The Right-Hand Side Problem:
Research Topics in
Requirements Engineering

Michael Jackson
The Open University
jacksonma@acm.org

RE Silver Jubilee
RE 2017, Lisbon
6th September 2017

Two ways of failing

Software-intensive systems can fail
in two fundamentally different ways

Program Bugs

Program execution
is not as intended
by the programmer

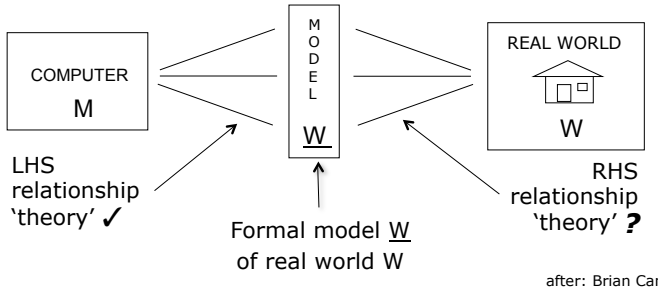
Wrong World
Assumptions

Intended program
execution doesn't
produce the right
real world effects

The Right-Hand Side problem

* What is "The RHS problem"?
* Why does it matter?
* What should be done?

What is the Right-Hand Side problem?

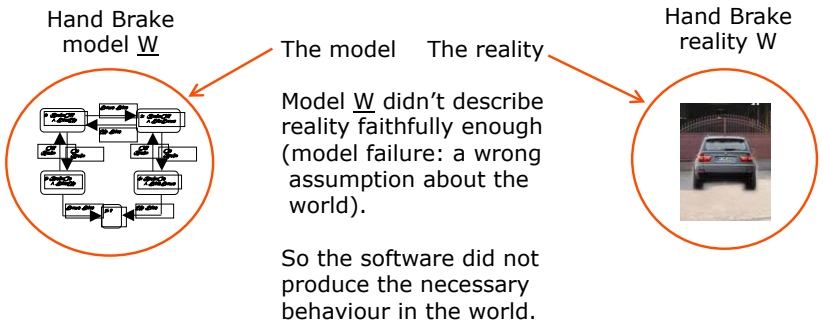


after: Brian Cantwell Smith;
The Limits of Correctness.

* W may be tacit or documented explicitly
  * The expected real world behaviour is M || W
  * The actual real world behaviour will be M || W

Why the RHS problem matters: an example

* BMW Press-Button Handbrake: a well-known failure (of a prototype)



Model W didn't describe reality faithfully enough (model failure: a wrong assumption about the world).

So the software did not produce the necessary behaviour in the world.

What was the RHS modelling failure?

* BMW Press-Button Handbrake: a well-known failure (of a prototype)

* Model W concepts for automatic release of the handbrake

"move!" ----> accel ----> ↑torque [axioms of the handbrake model]

↑torque => "driver wants to move" [a derived model: (no other cause)]

What was the RHS modelling failure?

* BMW Press-Button Handbrake: a well-known failure (of a prototype)

* Model W concepts for automatic release of the handbrake

"move!" ----> accel ----> ↑torque [axioms of the handbrake model]

↑torque => "driver wants to move" [a derived model: (no other cause)]

* Sometimes it worked properly, but sometimes it didn't

What was the RHS modelling failure?

* BMW Press-Button Handbrake: a well-known failure (of a prototype)

* Model W concepts for automatic release of the handbrake

"move!" ----> accel ----> ↑torque [axioms of the handbrake model]

↑torque => "driver wants to move" [a derived model: (no other cause)]

* Model W concepts for automatic control of the air-con system

↑heat ----> ↑A/C ----> ↑torque [axioms of the air-con model]

What was the RHS modelling failure?

* BMW Press-Button Handbrake: a well-known failure (of a prototype)

* Model basis for automatic release of the handbrake

"move!" ----> accel ----> ↑torque [axioms of the handbrake model]

↑torque => "driver wants to move" [a derived model: (no other cause)]

* Model basis for automatic control of the air conditioning system

↑heat ----> ↑A/C ----> ↑torque [axioms of the A/C model]

* Active air-con feature invalidates the derived model of handbrake!
  * This is an error: not in programming, but in real-world modelling

The RHS problem: What should be done?

1 Failures are easy to diagnose (even to repair!) after the event
  * Should have considered interference of features in combination
  * Should monitor driver controls, not Engine Management System

2 We need to develop sounder modelling discipline
  * To avoid and diagnose defects before the event
    (cf Structured Programming, Model Checking, Spark Ada, ...)

3 For questions and discussion
  * What would be elements of a sound discipline?
  * What are the challenges?
  * Possible research approaches?

Donald Mackenzie on fatal system failures

The Right-Hand Side problem is ubiquitous but poorly recognised in Requirements and Software Engineering

Program Bugs

Responsibility for fatal accidents:

Wrong World Assumptions

Responsibility for fatal accidents:

Donald Mackenzie on fatal system failures

The Right-Hand Side problem is ubiquitous but poorly recognised in Requirements and Software Engineering

It needs focused and imaginative research by good people–you!

Program Bugs

Responsibility for fatal accidents:

~4%

Wrong World Assumptions*

Responsibility for fatal accidents:

~92%

* incl. 'human error'

Thank you