Karlsruhe Institute of Technology

CONVIDE CRC 1608

Formal Foundations of Consistency in Model-Driven Development

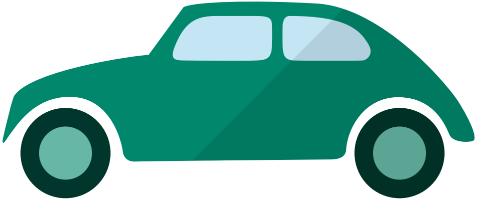
ISoLA 2024

R. Pascual, B. Beckert, M. Ulbrich, M. Kirsten, W. Pfeifer | October 29, 2024

Convide[1]

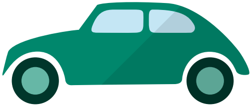
Consistency in the **Vi**ew-Based **De**velopment of Cyber-Physical Systems

- Software engineering
- Mechanical engineering
- Electrical engineering
- Formal methods

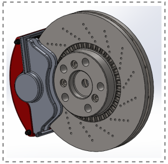


[1] Sonderforschungsbereich (SFB) financed by the Deutsche Forschungsgemeinschaft (DFG)

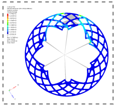
The Virtual Single Underlying Model methodology (V-SUM)



The Virtual Single Underlying Model methodology (V-SUM)

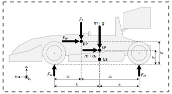


3D Brake Assembly View

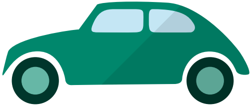


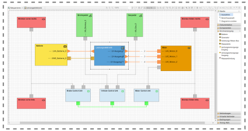
Tribological Simulation View

X-in-the-Loop Test Deployment View

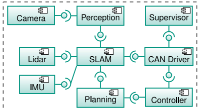


Simplified Vehicle Model View



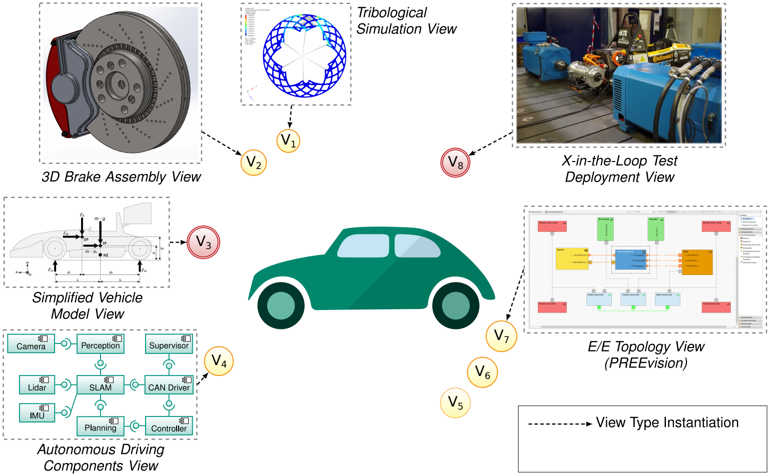


E/E Topology View (PREEvision)

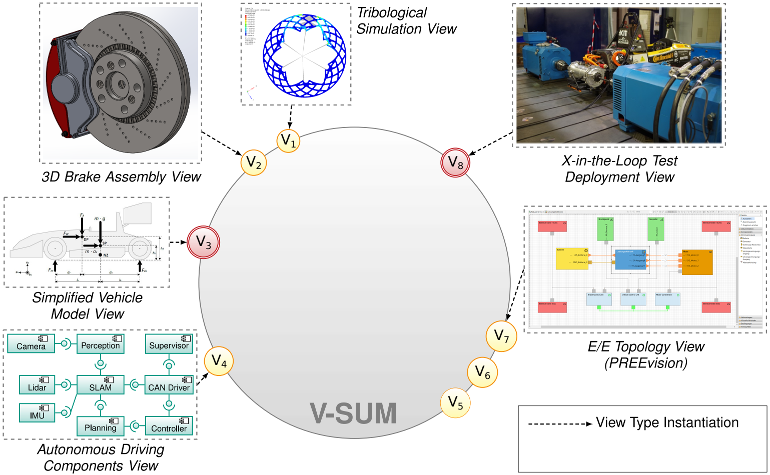


Autonomous Driving Components View

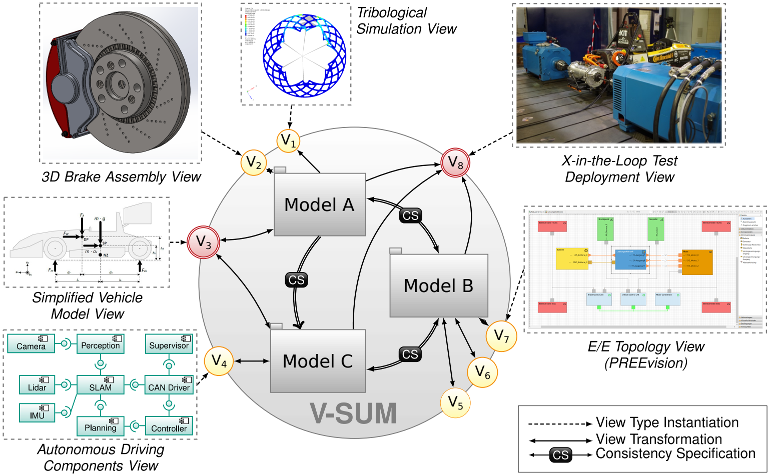
The Virtual Single Underlying Model methodology (V-SUM)



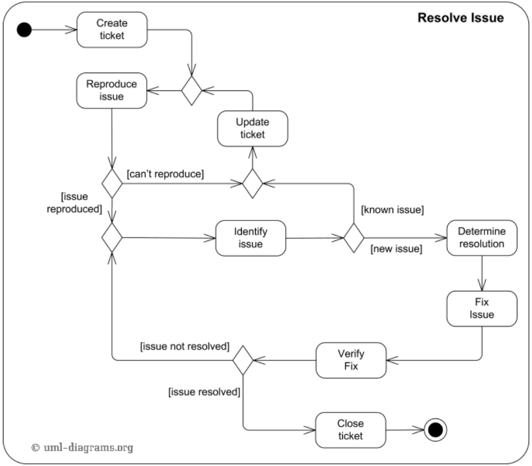
The Virtual Single Underlying Model methodology (V-SUM)



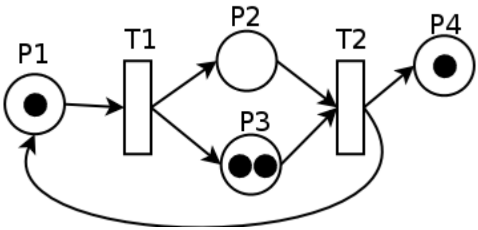
The Virtual Single Underlying Model methodology (V-SUM)



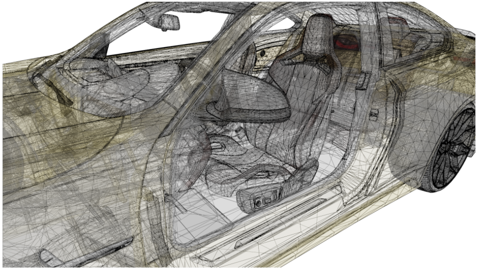
Models?

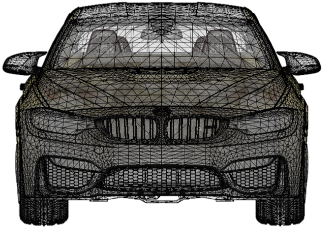

Resolve Issue
Create ticket
Reproduce issue
Update ticket
[can't reproduce]
[issue reproduced]
Identify issue
[known issue]
[new issue]
Determine resolution
Fix Issue
Verify Fix
[issue not resolved]
[issue resolved]
Close ticket
© uml-diagrams.org

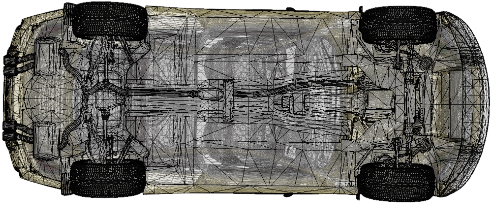
Models?



Models?



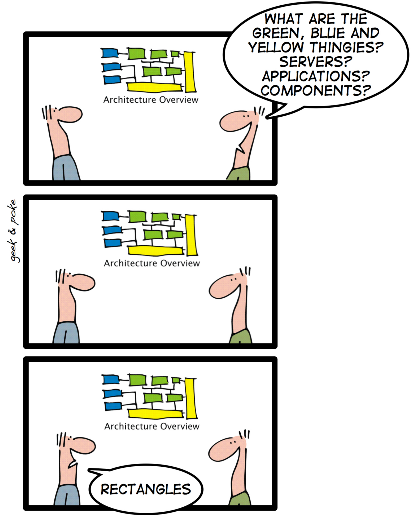




Models?

Models?

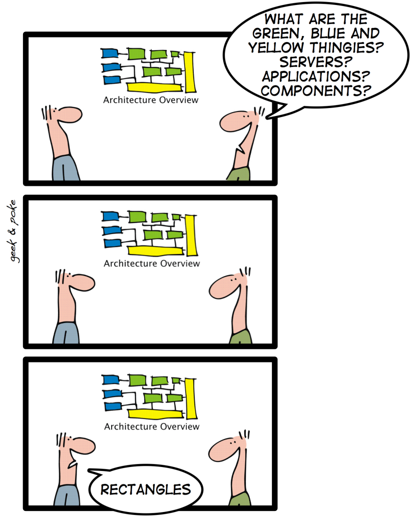
Contribution



Observations

- Multiple approaches and definitions
- Lack of a common understanding

Contribution

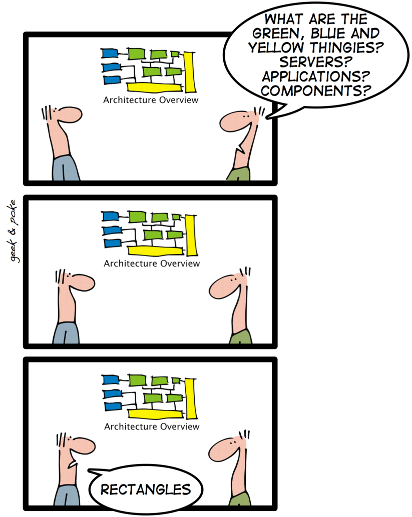


Observations

- Multiple approaches and definitions
- Lack of a common understanding

Common terminology for the project

Contribution



Observations

- Multiple approaches and definitions
- Lack of a common understanding

Common terminology for the project

Contribution: a formal framework of consistency in model-driven development

Formalizing the V-SUM approach

- A set-theoretic approach to V-SUM consistency

Definitions

Models are atomic entities, belonging to a meta-model and related by consistency

Definitions

Karlsruhe Institute of Technology

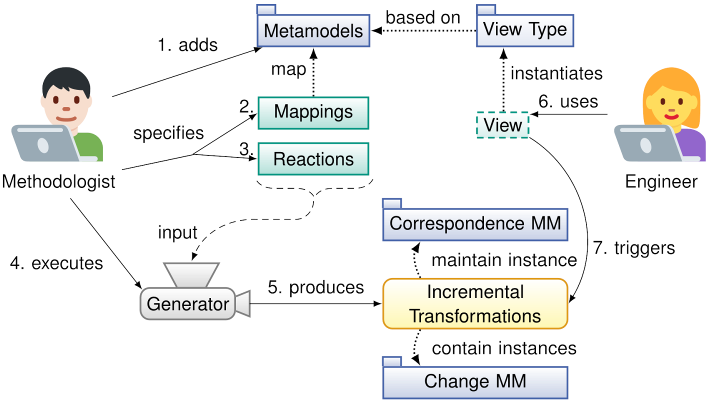
Models are atomic entities, belonging to a meta-model and related by consistency

- A **meta-model** M_i is the set of its well-formed models $m_i \in M_i$
- A **consistency relation** is a relation on a (finite) number of meta-models: $CR \subseteq \prod_{i \leq n} M_i$
- A **V-SUM meta-model** is a pair $\mathcal{V} = (V, CR)$ where $V = \prod_{i \leq n} M_i$ and $CR \subseteq V$
- A **V-SUM model** v of a V-SUM meta-model $\mathcal{V}$ is a tuple $v = (m_1, \ldots, m_n)$ of models $m_i \in M_i$
- A V-SUM model v is **consistent** wrt. CR if $v \in CR$, written $CR(v)$

Rule-based description of consistency

- The Vitruvius approach

Consistency preservation with Vitruvius [Klare et al. 2021]



- Consistency is defined at the meta-level by the methodologist

Consistency from semantics

- Semantical V-SUM

Semantics

Semantics with Java programs as models

- **trace semantics**

Semantics

Semantics with Java programs as models

- **trace semantics**
- **pre** and **post** conditions

Semantics

Semantics with Java programs as models

- **trace semantics**
- **pre** and **post** conditions
- **result** of **tests**

Semantics

Semantics with Java programs as models

- **trace semantics**
- **pre** and **post** conditions
- **result** of **tests**
- **termination** property

Semantics

Semantics with Java programs as models

- **trace semantics**
- **pre** and **post** conditions
- **result** of **tests**
- **termination** property
- **number of methods** or **attributes** of a class

Semantics

Semantics with Java programs as models

- **trace semantics**
- **pre** and **post** conditions
- **result** of **tests**
- **termination** property
- **number of methods** or **attributes** of a class

Abstract semantics

$$[\![\cdot]\!]: M \to S$$

M meta-model and S semantic space

Semantics

Semantics with Java programs as models

- **trace semantics**
- **pre** and **post** conditions
- **result** of **tests**
- **termination** property
- **number of methods** or **attributes** of a class

Abstract semantics

$$[\![\cdot]\!] : M \to S$$

M meta-model and S semantic space

It is purpose-dependent

How can we use semantics to define consistency?

Impose conditions on the semantic spaces!

How can we use semantics to define consistency?

Impose conditions on the semantic spaces!

A **semantic consistency relation** is a relation $SCR \subseteq \prod_{i \leq n} S_i$

- $v = (m_1, \ldots, m_n)$ in $V = \prod_{i \leq n} M_i$ is semantically consistent wrt. SCR if

$$SCR([\![m_1]\!]_1, \ldots, [\![m_n]\!]_n)$$

How can we use semantics to define consistency?

Impose conditions on the semantic spaces!

A **semantic consistency relation** is a relation $SCR \subseteq \prod_{i \leq n} S_i$

- $v = (m_1, \ldots, m_n)$ in $V = \prod_{i \leq n} M_i$ is semantically consistent wrt. SCR if

$$SCR([\![m_1]\!]_1, \ldots, [\![m_n]\!]_n)$$

We obtain a consistency relation CR_{SCR} on V

Reasoning on semantics

- A little bit of lattice theory

Main findings

For any meta-model and any consistency relation, there is a **natural semantics** that captures exactly the information needed to evaluate consistency of models

Main findings

Karlsruhe Institute of Technology

For any meta-model and any consistency relation, there is a **natural semantics** that captures exactly the information needed to evaluate consistency of models

- **1.** Semantics that contain enough information to distinguish between consistent and inconsistent models form a bounded lattice

Main findings

For any meta-model and any consistency relation, there is a **natural semantics** that captures exactly the information needed to evaluate consistency of models

- **1.** Semantics that contain enough information to distinguish between consistent and inconsistent models form a bounded lattice
- **2.** The natural semantics is the bottom element of the lattice

Irrelevance of the representation

m_1 and m_2 in M are equal modulo $[\![\cdot]\!]$:

$$m_1 \equiv m_2 \iff [\![m_1]\!] = [\![m_2]\!]$$

Irrelevance of the representation

m_1 and m_2 in M are equal modulo $\llbracket \cdot \rrbracket$:

$$m_1 \equiv m_2 \iff \llbracket m_1 \rrbracket = \llbracket m_2 \rrbracket$$

Factor out these equalities

Irrelevance of the representation

m_1 and m_2 in M are equal modulo $[\![\cdot]\!]$:

$$m_1 \equiv m_2 \iff [\![m_1]\!] = [\![m_2]\!]$$

Factor out these equalities

$$\begin{tikzcd} M \arrow[rr, "{[\![\cdot]\!]}"] \arrow[dr, "s"'] & & S \\ & M/\equiv \arrow[ur, "i"'] & \end{tikzcd}$$

Irrelevance of the representation

m_1 and m_2 in M are equal modulo $[\![\cdot]\!]$:

$$m_1 \equiv m_2 \iff [\![m_1]\!] = [\![m_2]\!]$$

Factor out these equalities

$$\begin{tikzcd} M \arrow[rr, "{[\![\cdot]\!]}"] \arrow[dr, "s"'] & & S \\ & M/\!\equiv \arrow[ur, "i"'] & \end{tikzcd}$$

S and $M/\!\equiv$ made isomorphic by formal restricting S to the image of $[\![\cdot]\!]$

Irrelevance of the representation

m_1 and m_2 in M are equal modulo $[\![\cdot]\!]$:

$$m_1 \equiv m_2 \iff [\![m_1]\!] = [\![m_2]\!]$$

Factor out these equalities

$$\begin{tikzcd} M \arrow[rr, "{[\![\cdot]\!]}"] \arrow[dr, "s"'] & & S \\ & M/\equiv \arrow[ur, "i"'] & \end{tikzcd}$$

S and $M/\equiv$ made isomorphic by formal restricting S to the image of $[\![\cdot]\!]$

Study to the quotient sets M/R for the equivalence relations $R \subseteq M \times M$

The lattice of semantics

Theorem ([Crawley and Dilworth 1973, Chap. 12] or [Grätzer 2003, Sect. IV.4])

The set of all equivalence relations on a set form a complete lattice called the **equivalence lattice** with set-inclusion as order

- Meet (infimum): $\bigwedge R = \bigcap R$
- Join (supremum): $\bigvee R = (\bigcup R)^*$

The lattice of semantics

Theorem ([Crawley and Dilworth 1973, Chap. 12] or [Grätzer 2003, Sect. IV.4])

The set of all equivalence relations on a set form a complete lattice called the **equivalence lattice** with set-inclusion as order

- Meet (infimum): $\bigwedge R = \bigcap R$
- Join (supremum): $\bigvee R = (\bigcup R)^*$

The isomorphism transfers the lattice structure from the equivalence relations to the abstract semantics, reserving the order:

$$M/R_1 \sqsubseteq M/R_2 \iff R_2 \subseteq R_1$$

Intuitions

Given two semantics $[\![\cdot]\!]_1$ and $[\![\cdot]\!]_2$, $[\![\cdot]\!]_1 \sqsubseteq [\![\cdot]\!]_2$ iff $[\![\cdot]\!]_2$ allows distinguishing between the same model as $[\![\cdot]\!]_1$ and possibly more

Intuitions

Given two semantics $[\![\cdot]\!]_1$ and $[\![\cdot]\!]_2$, $[\![\cdot]\!]_1 \sqsubseteq [\![\cdot]\!]_2$ iff $[\![\cdot]\!]_2$ allows distinguishing between the same model as $[\![\cdot]\!]_1$ and possibly more

Bottom element: $[\![\cdot]\!]_\perp : M \to M/M^2 \simeq \{\star\}$

- All models have the same semantics $[\![m]\!]_\perp = \star$

Intuitions

Given two semantics $[\![\cdot]\!]_1$ and $[\![\cdot]\!]_2$, $[\![\cdot]\!]_1 \sqsubseteq [\![\cdot]\!]_2$ iff $[\![\cdot]\!]_2$ allows distinguishing between the same model as $[\![\cdot]\!]_1$ and possibly more

Bottom element: $[\![\cdot]\!]_\perp : M \to M/M^2 \simeq \{\star\}$

- All models have the same semantics $[\![m]\!]_\perp = \star$

Top element $[\![\cdot]\!]_\top : M \to M/\mathrm{id}_M \simeq M$

- Every model $m \in M$ is its own semantic value $[\![m]\!]_\top = m$

Compatibility with *CR*

A family of abstract semantics $(\llbracket \cdot \rrbracket_i \colon M_i \to S_i)_{i \le n}$ is **compatible** with *CR* iff there is a semantic consistency relation $SCR \subseteq \prod_{i \le n} S_i$ st.

$$CR = CR_{SCR}$$

Compatible semantics encode enough information to determine if models are consistent

Natural semantics

For a metamodel M_i, $m_a,\ m_b \in M_i$,

$$m_a \sim_i m_b \iff CR \text{ cannot distinguish them}$$

The semantics $(\llbracket\cdot\rrbracket_i^{\mathrm{nat}}\colon M_i \to M_i/{\sim_i})_{i \leq n}$ are called the **natural semantics** for *CR*

Example

Suppose that $M = \prod_{i \leq n} M_i$ describe **components** of a car

The models are **consistent** if the total weight is $\leq$ **1000** kg

What are the natural semantics?

Example

Suppose that $M = \prod_{i \leq n} M_i$ describe **components** of a car

The models are **consistent** if the total weight is $\leq$ **1000** kg

What are the natural semantics?

$$[\![\cdot]\!]_i^{\mathrm{nat}} \colon M_i \to [0, 1000] \cup \{\text{too much}\}$$

Results

Proposition 1

The natural semantics are compatible with *CR*

Proposition 2

The semantics compatible with *CR* form complete lattices

Proposition 3

The natural semantics are the bottom elements of these lattices

Proof idea: By considering $SCR^{\mathrm{nat}} = \left\{ (\llbracket m_1 \rrbracket_1^{\mathrm{nat}}, \ldots, \llbracket m_n \rrbracket_n^{\mathrm{nat}}) \mid CR(m_1, \ldots, m_n) \right\}$ and the quotient sublattice (see [Crawley and Dilworth 1973, Chap. 2])

Conclusion

Karlsruhe Institute of Technology

A formal framework of consistency in model-driven development

Conclusion

A formal framework of consistency in model-driven development

Current and future works

- Add structure to the models (in a meta-model-agnostic way)
- Model slicing
- A (formal) language that can be used to define specific consistency relations

References I

[1] Peter Crawley and Robert P. Dilworth. **Algebraic theory of lattices**. Prentice-Hall, 1973. 201 pp.

[2] George Grätzer. **General Lattice Theory**. Second edition. Birkhäuser Verlag, 2003. ISBN: 978-3-7643-6996-5.

[3] Heiko Klare et al. “Enabling consistency in view-based system development — The Vitruvius approach”. In: **Journal of Systems and Software** 171 (Jan. 1, 2021), p. 110815. ISSN: 0164-1212. DOI: `10.1016/j.jss.2020.110815`.