Mise en Scene

A Scenario-Based Medium Supporting Formal Software Development

John Douglas Carter
Dept. of Computing & Information Science
Modeling & Design Automation Group
University of Guelph
Guelph, Ontario
Canada

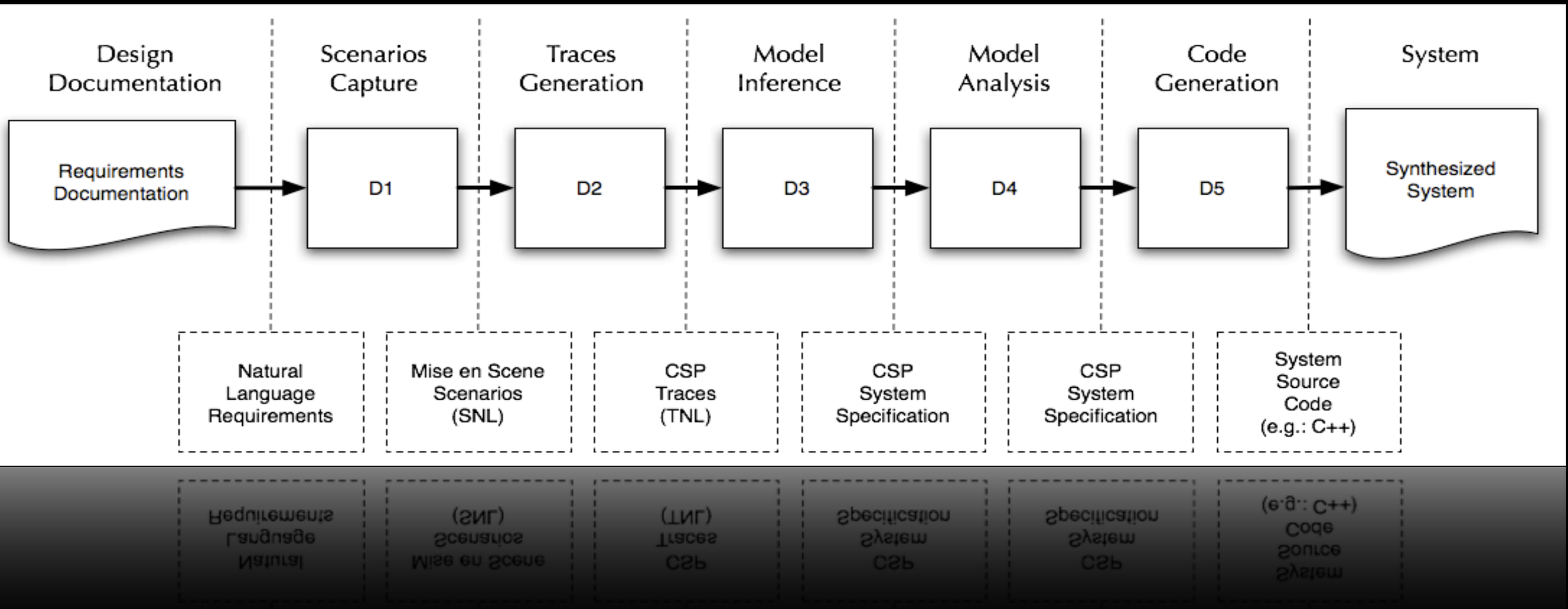
UNIVERSITY of GUELPH

R2D2C Project

- "Requirements 2 Design 2 Code"
- Multi-institution collaboration between parties at GSFC and a number of university researchers.
- Goal: From natural language req'ts, convert to a provably correct formal model, from which software can be synthesized.

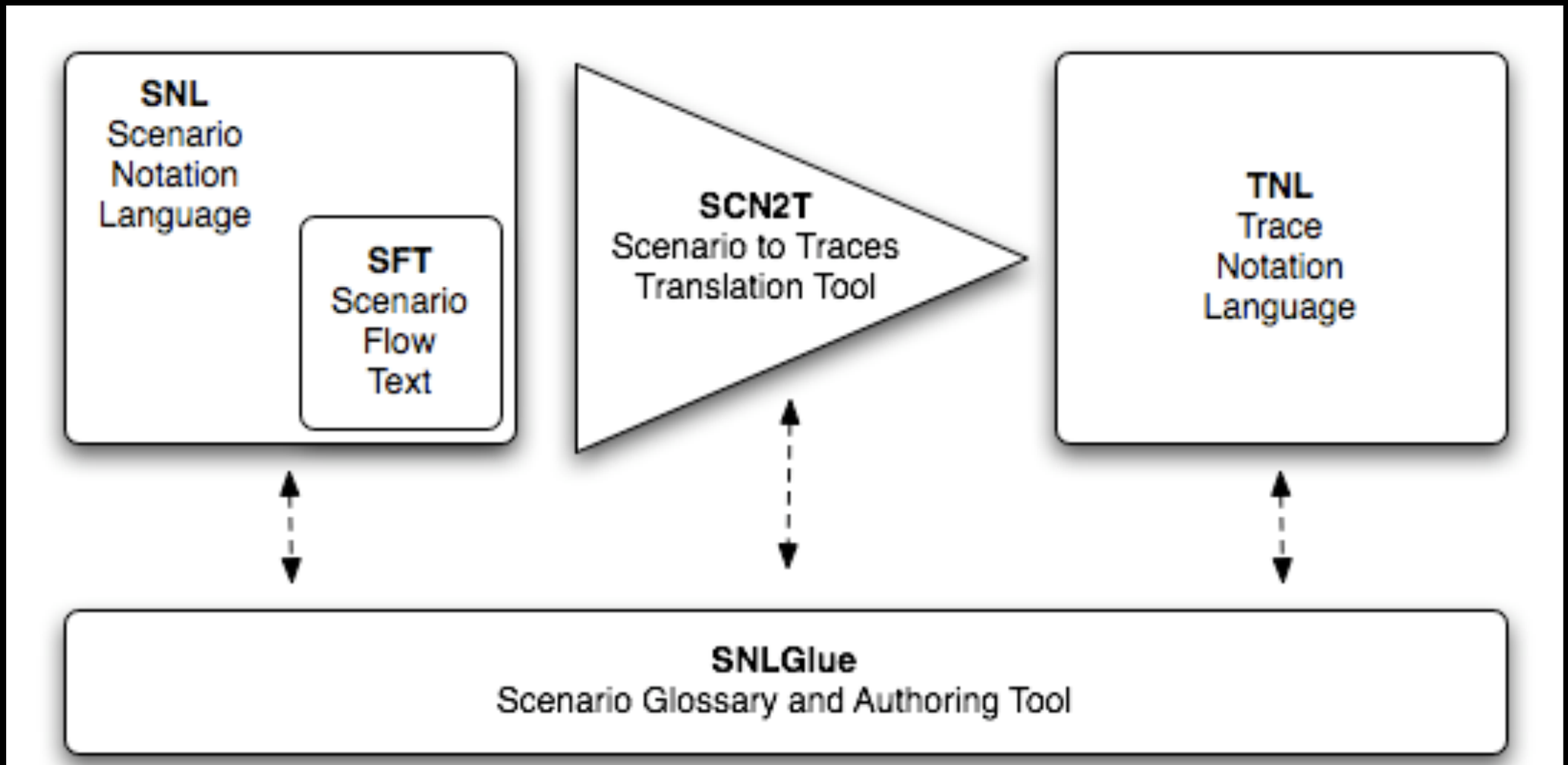
UNIVERSITY of GUELPH

R2D2C Process



UNIVERSITY of GUELPH

Mise en Scene



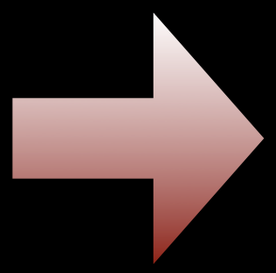
Mise en Scene Development

- Dozens of scenario interpretations, first step survey these interpretation, develop medium.
- Next, we needed to develop a trace medium -- avoid information loss.
- Lastly, conversion algorithm:
  - Individual Scenarios
  - System Composition

UNIVERSITY of GUELPH

Scenario ID: RobotStart
Description: Tasks performed by the robotic probe upon system start.
Author: John Carter
Primary Component: Probe
Supplemental Component: Station
Precondition: None
Trigger: System::start

Preamble:
{
COORDINATE xloc;
COORDINATE yloc;
}



terminal traces (Probe) = {
<robot_initialize,
Probe_Station_COORDINATE.xloc ,
Probe_Station_COORDINATE.yloc,
robot_ready> }

Scenario Flow:
1. Probe performs robot_initialize.
2. Probe sends xloc to Station.
3. Probe sends yloc to Station.
4. Probe performs robot_ready.

Extensions: None

UNIVERSITY of GUELPH

Challenges

- Unified scenario medium.
- Avoiding information loss in CSP traces.
- Conversion algorithm, scenario composition.
- Developed two case studies:
  - One original.
  - One based on previous R2D2C work.

UNIVERSITY of GUELPH

Future Work

- We've investigated SNL to CSPm
- Would be of interest to us to use scenarios for software synthesis using CSP++.
  - Identified conceptual "gaps", warrants further investigation.
- Extension of present 'naive' preconditions.
- Scenarios enrichment to allow infinite traces.
- Designed integrated scenario editor / repository, partially implemented.

UNIVERSITY of GUELPH

Conclusion

- Scenarios are information rich, but often lack a formal syntax.
- Traces are information poor, but allow powerful reasoning and/or formal development to take place.
- Bridging the two has great potential -- formal development in a medium readily understood by all stakeholders.
- Unlocks a world of verification and software synthesis.

UNIVERSITY of GUELPH

More Info

- Please see NASA/TM-2007-214155.

UNIVERSITY of GUELPH