FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Co-modeling Software Architecture and Policy In FORMULA

David Lindecker

Berkeley UNIVERSITY OF CALIFORNIA
Massachusetts Institute of Technology
MICHIGAN
VANDERBILT UNIVERSITY

FORMULA Overview

- Formal modeling language developed at Microsoft Research.
- Combines abstract data types and logic programming.
- Logic programs are structured into domains, models, and transformations.
- Execution of logic programs provides checking conformance of models to their respective domain and deriving new models as the outputs of transformations.
- Goal-based model finding via automated integration with Z3, a powerful SMT solver.

FORMULA Domains

Type definitions provide strong typing constraints for domain knowledge:

```
Vertex ::= new (idx:Integer).
Edge   ::= new (src:Vertex, dst:Vertex).
```

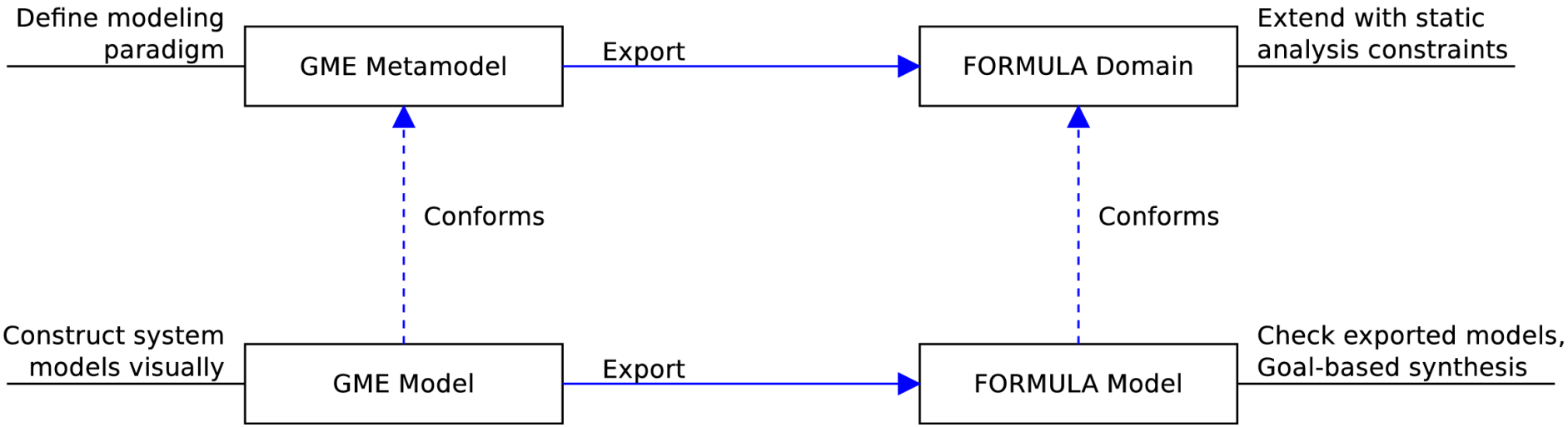
Logic rules for knowledge inference:

```
Path   ::= (src:Vertex, dst:Vertex).
Path(x,y) :- Edge(x,y).
Path(x,z) :- Path(x,y), Edge(y,z).
```

Conformance constraints for specifying restrictions on a domain:

```
conforms no Path(x,x).
```

Toolchain Integration

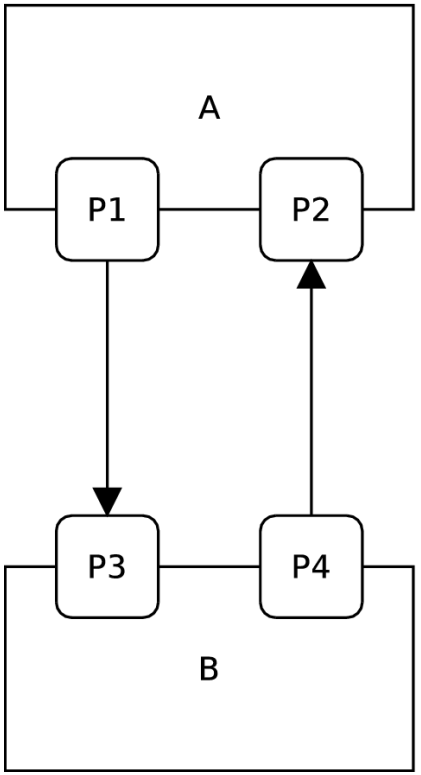


FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Modeling Software Architecture

```
domain SwArch {
  Component ::= new (name:String).
  Port ::= new (name:String, parent:Component).
  InformationFlow ::= new (src:Port, dst:Port).
}

model M of SwArch {
  A is Component("A").
  B is Component("B").
  P1 is Port("P1", A).
  P2 is Port("P2", A).
  P3 is Port("P3", B).
  P4 is Port("P4", B).
  InformationFlow(P1, P3).
  InformationFlow(P4, P2).
}
```



FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Annotating Ports with Static Information

Adding input/output directionality:

```
Port ::= new (name:String, parent:Component, dir:{INPUT,OUTPUT}).
```

Static analysis constraints:

```
conforms no { x | InformationFlow(x,_), x.dir = INPUT }.
conforms no { x | InformationFlow(_,x), x.dir = OUTPUT }.
```

In this case, we do context-free analysis of individual port connections.

Information Flow Policies

- Annotate individual ports with expectations of information flow restrictions.
- Trace flow of policies through system and check for compatibility at exit points.
- Ensure that hardware deployment of software architecture does not violate the information flow policy.

Questions?