



**27<sup>th</sup>** annual **INCOSE**  
international symposium

**Adelaide, Australia**

July 15 - 20, 2017



# Semantically-enabled Model-based Systems Engineering of Safety-critical Network of Systems

Leonard Petnga (1), Mark Austin (2) and Mark Blackburn (3)

Affiliations: (1) University of Alabama, (2) University of Maryland, and (3) Stevens Institute of Technology.

---



# Outline

1. Problem Statement
2. State-of-the-Art Capability
3. Semantic Foundations for MBSE
4. Problem Solving Strategies
5. Simple Example (Family-School-Urban Dynamics)
6. Temporal and Spatial Logic
7. Integration Challenge (Safety at Traffic Intersections)
8. Scaling things up (Work in Progress)
9. References

**Acknowledgement:** Financial support and collaborations with NAVAIR and NIST.

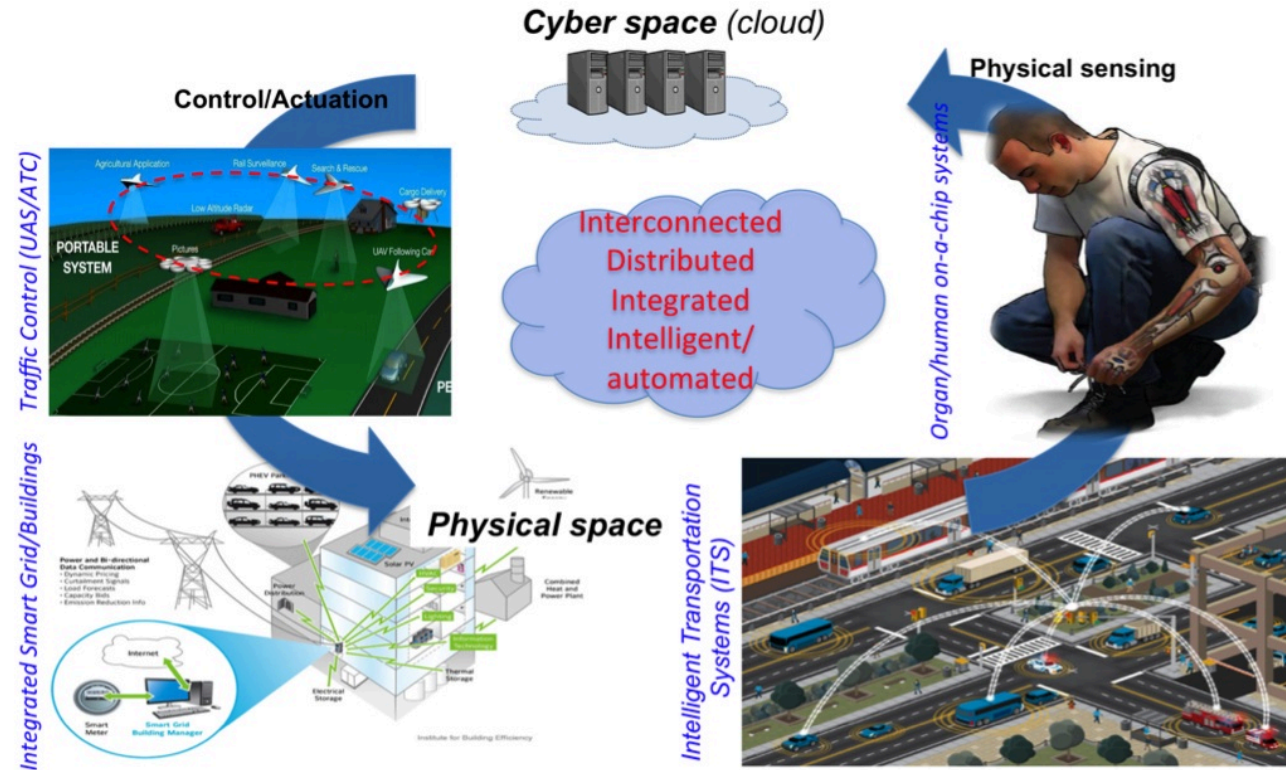


# Problem Statement

Need for Model-Based Systems Engineering  
Approaches for Network of Systems (NoS)



# What is a Network of Systems (NoS)?



**Definition:** Aggregation of **system of systems** (SoS) and complex **cyber-physical systems** (CPSs) operating in a **networked environment**.



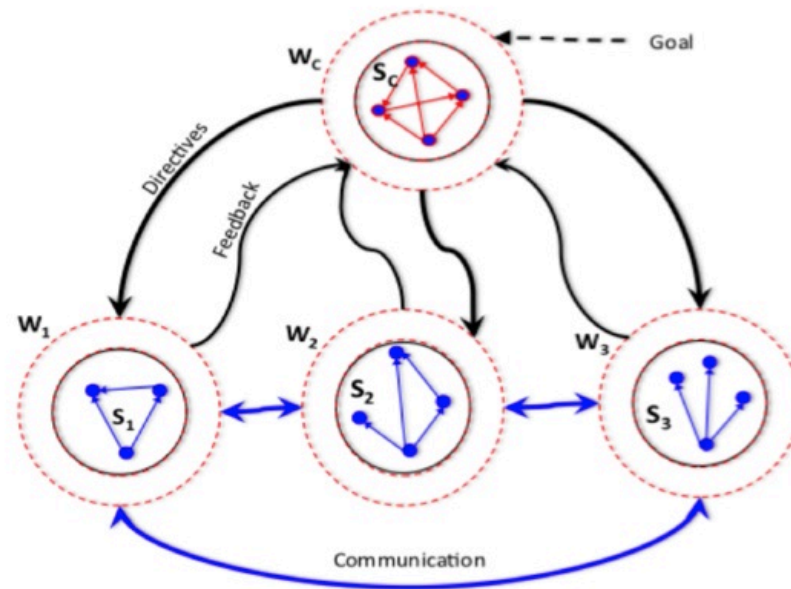
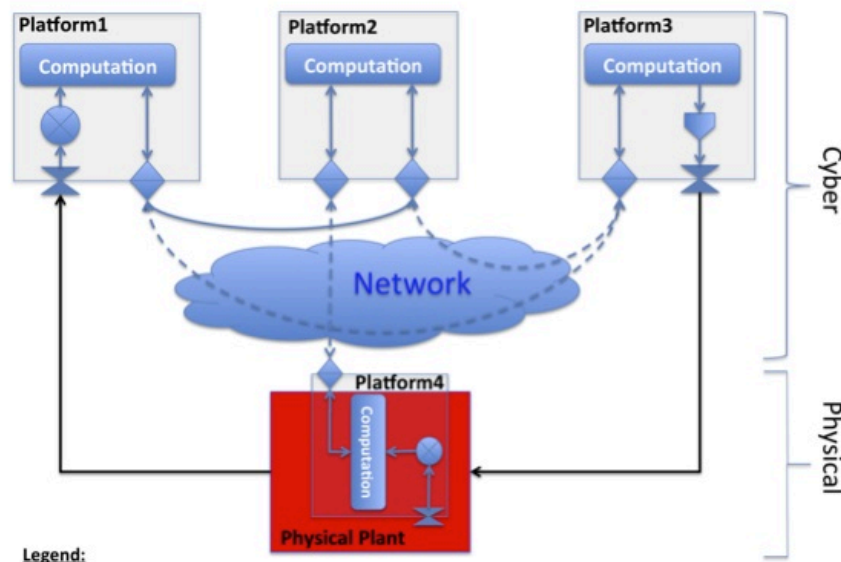
# Network of Systems Backbone: CPS and SoS

## Local: Cyber-Physical Systems(CPS)

- Tight integration of cyber and physical elements
- Distributed/networked system components
- Embedded computational platforms

## Global: System of Systems(SoS)

- Arrangement of systems into an independent, larger system
- Mission oriented, with weak (and/or tight) coupling of components
- Might have human in the loop

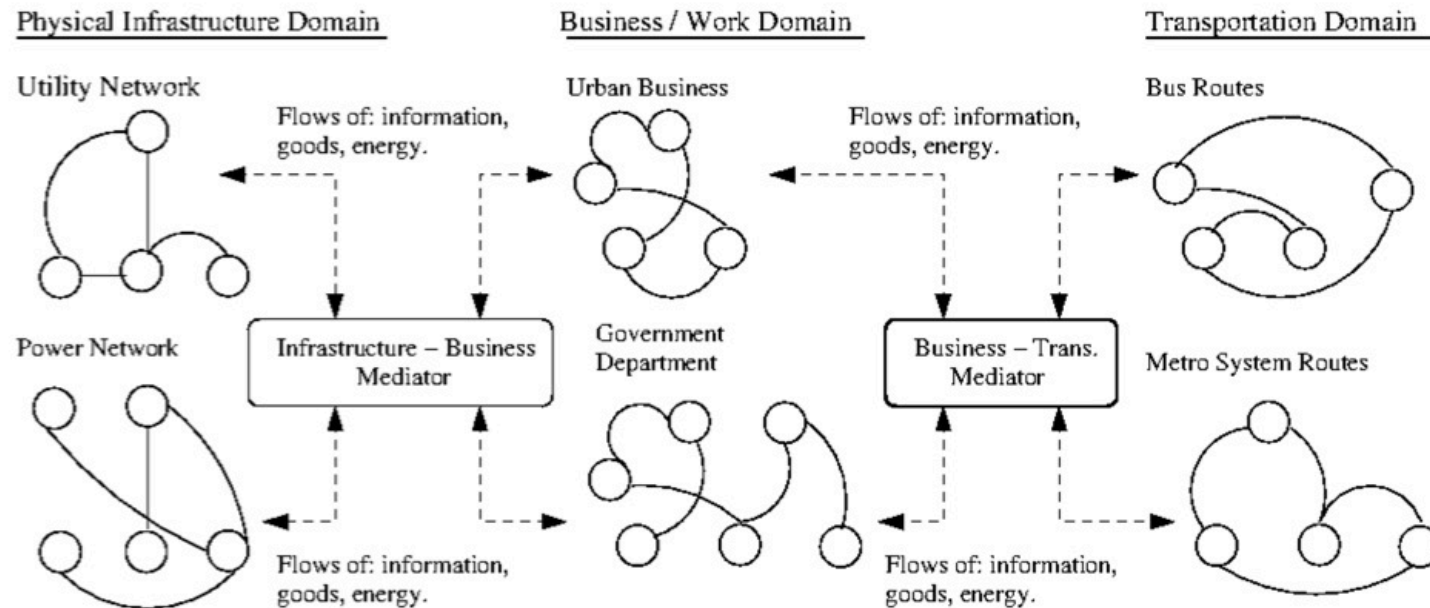


# Distributed System Behavior Modeling for NoS



## Enabling Distributed System Control

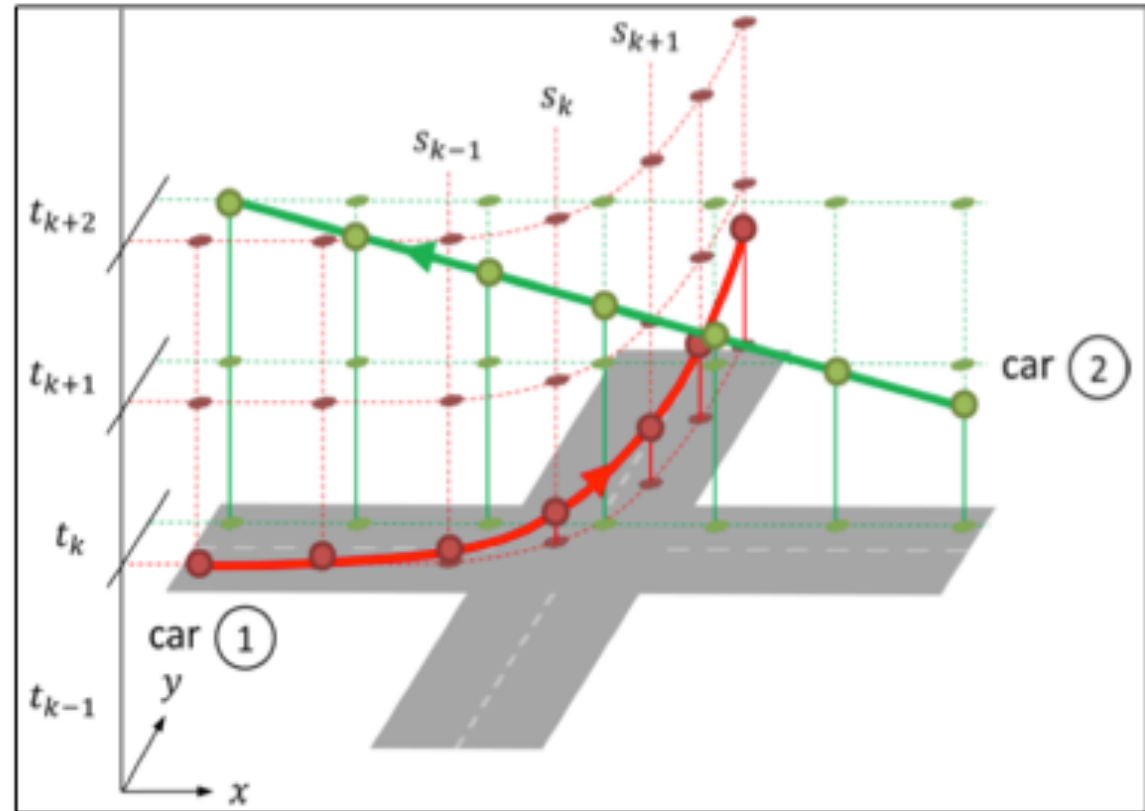
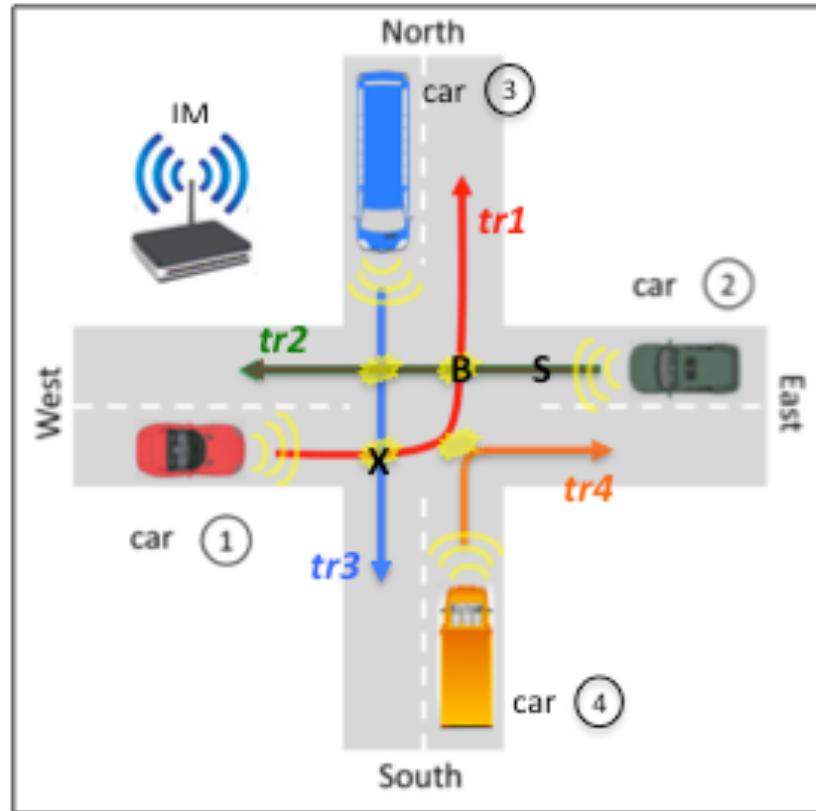
- **Research Question:** How should decision makers **cooperate** to achieve system-wide performance and management objectives in large scale NoS?
  - **Solution strategy:** behavior modeling with ontologies, rules and message-passing mechanisms  $\Rightarrow$  many-to-many interactions in the SP
- [Austin,2015]



**Source:** Coelho, Austin and Blackburn, 2017.



# Motivating Application: Safety of Self-driving Cars



**Key Challenges:** Distributed and concurrent behaviors; networking obstructions; delays; safety-critical operations; need for **formal approaches to analysis**.



# Transition to Semantically-enabled MBSE

**Two basic questions:** 1. What does state-of-the-art MBSE for NoS look like? 2. How efficient are the semantic foundations?



# State-of-the-Art MBSE Capability

Figure: Big picture MBSE [Austin, 2011]

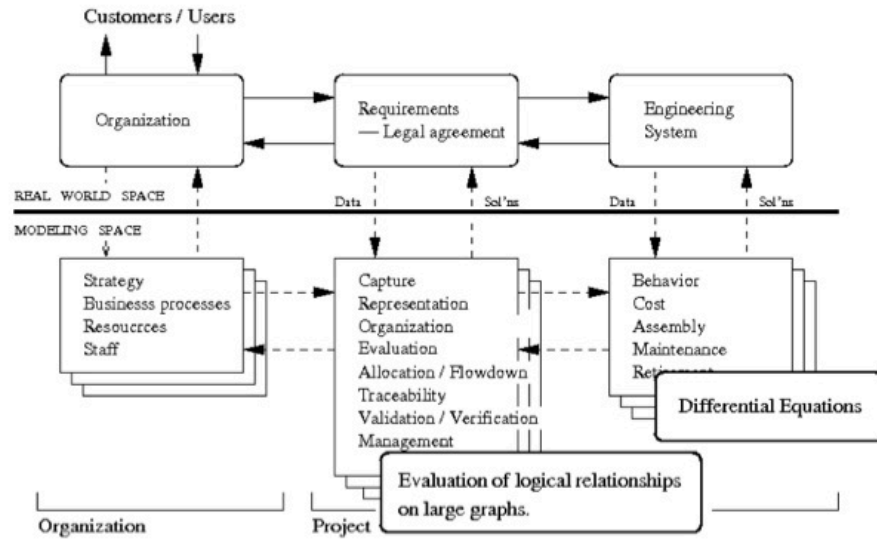
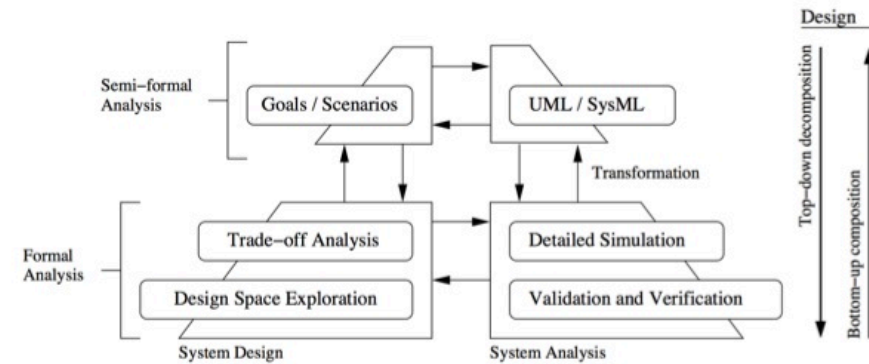


Figure: Multi-level approach [Mosteller, 2014]



Design correctness  $\Rightarrow$  **semantic-driven approach** to modeling/integration

## MBSE ill-equipped for decision making/reasoning

- Requirements elicitation/specification, weak language/physical semantics
- **Separation of concerns**  $\Rightarrow$  loose coupling
- **Broken integration approaches** formal vs semi-formal models.



# Semantics in MBSE

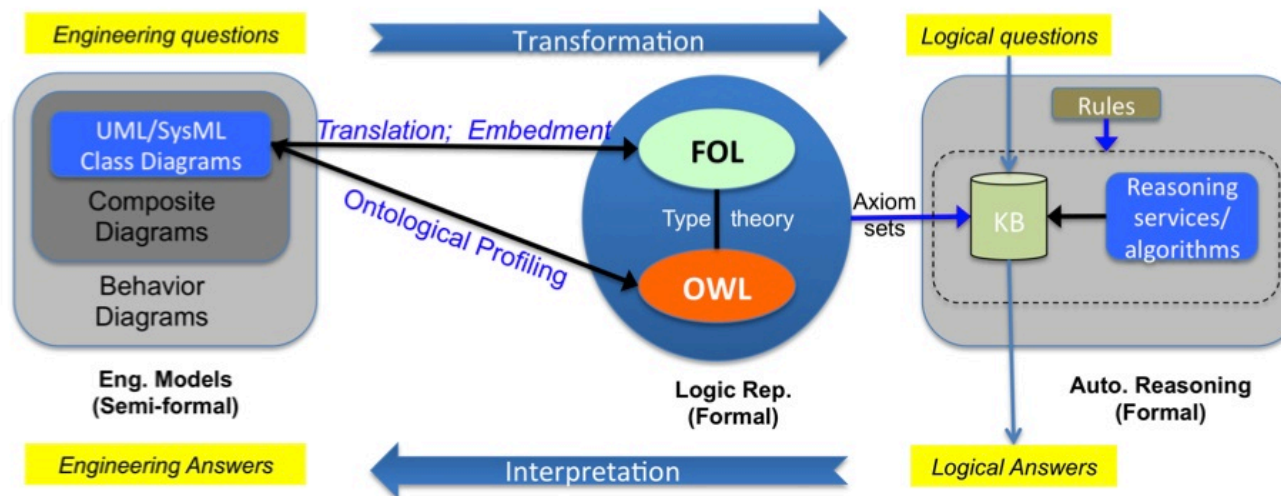


## Why semantics for MBSE?

- **Meaning of models:** formal VS lexical VS conceptual
- **In practice:** precise def. of intended behavior of ontology-based tools/systems;
- Semantics defined in terms of models in the sense of model theory

## Semantics Support Approaches for MBSE

- **Language retrofitting:** logic strengthens semantics of UML, SysML [Graves, 2012]
- **Ontological profiling:** profile in the modeling tool (OWL-SysML) [Wagner, 2012]



**Ans.:** Model inconsistencies, redundancies.

**Q.:** System level req. (safety)?, Dynamics?



# Strategic Approaches to Development

**Basic issue:** How to remain productive in the face of rapidly increasing system complexity?



# Tenets of Our Approach

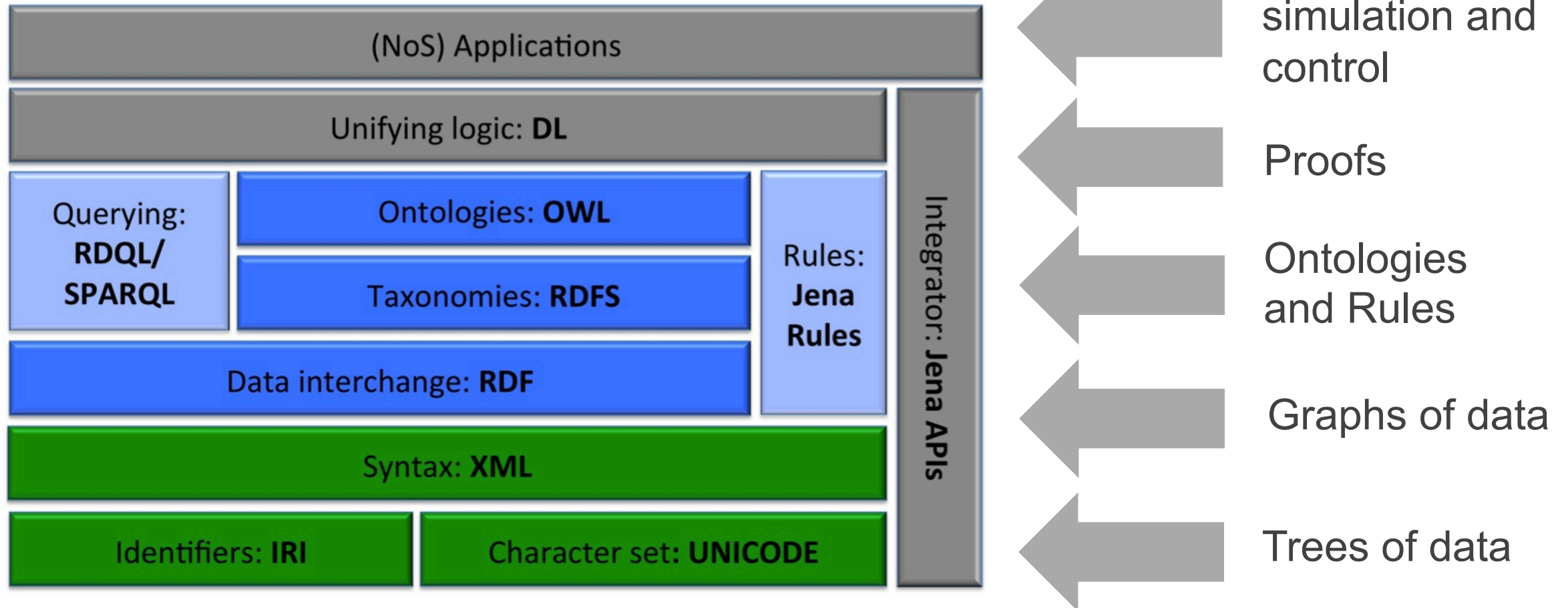
**Tenet 1:** NoS should be designed and managed through the use of models, as opposed to documents

- Bang for the bucks: minimal mechanism, maximal function
- Reliable operation in a wide range of environments
- Ease of accommodation for future technical improvements

**Tenet 2:** NoS design methodologies need to employ semantic descriptions of domains and formal reasoning

- Adaptive validation of requirements
- Multidiscipline/models communication and integration
- “Data” instead of “Tool-to-tool” interoperability
- Assessment of system capability in uncertain environments

# Enabling Infrastructure: Semantic Web Layer Cake



## Legend:

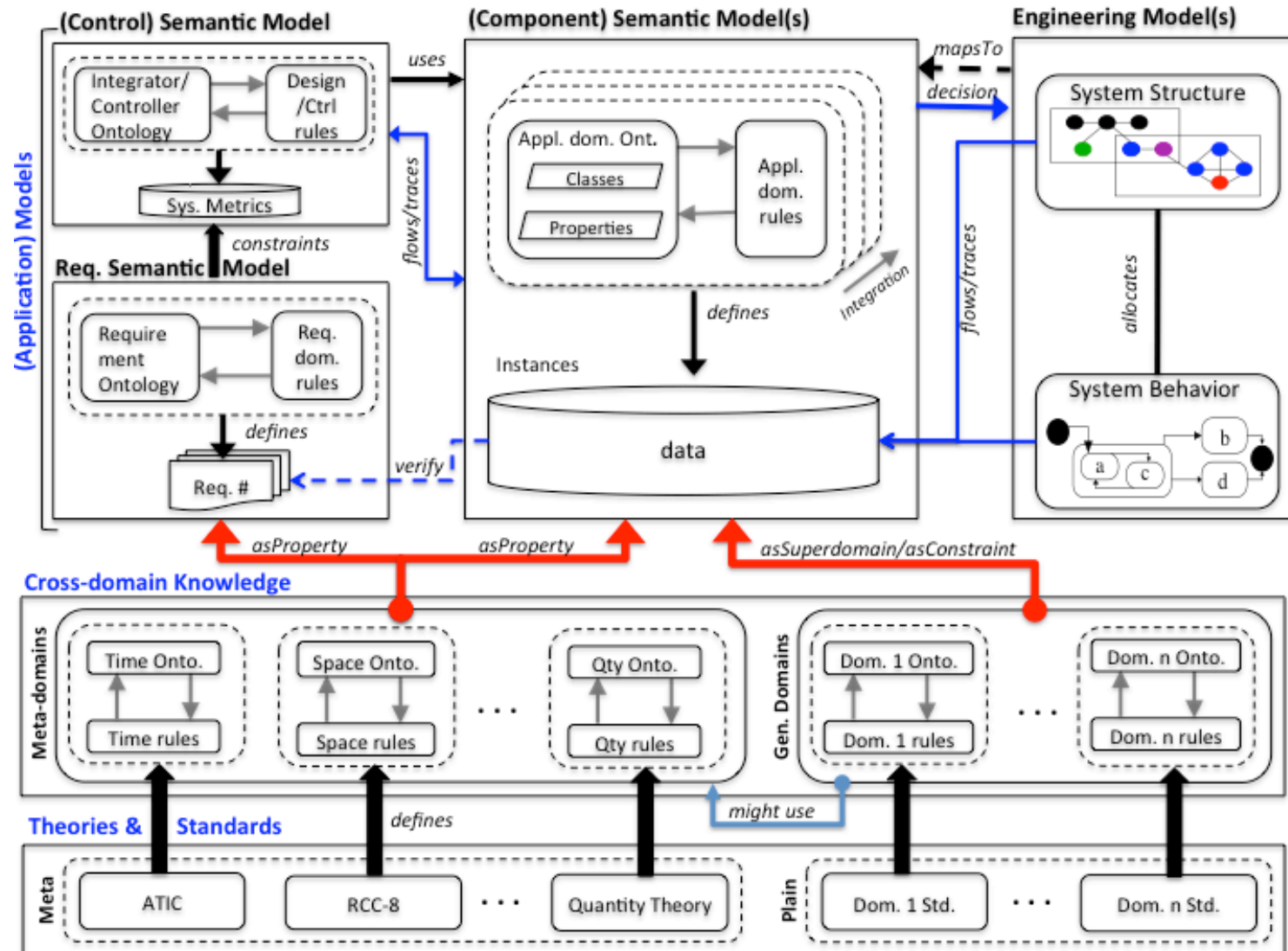




# System Architecture (Work in Progress)

Semantic Model

Cross-domain knowledge



Engineering Models

Theories and Standards



# Simple Example

# Simplified Semantic Modeling of a Family ....

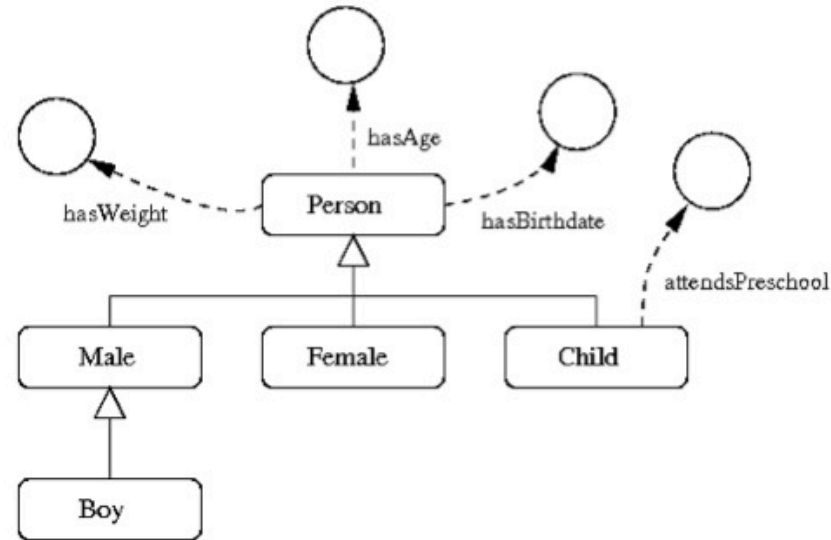


Fact. Sam is a boy. He was born October 1, 2007.

Rule 1: For a given date of birth, a built-in function `getAge()` computes a person's age.

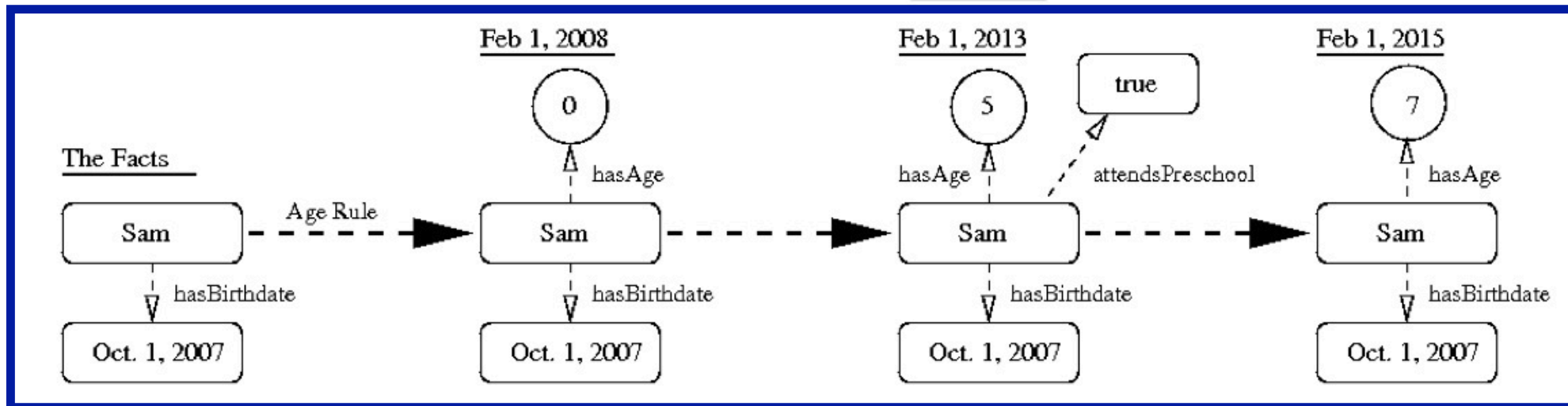
Rule 2: A child is a person with age < 18.

Rule 3: Children who are age 5 attend preschool.



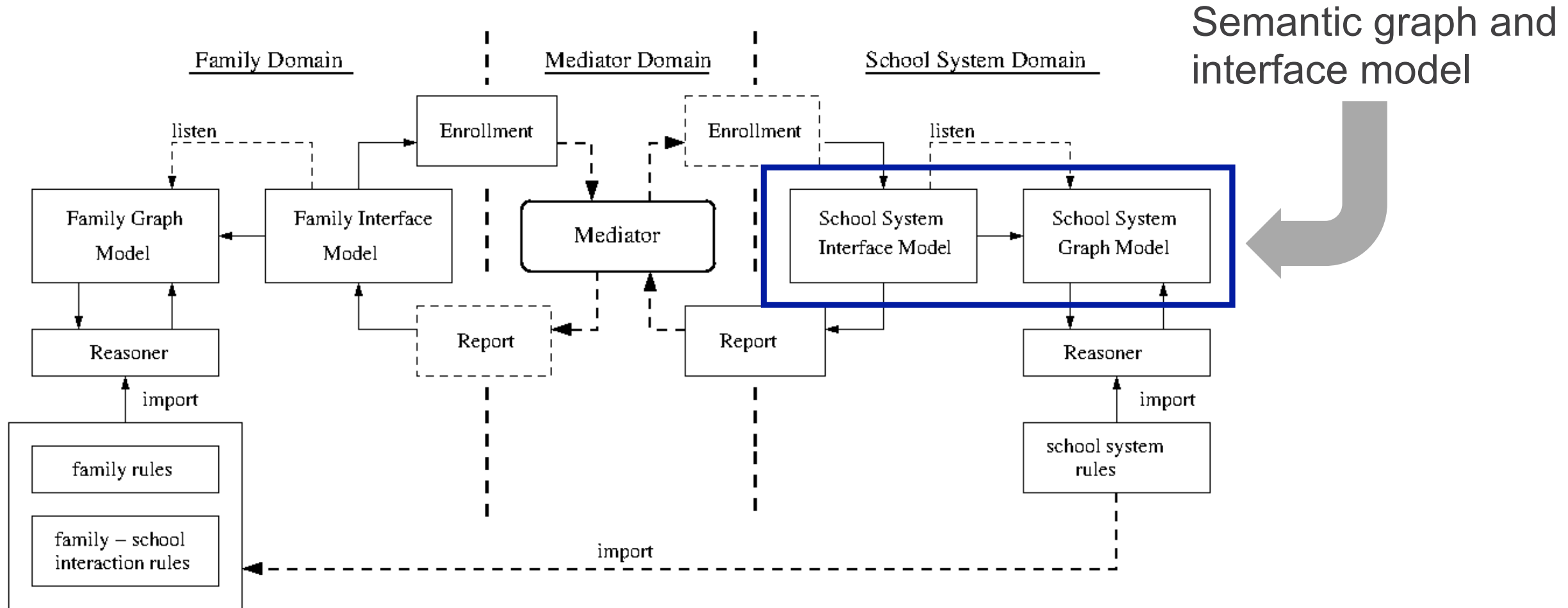
Ontology

Event-driven  
evolution of  
semantic graph.



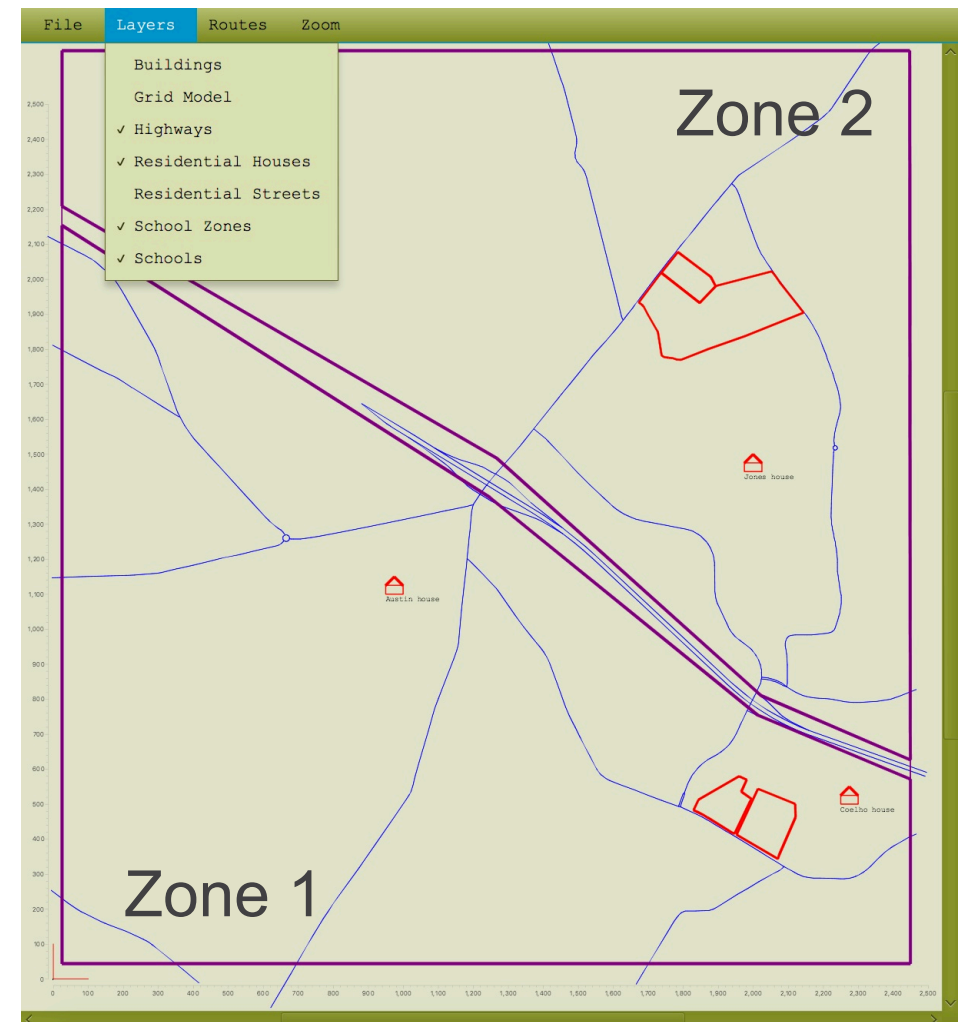
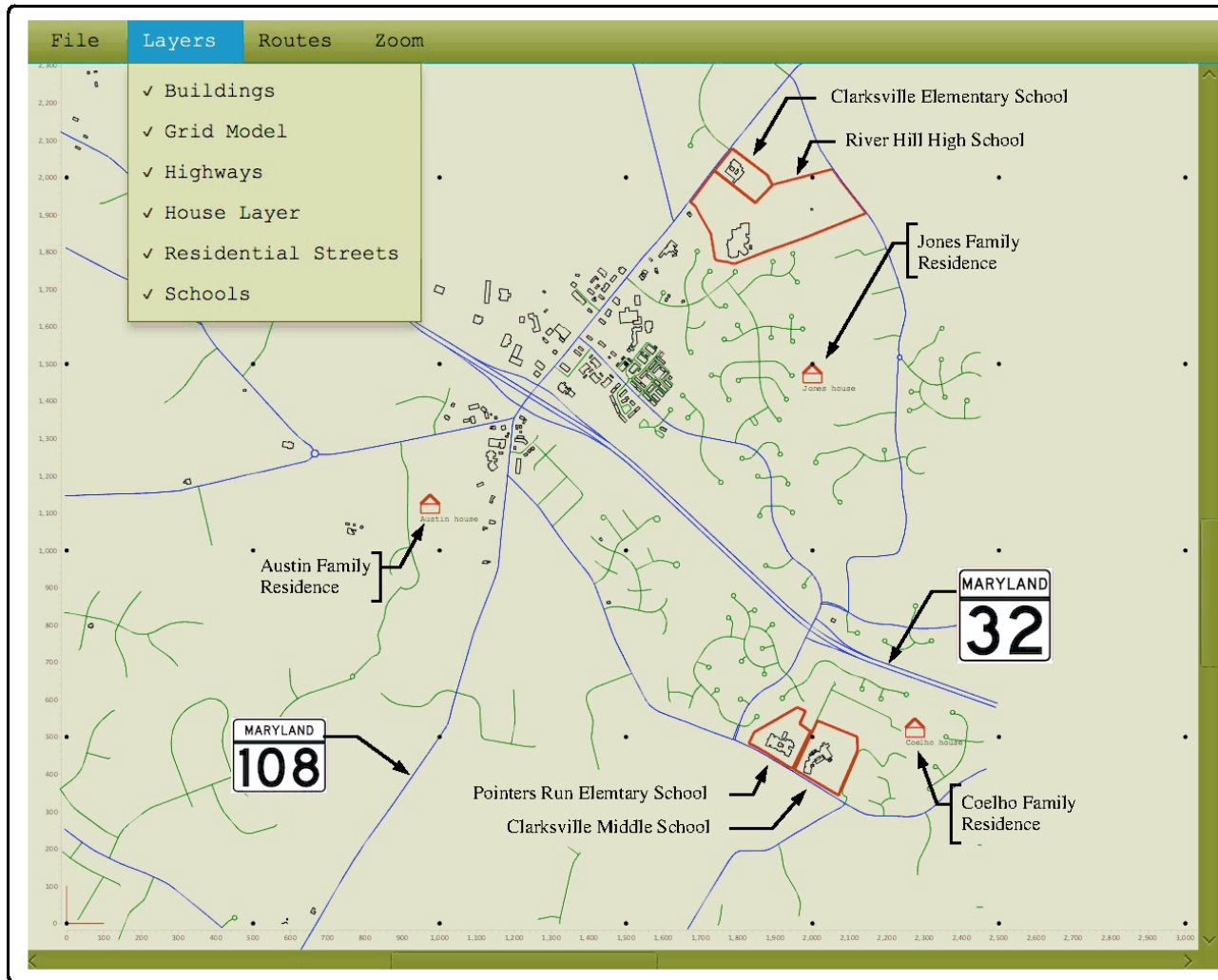
Source: Delgoshaei, Austin, Pertzborn 2014.

# Behavior Modeling of Family-School Interactions



**Source:** Coelho, Austin and Blackburn, 2017.

# Family-School-Urban System Dynamics





# Temporal and Spatial Logic

**Basic issue:** How do notions of space and time affect safety in safety-critical NoS? How should we reason with spatial and temporal phenomena?



# Hierarchies of Logic

**Temporal Logic:** Describes how the conditions of a system changes over time:

**We want to know what is true, and when?**

**Spatial Logic:** Is concerned with regions and their connectivity, allowing one to address issues of the form:

**We want to know what is true, and where?**

**Spatio-Temporal Logic:** Spatial logics are combined with temporal logics, allowing one to address issues of the form:

**We want to know not only what is true, but when and where?**



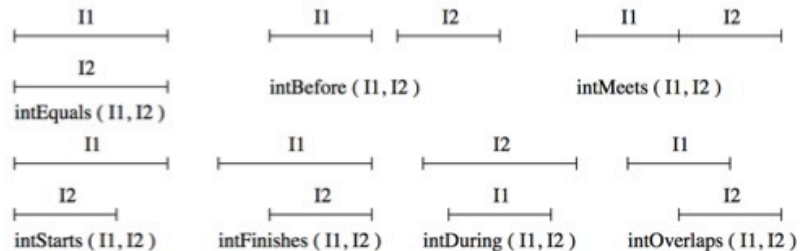
# Allen's Temporal Interval Calculus (ATIC)

## Features

- **Interval-based models:** formal analysis having time-dependent behavior
- **Proper Time Intervals** with fully specified Time-points for reasoning
- **Restricted axioms ensuring time reasoning decidability** (in OWL DL)
- **Temporal properties and their evolutions:**
  - (1) **Mereology** (part-of): Does  $t$  occur within  $I_1$ ?,
  - (2) **Topological**(connects): Do intervals  $I_1$  and  $I_2$  meet? and,
  - (3) **Logical** (rules-based) : Does proposition  $\phi$  hold within the interval  $I_1$ ?

## Thirteen (13) relations

### Seven main relationships

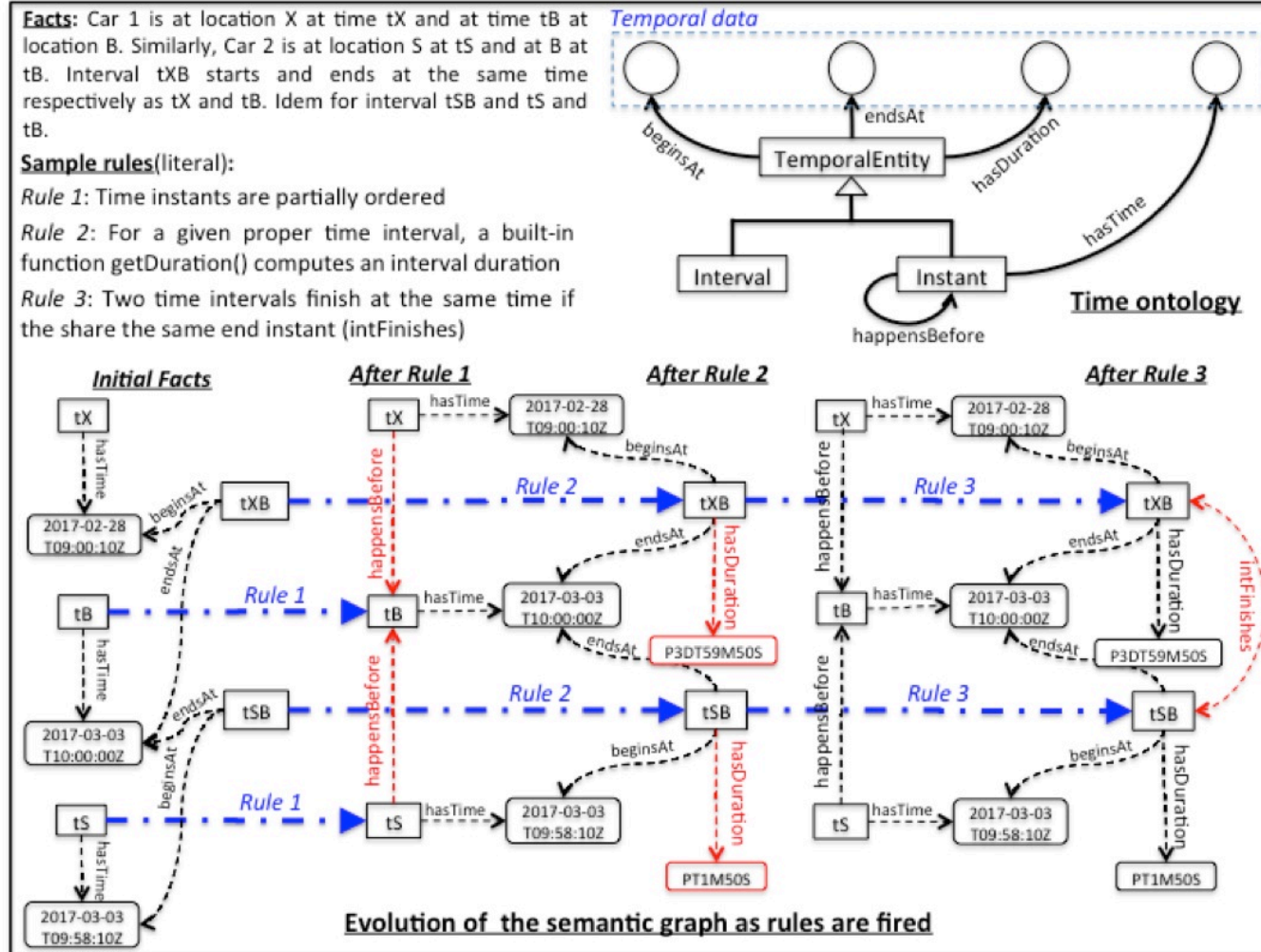


### Example (intOverlaps)

$$\begin{aligned} \text{intOverlaps}(I_1, I_2) \equiv & [\text{ProperInterval}(I_1) \wedge \text{ProperInterval}(I_2)] \\ & \wedge (\exists t_2, t_3)[\text{ends}(t_2, I_1) \wedge \text{begins}(t_3, I_2) \wedge \text{before}(t_3, t_2)] \\ & \wedge (\forall t_1)[\text{begins}(t_1, I_1) \Rightarrow \text{before}(t_1, t_3)] \\ & \wedge (\forall t_4)[\text{ends}(t_4, I_2) \Rightarrow \text{before}(t_2, t_4)] \end{aligned}$$



# Illustration: ATIC-based Time Ontology and Reasoning



Time Ontology

Event-driven  
evolution of the  
Semantic Graph

# Reusable Semantic Block (Time)

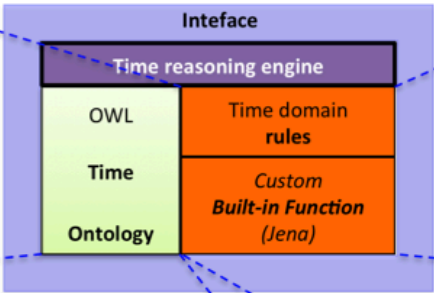


Ontology (OWL)

Jena Rules

Built-in Functions

```
time.rules
12
13 // Rule Def01: Definition of an BegDur Interval .... greaterThan(?d,P)
14
15 [ BegDurIntervDef: (?x rdf:type af:TemporalEntity) (?x af:hasDuration ?d) (?x
16
17 // Rule Def02: Definition of an EndDuration Interval .... greaterThan(?d,P)
18
19 [ EndDurIntervDef: (?x rdf:type af:TemporalEntity) (?x af:hasDuration ?d) (?x
20
21 // Rule Def03: Definition of an BegEnd Interval ....
22
23 [ BegEndIntervDef: (?x rdf:type af:TemporalEntity) (?x af:beginsAt ?t1) (?x d
24
25 // Rule Def04: Definition of an open Interval ....
```



```
myTimeOntology.owl
91
92 // Object Properties
93
94 -->
95 <!-- http://www.isi.edu/~pan/damlttime/time-entry.owl#happensBefore -->
96
97 <rdf:Description rdf:about="&time-entry;happensBefore">
98   <rdf:type rdf:resource="&owl;AsymmetricProperty"/>
99 </rdf:Description>
100
101 <!-- http://www.isi.edu/~pan/damlttime/time-entry.owl#hasDuration -->
102
103 <rdf:Description rdf:about="&time-entry;hasDuration">
104   <rdf:type rdf:resource="&owl;FunctionalProperty"/>
105 </rdf:Description>
```

```
GetGreaterThanUnit.java
85
86 @Override
87 public boolean bodyCall(Node[] args, int length, RuleContext context) {
88   checkArgs(length, context);
89   BindingEnvironment env = context.getEnv();
90   Node n1 = getArg(0, args, context);
91   Node n2 = getArg(1, args, context);
92   Node n3 = getArg(2, args, context);
93   String incompatibleUnits="";
94
95   System.out.println("");
96   System.out.println("In GetGREATER_THAN_UNIT.bodyCall()....");
97
98   if (n1.isLiteral() == true && n2.isLiteral() == true && n3.isLiteral() == true) {
99     Object v1 = n1.getLiteralValue();
100     Object v2 = n2.getLiteralValue();
101     Object v3 = n3.getLiteralValue();
102
103     Node leBoolean = null;
104
105     if (v1 instanceof String && v2 instanceof String && v3 instanceof String) {
```

# Region Connectedness Calculus (RCC)



## Features of RCC- 8

- 1 **Space-region theory:** convex region of any shape with  $D \geq 1$
- 2 **Mereotopological** description;
- 3 Boundaries; static and dynamic-based **reasoning support**

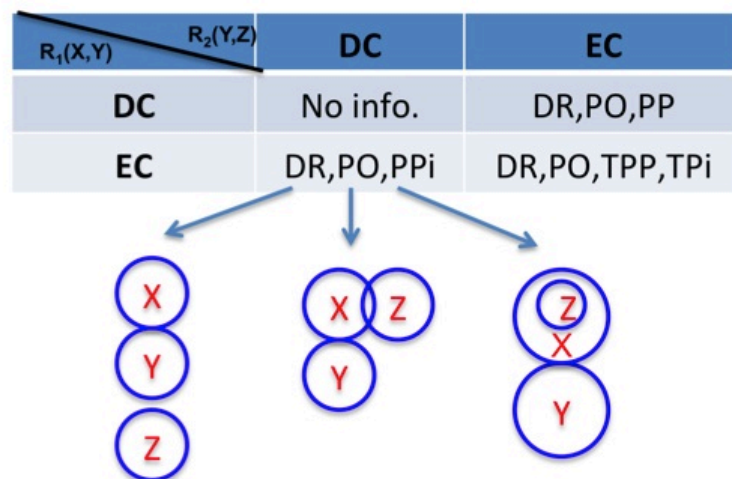


Figure: Composition table(excerpt)

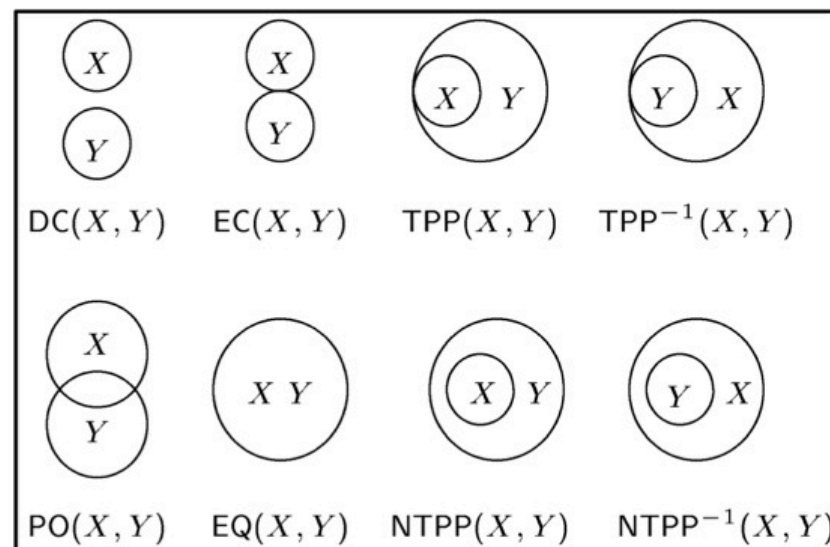


Figure: RCC-8, possibly -5 relations

## Example (Restrictions - for decidability)

- 1 3D abstraction with 0, 1, 2D rep.
- 2 Closed convex spatial entities;
- 3 Regular shapes; No transitivity deductions;



# Illustration: RCC8-based Ontology and Rules

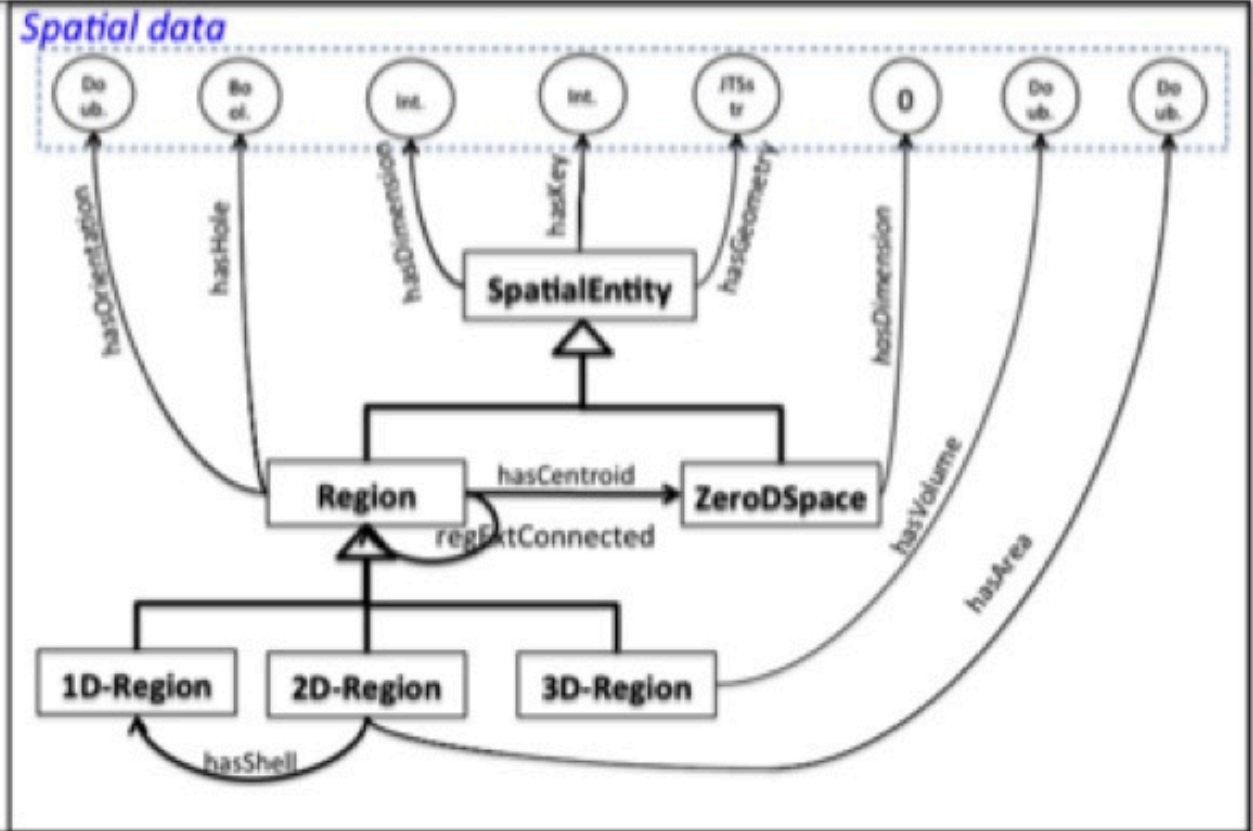
**Facts:** At a given instant  $t$ , cars, as spatial entities  $c1, \dots, c4$  are traveling through a subset of the intersection as spatial entities  $s1, \dots, s4$  respectively along trajectories  $tr1, \dots, tr4$ . Spatial entities types and (JTS) geometries - e.g., Point LineString, Polygon - are known

**Sample rules** (literal):

*Rule 1:* From a given JTS geometry, a built-in function `getGeometryType()` infers the type of a spatial entity

*Rule 2:* For a given type of space, a built-in function `getDimension()`, computes the dimension of a spatial entity

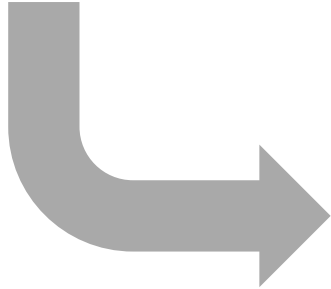
*Rule 3:* Two spatial entities are disconnected if their geometry are disjoint





# Spatial Reasoning with Jena and Jena Rules

Excerpt of  
Region Class



```
[java] Named Class(4): Region
[java] --- Full Name: http://petnga.org/ontologies/space#Region
[java] --- Superclass: Resource ...
[java] --- Superclass: SpatialEntity ...
[java] --- Superclass: Thing ...
[java] --- Subclass: ThreeDRegion ...
[java] --- Subclass: TwoDRegion ...
[java] --- Subclass: OneDRegion ...
[java] --- Disjoint with: ZeroDSpace ...
[java] --- Data Property Name: hasGeometryType ...
[java] --- Domain: SpatialEntity ...
[java] --- Data Property Name: hasDimension ...
[java] --- Domain: SpatialEntity ...
[java] --- Data Property Name: hasGeometry ...
[java] --- Domain: SpatialEntity ...
[java] --- Data Property Name: hasLength ...
[java] --- Domain: Region ...
[java] --- Data Property Name: hasName ...
[java] --- Domain: SpatialEntity ...
[java] --- Object Property Name: regTangPropPartInv ...
[java] --- Domain: Region ...
[java] --- Object Property Name: regNonTangPropPart ...
[java] --- Domain: Region ...
[java] --- Object Property Name: on ...
[java] --- Domain: SpatialEntity ...
[java] --- Object Property Name: regEquals ...
[java] --- Domain: Region ...
[java] --- Object Property Name: regNonTangPropPartInv ...
[java] --- Domain: Region ...
[java] --- Object Property Name: regPartialOverlaps ...
[java] --- Domain: Region ...
[java] --- Object Property Name: inside ...
[java] --- Domain: SpatialEntity ...
[java] --- Object Property Name: hasShell ...
[java] --- Domain: Region ...
[java] --- Object Property Name: regTangPropPart ...
[java] --- Domain: Region ...
[java] --- Object Property Name: regDisConnected ...
[java] --- Domain: Region ...
[java] --- Object Property Name: outside ...
[java] --- Domain: SpatialEntity ...
[java] --- Object Property Name: regExtConnected ...
[java] --- Domain: Region ...
[java] --- Object Property Name: hasCentroid ...
[java] --- Domain: Region ...

Statements: Statements for space s1 ...
Statement[ 1]
  Subject : http://petnga.org/ontologies/space#S1
  Predicate: http://petnga.org/ontologies/space#regEquals
  Object  : http://petnga.org/ontologies/space#S1
Statement[ 2]
  Subject : http://petnga.org/ontologies/space#S1
  Predicate: http://petnga.org/ontologies/space#regDisConnected
  Object  : http://petnga.org/ontologies/space#S0
Statement[ 3]
  Subject : http://petnga.org/ontologies/space#S1
  Predicate: http://petnga.org/ontologies/space#regDisConnected
  Object  : http://petnga.org/ontologies/space#Tr0
Statement[ 4]
  Subject : http://petnga.org/ontologies/space#S1
  Predicate: http://petnga.org/ontologies/space#hasGeometryType
  Object  : "Polygon"
Statement[ 5]
  Subject : http://petnga.org/ontologies/space#S1
  Predicate: http://petnga.org/ontologies/space#outside
  Object  : http://petnga.org/ontologies/space#S0
Statement[ 6]
  Subject : http://petnga.org/ontologies/space#S1
  Predicate: http://petnga.org/ontologies/space#hasDimension
  Object  : "2~http://www.w3.org/2001/XMLSchema#int"
Statement[ 7]
  Subject : http://petnga.org/ontologies/space#S1
  Predicate: http://petnga.org/ontologies/space#hasGeometry
  Object  : "POLYGON ((300 200, 300 400, 700 400, 700 200, 300 200))"
Statement[ 8]
  Subject : http://petnga.org/ontologies/space#S1
  Predicate: http://www.w3.org/1999/02/22-rdf-syntax-ns#type
  Object  : http://petnga.org/ontologies/space#TwoDRegion
Statement[ 9]
  Subject : http://petnga.org/ontologies/space#S1
  Predicate: http://www.w3.org/1999/02/22-rdf-syntax-ns#type
  Object  : http://petnga.org/ontologies/space#Region
Statement[ 10]
  Subject : http://petnga.org/ontologies/space#S1
  Predicate: http://www.w3.org/1999/02/22-rdf-syntax-ns#type
  Object  : http://petnga.org/ontologies/space#SpatialEntity
Statement[ 11]
  Subject : http://petnga.org/ontologies/space#S1
  Predicate: http://www.w3.org/1999/02/22-rdf-syntax-ns#type
  Object  : http://www.w3.org/2000/01/rdf-schema#Resource
Statement[ 12]
  Subject : http://petnga.org/ontologies/space#S1
  Predicate: http://www.w3.org/1999/02/22-rdf-syntax-ns#type
  Object  : http://www.w3.org/2002/07/owl#Thing
```

Statements  
associated  
with Spatial  
Reasoning





# Model Integration

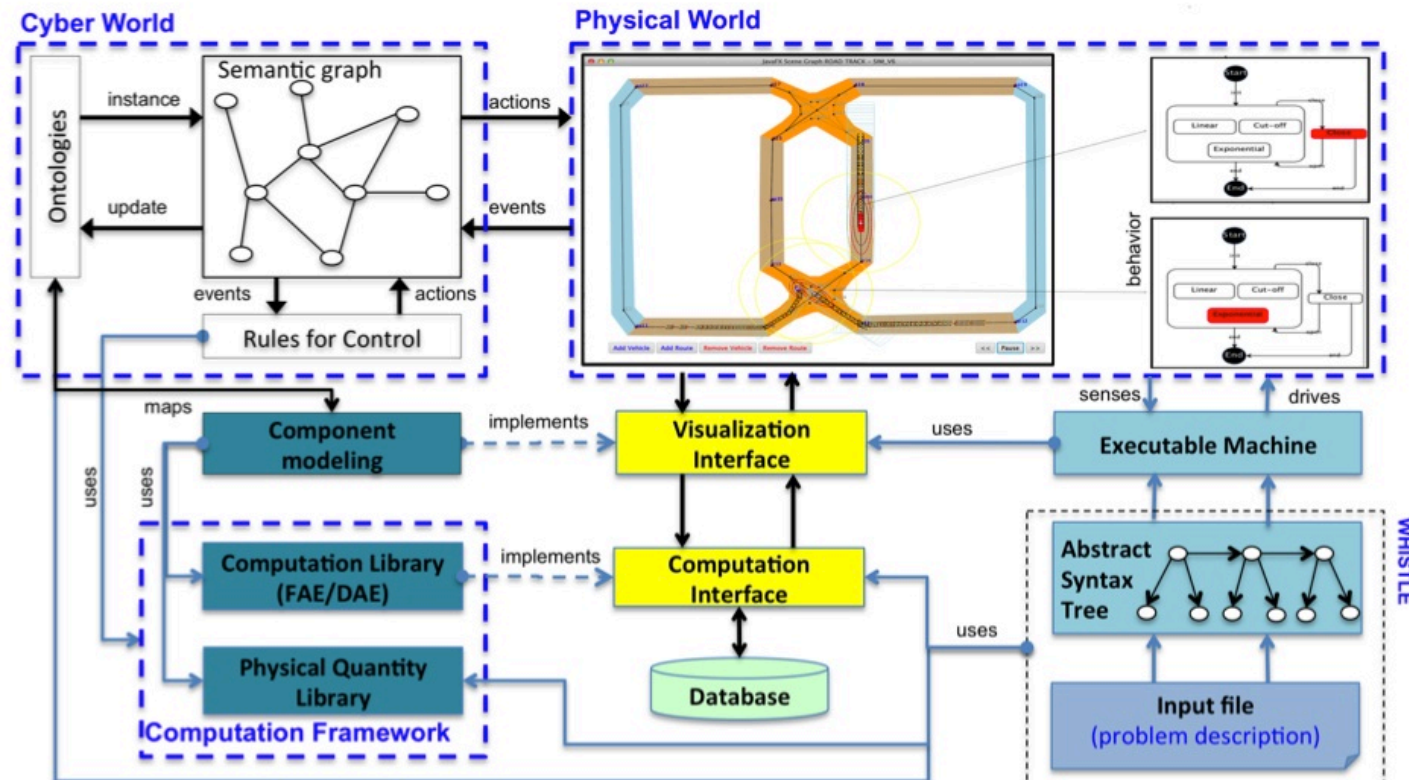
**Basic issue:** How to integrate models in the semantic framework for effective simulation and analysis of NoS?



- 1 Integration of models of physical components & computation
- 2 Simulation and analysis of continuous & discrete behaviors
- 3 Support: Units, branching, looping, Multi-format(XML,OSM,...)

```
x = 0 cm;
while ( x <= 10 cm ) {
    print "*** x = ", x;
    if ( x <= 5 cm ) {
        x = x + 1 cm;
    } else {
        x = x + 2 cm;
    }
}
```

# Networks of finite state machine behaviors



# Systems Integration

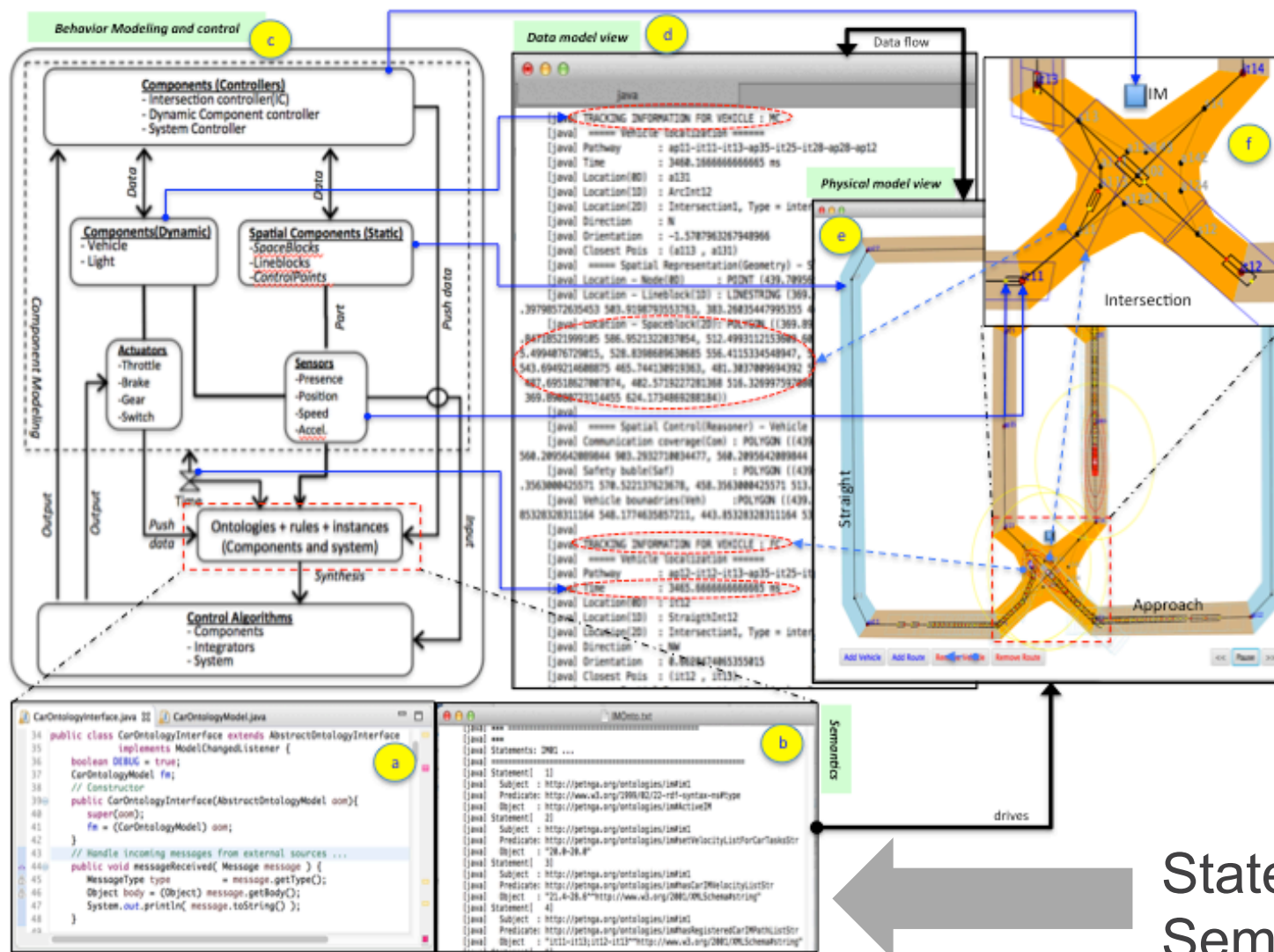
For a description of Whistle, see Delgoshaei, Austin and Pertzborn [2014].

# Application: Traffic Intersection with No Traffic Lights



Behavior modeling and control.

Car Ontology Interface



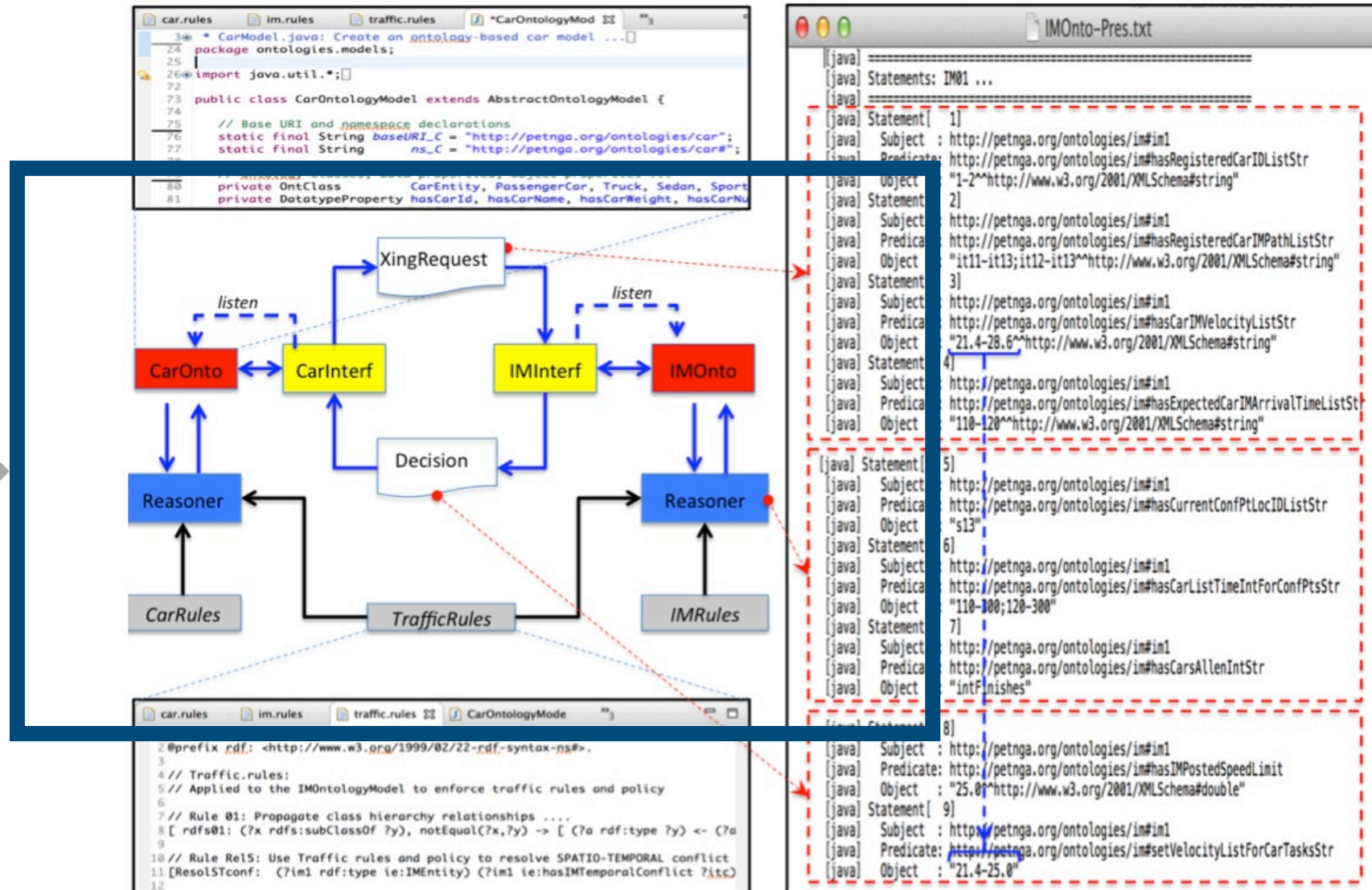
Visualization of race track pathways and geometry

Statements in the Semantic Model

# Spatio-Temporal: Reasoning, Communication and Control



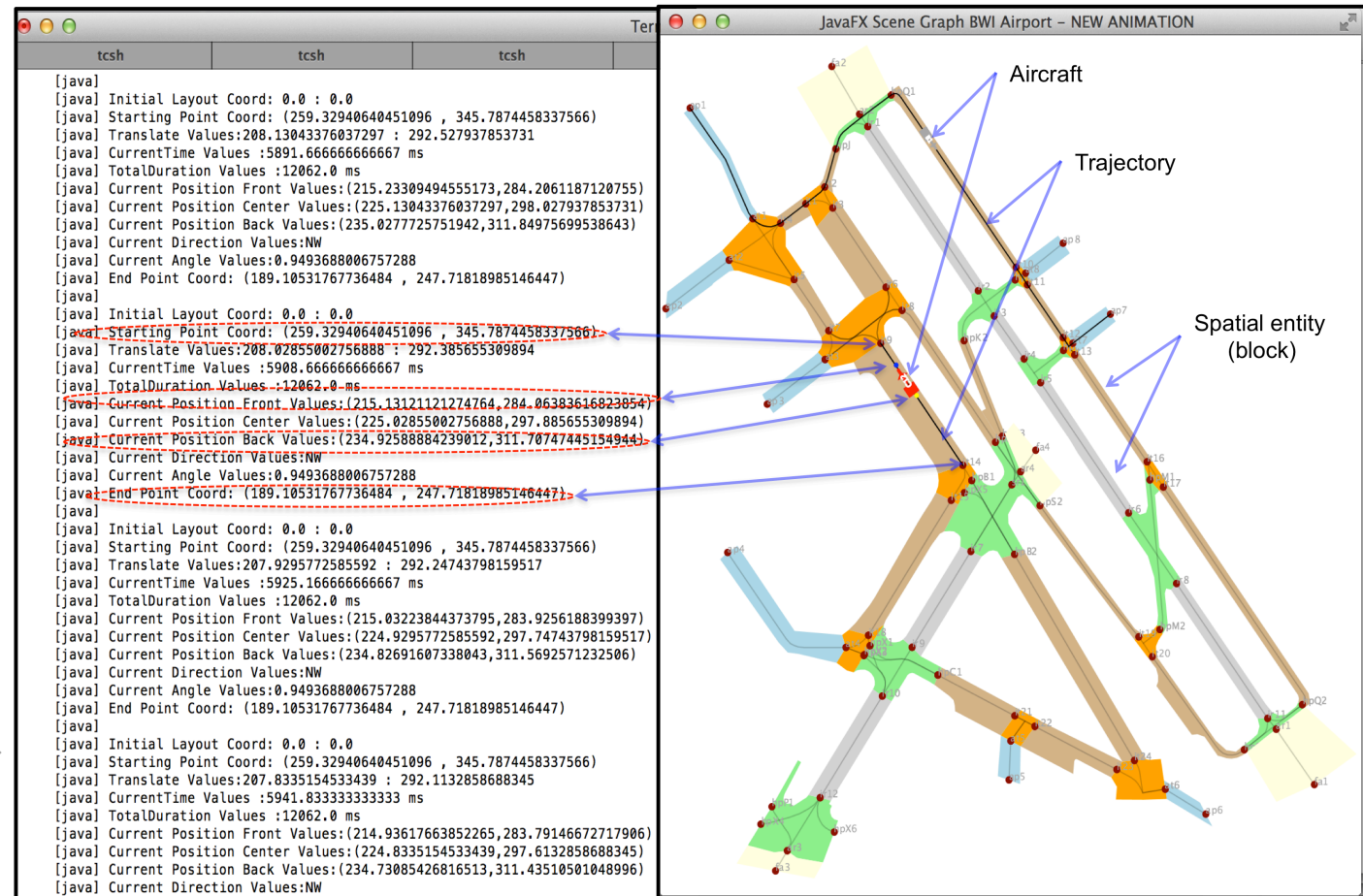
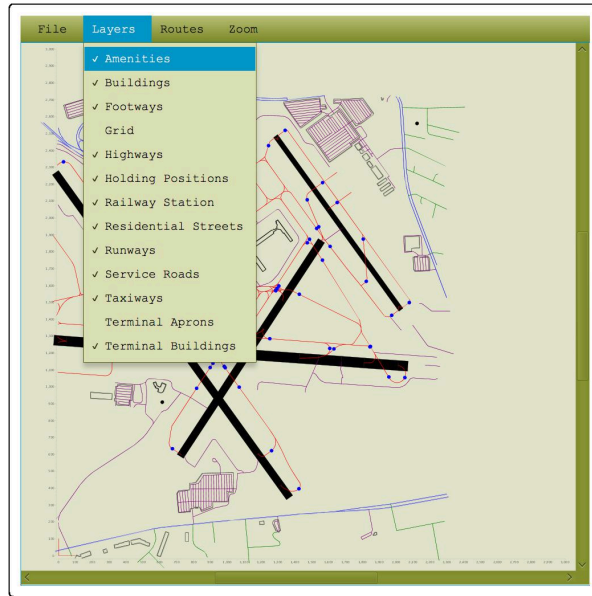
Intersection  
Manager / Vehicle  
Communication





# Scaling Things Up

# Work in Progress (2017-2018)



**Research Challenges:** Large volumes of data; semi-automated synthesis of semantic models; dynamic integration of ontologies and rules in decision making.

# Summary



## Design challenges of Network of Systems

- Increasingly **complex**, **heterogeneous**, **distributed** and **connected**
- **Limitations MBSE:** weak domain & language semantics, model inconsistencies

## Semantic-based platform for MBSE of NoS

- Formal model of systems (i.e domains and metadomains) using **decidable** OWL
- **Allen's Temporal Intervals Calculus** & restricted **Region Connection Calculus**
- Modular, flexible, reusable **reasoning-enabled** semantic blocks
- System integration with Whistle scripting language (under development)



# Select Publications

- Petnga L. and Austin M.A., An Ontological Framework for Knowledge Modeling and Decision Support in Cyber-Physical Systems, Advanced Engineering Informatics, Vol. 30, No. 1, January 2016, pp. 77-94.
- Petnga L. and Austin M.A., Ontologies of Time and Time-Based Reasoning for MBSE of Cyber-Physical Systems, 11th Annual Conference on Systems Engineering Research (CSER 2013), Georgia Institute of Technology, Atlanta, GA, March 19-22, 2013. **Best Conference Paper Award.**
- Petnga L. and Austin M.A., Cyber-Physical Architectures for Modeling and Enhanced Operations of Connected-Vehicle Systems, 2nd IEEE/TRB International Conference on Connected Vehicles (ICCVE 201), Las Vegas, December 2-6, 2013
- Delgoshaei P., Austin M.A., and Pertzborn A., A Semantic Framework for Modeling and Simulation of Cyber-Physical Systems, International Journal On Advances in Systems and Measurements, Vol. 7, No's 3-4, December 2014.
- Austin M.A., Delgoshaei P. and Nguyen A., Distributed Systems Behavior Modeling with Ontologies, Rules, and Message Passing Mechanisms, 13th Annual Conference on Systems Engineering Research (CSER 2015), Stevens Institute of Technology Campus, Hoboken, New Jersey, March 17-19, 2015, pp. 373-382, **MITRE Best Transition in Systems Engineering Research Award.**
- Coelho M., Austin M.A. and Blackburn M., Distributed System Behavior Modeling of Urban Systems with Ontologies, Rules and Many-to-Many Association Relationships, The 12th International Conference on Systems (ICONS 2017), Venice, Italy, April 23 - 27, 2017, pp. 10-15. **Best Paper Award.**

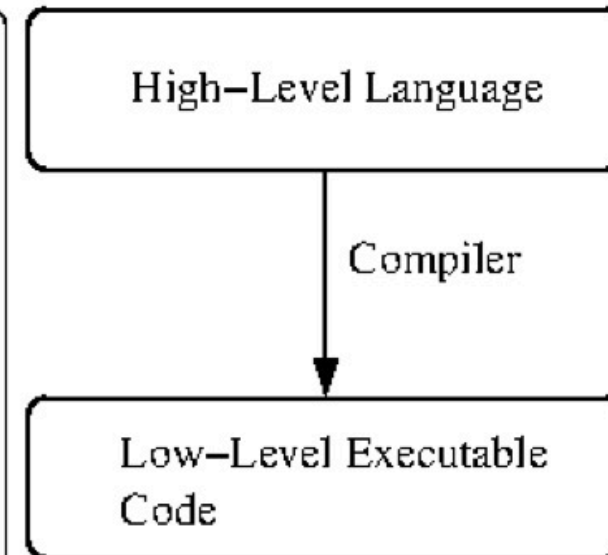
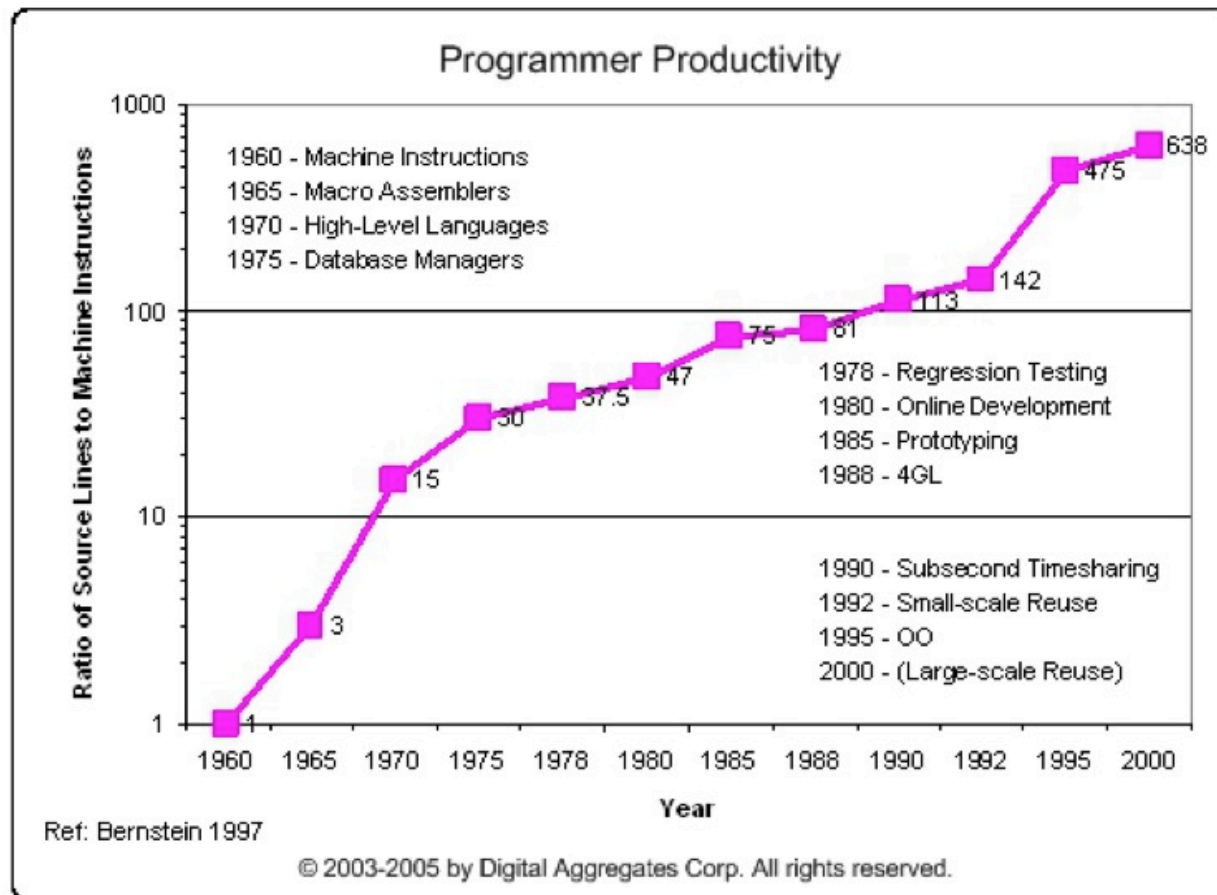


# Backup Slides

# Management of Software Complexity

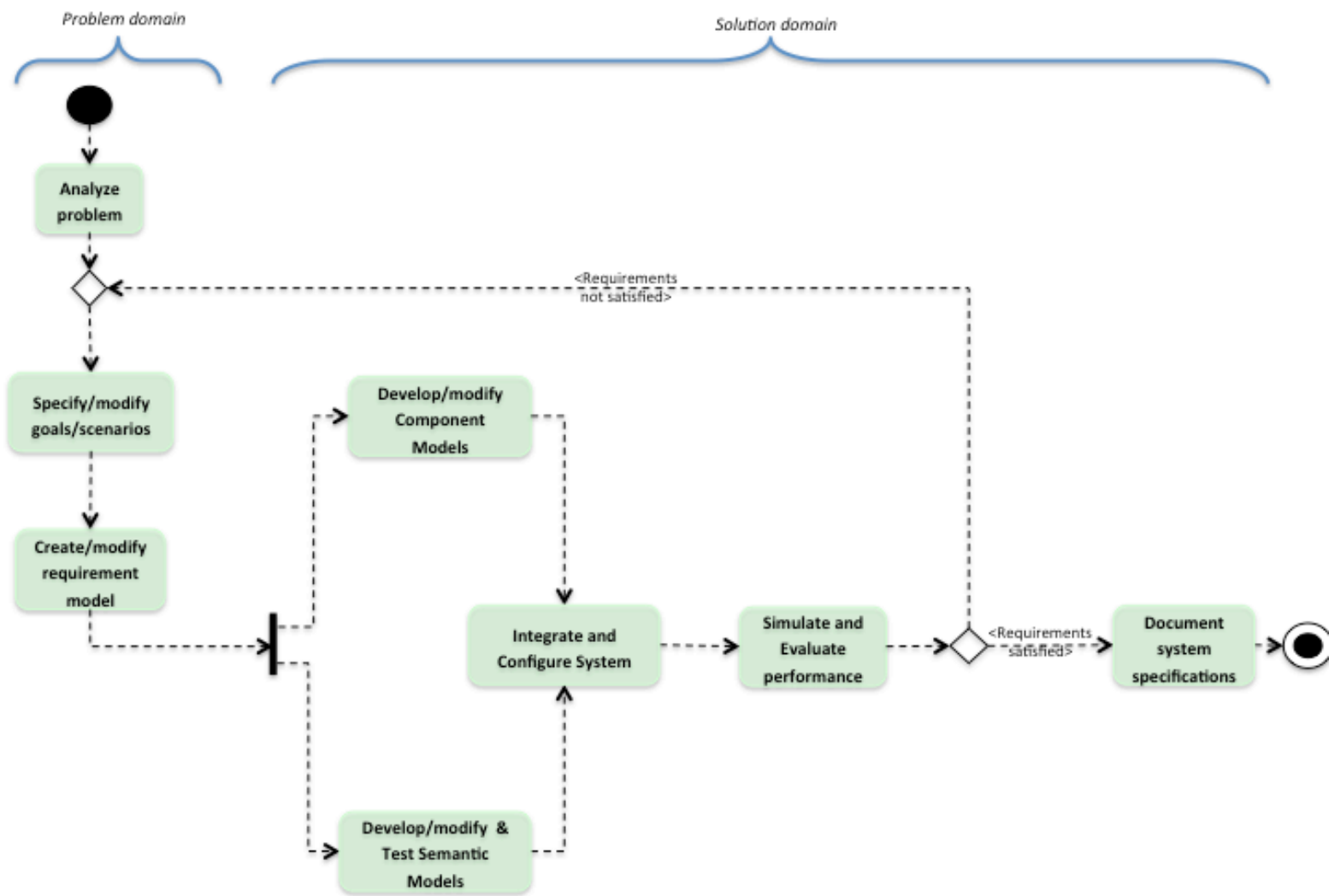


**Increasing System Complexity:** Software programmers need to find ways to solve problems at high levels of abstraction.





# Proposed Implementation Process





**27<sup>th</sup>** annual **INCOSE**  
international symposium

**Adelaide, Australia**

July 15 - 20, 2017

[www.incose.org/symp2017](http://www.incose.org/symp2017)

