GEFÖRDERT DURCH DIE DFG Deutsche Forschungsgemeinschaft

CONVIDE CRC 1608

TOWARDS FORMALIZING AND RELATING DIFFERENT NOTIONS OF CONSISTENCY IN CYBER-PHYSICAL SYSTEMS ENGINEERING

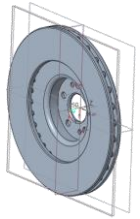
Kevin Feichtinger[1], Karl Kegel[2], Romain Pascual[1], Uwe Aßmann[2], Bernhard Beckert[1], and Ralf Reussner[1]

[1]Karlsruhe Institute of Technology
[2]Dresden University of Technology

CYBER-PHYSICAL SYSTEMS ENGINEERING

CONVIDE CRC 1608

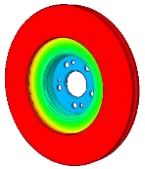
3D Construction View

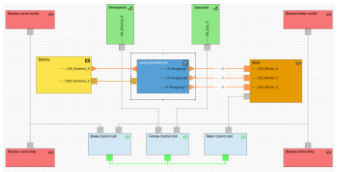


Dependencies between physical aspects

XiL Test Deployment View

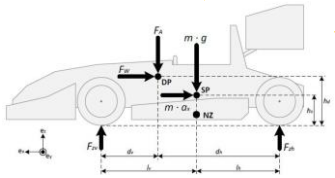
FE Analysis View

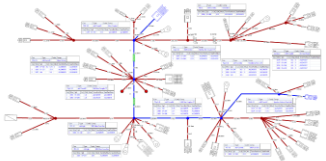




PREEvision E/E Topology View

Vehicle Model View

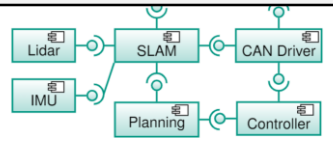


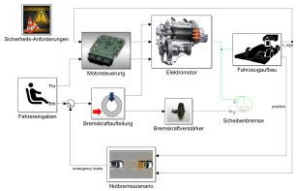


PREEvision Wiring Harness View

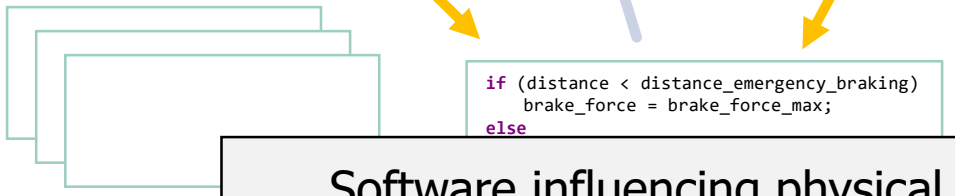
Differences between structure and behavior

Driving Functions Components View





Simulink Block Diagram View



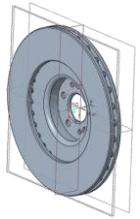
...

Software influencing physical properties

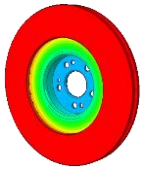
CYBER-PHYSICAL SYSTEMS ENGINEERING

CONVIDE CRC 1608

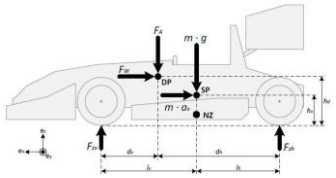
3D Construction View



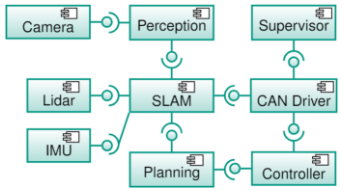
FE Analysis View



Vehicle Model View

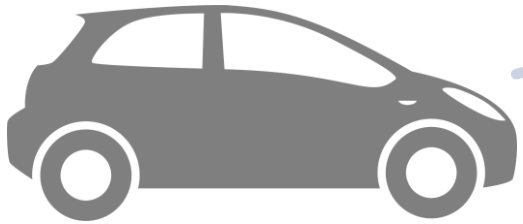


Autonomous Driving Functions Components View



...

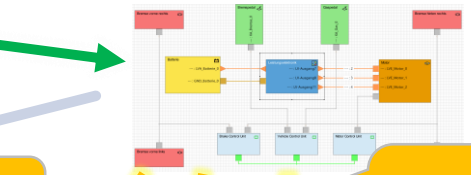
Manual Change



Analysis

Automatic Adaptation

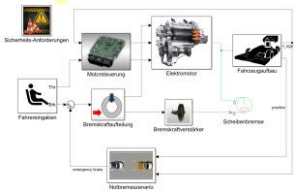
Hint / Interaction



PREEvision E/E Topology View

PREEvision Wiring Harness View

XiL Test Deployment View



Simulink Block Diagram View

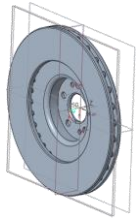
```
if (distance < distance_emergency_braking)
    brake_force = brake_force_max;
else
    brake_force = 0;
end
```

Source Code View

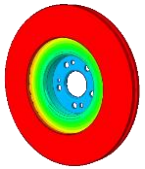
VIRTUAL SINGLE UNDERLYING MODEL (V-SUM)

CONVIDE CRC 1608

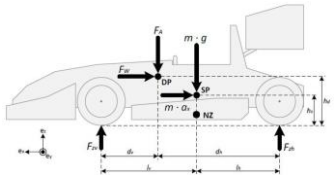
3D Construction View



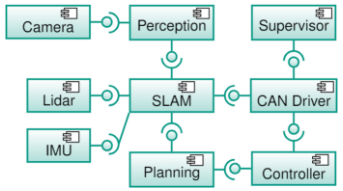
FE Analysis View

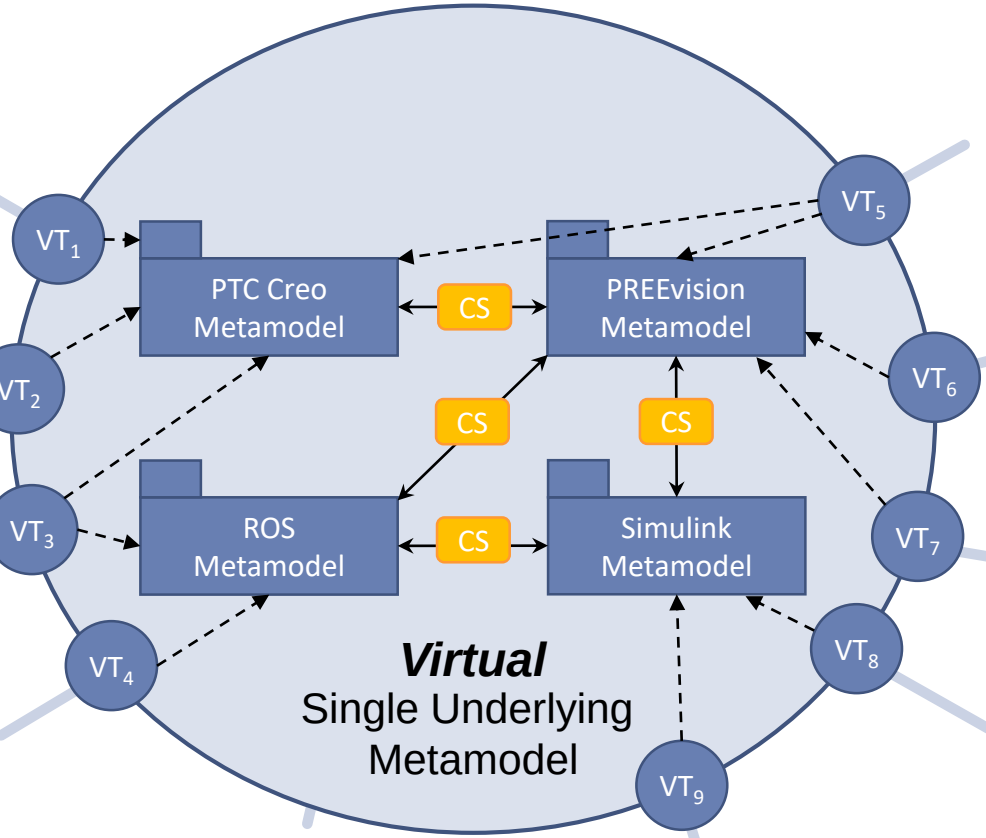


Vehicle Model View

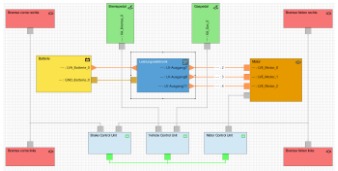


Autonomous Driving Functions Components View

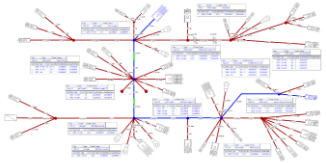




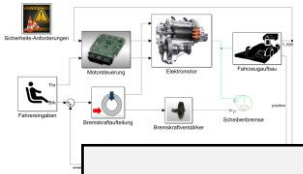
XiL Test Deployment View



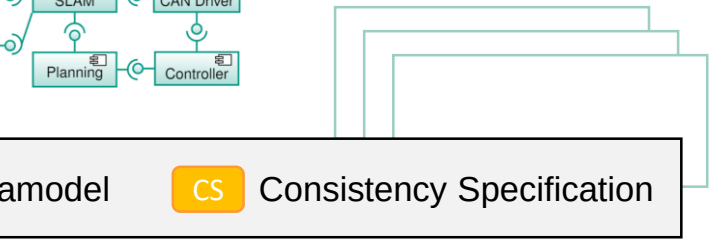
PREEvision E/E Topology View



PREEvision Wiring Harness View



Simulink Block Diagram View



```
if (distance < distance_emergency_braking)
    brake_force = brake_force_max;
else
    brake_force = 0;
end
```

Source Code View

#Metamodels < #View Types

Re-Usability
Compatibility with Standards

View Type | Metamodel | CS Consistency Specification

PROBLEM AND RESEARCH QUESTIONS

- Various domains have dealt with consistency and its definition, e.g., databases
- Different paradigms for specifying consistency exist
- Missing overview hinders adoption for Cyber-Physical Systems

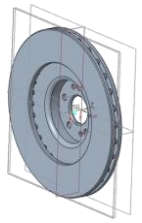
RQ1 How can the different paradigms for specifying consistency relations be combined in a single formal framework of consistency notions?

RQ2 How can such a framework of consistency notions be applied in a V-SUM to enable consistency aware, view-based development of Cyber-Physical Systems?

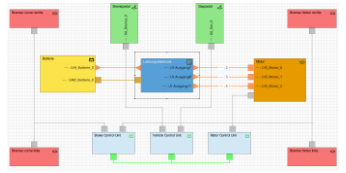
MULTIDIMENSIONAL CONSISTENCY

- Binary vs. N-ary
  We need a shift from binary to n-ary consistency specification as consistency questions may relate more than two models

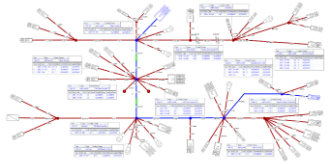
3D Construction View



Models depend on each other



PREEvision E/E Topology View

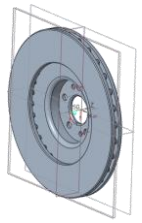


PREEvision Wiring Harness View

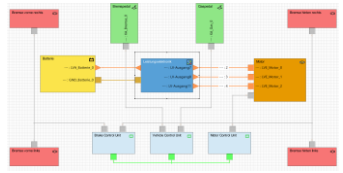
MULTIDIMENSIONAL CONSISTENCY

- Binary vs. N-ary
- Normative vs. Descriptive
  We need a shift from normative to descriptive consistency specifications to enable reasoning about their correctness

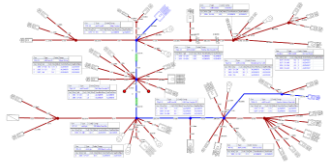
3D Construction View



Describe circular model dependencies



PREEvision E/E Topology View

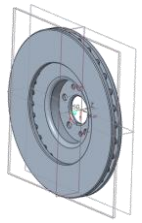


PREEvision Wiring Harness View

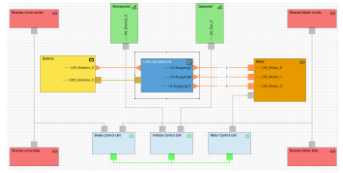
MULTIDIMENSIONAL CONSISTENCY

- Binary vs. N-ary
- Normative vs. Descriptive
- Qualitative vs. Quantitative
  We need a shift from Boolean assessment of consistency to quantitative metrics to reflect the complexity of Cyber-Physical Systems and propose consistency-increasing methods

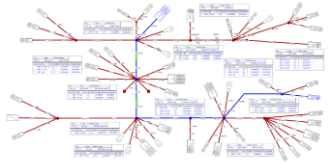
3D Construction View



Temporal inconsistencies are unavoidable



PREEvision E/E Topology View

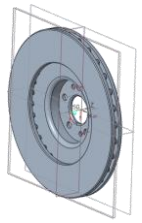


PREEvision Wiring Harness View

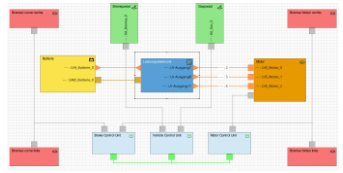
MULTIDIMENSIONAL CONSISTENCY

- Binary vs. N-ary
- Normative vs. Descriptive
- Qualitative vs. Quantitative
- Certainty vs. Uncertainty
  We need a shift from precisely defined models to models encoding uncertainty to account for the physical part of the system

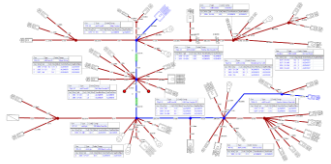
3D Construction View



Certification duration creates uncertainty



PREEvision E/E Topology View



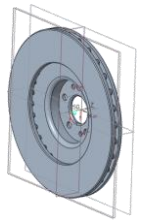
PREEvision Wiring Harness View

MULTIDIMENSIONAL CONSISTENCY

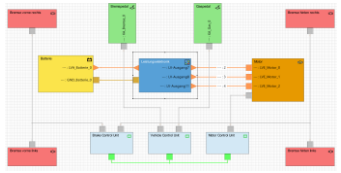
- Binary vs. N-ary
- Normative vs. Descriptive
- Qualitative vs. Quantitative
- Certainty vs. Uncertainty
- Syntax vs. Semantics

We need a shift from consistency of the model structure to behavioural aspects to allow for quality reasoning

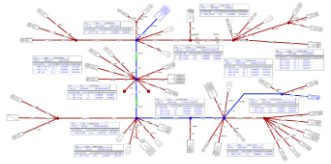
3D Construction View



Inconsistencies among derived values



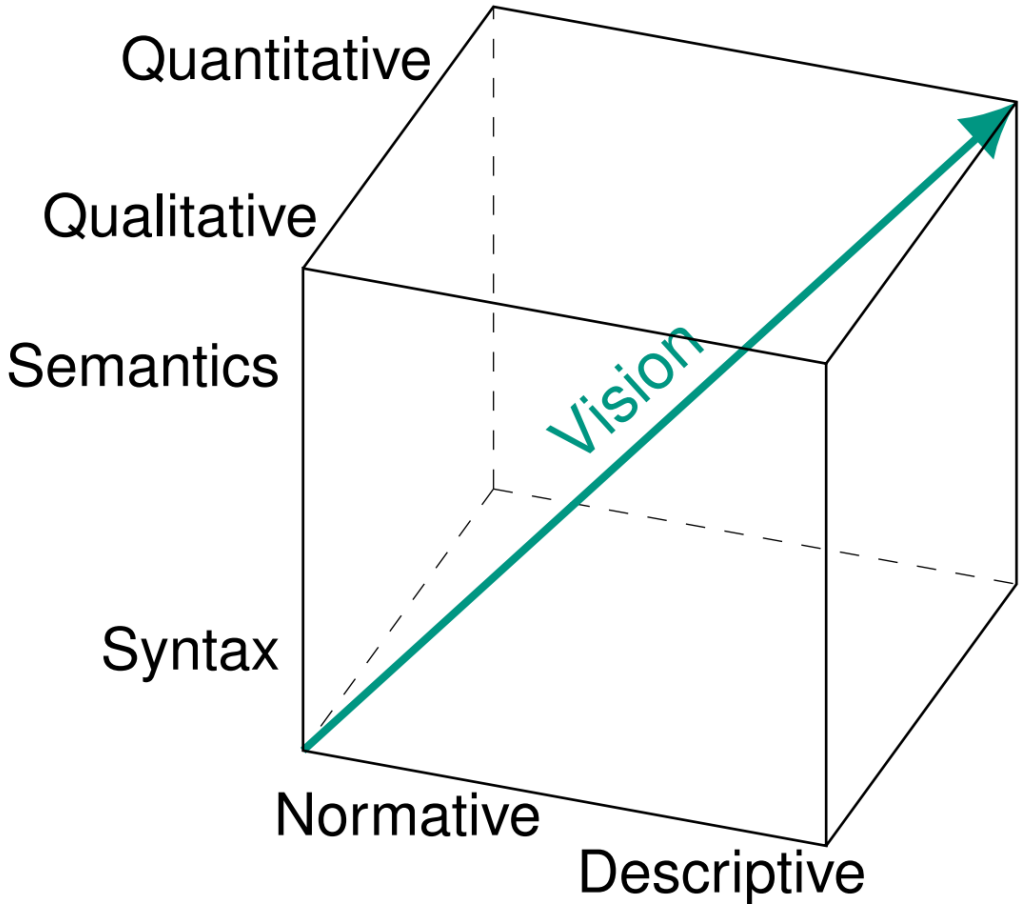
PREEvision E/E Topology View



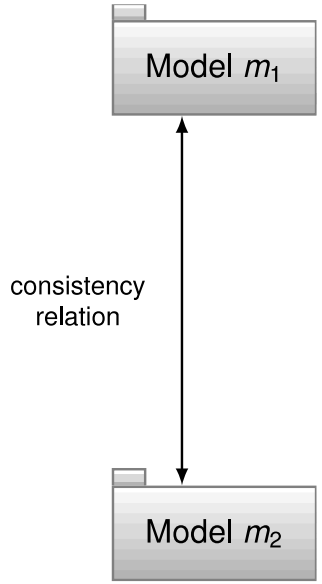
PREEvision Wiring Harness View

MULTIDIMENSIONAL CONSISTENCY

- Binary vs. N-ary
  Reason about multiple models
- Normative vs. Descriptive
  Reason about correctness
- Qualitative vs. Quantitative
  Reason about consistency-increasing methods
- Certainty vs. Uncertainty
  Reason about the physical part of the system
- Syntax vs. Semantics
  Reason about quality



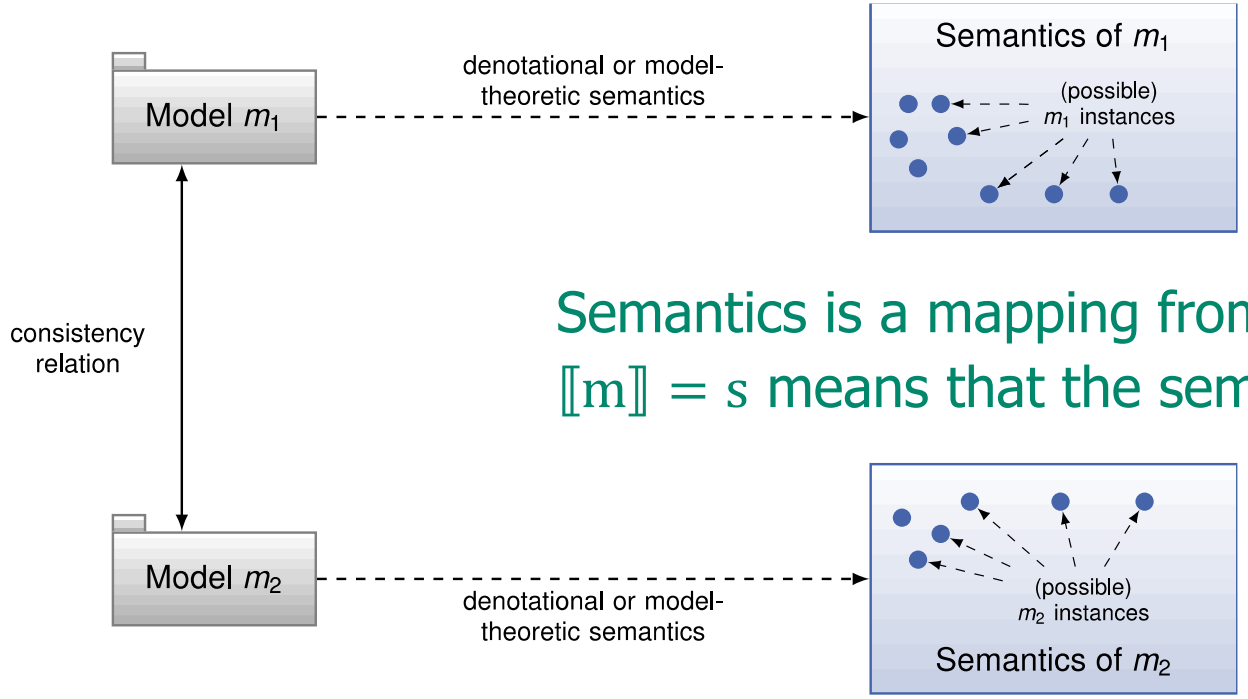
SYNTAX VS. SEMANTICS: FORMAL FOUNDATIONS OF CONSISTENCY



CR(m_1, m_2) means that m_1 and m_2 are consistent

Formal Foundations of Consistency in Model-Driven Development. Romain Pascual, Bernhard Beckert, Mattias Ulbrich, Michael Kirsten, Wolfram Pfeifer. Isola 2024

SYNTAX VS. SEMANTICS: FORMAL FOUNDATIONS OF CONSISTENCY

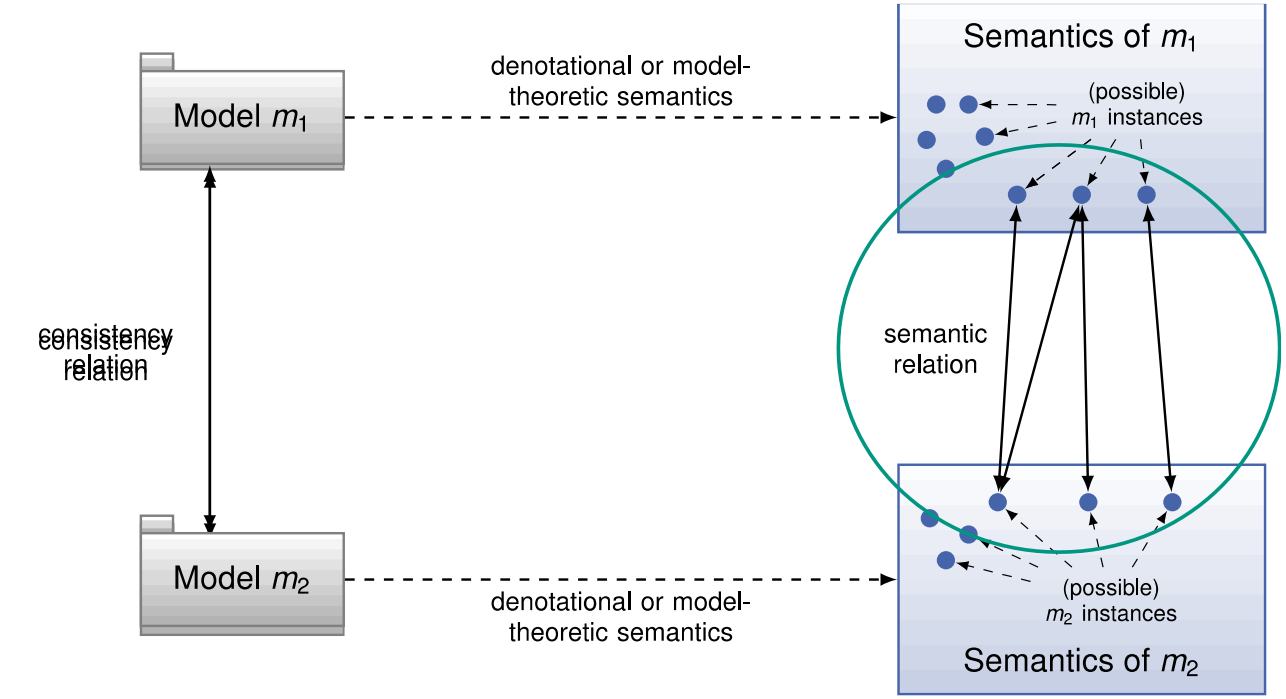


Semantics is a mapping from a model to some value $[\![-]\!]: \mathrm{M} \rightarrow \mathrm{S}$

$[\![\mathrm{m}]\!] = \mathrm{s}$ means that the semantics of m is s

Formal Foundations of Consistency in Model-Driven Development. Romain Pascual, Bernhard Beckert, Mattias Ulbrich, Michael Kirsten, Wolfram Pfeifer. Isola 2024

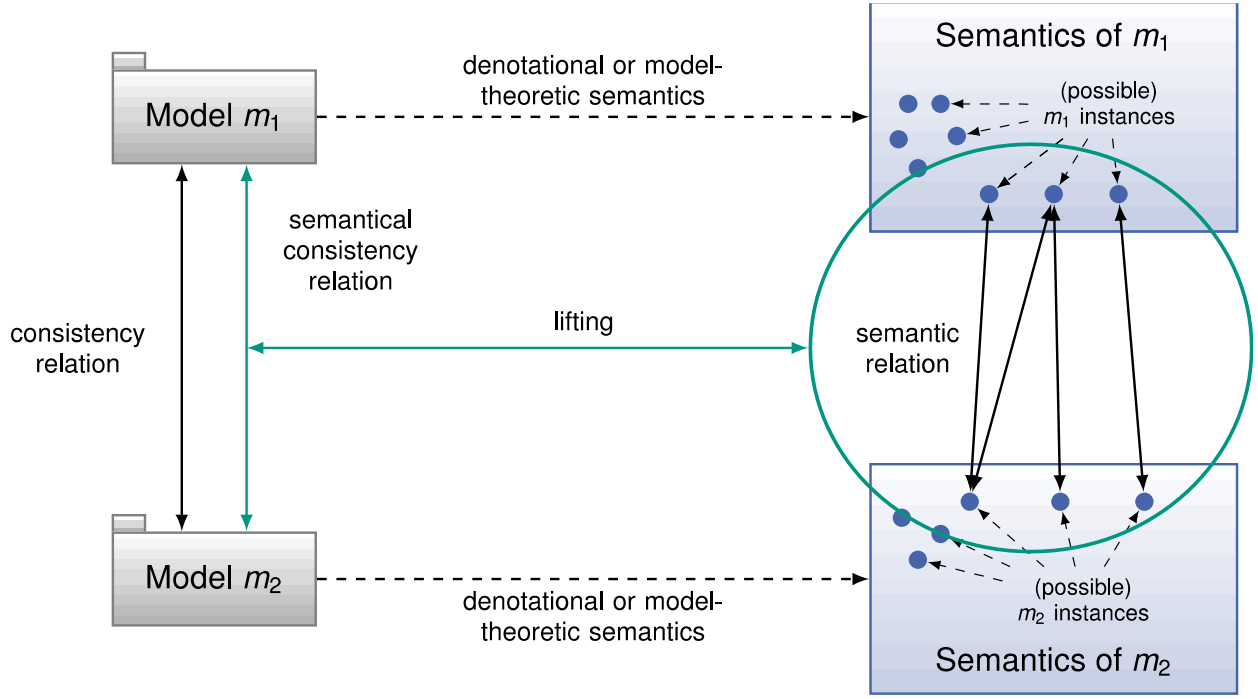
SYNTAX VS. SEMANTICS: FORMAL FOUNDATIONS OF CONSISTENCY



SR(s_1, s_2) means that the semantic values s_1 and s_2 are related (overlap)

Formal Foundations of Consistency in Model-Driven Development. Romain Pascual, Bernhard Beckert, Mattias Ulbrich, Michael Kirsten, Wolfram Pfeifer. Isola 2024

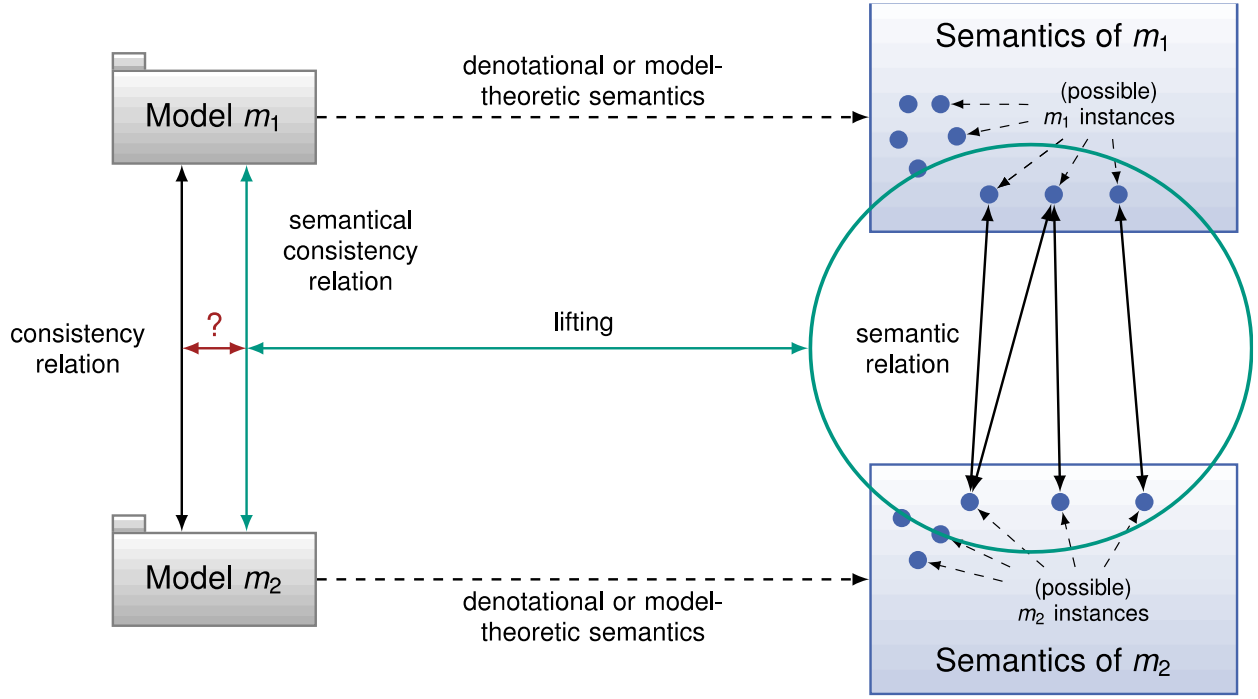
SYNTAX VS. SEMANTICS: FORMAL FOUNDATIONS OF CONSISTENCY



Tracing **SR** to the models and get **SCR**(m_1, m_2) given by $\mathbf{SR}([\![m_1]\!], [\![m_2]\!])$

Formal Foundations of Consistency in Model-Driven Development. Romain Pascual, Bernhard Beckert, Mattias Ulbrich, Michael Kirsten, Wolfram Pfeifer. Isola 2024

SYNTAX VS. SEMANTICS: FORMAL FOUNDATIONS OF CONSISTENCY



CR and **SCR** gives consistency on the models and their semantics.

We have to relate **CR** and **SCR**!

Formal Foundations of Consistency in Model-Driven Development. Romain Pascual, Bernhard Beckert, Mattias Ulbrich, Michael Kirsten, Wolfram Pfeifer. Isola 2024

VISION: CONSISTENCY-AWARE CYBER-PHYSICAL SYSTEMS ENGINEERING

- Find and classify different notions of consistency from different domains
- Formalize and relate these notions of consistency to each other
- Provide a common understanding implement within a V-SUM
- Investigate its effects on Cyber-Physical Systems Engineering