MoBIES meeting; 2-3 Nov 2000, St Louis MO

Formal Composition Technology (For Time-Triggered Systems)

John Rushby,

Computer Science Laboratory
SRI International
Menlo Park CA USA

Frameworks For Embedded Systems

- There are several, each aimed at a slightly different domain, or having a different "world view," or operating at a different level of abstraction
- High-level modeling frameworks
  - Matlab/Simulink, Matrix$_x$
- Lower-level design frameworks
  - Data: SCADE/Lustre/Signal/Esterel
    - SCADE is used to synthesize all the code on Airbus planes; has DO-178B-approved compiler
  - Control: Statecharts, Stateflow
- Bottom-level frameworks
  - Time-Triggered Architecture (TTA)

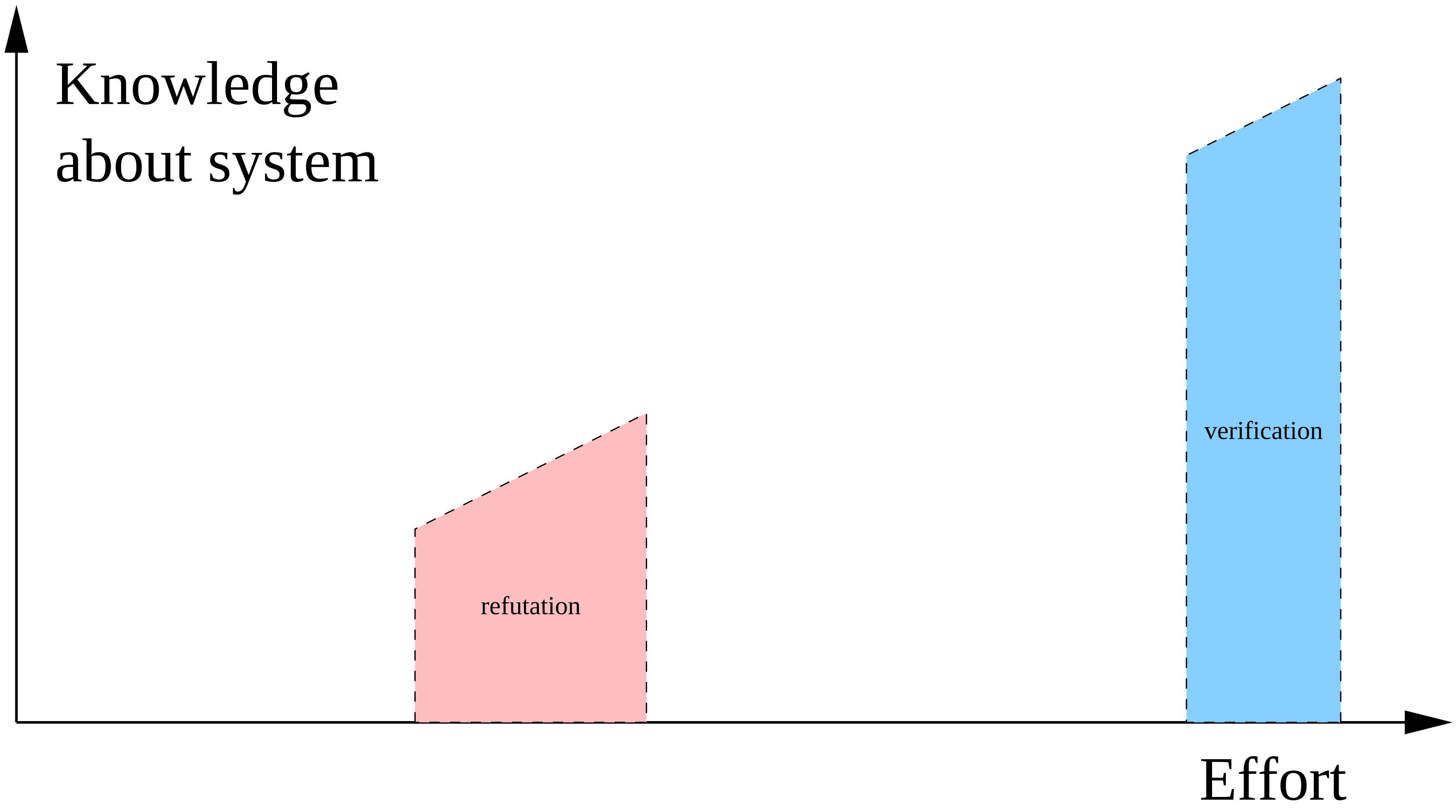
Our Project (Original Focus)

- Use mechanized formal methods to integrate frameworks at different levels
- E.g., design in Simulink, implement in Lustre and Statecharts, run on TTA
- Formal methods will justify transformations across frameworks
    - And generate glue code
- So that properties established at one level are preserved at the next, and properties of one system are preserved when composed with another
- With particular focus on nonfunctional properties such as timing, fault tolerance, partitioning
    - Because these dominate the development time, assurance costs, and failures in embedded systems

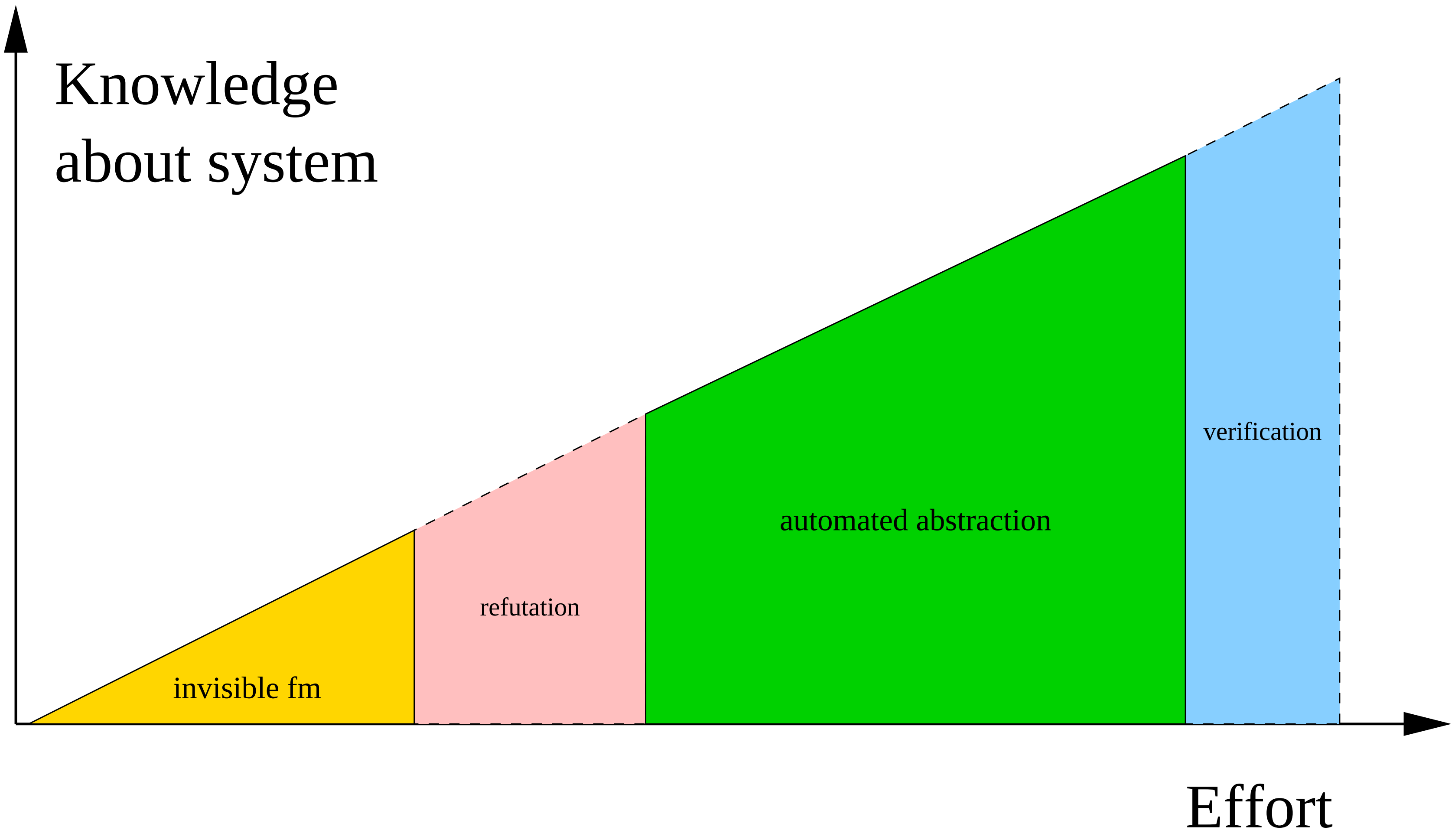
Current Focus

- Create invisible formal methods that add value in Matlab modeling and development
- Specifically, improved debugging, analysis, composition, assurance, of Stateflow models (and potentially improved autocode generation)
    - Note that Stateflow has some unconventional semantics
- Based on our existing technology (ICS, PVS, SAL)
- Because
    - Impact of Monterey meeting
    - Mathworks told us that was a major need of their customers (and gave us copies of Matlab)
    - And DARPA, too

Pre-Invisible Formal Methods



Invisible Formal Methods

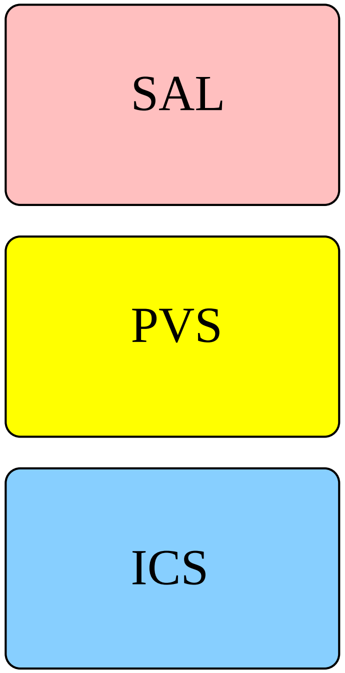


Examples

- Typecheck a Stateflow model (wrt. modern type system)
  - Another project in our lab received a Matlab model from an aerospace company that did a divide by zero
- Can these two states be active at the same time?
- Show me a path that activates this state
- Show me a path that makes this condition true

(As opposed to traditional model checking/formal verification applied to Stateflow)

Products We Offer (Independent of Mobies)



ICS = Integrated Canonizer-Solver (= ICanSolve)

Standalone Decision Procedures

An enabler for invisible formal methods

Products From This Effort

- Near term
  - Experimental Stateflow analyzer
- Longer term
  - Integration with Mathworks tool set (at least for Unix)
  - Test case generation
  - Export results of analysis to help code generation

Interfaces We Use/Need

- Tools
  - Mathworks has internal ascii formats
  - Our tools use XML for internal interfaces
  - Others. . . ?
  - These interfaces are needed for Solaris and Linux
- OEP
  - Stateflow examples
  - Insight into design process and problems