VERIFICATION
VALIDATION
METHODS

PROJECT of the PEGASUS FAMILY

DIGITAL DEPENDABILITY IDENTITIES – A CONCEPT TO MANAGE COMPLEXITY

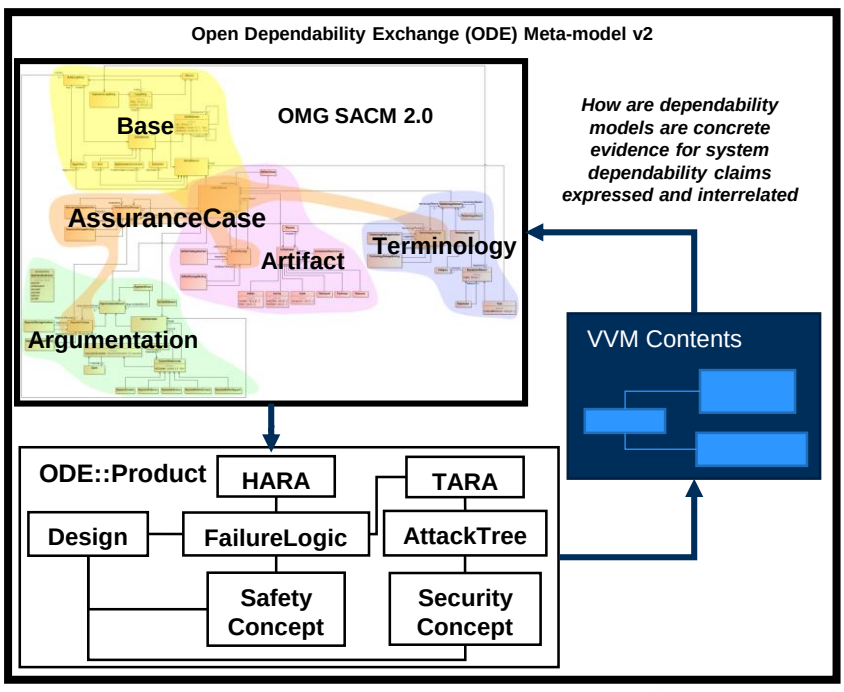
Creating formal traceability between engineering artifacts and safety case - applied to phenomena signal models

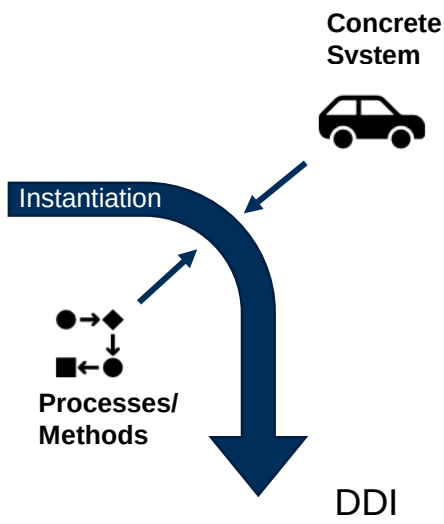
Daniel Hillen, Jan Reich, Joshua Frey, Fraunhofer IESE Kaiserslautern;
Nayel Fabian Salem, Marcus Nolte, TU Braunschweig;
Matthias Rauschenbach, Fraunhofer LBF Darmstadt; Veronica Haber, PROSTEP

Digital Dependability Identities (DDI) [1,2]

- **Framework** to enable continuous formal traceability between safety artifacts and safety case
- **Horizontal Traceability** between different safety artifacts
- **Vertical Traceability** between safety artifacts and safety case
- Built on **standardized** metamodels for single aspects (e.g. SACM [3])
- Open Dependability Exchange (ODE) Metamodel is a format for technical **safety artifact exchange between tool** throughout the development lifecycle
- Algorithm support to **automate** tasks, e.g. change impact, consistency

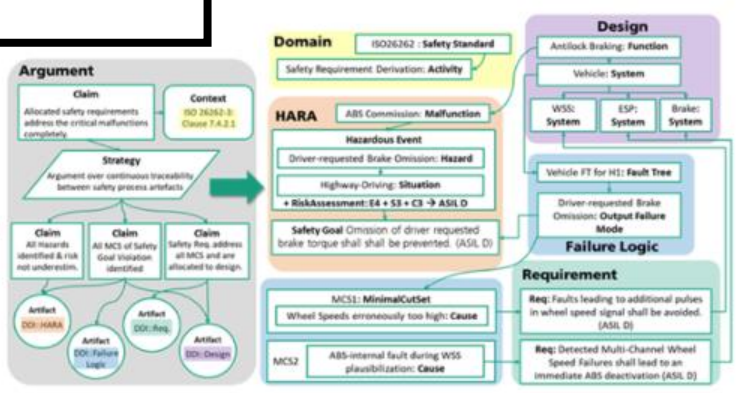
Relationship between DDI instance and metamodel





Metamodel

For a concrete system, artifacts and the safety case are instantiated as the DDI according to the metamodels.



The DDI concept is built to support iterative extension & tailoring

→ In VVM: Reuse what is there and extended for new VVM methods/artifacts

[1] DDIs and the Open Dependability Exchange Meta-Model https://www.deis-project.eu/
[2] Reich J. et al. (2020) Argument-Driven Safety Engineering of a Generic Infusion Pump with Digital Dependability Identities. DOI: https://doi.org/10.1007/978-3-030-58920-2_2
[3] OMG Structured Assurance Case Metamodel (SACM) https://www.omg.org/spec/SACM/2.2/About-SACM

www.vvm-projekt.de Twitter @vvm-project LinkedIn VVM Project

Projektpartner

A project developed by the VDA Leitinitiative autonomous and connected driving

Supported by: Federal Ministry for Economic Affairs and Climate Action
on the basis of a decision by the German Bundestag

VERIFICATION
VALIDATION
METHODS

PROJECT of the PEGASUS FAMILY

DIGITAL DEPENDABILITY IDENTITIES – A CONCEPT TO MANAGE COMPLEXITY

Creating formal traceability between engineering artifacts and safety case - applied to phenomena signal models

How can we integrate VVM artifacts formally into the DDI? - Exemplary shown for the Phenomenon Signal Model

Phenomenon Signal Model (PSM) [4]

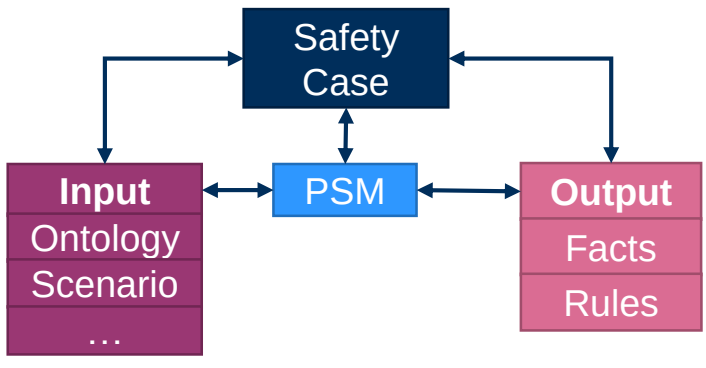
Formal method to analyze the ego behavior within a scenario, based on rules and facts, to support a safety evidence within a safety case.

Input:

Scenario, Ontology, Rules, etc.

Output:

PSM Graph that identifies rules and facts defining a safe behavior

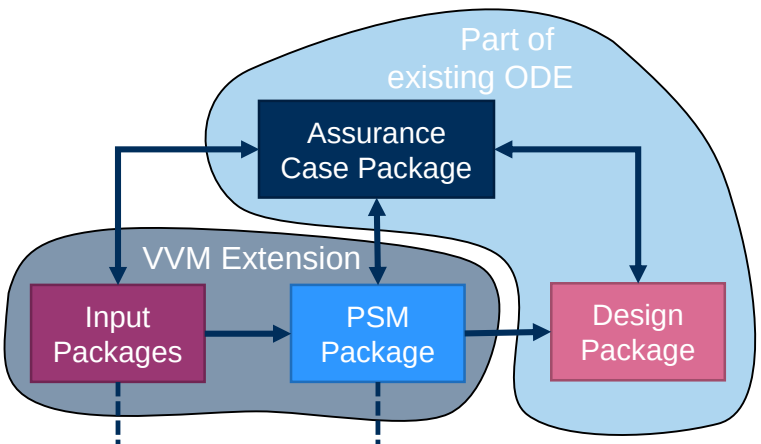


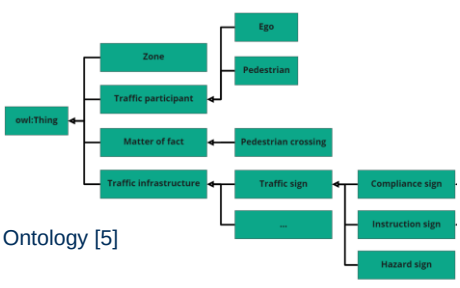
Problem:

PSM should be formally referenced within the safety case and linked to input and output artifacts

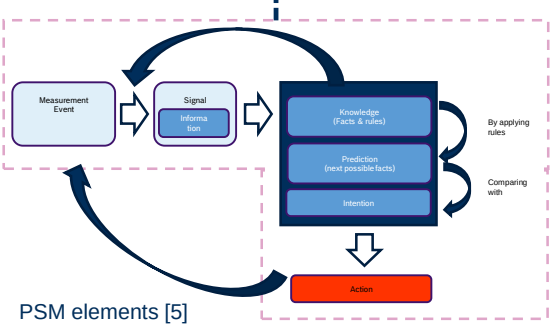
Solution

Specify formal metamodels of VVM artifacts and integrate them in DDI package





Ontology [5]



PSM elements [5]

[4] H. N. Beck, N. F. Salem, V. Haber, M. Rauschenbach, and J. Reich, Phänomen-Signal-Modell: Formalismus, Graph und Anwendung. 2021.

[5] Stream I/5a,b Contributions to a traceable behavior specification for automated driving systems using formal methods

www.vvm-projekt.de Twitter @vvm-project LinkedIn VVM Project

Projektpartner

A project developed by the VDA Leitinitiative autonomous and connected driving

Supported by: Federal Ministry for Economic Affairs and Climate Action on the basis of a decision by the German Bundestag

VERIFICATION
VALIDATION
METHODS

PROJECT of the PEGASUS FAMILY

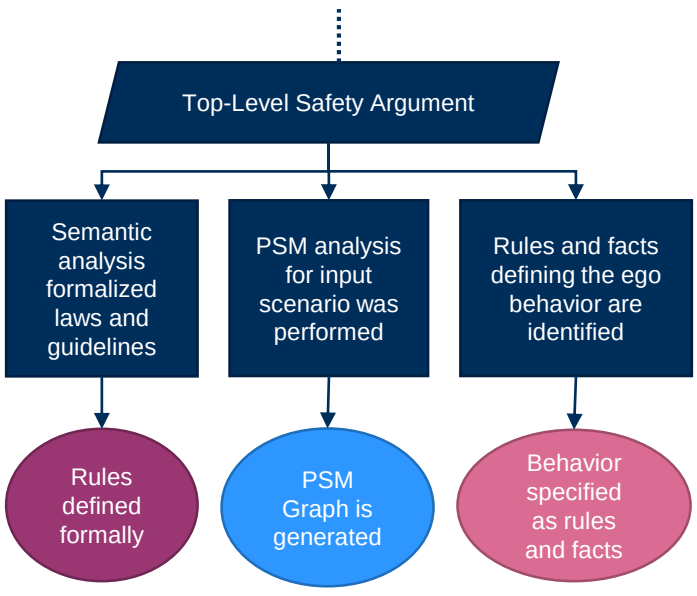
DIGITAL DEPENDABILITY IDENTITIES – A CONCEPT TO MANAGE COMPLEXITY

Creating formal traceability between engineering artifacts and safety case - applied to phenomena signal models

Example:

The PSM method and its input and output artifacts should support a safety case. In the example, the behavior of the vehicle at a zebra crossing is analyzed with the PSM method.

Here the arrows between exemplary artifacts show the horizontal traceability with regard to the PSM graph. The color of the safety evidence illustrates the vertical traceability.



Snapshot of a potential assurance case

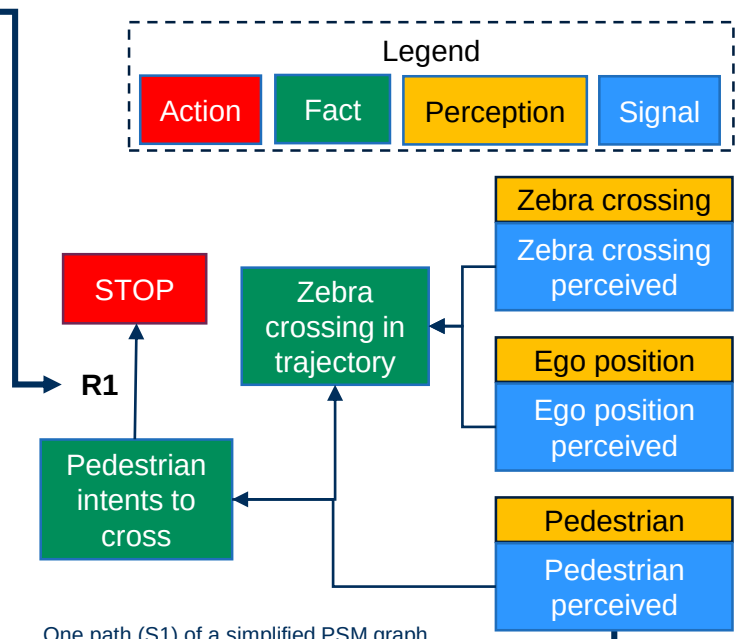
Ontology	Scenario
Zebra Crossing Pedestrian	Zebra Crossing In front, Pedestrian nearby, Ego drives towards crossing

StVO	Rule
§26	**R1**:If **zebra crossing** in front AND **pedestrian** intents to cross THEN stop

Example input artifacts

Input Artifacts

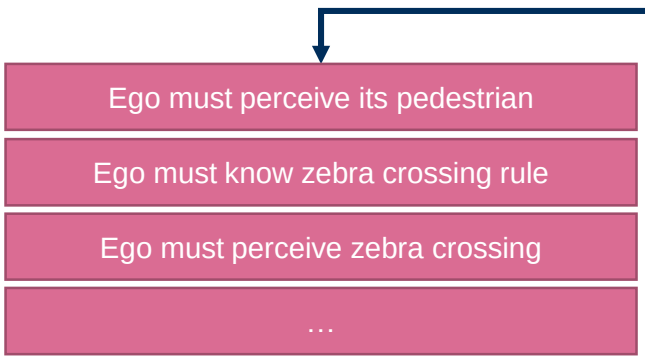
All input artifacts are formally included in the DDI. Each artifact, like for example the rule R1, can then be referenced explicitly within the DDI.



One path (S1) of a simplified PSM graph

PSM Graph

Here in Path S1, rule R1 was applied which led to the action stop and thus not to a collision. R1 reflects the StVO §26. All perceptions, facts and signals are important to correctly apply the Rule R1 and thus comply to §26 in this scenario



Snapshot of a potential assurance case

Output

Set of rules and facts that define the ego behavior. These rules and facts provide an initial input to derive capabilities in the following steps.

www.vvm-projekt.de Twitter @vvm-project LinkedIn VVM Project

Projektpartner

A project developed by the VDA Leitinitiative autonomous and connected driving

Supported by: Federal Ministry for Economic Affairs and Climate Action on the basis of a decision by the German Bundestag