Requirements

Are Properties

of System Behaviours

Michael Jackson
The Open University
jacksonma@acm.org

UCL CREST Workshop
11-12 February 2013

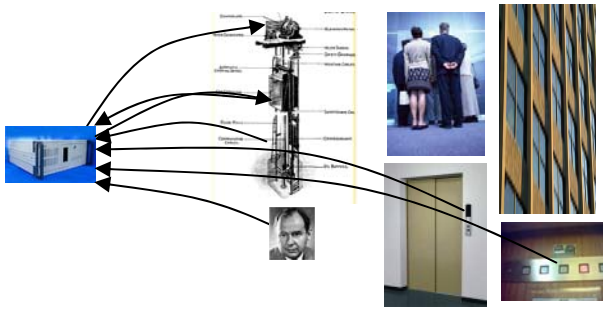
A view of requirements for cyber-physical systems (and some others)

Cyber-physical systems

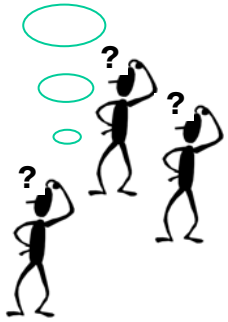
- A computer monitors and controls parts of the human and material world
- For example:
  - Control a radiation therapy machine
  - Control passenger lifts in a building
  - Control the Rotterdam storm barrier
  - Control vehicle speed on a highway
  - Control operation of an industrial press
  - Control road traffic at a complex junction

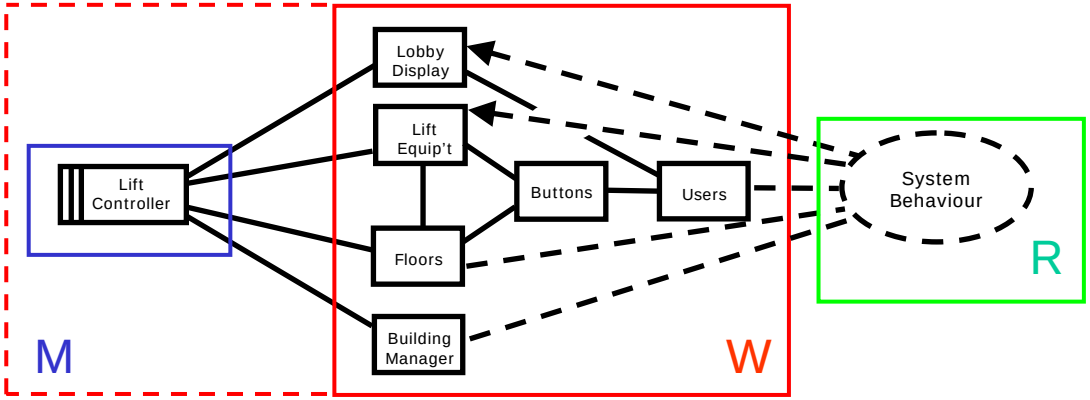
Here's the proposed view in one slide

Controlling lifts in a building



Does the system behaviour satisfy our requirements?





- Machine M controlling problem world W
  - System = {M, W} (W includes users &c)
- Formally: M,W |= R
  - M installed in W evokes behaviour R

The development task

- Design a feasible behaviour R …
- … satisfying stakeholder requirements

There are many stakeholders and they have diverse requirements

System Complies with All Safety Regulations!

Lift Is Easy to Use!

Lift Comes when I Request and Goes to the Floor I Want!

Special Mode for Operation by Firefighters!

Service I can Define to Meet the Varying Usage Demands!

Graceful Service Degradation on Minor Failures!

No Lower Classes Allowed on the Tycoon Floor!

Don’t Wear Out the Equipment by Misuse!

Helpful Operational Procedures for Monthly Maintenance!

Efficiency Means Fewer Lifts, More Rentable Space!

System behaviour is

loosely decomposed

to simple projections

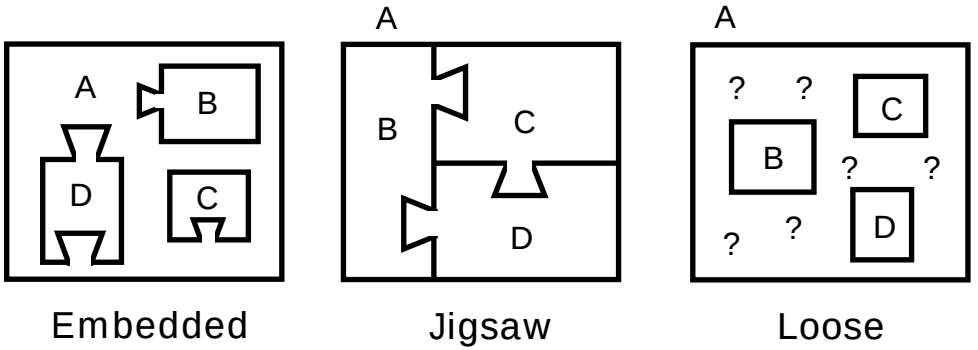
of machine effects

('governed behaviours')

Loose decomposition

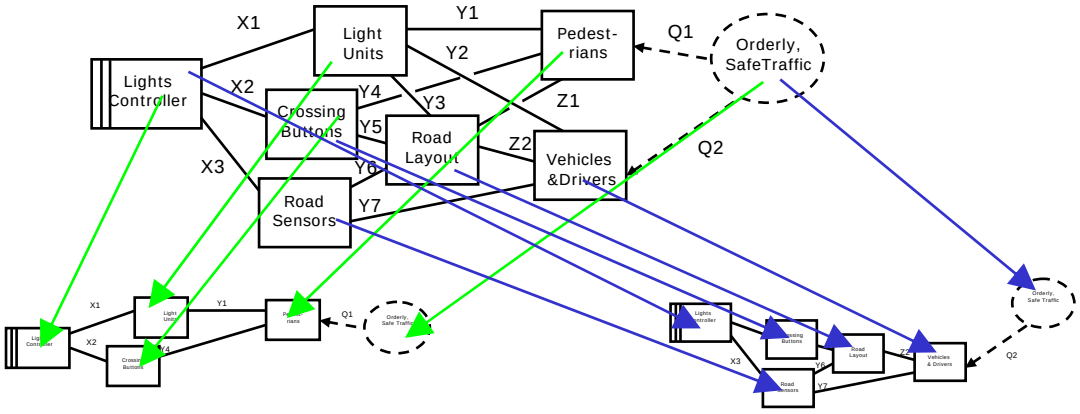
Interactions are ignored
- Closed ‘subproblems’

Interaction may be complex
- Recombining a later task



Simple behaviour projections

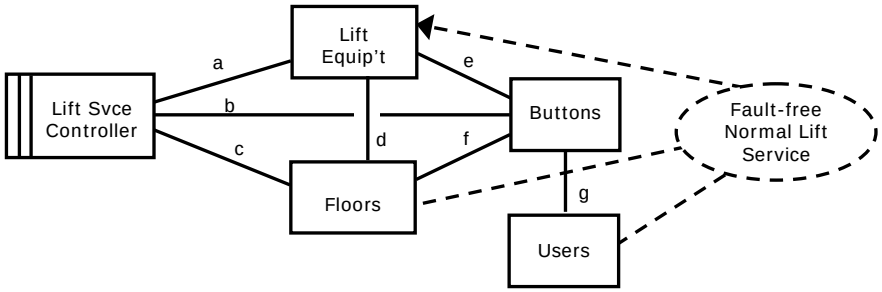
‘Governed behaviours’
- System behaviour projected by time, problem domains, functions, conditions, …

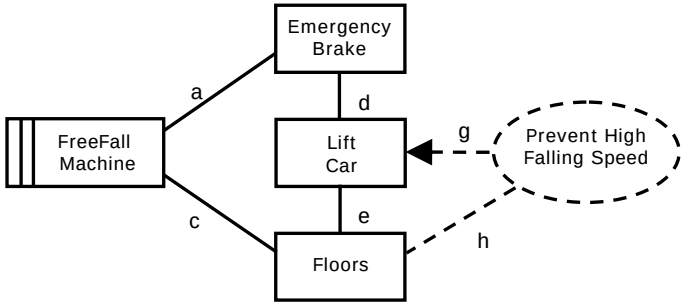


Here are some
candidate examples
of governed
behaviours
of the lift system

Some candidate governed behaviours

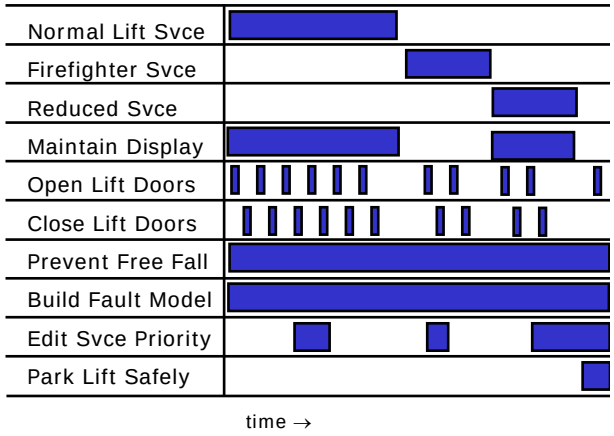
- Fault-free normal lift service
- Firefighter lift service
- Test mode behaviour
- Maintenance mode
- Failure-reduced service
- Maintain lobby display
- Door open and close
- Overloaded travel prevention (?)
- Fault detection and diagnosis
- Free fall prevention
- Editing priority scheme
- Managing priority schemes
- Safe lift parking
- Tycoon floor security (?)
- … ??



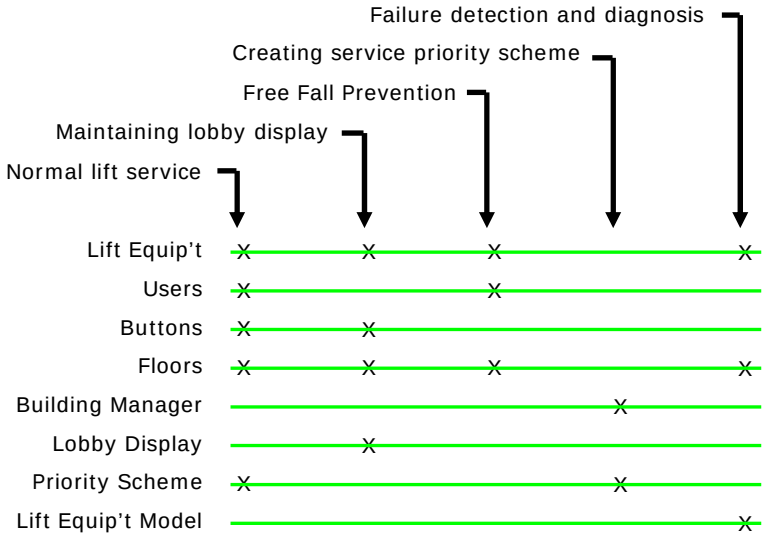


Loosely decomposed
behaviours must
be designed,
scheduled
and reconciled

Scheduling and reconciling behaviours



- Specifying behaviour time-span relationships
  - Overlapping, disjoint, consecutive, nested, ...
- Scheduling behaviours
  - Begin, end, conditional
  - Running & Halted states



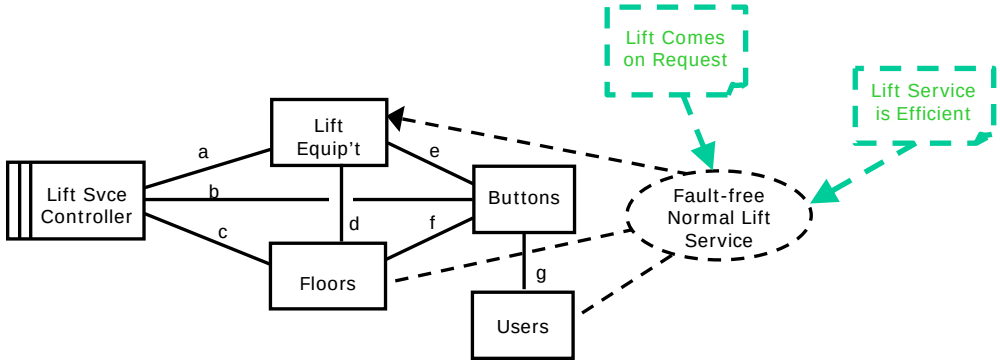
- Reconciling behaviour interactions
  - Behaviours interact at common problem domains
- cf telecoms feature-interaction problems

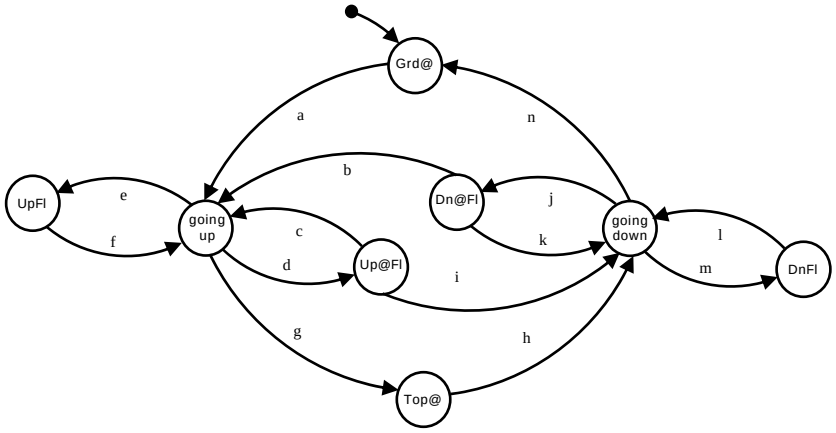
Stakeholder requirements are properties of the relevant behaviours

A governed behaviour and its requirements — 1

Normal lift service

- Requirements
  - Lift Comes on Request
  - Lift Service is Efficient
  - …





Behaviour design

- Which transitions?
- When?

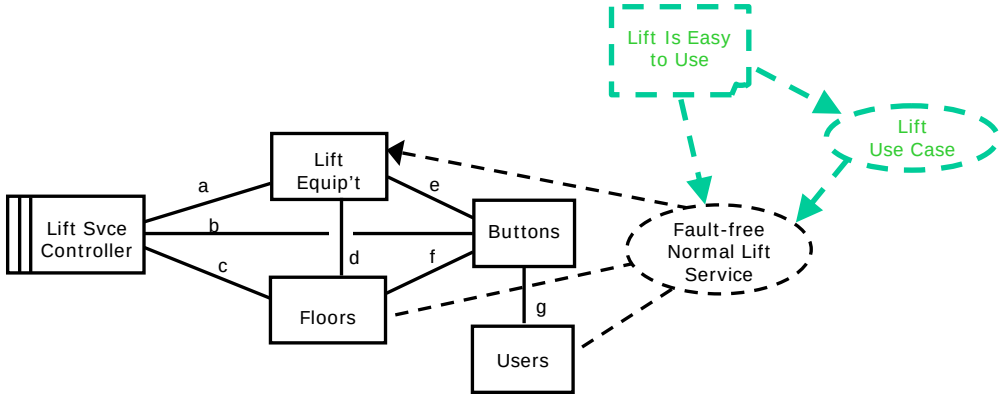
Request states

- Pending, ignored, …

A governed behaviour and its requirements — 2

Normal lift service

- Requirements
  - Lift Is Easy to Use (eg Lift Use Case)
  - …



---

1 Press UP hall button on floor f
2 (Lift arrives full or going DOWN)*
3 Lift arrives not full and going UP
4 Enter lift car
5 (Lift stops at intermediate floor f<h<g)*
6 Press car button for destination g>f
7 (Lift stops at intermediate floor f<h<g)*
8 Lift stops at destination floor g
9 Exit from lift car

This is an 'afforded' behaviour

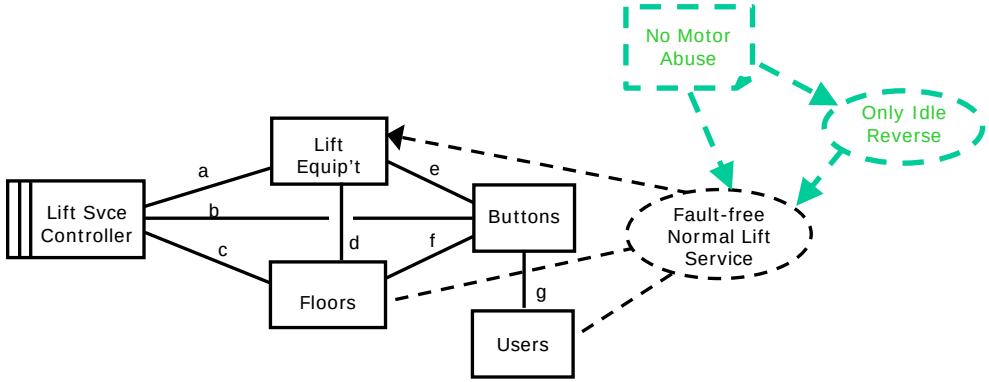
Use-case approved as 'Easy to Use' by stakeholder

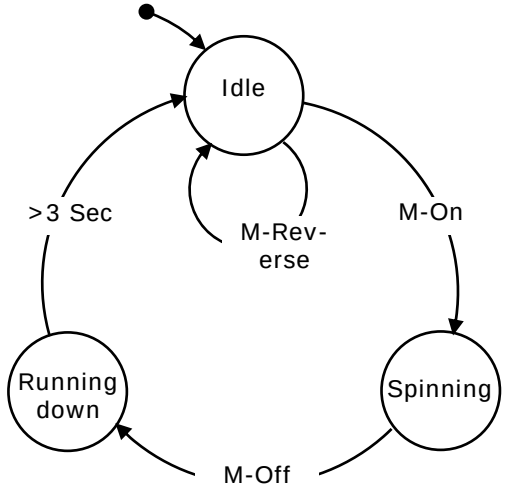
- More detail needed
  - Button deadline?
  - Rescind button press?
  - Failed behaviours?

A governed behaviour and its requirements — 3

Normal lift service

- Requirements
  - No Motor Abuse
    (eg Only Idle Reverse)
  - …





This is a required 'motor use-case'

Approved by equipment engineers as satisfying 'No Motor Abuse'

- No motor reverse unless idle

This requirement constrains many governed behaviours

- eg: Park at ground floor
- eg: Switch to firefighter lift service

Most requirements
are local to
(sets of)
current behaviours

Local requirements: no global invariants

Examples from three systems

- Access control system
  - “In_Room (p,r)” => “Authorised(p,r)”
    - Forbidden by fire regulations!

- Train control system
  - “Never 2 trains in one segment”
    - Assembling a train? Crash rescue?

- Lift control system
  - “Door_Open => Car_At_Floor”
    - Firefighter mode? Maintenance mode?
  - “Car_Stopped => Car_At_Floor”
    - Free-fall prevention on broken cable?

A final summary

A summary

1. System behaviour is complex ..
   .. embodying governed behaviours
2. Behaviours satisfy requirements ..
   .. which are properties of behaviours
3. Most requirements are local ..
   .. to specific governed behaviours
4. The vital requirements context ..
   .. is behaviour design and structure

Thank you