The *Railway Disaster* Exercises

The idea is to analyse the events leading up to historic railway disasters with the principles of LSD specification in mind. This analysis will illustrate the subtlety of the relationship between perceptions and privileges of agents and their corporate behaviour.

Note that it isn't difficult to write a program to simulate any of these accidents in a superficial sense ... what would be very difficult (if even possible) in general would be to simulate them in such a way that we could interrogate the simulation for info about the perception of the agents at an intermediate stage.

The basic idea of observations of agents, perceptions and actions are clear. We've seen how definitions can express *interpretation of observation* (cf the guard) that can be deemed "knowledge".

These examples illustrate practical difficulties that beset LSD specification in general interaction between agents (i.e. agent-oriented analysis).

Issues include:

How oracles, handles and privileges of agents are influenced by

locality - how are the agents distributed
roles - the same agent may play different roles
authority - one agent may delegate to another
knowledge
- motivations for action, cultural context, acquired experience, skills

How the effect of actions is influenced by

commitment - when is an agent required to act, pledged to act
conflict - two agents can act at cross purposes
synchronisation - when must actions occur at the same time
environment
- how do environmental factors influence outcome of actions
modes of communication - e.g. intermittent vs persistent

What can be modelled in LSD?

There's a spectrum from routine programming as interaction between reliable agents to very complex subjective human interaction in which emotion, judgement and intelligence etc play a part. Where does LSD fit into this? where is it inappropriate? are there criteria for its application to particular situations?

What can we identify as making safe automatic train control possible?

Consider for instance

making communication concrete through some physical ritual

using automatic equipment to advise the human agent

using automatic equipment to coerce the human agent

The place of **safety** and **liveness**. [Informally, safety guarantees that, provided protocols are followed, whatever happens isn't dangerous, and liveness guarantees that progress can be made towards a goal.]

One motivation for these exercise is that – presumably – activity that we can formulate more effectively in LSD will also be easier to automate.

Reference

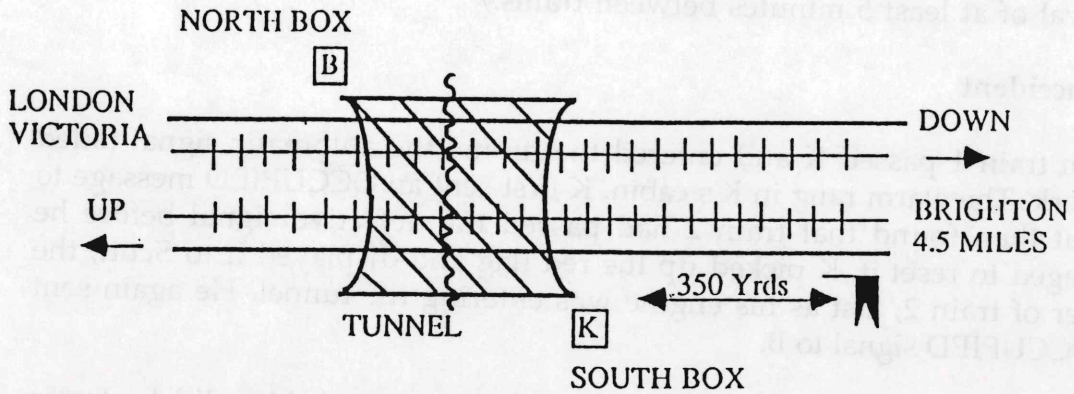
L.T.C. Rolt *Red for Danger*, The Bodley Head Press 1955

Historic Railway Accidents 1

Clayton Tunnel **August 25th 1861**

Three heavy trains leave Brighton for London Victoria on a fine Sunday morning, travelling on the London, Brighton and South Coast railway. The time interval system is applied along the track, except for the Clayton Tunnel – the first railway tunnel to be protected by a telegraph protocol designed to prevent two trains being in the tunnel at the same time

The layout at the Clayton Tunnel is as in this figure:



There is a signal box at each end of the tunnel. The North Box is operated by Brown and the South by Killick. K has been working for 24 hours continuously. In his cabin, he has

a clock
an alarm bell
a single needle telegraph

and a handwheel with which to operate a signal 350 yards down the line. He also has red (stop) and white (go) flags for use in emergency.

The telegraph has a dial with three indications thus:

NEUTRAL

OCCUPIED CLEAR

When K sends a train into the tunnel, he sends an OCCUPIED signal to B. Before he sends another train, he sends an IS LINE CLEAR? request to B, to which B can respond CLEAR when the next train has emerged from the North end of the tunnel. The dial at K's end only displays OCCUPIED or CLEAR when the appropriate key is being pressed by B – it otherwise displays NEUTRAL.

The distant signal is designed to operate automatically so that it returns to danger as a train passes it, but if this automatic mechanism fails, it rings

the alarm in K's cabin. This signal is to be interpreted by a train driver either as *all clear* or as *proceed with caution*.

The three trains leave Brighton according to the following schedule:

		Times of departure		
Train (from)	Size	As advertised	Stationmaster	**Actual**
1 PORTSMOUTH	16	8.5	8.22	**8.28**
2 BRIGHTON EX	17	8.15	8.27	**8.31**
3 BRIGHTON ORD	12	8.30	8.36	**8.35**

where the actual times of departure, as established at the inquiry, differ from those alleged by the stationmaster. (Officially there must be a time interval of at least 5 minutes between trains.)

The accident

When train 1 passed K and entered the tunnel the automatic signal failed to work. The alarm rang in K's cabin. K first sent an OCCUPIED message to B, but then found that train 2 had passed the defective signal before he managed to reset it. K picked up the red flag and displayed it to Scott, the driver of train 2, just as his engine was entering the tunnel. He again sent an OCCUPIED signal to B.

K didn't know whether train 1 was still in the tunnel. Nor did he know whether S had seen his red flag. He sent an IS LINE CLEAR signal to B. At that moment, B saw train 1 emerge from the tunnel, and responded CLEAR. Train 3 was now proceeding with caution towards the tunnel, and K signalled *all clear* to the driver with his white flag.

But S had seen the red flag. He stopped in the tunnel and cautiously reversed his train to find out what was wrong from K.

Train 3 ran into the rear of Train 2 after travelling 250 yards into the tunnel, propelling Train 2 forwards for 50 yards. The chimney of the engine of Train 3 hit the roof of the tunnel 24 feet above. In all 23 passengers were killed and 176 were seriously injured.

Your agenda:

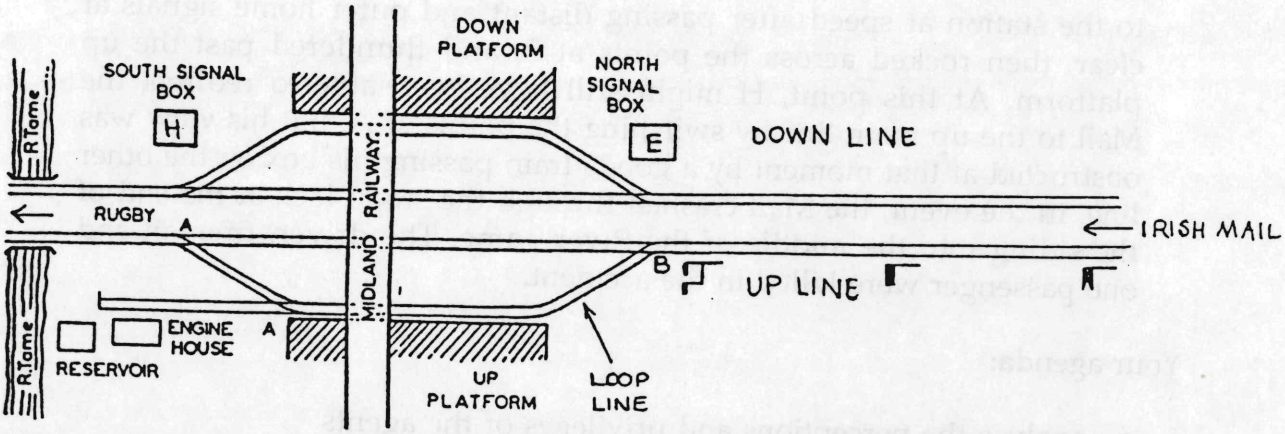
a. analyse the perceptions and privileges of the agents involved
b. discuss the role of knowledge (interpreted perception) in the events
c. what relevance has the mode of operation of the telegraph?
d. what is the role of the automatic signal device?
e. to what extent is time an important factor in the accident

What recommendations would you make for avoiding a recurrence?
What agents do you consider primarily responsible for the accident?
Is it possible / appropriate to write an LSD specification for the agents?
If so, what insight can be gained from this?

Historic Railway Accidents 2

Tamworth **September 4th 1870**

The layout at Tamworth Station in 1870 was as shown below:



The station caters for express trains that don't stop, but the points can also be set so that trains can stop at the platforms. The points at A are interlocked so that when they are set for an express train they are also automatically set for the siding that leads to a dead end near the engine house.

There are two signal boxes, the South manned by Higgins and the North by Evans. H and E cannot see each other because of the station buildings and the Midland railway bridge crossing above the line at right angles. A telegraph has just been installed but is not yet in operation, so that H and E receive no information from each other or elsewhere about approaching trains.

A train that approaches the station on the up line (from the North) passes signals on three occasions, first at the distant and outer home signals, then at the pair of inner home signals indicated above. These can be set by H in the South box, who is also responsible for the points at A. In a reciprocal manner, E has control over the points on the North side of the station. Because the points at B are interlocked with the inner home signal, setting the points at B has the effect of switching the settings of the pair of inner home signals.

The accident

At 3.53 a.m., the signalling arrangements for the arrival of the next train were put in place. H in the South Box, was expecting the late running Irish Mail train. H set the signals on the up line to **clear** and

the points at A to the main line to prepare for the Mail to pass through without stopping. Because his watch had stopped, E was confused about the train schedule, and expected a stopping goods train that would call at the up platform. E set the points at B for the loop line, so that the loop signal was reset to **clear** and the main signal to **stop** on the inner home signal.

The Mail arrived at speed at 4.09 a.m., thirteen minutes late. It came in to the station at speed after passing distant and outer home signals at clear, then rocked across the points at B, and thundered past the up platform. At this point, H might still have been able to redirect the Mail to the up main line by switching the points at A, but his view was obstructed at that moment by a goods train passing his box on the other line. In the event, the Mail crashed through the stop block at the end of the siding into the middle of the River Tame. The driver, fireman and one passenger were killed in the accident.

Your agenda:

a. analyse the perceptions and privileges of the agents
b. what role does time play in the accident?
c. where is knowledge (interpreted perception) involved?
d. what are the most significant environmental factors?
e. would redistribution of privileges between boxes have helped?
f. what interlocking would have helped?
g. had there been a telegraph, what communication was necessary?
h. what assumptions about scheduling could have guaranteed safety?
i. would you hold anyone responsible for the accident?

Can you devise an LSD specification for the signalmen agents?
Can you model the interlocking arrangements as dependencies in EDEN?

Historic Railway Accidents 3

The accidents described on these sheet are comparatively simple in nature. In fact, there are subtleties in them that are quite relevant to concurrency in general, and to issues for LSD specification in particular.

Sonning 1841

The Accident

A regular goods train sets out at 4.30 a.m. from London Paddington to Bristol. The train has the following constitution:

engine, 2 third-class carriages, a parcels van, 17 goods wagons.

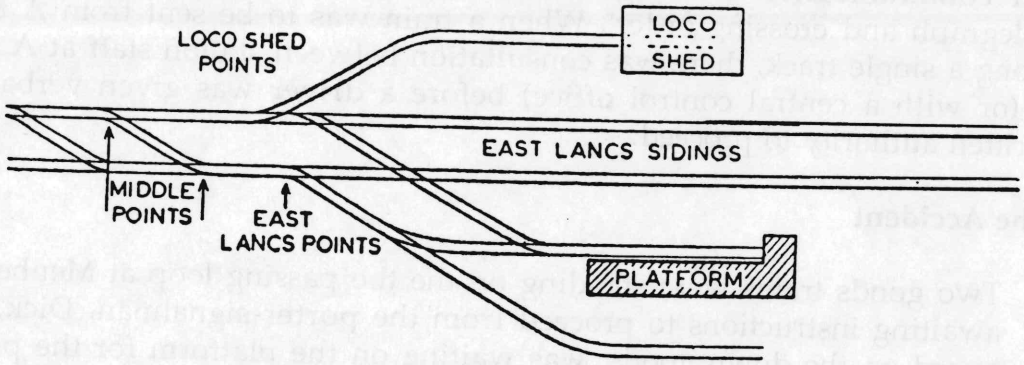
It runs into a landside at Sonning. The weight of the following wagons crushes the carriages against the engine and tender killing 8 passengers, and injuring 17 others. (Most of the casualties were employed in building the new House of Parliament and were returning home for Christmas.)

a. accidents of this nature were commonplace before continuous brakes were developed, and would have probably have been less serious has continuous braking been in operation. The inquiry commented on the absence of spring buffers between third-class carriages.

How would the nature of the braking mechanism and the connection between carriages be reflected in an LSD specification of the agents involved?

Burnley 1852

The layout of Burnley station in 1852 was as shown below:



BURNLEY STATION, 1852

The station is a terminus for a single line. It has no signals, and all the points are manually operated. The East Lancs Points are normally set to the platform, and are weighted in such a way that they have to be held in position with a lever in order to direct trains into the East Lancs

Sidings. The sidings can hold much longer trains however – at most 6 coaches can stand adjacent to the platform.

The Accident

Two school excursions set out from Burnley for York and Goole. Both are enormous double-headed trains of 35 and 45 coaches and have to be sent off and returned to the East Lancs Sidings. At the end of the day, the coaches are to be returned to the sidings by stopping the train before the middle points, uncoupling the locomotives and drawing them ahead into the engine shed, then allowing the coaches to run down the gentle gradient over the middle points and the East Lancs Points into the sidings. An obliging blacksmith Tom Bridge helps out at the station when the trains return, and is delegated to hold over the East Lancs Points by another amateur assistant. The driver of one of the engines coming down the parallel track asks TB to switch the Loco Shed Points. As TB does this, he releases the East Lancs Points, thus redirecting the coaches to the platform, where three children and a teacher are killed in the collision with the buffers.

b. What are the principal agents that are acting in the critical moments leading up to this accident? Can we express their interaction in LSD? How should we express the fact that TB can operate the East Lancs Points and the loco shed points, but can't operate both at once?

c. To what extent can the evolution of interlocking lever mechanisms for distributed control be modelled by definitive principles?

Menheniot on Cornwall Railway **1873**

All communication on single track lines was originally handled by 'telegraph and crossing order'. When a train was to be sent from A to B along a single track, there was consultation between station staff at A and B (or with a central control office) before a driver was given verbal or written authority to proceed.

The Accident

Two goods trains were standing on the the passing loop at Menheniot awaiting instructions to proceed from the porter-signalman. Dick, the guard on the down goods, was waiting on the platform for the p-s to return from the telegraph. When the Line Clear for the down line was confirmed, the p-s put his head round the door and shouted "Right away, Dick".

d. Why was there an accident?
e. In what respect was the signalling inadequate?
f. Discuss the nature of observations we would need to represent this incident using LSD.

Historic Railway Accidents 4

Thorpe-Brundall on Norfolk Railway 10th September 1874

Thorpe and Brundall are adjacent stations on Great Eastern Railway between Norwich and Yarmouth. The single line track was one of the first to be controlled by electric telegraph, and has been managed without mishap for 26 years. It is about to be upgraded to a double track – the track has been laid, but not yet inspected and approved.

The Accident

A regular express train travelling to Yarmouth from London normally passes through Thorpe at 9.00 p.m., then travels on to Brundall, where it crosses with the Mail train running up to London. Tonight it's late, and Thorpe and Brundall are communicating by telegraph to decide whether to hold the Express at Thorpe, so that the Mail can be sent up.

Thorpe Station is manned by a stationmaster, an inspector and a telegraph clerk. The stationmaster is responsible for deciding whether a change to the crossing arrangements is required, the inspector conducts the protocol for changing the arrangements, and the telegraph clerk transmits appropriate messages when authorised. To instruct the clerk, the inspector writes his instruction on a pad that is kept in a sliding window in the telegraph office (cf a booking office). This enables the inspector to patrol the platform and keep in touch with the telegraph office at the same time. Every message has to be signed by the inspector before transmission. A signed instruction is also given to the driver of the train concerned.

The night inspector **C**ooper has just come on duty at 9.16 p.m. The Express has yet to arrive. He consults the stationmaster **S**proule and proposes that they hold the Express so that the Mail can come forward. S doesn't want to do this, and the dialogue goes:

S: "We will not have the Mail up, certainly not."

C: "You know, sir, there is an order allowing us to detain the express as late as 9.35."

S: "All right, we will soon get her off."

C apparently interprets this as

"All right [I concede your point], we will soon get the Mail off".

C goes to the telegraph window and says to **R**obson, the clerk:

"Tell Brundall to send the Mail on to Thorpe".

R writes the message on the pad, but C walks off without signing it. Despite this, R transmits C's verbal message to Brundall as 'signed A. Cooper'. The time is 9.22 p.m.

The Express arrives 1 minute later. The day inspector **P**arker is waiting for it with an order authorising her driver to proceed already prepared.

As C comes up to him, P asks him whether he has arranged for the Mail to come on, to which C replies:

"No, certainly not; let us get the train away as soon as possible".

P then authorises the Express to proceed at 9.30 p.m.

R knows within moments that the Express has left, and confronts C as he returns to cancel the order:

C: "You haven't ordered the Mail up, have you?"

R: "You told me to order her up."

R telegraphs Brundall with the message "Stop Mail", to receive the immediate reply "Mail left". R then puts the pad with C's message in front of Cooper and asks him to sign it:

C: "No, No. I never gave you that message. I did not. I did not."

R: "Why, if you did not, have you come back to cancel it?"

In the collision that resulted, 25 people were killed and 73 injured. At the inquiry, R acknowledged that he was not authorised to send the message:

'I see my error. I did it to oblige C; I never did such a thing before in my life.'

R had a bell with which to summon the inspector if required, but did not like to use it because it made the inspectors angry. C maintained that he had heard the Express approaching as soon as he had given his instruction, that he cancelled it immediately, and that R had acknowledged the cancellation. R denied this.

Your agenda:

a. Analyse the roles and protocols of stationmaster Sproule, inspectors Cooper and Parker, clerk Robson.
b. Could you handle the concept of delegating authority in LSD?
c. Who was the inspector on duty at 9.23pm?
d. Is Cooper's "No certainly not" justified?
   Discuss C's position with reference to commitment to action in LSD.
e. Discuss the nature of the assumptions made by one agent of another in the events leading up to the departure of the Express.
f. Discuss R and C's perceptions of their actions at the inquiry.

In the light of the above issues, is there any prospect of using LSD

- to model the interactions leading up to the departure of the express
- to model these interactions and R and C's responses at the inquiry.

Who would you censure most for the accident?

Historic Railway Accidents 5

Abermule

January 26th 1921

Abermule station is a small country station on the single-line Cambrian railway track from Whitchurch to Aberystwyth on the west coast of Wales. The neighbouring stations are Newtown to the West and Montgomery to the East. Trains can pass each other at Abermule, and the single-line sections of track between Montgomery and Abermule and Abermule and Newtown are protected by the Tyer electric tablet instrument (patented in 1878).

The Tyer instrument at station X resembles an automatic slot machine that is connected by telegraph to a similar machine at the next station Y along the line. A train travelling from X to Y has to receive an XY-tablet from the machine at X before it is authorised to go. The Tyer machines at X and Y ensure that an XY-tablet can only be released from either machine through synchronised action of the operators at X and Y. They are also electrically interlocked so that once an XY-tablet has been withdrawn at X, no XY-tablet can be withdrawn at Y until all the XY-tablets issued at X have been inserted in the machine at Y.

Abermule is manned by the stationmaster **L**ewis, the signalman **J**ones, and two young staff: the porter **R**odgers and the ticket collector **T**hompson. The Tyer machine at Abermule is housed in the instrument room in the station building and not in the signal box. Only L and J are meant to use the machines, but in practice, all the staff do so from time to time.

The Accident

A stopping train that travels East-West from Whitchurch to Aberystwyth is scheduled to cross the West-East Aberystwyth-Manchester express at Abermule shortly before midday. The E-W train has just arrived at Montgomery, and the following sequence of events occurs:

- J at **A**bermule gives **M**ontgomery clearance to release an MA-tablet for the E-W train to come forward. J establishes by telegraph that the express has left Moat Lane, the next station west of Newtown.

  L is at lunch, so only J, R and T know about this event.

- R at **A**bermule gives **N**ewtown clearance to release an NA-tablet for the express to come forward.

  Only T is in the instrument room at the time, as L is in the goods yard, and J has gone to open the level crossing gates for the E-W train.

- R walks to the end of the platform opposite to the signal box to set the points for the express train to enter the passing loop. Before he gets around to this, he is distracted by the arrival of the E-W train.

  Had R set the points, he would have had to ask J to release the lock from the signalbox. In the event, the points are correctly set for the E-W train to leave and J is unaware that the express is expected.

- T meets the E-W train and collects the MA-tablet from the driver. T takes the tablet towards the instrument room, but meets L en route. L asks T where the express is, and T says "just passed Moat Lane". T then goes off to collect tickets and hands L the MA-tablet without further explanation.

  J does not know that the express is on its way. R doesn't expect the E-W train to depart yet. L assumes from his conversation with T that
  - the express is running late,
  - the tablet he has been given is the NA-tablet.

- L returns the MA-tablet to the driver of the E-W train believing it to be the NA-tablet. The driver doesn't check the identity of the tablet, and J signals the train on its way to Newtown.

The engine-men of the E-W train and 15 passengers are killed in the resulting collision. Its takes 50 hours continuous work by a breakdown gang to clear the line. The E-W breakdown train could not proceed from Montgomery to Abermule until the MA-tablet had been recovered from the wreckage. This tablet was discovered by the driver and fireman of the express, both of whom survived the crash with injuries.

Your agenda

a. What are the protocols and privileges of the various agents as laid down by regulation?
b. What are the protocols and privileges of the various agents as exercised in practice?
c. Analyse the knowledge each agent has at each stage as the events occur.
d. Analyse the knowledge that each agent should have had at each stage.
e. Analyse the assumptions the agents make in their communication.
f. Analyse the role that spatial distribution of agents plays in the events.

g. Can you work out what interlocking – recommended by the inquiry – would have prevented this accident? Would that have been foolproof?
h. What would have been the implications had the crew of the Express not been able to recover the MA-tablet?