Fraunhofer IESE

Fraunhofer Institute for Experimental Software Engineering IESE

#ENGINEERING THEDIGITALFUTURE since 96

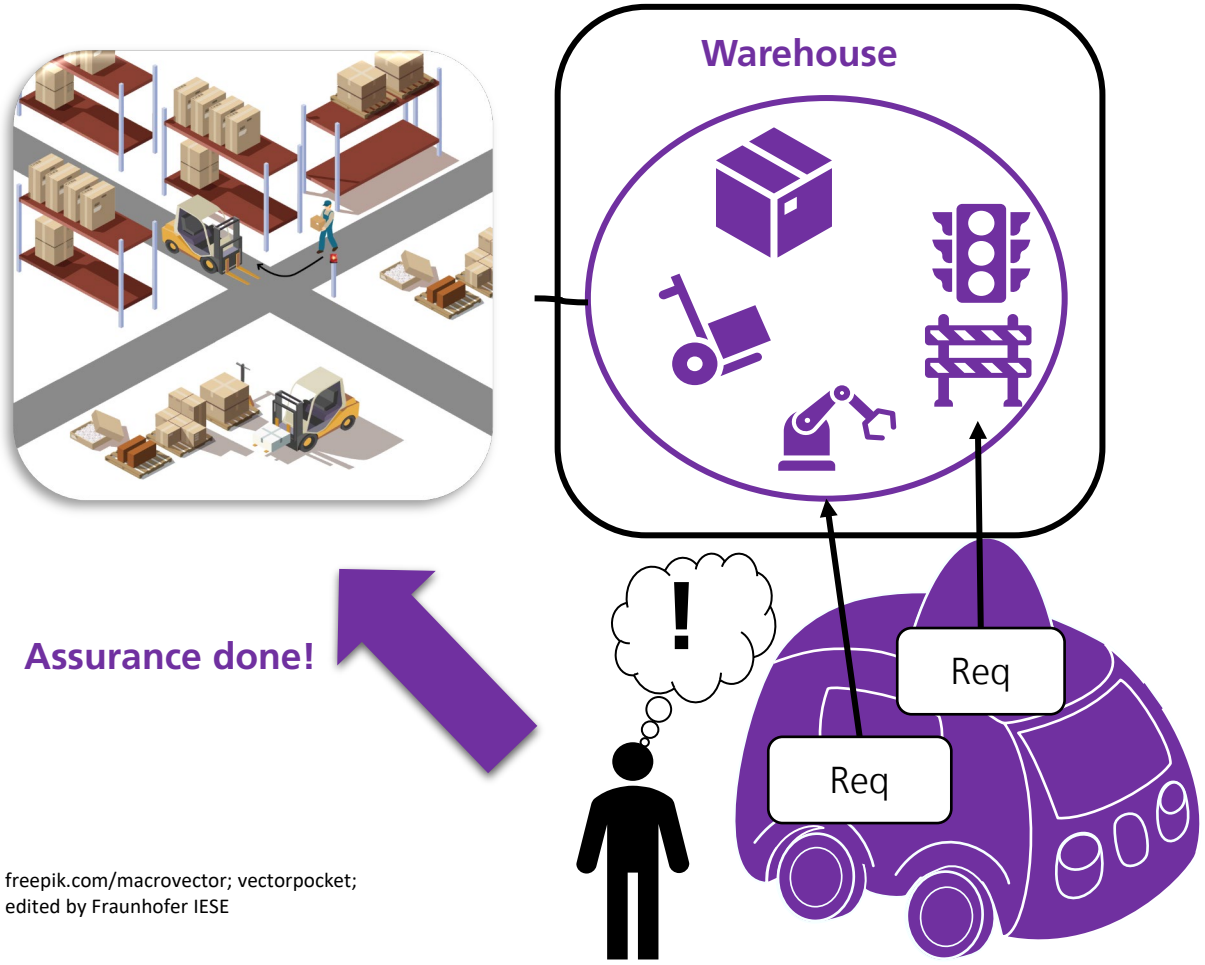
21. September 2023, SafeComp 2023

Concept and metamodel to support cross-domain safety analysis for ODD expansion of autonomous systems

Jan Reich, Daniel Hillen, Joshua Frey, Nishanth Laxman, Takehito Ogata, Donato Di Paola, Satoshi Otsuka, Natsumi Watanabe

Operational Design Domain (ODD) Extension

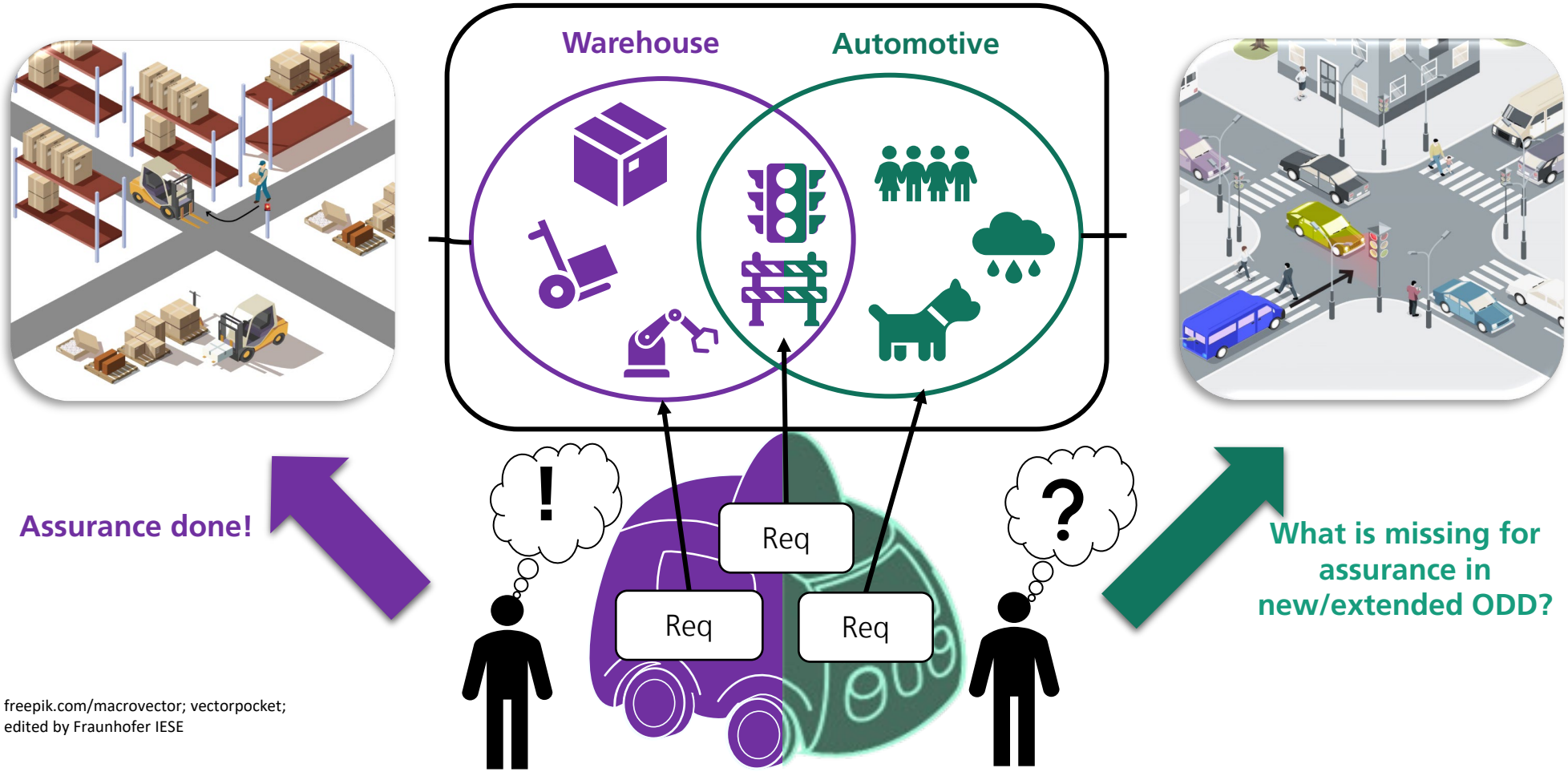
Motivation



freepik.com/macrovector; vectorpocket;
edited by Fraunhofer IESE

Operational Design Domain (ODD) Extension

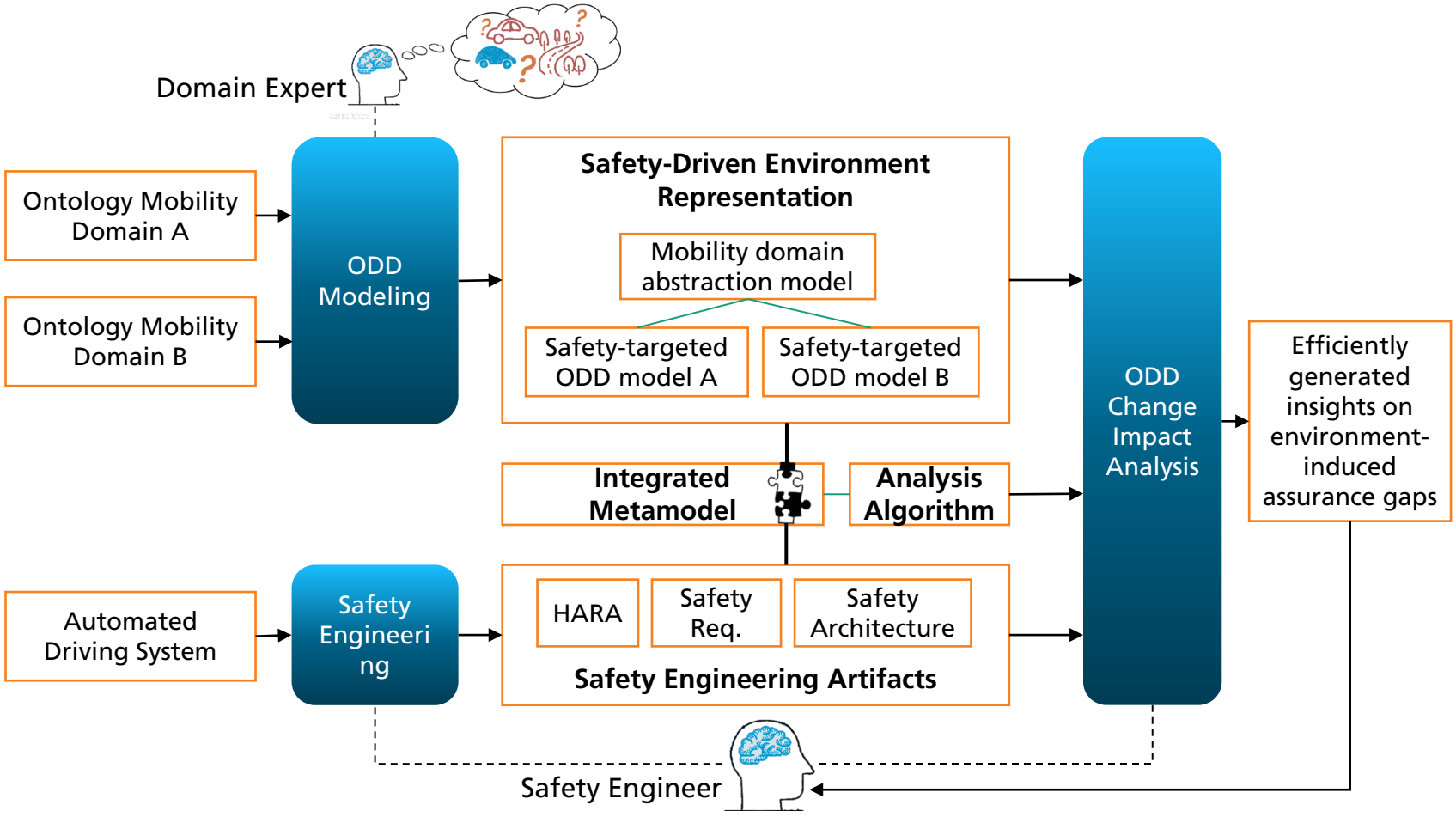
Motivation



freepik.com/macrovector; vectorpocket;
edited by Fraunhofer IESE

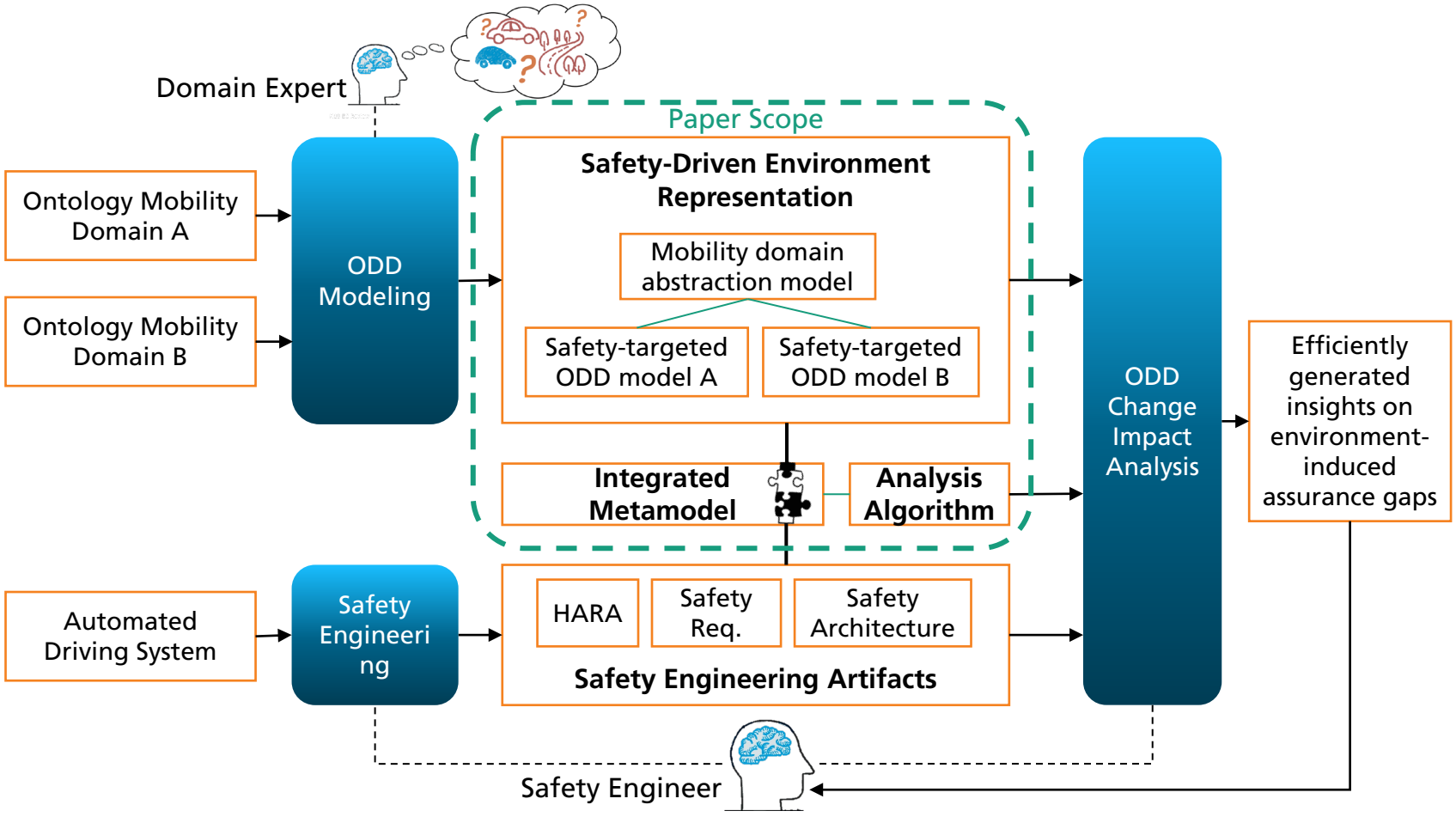
Safety-aware context engineering

Methodological Overview



Safety-aware context engineering

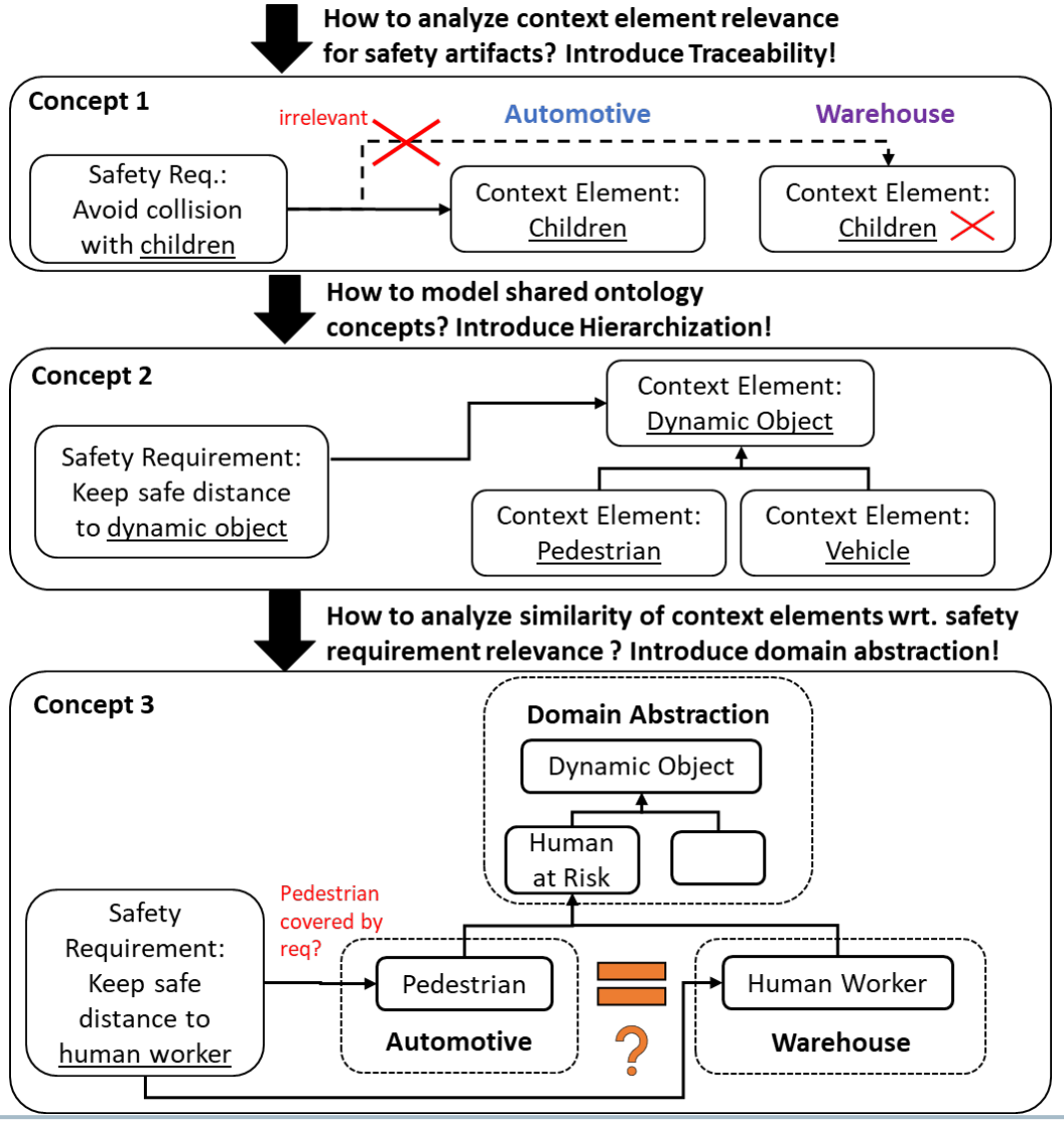
Methodological Overview



Safety-driven environment representation

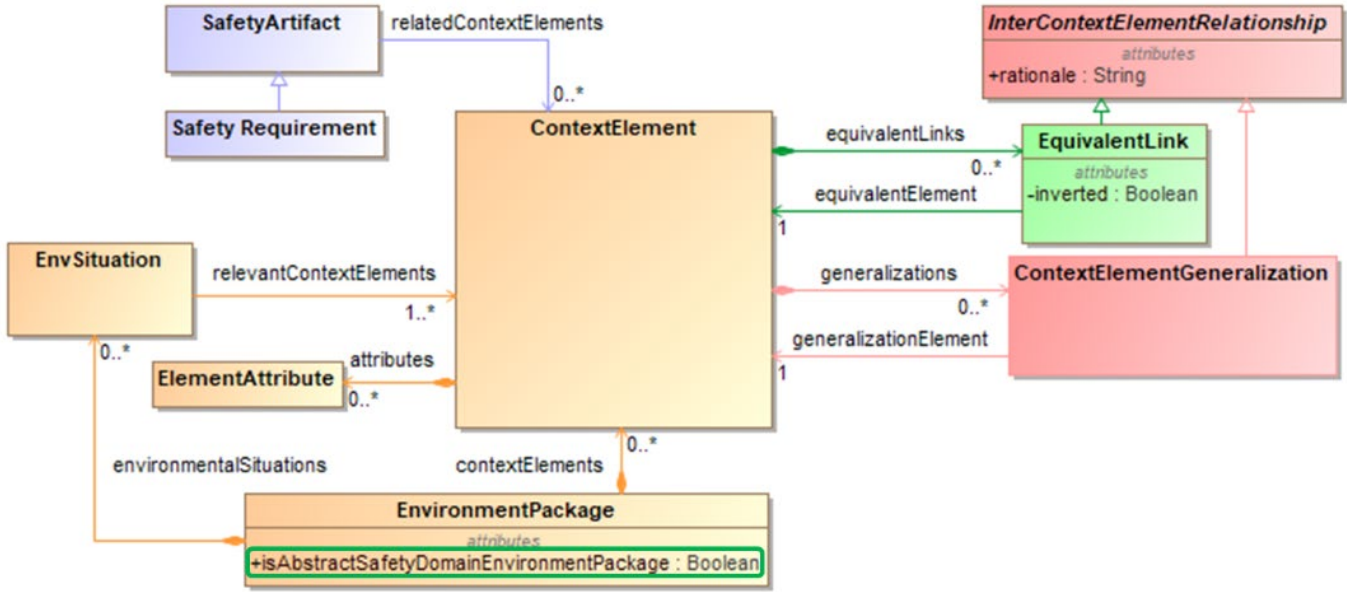
Concepts

- **Concept 1:** Linking safety engineering artifacts to context elements they refer to is the basis to analyze the safety impact of a changing ODD
- **Concept 2:** Hierarchization enables representing shared ontological concepts.
- **Concept 3:** Shared domain abstraction enables similarity specification.



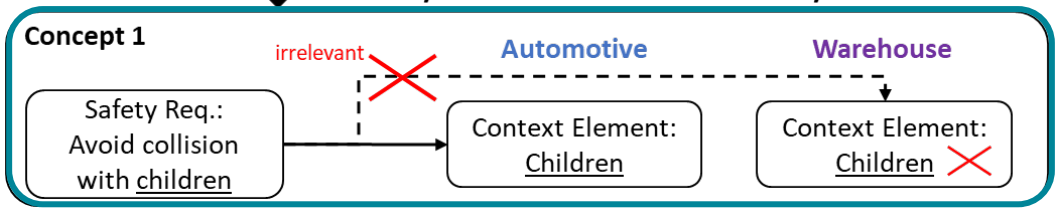
Concept Formalization

Metamodel



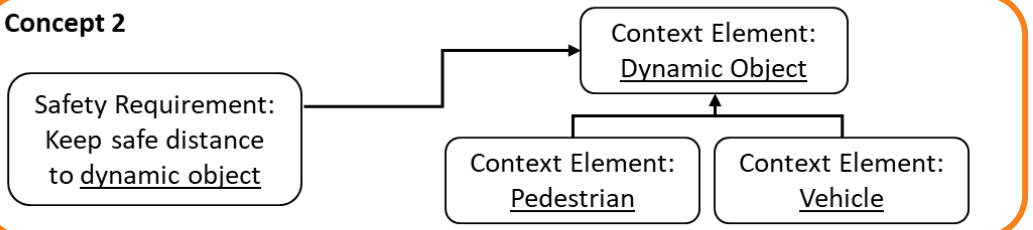
How to analyze context element relevance for safety artifacts? Introduce Traceability!

Concept 1



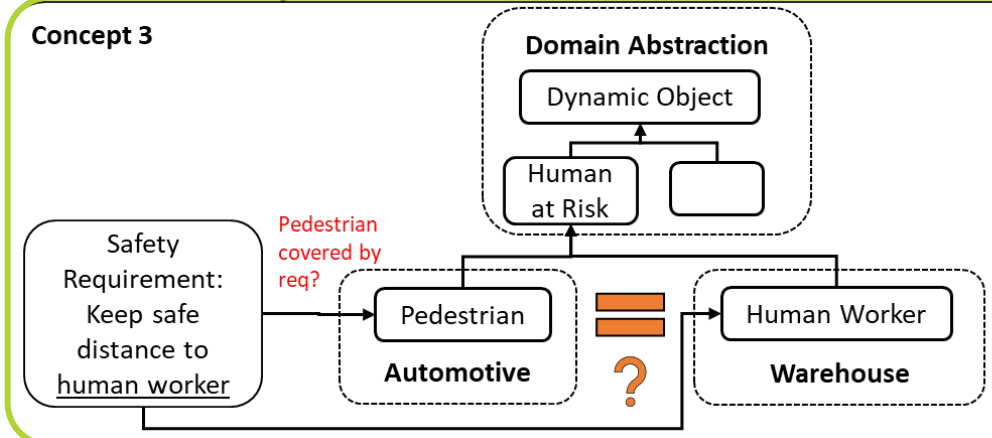
How to model shared ontology concepts? Introduce Hierarchization!

Concept 2



How to analyze similarity of context elements wrt. safety requirement relevance ? Introduce domain abstraction!

Concept 3

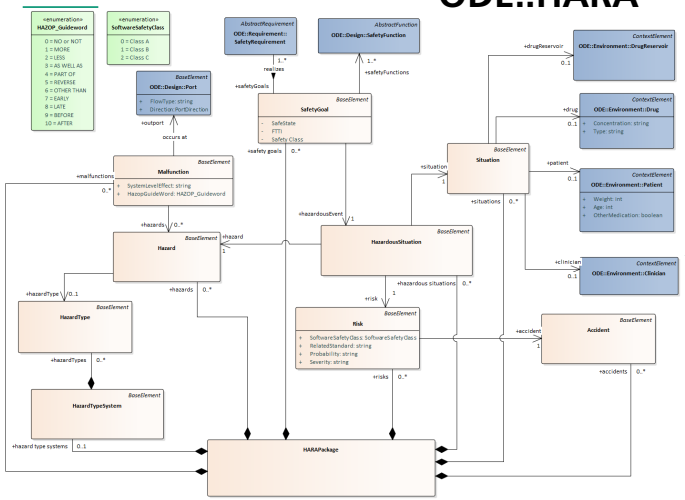


  Public

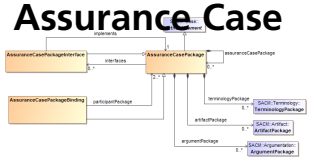
ODE::Environment Metamodel integration into the DDI

DDI Packages Overview

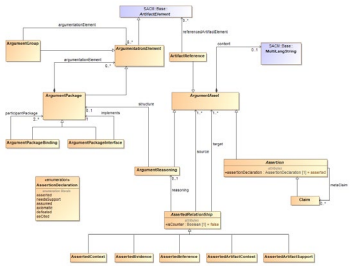
ODE::HARA



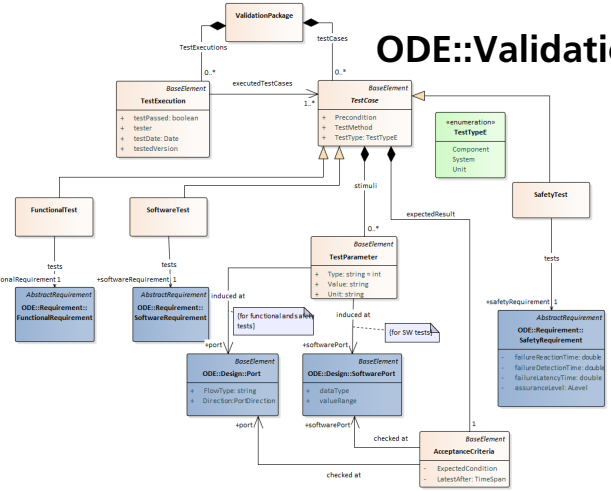
Assurance Case

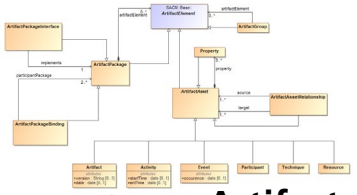


OMG SACM



ODE::Validation

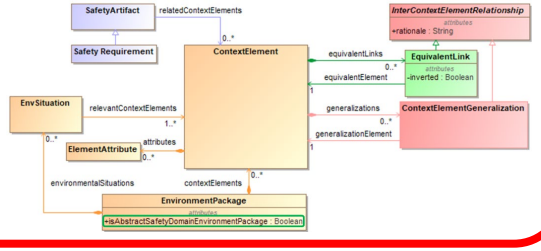




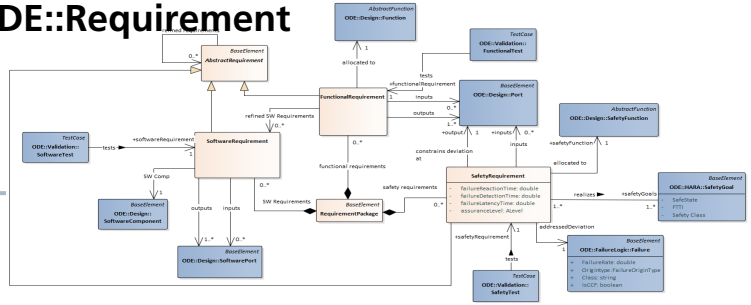
Artifact

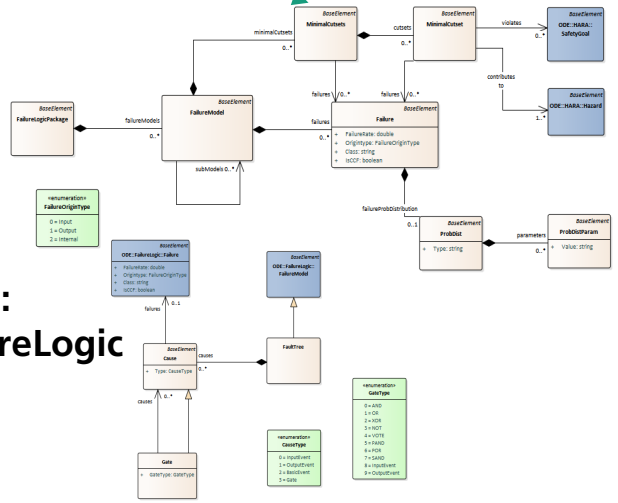
Argumentation

ODE::Environment



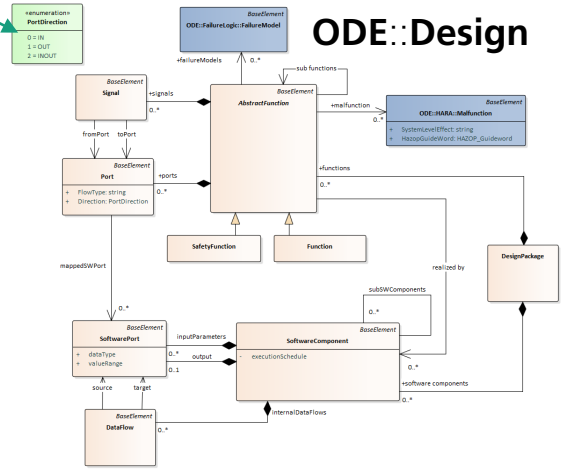
ODE::Requirement





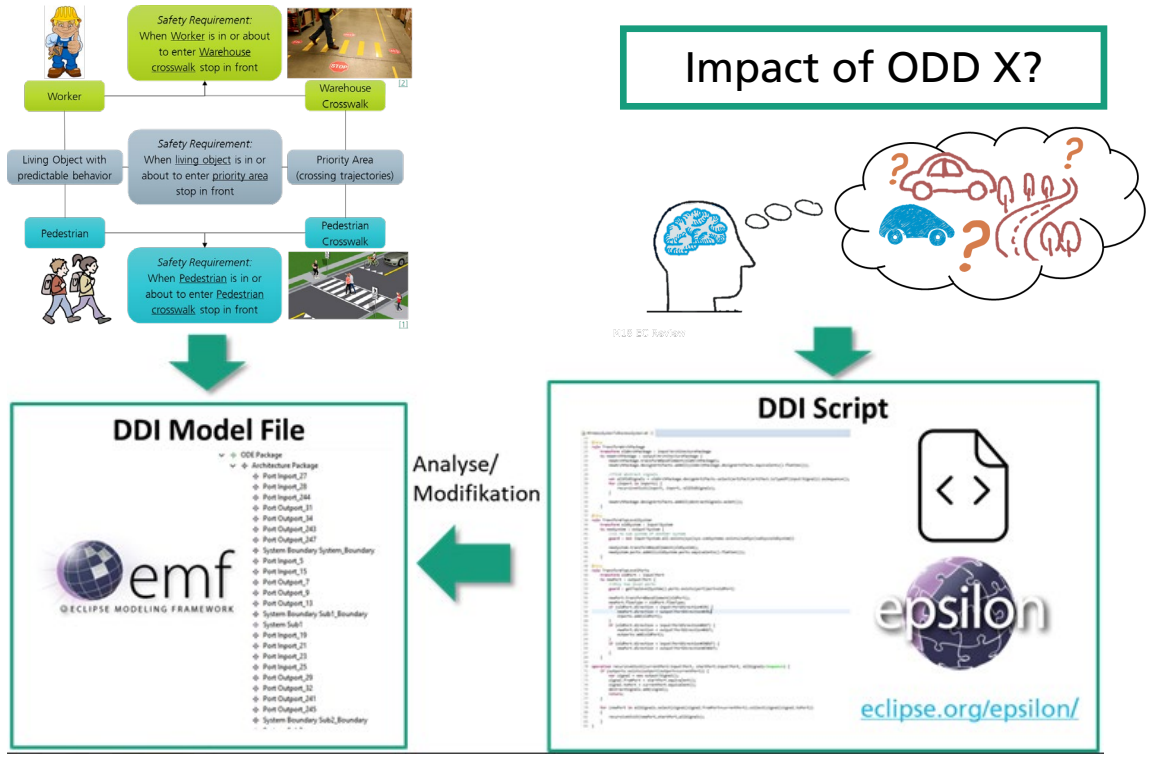
ODE:: FailureLogic

ODE::Design



Concept Formalization

Change Impact Analysis Algorithm




```
1  "Hierarchy of context elements".println();
2  "----------------------------".println();
3  "".println();
4
5
6  var highestAbstractionElements = ContextElement.
7                                       allInstances().
8                                       select(element | element.generalizations.isEmpty() or
9                                                        element.generalizations == null);
10
11 for (highestAbstractionElement : ContextElement in highestAbstractionElements) {
12     highestAbstractionElement.printHierarchyTreeRecursively("");
13     "".println();
14 }
15
16 operation ContextElement printHierarchyTreeRecursively(indentation : String) {
17     self.printHierarchyEntry(indentation);
18
19     var directChildElements = self.getDirectChildElements();
20
21     if (not directChildElements.isEmpty()){
22         for (childElem : ContextElement in directChildElements) {
```

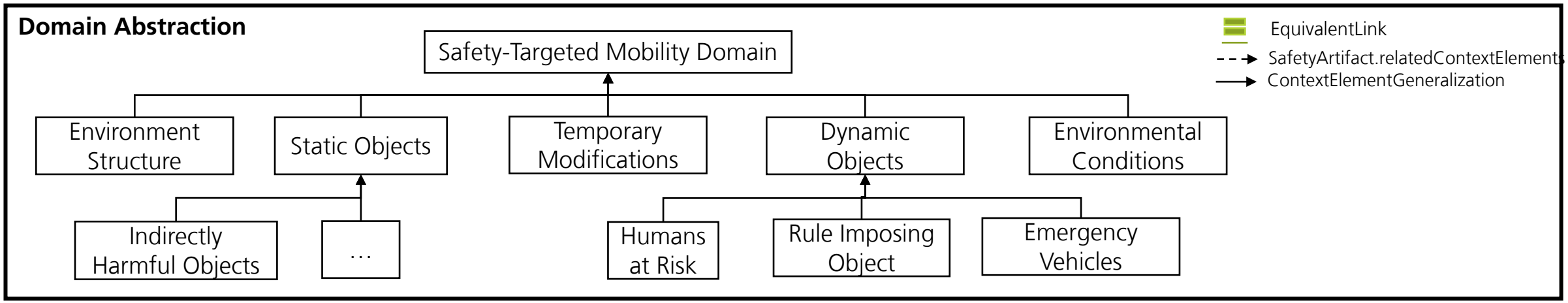
Problems | Javadoc | Declaration | Search | Console | Properties | Validation

Epsilon

```
Hierarchy of context elements
----------------------------

|-> Environment Structure (Safety-Targeted Mobility Domain)

|-> Static Objects (Safety-Targeted Mobility Domain)
       |-> Indirectly Harmful Objects (Safety-Targeted Mobility Domain)
              |-> Item Rack (Warehouse Domain)

|-> Temporary Modifications (Safety-Targeted Mobility Domain)

|-> Dynamic Objects (Safety-Targeted Mobility Domain)
       |-> Humans at Risk (Safety-Targeted Mobility Domain)
              |-> Human Worker (Warehouse Domain)
              |-> Police Officer (Automotive Domain)
       |-> Rule Imposing Object (Safety-Targeted Mobility Domain)
              |-> WH Leader (Warehouse Domain)
              |-> Police Officer (Automotive Domain)
       |-> Emergency Vehicles (Safety-Targeted Mobility Domain)
              |-> Fire truck (Automotive Domain)

|-> Environmental Conditions (Safety-Targeted Mobility Domain)
```

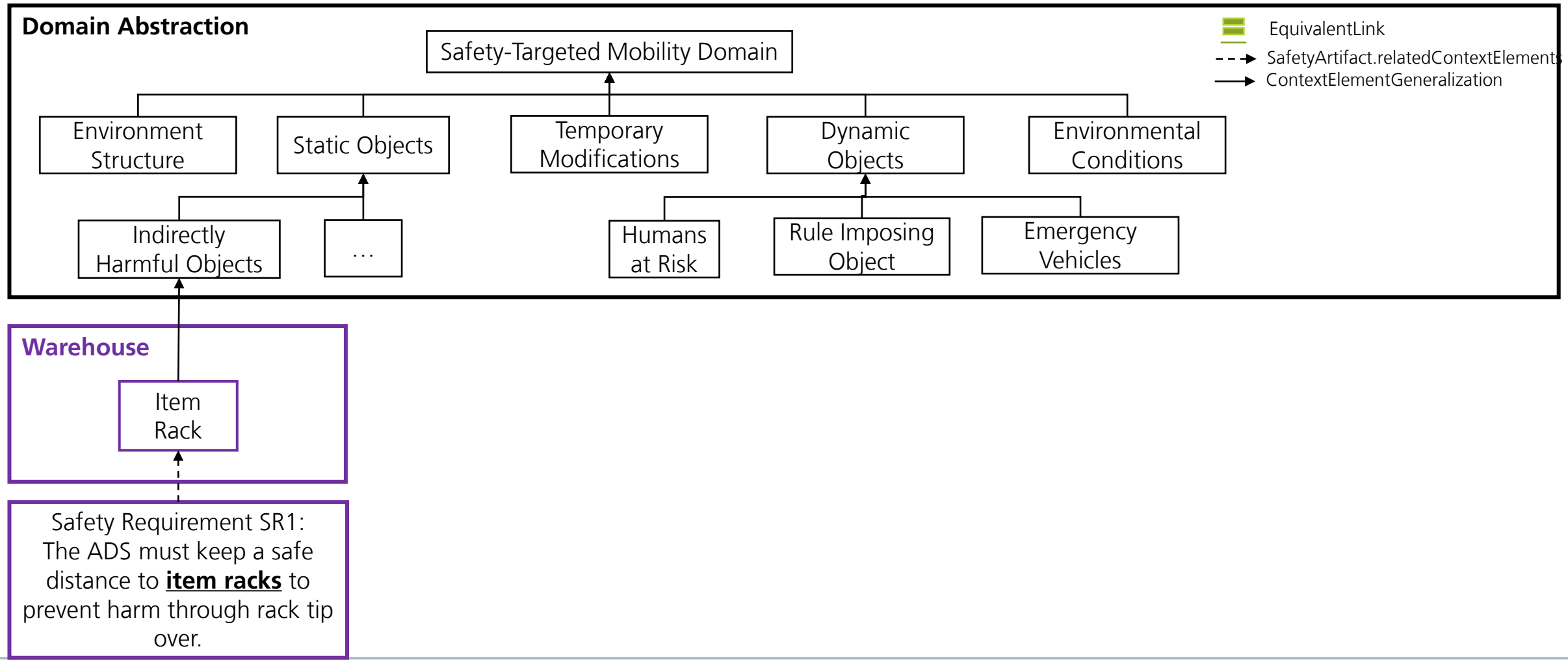
Initializing the metamodel

Example Model Instance



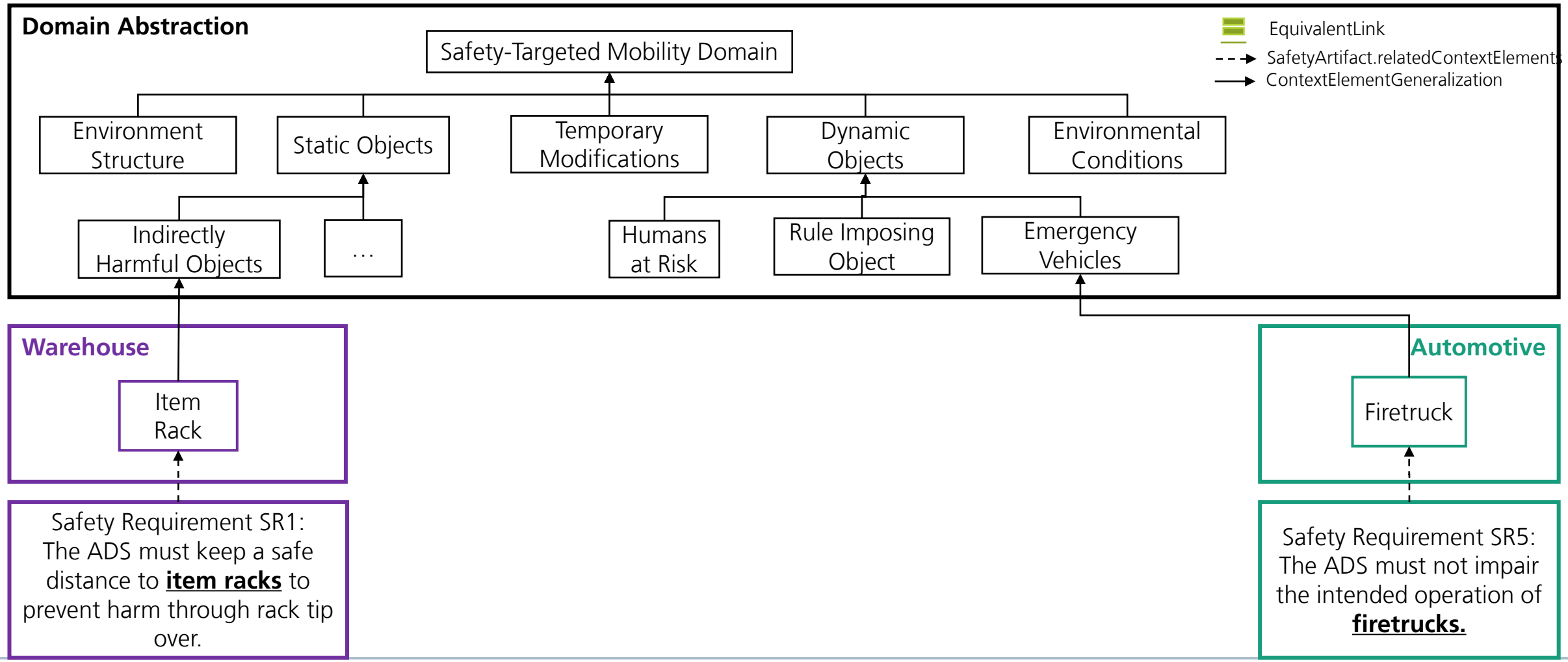
Initializing the metamodel

Example Model Instance



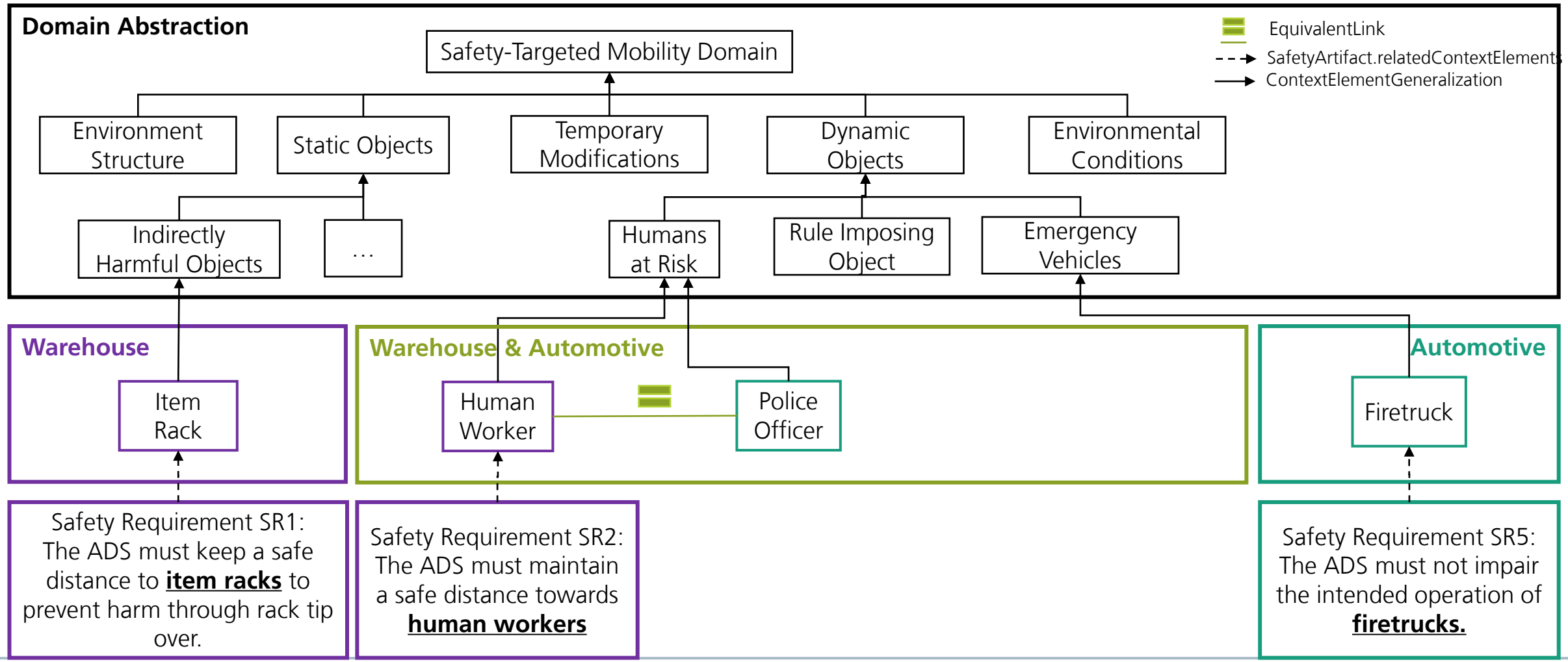
Initializing the metamodel

Example Model Instance



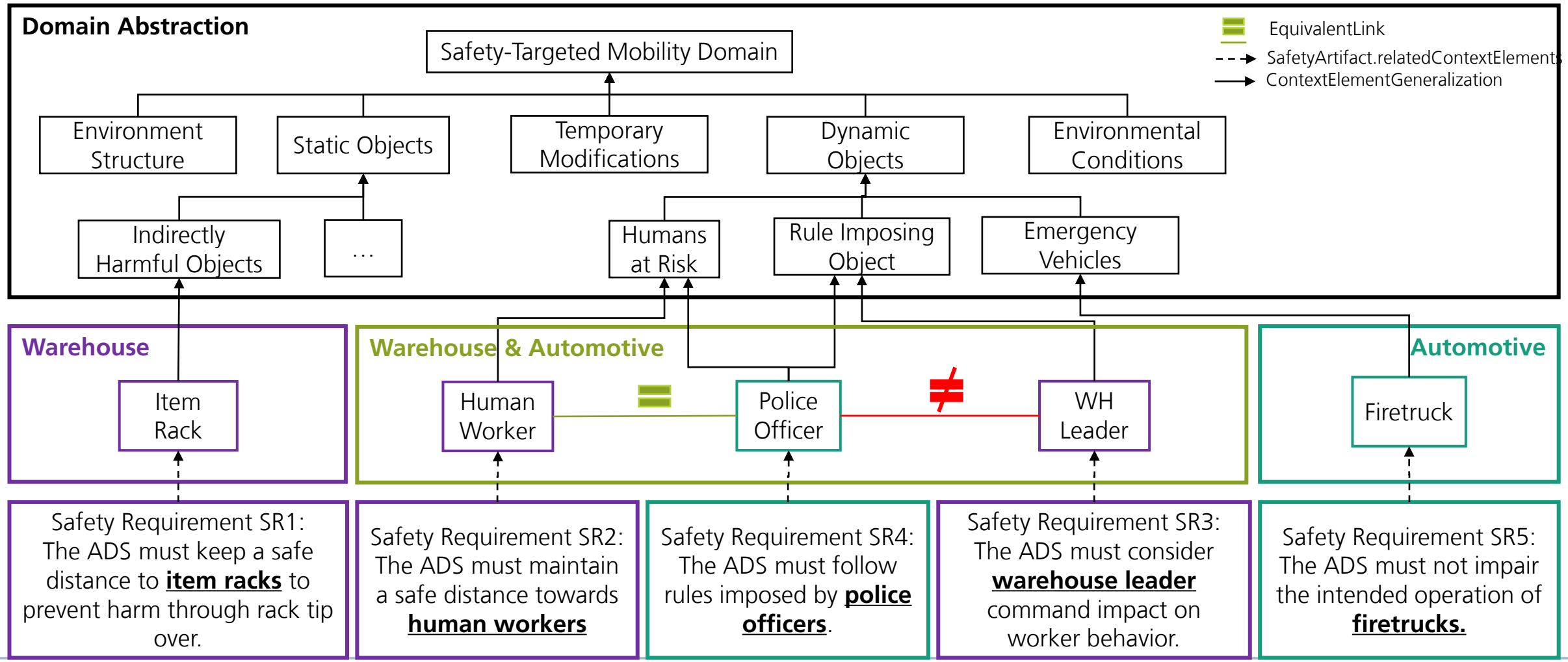
Initializing the metamodel

Example Model Instance



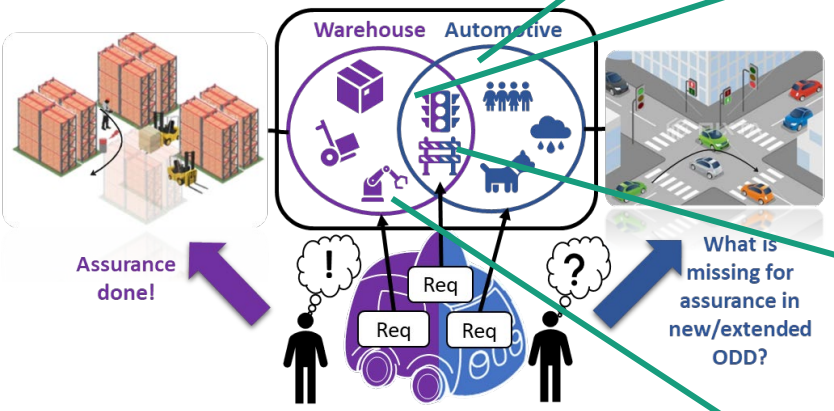
Initializing the metamodel

Example Model Instance



Script Output

Based on the Example Model Instance

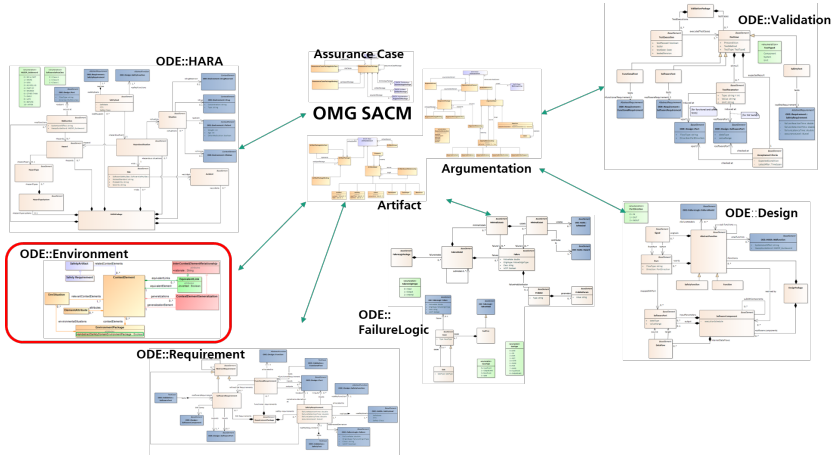


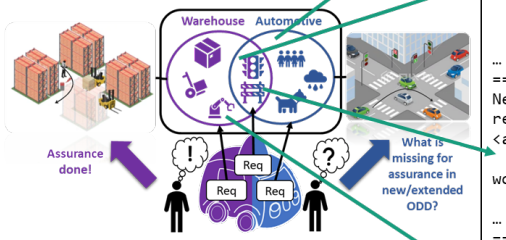

```
New elements exclusive for domain: Automotive – New safety requirements must be derived:
Firetruck
…
=============================================================================================
New elements of domain: Automotive with equivalent elements in domain: Warehouse – Requirements can be
reused:
<abstract> Humans at Risk:
    Police Officer = Human Worker -> Rational: Both are vulnerable humans that are in danger
        |-> SR2 - The ADS must maintain a safe distance towards Human Worker
        |-> Proposal: SR2.1 – The ADS must maintain a safe distance towards Police Officer
…
=============================================================================================
New elements of domain: Automotive that are nonequivalent to elements in domain: Warehouse – Safety
requirement must be derived:
<abstract> Rule Imposing Object:
    Police Officer != WH Leader -> Rational: Police officer imposes rules on the ADS and WH leader to
workers
        |-> SR3 - The ADS must consider warehouse leader command impact on worker behavior
…
=============================================================================================
Elements exclusive for domain: Warehouse – No action required:
Item Rack
        |-> The ADS must keep a safe distance to item racks to prevent harm through rack tip over
…
```

Summary & Conclusion

Recap

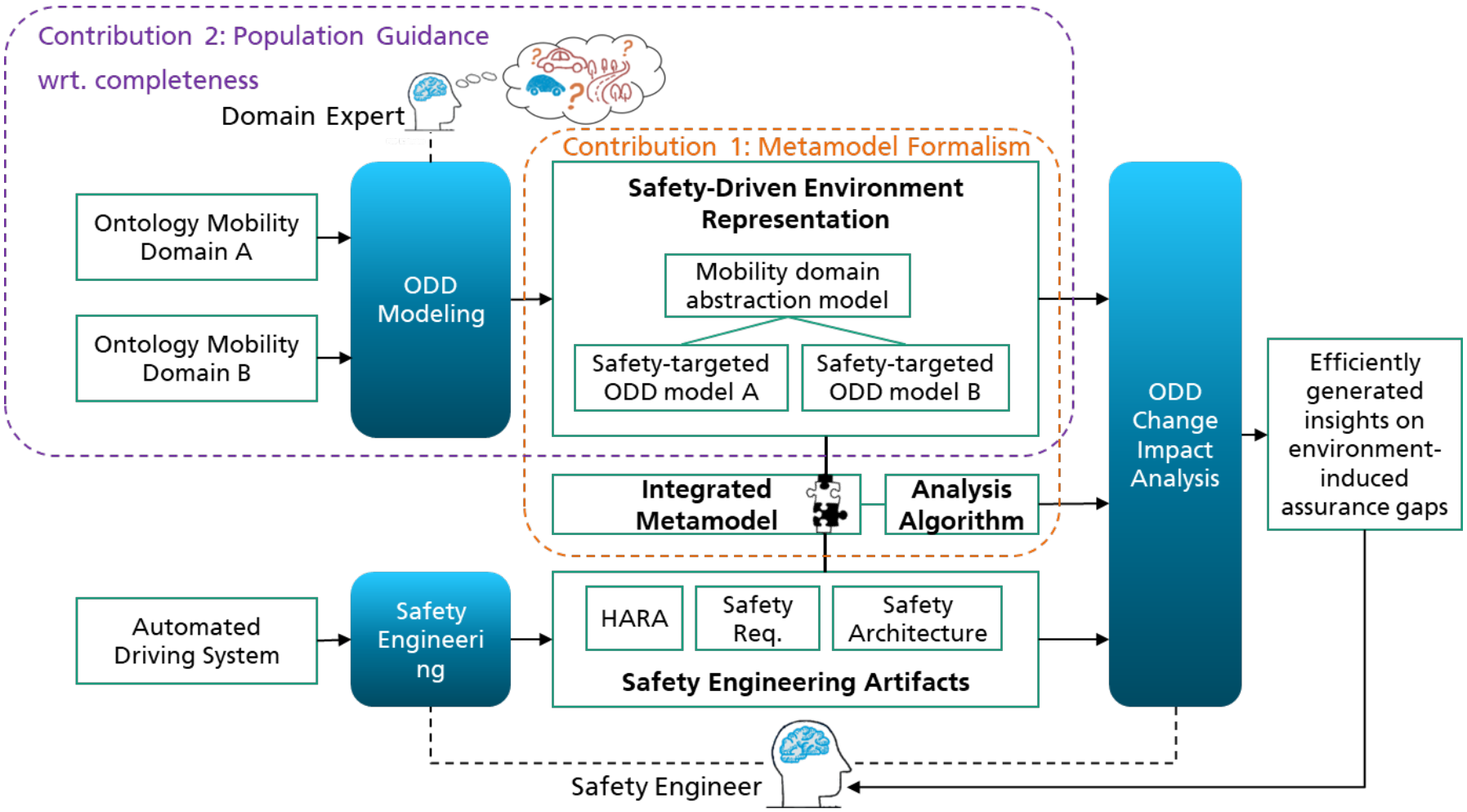
- Meta model to formalize the environment
- Integration into DDI to implement traceability between safety artifacts and environmental elements
- Scripts to support safety engineers with the change impact analysis






```
New elements exclusive for domain: Automotive – New safety requirements must be derived:
Firetruck
…
=============================================================================================
New elements of domain: Automotive with equivalent elements in domain: Warehouse – Requirements can be
reused:
<abstract> Humans at Risk:
    Police Officer = Human Worker -> Rational: Both are vulnerable humans that are in danger
        |-> SR2 - The ADS must maintain a safe distance towards Human Worker
        |-> Proposal: SR2.1 – The ADS must maintain a safe distance towards Police Officer
…
=============================================================================================
New elements of domain: Automotive that are nonequivalent to elements in domain: Warehouse – Safety
requirement must be derived:
<abstract> Rule Imposing Object:
    Police Officer != WH Leader -> Rational: Police officer imposes rules on the ADS and WH leader to
workers
        |-> SR3 - The ADS must consider warehouse leader command impact on worker behavior
…
=============================================================================================
Elements exclusive for domain: Warehouse – No action required:
Item Rack
        |-> The ADS must keep a safe distance to item racks to prevent harm through rack tip over
…
```

Outlook


Contribution 2: Population Guidance
wrt. completeness
Domain Expert
Contribution 1: Metamodel Formalism
Ontology Mobility Domain A
Ontology Mobility Domain B
ODD Modeling
Safety-Driven Environment Representation
Mobility domain abstraction model
Safety-targeted ODD model A
Safety-targeted ODD model B
Integrated Metamodel
Analysis Algorithm
ODD Change Impact Analysis
Efficiently generated insights on environment-induced assurance gaps
Automated Driving System
Safety Engineering
HARA
Safety Req.
Safety Architecture
Safety Engineering Artifacts
Safety Engineer

Thank you for your interest!

Contact

Feel free to reach out to me via mail or connect on LinkedIn

www.linkedin.com/in/daniel-hillen

daniel.hillen@iese.fraunhofer.de

Daniel Hillen
Safety Engineer

Safety Engineering (SAF)
@Fraunhofer IESE, Germany

Thank You!