FUTURE OF FORMAL METHODS

PETER GORM LARSEN (PGL@IHA.DK)
PROFESSOR
IN COLLABORATION WITH IN PARTICULAR FITZGERALD AND VERHOEF
FUTURE OF FORMAL METHODS

› Increasing use of formal techniques
  › Increasing automation support
  › “Hidden” formal methods
  › Better links to testing

› Significant increases in power of formal modelling & verification ... and a significant increase in product complexity!

› We look at two of the most demanding classes of future product: embedded systems and Systems of Systems.

› Both require thinking outside the traditional boxes!
USE FORMAL METHODS WHERE IT IS CHALLENGING

- Cyber-Physical Systems
- Will increase in the future
- Multi-disciplinary required
- How to select the best solution?
- Complexity in many dimensions
- How to guard against faults?
- Here usable formal methods can be beneficial!
- But this requires new research!
- Let me give you my vision
FUTURE OF FORMAL METHODS

- Embedded Systems Development
  - The DESTECS Technology
  - Industrial Case Studies
  - Systems of Systems Challenges
  - Cyber-Physical Systems
EMBEDDED SYSTEMS DEVELOPMENT (1)

- Highly competitive marketplace:
  - Requirements are volatile
  - Time to market is key

- Products are complex

- Early design stages are vulnerable to failure:
  - Engineering disciplines have distinct methods & tools
  - Design choices are often implicit or experience based
  - System dynamics are complex to grasp and express
  - Dependability (faults, fault tolerance) is often crucial
Problem decomposition into disciplines

Traditional approaches are “one discipline at a time”

Concurrent engineering required to improve time to market

... but important properties are multidisciplinary

... and so weaknesses are exposed late (integration)

So: how to cross the boundaries between disciplines?
Design gaps between disciplines lead to errors in designs.

Many of these errors are detected too late: during testing of first physical prototype.

Example: paper path setup

Paper jams for high speed paper handling.
FUTURE OF FORMAL METHODS

✓ Embedded Systems Development
➢ The DESTECS Technology
➢ Industrial Case Studies
➢ Systems of Systems Challenges
➢ Cyber-Physical Systems
DESTECS (WWW.DESTECS.ORG)

Methods (Modelling guidelines, patterns)
Tool Support (open platform)
Industry case studies: personal transportation, mail processing, dredging etc.
BASIC DESTECS CONCEPTS

**Ideal & Realistic Behaviours**

**Fault Modelling:** including error states & faulty functionality in the model

**Fault Injection** during a simulation managed by script

**Runs a co-simulation**
Forces selections and external updates, e.g. set point
Multiple co-simulation runs enables design space exploration
DESTECS TOOL ARCHITECTURE

Discrete-event system

Co-Simulation engine

Continuous-time system

Overture

DESTECS Tool

20-sim

Continuous-time system

FUTURE OF FORMAL METHODS
PETER GORM LARSEN
OCTOBER 2012
CO-SIMULATION ARCHITECTURE
EXAMPLE: WATER TANK

\[
\frac{dV}{dt} = \varphi_{in} - \varphi_{out}
\]

\[
\varphi_{out} = \begin{cases} 
\frac{\rho \cdot g}{A \cdot R} \cdot V & \text{if valve open} \\
0 & \text{if valve closed}
\end{cases}
\]
EXAMPLE: WATER TANK

class Controller

variables

-- Shared design parameters
sdp real maxlevel;
sdp real minlevel;

-- Monitored variables (seen from the DE controller)
monitored real level ;

-- Controlled variables (seen from the DE controller)
controlled bool valve;

-- events
event high;
event low;

1 = open
0 = close

-- link events to operations
event high = System.Controller.Open;
event low = System.Controller.Close;

mutex(Open, Close);
mutex(Close)
Sync

Open:() ==> ()
duration(50)
true);
Close:() ==> ()
cycles(1000)
false);

async
Open:() ==>
0 = Close;

Controller

DE-side

CT-side
"DESTECs" BOOK PLANNED

Part I Co-modelling and Co-simulation: the Technical Basis
- 1 Collaborative Development of Embedded Systems
- 2 Co-modelling and Co-simulation
- 3 Discrete-Event Models of Control Software: the VDM Technology
- 4 Continuous-Time Models of Plant: the 20-sim Technology
- 5 Modelling in Practice: Illustrative Examples
- 6 Tool Support for Co-modelling and Co-simulation

Part II Co-creating Embedded Systems: Methodology introduced through Applications
- 7 Key Case Studies
- 8 Creating Co-models
- 9 Faults and Fault Tolerance Mechanisms
- 10 Design Space Exploration
- 11 Applications

Part III Advanced Topics
- 12 Semantics of Co-simulation
- 13 Deploying Co-modelling in Commercial Practice
- 14 Distributed Controllers
- 15 Future Directions: from Embedded to Cyber-Physical Systems
DESTECS TOOL DOWNLOADABLE

- [http://www.destecs.org/downloads.html](http://www.destecs.org/downloads.html)
- Automatic installer for Windows
- Ask for temporary license for 20-sim
- User manual in pdf or hyperlink formats
- Sources of DESTECS and Overture accessible from SF
- Public examples repository available
- A zip file with all the co-models can be imported
- Then you will be able to experiment with this!
FUTURE OF FORMAL METHODS

✓ Embedded Systems Development
✓ The DESTECS Technology
➢ Industrial Case Studies
➢ Systems of Systems Challenges
➢ Cyber-Physical Systems
OTHER DESTECS CASE STUDIES
INDUSTRIAL CASE STUDIES

Case studies inside project
  > A personal transporter (SegWay-like)
  > A dredging excavator
  > A document handling system (printer-like)

Industrial Follow Group Challenges
  > Crisplant, DK: Banking function on conveyor belt
  > Terma, DK: Flare dispenses for aircraft
  > ESA-ESTEC, NL: Planetary rover
ADDITIONAL INDUSTRIAL PHD

- Sune Wolff (MSc, RT-embedded systems, BSc, EE)
- Terma A/S (Avionics)
- Case study: Co-simulation of EW for aircraft
- Research theme similar to DESTECS challenge
- Focus on industrially applicable methodology
- Wider-research scope than DESTECS
- Not fixed on discrete event and continuous-time formalisms
ESA – MARS ROVER

• Proposer: ESA-ESTEC (NL) Automation & Robotics Laboratory

• design studies for new planetary rover platform concepts

• investigation of novel locomotion modes (so-called “gaits”)

• existing 20-sim model(s) (locomotion, gait algorithm design, 3-D visualisation) provided by ESA/ESTEC Automation & Robotics Laboratory

• Gait algorithms (re-)implemented in VDM by DESTECS team
ESA – MARS ROVER

your favorite planet

DRIVE TRAIN

ROTATE SHOULDER (6)

ROTATE WHEEL (6)

STEERING (4)
Three gaits:
• linear
• point turn
• Ackermann turn

CT : contact model
DE : gait controller

fault tolerance: safety monitor prevents robot from falling over
VERHAERT – DREDGING EXCAVATOR

- Overload and end-stop protection
- Emergency switch and system reset behavior
- Advanced operator assistance (i.e. perform a straight dig)
OBSERVATIONS AND CONCLUSIONS

› Formal Methods helps to de-risk development
  › including de-risking detailed formal analysis
  › providing rapid, accurate, but maybe incomplete analyses
  › training and methodological guidelines are crucial
  › start formal, (higher chance to) remain formal

› What does formalism buy us?
  › Sound semantic basis for the co-simulation tools & methods
  › Comprehensive analytic solutions are a long way off…
    … so (trustworthy) executable specifications are legit!

› Co-modelling exposes issues that are often implicit
  › In individual disciplines (we knew that already!)
  › And across boundaries, e.g. where to model faults
  › Expose potential problems earlier (no-brainer)

› Co-simulation is enabler for Design Space Exploration
  › Collaboration (also between researchers and practitioners 😊)
FUTURE OF FORMAL METHODS

✓ Embedded Systems Development
✓ The DESTECS Technology
✓ Industrial Case Studies
➢ Systems of Systems Challenges
➢ Cyber-Physical Systems
WHAT IS SPECIAL ABOUT SOS?

› Different characteristics:
   › Operational Independence
   › Managerial Independence
   › Geographic Distribution
   › Evolutionary Development
   › Emergent Behaviour

› Different categories:
   › Directed [Maier98]
   › Virtual [Maier98]
   › Collaborative/ Voluntarily [Maier98]
   › Acknowledged [Dahmann&08]
Objectives

1. **Modelling languages and methods** for SoS Engineering.
2. **Demonstrate the viability of tool support** for static analysis, simulation and testing based on SoS models.
3. **Evaluate effectiveness** of model-based methods and tools in industrial settings.
4. **Pragmatic methods** for developing, realising, and maintaining SoSs, based on architectural modelling, consistent with current international standards and initiatives.
5. **Engage stakeholders** in SoSs in current and future research on model-based approaches to SoS design.
COMPASS: BASELINES & ADVANCES

• Baseline Technologies
  – Modelling: SysML
  – Simulation support: executable models

• Advances:
  – CML: modelling language specifically for SoS
  – Built from VDM and Circus (established formal languages)
  – SysML+CML: support for contracts
  – Tool Support exploiting existing technology (e.g. Overture, Artisan Studio)
### COMPASS: COMMUNITY MEMBERS

#### Consortium
- Newcastle University, UK
- Aarhus University, DK
- University of York, UK
- University of Bremen, DE
- Federal Univ. Pernambuco, BR
- Bang & Olufsen, DK
- Insiel, IT
- Atego Systems Ltd., UK

#### COMPASS Interest Group (so far)
- Mectron
- Nokia
- Rockwell Collins
- Roke Manor Research
- Rolls-Royce
- Selex Systems Integration
- Provincia di Udine
- UN University (e-Government), Macau
- BAESYSTEMS
- Embraer
- GridManager
- West Consulting
- Terma
- University of South Australia
- Jaguar Land Rover
- National Institute of Informatics, Japan
ENGINEERING SYSTEM OF SYSTEMS

› **SoS:**
  › constituent systems interacting via an *infrastructure*.
  › *rights and responsibilities* borne by constituent systems
  › Need to achieve a *global* (or end-to-end) performance
  › In the face of *heterogeneity* of ownership, management, stakeholders, evidence, …

› **Do SoS “just happen”?**
  › Decisions are made (constituents, allocation of responsibilities, coordination policies,…)
FUTURE OF FORMAL METHODS

✓ Embedded Systems Development
✓ The DESTECS Technology
✓ Industrial Case Studies
✓ Systems of Systems Challenges
✓ Cyber-Physical Systems
NEW LARGE APPLICATION COMING

› Extensions to network of heterogeneous embedded systems
› Follow up on the DESTECS project
› Incorporation of SysML and Mathlab/simulink
› More focus on automation
› Japanese partners can also participate but without EU funding
› Let me know if you are interested
› Also if only for the Industrial Follow Group
INTERESTING RESEARCH DIRECTIONS

› Embedded systems
  › How to unify different models of modelling/computation?

› System of Systems
  › How to model and analyse SoSs?

› Cyber Physical Systems
  › How to have multiple inter-acting constituent models?

› Formal methods can play an important role here
› Precision and analysis in early phases
› Fidelity of physical modelling depend on needs
TAKE AWAY POINTS

› Interesting new ways in which formal methods can be applied
› Usable formal methods are essential
› Increasing need for multi-disciplinary approach
› Cyber-physical systems become important
› Combinations between systems becomes important
› Interesting research areas that can have impact

If you are interested in collaboration, please let me know!
THANKS FOR YOUR ATTENTION

Any questions?