Critical Systems and their Verification
CS4271 – Introductory Lecture

Abhik Roychoudhury
http://www.comp.nus.edu.sg/~abhik

News Flash - 2012

- 5 top cyber threats for 2012
  - http://www.cbc.ca/news/technology/story/2012/01/03/sci-cyber-threats.html
  - **Attacking mobile devices:** Techniques used in the past for online banking, such as stealing from victims while they are still logged on, will now target mobile banking users.
  - **Embedded hardware:** Embedded systems, which are designed for a specific control function within a larger system, are commonly used in vehicles, GPS systems, medical devices, routers, digital cameras and printers. Hackers with access to malware that attacks the hardware layer of such systems will gain control and long-term access to the system and its data.

Embedded Systems

- A computing system which is part of a "larger system" (read – device).
- The "larger system" constitutes the environment – in continuous interaction with it.
- The computing system implements a specific functionality.
  - A dedicated computer implemented by a combination of hardware and software.

Examples – (1)

- Automobiles
- Train control systems
- Avionics / Flight control
- Nuclear Power Plants
- Inside medical devices (for image manipulation) and other purposes
- Safety first, our focus!

Examples – (2)

- More vanilla
- HDTV
- Washing Machines
- Microwave
- Controllers for other household devices such as Air-con
- Finally, smart room / wear (GA Tech etc.)
- Also, our focus ---
  - "if the TV does not work, nobody dies, but in the end the company dies"

Our focus - validation

- Rough meaning
  - The system functions "as intended"
- Need the following
  - Capturing of "intention" formally - Specification
  - Techniques to check system functioning – Verification
  - Tools to check system functioning – Verifiers.
- What kind of tools and techniques?

Validation in diff. “avatars”

- Testing
  - Execute system for a specific “input”
- Simulation
  - Run system for a specific “input”
  - Similar to testing, but differs in key aspects
    - What aspects?
- Verification
- Performance Analysis

Testing and Simulation

- Testing executes the actual system, on a real execution platform.
- Simulation
  - Functionality simulation: execute a model of the actual system
    - Actual system may be in the process of being designed.
  - Performance simulation: execute the system on a model of the execution platform.
    - Such as a software description of a processor.
    - This might be a way of choosing the “right” platform for a given embedded system.

Testing and simulation

- Testing
  - *Intention*: the expected system output.
  - *Output* of the method: Pass/Fail
  - *Validation*: Trivial (check o/p with expected o/p)
  - *Key issue*: Finding representative test cases.
- Simulation
  - *Output*: Pass/fail or estimates (for perf. simulations)
  - *Validation*: similar to testing
  - *Key issue*: Building the simulation infrastructure, apart from finding representative inputs.

Formal Verification

- Check that a system behaves “as intended” for all possible inputs.
  - Checking for system functionality.
  - *Popular method*: Model Checking
  - *Output of the method*:
    - Pass, or Counter-example evidence (if it fails).
  - *Intention captured by*: Temporal Logic Properties.
  - *Validation*: by automated search of the system’s behavioral description.
  - *Key issue*: Scalability of the search for real embedded systems.

Performance Analysis

- Check that a system performs “as intended” for all possible inputs.
  - Checking for system performance.
  - *Popular methods*: Several.
  - *Output of the method*:
    - An upper bound on the system performance.
    - This bound should “safe”, and “tight”.
  - *Intention capture*: Not needed.
  - *Validation*: Develop timing models of underlying platform to accurately estimate performance.
  - *Key issue*: Scalability, Growing list of new features in new platforms whose timing models need to be created.

An application domain

- Multiple processors
  - Up to 100
  - Networked together
- Multiple networks
  Body, engine, telematics, media, safety

More about cars

- Car electronics is an increasingly important market, requiring new design flows.
  - Software is important for value addition
- Comments by major manufacturers
  - Daimler Chrysler
    - More than 90% of the innovation is from the car electronics
  - BMW
    - More than 30% of the manufacturing cost of a car is from the electronic components !
- Reliable & robust ES design flows needed !

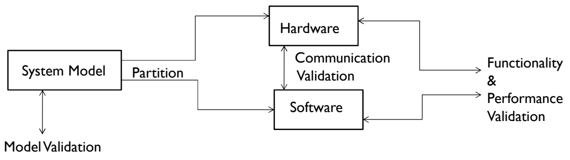
Car electronics

- 1. Critical features in the power train or chassis
  - Control engine, brakes, steering wheel
  - Safety-critical, hard real-time
  - Accomplished by communicating Electronic Control Units (ECUs) which contain
    - Micro-controller(s), RTOS, application program
    - ECUs communicate via buses
    - Communication between diff. micro-controllers in the same ECU also supported by dual-ported RAMs
    - Protocol design issues for the bus communication
- Validation: Formal modeling/verification/analysis?

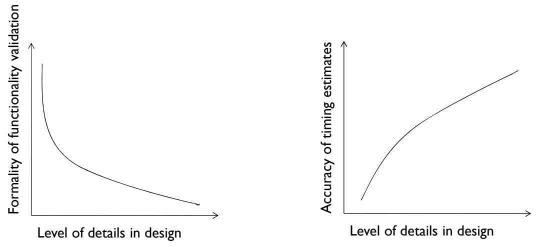
Car electronics

- 2. Controlling Cabin features
  - Power windows, air-conditioning
  - Often given as complex state-based specifications which get translated to code
- Validation: Modeling & Extensive testing?
- 3. Infotainment / Telematics
  - Relates to entertainment, not critical
  - Soft real-time constraints
  - Protocol standards for communication among media devices in a network …
- Validation: Performance analysis to satisfy soft real-time constraints.

Different kinds of validation

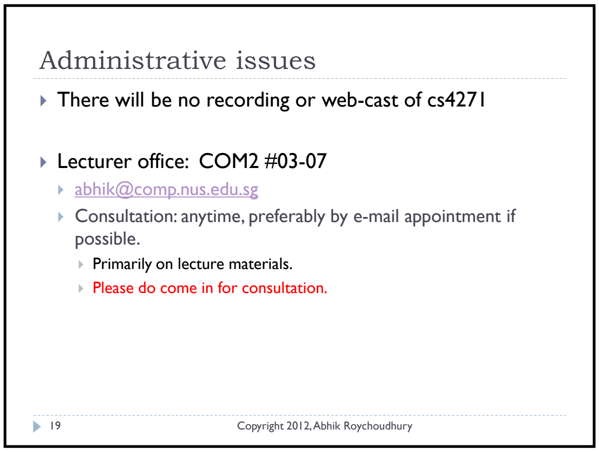


Validation w.r.t. level of details



Summary: Validation of ES

- Functionality Validation
  - Formal verification is better at higher levels of abstraction.
  - At lower levels, informal approaches like testing may be more useful.
- Performance Validation
  - Performance estimates are more accurate if we consider lower level details.

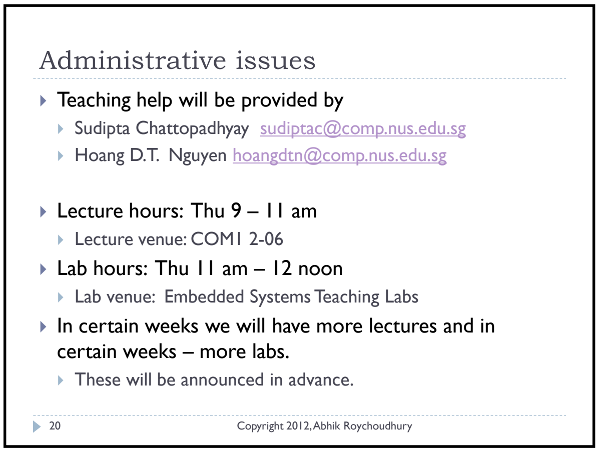


Administrative issues

- There will be no recording or web-cast of cs4271

- Lecturer office: COM2 #03-07
  - abhik@comp.nus.edu.sg
  - Consultation: anytime, preferably by e-mail appointment if possible.
    - Primarily on lecture materials.
    - Please do come in for consultation.

19 Copyright 2012, Abhik Roychoudhury

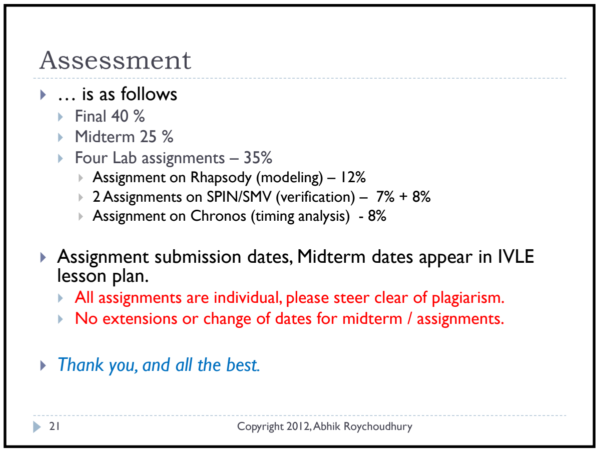


Administrative issues

- Teaching help will be provided by
  - Sudipta Chattopadhyay sudiptac@comp.nus.edu.sg
  - Hoang D.T. Nguyen hoangdtn@comp.nus.edu.sg

- Lecture hours: Thu 9 – 11 am
  - Lecture venue: COM1 2-06
- Lab hours: Thu 11 am – 12 noon
  - Lab venue: Embedded Systems Teaching Labs
- In certain weeks we will have more lectures and in certain weeks – more labs.
  - These will be announced in advance.

20 Copyright 2012, Abhik Roychoudhury



Assessment

- … is as follows
  - Final 40 %
  - Midterm 25 %
  - Four Lab assignments – 35%
    - Assignment on Rhapsody (modeling) – 12%
    - 2 Assignments on SPIN/SMV (verification) – 7% + 8%
    - Assignment on Chronos (timing analysis) - 8%

- Assignment submission dates, Midterm dates appear in IVLE lesson plan.
  - All assignments are individual, please steer clear of plagiarism.
  - No extensions or change of dates for midterm / assignments.

- *Thank you, and all the best.*

21 Copyright 2012, Abhik Roychoudhury