Cyber-Physical Programming

Challenge and Response

Michael Jackson
The Open University
jacksonma@acm.org
## Cyber-Physical Programming

<table>
<thead>
<tr>
<th>1</th>
<th>CP System Examples</th>
<th>6</th>
<th>Causal Failures</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>Behaviour Structure</td>
<td>7</td>
<td>Axioms &amp; Behaviours</td>
</tr>
<tr>
<td>3</td>
<td>The Bipartite System</td>
<td>8</td>
<td>Triplets</td>
</tr>
<tr>
<td>4</td>
<td>Programmability</td>
<td>9</td>
<td>Model Structure</td>
</tr>
<tr>
<td>5</td>
<td>Causality</td>
<td>10</td>
<td>Envoi</td>
</tr>
</tbody>
</table>
1 CP System Examples

Radiotherapy  Flight Control  Automotive  Drug Pump  Floor Cleaner  Vending

Cyber = steer or govern
(specifically: real world BEHAVIOUR)

Physical = CONCRETE tangible world
(mechatronic, natural, built, people, etc etc)

Many dimensions of variety
(COMPLEXITY, phenomena, size, locality, CRITICALITY, ..)
2 Behaviour Structure

* Many CP systems have complex behaviour

Self-park, limit speed, cruise control, anti-skid braking, air conditioning, clean charcoal filter, custom driver options, emission test, software update, fuel management, active suspension, ignition cycle, stop-start ...

* **CONSTITUENT** behaviours: **CONCURRENT**, terminating or not
  * **INTERACTING** both in software and in the physical world (parts of the physical world act as shared variables)
  * Mutual incompatibilities (eg aircon and stop-start)
  * System behaviour involves much more than the car itself (driver, road, weather, visibility, other road users, ... )
3 The Bipartite System

* The system to program has 2 parts: **MACHINE** M + **WORLD** W

- Domains are **ENTITIES** participating in **PHYSICAL BEHAVIOUR**
  - M, W share phenomena at interface domains
    - (M: only ■ shown; W: □, ■ include human participants)
  - □, ■ = physical **DOMAIN**    ■ = INTERFACE    — = **SHARED PHENOMENA**

* An inescapable (formerly manual) refinement task

M/C CODE FOR M

Program for M||W

Physical behaviour enacted in W
4 Programmability

* **M** is **FULLY PROGRAMMABLE**
  * Store and traverse a graph of m/c instructions
  * Specified instruction effects (‘add’, ‘jump’, …) are **AXIOMS**
  * Instruction execution is **RELIABLE** (though imperfectly)

* **W** is only **PARTLY PROGRAMMABLE**
  * Exernal programs only: W has no store and traverse
  * “Instructions” are shared phenomena at interface
    * The world is not formal: “axioms” are **CONTINGENT**
  * W’s interface and other domains are **UNRELIABLE**
5 Causality

* How can M govern W beyond the interface domains?
  * W “axioms” are **CAUSAL LINKS** in/between domains
  * Causes and effects are events, states, ...
  * Links can form chains

* Each causal link has an **EFFECTUATING DOMAIN** D in Wi ..
  .. specifies conditions (eg current state of D)
* Cause --> effect may be M --> W or W --> M
  * ‘Activator’ and ‘Sensor’ are relative terms
* Causality **SEMANTICS** may be intricate (**INHIBITION** etc)
  * Causality is the logic of **CONTRIVANCES** [Polanyi]
6 Causal Failures

* Some historic failures of causality modelling

- Reverse thrust only if plane is on ground
- Flooded runway: no wheel rotation caused
- ‘Rolling’ landing: only one leg compressed

* Causal link from relief valve to indicator .. .. was not imputed to any identified domain

* Relief valve stuck open but indicated closed

* 1960: USSR missile strike launch indicated

* Radar link: cause should be strike launch .. .. but was unexpected position of rising moon
7 Axioms & Behaviours

* Why AXIOMS? Judiciously chosen UNQUESTIONED ASSUMPTIONS
  * An allusion to Euclid’s axioms..
    .. defining the basis for constructions
* Why are axioms CAUSAL LINKS?
  * Because a CPS is a CONTRIVANCE
    * Is ‘the LOGIC of CONTRIVING’ [Polanyi] causality?
* Surely the laws of physics are the necessary axioms?
    * Scales; shapes; discrete properties; juxtapositions
8 Triplets

* W axioms support development of system **BEHAVIOUR**
  * Model (axioms) must be **GLOBAL** wrt behaviour activations

* **TRIPLET**: microcosmic CP system, one constituent behaviour
  * Triplet \(i = \{Mi \text{ program, } Wi \text{ model, } Bi \text{ behaviour } Mi||Wi\}\)
  * Bi combines contributions from both Mi and Wi
  * Wi model: axioms required to support Bi activation

* **DEVELOP** a triplet and **COMBINE** with others
  * Triplet activations are linked by their program texts
  * Combining is a separate (possibly invasive) task
9 Model Structure

* **MODELLING-IN-THE-LARGE**: structured wrt BEHAVIOURS
  * Wi model must hold during enactment of behaviour Bi ..
    .. so model structure is behaviour enactment structure
* **MODELLING-IN-THE-SMALL**: A, B, C are distinct aspects
  * AXIOMS for Wi are causal links in and between Wi domains
  * BEHAVIOUR Bi = Mi||Wi (eg state machine, trace set, ...)
  * CONSEQUENCES of Bi (satisfying relevant requirements)
* Modelling as a discipline
  * Rigorous DENOTATIONS in the physical world
  * Corpus of identified MODEL FAILURE CONCERNS
10 Envoi

* Reliable programming of an unreliable world
  * **Co-design** Mi program and Wi model
    * Both content and structure
  * A **Computing Science** perspective
    * **Formal specification** for M is **impossible** ..
      .. because W does not support reliable abstraction

* Are CPS development **Challenges** relevant for CS?
* Where is CS most relevant to CPS development?
Thank you