Cyber-Physical Systems
and the
Right-Hand Side Problem
–
An informal talk

Michael Jackson
The Open University
jacksonma@acm.org

Brown University
WG2.3 Meeting
7-11 May 2018

Cyber-physical systems and the right-hand side problem

Cyber-physical systems ..

.. and the role of models in them

The right-hand side problem ..

and how it's a problem

Behaviour-focused development ..

.. of large and small structures

Concerns and the right-hand side ..

.. in the large, in the small

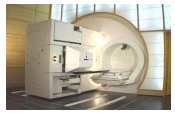
How behaviour focus helps RHS ..

.. and why it can interest WG2.3

Cyber-physical systems: the world and the machine

* ‘physical’ = non-formal world
* ‘cyber’ = governing behaviour

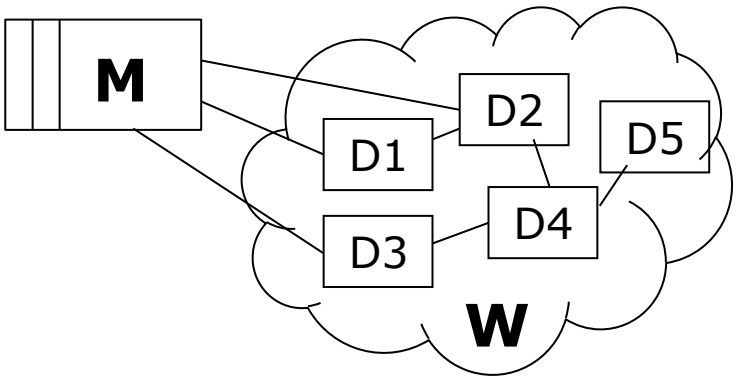
* Radiation Therapy, Flight Control, Railway Interlocking, Passenger Lift, Vending Machine, Industrial Press, Car Park, Automotive, ...








* For Software Engineering
  * The physical world **W** is given
    * Domains causally linked (–) ..
    * .. by shared phenomena
    * Human participants are domains
  * SE adds designed machine **M**
    * Causally linked to **W**
    * Governs **W**’s behaviour

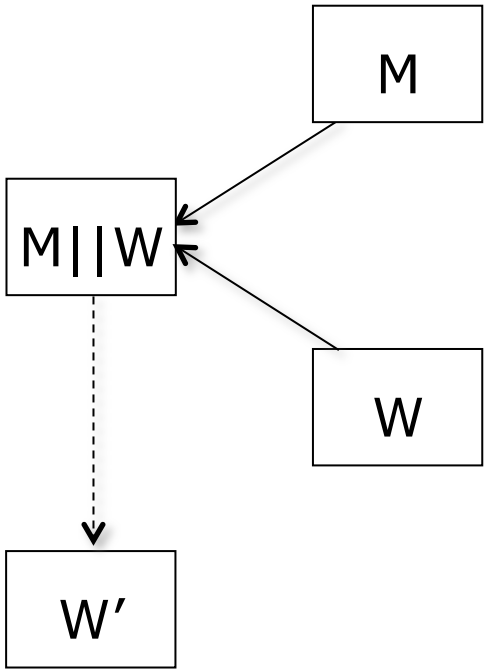


* This is Engineering BY Software
* Engineering OF Software is needed too

M, the given world W, and governed behaviour W’

M||W is the behaviour (B) of the system

W’ is the behaviour of W governed by M

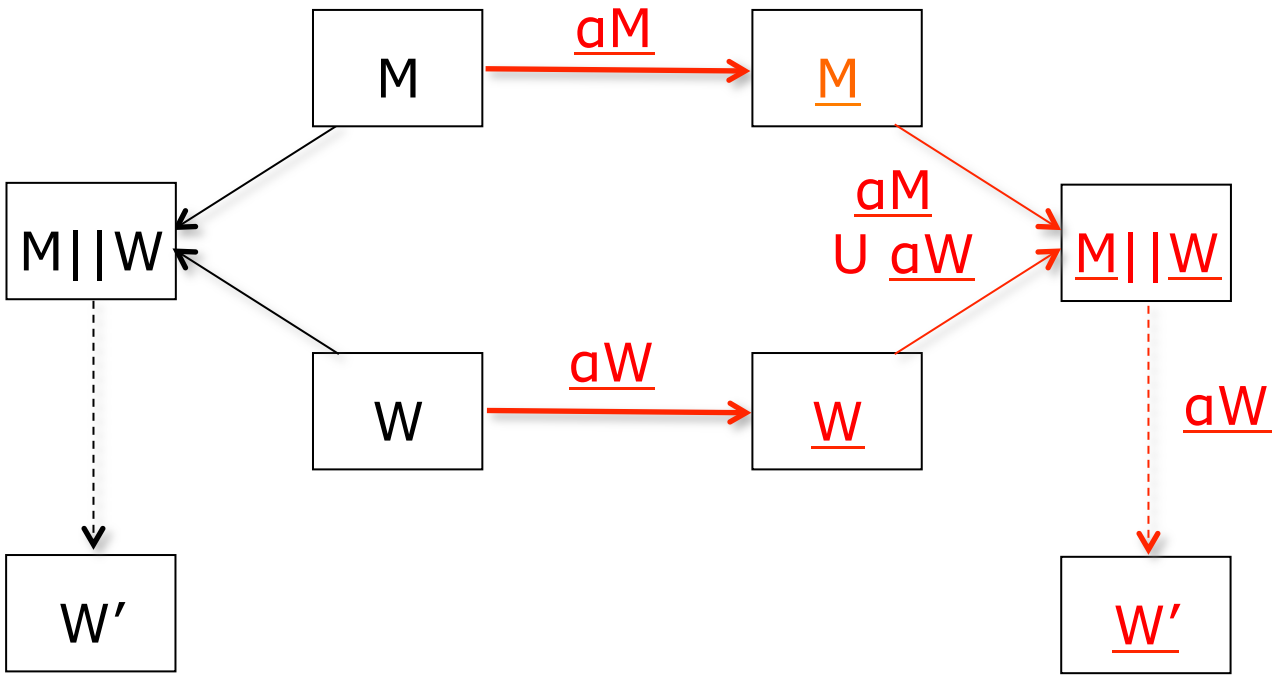


governed behaviour W’: what can happen in W constrained by M||W

Models of M, given world W, and governed behaviour W’

M||W is the behaviour (B) of the system

W’ is the behaviour of W governed by M



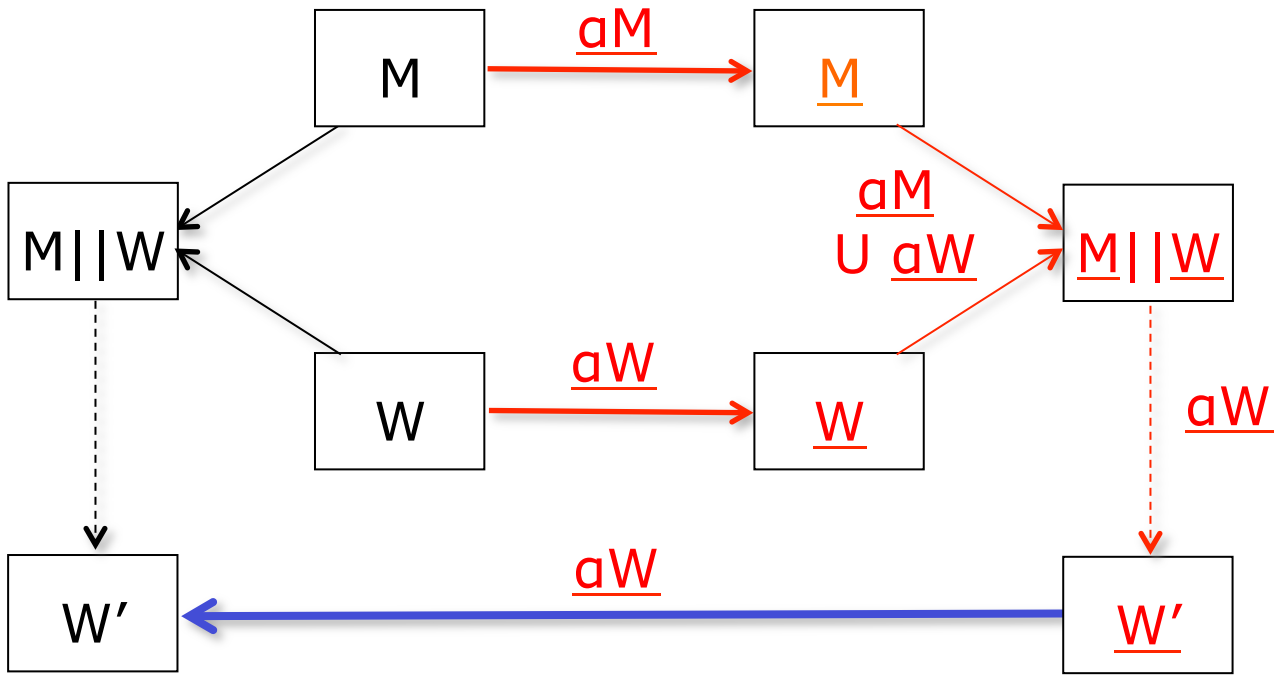
M||W is a closed model of M and W (interacting only with each other)

αM is alphabet of M, αW is alphabet of W (alphabets are the basis of interpretations)

The governed behaviour model W' and the reality W'

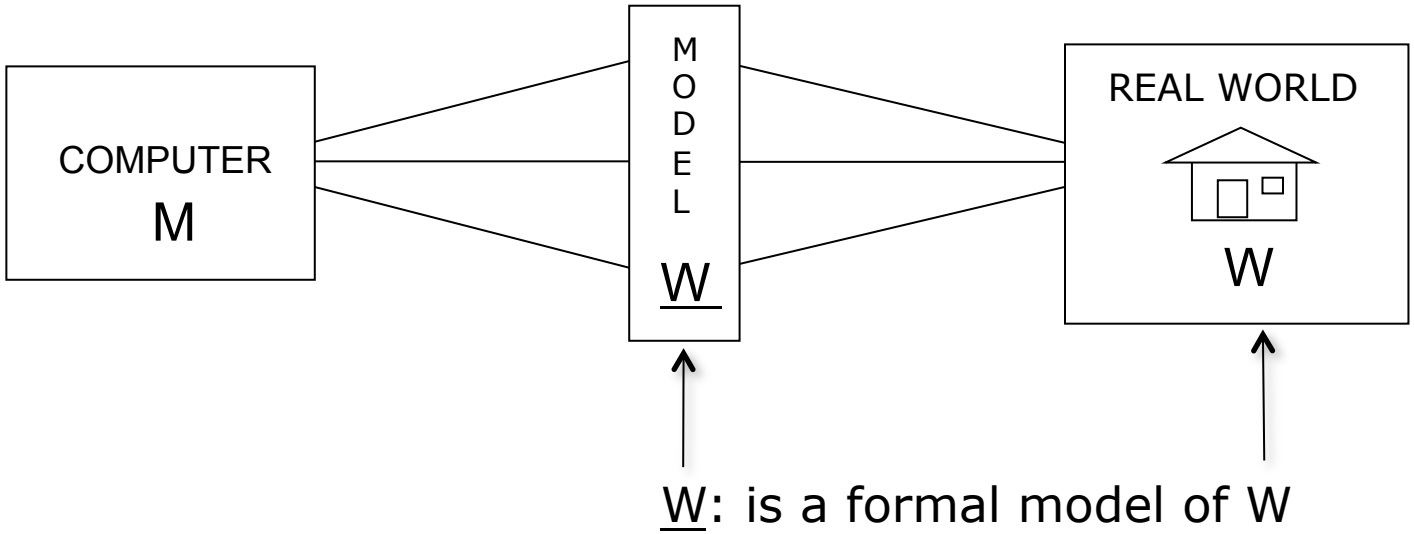
M||W is the behaviour (B) of the system

W' is the behaviour of W governed by M



W' should correctly predict W'
(ie have same traces wrt αW)

The Right-Hand Side problem (Cantwell Smith*)



Left-Hand Side is rarely problematic
(Relationship between M and W)

The Right-Hand Side is problematic
(Relationship between W and W)

* Brian Cantwell Smith:
The Limits of Correctness, 1985

How is the Right-Hand Side problematic?

The Real World	Formal Models
* No truly atomic phenomena	* Atomic ground terms
* TMI valve failure to close	
* Values are never exact	* Exact real values
* Proton therapy gantry creep	
* Relevance is unbounded	* Invulnerable properties
* BMEWS and BMW brake	
* Recursively contingent causality	* Support formal proof
* Comet 1 fuselage testing	

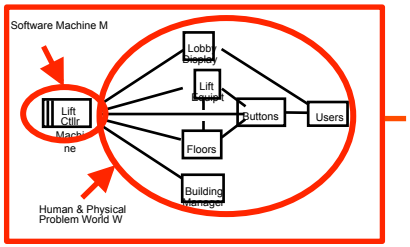
* Exaggeration! Some formal models do work quite well!

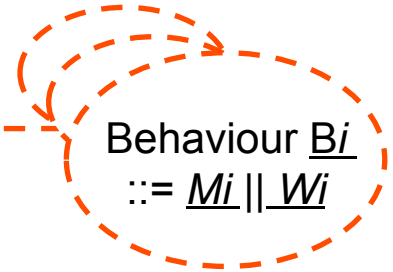
* Behaviour-based structuring mitigates the RHS problem

Behaviour-based structure (for RHS and other problems)

* Purpose of software is governing system behaviour
  * The behaviour itself is not a requirement
  * Requirements are effects, results etc of behaviours
* System behaviour combines constituent behaviours B*i*
  * Coherent and purposeful processes $\underline{B_i}$ ::= $\underline{W_i}$ || $\underline{M_i}$
  * Constituent behaviours satisfy simplicity criteria
  * Behaviour is governed by cause-and-effect links
* Dynamic tree of enactments: nodes M*i*; edges (M*i*,M*j*)
* Parent M*i* instantiates and controls M*j* execution
  * Execution of M*j* governs enactment of behaviour *Bj*
  * Standard protocols (as for procedure invocation) etc

System behaviour: combining constituent behaviours



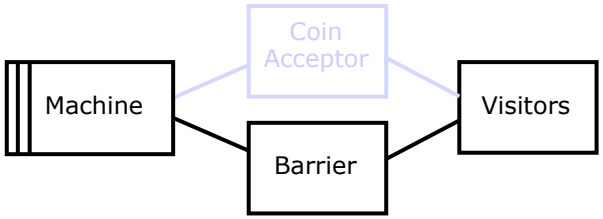


- Behaviour structure illustrated here by automotive features
  - Engine management is running: controlling mixture, throttle, etc
  - ABS is running: monitoring wheel speeds ready for braking
  - Stop-Start, Automatic Parking: no running instance now
  - Cruise Control is running: maintaining driver's chosen speed
  - Lane Departure Warning is running: watching lane markings
  - Speed Restriction is running: limiting speed to 110kph
  - Active Suspension is running: smoothing and stabilising ride
  - Air conditioning is running: cooling interior air
  - … …

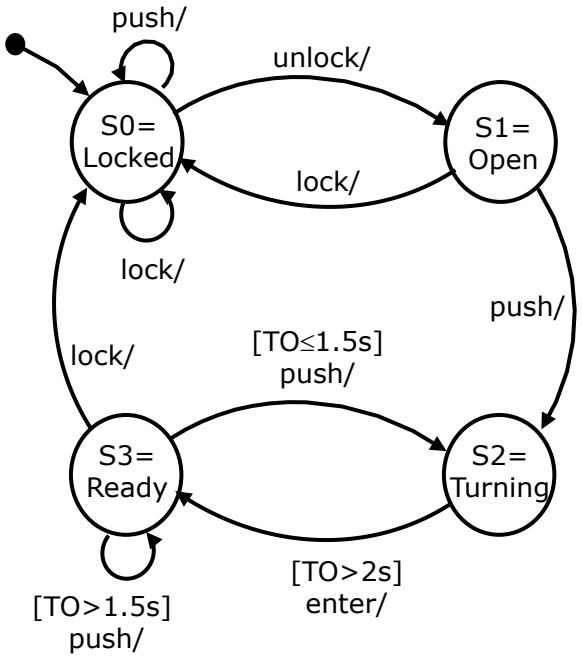
Developing behaviour-based structure

* Development order is chiefly bottom-up
  * Useful high-level abstractions are few (or absent) in CPS
  * Combination demands prior understanding of components
    * Combination may be invasive (W has no compositionality)
* Constituent behaviours are initially developed in isolation
  * Separating intrinsic from combinational complexity
  * Combination is a distinct design activity
* Checklists of concerns avoid known potential failures
  * cf programming concerns (null-deref, store leak, o'flow, etc)
  * Simple concerns, combination concerns ..
    * .. overlapped and extended by modelling concerns

Simple concerns: initialisation, breakage, totality



M! {lock, unlock}
V! {push, enter}



* Initialisation concern:
  * When M*i* execution starts, what is the state of W*i*?

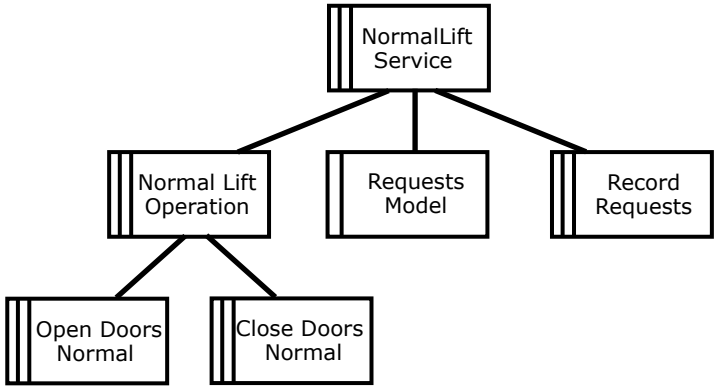
* Breakage concern:
  * Domain vulnerability to every alphabet event?

* Totality concern:
  * Possible effect of every alphabet event in every alphabet state?

Combination concerns: conflict, mutex, switching

* Conflict concern:
  * Conflicting demands on W state from B*i*, B*j*

* Mutual exclusion concern:
  * Simultaneous demands to ‘read’/’write’ W by B*i*, B*j*



* Switching concern:
  * Match W terminal state of B*i* to initial state for B*j*

Modelling concerns: granularity, creep, frame cond'n

event *pass*
g1: person *p* in room *r*
g2: *p* authorised for *s*
a1: *p* in *s*

* Granularity concern:
  * Atomic alphabet designations
  * Unicontrol abstraction

* Creep concern:
  * Iterated "set position to P; P:=position" for real position, floating-point P

W: *"move!" ==> accel ==> ↑torque*
M: *↑torque ==> "move!"*
==> release-brake

* Frame condition concern:
  * Dual completeness at each node in cause/effect graph

How behaviour focus helps RHS

* Directly addresses ‘how it works’ and ‘does it work?’
  * System success and failure are causal success and failure
* Behaviours support effective localisation of concerns
  * Components are small, simple, closed, comprehensible
* W*i* and M*i* are developed hand-in-hand (as they must be)
  * W’*i* makes no sense without M*i* (and *vice versa*)
* Alphabet designations compel conscious granularity choices
  * Explicitly designated phenomena, causal relations, domains
* W*i* is a minimal ‘axiomatic’ model, primarily causal
  * Requirements satisfaction shown by ‘theorems’ in W*i*
  * Enactment tree and W*i* provide maps to explore reliability

Why it can be interesting to WG2.3

* The behaviour approach is a work in progress
  * The work presented is ‘pre-formal’
  * ‘Pre-formal’ work must be followed by formal work
* Formal language is needed for causal models
  * Can temporal logics be enough?
  * A discipline of ‘operational principles’?
* Enactment tree still very roughly sketched
  * Parent-child control protocols invite study
  * Relationship between W*i* and M*i* in enactment tree
* A meeting place for practitioners and researchers?
  * A long-standing need?

Thank you