

AlloyInEcore: Deep Embedding of First-Order Relational Logic into Meta-Object Facility

Workshop on the Future of Alloy. May 1, 2018. Cambridge, MA

About me

- European Cooperation in Science and Technology (COST)
IC1404 “Multi-Paradigm Modelling for Cyber-Physical Systems”
 - http://www.cost.eu/COST_Actions/ict/IC1404
- European Cooperation in Science and Technology (COST)
IC1402 “Runtime Verification beyond Monitoring”
 - http://www.cost.eu/COST_Actions/ict/IC1402
- ITEA-ModelWriter: Synchronized Document Engineering
 - <https://itea3.org/project/modelwriter.html>
- ITEA-ASSUME: Affordable Safe & Secure Mobility Evolution
 - <https://itea3.org/project/assume.html>
- ITEA-XIVT: eXcellence In Variant Testing
 - <https://itea3.org/project/xivt.html>
- UNIT Information Technologies R&D Ltd., Turkey (Co-founder)



F. Erata et. al.

Tarski: A platform for automated analysis of dynamically configurable traceability semantics

The 32nd ACM SIGAPP Symposium On Applied Computing (SAC'17), pp. 1607-1614, 2017



F. Erata et. al.

A tool for automated reasoning about traces based on configurable formal semantics

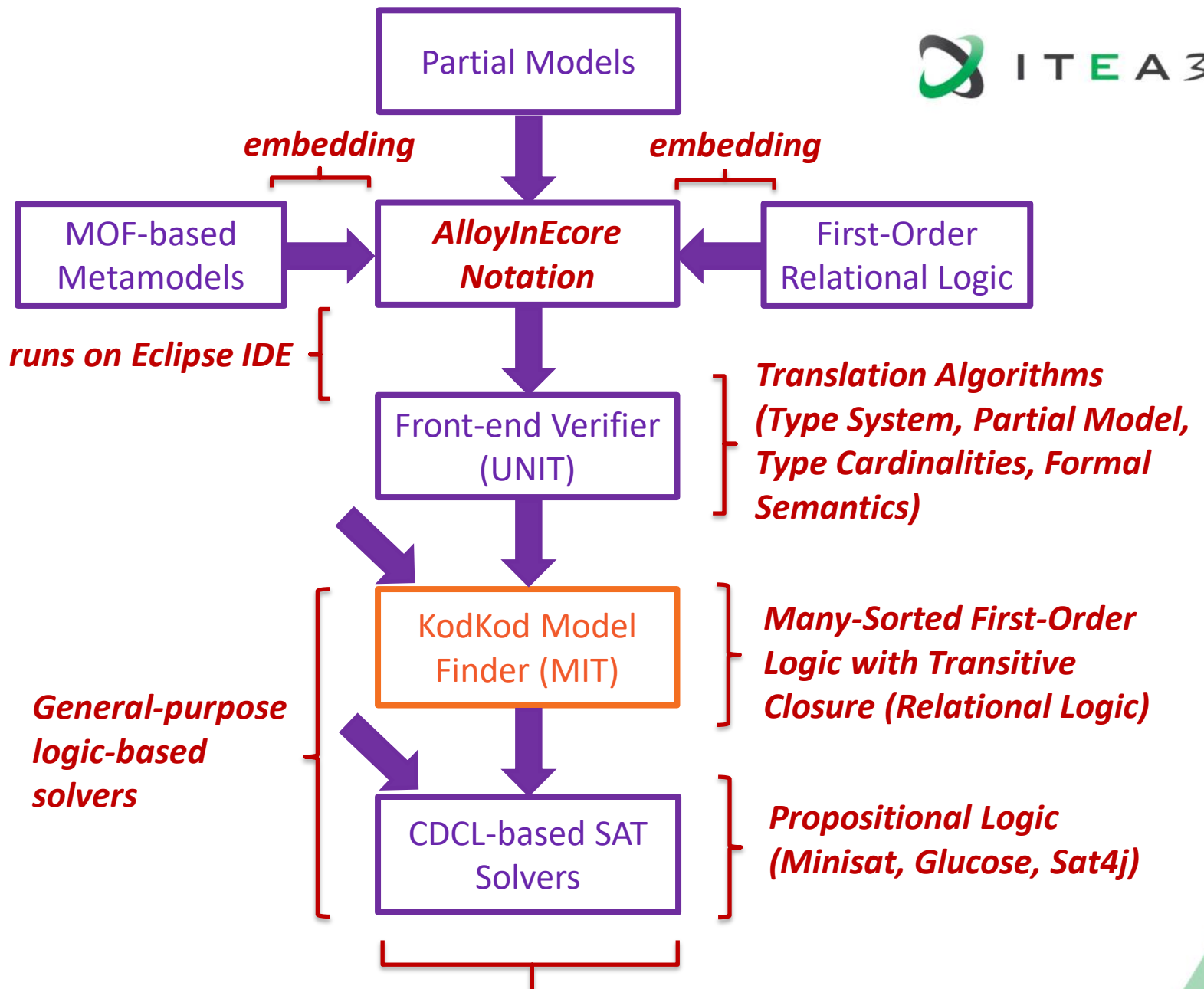
The 25th ACM Joint European Software Engineering Conference and Symposium on the Foundations of Software Engineering (ESEC/FSE'17), pp. 959-963, 2017



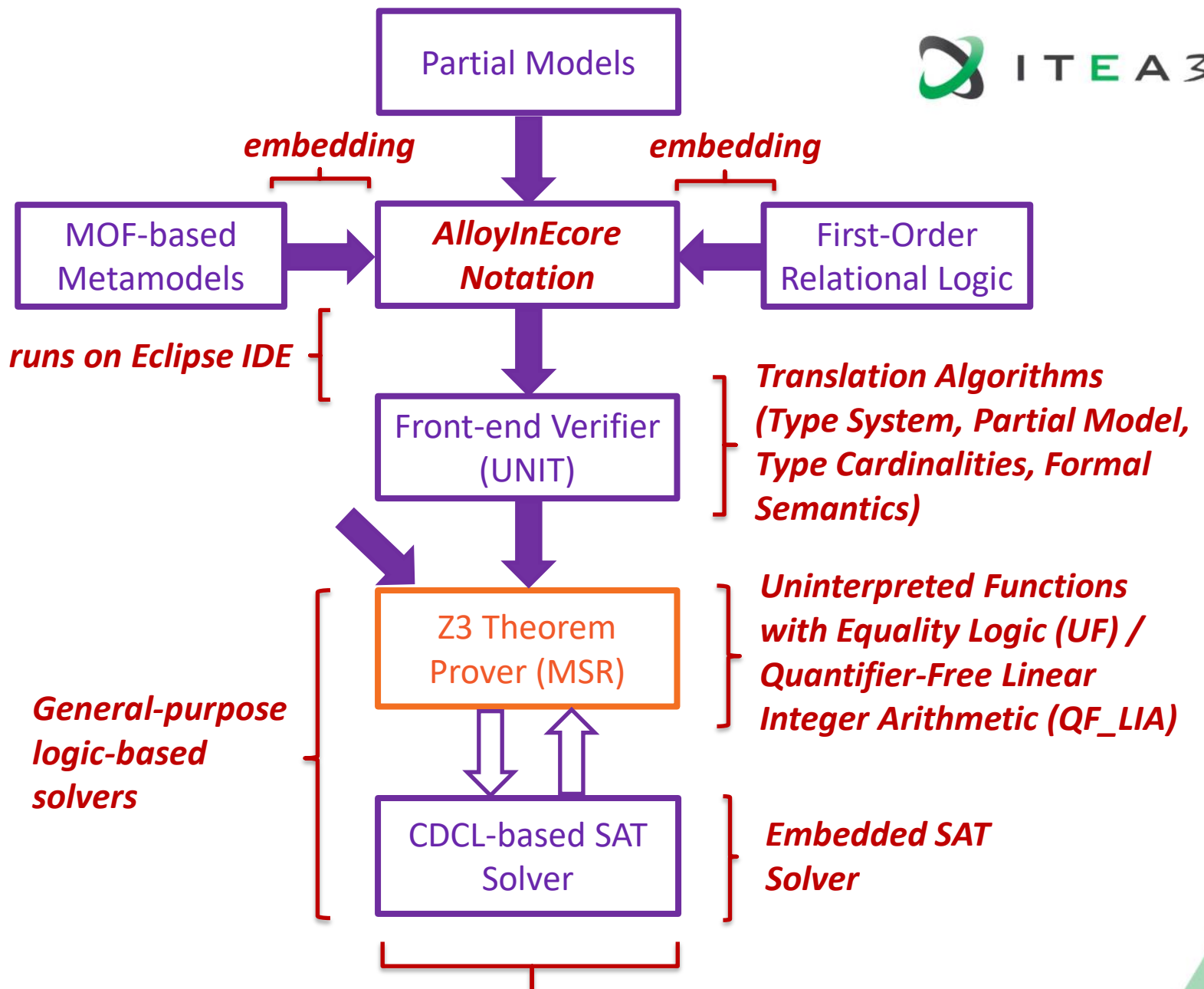
F. Erata et. al.

ModelWriter: Text and model-synchronized document engineering platform

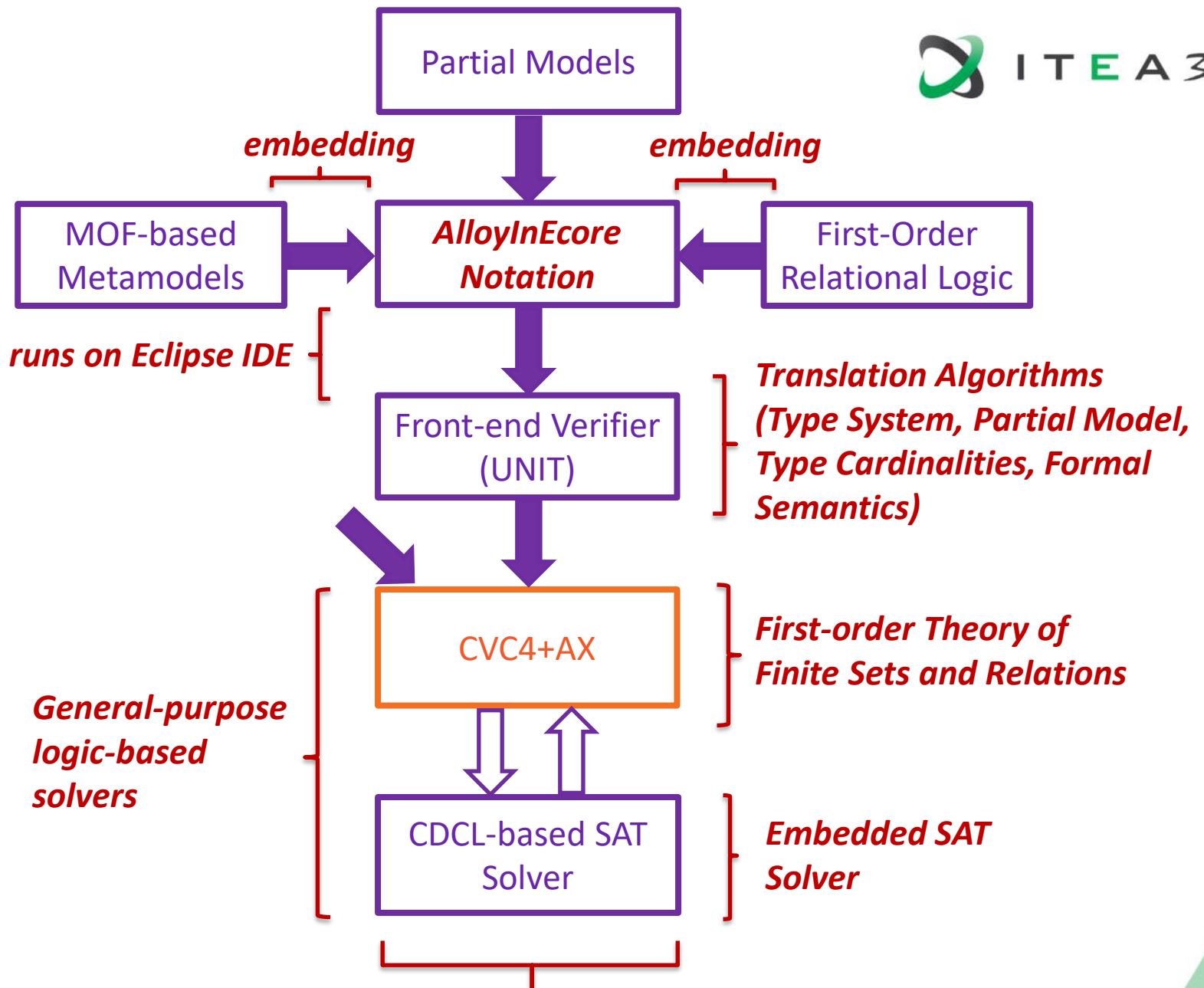
32nd IEEE/ACM International Conference on Automated Software Engineering (ASE'17), pp. 928-933, 2017



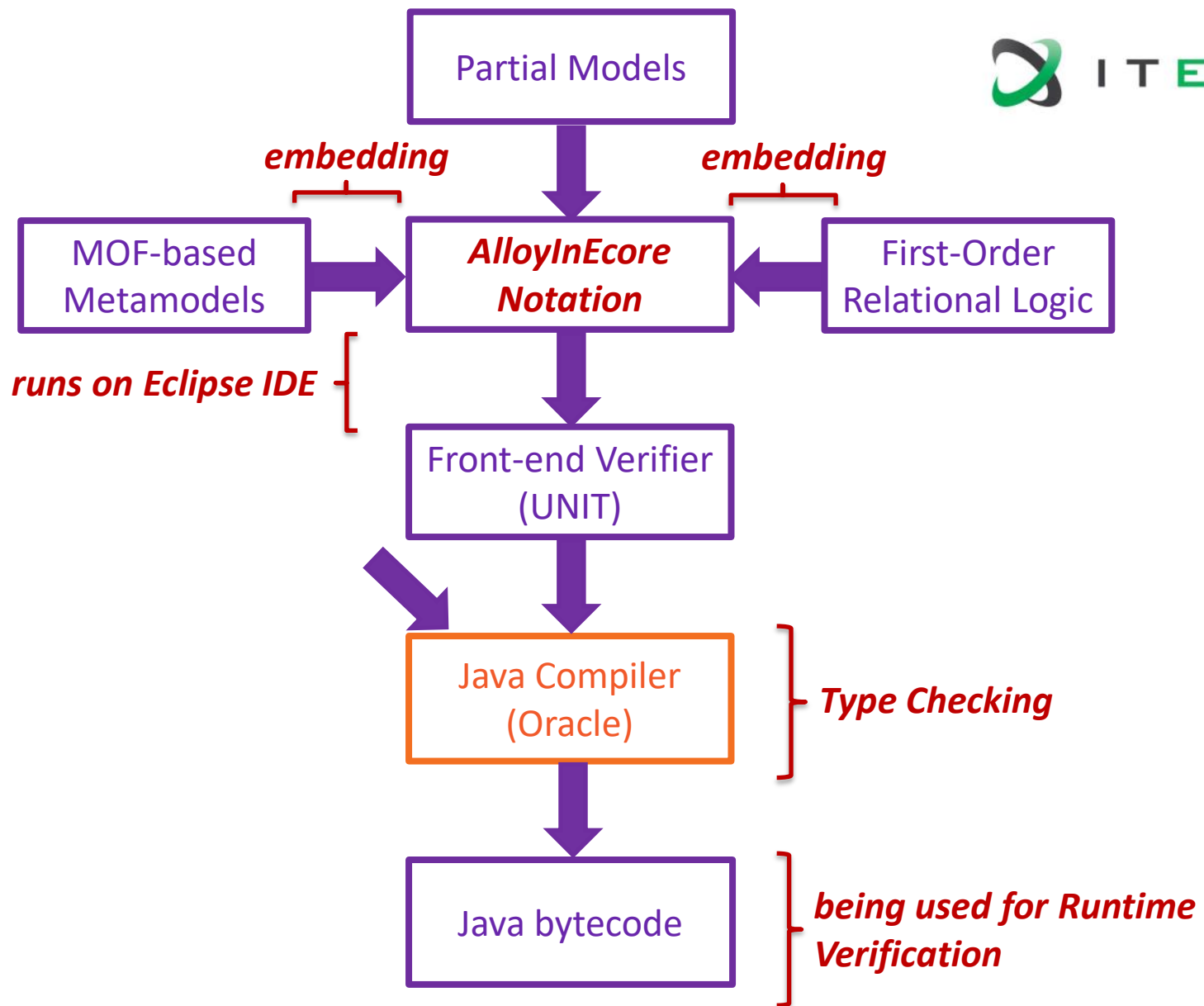
Partial Model Completion, Checking Consistency of Models

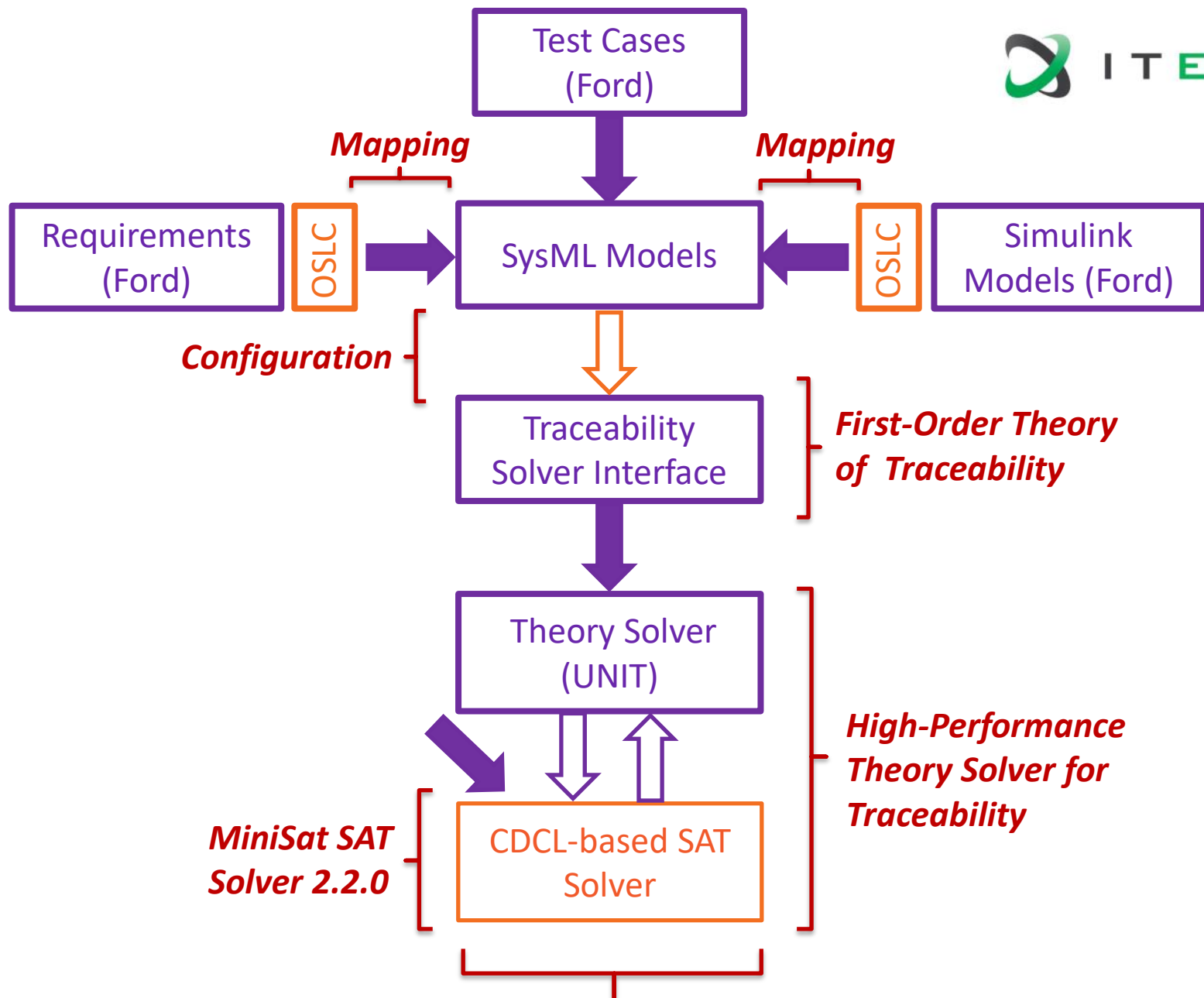


Finer-Grained Unsatisfiability Cores and Stronger Numerical Analysis



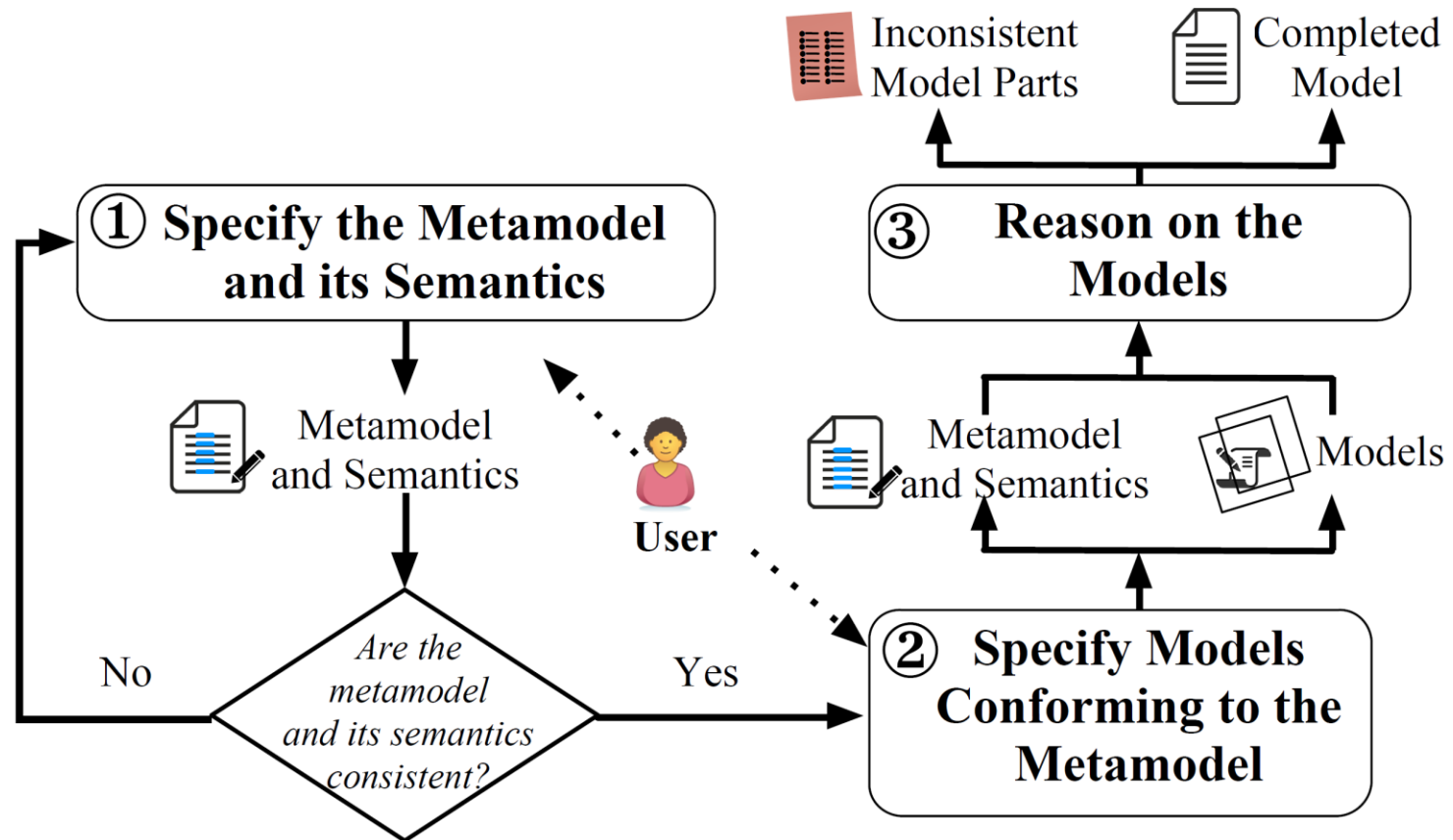
Checking properties without type cardinalities (type finitization)



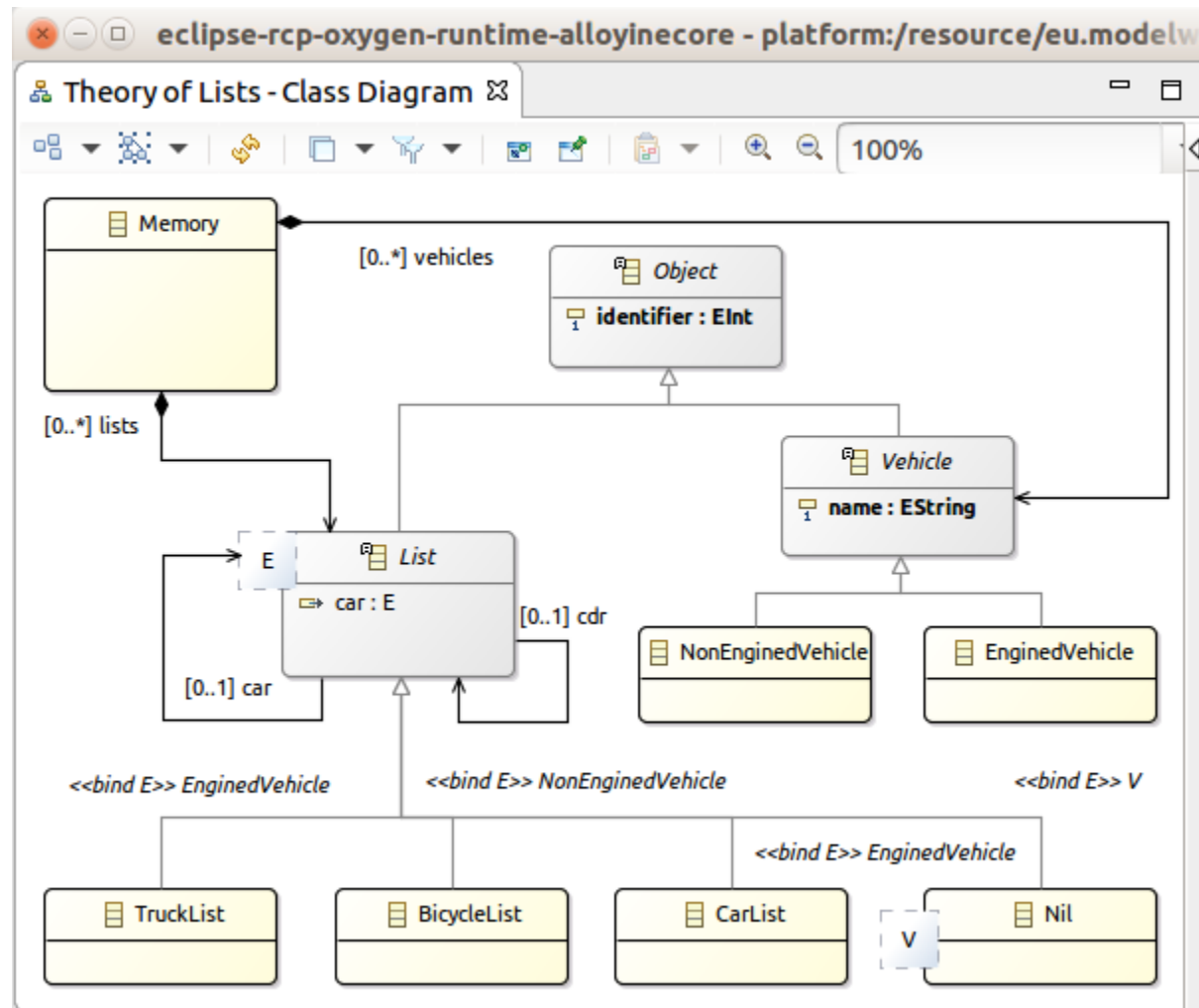


Consistency and Completeness Checking

AlloyInEcore – Tool Overview

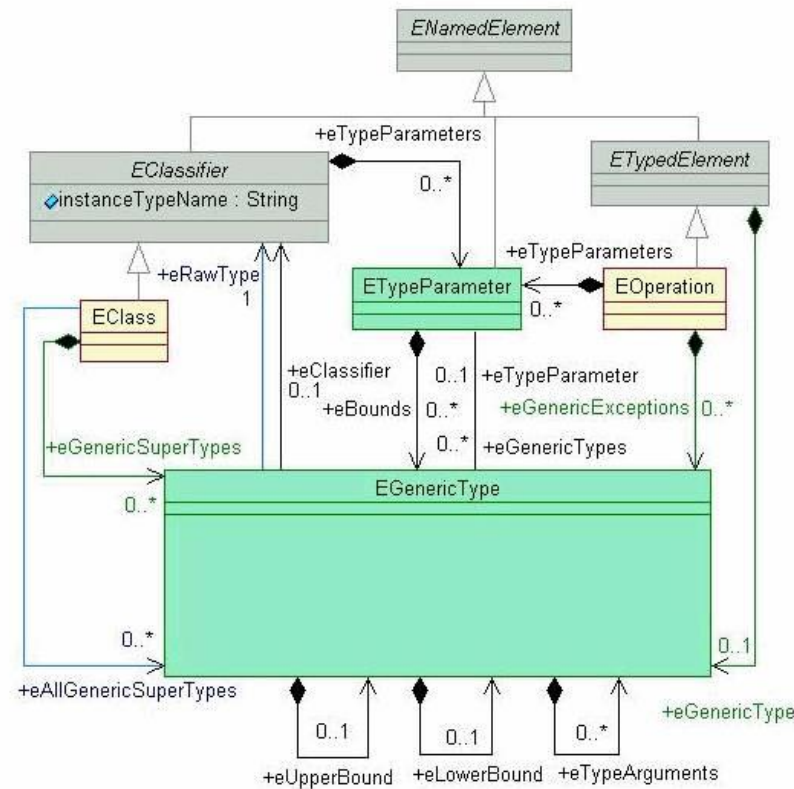


Metamodel – Class Diagram

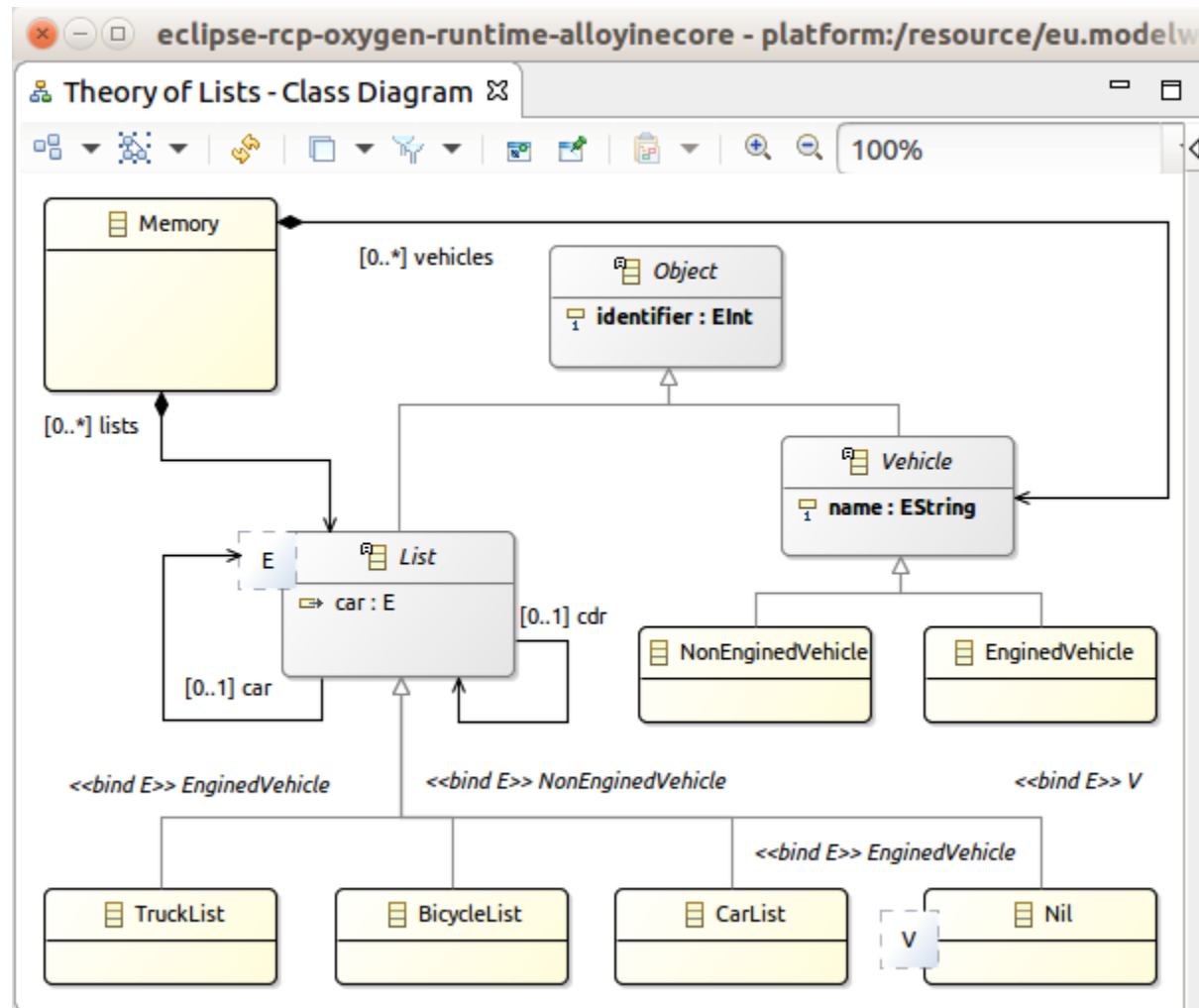




Meta-object Facility (MOF) in Eclipse Modeling Framework (EMF)



Metamodel / UML Class Diagram

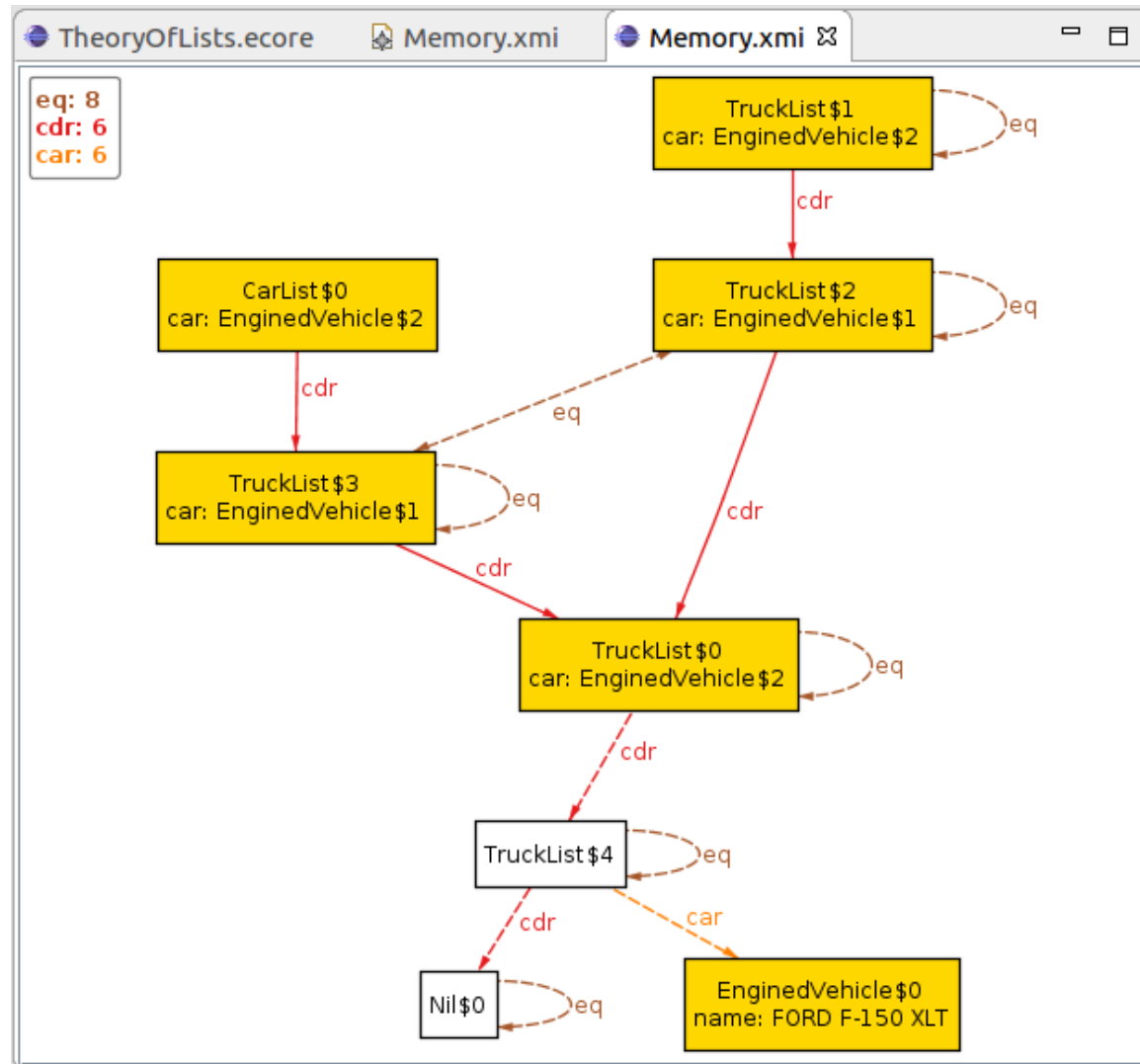


```

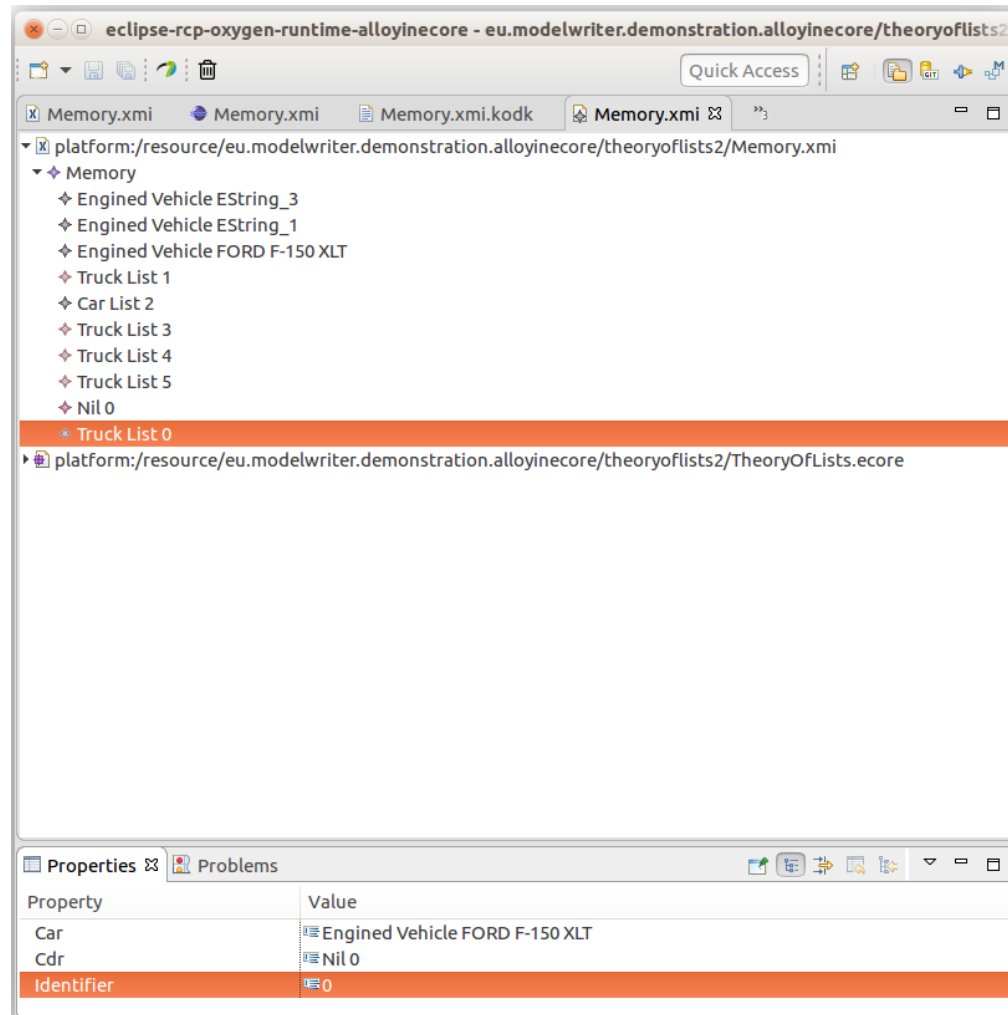
TheoryOfLists.ecore Memory.xmi Memory.xmi
1 import Ecore : 'http://www.eclipse.org/emf/2002/Ecore';
2
3 package theoryoflists: tol= 'eu.modelwriter.examples.theoryoflists'{
4   public abstract class Object {
5     ghost attribute identifier : Integer;
6   }
7
8   public abstract class List<E> extends Object [5,7] {
9     property car : E [?];
10    property cdr : List<E> [?] {acyclic};
11    model property eq : List<E> [*] ;
12
13    invariant: all a, b: List | a in b.eq iff (a.car = b.car
14      and a.cdr in b.cdr.eq and a.class = b.class);
15
16    invariant noStrayObjects: all v: Object - List | some v.~car;
17  }
18
19  public class one Nil<V> extends List<V>  {
20    invariant : no Nil.car;
21    invariant : no Nil.cdr;
22    invariant : all l: List - Nil | some l.cdr && some l.car;
23    invariant : all l: List | Nil in l.*cdr;
24  }
25
26  private class one Memory {
27    property some vehicles : Vehicle [*] {composes};
28    property some lists : List<? extends Vehicle> [*] {composes};
29  }
30
31  abstract class Vehicle extends Object [2,4] {
32    attribute name : String;
33    invariant : all disj a, b: Vehicle | a.name != b.name;
34    invariant : one v: Vehicle | v.name = "FORD F-150 XLT";
35  }
36
37  class EnginedVehicle extends Vehicle;
38  class NonEnginedVehicle extends Vehicle;
39
40  class TruckList extends List<EnginedVehicle>;
41  class CarList extends List<EnginedVehicle>;
42  class BicycleList extends List<NonEnginedVehicle>;
43 }

```

Completing Partial Model



Partial Objects/Models



The screenshot shows the Eclipse IDE interface. The top toolbar includes icons for file operations and a 'Quick Access' search bar. The project explorer on the left shows the project structure. The main editor area displays the contents of 'Memory.xmi', which is a list of objects. The 'Truck List 0' object is selected, and the Properties view at the bottom shows its properties.

Property	Value
Car	Engined Vehicle FORD F-150 XLT
Cdr	Nil 0
Identifier	0

Partial Objects/Models

eclipse-rcp-oxygen-runtime-alloyinecore - eu.modelwriter.demonstration.alloyinecore/theoryoflists2

Memory.xmi Memory.xmi Memory.xmi.kodk Memory.xmi

```

1 <?xml version="1.0" encoding="UTF-8"?>
2 <tol:Memory xmi:version="2.0" xmlns:xmi="http://www.omg.org/XMI"
3   xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
4   xmlns:tol="eu.modelwriter.examples.theoryoflists"
5   xsi:schemaLocation="eu.modelwriter.examples.theoryoflists TheoryOfLists.ecore">
6   <vehicles xsi:type="tol:EnginedVehicle" name="EString_3"/>
7   <vehicles xsi:type="tol:EnginedVehicle" name="EString_1"/>
8   <vehicles xsi:type="tol:EnginedVehicle" name="FORD F-150 XLT"/>
9   <lists xsi:type="tol:TruckList" identifier="1" car="//@vehicles.1" cdr="//@lists.6"/>
10  <lists xsi:type="tol:CarList" identifier="2" car="//@vehicles.1" cdr="//@lists.4"/>
11  <lists xsi:type="tol:TruckList" identifier="3" car="//@vehicles.1" cdr="//@lists.3"/>
12  <lists xsi:type="tol:TruckList" identifier="4" car="//@vehicles.0" cdr="//@lists.0"/>
13  <lists xsi:type="tol:TruckList" identifier="5" car="//@vehicles.0" cdr="//@lists.0"/>
14  <lists xsi:type="tol:nil"/>
15  <lists xsi:type="tol:TruckList" car="//@vehicles.2" cdr="//@lists.5"/>
16 </tol:Memory>
17

```

Design Source

Properties Problems

Property	Value
General	
car	//@vehicles.2
cdr	//@lists.5
xsi:type	tol:TruckList

Checking Inconsistency

Memory.xml
Memory.xml

cdr: 5
car: 5

CarList\$0
car: EngineVehicle\$1

TruckList\$1
car: EngineVehicle\$1

TruckList\$3
car: EngineVehicle\$0

TruckList\$2
car: EngineVehicle\$0

TruckList\$0
car: EngineVehicle\$1

EngineVehicle\$2

```

graph TD
    C[CarList$0  
car: EngineVehicle$1] -- cdr --> T3[TruckList$3  
car: EngineVehicle$0]
    T1[TruckList$1  
car: EngineVehicle$1] -- cdr --> T2[TruckList$2  
car: EngineVehicle$0]
    T3 -- cdr --> T0[TruckList$0  
car: EngineVehicle$1]
    T2 -- cdr --> T0
    T0 -- cdr --> T0
    
```

TheoryOfLists.ecore

```

8 public abstract class List<E> extends Object [6,7] {
9   property car : E [?];
10  property cdr : List<E> [?] {acyclic};
11  model property eq : List<E> [*] {reflexive};
12
13  invariant: all a, b: List | a in b.eq iff (a.car = b.car
14                                and a.cdr in b.cdr.eq and a.class = b.class);

```

Problems
1 error, 0 warnings, 0 others

Description	Location	Type
Errors (1 item) (all l: one List !(l in (l . ^cdr)))	line 10	AlloyInEcore Unsat Formula

Disseminations

Runtime Verification Summit - ARVI COST meeting
(19-23 March 2018, Grenoble, France)



ITEA-Assume Project Workshop @ Airbus Headquarters
(April 6-7, 2018. Toulouse, France)



Workshop on the Future of Alloy, CSAIL, Massachusetts Institute of Technology
(April 30 & May 1, 2018. Cambridge, MA, USA)



Formal Methods Division, Chalmers University of Technology and University of Gothenburg
(June 4-22, Gothenburg, Sweden)



International Summer School on Satisfiability, Satisfiability Modulo Theories, and Automated Reasoning (3-6 July 2018, University of Manchester, United Kingdom)



ACM SIGSOFT Symposium on the Foundations of Software Engineering (ESEC/FSE 2018)
(4 - 9 Nov 2018, Florida, United States)

Disseminations

Runtime Verification Summit - ARVI COST meeting
(19-23 March 2018, Grenoble, France)



ITEA-Assume Project Workshop @ Airbus Headquarters
(April 6-7, 2018. Toulouse, France)



Workshop on the Future of Alloy, CSAIL, Massachusetts Institute of Technology
(SA)

Wolfgang Ahrendts and Gerardo Schneider
StaRVOOrS (STatic and Runtime Verification of Object-ORiented Software)

Formal Methods Division, Chalmers University of Technology and University of Gothenburg
(June 4-22, Gothenburg, Sweden)



International Summer School on Satisfiability, Satisfiability Modulo Theories, and Automated Reasoning (3-6 July 2018, University of Manchester, United Kingdom)



ACM SIGSOFT Symposium on the Foundations of Software Engineering (ESEC/FSE 2018)
(4 - 9 Nov 2018, Florida, United States)

Disseminations

Runtime Verification Summit - ARVI COST meeting
(19-23 March 2018, Grenoble, France)



ITEA-Assume Project Workshop @ Airbus Headquarters
(April 6-7, 2018. Toulouse, France)



Workshop on the Future of Alloy, CSAIL, Massachusetts Institute of Technology
(April 30 & May 1, 2018. Cambridge, MA, USA)



Formal Methods Division, Chalmers University of Technology and University of Gothenburg
(June 4-22, Gothenburg, Sweden)



Koen Lindström Claessen (Paradox Model Finder)

International Summer School on Satisfiability, Satisfiability Modulo Theories, and Automated Reasoning (3-6 July 2018, University of Manchester, United Kingdom)



ACM SIGSOFT Symposium on the Foundations of Software Engineering (ESEC/FSE 2018)
(4 - 9 Nov 2018, Florida, United States)

Disseminations

Runtime Verification Summit - ARVI COST meeting
(19-23 March 2018, Grenoble, France)



ITEA-Assume Project Workshop @ Airbus Headquarters
(April 6-7, 2018. Toulouse, France)



Workshop on the Future of Alloy, CSAIL, Massachusetts Institute of Technology
(April 30 & May 1, 2018. Cambridge, MA, USA)



Formal Methods Division, Chalmers University of Technology and University of Gothenburg
(June 4-22, Gothenburg, Sweden)

Giles Reger (Vampire Theorem Prover – MACE-style Model Finding)



International Summer School on Satisfiability, Satisfiability Modulo Theories, and Automated Reasoning (3-6 July 2018, University of Manchester, United Kingdom)



ACM SIGSOFT Symposium on the Foundations of Software Engineering (ESEC/FSE 2018)
(4 - 9 Nov 2018, Florida, United States)

Disseminations

Runtime Verification Summit - ARVI COST meeting
(19-23 March 2018, Grenoble, France)



ITEA-Assume Project Workshop @ Airbus Headquarters
(April 6-7, 2018. Toulouse, France)



Workshop on the Future of Alloy, CSAIL, Massachusetts Institute of Technology
(April 30 & May 1, 2018. Cambridge, MA, USA)



Formal Methods Division, Chalmers University of Technology and University of Gothenburg
(June 4-22, Gothenburg, Sweden)



International Summer School on Satisfiability, Satisfiability Modulo Theories, and Automated Reasoning (3-6 July 2018, University of Manchester, United Kingdom)

Tool Demonstration Paper



ACM SIGSOFT Symposium on the Foundations of Software Engineering (ESEC/FSE 2018)
(4 - 9 Nov 2018, Florida, United States)

**Thank you for your attention
We value your opinion and
questions.**