State of the Practice of Formal Methods

Curt Clifton
Rose-Hulman Institute of Technology

Software engineers want to be real engineers. Real engineers use mathematics. Formal methods are the mathematics of software engineering. Therefore, software engineers should use formal methods.

– Michael Holloway
NASA Langley
Research Center

Q1

Software Model Checking Takes Off

- Steven P. Miller, Michael W. Whalen, and Darren D. Cofer
  - Miller and Cofer, Rockwell Collins
  - Whalen, University of Minnesota Software Engineering Center

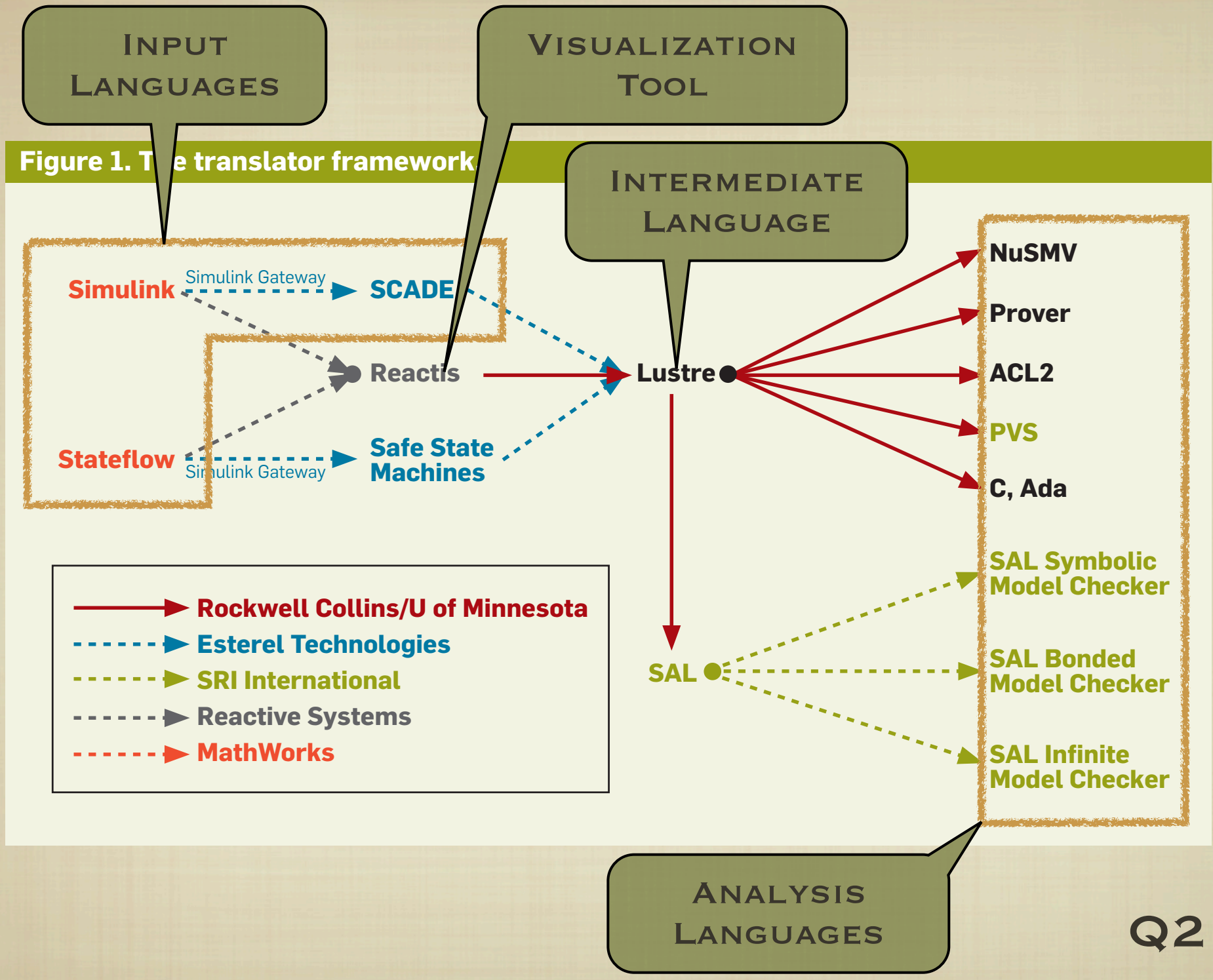
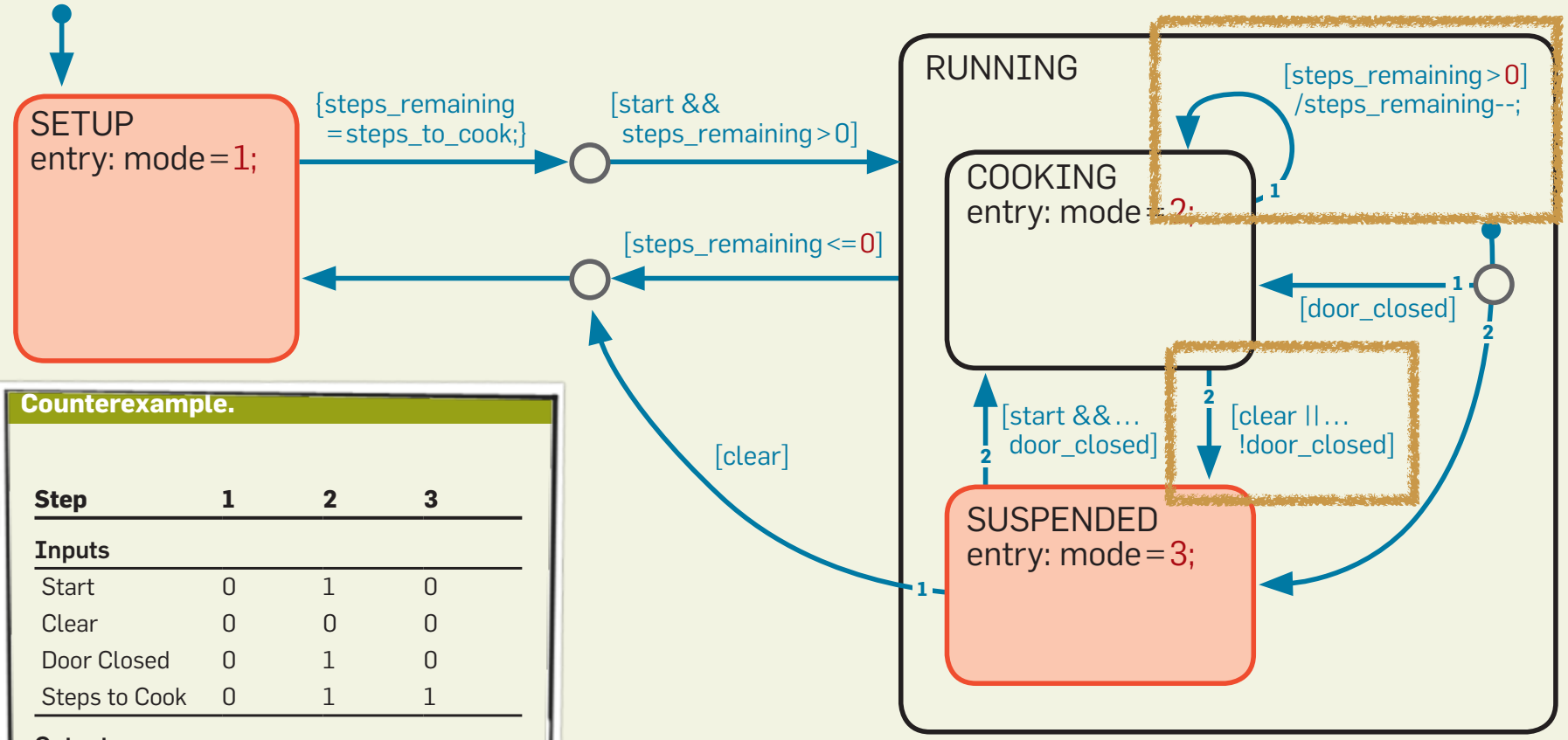


Figure 1. The translator framework

Q2

EXAMPLE

Figure 2. Microwave mode logic.



Counterexample.

Step	1	2	3
Inputs			
Start	0	1	0
Clear	0	0	0
Door Closed	0	1	0
Steps to Cook	0	1	1
Outputs			
Mode	Setup	Cooking	Cooking
Steps Remaining	0	1	0

assert Cooking ==> Door_Closed

Case Studies

ADGS-2100 Window Manager

- Modeled in Simulink
- Checked in NuSMV
  - Up to 1.5×10^{37} States
- Checked 563 properties
  - Found 98 errors

Without mandating it, Dev Team began model checking after every design change

CerTA FCS Phase 1

- Two independent verification teams
  - One used testing
  - One used formal model checking
- Formal team verified 62 properties
  - Found 12 errors
- Testing team
  - Invested 50% time
  - Found **no** errors
- Error types:
  - intermittent
  - Near simultaneous
  - Long sequences

Both teams agreed that model checking was more cost effective at finding errors

Why were Formal Methods a Good Idea Here?

Q3

The Exterminators

- by Philip E. Ross
- About Praxis High Integrity Systems

The Praxis Process

- Extensive, up-front work on requirements with the customer, using prototypes
- Model the system requirements in Z
- Implement the system in Spark-Ada
  - Includes formal specifications
  - Includes executable code
  - Includes static analysis tools to verify that specification and code match

Q4,5

The Results

- Less than 1 bug per 10,000 lines of code
  - 50 to 1000 times better than the industry average
- Praxis charges 50% more than competitors
- Praxis guarantees software
  - fixes bugs at no cost to the customer

Reminders

- Homework 12
  - Due Thursday morning
  - Covers [Ross06a]
- Project 4
  - Due Friday night
- No class, project days rest of this week

Course Evaluations