Bi-Directional Traceability: The Hi-Five Framework Approach to Reliable Validation of Early System Designs

Martin Ouimet and Kristina Lundqvist
Embedded Systems Laboratory
Massachusetts Institute of Technology
July 2nd 2007

Project Outline

- Motivations
  - High cost of Validation & Verification (V&V)
  - Benefits of modeling
    - Building confidence into the system early on
    - Economics of bug detection and correction
  - Reuse of the state-of-the-art
    - Verification
    - Test case generation

Overview of Hi-Five

Current State

Abstracted

High

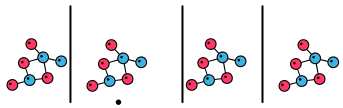
Level of Abstraction

Low

Needs Statements

Semi-Formal Specification

Formal Component and Interface Models

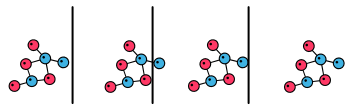


Implemented Code

Ongoing Research

Abstracted

Literate Specification Language



Traceability

Automated Test Case Generation

Autocode Generation

Leverage Existing Tools for Formal Analysis

WCET Analysis

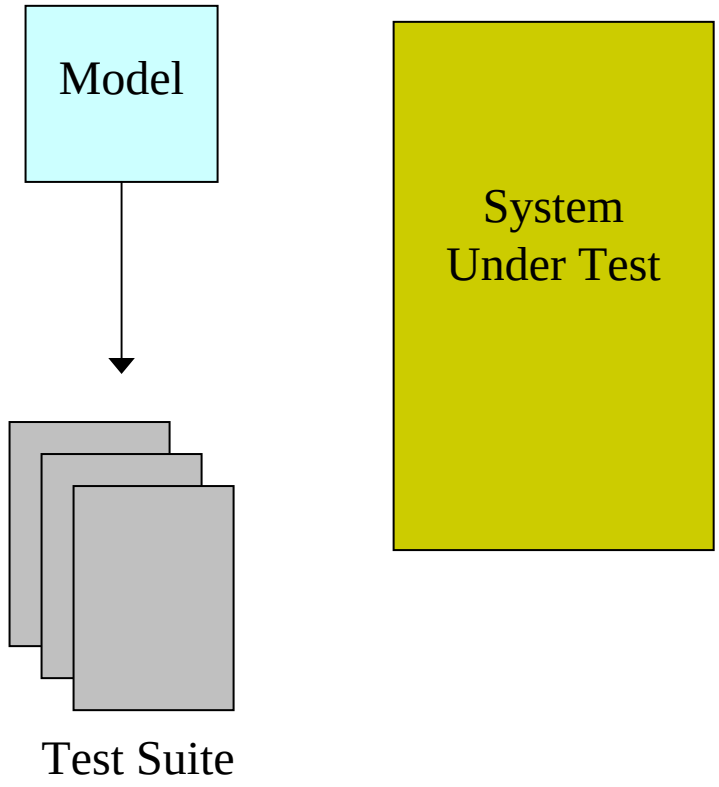
Implemented Code

Modeling Time and Non-Functional Properties

- Can time be reliably estimated for software, without an implementation?
  - Maybe you don't care
    - Level of abstraction
    - Speed of software vs. rest of system
    - Nature of system
  - Maybe you care
    - Do the best you can
    - Estimates become constraints on implementation
    - Use feedback from implementation in model
    - Develop around a known platform with a library of components

Test Case Generation

- Model-Based Testing
  - Use model to generate test cases
  - Model acts as an oracle
  - Meaning of model coverage vs. implementation coverage?



The TASM Language

- Literate modeling language based on ASM
- Function + Time + Resources
- Duration is the key paradigm to represent time
- Time specified as interval to capture BCET,WCET, and uncertainty

The TASM Toolset

- Graphical Front-End for Specification, Simulation, and Analysis
- Integrates UPPAAL
  - To verify BCET and WCET paths in the model
- Integrates the SAT4J SAT solver
  - To verify Completeness and Consistency of models

The TASM Toolset - Timeliner - C:\Documents and Settings\mouimet\My Documents\Work\Frequent Work\MIT - Research\PhD\TASM\Plant Simulator\Timeliner.tasm

File Edit Project Simulation View Help

Design

- PROJECT
- CONFIGURATIONS
  - simple
- ENVIRONMENT
- TEMPLATES
  - MAIN MACHINES
    - CONTROLLER
    - FAULT_INJECTER
    - HUMID
    - SCHEDULER
    - TEMP
    - TIMELINER
  - FUNCTION MACHINES
  - SUB MACHINES
    - EXECUTE_BUNDLES
    - EXECUTE_PLANTSIM_SEQUE
    - PLANTSIM_BUNDLE
    - SEQUENCE_HUMIDITY_MON
    - SEQUENCE_HUMIDITY_MON
    - SEQUENCE_TEMP_MONITOF
    - SEQUENCE_TEMP_MONITOF

Simulation

PROJECT | TIMELINER | SEQUENCE_HUMIDITY_MONITOR_WORK | SEQUENCE_TEMP_MONITOR_WORK

ABOUT

name : SEQUENCE_TEMP_MONITOR_WORK

description :

VARIABLES

monitored variables :

```
temp_seq_b;
temperature;
```

controlled variables :

```
temp_seq_b;
trying_to_cool_system;
temp_seq_s;
cooling;
```

RULES

```
R1: b0 -> b1
{
  t := 685;

  if temp_seq_b = b0 then
    temp_seq_b := b1;
}

R2: b1 -> b2
{
  t := 2285;

  if temp_seq_b = b1 and temperature >= 26 then
    temp_seq_b              := b2;
    trying_to_cool_system   := True;
    cooling                 := on;
}

R3: b1 -> b3
{
  t := 1730;

  if temp_seq_b = b1 and temperature < 26 then
    temp_seq_b := b3;
}

R4: b2 -> b2
{
  t := 1625;

  if temp_seq_b = b2 and temperature > 22 then
```

Behavior
- Solve
- Save to file

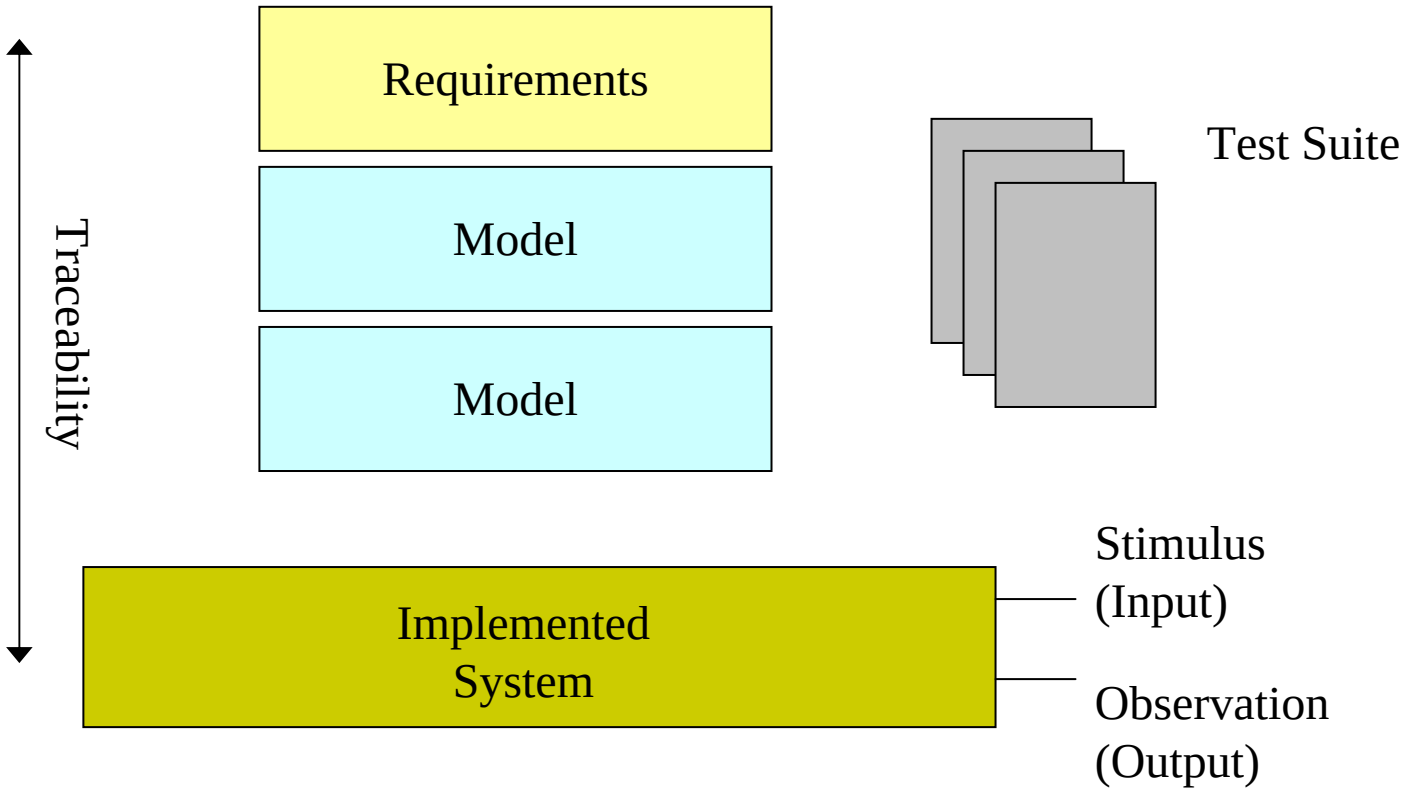
Solver
- SAT Solver
- MIP Solver

Default Values

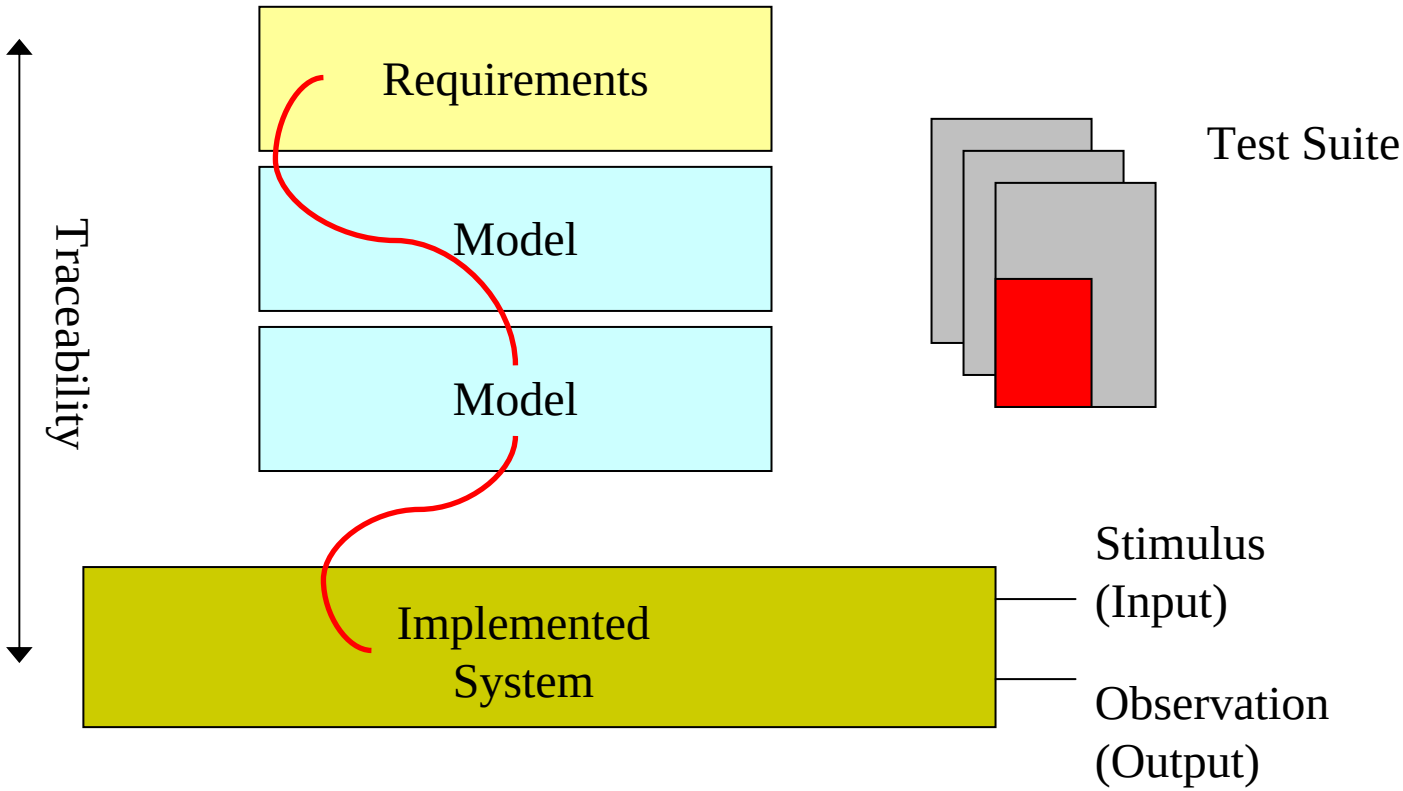
completeness

consistency

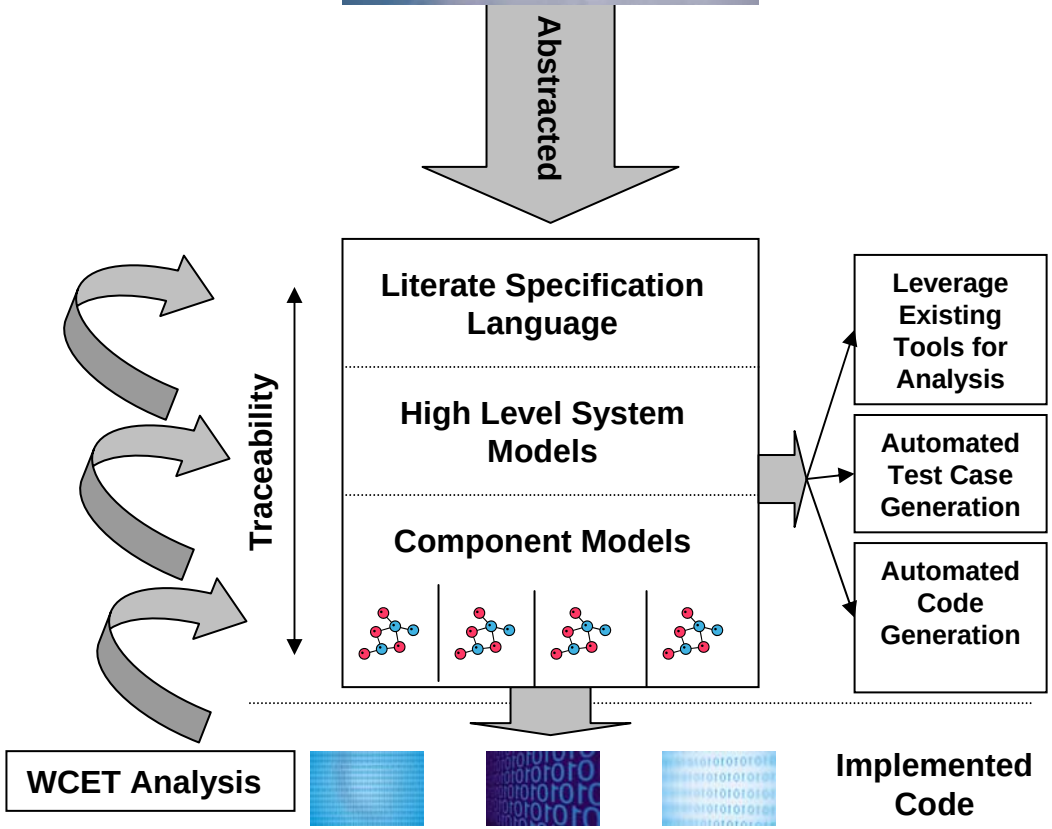
Bi-Directional Traceability



Bi-Directional Traceability



Overview of Hi-Five



Case Study

- The Timeliner System
  - How long should the timeslice be?
  - What is the maximum execution time for one "pass"
  - How about the minimum execution time?
  - What are the timing properties of scripts?

http://quest.arc.nasa.gov/space/photos/images/images/iss7x.jpg

Other Case Studies

- Electronic Throttle Controller (Ford)
- N-Modular Redundant Avionics (Draper)
- Production Cell

Questions?

- Thank you for your time

- For more information
  - http://esl.mit.edu/tasm
  - tasm@mit.edu