Evaluation of formal verification technology for model-based development of automotive software

Dr. Arun Chakrapani Rao
Arun.Chakrapani-Rao@warwick.ac.uk
Agenda for this presentation

- Background and motivation
  - Current software development; requirements engineering and model-based development.

- Introduction to Formal Methods

- Guiding questions for our research

- Formal verification through a demo model
  - Steps involved in using the technology; central locking system.

- Real-life case studies

- Conclusions
Current software development - Highly complex

- Size – Many ECUs, distributed, size of code
- Requirements – ambiguous, change often
Background

Model-based development

- MATLAB / Simulink / Stateflow
- Rhapsody, Rts etc.

Current Tools for Requirements Management (RM)

- Requirements traceability
- Impact Analyses of Requirement Changes

*Modelling + current RM methods important and necessary but not enough!*
Why is simulation not enough?

2 binary inputs means 4 simulations

10 binary inputs means 1024 simulations!

If inputs can get values not just 0 or 1 (ex., speed value of 0 to 200), then its infeasible to rely on simulations only!!
Introduction to Formal Methods

- Formal specifications – Z etc.
- Formal verification techniques
  - model-checking
  - theorem proving
- Verification based on commercial modelling tools such as Simulink / Stateflow / TargetLink.
Guiding questions for our research

- Which Formal Verification tools?
- Easy to integrate into current process?
- What are the benefits of using such tools?
- Training?
- Cost of adoption etc.?
Steps involved in using the technology

1. Requirements
2. Informal Requirement
3. Formalised Requirement
4. Model
5. Reformalise
6. Requirement satisfied?
   - True: Done
   - False: Investigate Current Model

© 2006 IARC
Demo model – Central Locking System

Requirements

- Motor Lock signal and Motor Unlock signal must not be generated at the same time.

- If the driver door is open, the lock signal must be ignored.

- If a crash has been detected, no unlock is allowed if the car is in park position.

- If a crash occurs during driving, all doors must be unlocked in a slot of 5 execution steps.
Demo model – Central Locking System

Evaluation of formal verification technology for automotive software
Steps involved

Requirements

- Motor Lock signal and Motor Unlock signal must not be generated at the same time.
- If the driver door is open, the lock signal must be ignored.
- If a crash has been detected, no unlock is allowed if the car is in park position.
- If a crash occurs during driving, all doors must be unlocked in a slot of 5 execution steps.

"(MLDD && MUDD) || (MLPD && MUPD) || (MLTRUNK && MUTRUNK)"
Steps involved

1. Requirements
2. Motor Lock and...
3. Formalised Requirement
4. Requirement satisfied?
   - Unreachable
   - Reachable
5. Investigate Current Model
6. Done

Reformalise
List of verification activities

- Robustness checks: range violations
  
  eg. Can LockDecoder get a value out of [0..8]?

- ‘Drive to’ analyses: drive to state, drive to configuration, drive to property
  
  eg. Unlocking and SecuringDD

- Certification: formalise functional and safety requirements and find any violations
Real life Case Studies with Industry

Hood Controller Model

Air Suspension Model
On additional steps

Convert Simulink subsystem to TargetLink subsystem
Provide ranges for variables

Existing models might need to undergo a costly re-design step!
Conclusions

Improvements in Industrial modelling process

- Documentation
  - Which requirements are to be verified?
  - Model information – variable meanings, value ranges etc.
  - Good modelling guidelines

- Follow modelling guidelines
  - Avoid using the language in such a way that it is unreadable!
  - Follow modelling guidelines that particularly ease verification effort.
Next Steps

Completion of case studies

- Results of verification for the Air Suspension System.
- Report on requirements and modelling guidelines.

Define and implement Technology transfer mechanisms

Final report on application of the technique

- Available to research partners.

Develop recommendations for further research

- Further studies to evaluate if tools lean enough for engineers.

Continuation in new projects

- DTI funded Validation of Complex Systems.