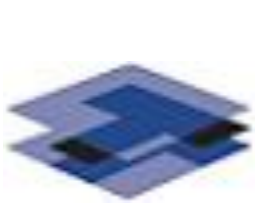
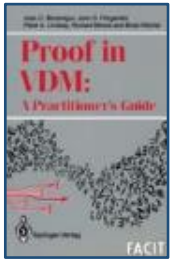
Who is this guy?

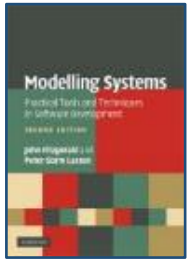
- Short Bros., Belfast; IBM Hursley; PhD (Manchester) on interaction of modular structuring with formal proof (pinnacle of hype?)
- Came to Newcastle, worked with BAESYSTEMS on avionics design; then evaluating new model-based formal techniques in BAE
- Learned that software correctness is a long way from system dependability (valley of disillusionment?)
- Developing accessible formal methods and tools
- Managed design team in Transitive Ltd.
- Returned to academia 2003. Group works to develop *and deploy* accessible formal methods (up the slope of enlightenment?)



"The most amazing software you'll never see“

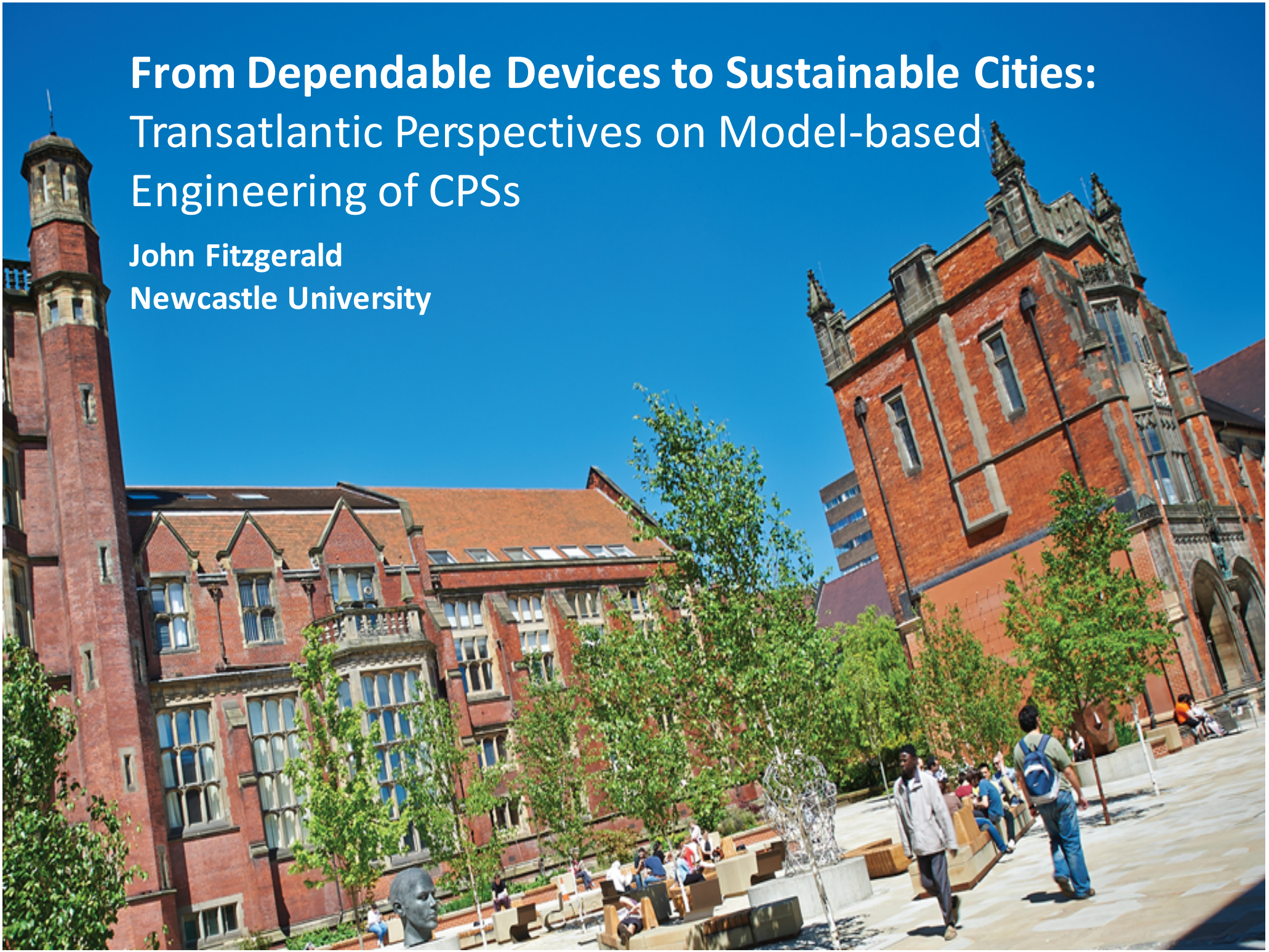
Steve Jobs





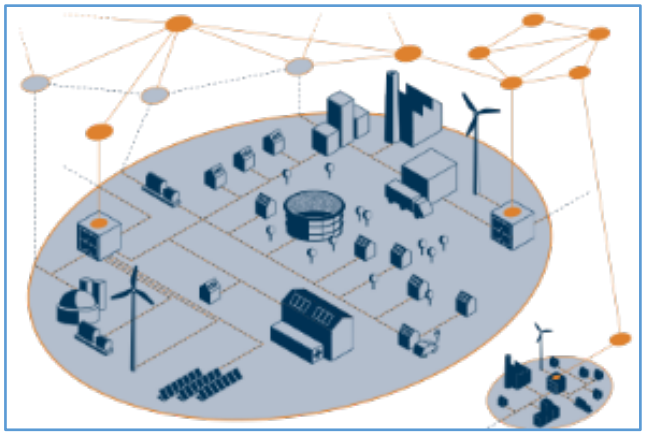
From Dependable Devices to Sustainable Cities:
Transatlantic Perspectives on Model-based Engineering of CPSs

John Fitzgerald
Newcastle University



Dependable Devices … Sustainable Cities

Vehicle localisation
Obstacle detection
Brake assist
Fleet management
Congestion control
Toll payment



Emergency shutoff
Predictive maintenance
Fault detection
Virtual Power plant
Load prediction
Dynamic pricing

Technical Process
Organisational Process

Mastering the engineering and operation of high-performant CPS upon which people can depend

- **Integrated cross-domain architectures**
- Required **trustworthiness versus evolving** CPS
- **Design-operation continuum** (continuous deployment, live experiments)
- Engineering methods and tools able to **cope with the full scale and complexity of CPS**
- **Integrated cross-disciplinary models and analysis** for distributed analog/digital control and management
- **Human-technology interaction**

Source: CyPhERS project, 2014
www.cyphers.eu

Dependable IoT-enabled Systems

We should expect many IoT-enabled systems to have the characteristics of:

- Systems of Systems (SoS):
  - independently owned and managed constituent systems
- Cyber-Physical Systems (CPS):
  - computational processes and some are physical
- Often, reliance has come to be placed on the behaviours that emerge from interactions between elements
- Engineering inherently multi-stakeholder and multi-disciplinary

Newcastle University

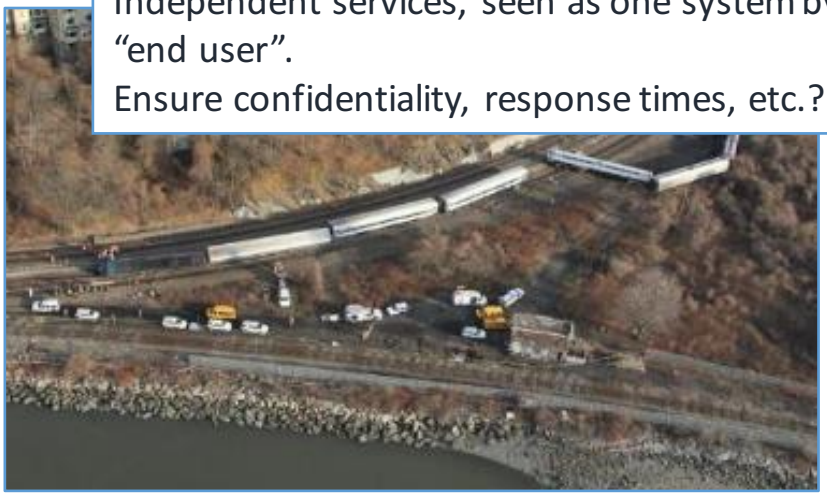
Dependable SoS & CPS

COMPASS

- Operational & Managerial Independence of Constituent Systems
  - Constituent systems evolve independently
- Complexity of confirming/refuting SoS-level properties
  - Verification of emergence
- Semantic heterogeneity (integrating models)
  - Wide range of interacting features in models (e.g. location, time, concurrency, data, communication)

Audio/Video (Bang & Olufsen)
Independent networks, devices, content services. Ensure a consistent "SoS experience"

Emergency Response (Insiel)
Independent services, seen as one system by "end user".
Ensure confidentiality, response times, etc.?



Dependable SoS & CPS

COMPASS

Independence and autonomy of constituent systems

Constituent systems evolve at the behest of their owners

Response: Collaborative SoS modelling by contractual (rely, guarantee) interface specification

Complexity of confirming/refuting SoS-level properties

Verification of emergence

Response: verified refinement for engineering of emergent properties; simulation tools allow exploration for unanticipated behaviours

Semantic heterogeneity (integrating models)

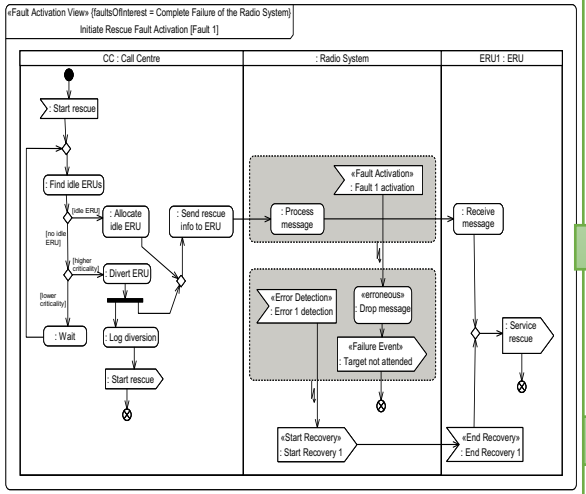
Wide range of interacting features in models (e.g. location, time, concurrency, data, communication)

Response: extensible semantic basis

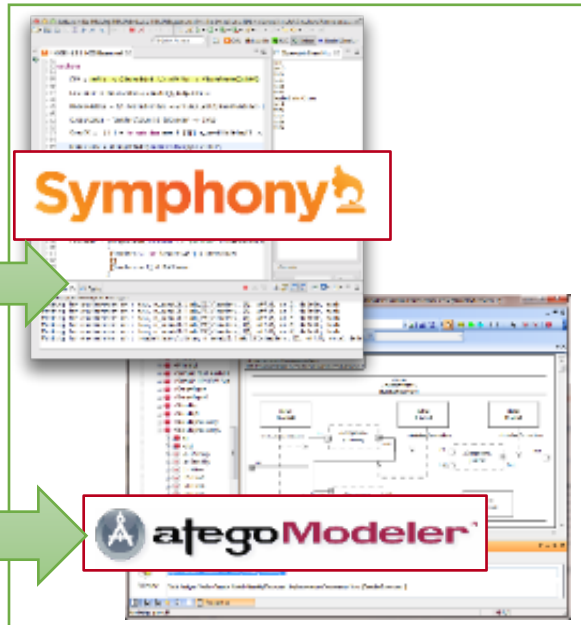
Newcastle University

COMPASS

www.compass-research.eu




```
process CallCentreProc = begin
...
actions
 MERGE1(r) =
  (dcl e: set of ERUId @ e := findIdleERUs();
   (do
     e = {} -> DECISION2(r)
     |
     e <> {} ->
      (dcl e1: ERUId @ e1 :=
        allocateIdleERU(e, r); MERGE2(e1, r))
   end)) ...

process InitiateRescue =
CallCentreProc [| SEND_CHANNELS |]
RadioSystemProc [| RCV_CHANNELS |] ERUsProc
```



Architectural Modelling

- SysML (relatively informal semantics)
- Useful guidance on SysML model structure
- Patterns and extensible frameworks can be described

Underpinning Formalisms

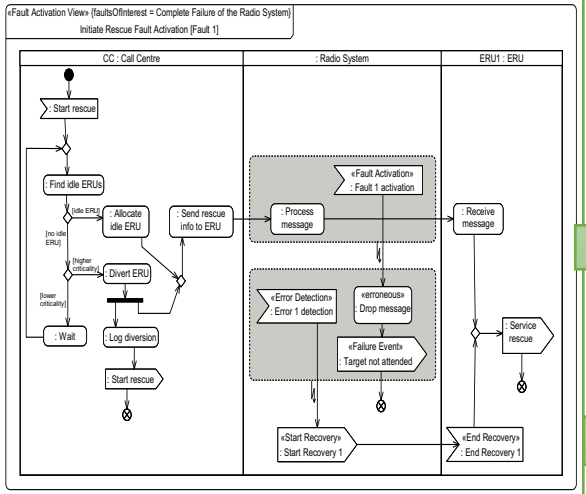
- CML (inspired by VDM and Circus) allows contractual representation of behavioural semantics of the SoS
- Extensible UTP semantic basis supports heterogeneity: describes functionality, object-orientation, concurrency, real-time, mobility.

Tool-supported Analysis

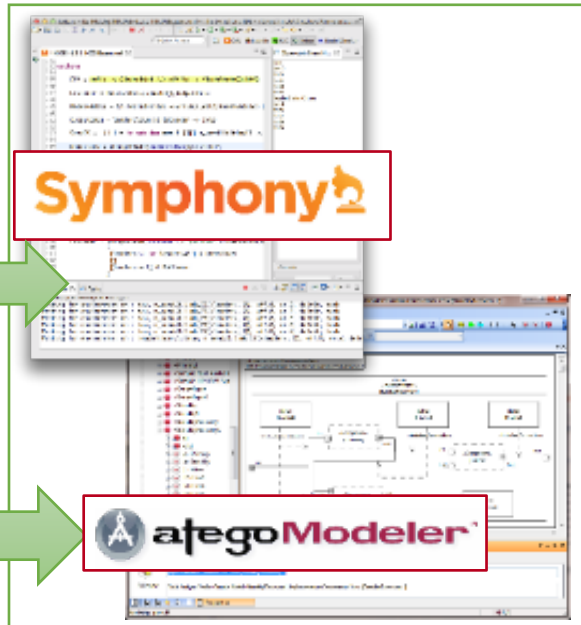
- Model-checker
- Automated proof
- Static Fault Analysis
- Test generation (RT-Tester)
- Simulation
- Model-in-Loop Test
- Exploration of design space

COMPASS

www.compass-research.eu




```
process CallCentreProc = begin
...
actions
 MERGE1(r) =
  (dcl e: set of ERUId @ e := findIdleERUs();
   (do
     e = {} -> DECISION2(r)
     |
     e <> {} ->
      (dcl e1: ERUId @ e1 :=
        allocateIdleERU(e, r); MERGE2(e1, r))
   end)) ...

process InitiateRescue =
CallCentreProc [| SEND_CHANNELS |]
RadioSystemProc [| RCV_CHANNELS |] ERUsProc
```



Architectural Modelling

- SoS Modelling Frameworks
- … instantiated to domains
- SoS Modelling patterns & profiles, e.g. Fault-Error-Failure
- Guidelines on negotiation, requirements, integration, test, etc.

Underpinning Formalisms

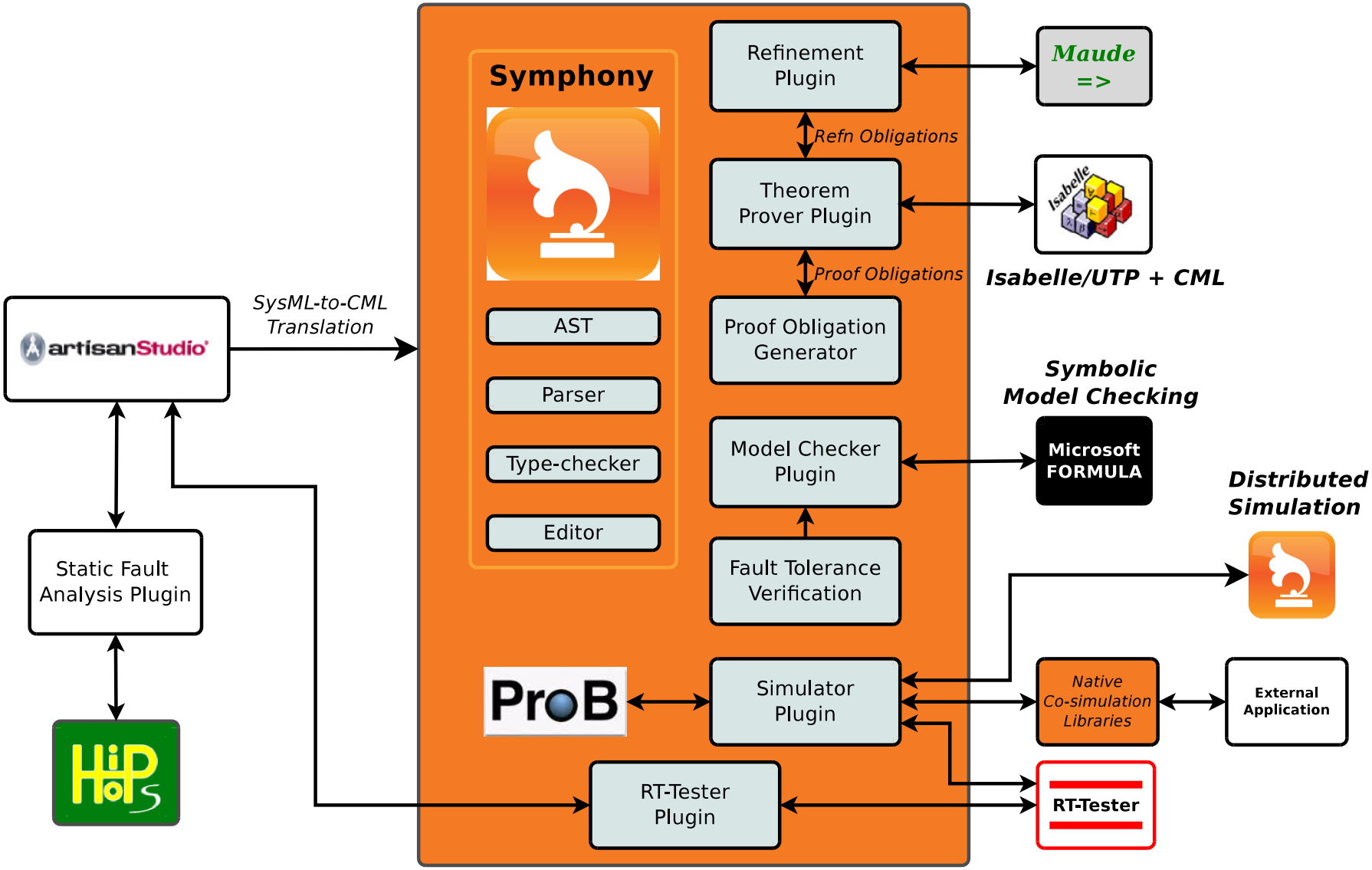
- Behavioural semantics of SoS
- Tight link to modelling frameworks
- Cope with multiple paradigms.
- Compositional Design
- Dynamic response to adaptation & evolution
- Covering cyber elements, physical, human, economic, social, …

Tool-supported Analysis

- Exploration of Design Space
- Efficient verification by model-checking and proof
- Test generation
- Simulation
- Tools Robustness
- Conformance during evolution, and emergence

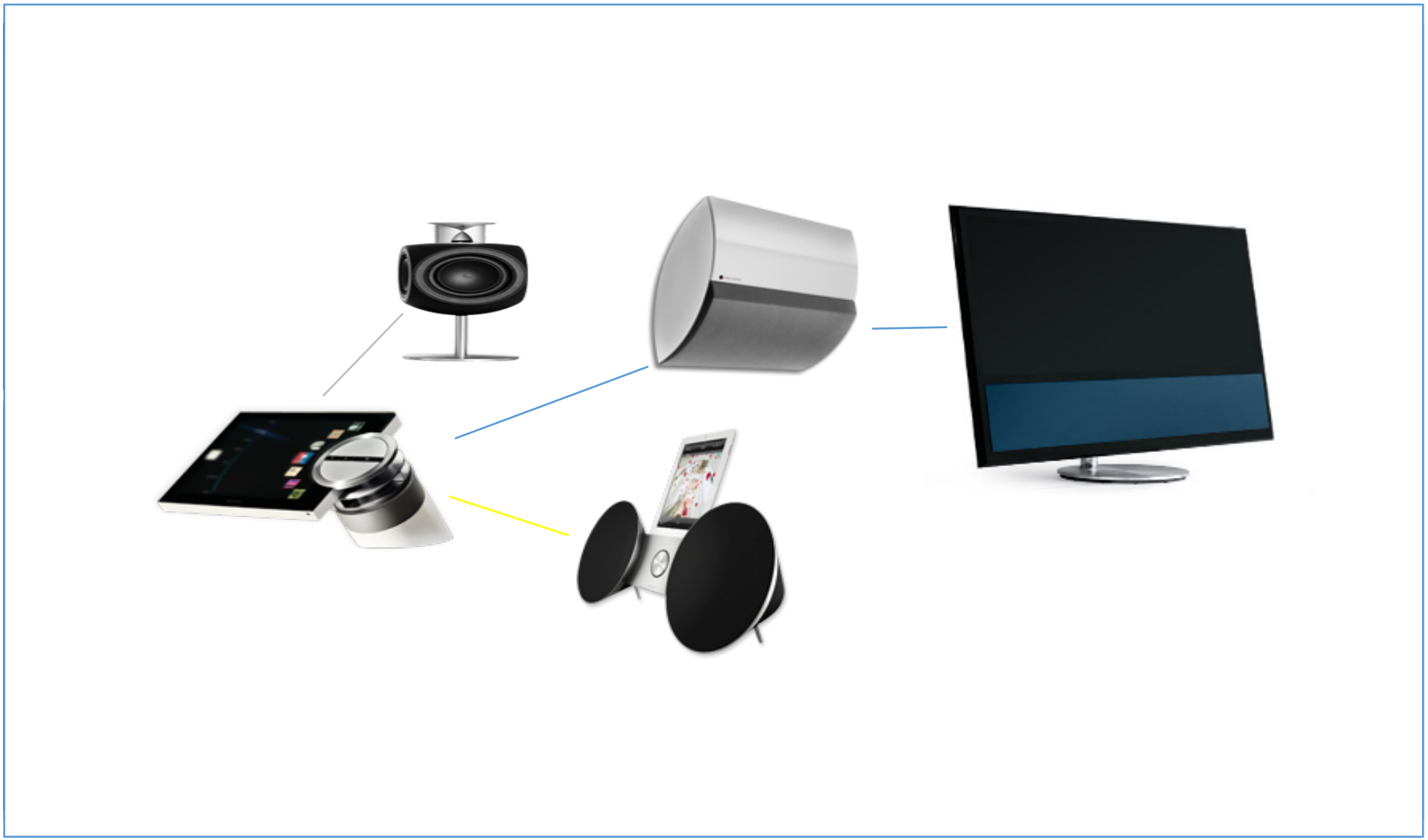
Dependable SoS & CPS

COMPASS



Dependable SoS & CPS

COMPASS



Dependable SoS & CPS

COMPASS

- Guidelines, Frameworks, Patterns:
  - Requirements, Architectural Modelling Framework, Integration, Fault Modelling
  - COMPASS Architectural Framework Framework
  - All “digital” models
  - No large scale models (but B&O state space was huge!)
- Foundations:
  - Modelling Language Semantics
  - Contractual basis allowed machine-assisted V&V
  - extend to stochastic models, continuous time models, agent-based?
- Tool Support:
  - Tools platform & integrations
  - Variety of tool TRLs

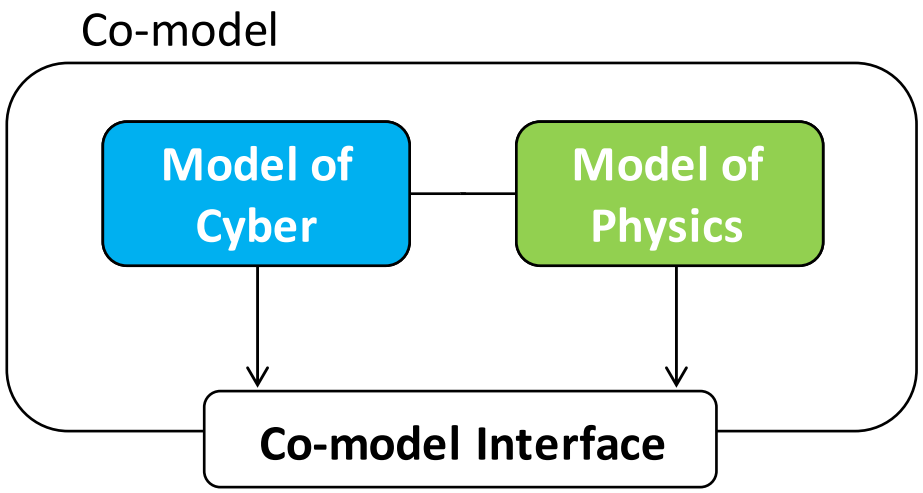
Newcastle University

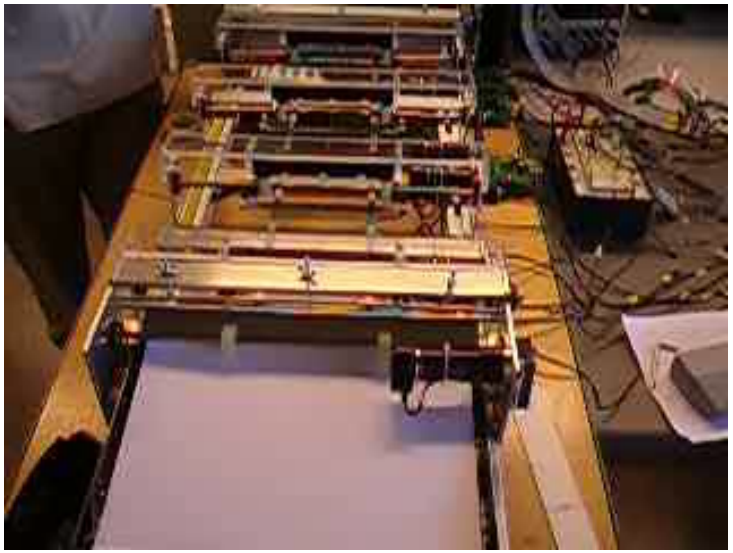
Dependable SoS & CPS

Co-modelling reduces early development risk by integrating diverse models

Software Models:
- Discrete
- Complex logic

Physics Models:
- Continuous
- Numerical





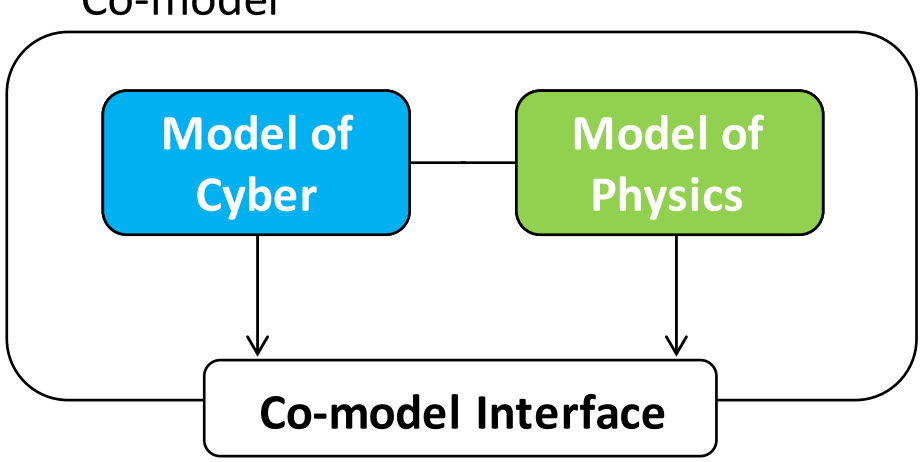
Newcastle University

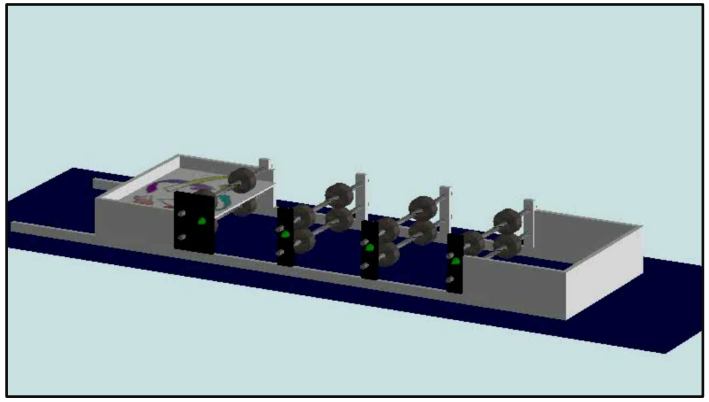
Dependable SoS & CPS

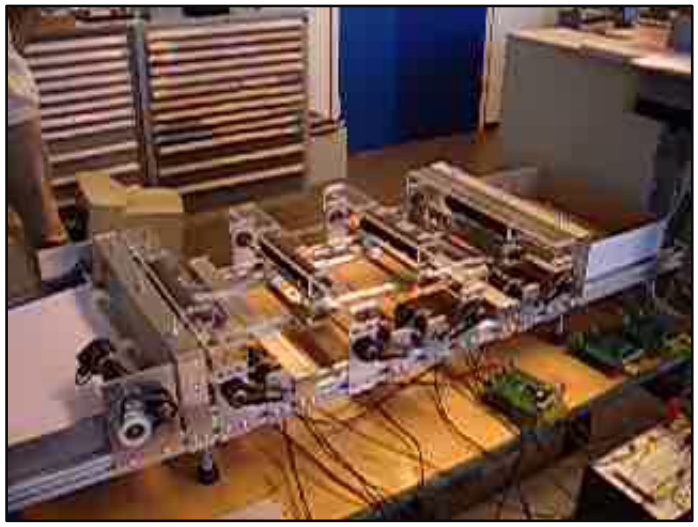
Co-modelling reduces early development risk by integrating diverse models

Software Models:
- Discrete
- Complex logic

Physics Models:
- Continuous
- Numerical

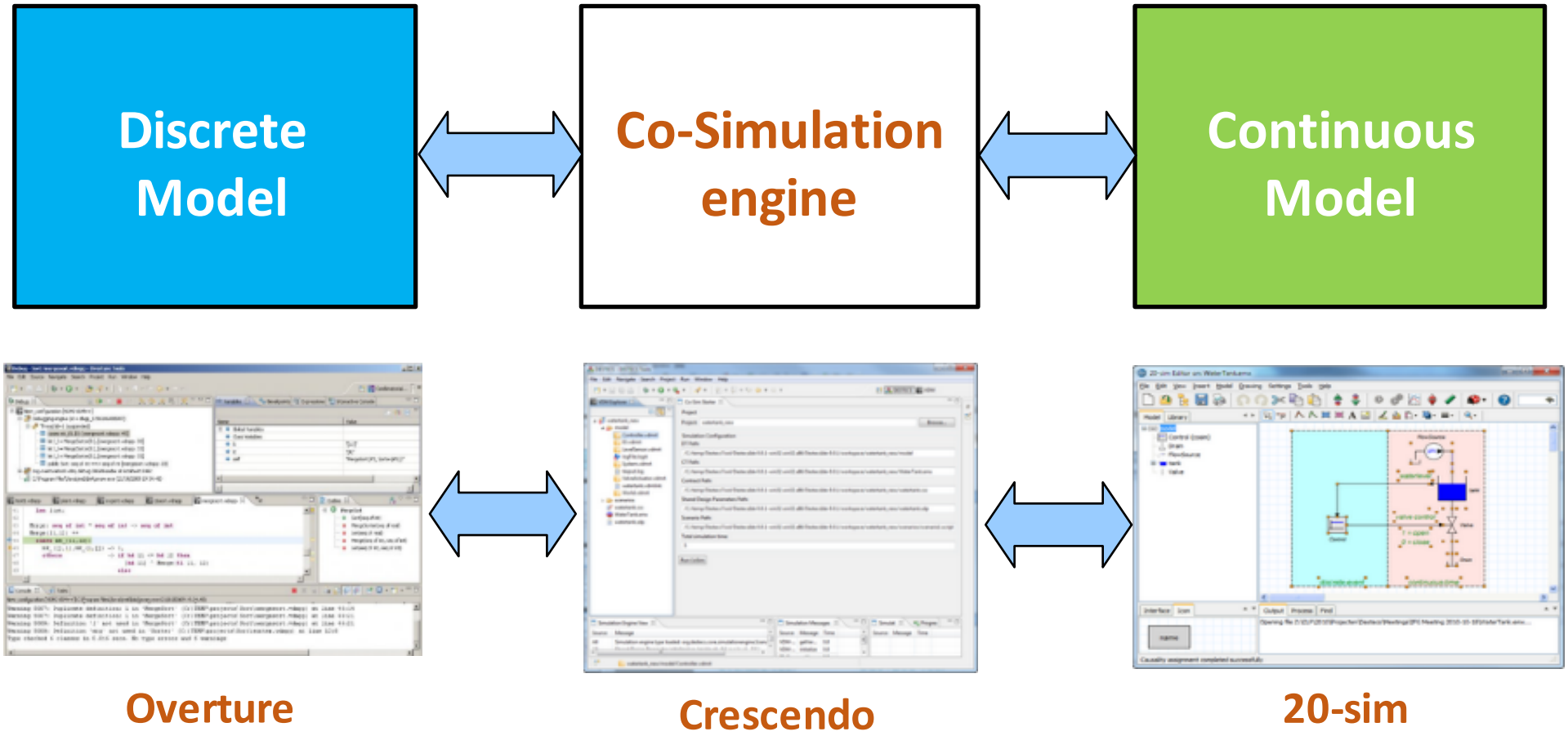






Newcastle University

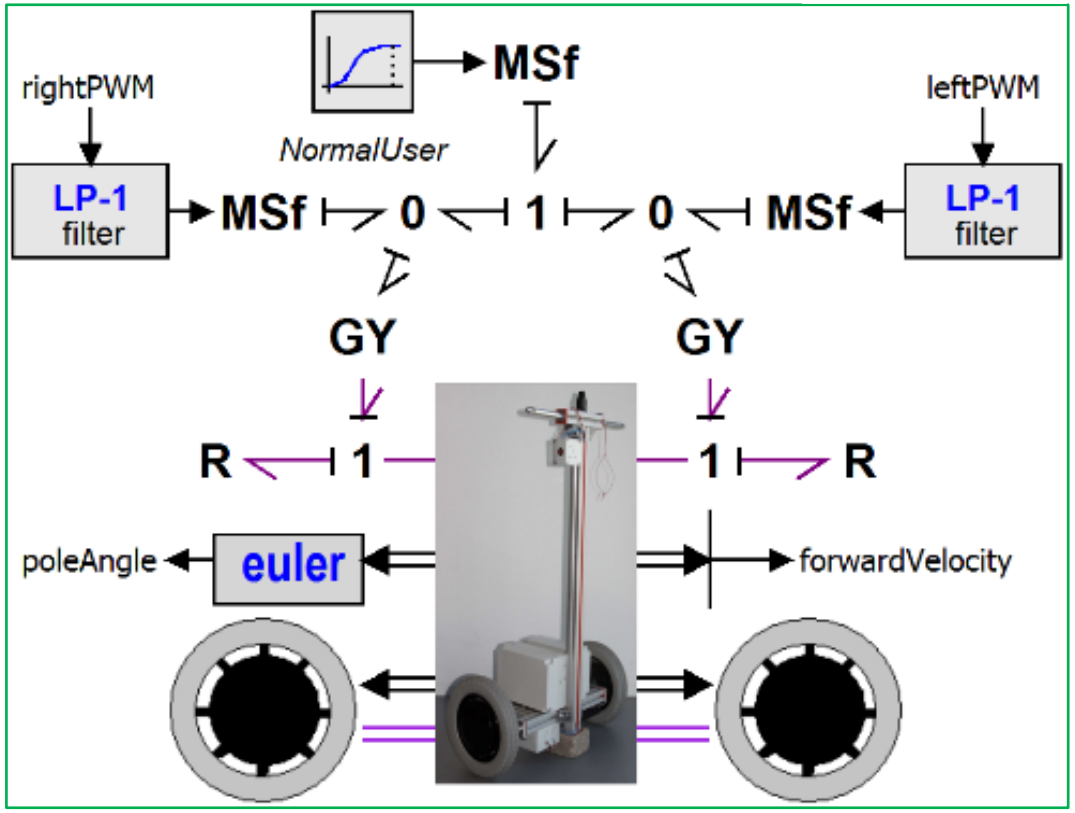
Dependable SoS & CPS



Newcastle University

Example: ChessWay

CT model



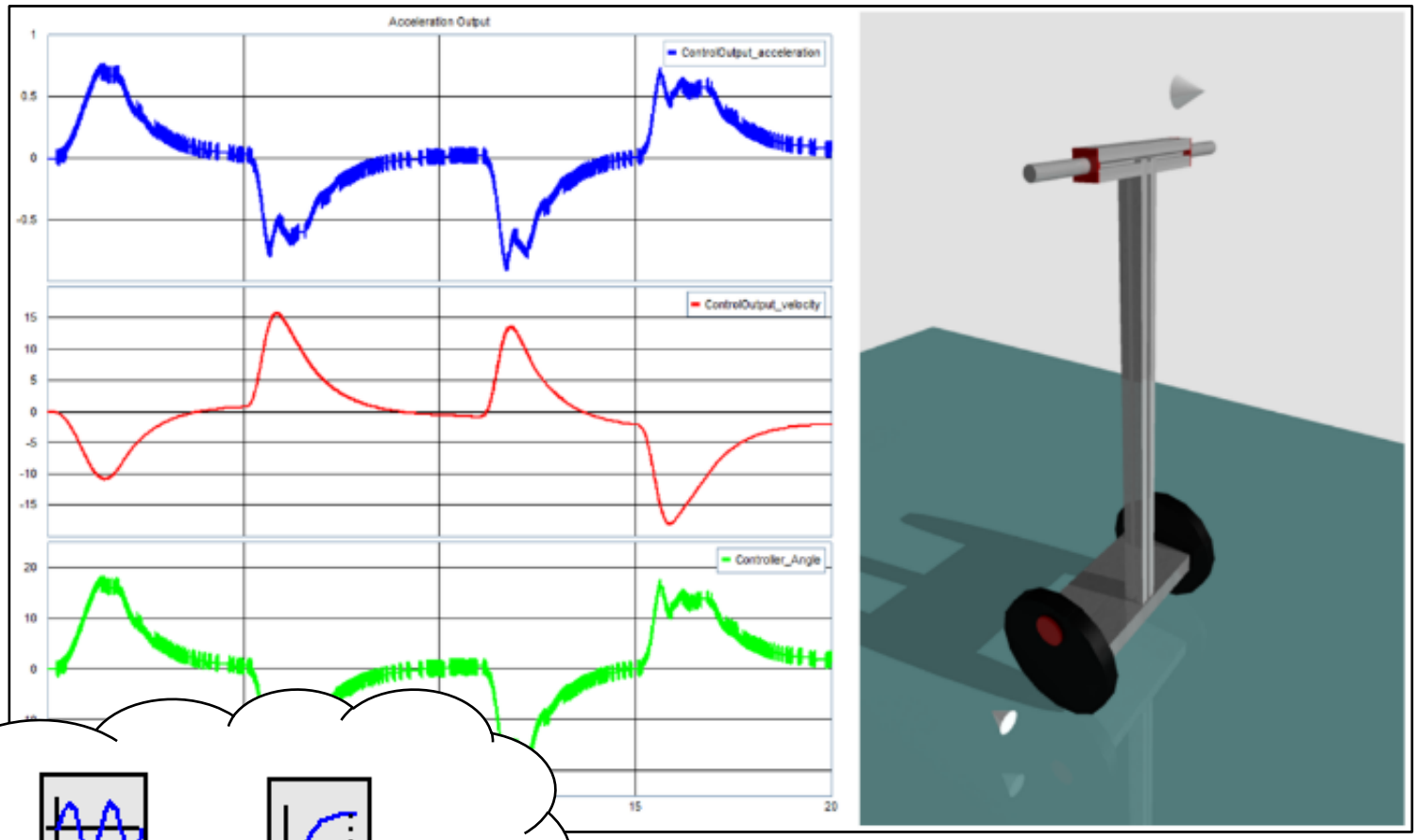
Interface

	Name	Type	Notes
controlled	leftPWM	real	range: [-1,1]
	rightPWM	real	range: [-1,1]
monitored	poleAngle	real	range: [0,2π]
	forwardVelocity	real	

DE model

```
class Controller

instance variables
  -- sensors
  private angle: real;
  private velocity: real;
  -- actuators
  private acc_out: real;
  private vel_out: real;
  -- PID controllers
  private pid1: PID;
  private pid2: PID;

operations
  public Step : () ==> ()
  Step() == duration(20) (
    dcl err: real := velocity - angle;
    vel_out.Write(pid2.Out(err));
    acc_out.Write(pid1.Out(angle));
  );

  public GoSafe : () ==> ()
  GoSafe() == (
    vel_out.Write(0);
    acc_out.Write(0);
  );

thread
  periodic(1E6,0,0,0)(Step); -- 1kHz

end Controller
```

Example: ChessWay



Newcastle University

Example: Dredging Excavator

DESTECS Project: Assisted mode for complex operations for a dredging excavator

Design Space Exploration optimised end-stop protection parameters

Koenraad Rambout (Verhaert): "A lot of time was saved on building physical prototypes. This ensures much faster iterations on physical models compared to traditional approaches. This enabled us to easily swap between different design solutions (e.g. hydraulic vs. electrical drives)"

Example: ChessWay

DESTECS Project: The ChessWay Personal Transporter

Early debugging in design

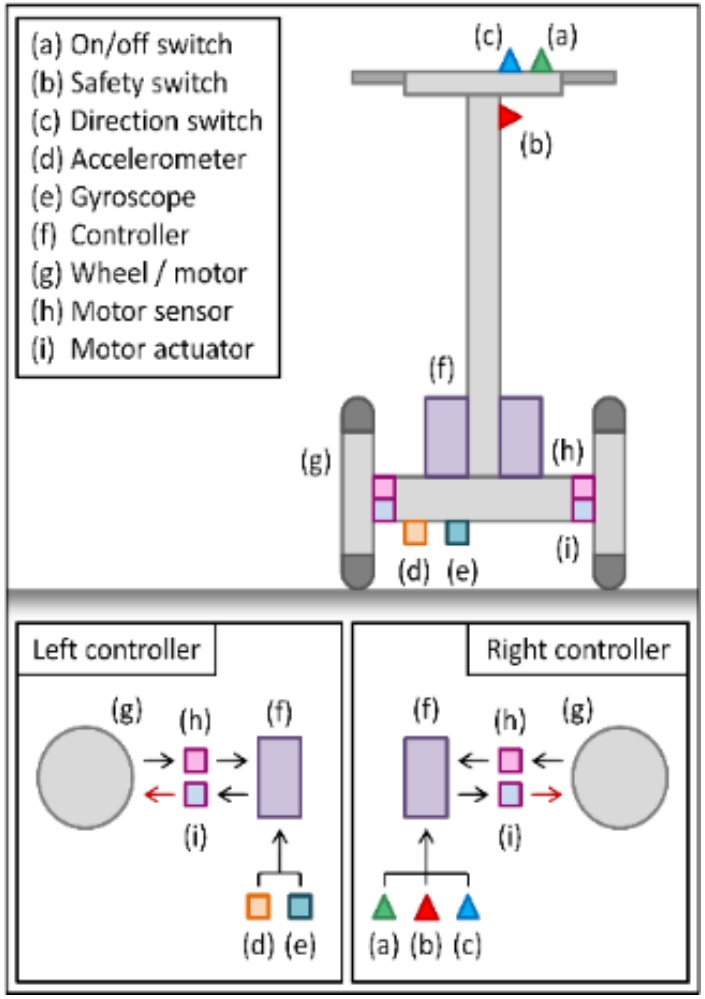
Bert Bos (Chess): "Debugging in the co-simulation environment is much quicker than debugging real-time embedded control software. … the initial implementation worked the first time… fault handling usually takes several cycles to work properly."

Dependable SoS & CPS: Design Space Exploration

- Systematic exploration of solution space
- Optimisation against defined criteria
- Ranges of design parameters
- Ranking of design alternatives
- Or further genetic or evolutionary optimisation on a Pareto front.

Example: a wireless ChessWay?

- What control loop frequencies provide safe balancing?
- Consider alternative frequencies and allocations of responsibilities between controllers.
- Explore how lossy comms can be, while maintaining safety conditions.



Dependable SoS & CPS

- Tools (Crescendo) method guidelines (notably fault modelling); Automated Co-model Analysis (sweeps, ranking)
- Evidence that co-model-based design can work: Reduced design iteration/cost
- **But little networking, and design phases only**

Newcastle University

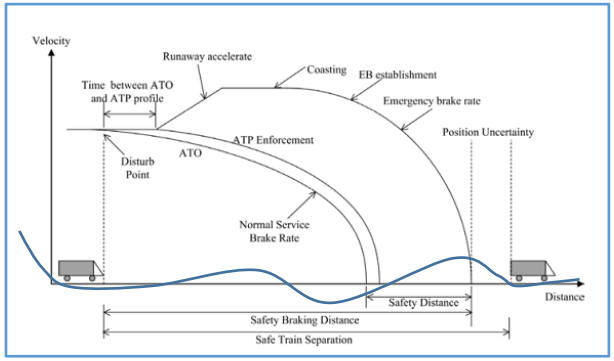
Dependable SoS & CPS: towards multi-models

- http://into-cps.au.dk
- Multi-Models (broader range)
- Well-founded tool chains, not a “factotum” tool:
  - Design Space Exploration
  - Raeability & Provenance support
  - Foundations in UTP
  - Static analysis of co-models
  - Requirements, Architectures (SysML) to code
- Baseline Technologies:
  - Modelio, VDM, 20-sim, Open Modelica, TWT co-sim engine, RT Tester.

Dependable SoS & CPS: towards multi-models

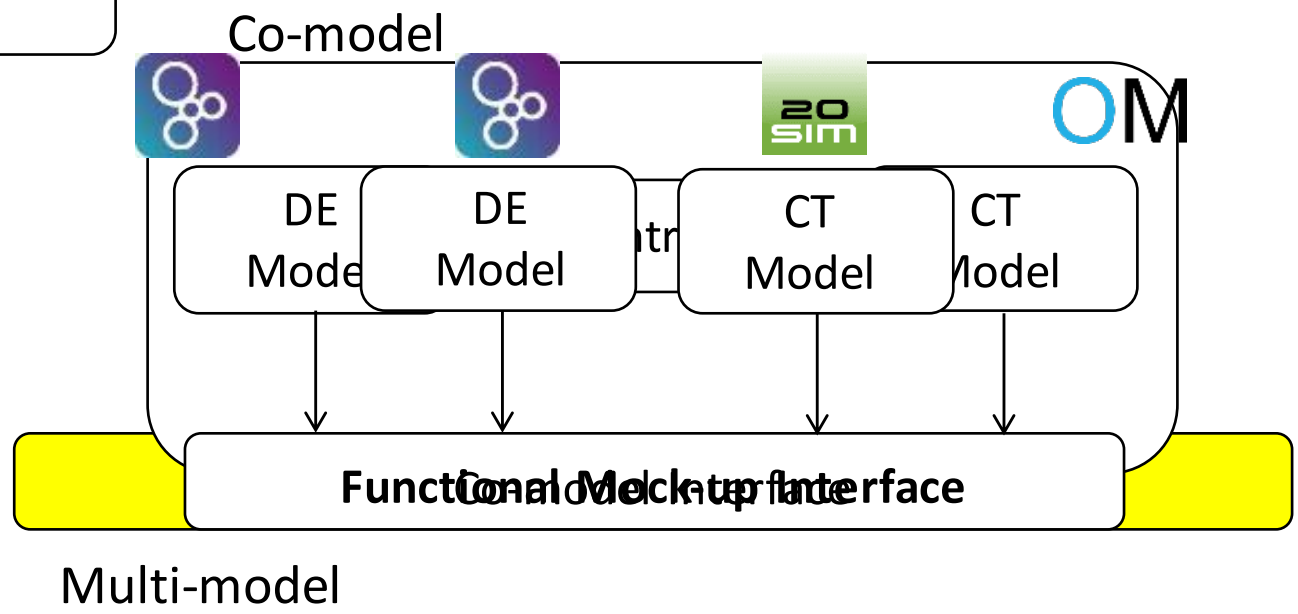
Applications underway:

- Railway interlocks, taking account of train dynamics and track topology
- Autonomous agricultural robots
- HVAC
- Electric vehicle driver advisories ("range anxiety")



Dependable SoS & CPS: towards multi-models

modelDescription.xml



Modelio — SysML modelling

Overture — Discrete-event modelling

20-sim — Continuous-time and physical-systems modelling

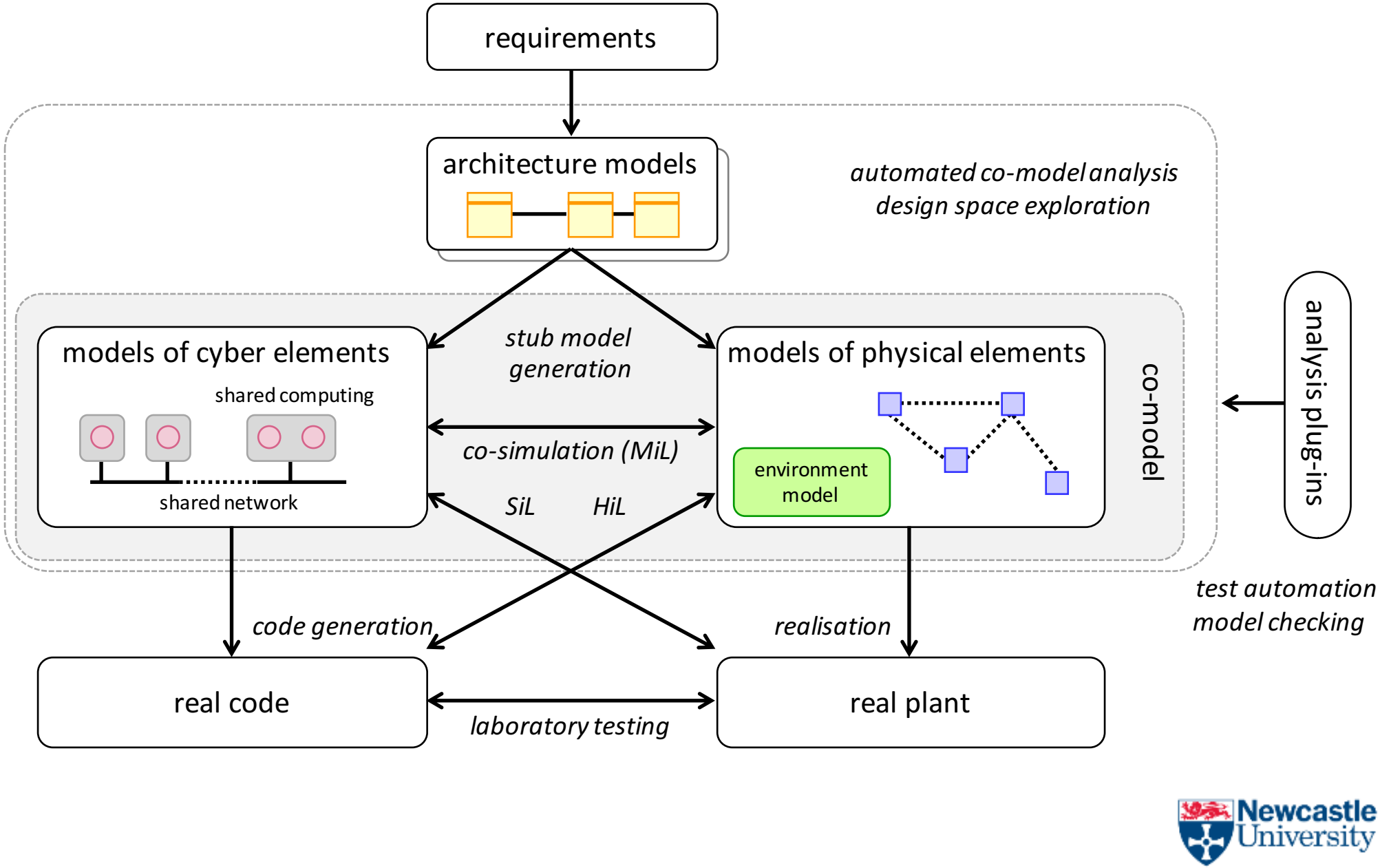
OpenModelica — Co-simulation solutions

Crescendo — Co-simulation solutions

TWT Engine — Test automation / model checking

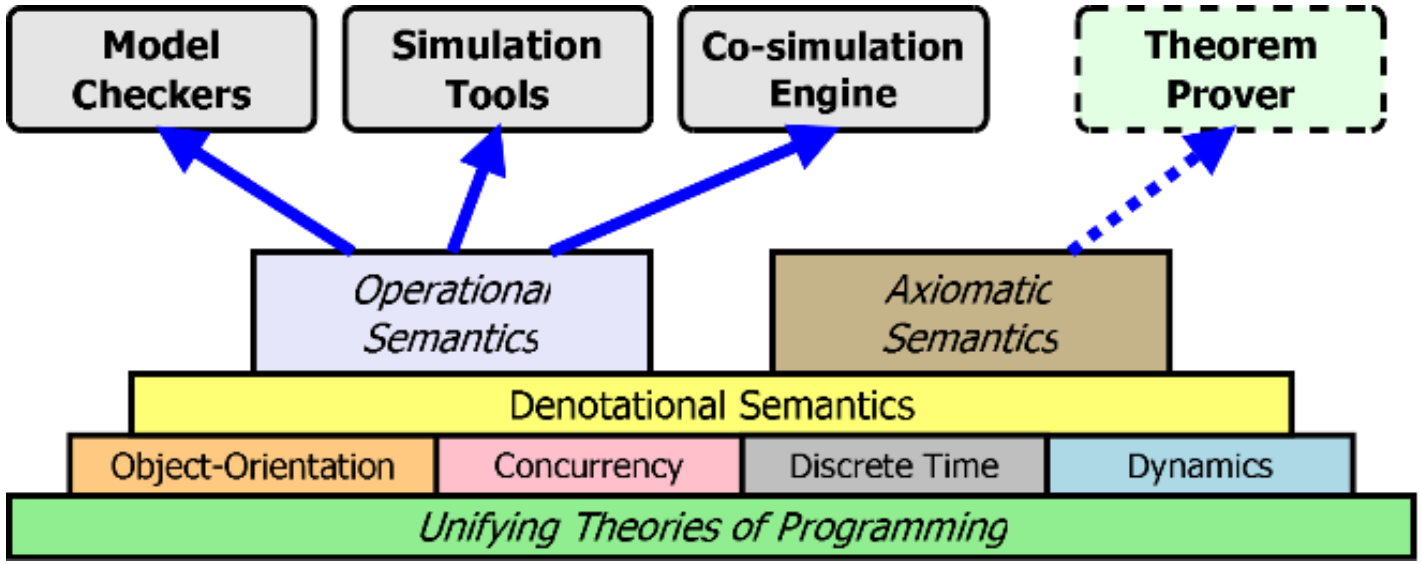
RT-Tester — Test automation / model checking

Dependable SoS & CPS: towards multi-models

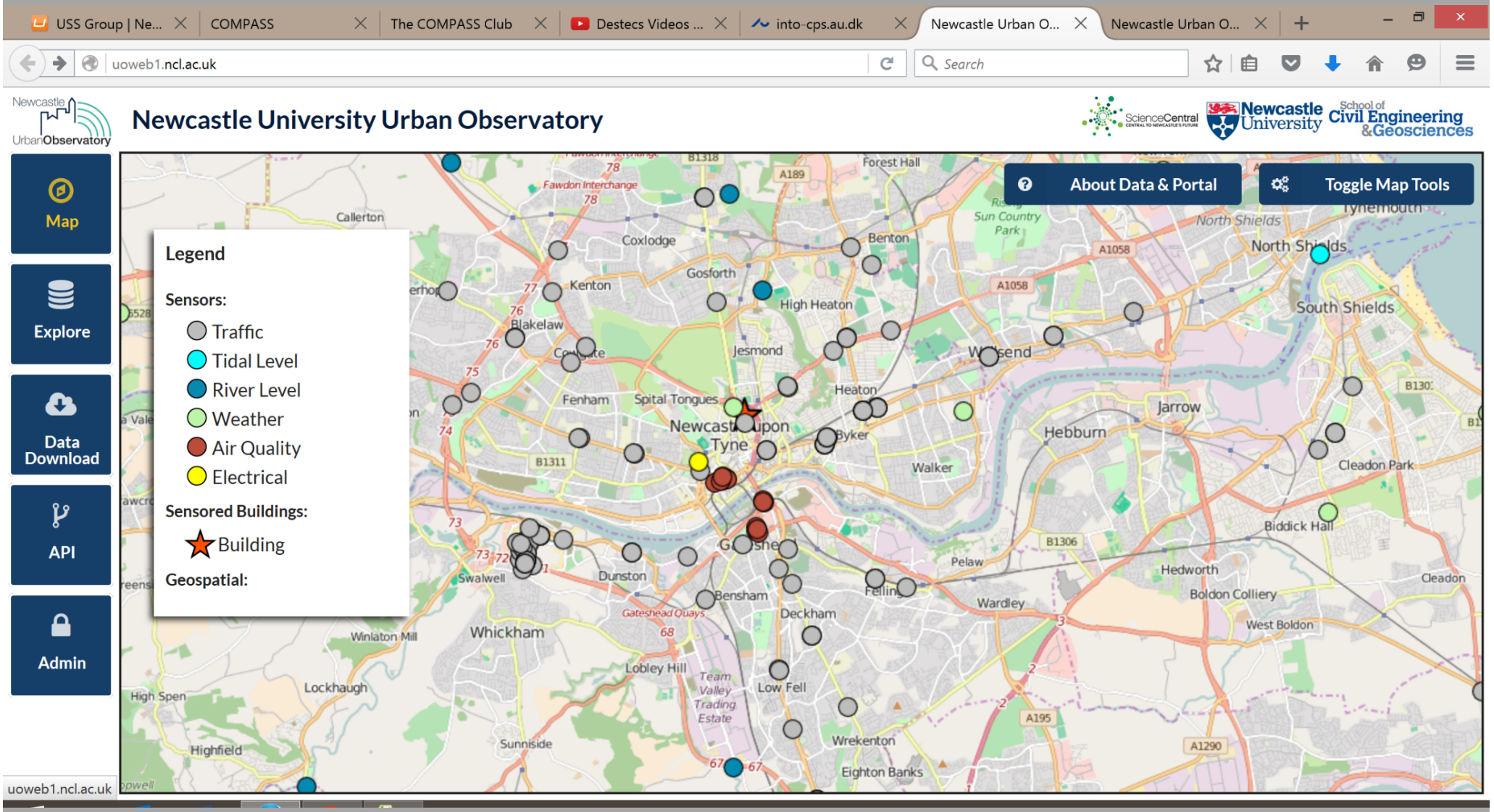


Newcastle University

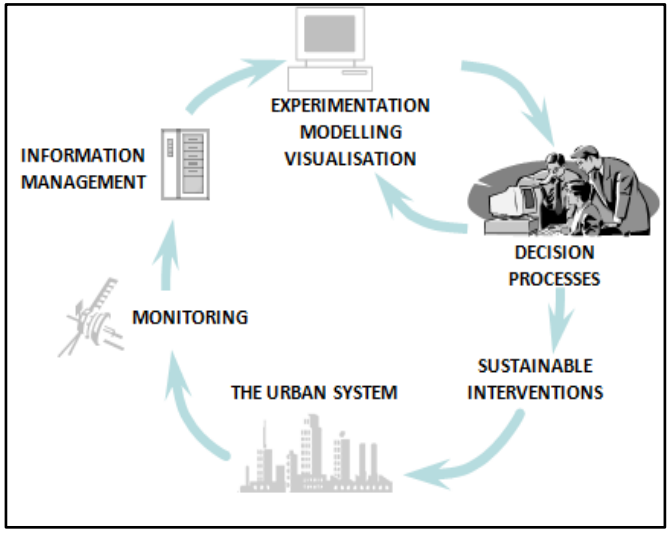
Dependable SoS & CPS: towards multi-models



CPS, SoS and the Sustainable City

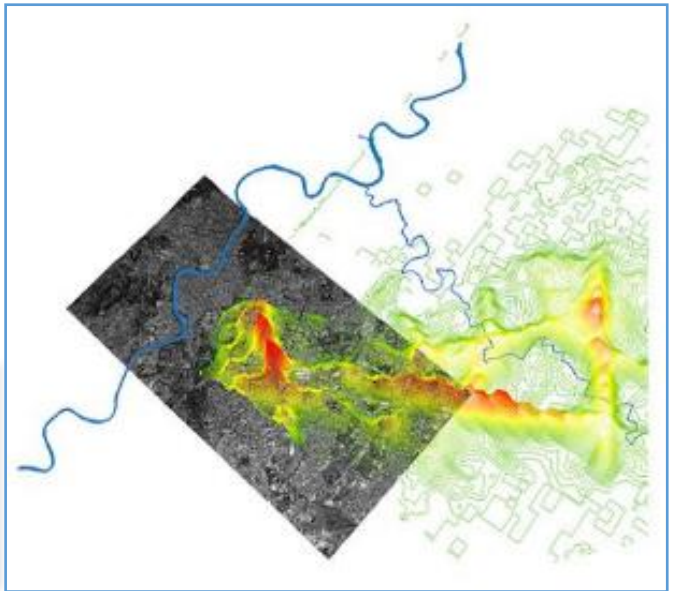


CPS, SoS and the Sustainable City

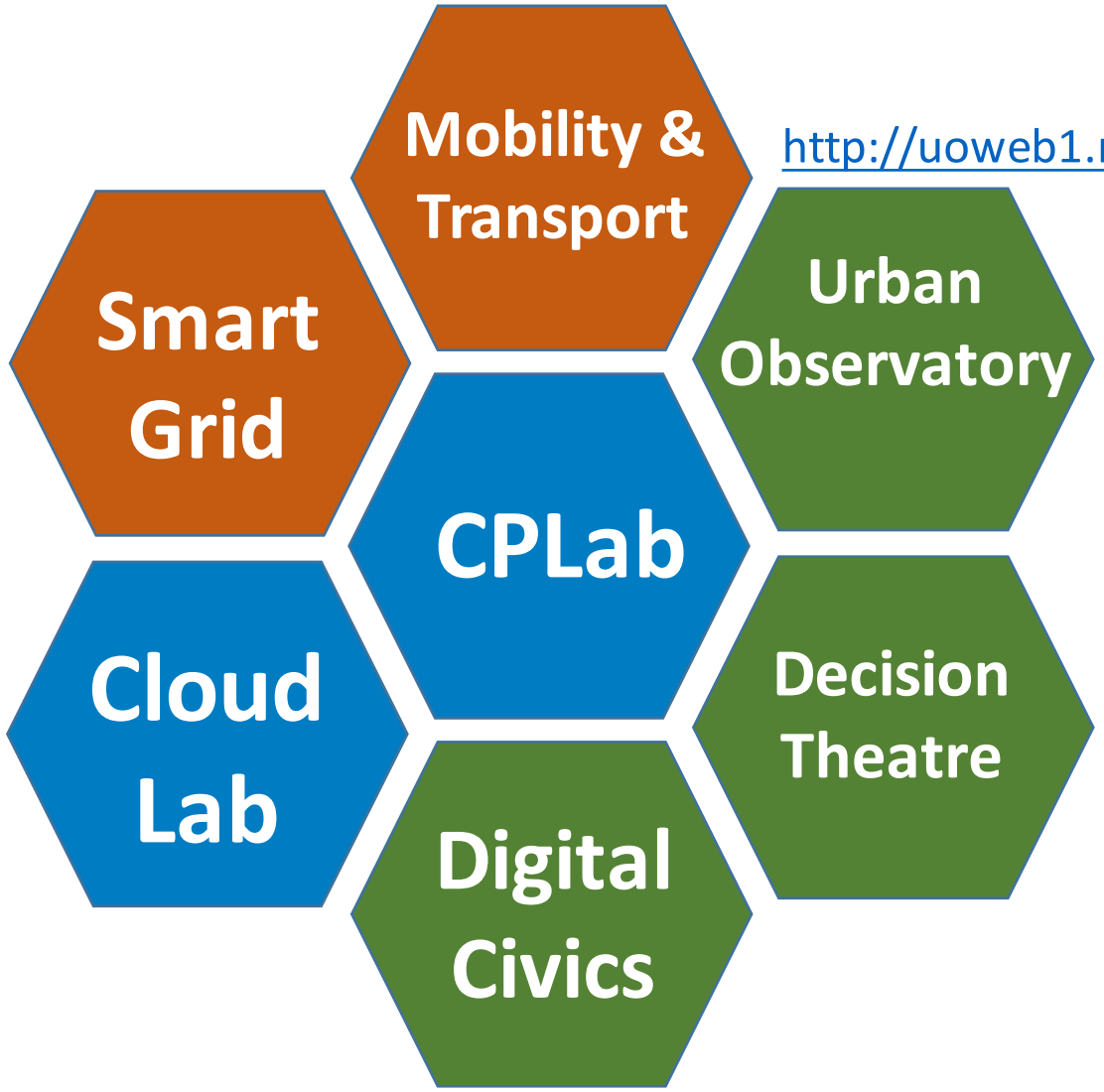


1970s (Reactive) **2010 (Intelligence)** **2050**

- Dependable CPSs are at the heart of achieving urban sustainability
- Digitally-enabled urban sustainability



New Laboratories ($84m project)



http://uoweb1.ncl.ac.uk/

Strategic Partnerships:

NORTHERN POWERGRID

SIEMENS

PHILIPS

NORTHUMBRIAN WATER *living water*

Scottish & Newcastle Brewery Site
2007

Science Central Site
2014

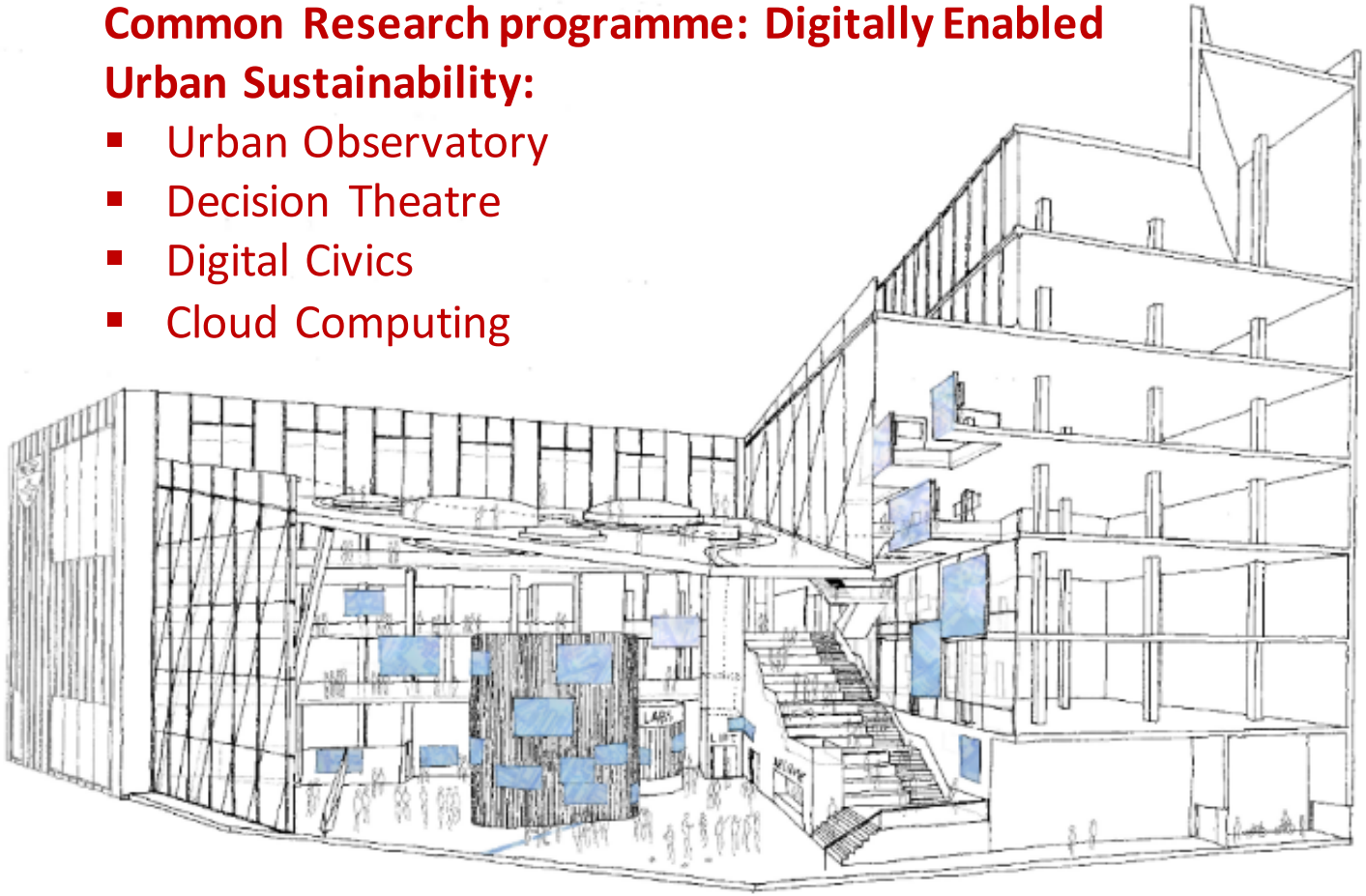
cctv.ussgroup.co.uk/Newcastleuni/


URBAN SCIENCES

New Laboratories: Urban Sciences Building

Common Research programme: Digitally Enabled Urban Sustainability:

- Urban Observatory
- Decision Theatre
- Digital Civics
- Cloud Computing



- Smart Grid
- Energy, Power & Transport
- Cyber Physical Lab

Research Groups and Business Spaces:

- Secure & Resilient Systems
- Model-based Engineering
- Complex Biosystems
- Scalable Computing
- OpenLab (Digital Interaction)
- Sustainability Institute

Public Realm: event spaces, café

Newcastle University

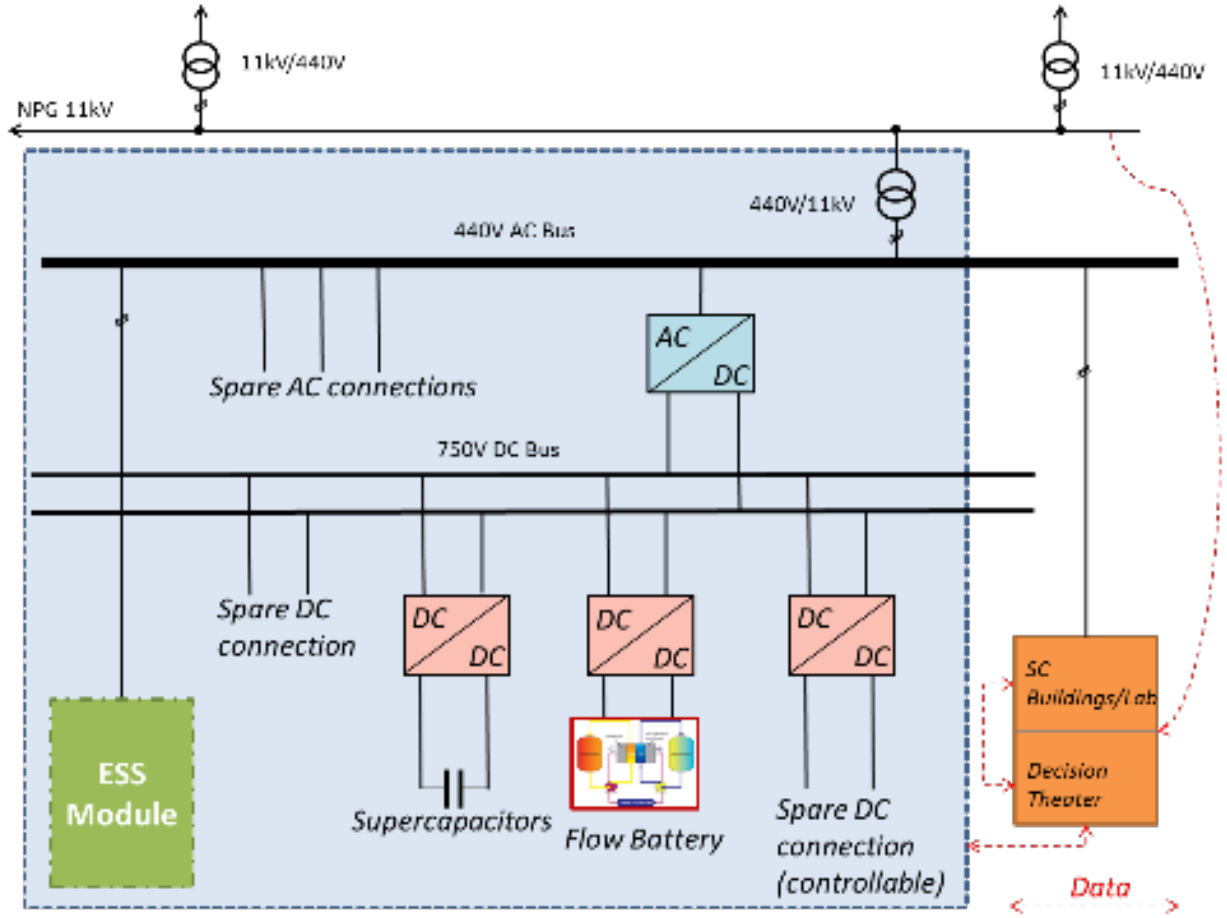
New Laboratories: Urban Sciences Building

Building as a Lab:

- Highly instrumented
- Green Infrastructure
- Water and waste
- Structures and Materials
- Electrical Systems
- HVAC
- Usability, health and wellbeing
- Secure and Resilient Systems
- Art and Engagement

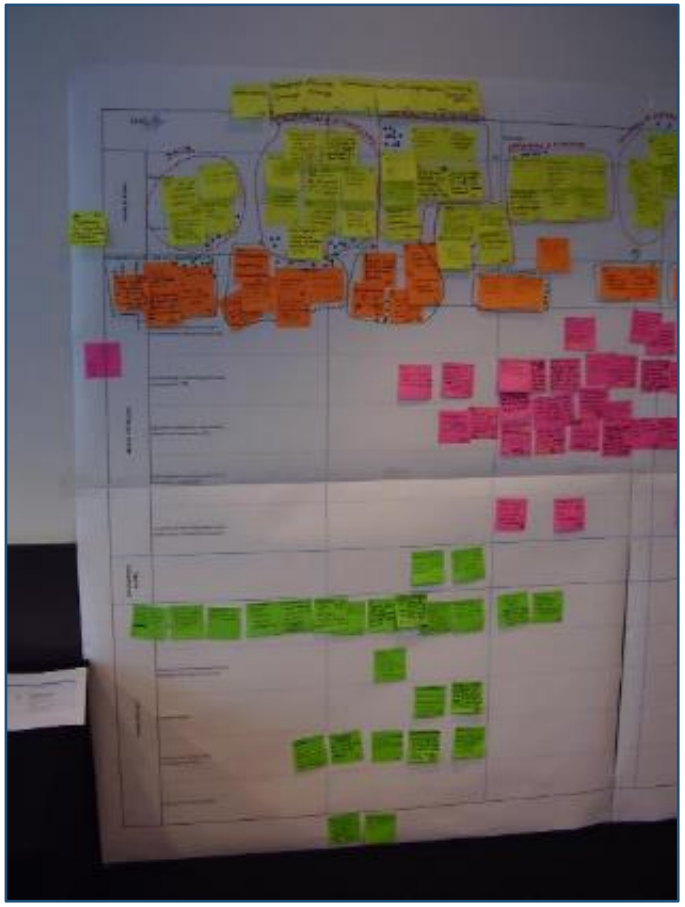
New Laboratories: Urban Sciences Building

The site as a Lab (local smart grid and energy storage test bed)



An Emerging Transatlantic and EU Perspective: TAMS4CPS

Transatlantic Perspectives



TAMS4CPS: Trans-Atlantic Modelling and Simulation for Cyber-Physical Systems

- 3 EU & 5 collaborators from the US
- Coordinator: Loughborough University, United Kingdom

George Mason University	Alex Levis
Georgia Institute of Technology	Dmitris Mavris
Purdue University	Dan Delaurentis
U. Texas at San Antonio	Mo Jamshidi
Stevens Institute	Arthur Pyster

- Scope and Priorities for US-EU collaboration
- Strategic agenda for research collaboration
- Identify key enablers

Transatlantic Perspectives: Workshop Themes

1. **Architectures principles and models for autonomous safe and secure CPSs**
2. **System design, modelling and virtual engineering for CPSs**
3. Real time modelling for autonomous adaptive and cooperative CPSs
4. Model-Based Systems Engineering (MBSE) applied to computing platforms and energy management
5. Integration of socio/legal/governance models within modelling framework

Newcastle University

Transatlantic Perspectives: “Dream Projects”

- Federated EU/US testbeds
- Characterise and improve entry and use of CPS
- Combining Formal Verification and Simulation Technology
- Common foundation for security metrics
- Hybrid dynamic system verification
- Integration and interoperability models and approaches
- Characterize and Model Dynamic Human Interaction with CPS
- Case studies for autonomous transportation in EU/US cities

Newcastle University

Transatlantic Perspectives: “Test Cases”

Requirements for Test Cases identified

Examples:

- A Model-driven and Tool-integration Framework for Whole Vehicle Co-simulation Environments
- Model-Based System Patterns for Automated Ground Vehicles Platforms
- Optimal Control of Power Flows and Energy Local Networks of Microgrids Modeled as a SoS
- Hurricane Katrina Response
- Toyota Powertrain Benchmark
- Campus Smart Grid
- Artificial Pancreas
- Manufacturing and Systems Design

Newcastle University

Transatlantic Perspectives: interim recommendations

1. Establishing links to link testbeds or establish new collaborative testbeds
2. Investigate the potential and opportunities of co-ordinated calls for research in modelling & simulation with a US National Laboratory
3. Note need for close coordination to ensure consistent priorities, funding criteria, etc.

Newcastle University

Final Remarks

- IoT-enabled systems at the urban level exhibit SoS and CPS characteristics
- Engineering for dependability requires multi-stakeholder and multi-disciplinary approaches
- Potential of formal model-based techniques is being realised, but …
  - Wide scope of concepts, e.g., Resilience, Governance
  - Socialising the idea of CPS
  - A wider range of well-founded co-models (human, economic, …)
  - Focus on verification of emergence
- The Dependability community has a critical role to play in the public discourse – it is not easy, but we must do it!

Newcastle University

Adverts

- Formal Methods 2016 Symposium has a special call on CPS:
  - http://fm2016.cs.ucy.ac.cy/ (Papers due May 30th)

- SoS Engineering: join www.thecompassclub.org
- INTO-CPS: www.into-cps.au.dk
  - CPS Week Workshop, Vienna, Monday 11 April
- CPSE Labs (Funded Innovation Opportunities for EU businesses): www.cpse-labs.eu
- TAMS4CPS: www.tams4cps.eu
- Road2CPS: www.road2cps.eu

- INCOSE International Workshop, Los Angeles, Jan 30 – Feb 2:
  - www.incose.org/iw2016
  - Workshop on SoS Patterns for MBSE: Saturday, Jan 30, 1330-1730
  - SoS Research Roundtable: Sunday, Jan 31, 1330-1530
  - SoS Working Group Business: Monday, Feb 1, 1000-1200

Thanks

- Universities of: Twente, Aarhus, York, Pernambuco, Bremen, Loughborough, Linköping, KTH, Madrid (Poli)
- Controllab, Verhaert, Chess, Neopost, Bang & Olufsen, Insiel, PTC, Verified Software Intl, TWT, Clearsy, Softeam, Kongskilde, Agro Intelligence, United Technologies, fortiss, Offis, Steinbeis Europa-Zentrum, Laas-CNRS, ONERA, Indra

Newcastle University