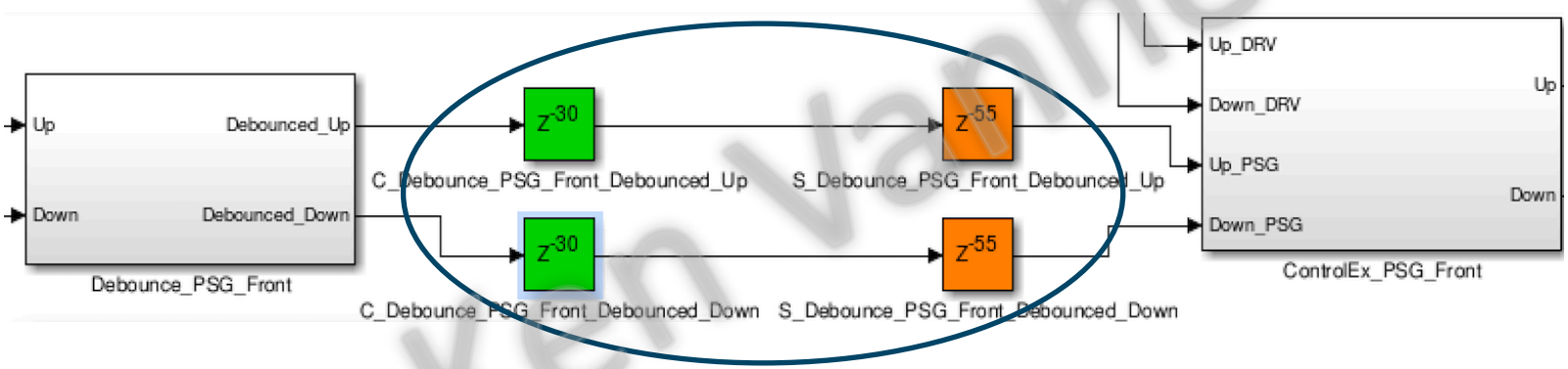
- Preliminary negotiation
- Set of assumptions and guarantees
- Maintain horizontal and vertical consistency
- Enables co-design

Cons

- What should be defined in a contract?
- Still hard to translate view-specific properties
- Lack of tool support

Tool Support – Round-Trip Engineering

Annotating/updating a Simulink model with hardware properties[3]:

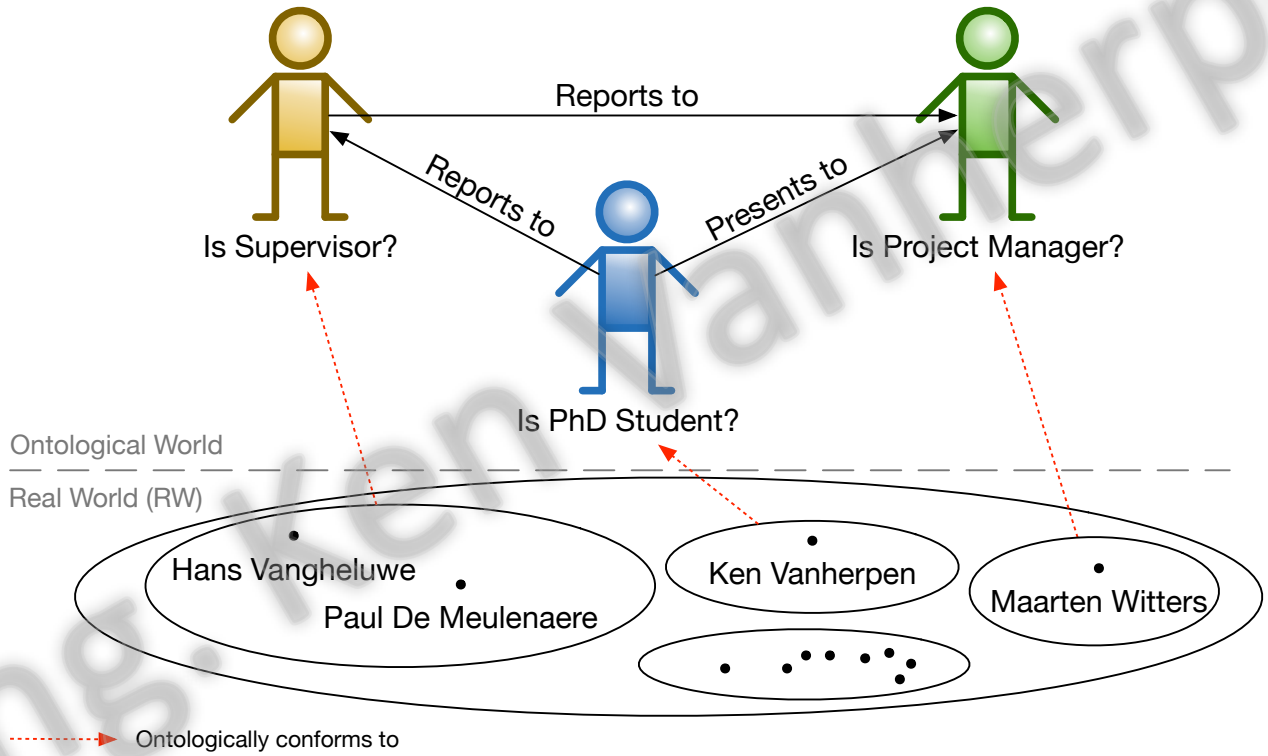


Lifted properties

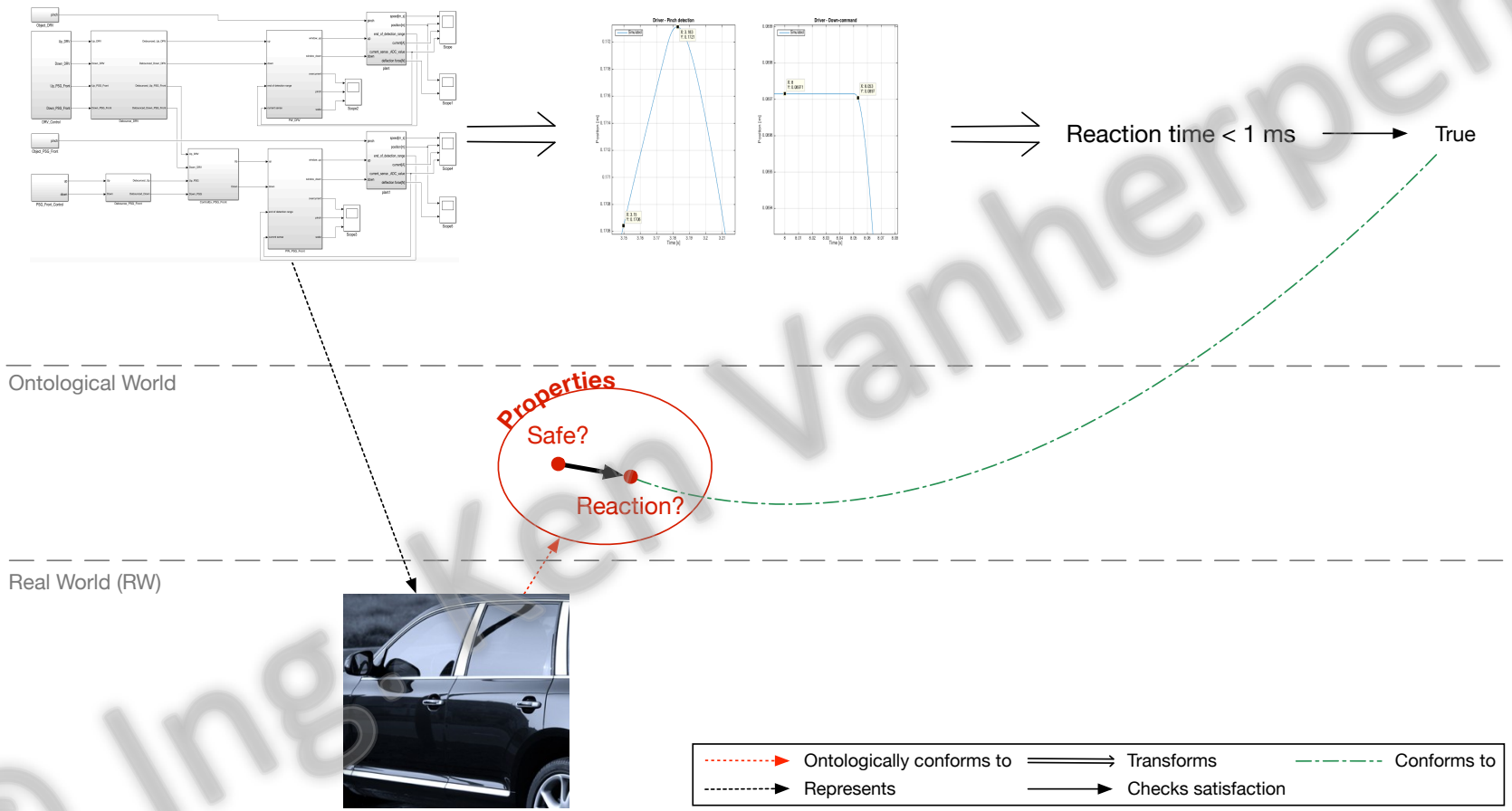
[3] K. Vanherpen, J. Denil, H. Vangheluwe, P. De Meulenaere, Model Transformations for Round-Trip Engineering in Control-Deployment Co-Design. Mod4Sim, 2015.

Ontological reasoning

What is an Ontology?

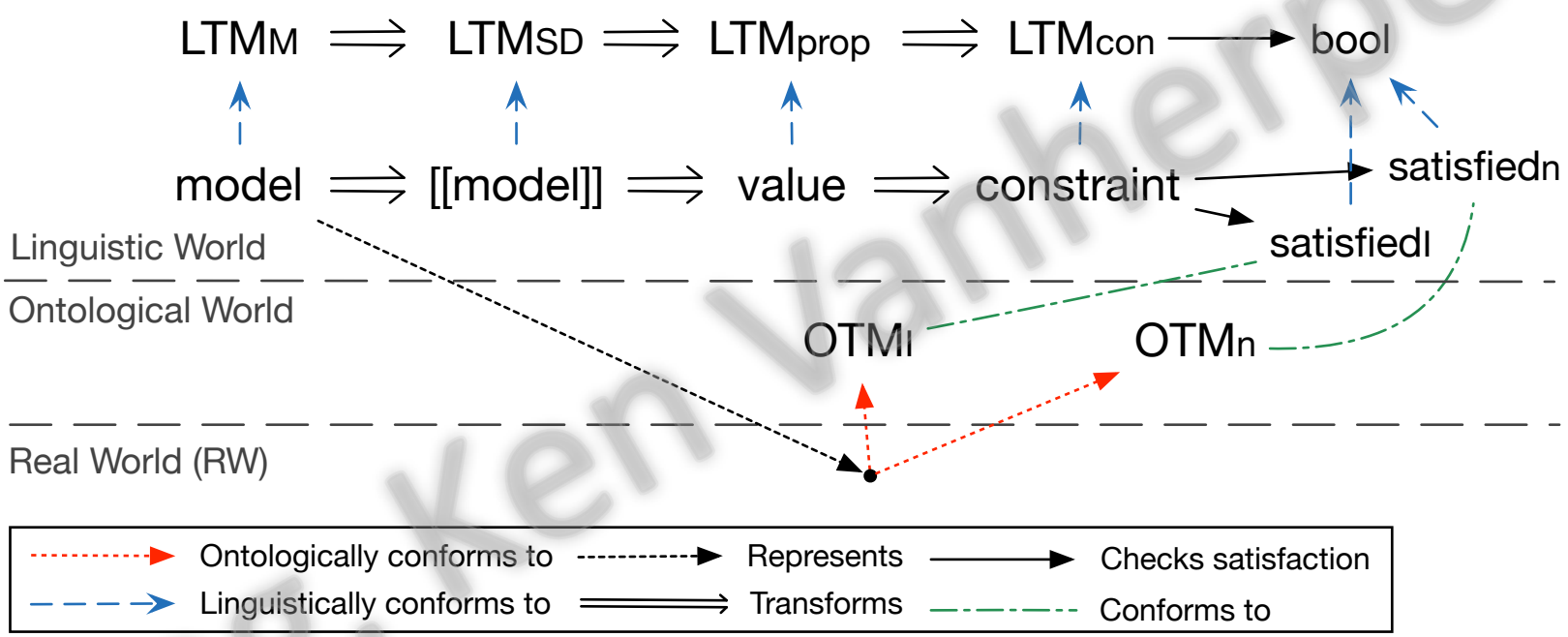


Ontological Reasoning in MBSE



Based on: [4] B. Barroca, T. Kühne, and H. Vangheluwe. Integrating language and ontology engineering. In MPM'14, volume 1237 of CEUR, pages 77–86, September 2014.

Ontological reasoning in MBSE



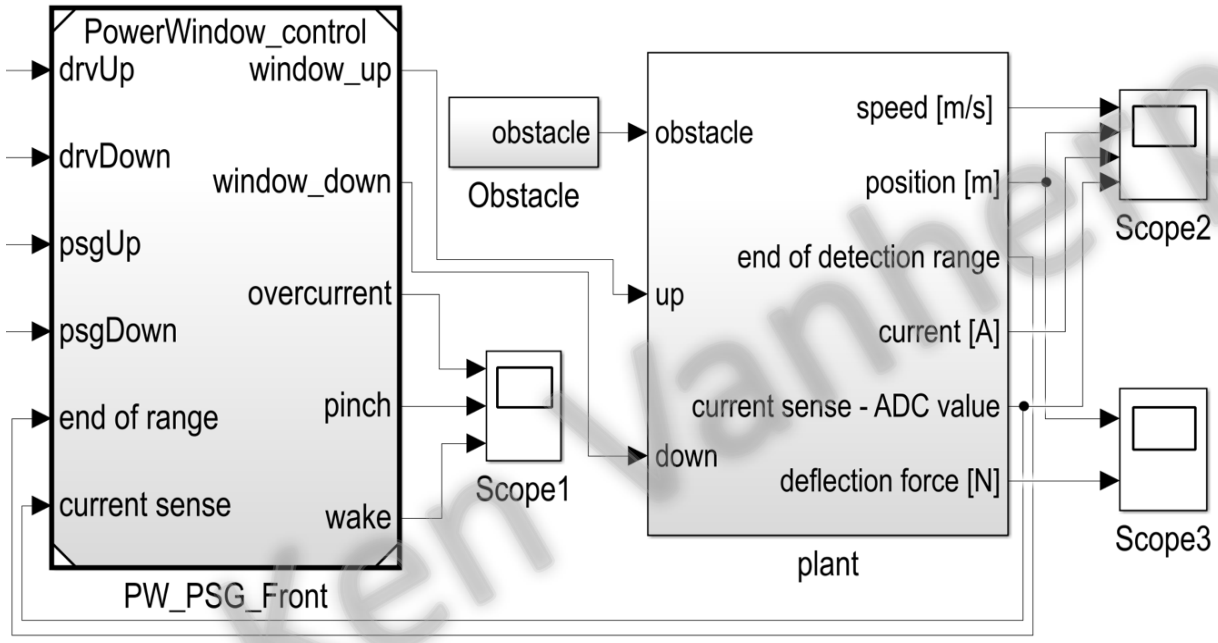
Based on: [4] B. Barroca, T. Kühne, and H. Vangheluwe. Integrating language and ontology engineering. In MPM '14, volume 1237 of CEUR, pages 77–86, September 2014.

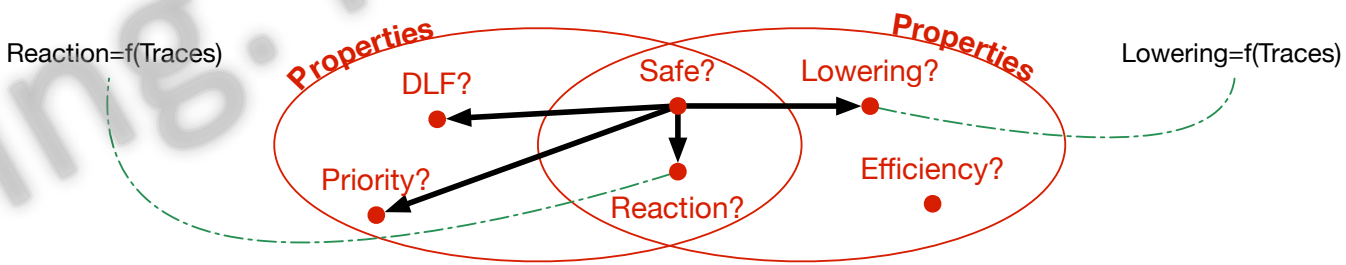
Ontological Reasoning in MBSE

Three fundamental relationships in design processes:

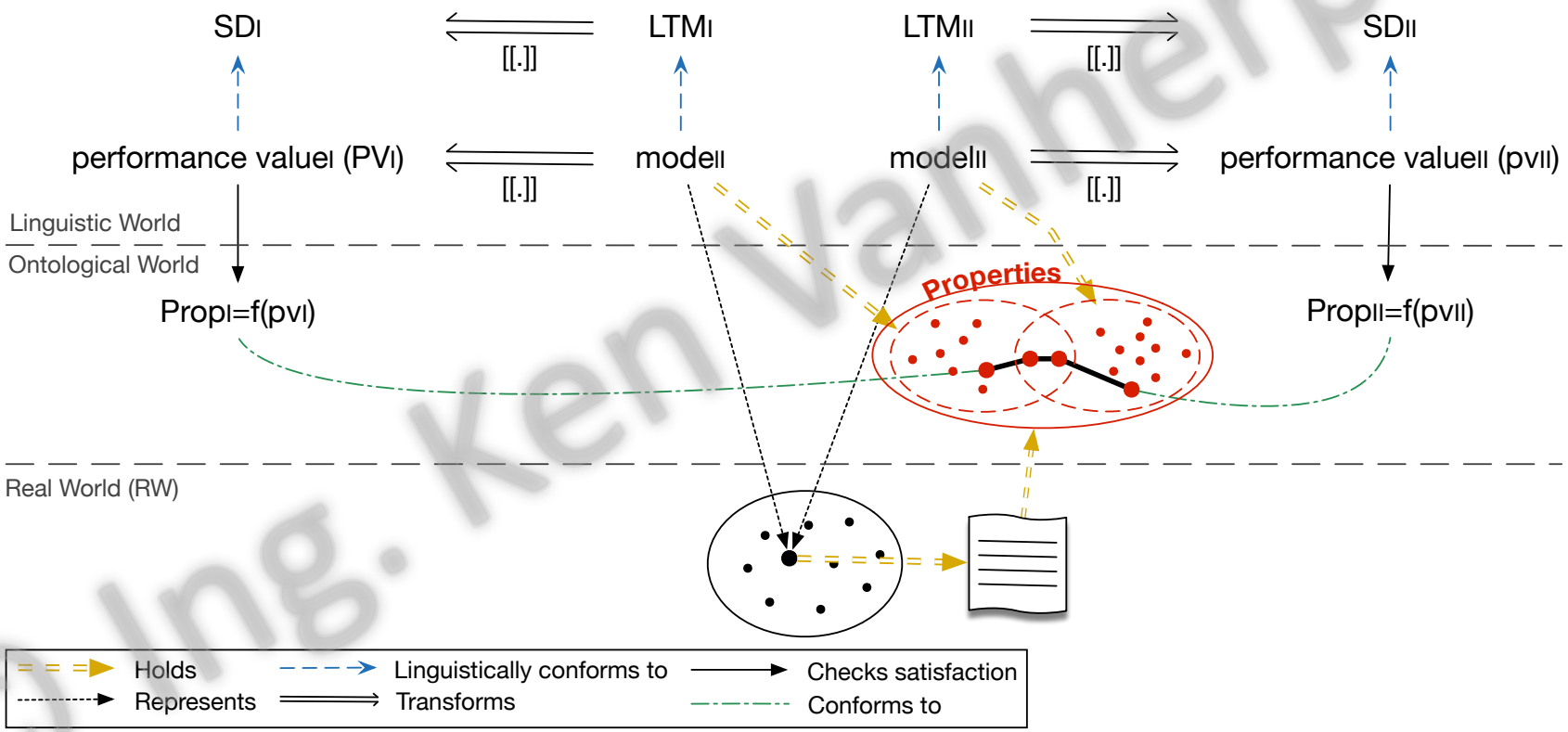
- Multi-Semantics (MS)
- Multi-Abstraction (MA)
- Multi-View (MV)

Ontological Reasoning in MBSE
Multi-View (MV) – example

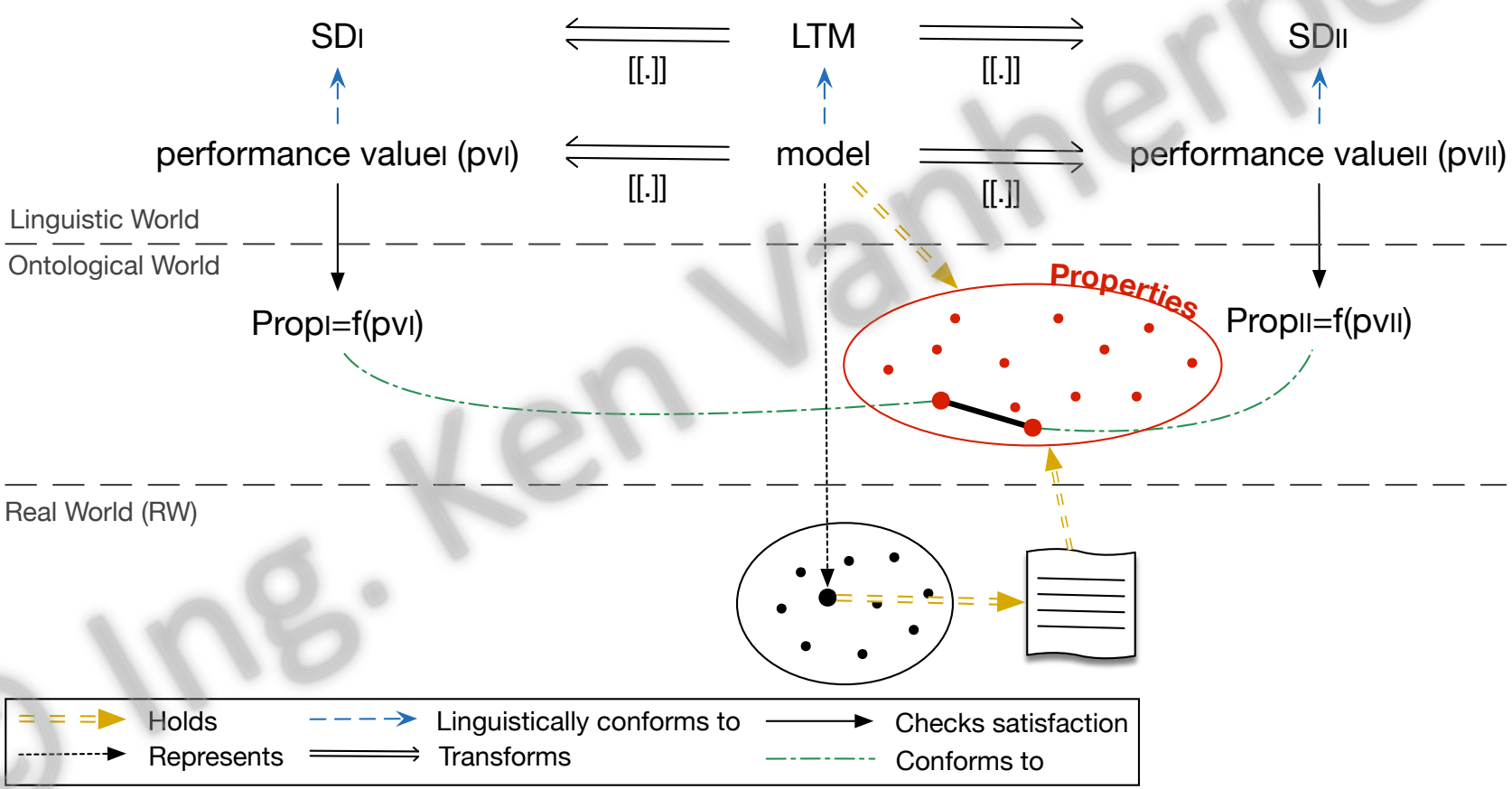




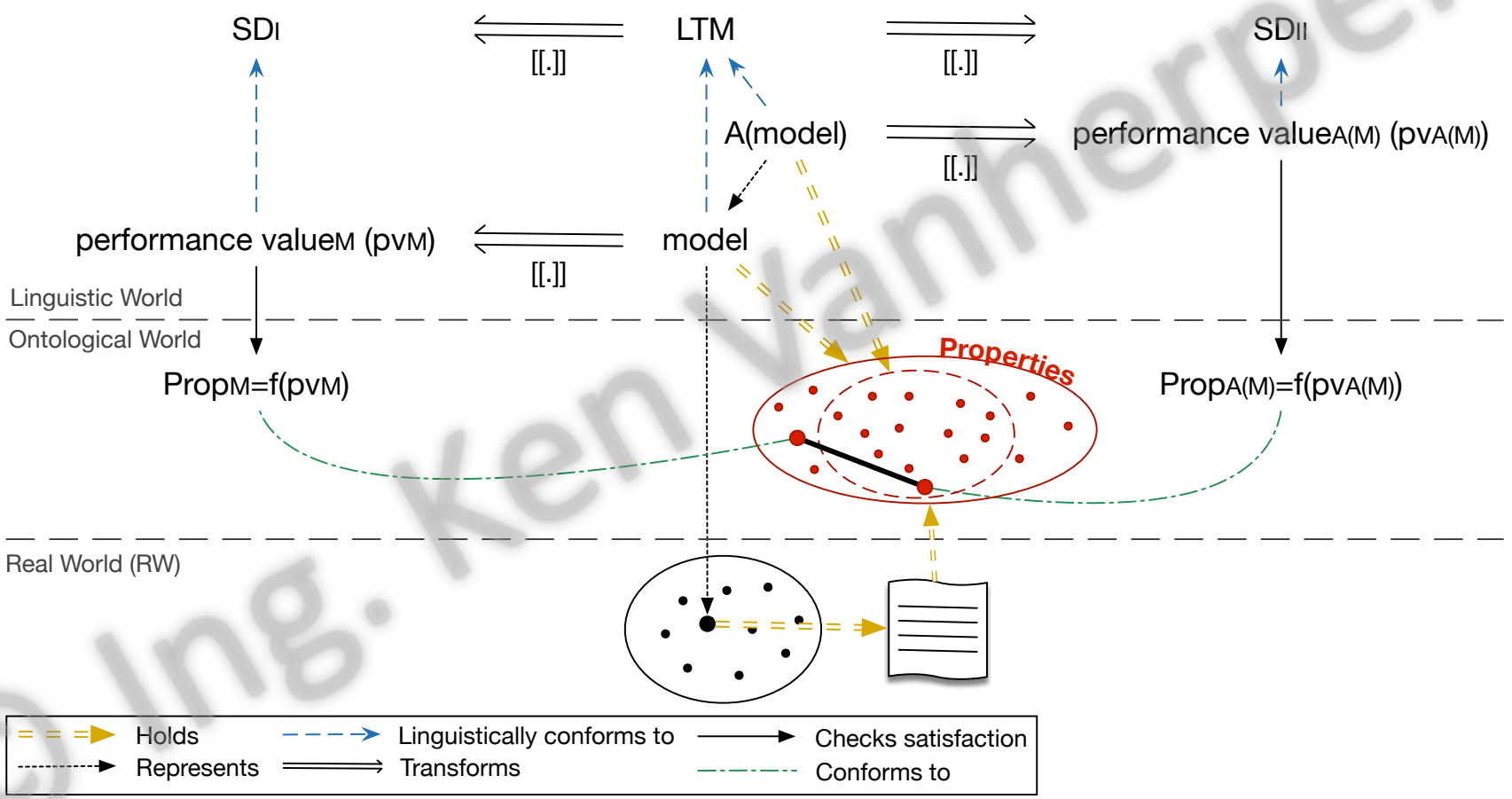
Ontological Reasoning in MBSE Multi-View (MV)



Ontological Reasoning in MBSE
Multi-Semantics (MS)



Ontological Reasoning in MBSE Multi-Abstraction (MA)



Power window revisited

Power Window – Negotiation Phase

Control Design

- Given the functional requirement, one may reason about **safety** and refines the above:
  - In the spatial dimension: if a clamped object is detected, the power window may continue to close for **maximum 0,2 mm**.
  - In the temporal dimension: given the dimensions of the window, safety can be guaranteed if the window will lower **within 1 ms.**

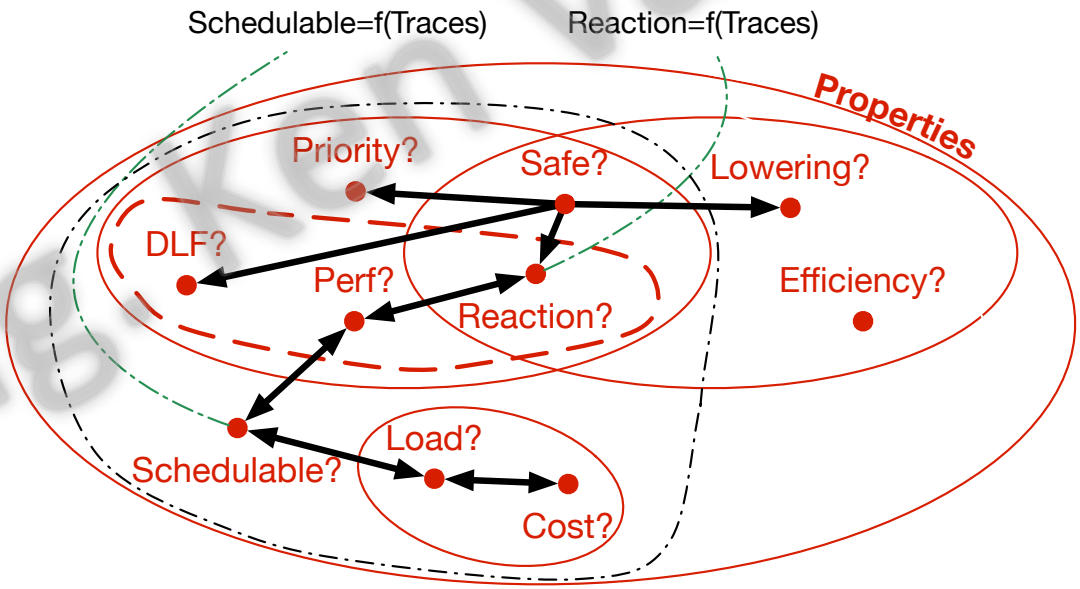
Embedded Design

- Embedded engineer is constrained by:
  - **The cost of a hardware architecture**
  - **The load of a processor (~safety)**: given a set of tasks, the load of a processor must be lower than **69%**

Power Window – Ontology

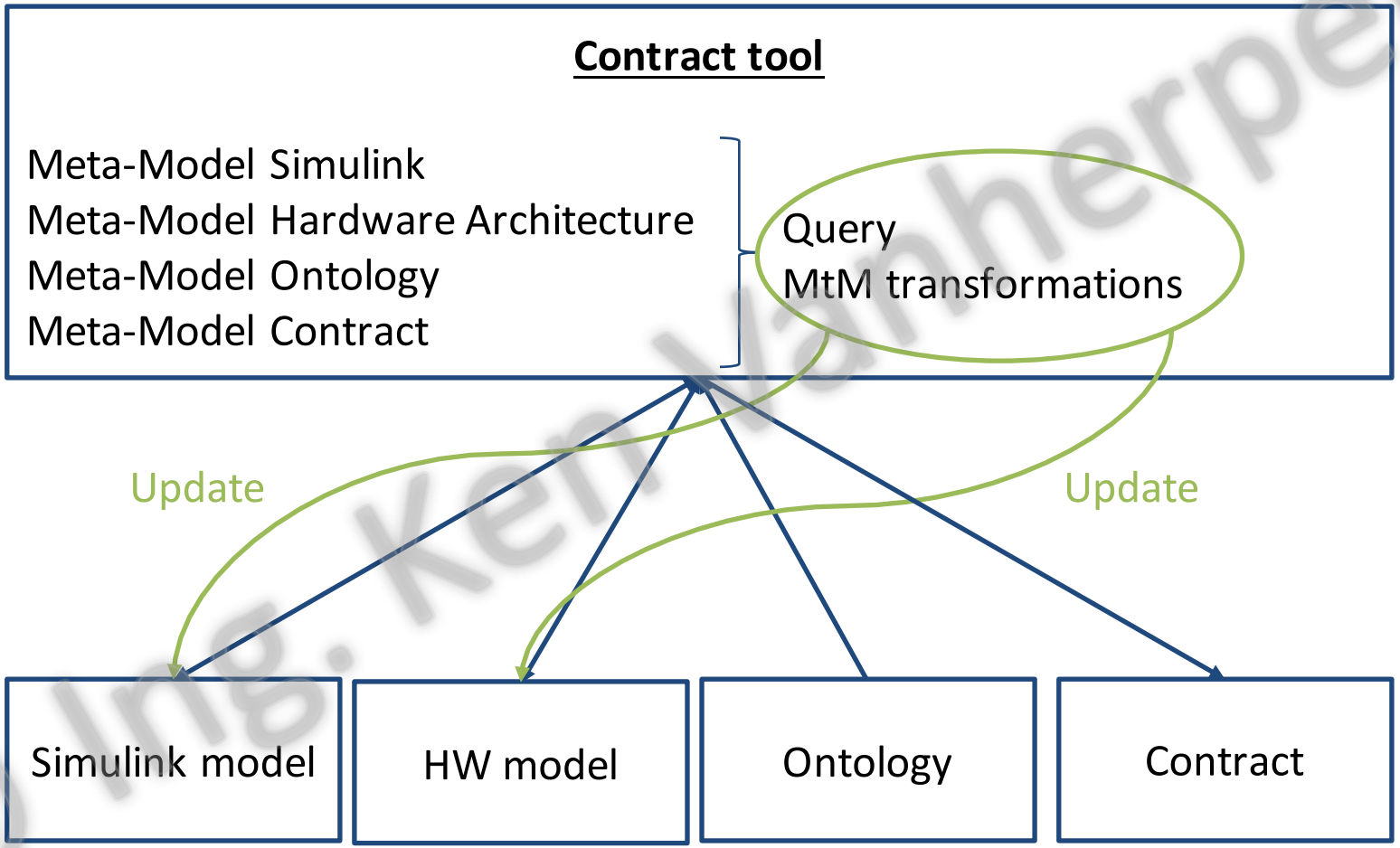
This results in an ontology which allows us to reason at the same level about:

- Multi-Semantics
- Multi-Abstraction
- Multi-View



Future Work

Tool Support



Tool Support

Integrate the Round-Trip Engineering method

Integrate Design-Space Exploration

Link with Inconsistency Management

Conclusion

Conclusion

We make the domain knowledge explicit using ontological properties

We make the ontological influence interrelations explicit

We trace back domain properties at the modelling level

We are developing tools which enable control-deployment co-design

Publications

K. Vanherpen, J. Denil, P. De Meulenaere, and H. Vangheluwe, “Design-Space Exploration in Model Driven Engineering – an Initial Pattern Catalogue”, *CMSEBA*, 2014.

K. Vanherpen, J. Denil, H. Vangheluwe and P. De Meulenaere, “Model Transformations for Round-Trip Engineering in Control Deployment Co-Design”, 2015.

K. Vanherpen et al., “Ontological Reasoning for Consistency in the Design of Cyber-Physical Systems”.

Thank you

Ing. Ken Vanherpen | ken.vanherpen@uantwerpen.be
http://msdl.cs.mcgill.ca/people/ken/