

## Back to the Future:

### Modern Computing in Railway History

How is a railway like a computer?

if all trains ran according to schedule and never broke down,  
there would be little need for a signalling system  
[BR Railway Signalling HB]

cf functional programming, formal specification  
where the behaviour can be successfully circumscribed, don't  
need to consider interaction between agents

cf C A R Hoare in Concurrent Sequential Processes

" ... no need to distinguish between events initiated by  
the object and those initiated by some agent outside  
the object ... avoidance of causality leads to  
simplification"

today, full automation if quite feasible

1

Understanding of a fully automated railway derives  
from state-based views

not black box, but make explicit stimulus-response patterns that  
are encapsulated in electronic components

cf model railway: synchronisation of signal and train is contrived.

Understand wrt to now obsolete mechanical signalling processes

Basic concepts

Signalling protocols: distant, home and starting signal

Blocks: absolute blocking, permissive working

Track circuits

Division of responsibility

+ transfer of control between signal boxes

Communication between station-supervisor and signal box

3

How has this come about?

railway history as a process of circumscription

circumscription, closed world

foolproof? – against foreseeable perturbation of the system

[Consider some examples of events protected against]

What are the dangers that remain?

To what extent is there still discretion for agents?

Trend towards fail-safe:

**safety** guarantees if not fairness and liveness

Key to automation

possibility of stimulus-response mechanisms

to detect & correct (or at any rate neutralise)

signalling of its nature is communication = stimulus/response

2

What purposes do these serve? Consider consequences of

ignoring signalling protocols

relaxing blocking restrictions

dispensing with track circuits

liberalising the communication regime

Role of agents complementary:

responsible driver slows down at distant

proceeds cautiously in permissive working

responsible signalman clears signals in particular sequence

follows the communication protocols faithfully

Other factors concerned with synchronisation of activity

interlocking of every point and signal is a free agent

continuous braking of every carriage can move independently

forms of prohibition: denial of privileges

signalman **can't** set the points against the signal

driver **can't** cross a stop signal: Automatic Train Control

synchronisation points in protocol

means of interrogation for confirmation

check the route is set-up

4

## One Day in Severn video

What perceptions and privileges do the agents have?  
signalmen, drivers, stationmaster  
track circuits, signals, points, trains

What training do the agents require?  
What specialised ability to interpret perceptions?

[knowledge = interpreted perception (?)]

How do these activities synchronise:  
what examples are there of definitive relationships?

what LSD guards apply to signalman privileges?  
enabling condition for all clear signal to driver

What perceptions / knowledge are in the world  
vs what's significant to model

what's **not** in the signalman's view of the railway operation

what's indirectly under the signalmen's control

How could agents influence fairness, safety and liveness?

human agents – through incompetence or conspiracy  
mechanical components, through failure

How could environmental factors impede the operation?

Propriety and efficiency vs safety

what are the goals of the railway operation?  
how fast could protocols achieve the goals?  
how would safety be compromised?  
what are the limitations on the speed of operation?

5

## General Theme

Initially, railway pioneers didn't know  
what should / shouldn't be considered relevant to safety,  
what could be changed

e.g. impact of telegraph technology, standard time

## Insensitive to issues of perception

"A Signal Ball will be seen at the entrance to Reading Station  
when the Line is right for the Train to go in. If the ball is not  
visible the Train must not pass it."  
Regulations, Daniel Gooch, March 1840

cf positive danger, but no positive all-clear

## Division of responsibility between human agents

Autonomous travel

Brunel and Babbage meet on Bristol-Paddington line

private carriages for gentry

travel on the roof (cf stage coach), leap off to retrieve hat

Scottish Central Highway regulation

Guards and brakemen are responsible that the proper signals are  
made in fogs and in all accidents and detentions on the road  
according to regulations; but if in these cases a difference of  
opinion should arise as to what is the proper course to pursue the  
engine-man to decide.

*criticised in an inquiry involving rear collision with a train that was  
35 coaches and several sheep trucks long. Time interval strategy  
and lengths of trains related.*

7

## Summary

move towards automated railway operation through

rationalising the perceptions of agents  
formalising their protocols  
restricting their privileges

subject to assumptions about reliability of operating environment

Must also delineate relevant knowledge for agents: training them  
to interpret perceptions according to established conventions

*PS who'd like 7 Day in Severn video?*

6

## Measures towards rationalisation

Enhance oracles

chain of switching men at signalling points      early days  
communicate by flags and lamps  
whistles / bells / hooters

telegraph and intercom      later

Restrict privileges

lock passengers into train      early days  
regulate access to trains  
restrict authority / define duties of railway personnel:  
up and down line convention  
despatch note starting time, place & time of returning

more sophisticated protocols      later  
more limited discretion

Formalise regulations and protocols

e.g. single line working  
by telegraph and crossing order  
by staff  
by staff and ticket  
by Tyler tablet block instrument

Regularise the environment

police the tracks      early days  
restrict access to tracks  
impose railway time

signalling      later  
interlocking  
fail-safe brakes

8

## Technological aspects

*block* telegraph between major stations (1850s)  
*brake* vacuum brakes for trials in 1875

pre-1889	post-1889	
independently controlled points	interlocking	<i>lock</i>
time interval system	blocking	<i>block</i>
manual brakes	continuous braking	<i>brake</i>

cf blocks control signals, signals can apply brakes

... My board fear that the telegraphic system of working recommended by the Board of Trade will, by transferring much responsibility from the engine drivers, augment rather than diminish the risk of accident.

John Chester Craven, for London, Brighton & South Coast Railway, 1861  
after the report on the Clayton Tunnel accident

Suspicion of interlocking:  
"removes the human agent's discretion to act in emergency"

## Summary

..... as we look back in railway history, we see a mirror image of the the issues that arise in modern reactive systems specification.

raw agent interaction has to be disciplined: concerned with how far analysis through LSD can assist in understanding how this should be done.

