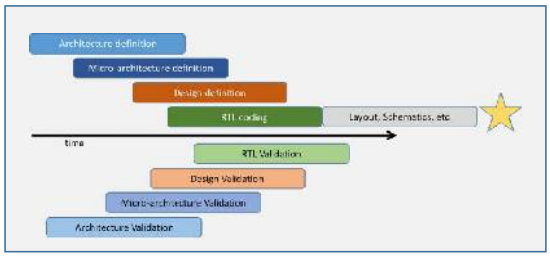
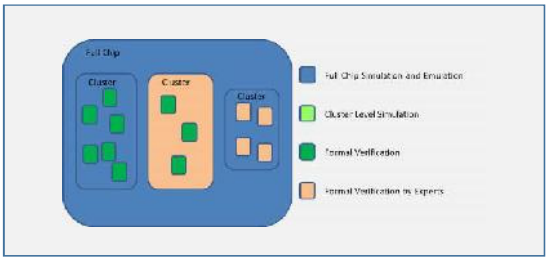
Preparation

System Specification and Verification

Validation has become the critical path to product development

- Documentation available later than desired
  Incomplete, ambiguous, and may be wrong





TLA+ Installation

Google “The TLA Home Page”

http://research.microsoft.com/en-us/um/people/lamport/tla/tla.html

Links on the TLA home page:

- The TLA Toolbox
  http://research.microsoft.com/en-us/um/people/lamport/tla/toolbox.html
  May require installation of java and eclipse
  Once installed, the application can be found in the tool box subdirectory

- TLA Book: Specifying Systems
  http://research.microsoft.com/en-us/um/people/lamport/tla/book.html

- TLA+ Hyperbook
  http://research.microsoft.com/en-us/um/people/lamport/tla/hyperbook.html
  Once downloaded, open start.pdf to view.

- The Pretty-Printer
  http://tla.msr-inria.inria.fr/tlatoolbox/doc/spec/pretty-printing.html
  http://www.miktex.org/
  After installing, I needed to logout/login for TLA to find it.
  On ECE machines, you may need to P:\Programs\MiKTex 2.9\miktex\bin\pdflatex

Preliminaries

Leslie B. Lamport is best known for his seminal work in distributed systems and as the initial developer of the document preparation system LaTeX.

Leslie Lamport was the winner of the 2013 Turing Award for imposing clear, well-defined coherence on the seemingly chaotic behavior of distributed computing systems, in which several autonomous computers communicate with each other by passing messages.

He devised important algorithms and developed formal modeling and verification protocols that improve the quality of real distributed systems.

These contributions have resulted in improved correctness, performance, and reliability of computer systems.

Wikipedia

TLA+ Installation/use

- TLA+ installed in WCC lab and FAB 55-17 lab
- Keep a copy of the book, hyperbook, and example programs on a usb-drive

- On your own machine: create shortcuts (not copy) to your desktop

- Sidenote: note GUI flexibility!
  - Can detach sub-windows
  - Module template provided
  - Reserve words in color, comments in another
  - Changed lines in color

TLA+ Tools

- Syntactic Analyzer (ch 12)
- TLATeX Typesetter (ch 13)
- TLC Model Checker (ch 14)
  - Finds errors by trying to verify spec satisfies properties.
    - Can run without properties to check for “silliness” errors and deadlock.
    - TLC doesn’t handle existential quantification

Principles and Specification Tracks Tutorial

New version 28 February 2015 now available!

- Open a new spec
  - Add simple 1 bit clock
    - Init1 and Next1
- Saving a module causes the toolbox to parse it.
  - See the errors, add declaration for variable *b*
- Try the pretty printer
- Create a new model to check the design
  - Identify Init1 and Next1 and run TLC
  - Replace 0 in def with string and rerun TLC
  - Observe statistics: diameter
- Add type invariant property
  - On the model overview page and rerun TLC
  - As a definition in the spec.
- Another language: PlusCal

Reading

- Read Lamport paper: "Use of Formal Methods at Amazon Web Services"
- Read Lamport, Chapter 1: A Little Simple Math
  - Propositional logic
  - Sets
  - Predicate logic
  - Formulas and language
- Read Lamport, Chapter 2: Specifying a Simple Clock
  - Behaviors
  - An hour clock
  - A closer look at the specification
  - The specification in TLA+
  - An Alternative Specification